Уральский государственный юридический университет
АНО “КримЛиб”
Союз криминалистов и криминологов

ТЕХНОЛОГИИ XXI ВЕКА В ЮРИСПРУДЕНЦИИ

5.0

Материалы Пятой международной научно-практической конференции

г. Екатеринбург

19 мая 2023 г.

ФГБОУ ВО
«Уральский государственный юридический университет
имени В. Ф. Яковлева»
АНО «КримЛиб»
Союз криминалистов и криминологов

ТЕХНОЛОГИИ XXI ВЕКА В ЮРИСПРУДЕНЦИИ

**Материалы
Пятой международной
научно-практической конференции
(Екатеринбург, 19 мая 2023 года)**

Екатеринбург
2023

УДК 34
ББК 67
Т38

Рецензенты:

И. Р. Бегишев – доктор юридических наук, доцент, заслуженный юрист Республики Татарстан, главный научный сотрудник Научно-исследовательского института цифровых технологий и права, профессор кафедры уголовного права и процесса Казанского инновационного университета имени В.Г. Тимирясова

А. А. Беляков – доктор юридических наук, профессор, заведующий кафедрой криминалистики Уральского государственного юридического университета имени В. Ф. Яковлева

Ответственный редактор:

Д. В. Бахтеев, доктор юридических наук, доцент, доцент кафедры криминалистики Уральского государственного юридического университета имени В. Ф. Яковлева

Т38 Технологии XXI века в юриспруденции: материалы Пятой международной научно-практической конференции (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. — Екатеринбург: АНО «КримЛиб» — 2023. — 495 с. – 1 CD-ROM. – Систем. требования: 512 MB RAM; Windows XP/Vista/7/8/8.1/10/11; 4,89 Мб свобод. пространства на жест.диске. – Загл. с титул.экрана. – Текст: электронный.

ISBN 978-5-6049815-0-4

В сборнике представлены статьи учёных-юристов, представителей юридической практики и начинающих исследователей, принявших участие в Пятой международной научно-практической конференции «Технологии XXI века в юриспруденции», посвящённой отдельным проблемам юридических науки и практики, связанным с современными технологиями.
Мнение авторов может не совпадать с мнением редакции.

УДК 34
ББК 67

ISBN 978-5-6049815-0-4

Содержание

ТРИБУНА НАЧИНАЮЩИХ ИССЛЕДОВАТЕЛЕЙ

УДК 34.096

Арефинкина Екатерина Геральдовна
кандидат юридических наук
заведующий кафедрой уголовного права и процесса
юридический факультет Сочинского института
Российского университета дружбы народов имени Патриса Лумумбы
(г. Сочи, Россия)
arefinkina@mail.ru

ЦИФРОВИЗАЦИЯ ЮРИДИЧЕСКОЙ ПРОФЕССИИ: РИСКИ, ПОТРЕБНОСТИ И ПЕРСПЕКТИВЫ РЕФОРМИРОВАНИЯ ЮРИДИЧЕСКОГО ОБРАЗОВАНИЯ

Аннотация. В статье рассмотрены перспективы дальнейшей цифровизации юриспруденции, которая оценивается в разрезе возможной замены человеческой деятельности трудом роботизированной техники, а также с позиции дальнейшего внедрения в профессиональную юридическую деятельность новых цифровых технологий. Перспективы вырождения юриспруденции в цифровую эпоху рассматриваются скептически. Вероятнее всего, цифровизация приведёт к качественному преобразованию профессии юриста, что изменит содержание и формы организации профессиональной юридической деятельности. В статье рассматриваются дискуссионные вопросы обучения будущих юристов новым цифровым технологиям, используемым в праве, анализируются проблемы совершенствования учебных программ в целях разумного сочетания в процессе обучения традиционных юридических дисциплин и новых предметов, призванных формировать у студентов базовые знания и навыки в области как правовых, так и цифровых технологий, а также развивать цифровую культуру.

Ключевые слова: цифровизация, цифровые технологии, юриспруденция, роботы, искусственный интеллект, информационные технологии, риски и угрозы цифровизации, цифровые знания, умения и навыки.

Для цитирования:
Арефинкина Е. Г. Цифровизация юридической профессии: риски, потребности и перспективы реформирования юридического образования // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 12–20.

У любых масштабных преобразований, к которым, несомненно, можно отнести цифровую трансформацию общества, какими бы перспективными они не были, всегда есть оборотная сторона. Безусловно, новейшие технологии повышают производительность труда и улучшают качество жизни. Сегодня намного проще, удобнее стало делать копии нужных документов из материалов дела в суде, отслеживать с помощью

соответствующих правовых систем последние изменения в действующем законодательстве или знакомиться с действующей судебной практикой по сложным вопросам, состоявшимися судебными актами по различным категориям дел и пр. Это те новшества, о которых юристы прошлых лет могли только мечтать. Но, с другой стороны, эти же блага технологического развития, безусловно, таят в себе и целый ряд угроз. Например, серьёзно стоит отнестись к перспективе замены человека в некоторых видах деятельности. Такая угроза не обойдёт стороной и юридическую профессию. В юриспруденции сегодня наиболее рутинная и трудоёмкая работа, связанная в первую очередь со сбором и обработкой данных, быстрыми темпами роботизируется, и наметилась серьёзная тенденция расширения сферы машинного труда. Большие обороты в последнее время набирает развитие искусственного интеллекта, который также в перспективе приведёт к сокращению рабочих мест, в том числе и в сфере юриспруденции, потому что многие рутинные функции получаются у компьютерных систем, способных к самообучению, довольно легко, и для работодателя их использование – наилучший способ экономии человеческих и денежных ресурсов. Следовательно, машины могут вытеснить человеческий труд, например, при оформлении ипотеки, приказном судопроизводстве, регистрации большинства юридических лиц и прав на недвижимость, наложении штрафов и арестов, получении разного рода выписок, сдачи налоговых деклараций и отчётов, совершении платежей, заключении простых договоров и в прочих областях, где задачи носят типовой характер. В этих сферах прежде всего и будет происходить полномасштабная цифровизация.

Чтобы оценить, какие угрозы для будущего юридической профессии несёт в себе этот глобальный процесс, нужно понимать, что именно он из себя представляет не гипотетически, а на основе анализа реальных технологий, имеющихся на данный момент или находящихся в разработке. Одним из наиболее известных проявлений цифровизации юридической деятельности является LegalTech. Обобщённо, LegalTech означает использование информационных технологий, онлайн-сервисов и специального программного обеспечения для повышения эффективности юридической деятельности[1]. В качестве примеров программ данного сегмента на российском рынке можно назвать, например:

– Casebook – сервис мониторинга судебных дел и контроля за деятельностью контрагентов;

– Caselook – инструмент для поиска и анализа судебной практики;

– Case.pro – система автоматизации юридических процессов;

[1] Певцова Е. А., Соколов Н. Я. Профессиональное поведение юристов в электронном государстве в случаях несовершенства законодательства // Журнал российского права. 2018. № 6. С. 42.

– Юрайт – программа для учёта судебных дел и претензионно-исковой работы;

– FreshDoc – онлайн-конструктор документов и т. д [2].

Наиболее известным широкому пользователю и давно вошедшим в практику примером информационных технологий в юриспруденции являются справочные правовые системы, такие как «КонсультантПлюс», «Гарант», «Кодекс» и т. д. Они представляют собой обширные базы данных, включающие материалы официального законодательства и судебной практики, и оснащены развёрнутой системой поиска по отдельным реквизитам.

Юристы без всяких сомнений должны оптимизировать свои процессы, а это без применения современных технологий невозможно. Следовательно, работа юристов в ближайшей перспективе будет становиться всё более технологичной. Это избавит специалистов указанной сферы, как уже отмечалось выше, от рутинной работы, существенно сократит расходы на юридические услуги и исключит свойственные человеку ошибки. Технологии позволяют не только анализировать прошлое и настоящее, но и определять будущее. На основе анализа больших данных юристы могут, например, строить свои стратегии ведения конкретного дела или вообще принять решение разрешить спор в досудебном порядке. Дополнительно можно было бы избежать правовых ошибок и описок при формировании решений, поскольку система гораздо меньше подвержена риску допустить элементарную опечатку, нежели человек.

При этом, считаем, что только синергия человеческого интеллекта и компьютерных алгоритмов способна вывести процесс аналитики и принятия решений на новый уровень. Цифровизация – это лишь средство. Без человеческой эрудиции, опыта, даже при наличии необходимых технических ресурсов она безжизненна. Кроме того, «автоматизация анализа информации вовсе не означает автоматизацию принятия решений на основе этой информации»[3]. Человеческий надзор за аналитической деятельностью искусственного интеллекта необходим, причём осуществлять такой контроль должны высокопрофессиональные специалисты со стажем и опытом. Можно ожидать, что со временем необходимость участия человека в принятии определённых решений будет прямо закреплена в законе.

В современных условиях нужно говорить об изменении содержания юридического труда. Появление новых требований к работникам и новых компетенций, прежде всего в области

[2] Гайворонская Я. В., Каримова Ю. И. Цифровизация юридической профессии: о рисках и угрозах цифровизации рынка труда // Advances in law studies. Т. 8. № 5. 2020. С. 60.

[3] Демиденко Д. Робот-адвокат: как юристам не остаться без работы // Forbes [Электронный ресурс]. 2017, 24 апреля. URL: https://www.forbes.ru/kompanii/343269-robot-advokat-kak-yuristam-ne-ostatsya-bez-raboty (дата обращения: 12.05.2023).

компьютерных и информационных технологий, а также новых методов организации юридической работы – это те реальные изменения юридической профессии, которые происходят уже сейчас, и удельный вес которых будет нарастать в ближайшее время. Современные юристы должны разбираться в информационных технологиях, использовать их в своей профессиональной деятельности и уметь с их помощью регулировать общественные отношения[4]. Цифровая трансформация юридической профессии – это не столько количественные изменения (хотя они, несомненно, есть), связанные с числом востребованных в отрасли работников, доходностью юридического бизнеса или распространённостью в обществе соответствующих услуг, сколько качественные, связанные с изменением содержания и форм организации профессиональной юридической деятельности. Юриста будет тяжело представить без ИТ-помощников: систем, обрабатывающих значительные объёмы информации, автоматически анализирующих судебную практику, подбирающих возможные аргументы для усиления позиции стороны в суде и формирующих простые договорные документы. Сейчас много сил уходит на поиск и анализ нужной информации, отслеживание изменений в законодательстве и судебной практике по различным источникам, а в будущем фокус внимания юриста должен переместиться в область управления юридическими рисками, а не просто информирование лиц о потенциальных опасностях или о том, как правильно поступить в конкретной ситуации.

При этом, в свете сказанного выше одной из первоочерёдных задач в сфере юридического образования становится необходимость перехода в процессе обучения от теории к практике. Все практические и семинарские занятия по практико-ориентированным юридическим дисциплинам нужно перестать проводить в основном на основе абстрактных теоретических заданий, предложенных сборниками, практикумами, задачниками, пособиями и т. п. Причин этому несколько:

1) Во-первых, зачастую, эти задания носят устаревший характер.

2) Во-вторых, можно много раз разобрать ситуацию, предложенную в сжатой форме, без конкретных материалов дела, деталей и т. п., но это не заменит конкретного практического анализа ситуации, совершения конкретных действий по разрешению казуса. Для того чтобы знать, как действовать в определённой правовой ситуации, нужно практически до автоматизма довести алгоритм совершения конкретных действий на практике. Именно тогда студент по окончании юридического факультета будет сразу востребован у потенциальных работодателей. На сегодняшний же день ситуация обстоит совершенно иначе. Получить юридическое образование, которое достаточно массово распространено,

[4] Храмцова Н. Г., Майборода Т. Ю. Подходы к развитию цифровых компетенций студентов юридических вузов // Перспективы науки и образования. 2019. № 1 (37). С. 86.

стало просто, а вот реализоваться в профессии – сложно, так как сегодня будущие юристы в вузе получают много теоретических и гораздо меньше практических, реально востребованных в юридической работе знаний, умений и навыков.

3) В–третьих, сегодня нужно уметь анализировать современную практику, новый материал, который предлагают действующие юристы-практики и диктуют масштабные социально-экономические изменения, влияющие в том числе и на правовую сферу, а не «избитые» правовые ситуации, предложенные авторами сборников и тысячу раз решённые студентами предыдущих лет обучения.

Внедрение цифровых технологий в сферу юридической деятельности и юридического образования бросает вызов юриспруденции. Готово ли сегодня юридическое образование выдержать его достойно? Как должны развиваться юридические знания, навыки и компетенции? Как следует преподавать новые и традиционные правовые дисциплины? Помогут ли эти знания получить работу, и если да, то какую? Расширит ли обучение IT-технологиям в праве возможности будущих юристов? Каковы цели юридического образования и задачи юридических вузов в «эпоху цифры»? – Вот неполный перечень вопросов, возникающих перед юридическими образовательными учреждениями и юридической наукой, обществом и государством[5].

Можно с уверенностью сказать, что, хотя большинству специалистов в сфере юриспруденции (как и профессионалам в других областях) следует иметь базовые знания о технологиях, существуют веские причины для юристов и студентов юридических вузов хорошо задуматься, прежде чем прилагать значительные усилия для получения знаний и навыков в сфере технологий, если они не планируют работать в качестве аналитиков или «инженеров-юристов», участвуя в разработке юридических технологий наравне с программистами или в составе междисциплинарных команд. Как видим, юридическое образование столкнулось сегодня с дилеммой: является ли основной задачей юридических образовательных учреждений подготовка юристов для профессиональной практики на основе знания новых цифровых технологий или обучение дисциплинам права остаётся по-прежнему ключевой задачей? С одной стороны, юридические школы должны быть местом, где можно пробовать идеи и внедрять инновации. С другой – получение юридического диплома обязывает выпускника сосредоточиться на том, что должны уметь делать классические юристы, а также на знаниях, которые позволят им легко ориентироваться в правовых источниках и различных базах данных, чтобы за считаные секунды получить необходимые ответы, в том числе с помощью искусственного интеллекта[6].

[5] Алферова Е. В. Дилеммы юридического образования в контексте цифровизации // Право и управление. 2022. Том 18. № 2.С. 21.

[6] Алферова Е. В. Дилеммы юридического образования в контексте цифровизации // Право и управление. 2022. Том 18. № 2. С. 23.

Представляется, что будущих юристов надо учить пользоваться информацией – и это важнее штудирования законов; учить ориентироваться в развивающихся цифровых условиях: в новом программном обеспечении, аналитических технологиях и платформах отчётности; осваивать несвойственные юриспруденции сферы знаний, чтобы быть конкурентоспособными на рынке труда; в учебную программу вузов включать дисциплины, позволяющие обучающемуся приобрести навыки в сфере новых технологий, в том числе сбор доказательств в сети, обеспечение кибербезопасности, электронное делопроизводство и др. Однако остаётся дискуссионным вопрос: до какого уровня надо погружать обучающегося в цифровые технологии, чтобы не допустить в будущем «ловушки компьютеризации»[7]. С точки зрения профессора М. А. Рожковой, «юристу, если он хочет стать продвинутым специалистом, нужно получить хорошее базовое образование и постоянно совершенствоваться, а вот становится программером в надежде, что это поможет стать успешным юристом, точно не стоит… ему нужны минимальные технические познания и элементарная заинтересованность в том, чтобы получать такие знания»[8]. Есть и такая сторона инноваций в юридическом образовании, которую описывают профессора А. В. Малько и А. Ю. Соломатин, – «бездумное использование компьютерных технологий». Одна из проблем здесь, по их мнению, – «научение студента навыкам интеллектуального труда»: «Интернет при его массовом использовании отучает от самостоятельного чтения книг, справочников, энциклопедий, от библиографической работы, самостоятельного научного поиска. Он заменяет оригинальную информацию из письменных источников некой усредненной (это в лучшем случае), а то и просто непроверенной, которая ошибочно воспринимается пользователями как абсолютная истина»[9]. Можно с грустью констатировать, что во многих отраслях уже наблюдается дефицит не искусственного, а естественного интеллекта. Анализ показывает, что разброс мнений и предложений по реализации задач юридического образования в условиях цифровизации – значительный, но пока нет ни одного

[7] Согомонян А. Юрист будущего: заучивать законы и кодексы больше нет нужды? // Информационно-правовой портал «ГАРАНТ.РУ» [Электронный ресурс]. 2017, 15 ноября. URL: https://www.garant.ru/article/1148675/ (дата обращения: 14.05.2023).

[8] «Новые юристы»: Какие специалисты нужны цифровой экономике: интервью с членом экспертного Совета комитета Госдумы по информационной политике, информационным технологиям и связи, профессор БФУ им. И. Канта М. А. Рожковой // РИА.Новости [Электронный ресурс]. 2019, 26 июня. URL: https://na.ria.ru/20190628/1555973745.html (дата обращения: 14.05.2023).

[9] Малько А. В., Соломатин А. Ю. Юридическое образование в глобализирующемся мире // Известия высших учебных заведений. Правоведение. 2017. № 5 (334). С. 28.

чёткого и хотя бы относительно согласованного решения.

Сегодня мы имеем дело не только с новаторскими достижениями в области цифровизации, но и с первыми значительными изменениями в обучении будущих юристов. Всё это новая и неизвестная «территория» как для студентов, так и для преподавателей юридических вузов, которые сегодня коллективно сталкиваются с описанными выше проблемами при организации образовательных процессах в своих группах и т. п.

Следует также отметить, что дистанционные технологии во многом изменили социальный статус преподавателя. Учёная степень и звание, ранее являющиеся показателем уровня подготовки преподавателя, отступают на второй план. Теперь востребованность предопределяется степенью интересности для студентов. Обучаемый в виртуальной среде не испытывает эмоций по отношению к преподавателю, это в свою очередь изменяет и отношение к изучаемому предмету, так как в традиционной системе интерес к дисциплине во многом формирует личность педагога. Если традиционная форма образования консолидировала студенческое сообщество, социализируя всех обучающихся, то цифровая, дистанционная форма, наоборот, изолирует студентов друг от друга. В случаях подготовки юристов это отрицательный фактор, так как одним из качеств представителей данного профессионального сообщества является умение взаимодействовать в системе «человек-человек». Развитие коммуникативных компетенций общения в реальном и виртуальном пространствах – это ещё одна из задач современного юридического образования. Живое общение студента и преподавателя, а также контакты в виртуальной среде должны быть сбалансированы и определяться учебными планами, равно как и лекционные, семинарские занятия.

До сих пор не выстроена концепция влияния новых технологий на образование и их рационального использования в учебном процессе. Нет консенсуса относительно воздействия цифровых технологий на отрасли права. Вместе с тем ясно, что это не просто модная тема, которая со временем исчезнет, а важное направление развития юридического образования и юридической практики. Можно выделить следующие важные тенденции, которые необходимо внедрить в современное юридическое образование:

1) междисциплинарность;
2) взаимодействие со специалистами из других областей;
3) освоение навыков программирования;
4) непрерывное образование и профессиональная подготовка.

Предугадать, каким будет юридическое образование через 10–20 лет, на сегодняшний день – нелёгкая задача. В условиях столь непредсказуемого будущего вузам необходимо подумать о том, как обучить студентов широкому набору цифровых навыков. Юрист цифровой эпохи – человек, способный работать не только в реальном, но и виртуальном пространстве. У академического юридического

образования есть два варианта: придерживаться своей традиционной функции преподавания основных правовых знаний или активно и творчески взаимодействовать с меняющейся средой, совершенствоваться вместе с меняющейся реальностью.

Список литературы

1. Алферова Е. В. Дилеммы юридического образования в контексте цифровизации // Право и управление. 2022. Том 18. № 2. С. 14–21.

2. Гайворонская Я. В., Каримова Ю. И. Цифровизация юридической профессии: о рисках и угрозах цифровизации рынка труда // Advances in law studies. 2020. Т. 8. № 5. С. 55–63.

3. Малько А. В., Соломатин А. Ю. Юридическое образование в глобализирующемся мире // Известия высших учебных заведений. Правоведение. 2017. № 5 (334). С. 16–31.

4. Певцова Е. А., Соколов Н. Я. Профессиональное поведение юристов в электронном государстве в случаях несовершенства законодательства // Журнал российского права. 2018. № 6. С. 40–49.

5. Храмцова Н. Г., Майборода Т. Ю. Подходы к развитию цифровых компетенций студентов юридических вузов // Перспективы науки и образования. 2019. № 1 (37). С. 80–93.

Ekaterina G. Arefinkina
PhD in Law, Associate Professor,
head of the Criminal Law and Process Department
Sochi Institute (branch) of the Russian University of
Peoples' Friendship named after Patrice Lumumba
(Sochi, Russia)
arefinkina@mail.ru

DIGITALIZATION OF THE LEGAL PROFESSION: RISKS AND NEEDS, PROSPECTS FOR REFORMING LEGAL EDUCATION

Abstract. The article discusses the prospects for further digitalization of jurisprudence, which is assessed in the context of the possible replacement of human activity by the work of robotic technology, as well as from the perspective of further introduction of new digital technologies into professional legal activity. Prospects for the degeneration of jurisprudence in the digital age are viewed skeptically. Most likely, digitalization will lead to a qualitative transformation of the legal profession, which will change the content and forms of organization of professional legal activity. The article discusses the controversial issues of teaching future lawyers new digital technologies used in law, analyzes the problems of improving curricula in order to intelligently combine traditional legal disciplines and new subjects in the learning process, designed

to form students' basic knowledge and skills in the field of both legal and digital technologies, as well as the development of digital culture.

Keywords: digitalization, digital technologies, law, robots, artificial intelligence, information technologies, risks and threats of digitalization, digital knowledge, skills and abilities.

УДК 343.98

Бадоян Сашик Маджитович
старший преподаватель кафедры
правосудия и правоохранительной деятельности
института права и управления,
Тульский государственный университет
(г. Тула, Российская Федерация)
Sashik_171@mail.ru

К ВОПРОСУ О ПРОТИВОДЕЙСТВИИ РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИЗГОТОВЛЕНИЕМ И ОБОРОТОМ МАТЕРИАЛОВ ИЛИ ПРЕДМЕТОВ С ПОРНОГРАФИЧЕСКИМИ ИЗОБРАЖЕНИЯМИ НЕСОВЕРШЕННОЛЕТНИХ

Аннотация: В статье рассмотрены некоторые особенности сокрытия преступлений, связанных с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних. Определены отдельные способы сокрытия изготовления и оборота детской порнографии, которые реализуются уже на этапе подготовки к совершению таких преступлений. Особое внимание уделено возможным активным действиям преступников, направленным на сокрытие цифровых следов совершения или подготовки рассматриваемого вида преступлений. К числу таковых отнесены: обеспечение анонимности (обезличивания) личности преступника, уничтожение различными способами цифровых следов и их носителей, установка программного обеспечения, уничтожающего хранящуюся в памяти компьютерного устройства информацию при несанкционированном доступе к нему, использование для соединения и передачи цифровых данных сетей Wi-Fi в общественных местах, использование для совершения преступлений специальных компьютеров, смартфонов, роутеров с последующим их утаиванием, использование программного обеспечения, позволяющего скрывать или подменять IP-адрес пользователя, его местонахождение, шифровать интернет-трафик, а также осуществлять доступ к ресурсам и взаимодействие с другими пользователями в теневом сегменте Интернета. Помимо этого, рассмотрены традиционные способы противодействия расследованию: переезд лиц в другие субъекты или выезд из страны, попытки использования в целях противодействия расследованию должностного или служебного положения, воздействие на соучастников, свидетелей, потерпевших с целью не допустить сообщения ими сведений о факте совершённого преступления, заставить их давать ложные показания об обстоятельствах совершения и причастных лицах.

Автором сделан вывод, что типовые сведения о способах совершения и сокрытия изготовления и оборота материалов или предметов с порнографическими изображениями несовершеннолетних связаны с иными составляющими соответствующей криминалистической характеристики.

Ключевые слова: сокрытие следов, порнографические материалы с изображениями несовершеннолетних, предметы с изображениями несовершеннолетних, сеть Интернет, сокрытие преступлений, противодействие расследованию.

Для цитирования:
Бадоян С. М. К вопросу о противодействии расследованию преступлений, связанных с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 21–28.

Противодействие раскрытию и расследованию преступлений давно и активно изучается криминалистикой. Более того, на сегодняшний день можно с уверенностью констатировать существование самостоятельного частного криминалистического учения, содержащего комплекс теоретических положений, описывающих рассматриваемое явление в целом и его отдельные формы, в числе которых особо выделяется сокрытие преступных деяний.

Существенный вклад в развитие учения о противодействии раскрытию и расследованию преступлений и его преодолении внесли многие учёные-криминалисты. За последние три десятилетия этой проблематике посвятили свои труды А. С. Андреев, Э. У. Бабаева, Р. С. Белкин, А. В. Варданян, А. Ф. Волынский, Б. Я. Гаврилов, Ю. П. Гармаев, А. Ю. Головин, О. П. Грибунов, В. Н. Карагодин, Д. В. Ким, А. М. Кустов, В. П. Лавров, А. Ф. Лубин, И. А. Николайчук, И. В. Тишутина, В. В. Трухачев и многие другие авторы[1]. При этом, впрочем, ряд базовых положений этого учения остаются объектом научных дискуссий.

Не ставя цель освещать в рамках настоящего исследования различные взгляды на сущность и содержание противодействия раскрытию и расследованию преступлений и учитывая проведенные в новейшей криминалистической литературе обобщения позиций по указанному вопросу[2], полагаем возможным определить противодействие

[1] См., например: Белкин Р. С. Противодействие расследованию и пути его преодоления // Криминалистика; под ред. А. Ф. Волынского. М.: Закон и право, Юнити-Дана, 1999. С. 240; Головин А. Ю., Грибунов О. П., Бибиков А. А. Криминалистические методы преодоления противодействия расследованию транспортных преступлений. Иркутск: ВСИ МВД России, 2015. 164 с.; Волынский А. Ф. О способах противодействия расследованию экономических преступлений // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4–2. С. 29; Тишутина И. В. Противодействие расследованию организованной преступной деятельности: теория и практика выявления и преодоления. М.: Юрлитинформ, 2012. 346 с.

[2] Варданян А. В. Противодействие предварительному расследованию: в продолжение научной дискуссии // Вестник Восточно-Сибирского института МВД России. 2021. № 1. С. 143.

раскрытию и расследованию преступной деятельности по изготовлению и обороту материалов или предметов с порнографическими изображениями несовершеннолетних как реализуемую путём сокрытия следов или в иных формах умышленную деятельность преступников или других связанных с ними лиц, направленную на воспрепятствование выявлению факта совершения преступлений рассматриваемого вида, установлению лиц, их совершивших, и доказыванию их вины, а также достижению других целей предварительного расследования.

Реализуемые по отдельности и в комплексе способы сокрытия изготовления и оборота материалов или предметов с порнографическими изображениями несовершеннолетних, а также сопутствующей преступной деятельности, выступают основной формой рассматриваемого противодействия и обладают существенной криминалистической спецификой.

Во-первых, как показывают результаты проведённого эмпирического исследования, отдельные способы сокрытия изготовления и (или) оборота материалов или предметов с порнографическими изображениями несовершеннолетних реализуются уже на этапе подготовки к совершению таких преступлений.

Во-вторых, в целях сокрытия изготовления и (или) оборота материалов или предметов с порнографическими изображениями несовершеннолетних и сопутствующей преступной деятельности преступниками могут совершаться другие более тяжкие преступления, в том числе убийства.

Так действовал 27-летний житель Красноярского края. Встретив в вечернее время на улице двух малолетних мальчиков, преступник обманным путём завел детей в лес, где предложил им сфотографироваться в обнажённом виде. Преступник не смог реализовать криминальный замысел, однако услышав обещание детей рассказать родителям о происшедшем, в целях сокрытия своей преступной деятельности совершил их убийство и закопал тела в лесу[3].

В-третьих, высокая доля преступлений рассматриваемого вида, совершаемых с использованием компьютерной и телекоммуникационной техники и технологий, обусловливает активные действия преступников, направленные на сокрытие цифровых (компьютерных, виртуальных) следов таких деяний. Основываясь на трудах учёных-криминалистов, затрагивающих вопросы сокрытия цифровых следов и компьютерной информации[4], анализе эмпирического

[3] В Красноярском крае перед судом предстанет местный житель, обвиняемый в убийстве малолетних детей // Официальный Следственного комитета РФ [Электронный ресурс]. 2013, 21 февраля. URL: https://sledcom.ru/news/item/582059/ (дата обращения: 14.04.2023).

[4] Головин А. Ю., Давыдов В. О. Значение виртуальных следов в расследовании преступлений экстремистского характера // Известия Тульского государственного

материала, можно выделить следующие способы такого сокрытия:

– Обеспечение анонимности (обезличивания) личности преступника. Например, в социальных сетях, мессенджерах, на различных сайтах, облачных хранилищах данных преступники, как правило, регистрируются и действуют под вымышленными именами и фамилиями, виртуальными псевдонимами (так называемыми никнеймами или никами) либо случайным набором букв, цифр и символов. Указанный способ, по сути, стал типовым для сокрытия киберпреступлений, совершаемых с использованием социальных сетей. Как справедливо отмечает Ю. П. Гармаев, особенностью совершения преступления в социальной сети является механизм сокрытия самого злоумышленника, поскольку одной из особенностей действий в пространстве является именно их непрямой характер, сопряжённый с обезличенностью и анонимностью[5]. Добавим, что при регистрации в социальных сетях и других ресурсах преступники также могут предоставлять ложные сведения, использовать номера мобильной связи, оформленные на других лиц, в том числе подставных.

– Создание в криминальных целях адресов электронной почты, использование сайтов и других ресурсов, переправляющих сообщения с одного адреса электронной почты на другой (ремейлеров), с уничтожением информации о реальном отправителе.

– Использование программного обеспечения, позволяющего скрывать или подменять IP-адрес пользователя, его местонахождение, шифровать интернет-трафик, а также осуществлять доступ к ресурсам и взаимодействие с другими пользователями в теневом сегменте Интернета (различные VPN-сервисы и другие программы-анонимайзеры, TOR Browser и пр.).

– Маскировка ресурсов, содержащих или транслирующих материалы с порнографическими изображениями несовершеннолетних, под легальный контент.

– Маскировка (сокрытие) лица на распространяемых фотоснимках или в кадре путём «размытия» изображения, наложения «мозаики» и пр. Данной метод применяется при съёмке преступником детской порнографии с собственным участием в кадре.

– Уничтожение различными способами цифровых следов и их носителей.

– Хранение файлов с порнографическими изображениями несовершеннолетних, иной цифровой информацией о совершённых преступлениях на внешних носителях данных (съёмных дисках, flash-картах,

университета. Экономические и юридические науки. 2016. № 3. С. 256.

[5] Гармаев Ю. П. Противодействие уголовному преследованию по уголовным делам о киберпреступлениях и средства его преодоления: проблемы теории и дидактики // Цифровые технологии в юриспруденции: генезис и перспективы. Материалы I Международной межвузовской научно-практической конференции. Красноярск, 2020. С. 34.

облачных хранилищах данных и пр.) и их сокрытие, в том числе в тайниках.

– Шифрование (кодирование) доступа к компьютерам, смартфонам и иным устройствам, использовавшимся в целях изготовления или оборота материалов с порнографическими изображениями несовершеннолетних, сайтам, облачным хранилищам данных, запоминающим устройствам, на которых размещены такие изображения, создание криптоконтейнеров[6] для хранения файлов и т. п.

– Установка программного обеспечения, уничтожающего хранящуюся в памяти компьютерного устройства информацию при несанкционированном доступе к нему.

– Использование в целях криминального общения и пересылки данных сторонних программ, например, диалоговых окон в онлайн-играх.

– Включение использующих мобильное соединение устройств и передачу цифровых данных из различных мест на короткий период времени.

– Использование для соединения и передачи цифровых данных сетей Wi-Fi в общественных местах.

– Использование для совершения преступлений специальных компьютеров, смартфонов, роутеров с последующим их утаиванием.

Преступниками могут реализовываться и другие способы сокрытия цифровых следов и криминального общения с использованием современных телекоммуникационных технологий.

Добавим также, что изготовление детской порнографии может маскироваться под фотосессии, кастинги, деятельность фотостудий, модельных агентств и т. п. Реализация таких материалов или предметов может осуществляться в торговых точках продажи печатной продукции, видеофильмов, программного обеспечения, компьютерной техники и пр. с маскировкой под легальный товар. В случае распространения порнографических материалов или предметов с изображением несовершеннолетних либо привлечения несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера преступниками может утаиваться или фальсифицироваться информация о реальном возрасте несовершеннолетних.

Необходимо отметить и некоторые другие способы противодействия возможному или осуществляемому расследованию преступлений рассматриваемого вида. Так, в следственной практике встречались попытки переезда лиц, совершивших такие деяния, в другие регионы страны или выезда в другие

[6] Криптоконтейнер – создаваемый с использованием специального программного обеспечения (например, DriveCrypt, TrurCrypt, PGCrypt и пр.) логический диск, хранящий файлы в зашифрованном виде. Чтобы увидеть файлы, требуется ввести пароль / ключ. Может иметь многоуровневое кодирование («двойное дно») и устойчив к взлому.

государства, попытки использования в целях противодействия расследованию должностного или служебного положения. Кроме того, имеют место случаи воздействия на потерпевших, свидетелей, других соучастников преступлений в целях не допустить с их стороны сообщения о факте таких преступлений, заставить их давать ложные показания об обстоятельствах таких деяний и лицах, причастных к их совершению.

Примером тому может служить получившее широкий общественный резонанс уголовное дело в отношении группы лиц, включавшей в свой состав бывших директора, сотрудников и воспитанников школы-интерната в г. Санкт-Петербург, совершивших в период 2002–2017 годов десятки преступлений, предусмотренных статьями 132 и 242.1 УК РФ, в отношении несовершеннолетних воспитанников этого учреждения. В ходе расследования, помимо прочего, в отношении отдельных обвиняемых и связанных с ними лиц было возбуждено уголовное дело по ч. 2. ст. 309 УК РФ по фактам принуждения потерпевших к даче ложных показаний, уклонению от дачи показаний путём шантажа и угроз убийством[7].

Также в следственно-судебной практике встречаются преследующие цель уклонения от уголовной ответственности случаи симуляции обвиняемыми по рассматриваемой категории болезней, в том числе психических расстройств, обвинений правоохранительных органов в провокациях распространения порнографических материалов.

Система типовых сведений о способах совершения и сокрытия изготовления и оборота материалов или предметов с порнографическими изображениями несовершеннолетних коррелирует в структуре криминалистической характеристики с другими данными об элементах преступной деятельности рассматриваемого вида. Особое значение имеют научно обобщённые сведения о субъектах совершения преступлений рассматриваемого вида, потерпевших и иных элементах механизма таких деяний.

Список литературы

1. Белкин Р. С. Противодействие расследованию и пути его преодоления // Криминалистика; под ред. А. Ф. Волынского. М.: Закон и право, Юнити-Дана, 1999. 615 с.

2. Варданян А. В. Противодействие предварительному расследованию: в продолжение научной дискуссии // Вестник Восточно-Сибирского института МВД России. 2021. № 1. С. 137–145.

[7] В Санкт-Петербурге перед судом предстанут экс-директор школы и его соучастники, обвиняемые в совершении преступлений против половой неприкосновенности детдомовцев // Официальный Следственного комитета РФ [Электронный ресурс]. 2018, 6 декабря. URL: https://sledcom.ru/news/item/1278085/ (дата обращения: 14.04.2023).

3. Волынский А. Ф. О способах противодействия расследованию экономических преступлений // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4–2. С. 27–36.

4. Гармаев Ю. П. Противодействие уголовному преследованию по уголовным делам о киберпреступлениях и средства его преодоления: проблемы теории и дидактики // Цифровые технологии в юриспруденции: генезис и перспективы. Материалы I Международной межвузовской научно-практической конференции. Красноярск, 2020. С. 29–35.

5. Головин А. Ю., Грибунов О. П., Бибиков А. А. Криминалистические методы преодоления противодействия расследованию транспортных преступлений. Иркутск: ВСИ МВД России, 2015. 164 с.

6. Головин А. Ю., Давыдов В. О. Значение виртуальных следов в расследовании преступлений экстремистского характера // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3. С. 254–259.

7. Тишутина И. В. Противодействие расследованию организованной преступной деятельности: теория и практика выявления и преодоления. М.: Юрлитинформ, 2012. 346 с.

Sashik M. Badoyan
Senior Lecturer of the Department
of Justice and Law Enforcement at the
Institute of Law and Management
Tula State University
(Tula, Russian Federation)
Sashik_171@mail.ru

ON THE ISSUE OF COUNTERING THE INVESTIGATION OF CRIMES RELATED TO THE PRODUCTION AND TRAFFICKING OF MATERIALS OR OBJECTS WITH PORNOGRAPHIC IMAGES OF MINORS

Abstract. In the article, the author defines counteraction to the disclosure and investigation of criminal activity in the manufacture and circulation of materials or objects with pornographic images of minors as realized, by hiding traces or in other forms, the deliberate activity of criminals or other persons associated with them, aimed at preventing the detection of the fact of committing crimes under consideration type, identifying the persons who committed them and proving their guilt, as well as achieving other goals of the preliminary investigation. Implemented individually and in combination, methods of concealing the manufacture and circulation of materials or objects with pornographic images of minors, as well as related criminal activities, are the main form of the counteraction in question and have significant forensic specifics. The

author emphasizes that the methods of concealing the manufacture and circulation of materials or objects with pornographic images of minors, as well as related criminal activity, are the main form of the counteraction in question and have significant forensic specificity. Also that a high proportion of crimes of this type, committed using computer and telecommunications equipment and technologies, determines the active actions of criminals aimed at hiding digital (computer, virtual) traces of such acts. For example, ensuring the anonymity (depersonalization) of the identity of the offender, the destruction of digital traces and their media in various ways, the installation of software that destroys information stored in the memory of a computer device in case of unauthorized access to it, the use of Wi-Fi networks in public places to connect and transmit digital data , the use of special computers, smartphones, routers to commit crimes with their subsequent concealment, the use of software that allows you to hide or replace the user's IP address, location, encrypt Internet traffic, as well as access resources and interact with other users in the shadow segment of the Internet and other actions.

The author concluded that typical information about the methods of committing and concealing the manufacture and circulation of materials or objects with pornographic images of minors correlates in the structure of the forensic characteristics of such acts with other data on the elements of criminal activity of the type in question.

Keywords: concealment of traces, pornographic materials or objects with images of minors, the Internet, concealment of crimes, counteraction to the investigation of crimes.

УДК 378.1

Балдин Александр Константинович
Кандидат юридических наук, доцент кафедры
гражданского права и процесса юридического факультета
Национальный исследовательский Нижегородский государственный университет
имени Н. И. Лобачевского
(г. Нижний Новгород, Российская Федерация)
akbaldin@unn.ru

Биюшкина Надежда Иосифовна
Доктор юридических наук, профессор, заведующий кафедрой судебной и
прокурорской деятельности юридического факультета
Национальный исследовательский Нижегородский государственный университет
имени Н. И. Лобачевского
(г. Нижний Новгород, Российская Федерация)
asya_biyushkina1@list.ru

ЭЛЕКТРОННАЯ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНАЯ СРЕДА КАК ЭЛЕМЕНТ ИНФОРМАЦИОННОЙ ОТКРЫТОСТИ УНИВЕРСИТЕТА

Аннотация. в статье рассматриваются вопросы формирования, внедрения и развития электронной информационно-образовательной среды высшего учебного заведения как одного из элементов его информационной открытости. Проведён краткий анализ действующего законодательства, регламентирующего данный институт. На примере конкретной образовательной организации раскрыта структура электронной информационно-образовательной среды (ЭИОС), исследованы её элементы, подтверждена зависимость качества образовательного процесса от наличия эффективно функционирующей ЭИОС.

Ключевые слова: электронная информационно-образовательная среда, образовательное пространство, информационное пространство университета, электронная библиотека, электронные ресурсы, электронное обучение, дистанционные образовательные технологии.

Для цитирования:
Балдин А. К., Биюшкина Н. И. Электронная информационно-образовательная среда как элемент информационной открытости университета // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 29–36.

В настоящее время информационная открытость высшего учебного заведения предполагает обязательное формирование электронной информационно-образовательной среды (ЭИОС), обеспечивающей доступ обучающихся и научно-педагогических работников к

информационно-образовательным ресурсам, создание коммуникационной площадки между обучающимися и педагогическими работниками, реализацию индивидуальной образовательной траектории с учётом особенностей и образовательных потребностей конкретного обучающегося. ЭИОС призвана способствовать функционированию механизмов и процедур мониторинга качества образовательного процесса.

Помимо объективных причин появления в университетах электронной информационно-образовательной среды, связанных со всеобщей цифровизацией различных сфер жизни, её наличие в образовательном пространстве обусловлено законодательными требованиями. ЭИОС тесно связана с понятием «электронное обучение», под которым подразумевается «организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников»[1]. На основании п. 3 ст. 16 Федерального закона «Об образовании в Российской Федерации»[2] ВУЗами при реализации образовательных программ с применением электронного обучения, дистанционных образовательных технологий должны быть созданы условия для функционирования электронной информационно-образовательной среды, включающей в себя *информационные технологии, технические средства, электронные информационные ресурсы, электронные образовательные ресурсы*, которые содержат электронные учебно-методические материалы, и т. д.

Кроме того, в силу требований федеральных государственных образовательных стандартов, устанавливающих обязательные требования к образованию, каждый обучающийся в течение всего периода обучения должен быть обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде образовательной организации из любой точки, в которой имеется доступ к сети «Интернет»: как на территории ВУЗа, так и вне её. Учитывая упоминание об ЭИОС в основных документах, устанавливающих совокупность требований, обязательных при реализации образовательных программ, её разработка и внедрение в образовательную систему каждого университета рассматриваются необходимыми. Отсутствие ЭИОС в образовательной организации является основанием для квалификации её деятельности как не соответствующей требованиям федеральных государственных образовательных

[1] Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» // СЗ РФ. 2012. № 53. Ст. 7598.

[2] Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» // СЗ РФ. 2012. № 53. Ст. 7598.

стандартов со всеми вытекающими из этого негативными последствиями. Таким образом, электронная информационно-образовательная среда выступает одним из аккредитационных показателей, характеризующих качество образования.

В образовательной юридической практике существуют определённые сложности с пониманием ЭИОС, поскольку Федеральный закон об образовании не содержит её дефиницию, частично перечисляя только компоненты: *электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных и телекоммуникационных технологий; технологические средства*. ФГОСы также не фиксируют нормативное определение рассматриваемого института, лишь формулируя цели электронной среды:

– обеспечение доступа участников образовательных отношений к учебным материалам и к электронным образовательным ресурсам, указанным в рабочих программах дисциплин;

– фиксация хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательных программ;

– проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

– формирование электронного портфолио обучающегося;

– взаимодействие между участниками образовательного процесса, в том числе посредством сети «Интернет».

Организационно-техническим обеспечением функционирования ЭИОС рассматриваются средства информационно-коммуникационных технологий и квалификация работников, её использующих и поддерживающих.

Ввиду отсутствия единого федерального определения термина «электронная информационно-образовательная среда», каждый ВУЗ решает данную проблему путём принятия локальных нормативных актов, регламентирующих назначение, состав и условия функционирования ЭИОС. Обычно определение электронной информационно-образовательной среды даётся посредством указания на её основные элементы, так, под ней понимается *совокупность электронных информационных ресурсов, информационных технологий, телекоммуникационных технологий, соответствующих технологических средств, обеспечивающих освоение обучающимися образовательных программ или их частей, а также взаимодействие обучающихся с педагогическим, учебно-вспомогательным, административно-хозяйственным персоналом и между собой*. Ключевой целью её функционирования декларируется создание единого образовательного пространства для повышения качества и эффективности образования. По мнению ряда учёных, «ЭИОС сегодня

позиционируется в числе важнейших элементов достижения нового уровня качества образования»[3]. Наличие элементов ЭИОС у университетов даёт возможность обучающимся освоить образовательные программы в полном объёме независимо от места нахождения.

Кроме того, электронная образовательная среда, как уже отмечалось, *позволяет использовать современные информационные технологии на всех этапах процесса обучения, применять электронное обучение и элементы дистанционных образовательных технологий, контролировать успеваемость обучающихся, создавать их электронное портфолио, обеспечивать взаимодействие всех участников образовательного процесса*. ЭИОС создаётся в образовательной организации независимо от вариантов внедрения систем электронного обучения и дистанционных образовательных технологий.

Представляется целесообразным проиллюстрировать функциональные возможности электронной информационно-образовательной среды на примере конкретного высшего учебного заведения – Национального исследовательского Нижегородского государственного университета им. Н. И. Лобачевского (далее – Университет Лобачевского, Университет, ННГУ).

В Университете Лобачевского составными элементами ЭИОС рассматриваются: *официальный сайт Университета и его филиалов в сети «Интернет», корпоративный интернет-портал, информационный ресурс «Работы обучающихся», образовательная платформа «Система электронного обучения», библиотека Университета с подключёнными электронно-библиотечными системами, система управления вузом* («Галактика», 1С Бухгалтерия, Зарплата и Кадры, Электронный документооборот, Расписание учебных занятий, LMS MOODLE, иные информационные сервисы ННГУ). Вопросы создания ЭИОС, её функционирования, состав элементов урегулированы локальным актом образовательной организации.

В ННГУ доступ к учебным материалам обеспечивается путём их размещения на официальном сайте Университета в режиме общего доступа. Доступ к изданиям электронных библиотечных систем (ЭБС), электронным учебным изданиям и электронным образовательным ресурсам реализуется посредством размещения соответствующих ссылок на сайте Фундаментальной библиотеки Университета.

Федеральные государственные образовательные стандарты устанавливают необходимость фиксации с помощью электронной информационно-образовательной среды ВУЗа хода образовательного процесса, результатов промежуточной аттестации и результатов освоения

[3] Уджуху И. А., Мешвез Р. К., Манченко Ю. В., Галюнко Т. Э. Электронная информационно- образовательная среда современного вуза: понятие, структура, применение // Вестник Майкопского государственного технологического университета. 2020. № 1 (44). С.116.

образовательной программы. *Фиксация хода образовательного процесса, результатов промежуточной аттестации, результатов освоения образовательных программ* осуществляется путём размещения, соответственно, информации о расписании учебных занятий и аттестационных испытаниях, о результатах промежуточной аттестации, о результатах итоговой аттестации в личном кабинете обучающегося на корпоративном интернет-портале Университета в соответствующем разделе. Таким образом, принимая во внимание автономию образовательной организации, выраженную в самостоятельном осуществлении образовательной, научной, административной, финансово-экономической деятельности, разработке и принятии локальных нормативных актов, в ННГУ вопросы создания электронной информационно-образовательной среды, в частности установление способов и форм фиксации хода образовательного процесса, урегулированы на уровне локального нормотворчества. Проведение занятий, процедур оценки результатов обучения обеспечивается посредством образовательной платформы «Система электронного обучения».

Создание электронного портфолио обучающихся, в том числе сохранение их работ, а также рецензий и оценок на них осуществляется с помощью создания технической возможности размещения информации об учебных и внеучебных достижениях в личных кабинетах студентов на корпоративном интернет-портале Университета и на информационном ресурсе «Работы обучающихся».

Взаимодействие между участниками образовательного процесса, в том числе посредством сети Интернет, возможно благодаря соответствующим техническим возможностям в личном кабинете обучающегося или работника Университета на корпоративном интернет-портале (в разделах «Сотрудники», «Обучающиеся», «Живая лента»). При нахождении всех участников образовательных отношений в онлайн-режиме осуществляется синхронное взаимодействие посредством текстовых сообщений или видеосвязи, если данные субъекты пребывают в офлайн-режиме, имеет место асинхронное взаимодействие посредством текстовых сообщений. Состав и информационное наполнение электронной информационно-образовательной среды Университета Лобачевского определяются потребностями самих пользователей, а перечень элементов ЭИОС и требований к ним при необходимости может быть расширен.

Официальный сайт Университета включает в себя сайты его структурных подразделений и официальные сайты филиалов. Данные ресурсы являются открытыми и общедоступными информационными ресурсами, содержащими информацию о деятельности ННГУ, обеспечивают участникам образовательного процесса свободный доступ к учебной документации. Посредством официального сайта, на котором размещается и своевременно

обновляется информация об образовательной организации, Университет обеспечивает выполнение требований федерального законодательства об информационной открытости. Наличие альтернативной версии официального сайта Университета и его филиалов позволяет делать эти ресурсы доступными для лиц с ограниченными возможностями здоровья.

Корпортивный интернет-портал представляет собой внутренний информационно-коммуникационный ресурс для работников и обучающихся Университета, интегрированным в учебный процесс. Доступ к информации и ресурсам портала осуществляется через личные кабинеты пользователей работников и обучающихся Университета. Информация о порядке осуществления регистрации пользователей размещена на корпоративном портале в разделе «Регистрация». Именно корпоративный интернет-портал обеспечивает фиксацию хода образовательного процесса, формирование электронного портфолио обучающегося, взаимодействие между участниками образовательного процесса.

Информационный ресурс «Работы обучающихся» является базой данных, содержащей информацию о выполненных обучающимися выпускных квалификационных работах, курсовых проектах, отчётов о практике, а также копии этих работ и отчётов. Тексты работ обучающихся, отзывы и рецензии на эти работы размещаются на информационном ресурсе «Работы обучающихся» и доступны для просмотра всеми участниками образовательных отношений до момента отчисления автора работы. Для получения доступа к тексту работы обучающегося со стороны участников образовательного процесса необходимо получить согласие автора работы посредством соответствующего электронного сервиса.

Образовательная платформа «Система электронного обучения» рассматривается как информационная среда, обеспечивающая функционирование системы управления обучения с использованием электронного обучения и дистанционных образовательных технологий: создание и обслуживание онлайн-курсов, регистрацию обучающихся и управление работой с ними, администрирование процесса обучения. Особенности реализации образовательных программ посредством рассматриваемой платформы устанавливаются соответствующими образовательными программами и локальными нормативными актами Университета.

Электронная библиотека Университета представляет собой электронный образовательный ресурс, используемый участниками образовательного процесса при реализации и освоении образовательных программ. Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным доступом к электронно-библиотечной системе (ЭБС) образовательной организации. ЭБС обеспечивает возможность

доступа обучающегося из любой точки, в которой имеется доступ к сети «Интернет». Электронная библиотека Университета включает в себя как внутренние (размещённые на сайте Университета) электронные ресурсы, так и внешние электронные ресурсы (общедоступные и ограниченного доступа, на которые имеется подписка). Доступ к электронным ресурсам ЭБС обеспечивается через сайт Фундаментальной библиотеки Университета.

Университет Лобачевского обеспечивает соответствие функционирование электронной информационно-образовательной среды требованиям законодательства посредством наделения пользователей необходимыми полномочиями для доступа к ресурсам ЭИОС, а также получения согласия на обработку персональных данных.

В целом необходимо констатировать, что ЭИОС Университета отвечает требованиям современного образования, позволяя реализовывать индивидуальную образовательную траекторию с учётом особенностей и образовательных потребностей конкретного обучающегося. Повышение качества образовательного процесса зависит от высокой эффективности электронной образовательной среды, её своевременной актуализации, развития и функционального дополнения.

Список литературы

1. Уджуху И. А., Мешвез Р. К., Манченко Ю. В., Галюнко Т. Э. Электронная информационно- образовательная среда современного вуза: понятие, структура, применение // Вестник Майкопского государственного технологического университета. 2020. № 1 (44). С. 113–121.

Alexander K. Baldin
PhD in Law, Associate professor at the Department
of Civil Law and Process of the Faculty of Law
State University of Nizhny Novgorod named after N. I. Lobachevsky
(Nizhny Novgorod, Russia)
akbaldin@unn.ru

Nadezhda I. Byushkina
Doctor of Law, Professor, Head of the Department
of Judicial and Prosecutorial Activity of the Faculty of Law
State University of Nizhny Novgorod named after N. I. Lobachevsky
(Nizhny Novgorod, Russia)
asya_biyushkina1@list.ru

ELECTRONIC INFORMATION AND EDUCATIONAL ENVIRONMENT AS AN ELEMENT OF INFORMATION OPENNESS OF THE UNIVERSITY

Abstract. the article deals with the issues of formation, implementation and development of the electronic information and educational environment of a higher educational institution as one of the elements of its information openness. A brief analysis of the current legislation regulating this institution is carried out. Using the example of a specific educational organization, the structure of the electronic information and educational environment (EIOS) is revealed, its elements are investigated, and the dependence of the quality of the educational process on the availability of an effectively functioning EIOS is confirmed.

Keywords: electronic information and educational environment, educational space, university information space, electronic library, electronic resources, e-learning, distance learning technologies.

УДК 342.70

Барашева Елена Викторовна
Кандидат экономических наук, доцент кафедры общетеоретических и государственно-правовых дисциплин,
ВСФ ФГБОУ ВО Российский государственный университет правосудия
(г. Иркутск, Российская Федерация)
barahevaev@bk.ru

Степаненко Диана Аркадьевна
Доктор юридических наук, профессор кафедры криминалистики, судебных экспертиз и юридической психологии,
заслуженный юрист Иркутской области,
Институт государства и права
Байкальского государственного университета,
(г. Иркутск, Российская Федерация)
diana-stepanenko@mail.ru

К ВОПРОСУ О ПРАВОВОМ РЕГУЛИРОВАНИИ ГЕНОМА ЧЕЛОВЕКА

Аннотация. Развитие технологий, в том числе в области медицины, делает весьма актуальными вопросы донорства, генной инженерии. Так, сегодня уже существует возможность создавать искусственные органы для имплантации человеку, однако в России отсутствуют правовые механизмы осуществления данного вида деятельности.

В статье на основе анализа проблем, существующих в сфере донорства органов, рассмотрения положительных примеров трансплантации искусственно созданных органов и выделения достоинств осуществления таких операций делается вывод о необходимости внедрения соответствующего направления медицины. Так, в России реализуется специальная программа, нацеленная на развитие технологий в сфере генетических исследований, и в настоящее время необходимо акцентировать усилия на правовом регулировании геномных исследований и практической реализации генетических технологий. Совершенно очевидно, что законодательство в сфере генетики должно открывать простор для научного поиска и создания инноваций в медицине, ветеринарии, селекции, в других сферах. Авторами статьи предлагаются пути возможного совершенствования юридического регулирования в Российской Федерации вопросов, связанных с донорством в целом и трансплантацией искусственных органов в частности.

Ключевые слова: геном, право, регулирование, исследование, программа.

Для цитирования:
Барашева Е. В., Степаненко Д. А. К вопросу о правовом регулировании генома человека // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 37–42.

На сегодняшний день достаточно большое число вопросов в сфере геномной инженерии уже урегулировано со стороны законодателя, однако остались правовые пробелы, в том числе в части выращивания органов человека искусственным путём и их трансплантации.

Трансплантация даёт возможность продлевать жизнь человека за счёт замены органа, ненормально выполняющего свои функции. О. П. Грибунов отмечает: «В России трансплантология развивается и уже находится на уровне западной. Каждая страна имеет свои законодательные ограничения на трансплантацию и донорство, чтобы поддерживать баланс между уважением к умершим, но и спасать тех, кто еще жив»[1].

Проведя анализ результатов статистики в России в области генома, А. А. Рыжова пишет: «Более 50 % пациентов в списках на трансплантацию всё ещё не могут дождаться операции, которая даст им шанс. За рубежом в отдельных странах, где донорство развито значительно сильнее, нежели в России, эта цифра не превышает 10 %»[2]. Таких показателей удалось достичь только с помощью законодательного урегулирования вопросов донорства, в том числе и посмертного.

Пересаженный орган может продлить жизнь человека на несколько лет. Так, в своей работе А. А. Рыжова отмечает: «Почка с вероятностью 75 % продлевает жизнь на срок до 5–10 лет, а наибольший срок работы пересаженного в России сердца составил 17 лет»[3]. Сложность совместимости организмов, приводит к тому, что полной гарантии успеха и приживаемости при пересадке никто не даст. Это маленький, но шанс на то, чтобы прожить ещё несколько лет с нормально функционирующим организмом.

Проведя анализ практики, которая касается вопроса геномной инженерии, Е. П. Ищенко пишет: «В России на законодательном уровне запрещена прижизненная пересадка от донора к пациенту, если они не являются генетическими родственниками. Кроме того, запрещена продажа органов, все проводится только на безвозмездной основе. Бороться с коррупцией пока не представляется возможным из-за несовершенности системы

[1] Грибунов О. П. Совершенствование правового регулирования геномной регистрации в контексте предупреждения преступности // Всероссийский криминологический журнал. 2022. Т. 16. № 1. С. 102.

[2] Рыжова А. А. Правовая защита геномных данных граждан России // Наука. Общество. Государство. 2020. № 3. С. 13.

[3] Рыжова А. А. Правовая защита геномных данных граждан России // Наука. Общество. Государство. 2020. № 3. С. 13.

распределения донорских органов. Достаточно часто врачам разного уровня предлагают взятки за продвижение пациента в очереди»[4].

Стоит отметить, что операция по трансплантации не должна навредить здоровью донора и проводится только с обоюдного согласия между генетическими родственниками. Дети могут выступать только донорами костного мозга, а вот почка и печень обычно пересаживаются от родителя ребёнку. По закону донорство между супругами противозаконно, как и в случае с приёмными детьми. Принуждение к донорству, купля-продажа органов, убийство ради получения органов караются по соответствующим статьям Уголовного кодекса.

Е. П. Ищенко отмечает: «Количество доноров удается увеличивать за счет презумпции согласия – каждый умерший становится потенциальным донором, если не озвучивал отказ или не отказались его родные. Эта норма вызывает множество споров, а иногда и судебных исков, но благодаря ей каждый год количество спасённых жизней увеличивается. Каждый здоровый человек в случае случайной смерти может ещё спасти 5–6 человек, в зависимости от состояния здоровья»[5].

В случае с посмертным донорством у родственников есть два часа, чтобы озвучить отказ от донорства, если он не был озвучен раньше. Врачи могут прилагать максимум усилий, чтобы поддержать жизнедеятельность пациента, даже при смерти мозга, если органы пациента могут использоваться в качестве донорских.

Изучая вопросы генной инженерии и трансплантации, Т. А. Ханов в своей работе пишет: «Человек считается умершим в случае гибели головного мозга, даже если остальные органы и системы ещё работают. Так как если мёртв мозг, сознательность к человеку уже не вернётся, и он не сможет жить дальше без систем жизнеобеспечения. Врачи имеют право поддерживать жизнедеятельность органов и систем во время подготовки пациента к операции»[6].

Однако описанные проблемы, связанные с трансплантацией, можно разрешить, если обратиться к практике создания искусственных органов. В зарубежных странах с конца 1990-х годов ведутся разработки в этой области, именно тогда было выращено ухо на спине мыши. Такой орган нельзя считать полностью

[4] Ищенко Е. П., Кручинина Н. В. Геномная регистрация как универсальный идентификатор личности в системе мер предупреждения преступности: исследование и перспективы внедрения // Всероссийский криминологический журнал. 2022. Т. 16. № 2. С. 201.

[5] Ищенко Е. П., Кручинина Н. В. Геномная регистрация как универсальный идентификатор личности в системе мер предупреждения преступности: исследование и перспективы внедрения // Всероссийский криминологический журнал. 2022. Т. 16. № 2. С. 201.

[6] Ханов Т. А., Сихимбаев М. Р., Биржанов Б. К., Биржанов К. К. Геномная регистрация как универсальный идентификатор личности в системе мер предупреждения преступности: исследование и перспективы внедрения // Всероссийский криминологический журнал. 2016. Т. 10. № 3. С. 546.

искусственным, и всё же, он лучше донорского, так как не содержит его клеток и не вызывает отторжения иммунной системы.

Приведём следующий пример успешных исследований в рассматриваемой области. Энтони Атала – директор института регенеративной медицины Уэйк Форрест – занимается созданием искусственных органов мочеполовой системы. Начал он с мочевого пузыря. Такие искусственные мочевые пузыри вживили нескольким мальчикам с патологиями в 1999 году. Спустя 5 лет наблюдений Энтони Атала с коллегами доложили, что искусственные органы прижились хорошо и не вызвали осложнений у реципиентов. В дальнейшем он выращивал такие органы как: влагалище, уретру, печень, сердце и лёгкие.

В качестве другого примера можно назвать выращивание многослойной ткани глаза из стволовых клеток человека. Искусственный «глаз» был пересажен кроликам, у которых искусственно вызвали роговичную слепоту. Трансплантация помогла восстановить зрение животных.

Можно отметить следующие преимущества выращивания органов из клеток живого организма:

1. Не надо ждать длинных очередей, чтобы получить необходимый орган.

2. Меньше вероятность отторжения организмом иногороднего органа, так как он состоит из гена человека, для которого выращивается.

Данные процедуры используются в других странах и разрешены законом, однако в России они запрещены. На наш взгляд, это может быть связано со следующими обстоятельствами.

Во-первых, выращивание органов неизбежно приведёт к изменению структуры медицины, так как многие профессии врачей исчезнут и придётся переквалифицировать медицинских сотрудников.

Во-вторых, государство считает, что данные услуги слишком дороги для нашего населения.

В-третьих, для развития данного направления требуется значительное финансирование.

Однако многие учёные в сфере медицины и физиологии считают необходимым внедрить в России выращивание искусственных органов, обосновывая свою позицию нижеследующим.

Во-первых, возрастёт демография населения, так как увеличится продолжительность жизни людей. Людям не надо будет ждать очереди на нужный им орган.

Во-вторых, найдутся пути решений многих болезней, что также приведёт к увеличению роста населения и снижению смертности.

В-третьих, возрастёт численность медицинского туризма. Это будет означать увеличение доходной части бюджета Российской Федерации.

Например, в г. Уфе Российской Федерации провели уникальную операцию по пересадке роговицы. Трансплантация была сделана 63-летней женщине, которая долгие годы видела практически одним глазом. Затем, как хирурги восстанавливают пациенту зрение, в режиме реального времени следили сотни

офтальмологов. На данный момент жители разных стран и городов, в том числе и самой России посещают данную клинику, чтобы получить зрение, о котором долго мечтают.

Следует отметить, что законодатель в Российской Федерации начинает решать данный вопрос. Так, например, приказом Министерства здравоохранения Российской Федерации от 24 декабря 2020 г. № 1365 была утверждена ведомственная целевая программа «Модернизация первичного звена здравоохранения Российской Федерации». Целью данной программы является эффективная реализация государственной политики в сфере здравоохранения, обеспечивающая достижение к 2024 году целей, в числе которых можно отметить: снижение младенческой смертности до 4,5 случая на 1000 родившихся живыми, смертности от болезней системы кровообращения до 555 случаев на 100 тыс. населения, смертности от новообразований, в том числе от злокачественных до 195,1 случаев на 100 тыс. населения. Программа реализуется в 2021–2025 годах.

Таким образом, в Российской Федерации урегулирован вопрос о геномной инженерии и о трансплантации, но о выращивании органов – нет. На наш взгляд, законодателю Российской Федерации стоит обратить большее внимание на данную тему, так как она спасла бы жизни многих людей.

Список литературы

1. Грибунов О. П. Совершенствование правового регулирования геномной регистрации в контексте предупреждения преступности/ О.П. Грибунов// Всероссийский криминологический журнал. 2022. Т. 16. № 1. С. 101–110. DOI: 10.17150/2500-4255.2022.16(1).101-110.

2. Ищенко Е. П., Кручинина Н. В. Геномная регистрация как универсальный идентификатор личности в системе мер предупреждения преступности: исследование и перспективы внедрения // Всероссийский криминологический журнал. 2022. Т. 16. № 2. С. 199–206. DOI: 10.17150/2500-4255.2022.16(2).199-206.

3. Рыжова А. А. Правовая защита геномных данных граждан России // Наука. Общество. Государство. 2020. № 3. С. 12–15.

4. Ханов Т. А., Сихимбаев М. Р., Биржанов Б. К., Биржанов К. К. Геномная регистрация как универсальный идентификатор личности в системе мер предупреждения преступности: исследование и перспективы внедрения // Всероссийский криминологический журнал. 2016. Т. 10. № 3. С. 544–553. DOI: 10.17150/2500-4255.2016.10(3).544-553.

Elena V. Barasheva
PhD of Economic Sciences, Associate Professor
of the Department of General Theoretical and State-Legal Disciplines,
VSF Russian State University of Justice
(Irkutsk, Russian Federation)

barahevaev@bk.ru

Diana A. Stepanenko
PhD of Law, Professor of the Department of Criminalistics,
Forensic Examinations and Legal Psychology,
Honored Lawyer of the Irkutsk Region,
Institute of State and Law of Baikal State University,
(Irkutsk, Russian Federation)
diana-stepanenko@mail.ru

ON THE ISSUE OF LEGAL REGULATION OF THE HUMAN GENOME

Abstract. The development of technology, including in the field of medicine, makes the issues of donation and genetic engineering very topical. So, today it is already possible to create artificial organs for implantation in humans, but in Russia there are no legal mechanisms for this type of activity.

In the article on the basis of analysis of the problems existing in the sphere of organ donorship, consideration of positive examples of transplantation of artificially created organs and singling out the advantages of such operations the conclusion is made about the necessity of introduction of the corresponding direction of medicine. Thus, Russia is implementing a special program aimed at developing technologies in the field of genetic research, and it is now necessary to focus on the legal regulation of genomic research and the practical implementation of genetic technologies. It is obvious that the legislation in the field of genetics must open up space for scientific search and creation of innovations in medicine, veterinary medicine, breeding and other areas. The authors of the article suggest ways of possible improvement of legal regulation in the Russian Federation of issues related to donation in general and transplantation of artificial organs in particular.

Keywords: genome, law, regulation, research, program.

УДК 004.5; 343

Бахтеев Дмитрий Валерьевич
доктор юридических наук, доцент
доцент кафедры криминалистики
Уральский государственный юридический университет имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
ae@crimlib.info

Цветкова Анна Денисовна
Младший научный сотрудник
АНО «КримЛиб»,
Студент Института юстиции
Уральский государственный юридический университет имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
at@crimlib.info

ИНТЕРФЕЙС В ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЕ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ КАК ФАКТОР ПРИНЯТИЯ РЕШЕНИЯ НА ПРИМЕРЕ ПРОЕКТА ПО ВЕРИФИКАЦИИ ПОДПИСЕЙ*

Аннотация. В статье рассматривается важность интерфейса выдачи решения интеллектуальной системы на примере проекта NSP-SigVer. Для взвешенной оценки реквизитов юридического документа человеком могут быть использованы интеллектуальные системы, которые способны предлагать (или навязывать) человеку собственное решение. Для снижения этой вероятности и, соответственно, повышения качества взаимодействия человека с системой ИИ возможно, в числе прочего, оптимизация формата выдачи решения системы, которая может включать цветовые индикаторы, текстовый ответ, количественные характеристики ответа системы.

Ключевые слова: машинное обучение, система поддержки принятия решения, принятие решения, человеко-машинный интерфейс, верификация подписей.

Для цитирования:
Бахтеев Д. В., Цветкова А. Д. Интерфейс в интеллектуальной системе поддержки принятия решения как фактор принятия решения на примере проекта по верификации подписей // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 43–50.

* Исследование выполнено при финансовой поддержке УрГЮУ имени В.Ф. Яковлева в рамках реализации проекта ведущей научной школы № 0304/23.

Профессиональное сообщество сегодня почти в полном объёме вовлечено в дискуссию по вопросу возможностей использования искусственных интеллектуальных систем в правоохранительной деятельности. С одной стороны выступают полные противники такого шага, обосновывающие свою позицию недопустимостью замены человека, с его эмоциональными свойствами и доступной для осознания остальными членами социума логикой принятия решений, машиной[1]. Оппоненты, не отрицая выдвигаемых противной стороной тезисов, говорят о значительном потенциале систем искусственного интеллекта, которые будут выступать в роли вспомогательных, но не замещающих инструментов[2]. Относя себя ко второй группе более открытых новому исследователей, подчеркнём, что системы искусственного интеллекта, внедрённые в практику правоохранительной деятельности, могут осуществлять, если говорить обобщённо, две группы функций:

1) классифицировать, систематизировать и иным образом обрабатывать большие объёмы данных (big data), играя таким образом справочно-информационную роль;

2) воспроизводить отдельные познавательные операции человека (выдвигать версии, прогнозировать дальнейшее, посткриминальное поведение преступника и т. п.), оказывая за счёт этого поддержку в принятии непосредственных решений субъектом правоохранительной деятельности (судом, следователем, экспертом и т. д.).

В рамках второго направления взаимодействие человека и системы искусственного интеллекта можно описать следующим образом: заинтересованный субъект подаёт на вход искусственной интеллектуальной системе массив информации; система, обученная на аналогичных материалах, обрабатывает запрос и выдаёт решение; человек получает решение системы и, отталкиваясь от него, организует свою дальнейшую деятельность. Рассмотрим это на примере функционирования интеллектуальной системы, разрабатываемой на кафедре криминалистики Уральского государственного юридического университета имени В. Ф. Яковлева, «SigVer», призванной выявлять в рамках предэкспертных стадий подлог рукописной подписи[3]. Планируется, что после её внедрения в практическую

[1] См., например: Маслов И. В. Отзыв на монографию доктора юридических наук, профессора Аликперова Ханлара Джафаровича «Электронная технология определения меры наказания» («Электронные весы правосудия») // Российский судья. 2020. № 11. С. 55–60.

[2] См., например: Заплатина Т. С. Искусственный интеллект в вопросе вынесения судебных решений, или ИИ-судья // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 4 (56). С. 160–168. DOI 10.17803/2311-5998.2019.56.4.160-168; Кравчук Р. Г. Искусственный интеллект как судья: перспективы и опасения // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4. Государство и право: Реферативный журнал. 2021. С. 115–122. DOI 10.31249/rgpravo/2021.01.12.

[3] Bakhteev D. V., Sudarikov R. O. NSP dataset and offline signature verification //

деятельность широкого профиля, а не только правоохранительную, субъект данной деятельности (лицо, в чьи служебные функцию входит проверка реквизитов юридических документов, которое при этом не обладает специальными знаниями в области почерковедения), если встретится с подписью, в подлинности которой не уверен, сможет осуществить её проверку. По результатам этого субъект может инициировать дальнейшие стадии проверки: сообщить о своих сомнениях в службу безопасности, организовать проведение специального исследования или судебной экспертизы. Таким образом, описанная система имеет функцию именно *поддержки* принятия решения человеком, а не принятия решения за него. Это особенно важно в том числе потому, что, как верно отмечает А. А. Бессонов, «в определённой мере является заблуждением мнение относительно абсолютной объективности базирующихся на таких технологиях систем при оценке доказательств, иной криминалистически значимой информации и применении норм материального права. Прежде всего такие системы представляют собой алгоритмы, обученные на соответствующих прецедентах, а последние, являясь продуктами человеческой жизнедеятельности, нередко не лишены определённой доли субъективности и неполноты»[4].

Функционал приложения предполагает загрузку пользователем в программу снимков оригинала и спорной подписи. При этом происходит обработка фотографий: штрихи дифференцируются от фона, по интенсивности выраженности штрихов определяется нажим и т. д. После этого при нажатии на кнопку «сравнить» система выдаёт свою оценку по результатам сравнения изображений подписи. Форма выдачи этой оценки и является предметом настоящей статьи, поскольку от неё зависит специфика восприятия человеком решения интеллектуальной системы.

В настоящее время выдача результата сравнения представляет собой демонстрацию ответа («оригинальная» либо «спорная») и числовую оценку вероятности предложенной характеристики: например, «спорная 0,35», где «1.00» – достоверно подложная (см. Рис. 1).

Communications in Computer and Information Science. 2020. Vol. 1266. Pp. 41–49. DOI 10.1007/978-3-030-58793-2_4.

[4] Бессонов А. А. Преимущества и ограничения использования технологий искусственного интеллекта в расследовании преступлений // Наука и технологии XXI века: тренды и перспективы: Сборник статей по итогам IV Профессорского форума. В 2-х томах, Москва, 27–30 сентября 2021 года. Том 1. Москва: Общероссийская общественная организация «Российское профессорское собрание», 2021. С. 15. С. 13–16.

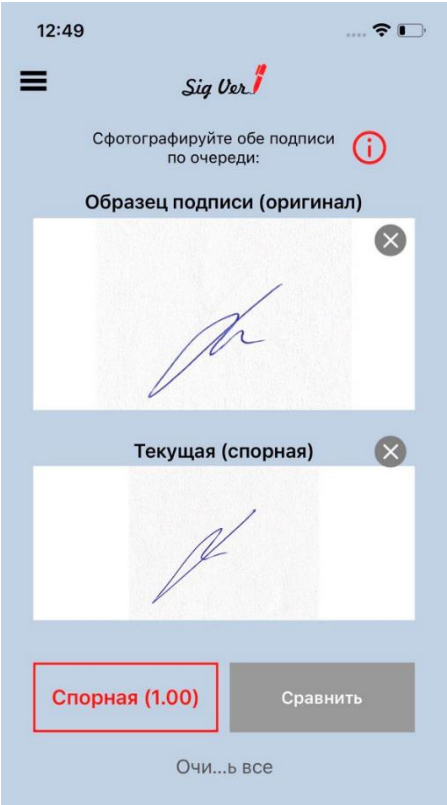

Рис. 1. Интерфейс тестируемого мобильного приложения NSP-SigVer

После этого субъект проверки документа может или принять подпись за достоверную, или затребовать дополнительные способы проверки. Если же система используется непосредственно экспертом-почерковедом, то результат её работы, как свидетельствуют результаты опроса судебных экспертов, должен будет выступить дополнительным источником проверки вывода самого эксперта. Важно отметить, что, учитывая эффект «чёрного ящика», свойственного большинству современных интеллектуальных систем, использование их как источника доказательственной информации является пока явно недопустимым, так как невозможной остаётся проверка решения на достоверность – обязательное свойство доказательств в суде, – именно поэтому рассматриваемый проект ориентирован именно на предэкспертную проверку подписи. Помимо этого, одним из наиболее важных руководящих положений, на которых основывается деятельность суда, судебных экспертов и иных представителей правоохранительных органов является принцип объективности, под которым традиционно понимается осуществление перечисленными субъектами своей профессиональной деятельности «беспристрастно, независимо от представлений, интересов, взглядов, предпочтений субъектов её осуществляющих, либо иных лиц, участвующих в данной деятельности, экспертов, переводчиков, специалистов»[5]. Таким образом, объективное решение должно приниматься человеком самостоятельно: с опорой на законодательные предписания, имеющиеся в деле доказательственные материалы, но по собственному усмотрению.

В работах К. Становича и О. П. Кузнецова, описывается три уровня принятия решений: рефлективный, алгоритмичный и автономный[6]. В контексте рассматриваемой темы при

[5] Даровских О. И. Принцип объективности как средство, обеспечивающее эффективность уголовно-процессуальной деятельности // Правопорядок: история, теория и практика. 2021. № 2 (29). С. 111

[6] Станович К. Рациональное мышление. Что не измеряют тесты способностей. М.: Карьера Пресс, 2016. С. 38–42. 352 с.; Кузнецов О. П. Ограниченная рациональность и принятие решений. // Искусственный интеллект и принятие решений. № 1. 2019. С. 7. С. 3–15.

работе с интеллектуальной системой должна быть полностью исключена возможность мышления на рефлективном уровне, алгоритмичное мышление свойственно субъекту, который правильно пользуется системой поддержки принятия решений, а при высоком профессионализме человек должен принимать решения автономно.

Одновременно с этим, в психологии уже хорошо изучен феномен, согласно которому модель представления информации влияет на принимаемое человеком решение. Так и в ситуации с работой систем искусственного интеллекта: необходимо при их создании учитывать данный факт и оформлять интерфейс таким образом, чтобы исключить подмену решения человека результатом работы искусственной интеллектуальной системы. То есть, чтобы сохранить за последними действительную роль исключительно помощников, советчиков, но не внешнего мыслительного компонента, детерминирующего выводы человека-субъекта правоохранительной деятельности, можно либо повышать квалификацию субъектов путём разъяснения им самой технологии интеллектуальных систем и неизбежно вытекающих из неё рисков и ограничений, либо же подбирать такую модель представления результатов, которая бы не содержала исчерпывающего ответа на все вопросы, стоящие перед следователем, судом, оперативным сотрудником, экспертом. Приоритетно, естественно, параллельно работать по обоим направлениям, так как даже информированность о потенциальной предвзятости и зависимости решения не гарантирует полного освобождения от указанного когнитивного искажения[7], а создание интерфейса, при котором результат не является исчерпывающим, без объяснения мотивов такого оформления, может вызвать необоснованное недовольство со стороны пользователей. При этом, специалисты разных областей должны заниматься собственными задачами: субъекты образовательной и просветительской деятельности – повышать компьютерную грамотность потенциальной целевой аудитории создающихся программ, – а разработчики искусственных интеллектуальных систем – предлагать не исключающие объективности пользователей интерфейсы.

Последняя задача стояла и перед авторами настоящей работы при создании упомянутой выше искусственной нейронной сети «SigVer», в связи с чем был организован и проведён эксперимент. В первую очередь были сформулированы возможные формы представления результата работы программы, включающие в себя такие элементы, как цвет рамки (красный для высокой вероятности подлога, зелёный – для низкой, либо нейтральный чёрный цвет), ответ системы в текстовой форме («спорная» или «оригинальная»), вероятность решения

[7] Канеман Д. Думай медленно… решай быстро: [перевод с английского]. Москва: Издательство АСТ, 2021. С. 41.

системы (в числовом или процентном выражении, где 0 % – достоверно оригинальная подпись, 100 % – достоверно подложная подпись). В результате были сформированы следующие подходы:

1) Текстовый ответ с окрашенной рамкой. Мы считаем, что такая форма выражения наиболее склонна формировать навязанное мнение у человека, поэтому она использовалась лишь на раннем этапе разработки проекта.

2) Текстовый ответ с числовым выражением вероятности в формате 0.90, рамка окрашена.

3) Текстовый ответ с процентным выражением вероятности в формате 90 %, рамка окрашена.

4) Процентное выражение вероятности решения системы с окрашенной рамкой.

5) Процентное выражение вероятности решения системы с нейтральной чёрной рамкой.

6) Градиентная цветовая шкала, где ярко красный – достоверно подложная подпись, белый – соответствует НПВ в экспертных заключениях, ярко зелёный – достоверно оригинальная подпись. Точное значение вероятности и текстовый ответ системы в данном случае отсутствуют, что снижает степень влияния на решение человека, однако данный способ не является интуитивно понятным[8].

Примерный вид указанных моделей интерфейса выдачи представлен на рис. 2.

Рис. 2. Модели представления решения интеллектуальной системы

Для проверки восприятия разных моделей представления выдачи интеллектуальной системы был проведён опрос 114 респондентов, в рамках которого предлагалось оценить модели по характеристикам удобства восприятия и сохранения независимости решения человеком и выбрать одну наилучшую, отвечающую указанным критериям. Были получены следующие результаты:

1 – 9 %;
2 – 1 %;
3 – 24 %;
4 – 6 %;
5 – 25 %;
6 – 35 %.

[8] Авторы не исключают возможность разработки и других, более оптимальных моделей в будущем.

Разумеется, в предложенной совокупности моделей отражены не все возможные варианты формата выдачи. Результаты опроса демонстрируют широкий спектр мнений, что подтверждает тезис о том, что для использования интеллектуальных систем поддержки принятия решения требуется глубокая проработка навыков пользователя, равно как правильное позиционирование результатов работы интеллектуальной системы в структуре человеческой деятельности.

В заключение ещё раз подчеркнём, что люди склонны верить автоматизированным системам, в результате чего технологии машинного обучения, которые объективно, в силу своей несовершенности, на сегодняшний день не могут заменить человека, несут в себе риск подмены решения пользователя искусственно сгенерированным ответом, тогда как требуется, чтобы человек лишь учитывал *мнение системы*, но итоговое решение принимал самостоятельно. Соответственно, стоит задача сделать так, чтобы не исключать *сомнение человека* в достоверности предлагаемого ему вывода, что достижимо посредством небольшой правки интерфейса. Таким образом, для обеспечения исключительно вспомогательной роли искусственных интеллектуальных систем при реализации функции поддержки принятия решения, помимо подготовки субъектов применения таких систем, требуется оценка того, как человек воспринимает и интерпретирует предлагаемый ему вывод. В юридической оценке фактов нет незначительных деталей и даже такая мелочь, как дизайн одной кнопки может повлиять на объективность принимаемых решений.

Список литературы

1. Бессонов А. А. Преимущества и ограничения использования технологий искусственного интеллекта в расследовании преступлений // Наука и технологии XXI века: тренды и перспективы: Сборник статей по итогам IV Профессорского форума. В 2-х томах, Москва, 27–30 сентября 2021 года. Том 1. Москва: Общероссийская общественная организация «Российское профессорское собрание», 2021. С. 13–16.

2. Даровских О. И. Принцип объективности как средство, обеспечивающее эффективность уголовно-процессуальной деятельности // Правопорядок: история, теория и практика. 2021. № 2 (29). С. 109–115.

3. Заплатина Т. С. Искусственный интеллект в вопросе вынесения судебных решений, или ИИ-судья // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 4 (56). С. 160–168. DOI 10.17803/2311-5998.2019.56.4.160-168.

4. Канеман Д. Думай медленно… решай быстро: [перевод с английского]. Москва: Издательство АСТ, 2021. 653 с.

5. Кравчук Р. Г. Искусственный интеллект как судья: перспективы и опасения // Социальные и гуманитарные науки. Отечественная и зарубежная

литература. Сер. 4. Государство и право: Реферативный журнал. 2021. С. 115–122. DOI 10.31249/rgpravo/2021.01.12.

6. Кузнецов О. П. Ограниченная рациональность и принятие решений. // Искусственный интеллект и принятие решений. № 1. 2019. С. 3–15.

7. Маслов И. В. Отзыв на монографию доктора юридических наук, профессора Аликперова Ханлара Джафаровича «Электронная технология определения меры наказания» («Электронные весы правосудия») // Российский судья. 2020. № 11. С. 55–60.

8. Станович К. Рациональное мышление. Что не измеряют тесты способностей. М.: Карьера Пресс, 2016. 352 с.

9. Bakhteev D. V., Sudarikov R. O. NSP dataset and offline signature verification // Communications in Computer and Information Science. 2020. Vol. 1266. P. 41–49. DOI 10.1007/978-3-030-58793-2_4.

Dmitriy V. Bakhteev
Doctor of Law, Associate Professor
associate professor of the Department of criminalistics
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
ae@crimlib.info

Anna D. Tsvetkova
Junior Researcher
ANO «CrimLib»,
Student of the Institute of Justice
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
at@crimlib.info

INTERFACE IN INTELLIGENT DECISION SUPPORT SYSTEM AS A DECISION-MAKING FACTOR ON EXAMPLE OF SIGNATURE VERIFICATION PROJECT

Abstract. This article discusses the importance of the intelligent system's decision-making interface on the example of the NSP-SigVer project. Intelligent systems can be used to make an informed decision on the evaluation of legal document requisites, which can suggest (or impose) a person's own decision. To reduce this probability and, consequently, to improve the quality of human interaction with AI system, it is possible, among other things, to optimize the format of the output of the system's decision, which may include color indicators, textual response, quantitative characteristics of the system's response.

Keywords: machine learning, decision support system, decision making, human-machine interface, signature verification.

УДК 343.1

Вдовцев Павел Викторович
кандидат юридических наук, доцент кафедры уголовного процесса
Екатеринбургский филиал Московской академии
Следственного комитета Российской Федерации
(г. Екатеринбург, Россия)
ekb@advokat66.su

Чарыков Александр Викторович
Адвокат Адвокатской палаты Свердловской области
адвокатский кабинет «Консильери»
(г. Екатеринбург, Россия)
ekb@advokat66.su

ЭЛЕКТРОННАЯ ПОДПИСЬ В ДЕЯТЕЛЬНОСТИ АДВОКАТА-ЗАЩИТНИКА

Аннотация. В работе анализируется действующее законодательство в сфере использования адвокатом электронной подписи, констатируется наличие организационных сложностей при использовании адвокатами современных технологий, описываются имеющиеся пути решения проблемы.

Ключевые слова: уголовное производство, адвокат-защитник, электронная подпись, ордер.

Для цитирования:
Вдовцев П. В., Чарыков А. В. Электронная подпись в деятельности адвоката-защитника // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 51–53.

С 01.01.2017 года в судах общей юрисдикции России приказом Судебного департамента при Верховном Суде РФ от 27.12.2016 № 251 «Об утверждении порядка подачи в федеральные суды общей юрисдикции документов в электронном виде, в том числе в форме электронного документа»[1] (далее – Порядок) введена возможность подачи обращения в электронном виде.

Порядок оперирует понятиями электронный документ – это документ, созданный в электронной форме без предварительного документирования на бумажном носителе, и электронный

[1]Приказ Судебного департамента при Верховном Суде РФ от 27.12.2016 № 251 «Об утверждении порядка подачи в федеральные суды общей юрисдикции документов в электронном виде, в том числе в форме электронного документа» // СПС Консультант Плюс [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_209690/ (дата обращения 14.05.2023).

образ документа (электронная копия документа, изготовленного на бумажном носителе) – переведённая в электронную форму с помощью средств сканирования копия документа, изготовленного на бумажном носителе.

Каждый такой документ должен быть заверен электронной подписью каждого лица, чья подпись содержится на документе (п. 2.3.6 Порядка).

В уголовном производстве в силу п. 3.4.1 Порядка обращение подаётся в виде электронного документа, подписанного усиленной квалифицированной электронной подписью лица, подающего обращение, либо в виде электронного образа документа, заверенного усиленной квалифицированной электронной подписью лица, подающего обращение. Таким образом, в уголовном процессе допускается использование только усиленной квалифицированной электронной подписи.

Пунктом 3.1.3 Порядка предусмотрено, что к обращению в суд, подаваемому представителем (защитником), должен быть приложен документ, подтверждающий полномочия. Как известно, полномочия адвоката-защитника по уголовному делу подтверждаются ордером (ч. 4 ст. 49 УПК РФ). Порядок разъясняет, что ордер на исполнение поручения, выдаваемый соответствующим адвокатским образованием, представляется в виде электронного образа документа, заверенного усиленной квалифицированной электронной подписью должностного лица, выдавшего ордер.

Форма ордера утверждена приказом Минюста РФ от 10 апреля 2013 г. № 47 «Об утверждении формы ордера»[2]. Согласно данной форме, ордер всегда содержит подпись руководителя адвокатского образования, выдавшего ордер. В силу ст. 20 Федерального закона от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» существует четыре формы адвокатских образований: адвокатский кабинет, коллегия адвокатов, адвокатское бюро и юридическая консультация.

Очевидно, что из четырёх форм адвокатских образований три являются коллегиальными и состоят более чем из одного адвоката. В такой ситуации любой адвокат коллегии, бюро или консультации, не являющийся руководителем, столкнётся со сложностью подачи любого процессуального документа в уголовном производстве, так как его ордер должен каждый раз заверяться усиленной квалифицированной электронной подписью руководителя адвокатского образования. Не испытывают таких проблем только адвокатские кабинеты или (возможно) небольшие адвокатские образования, состоящие из нескольких адвокатов.

Фактически, такое положение вещей приводит к невозможности адвокатов крупных коллегий пользоваться современными технологиями подачи документов в

[2]Приказ Минюста России от 10.04.2013 № 47 «Об утверждении формы ордера» // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_144981/ (дата обращения 14.05.2023).

электронном виде. Учитывая тот факт, что по состоянию на 2021 год из 75 504 адвокатов в России деятельность в форме адвокатского кабинета осуществляют 22 521 человек[3], большинство активных участников различных видов судопроизводства не имеют возможности «двигаться в ногу со временем», реализуя государственные программы всеобщих цифровизации и перехода на электронный документооборот.

Решение сложившейся проблемы видится в нахождении адвокатским сообществом организационных решений, которые бы упростили процесс получения электронной квалифицированной подписи руководителя адвокатского образования. Например, токен с электронной подписью может размещаться на компьютере в офисе коллегии с возможностью любого адвоката заверить свой ордер при возникновении такой необходимости. Думается, возможна настройка и удалённого доступа к такому компьютеру. Поиск оптимальных решений – это вопрос будущей цифровизации адвокатуры.

Pavel V. Vdovtsev
PhD in Law,
Associate Professor of the Department of Criminal Procedure
Yekaterinburg Branch of the Moscow Academy
of the Investigative Committee of the Russian Federation
(Yekaterinburg, Russia)
ekb@advokat66.su

Alexander V. Charykov
Lawyer of the Chamber of Lawyers of the Sverdlovsk Region
Law Office «Consigliere»
(Yekaterinburg, Russia)
ekb@advokat66.su

ELECTRONIC SIGNATURE IN THE ACTIVITIES OF A DEFENDER LAWYER

Abstract. The current legislation in the field of using an electronic signature by a lawyer is analyzed, the presence of organizational difficulties in the use of modern technologies by lawyers is stated, describes the available ways to solve the problem.

Keywords. criminal proceedings, defense attorney, electronic signature, warrant.

[3] Сведения о составе адвокатского сообщества за 2021 год // Официальный сайт ФПА РФ [Электронный ресурс]. URL: https://fparf.ru/upload/iblock/2ea/69z34wf4elzsczup72rkao794c821pqi/Svedeniya-o-sostave-advokatskogo-soobshchestva_.pdf (дата обращения 10.05.2013).

УДК 343.14

Глушков Максим Рудольфович
Заведующий лабораторией по исследованию проблем
процессуальной деятельности следственных органов,
Научно-исследовательский отдел,
Санкт-Петербургская академия
Следственного комитета Российской Федерации
(г.Санкт-Петербург, Российская Федерация)
glushkov.mr@skspba.ru

К ВОПРОСУ ОБ «ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВАХ»

Аннотация. В статье рассматривается распространившаяся в последние годы точка зрения о том, что специфика информации, представленной в электронном виде, обуславливает потребность выделения особой категории доказательств в уголовном судопроизводстве – так называемых электронных доказательств. Данный подход автором не разделяется, обосновывается мнение о том, что работа с электронной информацией и её носителями возможна при помощи имеющихся уголовно-процессуальных средств.

Ключевые слова: информация в электронном виде, доказательства в уголовном судопроизводстве, электронные доказательства, виды доказательств, первоисточник данных, копия, оригинал.

Для цитирования:
Глушков М. Р. К вопросу об «электронных доказательствах» // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 54–60.

Информация, представленная в электронном виде, нередко истребуется и изучается в ходе расследования преступлений. При этом она подчас имеет специфическую форму, например, представляет собой поименованную область данных на удалённом сервере, которая, к тому же, может менять локацию в целях оптимизации дискового пространства.

Эта специфичность породила широко обсуждаемую в отечественной уголовно-процессуальной науке проблему «электронных доказательств». Одним из её аспектов является дискуссия о придании электронной информации статуса самостоятельного вида доказательств. Сторонники придания[1] в качестве аргумента приводят то обстоятельство,

[1] Воронин М. И. Электронные доказательства в УПК: быть или не быть? // Lex Russica. 2019. № 7 (152). С. 79; Зигура Н. А., Кудрявцева А. В. Компьютерная информация как вид доказательства в уголовном процессе России: монография. М.: Юрлитинформ, 2011. С. 30; Макарова О. В. Совершенствование судопроизводства путем внедрения электронной формы уголовного дела // Журнал российского права. 2019. № 2. С.

что такая информация обладает рядом особенностей, которые должны быть учтены в уголовно-процессуальном законе.

Так, отмечают, что электронные данные формируются не только посредством физических закономерностей, но и согласно программному алгоритму[2]. Электронная информация имеет собственные признаки, не присущие в чистом виде ни «материальным», ни «идеальным» следам, поскольку может находиться не на всех материальных объектах, а только в памяти компьютеров и на машинных носителях, при копировании электронной информации её первоисточник не претерпевает никаких изменений, что делает в отношении электронной информации понятия «оригинал» и «копия» весьма условными[3]. Приходят к выводу о том, что никакая цифровизация невозможна, пока законодатель не признает доказательства информацией, а не формально определённым документом и не приравняет файл к протоколу[4].

В качестве примера того, как сильно виртуальная реальность может отличаться от материальной, приводится уголовное дело в отношении Дмитрия Богатова. Он обвинялся в совершении экстремистских преступлений с использованием сети Интернет, но в итоге уголовное преследование прекратили, поскольку компьютерно-техническая экспертиза «не смогла подтвердить связи с преступлением»[5], а версия обвиняемого не была опровергнута: он утверждал, что в его квартире функционировал выходной узел сети Tor, с помощью которой с его IP-адреса мог публиковать сообщения кто угодно[6].

159–168; Гришина Е. П. К вопросу об использовании электронных доказательств в уголовном судопроизводстве // Администратор суда. 2020. № 3. С. 31–34; Обидин К. В. Электронное доказательство: необходимый этап развития уголовного судопроизводства // Актуальные проблемы российского права. 2020. № 11. С. 198–206.

[2] Оконенко Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дисс. ... канд. юрид. наук. М., 2016. С. 23.

[3] Стельмах В. Ю. Электронная информация в доказывании по уголовным делам: способы получения и место в системе доказательств // Библиотека криминалиста. 2018. № 3. С. 94–95. На проблему первоисточника электронной информации указывают и другие авторы, см., например: Обидин К. В. Электронное доказательство: необходимый этап развития уголовного судопроизводства // Актуальные проблемы российского права. 2020. № 11. С. 203. В этой же работе автор отмечает ещё одну особенность компьютерной информации – она всегда сопровождается метаданными (их самая известная разновидность – атрибуты файла).

[4] Ищенко П. П. Современные подходы к цифровизации досудебного производства по уголовным делам // Lex russica. 2019. № 12. С. 78.

[5] Обидин К. В. Электронное доказательство: необходимый этап развития уголовного судопроизводства // Актуальные проблемы российского права. 2020. № 11. С. 204.

[6] Муртазин И. Отбили. Уголовное дело Дмитрия Богатова прекращено // Новая газета. № 52. 21 мая 2018. [Электронный ресурс]. URL: https://novayagazeta.ru/articles/2018/05/20/76538-otbili (дата обращения: 18.04.2023).

Сообразно приводимым аргументам предлагаются и изменения в уголовно-процессуальный закон – дополнить ст. 74 УПК РФ частью 1.1 следующего содержания «Электронными доказательствами по уголовному делу признаются закрепленные в электронной или цифровой форме сведения, при помощи которых в ходе предварительного расследования или судебного разбирательства уголовного дела устанавливаются обстоятельства, указанные в ст. 73 настоящего Кодекса»[7].

Эта точка зрения представляется, однако, спорной. Деление доказательств на виды действительно обусловлено различием их природы, но это различия не физического плана (между способами представления информации), а познавательного. При этом приведённое выше определение электронных доказательств в качестве их сущностного признака указывает как раз на форму представления («закреплённые в электронной форме»), но не на особенности работы с данными.

Апеллируя к «капитальному теоретическому труду прошлого века», сторонники самостоятельности электронных доказательств, как представляется, делают акцент не на том месте. Советские юристы действительно отмечали, что основу деления доказательств на виды составляет «специфика способа сохранения и передачи информации о существенных обстоятельствах исследуемого события с тем, чтобы применить такие и только такие методы ее собирания, которые обеспечили бы полноту и точность полученных фактических данных»[8]. Но в приведённом фрагменте смысловой центр тяжести находится не в начале, а в конце – важна не специфика представления данных, а (хоть и связанная с нею) специфика методов их получения следствием.

Так, сведения, поступающие в уголовное дело «со стороны», оформляются как документы и, если нет оснований в них сомневаться, следователь не выясняет изложенные факты сам, а принимает их как готовое доказательство. Выводы, требующие специальных знаний, оформляются как заключения эксперта или специалиста. Собственную деятельность по установлению обстоятельств преступления следователь документирует в виде протоколов следственных действий и т. д.

С указанных позиций электронная информация не имеет каких-либо отличий познавательного свойства от любых других видов информации (визуальной, вкусовой, аудиальной и т. п.), хоть, безусловно, и более распространена. Соответственно, не требуется и специальных правил работы с нею – сведения, находящиеся на электронных носителях, устройствах и ресурсах, могут быть получены

[7] Гришина Е. П. К вопросу об использовании электронных доказательств в уголовном судопроизводстве // Администратор суда. 2020. № 3. С. 34. Почти дословно повторяет эту формулировку Воронин М. И. в упомянутой выше работе.

[8] Теория доказательств в советском уголовном процессе / отв. ред. Н. В. Жогин. Изд. 2-е, испр. и доп. М.: Юрид. лит., 1973. С. 635.

существующими процессуальными средствами[9].

По этой причине многие известные учёные[10] считают выделение электронных доказательств в особый вид нецелесообразным.

Отмечается, что судебной практике удаётся адаптироваться к новым реалиям, вкладывая не существовшие ранее смыслы в традиционные понятия, например, когда вещественными доказательствами стали признаваться не только ножи и пистолеты, но и разного рода носители, на которые в ходе следственных действий переносится информация из социальных сетей, Интернета и т. п.[11]

Также следует обратить внимание на зарубежный опыт – в европейской части континента большинство стран не предусматривают в своих нормативно-правовых актах конкретного определения того, что является электронными доказательствами, отсутствуют чёткие национальные правила, связанные с допустимостью электронных доказательств[12]. Напомним здесь же об инициативе Следственного комитета Беларуси, не поддержанной законодателем, – о выделении компьютерной информации в особый вид доказательств[13].

Рассмотренный выше пример с уголовным делом Дмитрия Богатова иллюстрирует как раз идею, противоположную той, ради которой он приводится, а именно – никаких проблем с электронными доказательствами нет. Уголовное дело было возбуждено по факту размещения неустановленным лицом экстремистских материалов, первоначальные ОРМ дали основания подозревать Богатова, поскольку материалы размещались с его IP-адреса. Затем оказалось, что обвиняемый – волонтёр проекта Tor, созданного для обеспечения анонимности в Интернете, и его компьютер «достался» в качестве выходного узла преступнику,

---

[9] По образному выражению одного автора – признак «электронности» может быть растворён в иных видах доказательств – см.: Марфицин П. Г. Некоторые подходы к формулированию понятия «электронное доказательство» в уголовном судопроизводстве // Вестник Нижегородской академии МВД России. 2017. № 3 (39). С. 107.

[10] Головко Л. В. Цифровизация в уголовном процесс: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 22; Пастухов П. С. К вопросу о создании процедуры использования «электронных доказательств» в уголовном судопроизводстве // Международное уголовное право и международная юстиция. 2015. № 2. С. 5– 8; Кувычков С. И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: автореф. дис. ... канд. юрид. наук. Н. Новгород, 2016. С. 14–15.

[11] Курс уголовного процесса / Под ред. д. ю. н., проф. Л. В. Головко. М.: Статут, 2016. С. 444.

[12] Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / отв. ред. С. В. Зуев. Москва: Издательство Юрайт, 2020. С. 14.

[13] Андреева Н. А. Правовая регламентация работы с электронными доказательствами в ходе досудебного уголовного производства // Совершенствование следственной деятельности в условиях информатизации: сб. материалов науч.-практ. конф. (Минск, 12–13 апреля 2018 г.). Минск: Редакция журнала «Промышленно-торговое право». С. 12.

размещавшему экстремистский контент. Не обнаружив иных данных, уличающих Богатова, следствие прекратило уголовное преследование, то есть произошло то, что должно было произойти – в штатном режиме отработала правоохранительная система, а энтузиаст, под свою ответственность предоставивший компьютер анонимайзеру, провёл несколько месяцев под подозрением, вполне ожидаемым и понятным, в первую очередь – для него самого.

В литературе встречаются и иные данные из судебной практики – когда ошибки следствия и суда первой инстанции исправлялись лишь на апелляционной стадии[14]. Вместе с тем, назвать системными эти ошибки едва ли возможно, а неправильное понимание правоприменителем сущности электронной информации в конкретном уголовном деле[15] – не повод пересматривать базовые положения доказательственного права. Кроме того, отметим, что допущенные недочёты и здесь были выявлены системой, пусть и на более поздних стадиях процесса, но для того эти стадии и существуют.

Таким образом, представляется ошибочной приведённая в начале работы точка зрения о необходимости выделения электронной (компьютерной, цифровой) информации в отдельный вид доказательств. Формы её представления в уголовном деле могут быть любыми из перечня, приведённого в ч. 2 ст. 74 УПК РФ. Чаще всего это вещественное доказательство и иной документ[16], что не исключает других форм представления. Например, по поводу электронной информации могут быть даны подробные и точные показания. Она может стать предметом осмотра и получить отражение в его протоколе. Её может привести в своём заключении эксперт, если он получил эту информацию в ходе исследования. Таким образом, любые следственные задачи, связанные с исследованием электронной информации, разрешимы имеющимися в арсенале правоохранительных органов методами.

[14] Воронин М. И. Особенности оценки электронных (цифровых) доказательств // Актуальные проблемы российского права. 2021. № 8 (129). С. 118–128.

[15] Автором причины следственных ошибок обозначены именно так – «ошибочная оценка электронных доказательств».

[16] Есть точка зрения, что только в этих двух формах и может воплощаться электронная информация – см., например: Бикмиев Р. Г., Бурганов Р. С. Собирание электронных доказательств в уголовном судопроизводстве // Информационное право. 2015. № 3. С. 18; Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. 2013. № 10. С. 23; Смахтин Е. В. Цифровые технологии и криминалистика: некоторые проблемные аспекты // Российский юридический журнал. 2018. № 4. С. 80. Не вполне понятно, почему указанные авторы игнорируют остальные формы доказательств.

Список литературы

1. Андреева Н. А. Правовая регламентация работы с электронными доказательствами в ходе досудебного уголовного производства // Совершенствование следственной деятельности в условиях информатизации: сб. материалов науч.-практ. конф. (Минск, 12–13 апреля 2018 г.). Минск: Редакция журнала «Промышленно-торговое право». С. 11–15.

2. Бикмиев Р. Г., Бурганов Р. С. Собирание электронных доказательств в уголовном судопроизводстве // Информационное право. 2015. № 3. С. 17–21.

3. Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. 2013. № 10. С. 22–24.

4. Воронин М. И. Электронные доказательства в УПК: быть или не быть? // Lex Russica. 2019. № 7 (152). С. 74–84.

5. Головко Л. В. Цифровизация в уголовном процесс: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 15–25.

6. Гришина Е. П. К вопросу об использовании электронных доказательств в уголовном судопроизводстве // Администратор суда. 2020. № 3. С. 31–34.

7. Зигура Н. А., Кудрявцева А. В. Компьютерная информация как вид доказательства в уголовном процессе России: монография. М.: Юрлитинформ, 2011. 176 с.

8. Ищенко П. П. Современные подходы к цифровизации досудебного производства по уголовным делам // Lex russica. 2019. № 12. С. 68–79.

9. Кувычков С. И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: автореф. дис. ... канд. юрид. наук. Н. Новгород, 2016. 34 с.

10. Курс уголовного процесса / Под ред. д. ю. н., проф. Л. В. Головко. М.: Статут, 2016. 1278 с.

11. Макарова О. В. Совершенствование судопроизводства путем внедрения электронной формы уголовного дела // Журнал российского права. 2019. № 2. С. 159–168.

12. Марфицин П. Г. Некоторые подходы к формулированию понятия «электронное доказательство» в уголовном судопроизводстве // Вестник Нижегородской академии МВД России. 2017. № 3 (39). С. 106–109.

13. Обидин К. В. Электронное доказательство: необходимый этап развития уголовного судопроизводства // Актуальные проблемы российского права. 2020. № 11. С. 198–206.

14. Оконенко Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дисс. ... канд. юрид. наук. М., 2016. 158 с.

15. Пастухов П. С. К вопросу о создании процедуры использования электронных доказательств» в уголовном судопроизводстве // Международное уголовное право и международная юстиция. 2015. № 2. С. 5– 8.

16. Смахтин Е. В. Цифровые технологии и криминалистика: некоторые проблемные аспекты // Российский юридический журнал. 2018. № 4. С. 78–83.

17. Стельмах В. Ю. Электронная информация в доказывании по уголовным делам: способы получения и место в системе доказательств // Библиотека криминалиста. 2018. № 3. С. 94–95.

18. Теория доказательств в советском уголовном процессе / отв. ред. Н. В. Жогин. Изд. 2-е, испр. и доп. М.: Юрид. лит., 1973. 736 с.

19. Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / отв. ред. С. В. Зуев. Москва: Издательство Юрайт, 2020. 193 с.

Maksim R. Glushkov

Head of the Laboratory for the Study of Problems of Procedural Activity of Investigative Bodies of the Research Department of the St. Petersburg Academy of the Investigative Committee of the Russian Federation (St. Petersburg, Russian Federation)

glushkov.mr@skspba.ru

ON THE ISSUE OF «ELECTRONIC EVIDENCE»

Abstract. The article presents the point of view that has spread in recent years that the specifics of the information presented in electronic form necessitates the allocation of a special category of evidence in criminal proceedings – the so-called electronic evidence. This approach is not shared by the author, the opinion is substantiated that working with electronic information and its carriers is possible with the help of available criminal procedural means.

Keywords: information in electronic form, evidence in criminal proceedings, electronic evidence, types of evidence, primary data source, copy and original.

УДК 347.9

Дубровский Вячеслав Владимирович
Ведущий эксперт
АНО «Лаборатория Судебных Экспертиз и Исследований»
(г. Москва, Российская Федерация)
forensicdv@yandex.ru

МЕТОДИЧЕСКИЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ СРАВНИТЕЛЬНОГО ИССЛЕДОВАНИЯ ПРОГРАММ ДЛЯ ЭВМ В ДЕЛАХ, СВЯЗАННЫХ С ЗАЩИТОЙ ПРАВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Аннотация. В статье рассматриваются особенности сравнительного исследования объектов интеллектуальной собственности – программ для ЭВМ – с позиций практического и методологического обеспечения данного вида исследований, основанного на практике проведения подобных исследований и защите их в судах Российской Федерации. Автором уделяется внимание методам сравнительного исследования и особенностям их применения при проведении исследований экспертами и специалистами. В статье также обозначаются проблемы, связанные с данными видом исследований в разрезе текущего развития экспертной практики.

Ключевые слова: информационные ресурсы, интеллектуальная собственность, программы для ЭВМ, исходный код, сравнение исходного кода.

Для цитирования:
Дубровский В. В. Методические и практические аспекты сравнительного исследования программ для ЭВМ в делах, связанных с защитой прав интеллектуальной собственности // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 61–72.

Программное обеспечение играет важную роль в жизни современного общества. Оно используется повсюду: от мобильных приложений на смартфонах до сложных систем управления производством в промышленности. Разработка программного обеспечения является одним из ключевых направлений развития экономики. Очевидным является и то, что с развитием технологий и увеличением числа разработчиков и самих разработок также растёт и количество судебных споров, которые так или иначе связаны с защитой правой интеллектуальной собственности на программы для ЭВМ.

Следует отметить, что юридически верным является понятие программа для ЭВМ, а не программное обеспечение, программа, ПО, софт или иные общеупотребительные термины. Согласно ст. 1261 ГК РФ программой для ЭВМ является представленная в объективной форме совокупность

данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определённого результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения[1]. Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы. При этом, при возникновении каких-либо споров, связанных с защитой авторских или исключительных прав, связанных с программами для ЭВМ речь неизбежно заходит о проведении судебной экспертизы или внесудебного исследования. В связи с вышеуказанным на первый план выходят вопросы о специальных познаниях и их объёме, методиках и возможности реализовать такие методики на практике.

Как следует из определения, программа для ЭВМ представляет собой информационный объект, состоящий из исходного текста, объектного кода, аудиовизуальных отображений, порождаемых программой, а также подготовительных материалов, полученных в ходе её разработки.

Исходный текст (также – исходный код) – это текст программы на любом языке программирования или языке разметки[2].

Необходимо отметить, что единой правовой позиции относительно иных понятий, входящих в состав определения программы для ЭВМ, в настоящий момент нет.

Так, отсутствует законодательное закрепление понятия объектного кода. С технической точки зрения, объектный код представляет собой скомпилированную программу для ЭВМ, однако ещё не исполняемый файл.

Аналогичным образом не решён вопрос с аудиовизуальными отображениями, порождаемыми программой для ЭВМ[3]. С одной стороны, исполнение программы порождает интерфейс, элементы управления, условные графические обозначения, цветовые решения, логотипы. С другой стороны, исполнение программы может порождать, например, компьютерную игру, которая состоит исключительно из графики.

Что считать подготовительными материалами остаётся неясным.

[1] Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_64629/ (дата обращения: 12.05.2023).

[2] ГОСТ Р 57429-2017 Судебная компьютерно-техническая экспертиза. Термины и определения // Электронный фонд нормативно-технической и нормативно-правовой информации «Кодекс» [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200144960 (дата обращения: 11.05.2023).

[3] Юрлов И. А. Правовой статус интерфейса компьютерных программ // Право и государство: теория и практика. 2017. № 10 (154). С. 61–64.

Возможно, законодатель имел в виду сопроводительную документацию.

На практике наиболее востребованными и репрезентативными являются исходный код программ для ЭВМ и её дистрибутив. Эти два объекта позволяют составить полное представление о том, как работает программа и какие функции она выполняет.

Защита интеллектуальных прав на программу для ЭВМ, как правило, связана с доказыванием факта нарушения такого права. Нередки случаи, когда работодатель или работник присваивают программу для ЭВМ или уходят с наработками и командой программистов в другую организацию. В каждой из таких ситуаций необходимо, проведя сравнительное исследование, установить, что речь идёт об одной и той же программе для ЭВМ.

Сравнительное исследование программ для ЭВМ предполагает проведение анализа двух программ для ЭВМ и ответ на вопрос о том, являются ли они тождественными полностью или частично. Такое исследование проводится в рамках компьютерно-технической экспертизы.

Данное направление в компьютерно-технической экспертизе не является распространённым. При этом почти каждый эксперт считает себя программистом настолько, что может прочитать, понять текст программы для ЭВМ на любом языке программирования и корректно его идентифицировать. По этой причине многие исследования, которые проводятся в данной области, имеют крайне низкое качество, вследствие бессистемности, отсутствия какого-либо методического обеспечения, отсутствия конкретных методов, которые позволили бы получить объективный и обоснованный результат.

Таким образом, целью данной статьи является формирование единообразного представления об идентификационных признаках программ для ЭВМ, способах и методах получения информации об обстоятельствах и процессе их создания, подходах к сравнительному исследованию и критериях оценки его результатов.

В настоящий момент судебная практика насчитывает достаточно много громких дел, связанных с защитой интеллектуальных прав на программы для ЭВМ. Среди них можно выделить такие, как ООО «Альтель» против «Нума Технологии»[4], АО «СткалерСофт» против Бутенко А. В.[5], Мамичев А. Е. против ООО «Интервим»[6]. По

[4] Ализар А. В России заведено уголовное дело за плагиат исходного кода // Хабр [Электронный ресурс]. 2019, 26 сентября. URL: https://habr.com/ru/news/469069/ (дата обращения:10.05.2023).

[5] Воейко Д. Дочь и коллеги покойного создателя знаменитого российского ПО начали войну за его наследие // CNews [Электронный ресурс]. 2021, 18 августа. URL: https://biz.cnews.ru/news/top/2021-08-18_za_nasledie_sozdatelya_znamenitogo (дата обращения:10.05.2023).

[6] Аразуманян А. Дело Антона Мамичева: как программист изменил Гражданский кодекс // Skillbox Media [Электронный ресурс]. 2022, 22 августа. URL: https://skillbox.ru/media/code/programmist-vs-

каждому из этих дел проводились и досудебные исследования, и судебные экспертизы. В некоторых из них автору статьи удалось поучаствовать лично.

С экспертной точки зрения программа для ЭВМ, как объект исследования, может быть представлена в различной форме:

1) с точки зрения носителя:
- на материальном носителе;
- в облачном хранилище;
- в репозитории;

2) с точки зрения формы:
- исходный код в виде файлов;
- исходный код, полученный из Роспатента;
- дистрибутив;
- скомпилированный исходный код.

Носитель, на котором представлен объект исследования требует от эксперта или специалиста корректной идентификации, как самого носителя, так и его содержимого. Стадия идентификации является неотъемлемой частью любого исследования. Сложностью в данном случае является лишь то, что необходимо идентифицировать и объект-носитель, и непосредственный объект исследования.

В случае, когда объект представлен на материальном носителе способ идентификации зависит от вида такого носителя. При этом необходимо помнить о процедурах, предотвращающих повреждение данных на носителе – использовании программных или аппаратных блокираторов, создании образов или криминалистических копий носителя с использованием специализированного программного обеспечения (Access Data FTK, PC 3000, Acronis True Image, Acronis Disk Director) или операционных систем (Kali Linux, CAINE). Как правило, программы для ЭВМ предоставляются на исследование на оптических дисках или флэш-накопителях. Идентификационными признаками оптического диска являются: его тип, объём, серийный номер вокруг посадочного кольца, надписи, нанесённые на стороне, не предназначенной для записи. Для флэш-накопителя идентификационными данными являются объём, цвет и серийный номер. Серийный номер можно получить, воспользовавшись вышеуказанным программным обеспечением или с помощью программного обеспечения «Victoria HDD».

В случаях, когда объект представлен в облачном хранилище основными идентификационными признаками объекта-носителя становится ссылка на страницу загрузки и дата обращения к ней. Фактически, в данном случае достаточно сделать снимок экрана, указывающий на имя файла или файлов, расположенных в хранилище и описать процесс доступа к нему в заключении или отчёте. Далее необходимо сохранить файл(-ы) на рабочую станцию и идентифицировать их.

grazhdanskiy-kodeks-delo-antona-mamicheva/ (дата обращения:10.05.2023).

С точки зрения идентификации репозиторий является одним из самых информативных и методологически обделённых носителей программ для ЭВМ. Репозиторий представляет собой хранилище системы контроля версий, который непосредственно интегрирован в процесс разработки программы для ЭВМ. Репозиторий также является облачным хранилищем, однако может располагаться на локальных серверных мощностях. Основным его отличием от иных систем хранения является возможность идентифицировать каждый этап жизненного цикла каждого отдельного файла. Репозиторий является незаменимым источником информации в тех случаях, когда помимо сравнения необходимо также определить вносились ли в исходный код программы какие-либо изменения.

Идентификация непосредственного объекта исследования может быть выполнена путём создания листинга файлов с указанием контрольных сумм, например с использованием программы «Directory Lister Pro». В случае с материалами, предоставленными Роспатентом, исходный код программы предоставляется либо в печатном виде, либо в формате «.pdf»-файла, что оказывает влияние на возможность применения автоматизированных средств анализа.

Следует отметить, что сравнение программ для ЭВМ в зависимости от формы представления может требовать их приведение к единому виду. Например, в некоторых случаях исходный код программы может быть обфусцирован, иными словами, запутан[7], в том числе для того, чтобы затруднить его анализ. Другим примером может служить представление на исследование скомпилированного исходного кода, который необходимо сравнить с исходным кодом, который не был компилирован. В этом случае может потребоваться декомпиляция, которая выполняется специализированным программным обеспечением, специфичным для каждого из языков программирования.

Дальнейшее сравнительное исследование сводится к выделению критериев и их обоснованию. Именно на данном этапе большинство исследований переходят в область догадок и предположений. Зачастую, сравнение программ для ЭВМ проводится визуально либо с использованием программного обеспечения для поиска заимствований в тексте (например, AntiPlagiarism.Net), используя одну программу, как основу для поиска заимствований в другой. Однако такой подход к исследованию не может привести к объективному результату, поскольку:

1. Программы для ЭВМ, использующие одинаковые языки программирования, в любом случае будут иметь совпадающие участки, как минимум, поскольку синтаксис таких программ будет тождественен. Нельзя

[7] Варновский Н. П., Захаров В. А., Кузюрин Н. Н., Шокуров А. В. Современное состояние исследований в области обфускации программ: определения стойкости обфускации // Труды ИСП РАН. 2014. № 3. С. 167–198.

по-другому вызвать функцию, или иначе описать переменную.

2. Современный подход к разработке предполагает широкое использование сторонних библиотек. Поскольку программа для ЭВМ может содержать значительное количество таких сторонних библиотек, процент совпадений при сравнении также окажется крайне высоким.

3. Некоторые программы для ЭВМ могут иметь общую основу, например, при сравнении всех операционных систем на базе Linux будет обнаружено поразительное количество совпадений, которые никак не связаны с заимствованием.

4. Программа может быть модифицирована, удалены комментарии, переименованы названия переменных и функций.

5. На результат сравнения могут оказывать влияние настройки программы, с помощью которой проводится анализ. Настройки могут оказывать влияние на точность результата.

6. Не все заимствования являются уникальными. Как правило, помимо вопроса о тождестве, на исследование также ставится вопрос о том, выполняет ли заимствованный исходный код основополагающую функций;

7. Не все файлы, присутствующие в программе для ЭВМ, являются результатом интеллектуальной деятельности автора. Некоторые файлы являются техническими и создаются автоматически.

Визуальный метод сравнения, безусловно, является одним из методов анализа, однако не может являться единственным, поскольку не позволяет получить объективный результат, даже в тех случаях, когда исходный код программы для ЭВМ представлен единственным файлом.

Фактически для того, чтобы провести корректное сравнение двух программ для ЭВМ необходимо учесть все особенности, описанные выше в п.1–7.

Программы для ЭВМ могут состоять из сотен или тысяч файлов и ещё большего количества строк кода, поэтому сперва необходимо оценить состав программы, например, с использованием программы «cloc» (https://github.com/AlDanial/cloc). Преимущество данной программы заключается в распределении строк исходного кода по языкам программирования, а также подсчёт количества пустых строк и комментариев. Уже на данном этапе можно получить полезную информацию об исследуемых объектах, выбрать необходимый инструментарий, определить пригодность представленных объектов для проведения сравнительного анализа. Например, если уже на этом этапе видно, что одна программа для ЭВМ написана на языке программирования «Swift», а другая на «JavaScript», «HTML» и «CSS», то

очевидным является тот факт, что это разные программы[8].

Как говорилось выше, не имеет смысла сравнивать программы для ЭВМ до тех пор, пока в их составе присутствуют библиотеки третьих лиц (сторонние библиотеки). Для того, чтобы идентифицировать их в исходном коде имеет смысл воспользоваться следующими методами:

1. Поиск файлов, содержащих ключевые слова «LICENSE», «COPYRIGHT», «APACHE», «GPL», «BSD» и иным, связанным с лицензиями и их типами.

2. Поиск каталогов с наименованиями «libraries», «TPL», «3PL», «third-party», в которые, как правило помещаются сторонние библиотеки при динамическом типе связанности.

3. В некоторых случаях в состав программы для ЭВМ включается отдельный файл с правовыми уведомлениями.

Существуют автоматизированные средства поиска, входящие, например, в состав анализаторов безопасности исходного кода. В случаях, когда информацию о библиотеках третьих лиц идентифицировать не удаётся, разумным будет запросить её у правообладателей.

Сравнительный анализ программ для ЭВМ требует тщательной проверки всех источников, используемых для формирования выводов. Нередки случаи, когда часть исходного кода намеренно выкладывают в общедоступный репозиторий для того, чтобы эксперт счёл его библиотекой третьих лиц и исключил из объёма сравнения.

Аналогичным образом, не имеет никакого смысла сравнивать программы для ЭВМ, из которых не удалены технические файлы. Данные файлы не имеют никакого значения для сравнения, поскольку не несут в себе идентификационных признаков. К таким файлам относятся «.git», «CMake», «.config».

Как говорилось выше, сравнение программ для ЭВМ проводится по критериям, которыми являются результаты использования отдельных методов. Возможно выделить следующие методы сравнения:

I. Статический анализ: применяется для анализа исходного кода.

1. Анализ иерархической логической структуры программ для ЭВМ – включает в себя анализ взаиморасположения каталогов, подкаталогов и файлов, с учётом их наименований. Данный вид анализа достаточно удобно выполнять с использованием специализированного программного обеспечения, например BeyondCompare или аналогов. Данный метод позволяет сравнить структуру каталогов, выделить схожие файлы или обнаружить тождественные.

2. Анализ метрик исходного кода программы для ЭВМ – с использованием упоминавшейся выше программы «cloc» возможно посчитать

[8] SWIFT – язык программирования для iOS, JavaScript, HTML, CSS – используется в веб-разработке

достаточно простые метрики, например плотность исходного кода, плотность комментариев, число строк. Наибольший интерес представляют прежде всего комментарии. Их наличие и количество является серьёзным заделом для дальнейшего исследования.

3. Анализ метаданных авторства. Под метаданными авторства понимаются любые артефакты, указывающие на принадлежность программы для ЭВМ. Это могут быть названия программы для ЭВМ, имена и фамилии авторов, даты создания, копирайты, уникальные комментарии. Как правило именно по совпадению комментариев возможно определить совпадающие участки. Указание знака охраны авторского права не является обязательным, однако широко применяется. Как правило, копирайт генерируется и добавляется в заголовок файла исходного кода автоматически. К метаданным авторства также следует относить файлы документации, например «.md» файлы, а также «README» и «LICENSE».

4. Анализ метрик сложности[9] исходного кода. Наиболее простой в расчётах метрикой является цикломатическая сложность программы для ЭВМ или метрика Мак-Кейба. Данное значение является уникальным и не зависит от модификаций, связанных с переименованием функций или переменных.

5. Анализ словарей программы для ЭВМ. Суть данного метода заключается в индексации программы для ЭВМ специализированным программным обеспечением для поиска файлов, по ключевым словам, выгрузки словаря в файл. В дальнейшем словари сравниваются между собой с использованием программного обеспечения для поиска дубликатов в тексте.

6. Сравнение текста. Как правило, данный метод применяется в том случае, когда в составе исходного кода имеются файлы с тождественным наименованиями, но различным содержимым. Для сравнения можно использовать программное обеспечение WinMerge или BeyondCompare. Данный этап является достаточно уязвимым, поскольку требует от эксперта вчитываться в исходный код программы и понимать, на что влияет то или иное изменение в тексте.

7. Ручной поиск. К сожалению, в случае с предоставлением исходного кода в формате «.pdf» вышеуказанные методы можно применять только после использования средств автоматизированного распознавания текст (OCR). Поскольку данный способ перевода в текст может повлечь искажение его содержания, необходимо перепроверять данные,

[9] Звездин С. В. Проблемы измерения качества программного кода // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2010. № 2 (178). С. 62–66; Новичков А. Н. [и др.]. Метрики кода и практическая реализация по их сбору и анализу. Часть 1 – метрики // CNewsКлуб [Электронный ресурс]. URL: https://club.cnews.ru/blogs/entry/metriki_koda_i_prakticheskaya_realizatsiya_po_ih_sboru_i_analizu_chast_1_ (дата обращения: 12.05.2023).

которые получены другими методами, вручную. Депонированный исходный код лишь в редких случаях содержит программу для ЭВМ в полном объёме. Как правило, такие материалы содержат отдельные фрагменты или файлы исходного кода. В данном случае имеет смысл производить поиск по именам файлов, комментариям, характерным наименованиям функций и переменных, а затем производить сравнение текста.

8. Использование автоматизированных средств анализа. Существуют автоматизированные средства поиска дубликатов в исходном коде. Данные средства могут использовать как уже описанные, так и иные методы анализа, например, токенизацию (строки, вне зависимости от текста преобразуется в токены). В данном случае можно отметить CCFinder[10].

II. Динамический анализ: применяется для анализа дистрибутивов.

1. Трассировка установки программы для ЭВМ. Исполняемый файл является самораспаковывающимся архивом. Такая особенность позволяет отследить пути распаковки. В некоторых случаях эта информация может позволить идентифицировать установку стороннего программного обеспечения совместно с основной программой и не включать их в сравнение.

2. Анализ исполняемого файла. Исполняемые файлы также содержат текстовое содержимое. Его количество достаточно мало, однако может содержать метаданные, указывающие на принадлежность программы для ЭВМ, которые могут позволить её идентифицировать.

3. Дизассемблирование и отладка. Дизассемблеры и отладчики являются инструментами реверс-инжиниринга, однако также могут помочь понять, к каким данным обращается программа для ЭВМ, каков алгоритм её работы. Применение данного метода достаточно затруднено, ввиду необходимости наличия у лица, проводящего исследование, знаний низкоуровневого языка ассемблер.

4. Анализ распакованных файлов. Распакованные и установленные в операционную систему файлы программы для ЭВМ могут анализироваться и сравниваться с применением методов статического анализа.

5. Анализ пользовательского интерфейса. В тех случаях, когда программа для ЭВМ имеет клиентскую часть, целесообразно начать сравнение с интерфейса инсталлятора, изучить пользовательское соглашение. Нередки случаи, когда сам инсталлятор выполнен столь специфично, что позволяет судить о наличии заимствований. Далее необходимо сравнивать сведения о программе, включая её версию (обычно доступны во вкладках «About» или по графическому обозначению «?» в верхней панели

[10] Toshihiro K., Shinji K. Katsuro I. CCFinder: A multilinguistic token-based code clone detection system for large scale source code // IEEE Transactions on Software Engineering. 2002. Vol. 28. Pp. 654–670. DOI: 10.1109/TSE.2002.1019480.

управления). Сущность данного метода заключается в сравнении элементов интерфейса, вкладок, графических элементов.

6. Анализ функциональных возможностей. Применяется путём выполнения действий в программе для ЭВМ с целью описания её функциональных возможностей. В тех случаях, когда программа для ЭВМ не имеет клиентской части применение данного метода может основываться на сопроводительной документации, при её наличии, а также системах постановки задач, таких как «Jira», «YouTrack», доступ к которым имеет смысл запрашивать на формирования требований к объектам исследования.

К сожалению, сущность данного вида исследований такова, что объективный результат сравнения может быть получен только путём применения всех методов исследования. Каждый из них выполняет свою роль, обосновывая совпадения с точки зрения текста, математически, визуально. Во всех случаях результаты анализа должны иметь формальное выражение. Например, если рассчитываются метрики, то необходимо приводить формулы, описывать значения и источник их происхождения, строить таблицы. Применяя методы, имеющие визуальное выражение, например сравнение текста, разумно подкреплять логические выкладки иллюстративным материалом, обеспечивая тем самым соответствие результатов исследования требованиям ст. 4, 8 Федерального закона № 73 «О государственной судебно-экспертной деятельности в Российской Федерации»[11]. Практика рецензирования заключений показывает, что эксперты и специалисты зачастую проводят анализ делая упор на применение сравнения текста, о чём говорилось выше. Достаточно часто встречаются заключения, в которых исследование проводится с использованием линеек, штангенциркулей, луп, тогда как реально применяемое программное обеспечение или оборудование не указывается в Заключении. Отсутствие такой информации, в том числе о версии программного продукта, не позволяет другому специалисту повторить выполненные в ходе исследования действия, поскольку использование различного программного обеспечения может повлиять на результат исследования. Таким образом, нарушается принцип повторяемости.

Проблемным местом сравнительного анализа является необходимость обеспечить обоснованность каждого из применяемых методов. Зачастую суды с гораздо большим энтузиазмом воспринимают результаты исследования, основанные на результатах визуального анализа. Остаётся большим вопросом, как эксперт может оценить тысячи строк исходного кода визуально. Методы

[11] Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // Информационно-правовой портал «Гарант.ру» [Электронный ресурс]. URL: https://base.garant.ru/12123142/ (дата обращения: 12.05.2023).

математического анализа точны и объективны, однако имеют низкую наглядность, что требует тщательного методического обоснования возможности применения каждого из них и значения, которое они имеют, как критерии сравнительного исследования.

Сравнительное исследование программ для ЭВМ является сложным именно с точки зрения практической применимости, тогда как теоретических разработок, связанных с разработкой методов сравнения исходного кода или даже программного обеспечения для этого, нет[12]. Однако теоретические разработки, сколь точны бы не были результаты, получаемые в рамках них, не учитывают ни реального состава исходного кода, ни способов его предоставления, ни объёмов. Применить результаты таких научных изысканий на практике невозможно.

Цифровая трансформация, которая является одной из национальных целей развития России до 2030 года, неразрывно связана с другим реализуемым в стране масштабным проектом – по импортозамещению в сфере информационно-коммуникационных технологий[13]. При этом, достаточно многие зарубежные программы для ЭВМ пытаются выдать за отечественные, что делает сравнительные исследования, в какой-то мере необходимым элементом анализа, например, для включения в Реестр отечественного ПО. Цифровая трансформация – это глобальный процесс, который затрагивает в том числе и судебной-экспертную деятельность. В настоящий момент методический аппарат компьютерно-технической экспертизы сосредоточен на изъятии и анализе данных в различных источниках информации: мобильных устройствах, документах, операционных системах. Интеллектуальная собственность, которая также требует специальных знаний и соответствующих исследований, существующими методиками никак не покрывается. Исследование программ для ЭВМ, как с точки зрения исходного кода, так и в целом, требует разработки единого методического аппарата, учитывающего особенности различного программного обеспечения, позволяющего повысить объективность и обоснованность получаемых результатов в соответствии с принципами судебно-экспертной деятельности.

[12] Осадчая А. О., Исаев И. В. Метод поиска клонов в программном коде // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 5. С. 716–719. DOI: 10.17586/2226-1494-2020-20-5-714-721.

[13] Шувалова М. Импортозамещение в сфере IT // Информационно-правовой портал «Гарант.ру» [Электронный ресурс]. 2022, 4 мая. URL: https://www.garant.ru/article/1542142/ (дата обращения: 12.05.2023).

Список литературы

1. Toshihiro K., Shinji K. Katsuro I. CCFinder: A multilinguistic token-based code clone detection system for large scale source code // IEEE Transactions on Software Engineering. 2002. Vol. 28. Pp. 654–670. DOI: 10.1109/TSE.2002.1019480.

2. Варновский Н. П., Захаров В. А., Кузюрин Н. Н., Шокуров А. В. Современное состояние исследований в области обфускации программ: определения стойкости обфускации // Труды ИСП РАН. 2014. № 3. С. 167–198.

3. Звездин С. В. Проблемы измерения качества программного кода // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2010. № 2 (178). С. 62–66.

4. Новичков А. Н. [и др.]. Метрики кода и практическая реализация по их сбору и анализу. Часть 1 – метрики // CNewsКлуб [Электронный ресурс]. URL: https://club.cnews.ru/blogs/entry/metriki_koda_i_prakticheskaya_realizatsiya_po_ih_sboru_i_analizu_chast_1_ (дата обращения: 12.05.2023).

5. Осадчая А. О., Исаев И. В. Метод поиска клонов в программном коде // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 5. С. 714–721. DOI: 10.17586/2226-1494-2020-20-5-714-721.

6. Юрлов И. А. Правовой статус интерфейса компьютерных программ // Право и государство: теория и практика. 2017. № 10 (154). С. 61–64.

Vyacheslav V. Dubrovsky
Leading Expert
ANO «Laboratory of Forensic Investigations and Research»
(Moscow, Russian Federation)
forensicdv@yandex.ru

METHODOLOGICAL AND PRACTICAL ASPECTS OF COMPARATIVE EXAMINATION OF COMPUTER PROGRAMS IN CASES RELATED TO THE PROTECTION OF INTELLECTUAL PROPERTY RIGHTS

Abstract. The article deals with the peculiarities of comparative research of intellectual property objects - computer programs with practical and methodological support of this type of research based on the practice of such research and their protection in courts of the Russian Federation. The author pays attention to the methods of comparative research and peculiarities of their use in conducting research by experts and specialists. The article also outlines the problems associated with this type of research in the context of the current development of expert practice.

Keywords: computer science, information resources, law, intellectual property, computer programs, source code, expertise, methodology, source code comparison.

УДК 343.131

Зуев Сергей Васильевич
доктор юридических наук, доцент,
профессор кафедры судебной и правоохранительной деятельности,
Южно-Уральский государственный университет
(национальный исследовательский университет)
(г. Челябинск, Российская Федерация)
zuevsergej@inbox.ru

ПРОЦЕССУАЛИЗАЦИЯ ЦИФРОВОЙ СРЕДЫ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Аннотация. В статье автор утверждает, что применение цифровых технологий требует дополнительной правовой регламентации в Уголовно-процессуальном кодексе. В частности, это касается деятельности адвоката-защитника. Обращается также внимание, что чрезмерная процессуализация деятельности органов расследования и суда превращает данный закон в Инструкцию, что усложняет его восприятие и возводит возможно несущественные требования в ранг законности.

Ключевые слова: цифровизация, уголовный процесс, право, электронная информация.

Для цитирования:
Зуев С. В. Процессуализация цифровой среды уголовного судопроизводства // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 73–76.

В настоящее время уголовный процесс испытывает некую трансформацию в связи с развитием цифровизации во всех сферах жизнедеятельности человека. Уголовное судопроизводство не может оставаться в стороне. Однако, в отличие от многих других социальных явлений, уголовное судопроизводство в большей степени процессуальное. Уголовно-процессуальный кодекс предназначен для правовой регламентации действий и решений по уголовным делам. При этом просматривается ярко выраженная процедурность, то есть последовательность, а значит порядок. Возникает вопрос: насколько цифровизация должна найти отражение в упомянутом законе. Как определить соотношение «процессуального» и «организационно-технического» обеспечения использования цифровых технологий при производстве по уголовным делам?

В последнее время в литературе можно встретить критику в адрес уголовного судопроизводства в связи с излишне подробной регламентацией в

законе тех или иных процессуальных действий и решений.

А. М. Баранов отмечает, что «кроме усложнения процедуры производства и увеличения сроков расследования, ситуация, с точки зрения законности и обоснованности осуществляемых действий и принимаемых решений в досудебном производстве, не меняется в лучшую сторону»[1].

Представляется, что нельзя легко взять и отказаться от привычного законодательного регулирования уголовного процесса. Дело в том, что за требованиями Уголовно-процессуального кодекса по порядку проведения действия или принятия решений скрываются требования к законности, а значит и к допустимости доказательств.

Согласно ч. 2 ст. 146 УПК РФ в постановлении о возбуждении головного дела указываются: 1) дата, время и место его вынесения; 2) кем оно вынесено и т. д. Возможно, кому-то может показаться, что это следует отнести к делопроизводству. Но с датой и временем связаны сроки расследования и возможное время задержания подозреваемого в совершении преступления. Кем вынесено постановление имеет значение для решения вопросов правосубъектности. Данное постановление может быть вынесено теми, кто указан в ч. 1 ст. 145 УПК РФ. Если постановление вынесено другим лицом, то оно будет незаконным.

Изъятию электронных носителей информации и копированию электронной информации посвящена ст. 164.1 УПК РФ. Нарушения требований, в ней указанных, следует считать существенными, что должно влечь признание полученных доказательств недопустимыми.

В настоящее время на рассмотрении Государственной Думы находится законопроект с предложением внедрить электронный документооборот в уголовный процесс. В частности, предусматривается осуществить правовую регламентацию вопросов, связанных с использованием электронной подписи. При этом отдельным лицам может показаться, что указанное следует вывести за рамки Уголовно-процессуального кодекса. Но тогда возникнут сложности с реализацией соответствующего права обвиняемого, закрепленного в п. 2 ч. 4 ст. 47 УПК РФ, что всегда рассматривалось как нарушение права на защиту.

Вместе с тем В. Н. Григорьев отмечает, что существует «очевидный тренд последнего времени – низведение процессуальной формы к административному регламенту, что не соответствует ни ее природе, ни предназначению, особенно если учесть сложный, творческий характер деятельности следователя, судьи, прокурора, да и дознавателя»[2].

Однако деятельность защитника требует дополнительной

[1] Баранов А. М. Уголовно-процессуальная политика России: вчера, сегодня, завтра // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 20.

[2] Григорьев В. Н. Уголовно-процессуальная форма и административный регламент: современные тренды // Вестник СПбГУ. Право. 2018. Т. 9. № 1. С. 44.

правовой регламентации в УПК РФ. По мнению А. С. Каменева, более подробная правовая регламентация способов собирания доказательств адвокатом позволит признать их процессуальными действиями, что также положительно скажется на порядке получения электронной информации по уголовным делам[3]. С этим можно согласиться, так как это позволит в какой-то степени контролировать законность действий самого адвоката. В этом просматривается и наделение защитника обязанностями по доказыванию невиновности своего подзащитного или сбора доказательственной информации, способной положительно повлиять на итоговое решение по уголовному делу.

Таким образом, с одной стороны, чрезмерная процессуализация деятельности органов расследования и суда усложняет текст закона и превращает его в инструкцию по делопроизводству. С другой, применение цифровых технологий требует дополнительной правовой регламентации в Уголовно-процессуальном кодексе.

Список литературы

1. Баранов А. М. Уголовно-процессуальная политика России: вчера, сегодня, завтра // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 16–22.

2. Григорьев В. Н. Уголовно-процессуальная форма и административный регламент: современные тренды // Вестник Санкт-Петербургского университета. Право. 2018. Т. 9. № 1. С. 42–51.

3. Каменев А. С. Процессуальные действия адвоката (защитника) по уголовным делам: проблема правовой регламентации порядка получения электронной информации // Вестник Южно-Уральского государственного университета. Серия: Право. 2022. Т. 22. № 3. С. 21–27.

Sergey V. Zuev
Doctor of Law, assistant professor,
professor of the Department of Judicial and Law Enforcement Activities
South Ural State University (national research university)
(Chelyabinsk, Russian Federation)
zuevsergj@inbox.ru

THE MAIN DIRECTIONS OF CONVERGENCE OF PHYSICS AND LAW IN CRIMINAL PROCEEDINGS UNDER CONDITIONS OF DIGITALIZATION

[3] Каменев А. С. Процессуальные действия адвоката (защитника) по уголовным делам: проблема правовой регламентации порядка получения электронной информации // Вестник Южно-Уральского государственного университета. Серия: Право. 2022. Т. 22. № 3. С. 24.

Abstract. In the article the author states that digitalization leads to convergence of exact sciences and humanities, in particular physics and law in criminal proceedings. Determines the main directions of this phenomenon, which are associated with the development of information relations in the criminal proceedings, with the widespread use of electronic means of proof in criminal cases, as well as the interaction of material criminal procedure objects.

Keywords: digitalization, criminal procedure, physics, law, electronic information.

УДК 343.98

Иванов Владислав Юрьевич
Преподаватель кафедры криминалистики
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
blad02051995@mail.ru

Мышляшина Валерия Сергеевна
Курсант факультета подготовки следователей
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
vvmaussleria@gmail.com

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ЖЕСТОКОГО ОБРАЩЕНИЯ С ЖИВОТНЫМИ

Аннотация. В статье анализируется следовая картина, возникающая в результате совершения преступления, предусмотренного ст. 245 УК РФ. Авторы акцентируют внимание на необходимость изучения страниц социальных сетей преступника в целях поиска криминалистически значимой информации. Рассматривается целесообразность привлечения к следственному осмотру специалистов не только в области ветеринарии, но и информационно-телекоммуникационных технологий.

Ключевые слова: жестокое обращение с животными, осмотр места происшествия, осмотр животных и их трупов, использование специальных знаний.

Для цитирования:
Иванов В. Ю., Мышлянина В. С. Использование информационно-телекоммуникационных технологий и специальных знаний при расследовании жестокого обращения с животными // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 77–84.

Успешное расследование большинства преступлений зависит от эффективного использования специальных знаний. Исключением не является и жестокое обращение животными. Учитывая специфику преступления, предусмотренного ст. 245 УК РФ, вопрос использования специальных знаний требует отдельного внимания.

Следует согласиться с устоявшимся мнением о том, что в судебно-следственной практике реализуется две основные формы использования специальных знаний:

процессуальные и непроцессуальные[1]. В первом случае речь идёт о привлечении специалистов для участия в следственных действиях и производстве судебных экспертиз. Во втором – о получении консультационной помощи в узких областях знаний, необходимых для эффективного и качественного расследования уголовных дел. Наиболее сложным, но и достаточно большим значением в этом ряду обладают судебные экспертизы. Поэтому на это в настоящей работе будет смещён акцент.

С учётом развития информационно-телекоммуникационных технологий, общественный резонанс вызывают случае жестокого обращения с животными с последующим демонстративным распространением записей таких издевательств через информационно-телекоммуникационные сети.

На современном этапе развития криминалистических знаний вопросы расследования преступлений всё чаще стали рассматриваться через призму цифровой трансформации. В результате совершения практически любого преступления образуются цифровые следы, которые, вероятно, имеют весомое доказательственное значение. Их должное исследование целесообразно проводить с использованием современных возможностей криминалистического оборудования. В процессе исследования, сбора и фиксации таких следов по преступлениям, квалифицируемым по статье 245 УК РФ, необходима помощь именно такого лица, которое посредством имеющихся у него специальных знаний окажет содействие в решении указанных выше задач, не забывая о познаниях в сфере зоологии и ветеринарии.

Необходимо учитывать тактику производства конкретных следственных действий при расследовании указанного состава преступления. Знаний, которыми обладает следователь (дознаватель) в области ветеринарии и других смежных областей, недостаточно, чтобы установить все обстоятельства преступления[2]. Затруднение, в первую очередь, здесь возникает в связи с отсутствием нужного специалиста. По итогу нарушается требуемый порядок описания, используется ошибочная или неточная номенклатура. Прежде всего, это объясняется отсутствием таких специалистов в системе органов внутренних дел, что, в свою очередь, усложняет процесс их привлечения к участию в следственных действиях, что может повлечь утрату или уничтожение важных доказательств по уголовному делу[3]. В целом, расследование случаев жестокого обращения с животными требует

[1] Варданян А. В. Современные проблемы использования специальных знаний в уголовном судопроизводстве // Юрист-Правоведъ. 2019. № 2 (89). С. 160.

[2] Тебиев Р. Р. Методика расследования жестокого обращения с животными: дис. ... канд. юрид. наук. Москва, 2022. С. 147.

[3] Мосина С. В., Андроник Н. А. Актуальные проблемы расследования жестокого обращения с животными на первоначальном этапе: теоретико-прикладной анализ // Вестник Уфимского юридического института МВД России. 2022. № 3 (97). С. 118

специализированных знаний и опыта криминалиста, а также тесного сотрудничества с другими профессионалами: ветеринарами, организациями по защите животных, судебными экспертами и правоохранительными органами.

В целях бесспорной объективности требуется захватывать сферы судебной медицины, судебной ветеринарии, зоологии, трасологии.

Криминалист должен понимать анатомию и физиологию животных, а также знать особенности различных видов животных и их поведение. Это поможет ему понять, какие травмы и травматические повреждения могут быть вызваны определёнными видами жестокости. Следователь также должен иметь опыт в сборе и обработке физических доказательств, таких как кровь, волосы, кости, и другие следы, чтобы идентифицировать жертву, определить механизмы, использованные в преступлении, а также установить время и место его совершения; должен быть знаком с законами, которые регулируют жестокое обращение с животными, чтобы помочь в обеспечении справедливого расследования и привлечении к ответственности виновных лиц.

При обращении к специалистам, правильным будет прибегнуть к помощи ветеринаров, которые могут оказать неоценимую помощь, определив характер и тяжесть травм, которые были нанесены животному. Они также могут установить возраст животного, его состояние здоровья, и наличие других признаков, указывающих на жестокое обращение. Ветеринар может выдать заключение о том, было ли животное убито или его мучали на протяжении длительного времени; определить повреждения механического происхождения, вызванные действием крайних температур, последствия электротравмы; выявить факт происхождения какого-либо заболевания животного от нарушений режима кормления (патогенез, клинические симптомы, патоморфологические изменения). Например, эксперту следует учитывать, что в большинстве случаев алиментарное истощение может осложняться другими заболеваниями, такими, как пневмония, катаральный гастроэнтерит и т. д. В заключение эксперта всегда необходимо указать, чем вызвано истощение: недокормом или хроническим заболеванием, если нет этого указания, то заключение считается неправильным.

Важность обращения при расследовании данной категории дел к специалистам обосновывается также наличием в ветеринарных клиниках профессионального оборудования, которое позволяет использовать радиологию, визуализацию, пульсоксиметрию и т. п., обеспечивая получение более точных сведений о состоянии животного, природе его повреждений, причинах гибели.

Также, возможным будет оценить условия содержания животного. Этот этап проводится с целью оценки условий содержания животного в домашних условиях или на территории животноводческих хозяйств и зоопарков. Эксперты могут определить, соответствуют ли условия содержания животного установленным нормам и требованиям, и в какой

степени они влияют на его здоровье и благополучие. При этом осуществляется проверка не только на соответствие требованиям гигиены и безопасности, но и на комфортность условий содержания для конкретного вида животного. Может рассматриваться площадь помещения, в котором содержится животное, условия питания, его регулярность и правильность, соответствие рациона. Ещё одним важным критерием оценки является проверка его здоровья и наличия медицинского ухода. Эксперты оценивают, соответствует ли состояние животного его возрасту и породе, выявляют наличие признаков заболевания: кашель, насморк, кожные высыпания, а также наличие ран, переломов или других травм. Проводится оценка наличия необходимых прививок и лечения, которые требуются для данного вида животных и т. д.

Организации по защите животных могут оказать помощь в обнаружении свидетелей, которые могут дать полезные сведения о жестоком обращении. Они также могут предоставить финансовую помощь для лечения пострадавших животных и помочь в их устройстве на новое место жительства. К тому же, данные организации в большинстве случаев проявляют инициативу в собирании информации, посредством использования собственных форумов с неравнодушными сторонниками их дела, изучения социальных сетей.

Вследствие совершения такого преступления, как жестокое обращение с животными, вероятно, понадобится произвести обследование животного с целью установления его общего состояния, исследование трупа животного с определением причин его смерти, исследование фотографий или видеозаписей, содержащих факт жестокости по отношению к животному с возможностью определить, какие действия были совершены. В этом случае встанет необходимость изучения цифровых следов.

Для более эффективного расследования преступлений необходимо обращать особое внимание на изъятие и исследование компьютерных устройств, таких как смартфоны и ноутбуки, которые могут содержать важную криминалистически значимую информацию, хранящуюся в памяти электронных устройств. Особое внимание следует уделять содержанию галереи – видео и фото. Также важным представляется проанализировать личные страницы в социальных сетях и переписки, так как там, в «своих кругах», обычно обсуждаются происшествия, пересылаются и распространяются различные фото- и видеоматериалы, которые в свою очередь могут иметь значение в расследовании уголовного дела.

Использование компьютерных технологий и электронно-цифровых доказательств стало неотъемлемой частью современных методов расследования жестокого обращения с животными в России. Среди наиболее распространённых технологий можно выделить программные и аппаратные средства, специальные приложения и сервисы, а также методы сбора и анализа данных.

Так, ярким примером задействования современных

технологий является применение системы ГЛОНАСС или специальных трекеров для отслеживания движения животных. Такая система может быть полезна при поиске пропавших животных или при их спасении.

Например, технологии отслеживания оленей в настоящее время широко применяются на территории Российской Федерации[4]. Данную разработку в дальнейшем было бы допустимо распространить для контроля перемещений домашних животных. Также, при помощи данных устройств, можно наблюдать специфичное поведение животного: учитывая те же перемещения, специалист в области ветеринарии или зоологии может указать на какие-либо особенности, свойственные животному.

Кроме того, использование компьютерных технологий позволяет проводить дистанционное наблюдение за животными, например, с помощью камер видеонаблюдения. Такие технологии могут быть полезными при выявлении случаев жестокого обращения в зоопарках, на зоофермах и в других местах содержания животных.

Следует рассмотреть также регулирование сети Интернет при расследовании жестокого обращения с животными. В нашей стране существуют законы, которые запрещают публикации, содержащие информацию о жестоком обращении с животными в любой форме её представления, в Интернете. В случае нарушения, лица, распространяющие запрещённый контент, могут быть привлечены к административной или уголовной ответственности. Запрещаются производство, изготовление, показ и распространение пропагандирующих жестокое обращение с животными кино-, видео- и фотоматериалов, печатной продукции, аудиовизуальной продукции, размещение таких материалов и продукции в информационно-телекоммуникационных сетях (в том числе в сети Интернет) и осуществление иных действий, пропагандирующих жестокое обращение с животными[5].

Актуальным в настоящее время является блокирование сайтов и веб-страниц, содержащих и распространяющих информацию, которая может причинить вред психическому здоровью неограниченного круга лиц, о жестоком обращении с животными. Отдельный законопроект, закладывающий соответствующую идею, «О внесении изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации» в части

[4] Хаймина Л. Э., Зеленина Л. И., Хаймин Е. С., Антуфьев Д. И. Технологии отслеживания северного оленя на территории Российской Федерации // Арктика и Север. 2021. № 45. С. 50.

[5] Об ответственном обращении с животными и о внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 27 декабря 2018 г. № 498-ФЗ // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201812270064 (дата обращения: 15.05.2023).

оперативного ограничения доступа к информации в сети «Интернет», содержащей материалы жестокого обращения с животными», к сожалению, был отклонён государственной думой.

Одной из важнейших задач при расследовании жестокого обращения с животными является проведение соответствующих судебных экспертиз. Обобщая материалы судебно-следственной практики, можно сделать вывод, что к самым типичным и специфическим видам экспертиз по ст. 245 УК РФ следует отнести: судебно-ветеринарную, судебно-зоологическую, судебно-баллистическую, судебно-трасологическую[6].

Судебно-ветеринарная экспертиза – это вид экспертизы, который имеет важное значение в ориентировочно-поисковой и доказательственной практике. Она позволяет определить причину смерти животного и выявить конкретные травмы или увечья, полученные выжившим животным. Знание этих факторов помогает следователю принять решение о возможном совершении преступления. Судебно-ветеринарная экспертиза также предоставляет ответы на вопросы, связанные с заболеванием животного, правильностью ухода за ним, его содержания и кормления, а также другие аспекты, которые могут влиять на его здоровье и благополучие.

Проведение судебно-ветеринарной экспертизы предполагает решение в основном диагностических задач: *что стало причиной смерти; сколько прошло времени с момента смерти; каковы вид, порода и возраст животного; болело ли животное и т. д*.

В ряду специфичных по делам о жестоком обращении с животными следует назвать судебно-зоологическую экспертизу, которая относится к судебно-биологическим по роду. При производстве отдельных видов следственных действий, в особенности осмотра места происшествия, обыска, освидетельствования, как правило, обнаруживаются биологические следы животных: кровь, шерсть, частицы кожи, биологические выделения и т. д. Если обнаруживаются соответствующие объекты, чаще всего в отношении них назначается проведение судебно-зоологической экспертизы.

Судебно-зоологическая экспертиза представляет собой комплексное исследование. Это предполагает применение метода анализа морфологических свойств и признаков объектов. Такая экспертиза позволяет решить широкий комплекс диагностических, ситуационных, идентификационных и классификационных задач, способствуя раскрытию и расследованию анализируемого преступления[7].

---

[6] Волынский А. Ф. Экспертно-криминалистическая деятельность в правоохранительных органах: цель – раскрытие и расследование преступлений // Вестник экономической безопасности. 2020. № 5. С. 17.

[7] Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе:

Таким образом, использование специальных знаний и проведение экспертиз при расследовании жестокого обращения с животными является необходимым условием для обеспечения защиты жизни и здоровья животных и привлечения виновных лиц к ответственности, а компьютерные технологии и электронно-цифровые доказательства играют важную роль в расследовании жестокого обращения с животными в России. Кроме того, важно продолжать работу по повышению осведомлённости населения о защите прав животных и ответственности за их нарушение.

Список литературы

1. Варданян А. В. Современные проблемы использования специальных знаний в уголовном судопроизводстве // Юрист-Правоведъ. 2019. № 2 (89). С. 158–163.

2. Волкова Г. П. Особенности осмотра животных и их трупов по делам о жестоком обращении с ними // Теоретико- методологические и прикладные аспекты социальных институтов права, экономики, управления и образования: материалы всероссийской научной конф. с международным участием. М.: Перо, 2016. С. 352–355.

3. Волынский А. Ф. Экспертно-криминалистическая деятельность в правоохранительных органах: цель – раскрытие и расследование преступлений // Вестник экономической безопасности. 2020. № 5. С. 15–21.

4. Криминалистическая методика для дознавателей: учебник для среднего профессионального образования / Под ред. А. Г. Филиппова. М.: Юрайт, 2022. 414 с.

5. Мосина С. В., Андроник Н. А. Актуальные проблемы расследования жестокого обращения с животными на первоначальном этапе: теоретико-прикладной анализ // Вестник Уфимского юридического института МВД России. 2022. № 3 (97). С. 115–121.

6. Основы патологической анатомии и судебно-ветеринарной экспертизы: учебное пособие для студентов факультета ветеринарной медицины по специальности «Ветеринария» и направления подготовки «Ветеринарно-санитарная экспертиза» / Б. П. Шевченко [и др.]. Оренбург: Издательский центр ОГАУ. 2017. 440 с.

7. Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. 4-е изд., перераб. и доп. М.: Норма: ИНФРА-М, 2020. 576 с.

8. Тебиев Р. Р. К вопросу о способах жестокого обращения с животными как элементе криминалистической характеристики преступлений данного вида // Актуальные проблемы борьбы с преступностью: вопросы теории и практики:

монография. 4-е изд., перераб. и доп. М.: Норма: ИНФРА-М, 2020. С. 112.

материалы XXIV международной научно-практ. конф.: в 2 ч. / отв. ред. Д. В. Ким. Красноярск: СибЮИ МВД России, 2021. Ч. 1. С. 307–309.

9. Тебиев Р. Р. Методика расследования жестокого обращения с животными: дис. … канд. юрид. наук. Москва, 2022. 218 с.

10. Хаймина Л. Э., Зеленина Л. И., Хаймин Е. С., Антуфьев Д. И. Технологии отслеживания северного оленя на территории Российской Федерации // Арктика и Север. 2021. № 45. С. 48–60.

Vladislav Yu. Ivanov
Lecturer at the Department of Forensic Science
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
blad02051995@mail.ru

Valeria S. Myshlyashina
Student of the faculty training of investigators
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
vvmaussleria@gmail.com

THE USE OF SPECIAL KNOWLEDGE IN THE INVESTIGATION OF ANIMAL CRUELTY

Abstract. The article analyzes the trace picture resulting from the commission of a crime under Art. 245 of the Criminal Code of the Russian Federation. The authors focus on the need to study the pages of the criminal's social networks in order to search for forensically significant information. The expediency of involving specialists in the investigative examination not only in the field of veterinary medicine, but also in information and telecommunication technologies is considered.

Keywords: cruelty to animals, inspection of the scene, examination of animals and their corpses, use of special knowledge, veterinarian.

УДК 343.98

Кадиев Руслан Сергеевич
Старший следователь-криминалист
Второй отдел криминалистического сопровождения
следствия управления криминалистики
Главного следственного управления Следственного комитета
Российской Федерации по г. Санкт-Петербургу
(г. Санкт-Петербург, Россия)
r.s.kadiev@yandex.ru

РАСКРЫТИЕ И РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЁННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ГЛАВНОМ СЛЕДСТВЕННОМ УПРАВЛЕНИИ СЛЕДСТВЕННОГО КОМИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО Г. САНКТ-ПЕТЕРБУРГУ

Аннотация. В данной статье проанализирован опыт в работе Главного следственного управления Следственного комитета Российской Федерации по г. Санкт-Петербургу по направлению раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Ключевые слова: уголовное право, преступление, уголовный кодекс, юриспруденция, право, предварительное следствие, раскрытие преступлений, расследование преступлений, информационные технологии.

Для цитирования:
Кадиев Р. С. Раскрытие и расследование преступлений, совершённых с использованием информационно-телекоммуникационных технологий в Главном следственном управлении Следственного комитета Российской Федерации по г. Санкт-Петербургу // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 85–91.

В нашей стране ежедневно и более того ежечасно совершаются десятки и сотни различных преступлений, на которые правоохранительным органам необходимо динамично реагировать и принимать процессуальные решения. На современном этапе в условиях стремительного развития общества Российской Федерации, в частности в отрасли информационных технологий, а также увеличения интернет-аудитории наблюдается существенный рост преступлений (различных категорий), способ совершения которых либо причины их совершения напрямую связаны с использованием информационно-телекоммуникационной сети «Интернет». Как отмечали Ю. М.

Батурин, С. В. Полубинская: «Высокотехнологический уклад жизни порождает и высокотехнологические преступления»[1]. Следы совершённого преступления либо информация, имеющая значение для раскрытия, расследования преступления и установления всех обстоятельств произошедшего, находятся «на просторах» сети «Интернет», в частности, на персональных страницах социальных сетей, мобильных мессенджеров, а также иных ресурсах.

В своих работах такой учёный, как И. А. Кучерков, отмечал, что: «В юридической и иной научной литературе для обозначения общественно-опасных деяний, осуществляемых с использованием информационно-телекоммуникационных технологий, используются различные термины и формулировки. Такими формулировками могут быть: «интернет-преступления», «преступления, совершаемые с использованием интернет-технологий», «компьютерные преступления», «киберпреступления», «преступления, совершаемые с помощью информационно-телекоммуникационных технологий», «преступления, совершаемые в виртуальной среде», «преступления, совершаемые в Интернете», «компьютерная преступность», «киберпреступность», «интернет-преступность» и другие»[2].

В результате анализа практики выявления и расследования преступлений, совершённых в сфере и с использованием информационно-телекоммуникационных технологий установлено, что в соответствии со статьёй 151 УПК РФ расследование преступлений в сфере компьютерной информации (гл. 28 УК РФ) относится к подследственности органов внутренних дел Российской Федерации. Иные преступления, связанные с посягательством на безопасность в сфере использования информационно-телекоммуникационных технологий (ст. 158, 159, 228.1 УК РФ и др.) также зачастую относятся к составам преступлений, расследование которых входит в компетенцию органов полиции. Однако ряд преступлений указанной категории относится к компетенции Следственного комитета Российской Федерации.

В Главном следственном управлении Следственного комитета РФ по г. Санкт–Петербургу (далее по тексту – Главное следственное управление) уделяется особое внимание вопросу раскрытия и расследования преступлений, совершённых с использованием информационно-телекоммуникационных технологий.

Можно выделить следующие категории преступлений, совершаемых с использованием информационно-коммуникационных технологий,

[1] Батурин Ю. М., Полубинская С. В. Совершенствование законодательных норм уголовно-правового цикла в контексте высокотехнологического будущего // Преступность в XXI веке. Приоритетные направления противодействия: монография / под ред. А. Н. Савенкова. Москва: ЮНИТИ-ДАНА: Закон и право, 2020. С. 78.

[2] Кучерков И. А. О понятии «киберпреступление» в законодательстве и научной доктрине // Юридическая наука. 2019. № 10. С. 78-81

уголовные дела о которых расследуются подразделениями Главного следственного управления[3]:

1. Террористического характера и экстремистской направленности, в том числе финансирование терроризма, вовлечение в занятие террористической и экстремистской деятельностью, возбуждение ненависти либо вражды, унижение достоинства человека по различным признакам, подстрекательство к противоправным действиям массового характера, в том числе связанным с незаконными протестными выступлениями.

2. Против половой неприкосновенности, в совершение которых в подавляющем большинстве случаев вовлекаются несовершеннолетние, как то: развратные действия, оборот порнографических материалов.

3. Различные виды мошенничеств и иных способов хищений, в том числе путём введения в заблуждение наиболее незащищённых граждан из числа пенсионеров, ветеранов, лиц с ограниченными возможностями и пр.

4. Незаконный оборот наркотических средств и психотропных веществ.

5. Преступления в сфере экономической деятельности (незаконная банковская деятельность, фальсификация ЕГРЮЛ, незаконная предпринимательская деятельность).

При этом, по мнению учёных-теоретиков основными векторами распространения ИТ-угроз выступают: использование шифровальщиков, деятельность по продаже доступа в скомпрометированные сети, мошенничество, фишинг и спам[4].

Анализ статистических данных, касающихся количества зарегистрированных сообщений о преступлениях, возбуждённых уголовных дел, а также прекращённых, приостановленных и направленных в суд за отчётные периоды 2018, 2019, 2020, 2021, 2022 гг. (в сравнении с АППГ), свидетельствует о планомерном увеличении количества преступлений, совершаемых с использованием информационно-коммуникационных технологий, что является естественным процессом по мере развития информационной отрасли, глобализации и популяризации информационных сетей, перевода значительных сфер жизни общества и граждан в онлайн среду, а следовательно, и возрастающего интереса к данному направлению со стороны лиц с сформировавшимся преступным поведением.

Так, за 12 месяцев 2022 года в Главном следственном управлении было зарегистрировано 327 сообщений о преступлениях анализируемой категории (+ 80 к АППГ), что в общей сумме составляет 10,8 % от общего количества сообщений о

[3] Здесь и далее сведения из аналитической работы Главного следственного управления Следственного комитета Российской Федерации по г. Санкт-Петербургу.

[4] Елин В. М. О подходах к криминологической характеристике лиц, совершающих преступления в сфере компьютерной информации // Российский следователь. 2022. № 7. С. 61–65.

преступлениях, зарегистрированных в Главном следственном управлении (+ 3,5 к АППГ). По результатам рассмотрения указанных сообщений о преступлениях возбуждено 307 уголовных дел (+ 72 к АППГ)[5].

В анализируемый период предварительно расследовано преступлений – 203 (+ 39 к АППГ), из них в суд направлено 196 уголовных дел (+ 40 к АППГ) (что составляет 6,9 % от общего количества раскрытых преступлений (+ 1,6 к АППГ), по 7 уголовным делам приняты решения о приостановлении предварительного следствия (+ 1 к АППГ).

Следует отметить, что помимо решений о возбуждении уголовных дел, следователями принимались решения об отказе в возбуждении уголовных дел, а также о направлении сообщений о преступлениях по территориальности. Последние решения являлись логичным и закономерным результатом для значительного количества зарегистрированных сообщений о преступлениях анализируемой категории, поскольку таким преступлениям характерна межрегиональность, либо возможность дистанционного их совершения из других субъектов Российской Федерации.

Анализируя приведённые сведения, нельзя не обратить внимание на резко увеличившееся количество преступлений в сфере информационно-коммуникационных технологий за последние два года. Помимо обозначенной выше причины в виде естественных процессов, связанных со стремительным развитием указанной сферы, определённое влияние на статистические данные оказывает отражение отдельных показателей и характеристик совершённых преступлений в документах первичного статистического учёта при возбуждении уголовных дел, а также по результатам их расследования.

Так, усиление контроля со стороны руководства Главного следственного управления, а также надзора органов прокуратуры города за качеством и полнотой сведений при заполнении указанных статистических документов, повлияло на более полное отображение реальной картины преступности с использованием ИКТ.

Возникающие в настоящее время информационные угрозы, обусловленные распространением в сети «Интернет» противоправной информации, представляются очень опасными, так как захватывают не только процессы, связанные с функционированием компьютерных систем и обменом информации, но также оказывают негативное влияние на сознание граждан и в особенности социально незащищённых слоёв населения – детей, лиц пожилого возраста.

Как было отмечено выше, росту преступлений в сфере информационно-коммуникационных технологий способствует, как активное развитие современных информационно-телекоммуникационных технологий,

[5] Здесь и далее используются сведения организационно-контрольного отдела Главного следственного управления Следственного комитета Российской Федерации по г. Санкт-Петербургу

так и отсутствие необходимых теоретических и практических знаний в данной области у сотрудников правоохранительных органов, а также недостаточная техническая оснащённость оперативно-розыскных и следственных органов.

Несмотря на это, правоохранительными органами Санкт-Петербурга, и в том числе Главным следственным управлением, принимаются активные меры к исправлению сложившейся ситуации.

Так, в составе следственной части Главного следственного управления ГУ МВД России по г. Санкт-Петербургу и Ленинградской области сформировано и функционирует отдел по расследованию преступлений в сфере информационно-телекоммуникационных технологий, а также специализированных оперативных групп по раскрытию указанных преступлений.

В соответствии с приказом Председателя Следственного комитета Российской Федерации от 15.04.2021 г. в первом управлении по расследованию особо важных дел Главного следственного управления города созданы штатные единицы следователей по борьбе с киберпреступлениями и преступлениями в сфере высоких технологий.

В целях изучения практики расследования преступлений указанной категории, повышения профессиональной квалификации следователей, а также обмена опытом, сотрудники Главного следственного управления в 2021–2022 годах принимали участие в различных совещаниях и конференциях, посвящённых особенностям расследования преступлений, совершённых в сфере информационно-телекоммуникационных технологий.

В связи с ростом количества преступлений, совершённых с использованием информационно-телекоммуникационных технологий и в сфере компьютерной информации, руководителям следственных подразделений Главного следственного управления указано на необходимость своевременного выявления таких преступлений и реагирования на заявления граждан, содержащие информацию о совершении преступлений, а также указано на необходимость незамедлительно решать вопрос о возбуждении уголовных дел по указанным фактам либо изъятии возбуждённых уголовных дел из производства органов внутренних дел при совершении преступлений альтернативной подследственности, в отношении социально-незащищённых слоёв населения, а также преступлений, вызвавших широкий общественный резонанс.

Кроме того, дежурная служба управления криминалистики Главного следственного управления ориентирована на изучение поступающих ежесуточно сводок происшествий, зарегистрированных на территории г. Санкт-Петербурга, в целях выявления регистрируемых сообщений о совершении преступлений с использованием информационно-телекоммуникационных технологий

для оперативного решения вопроса о возбуждении уголовных дел по указанным сообщениям либо инициирования передачи возбуждённых органами внутренних дел уголовных дел в производство следственных подразделений Главного следственного управления.

В качестве положительного примера указанной работы можно привести раскрытие преступления против половой неприкосновенности малолетней Блоцкой В. В., 2009 г. р., явившееся предметом расследования уголовного дела № 12202400003000041, возбуждённого следственным отделом по Василеостровскому району Главного следственного управления по ч. 2 ст. 135 УК РФ.

На телефон «горячей» линии «Ребёнок в опасности» дежурной службы Главного следственного управления обратилась Блоцкая В. В., которая сообщила, что в порядке родительского контроля, изучая контент мобильного телефона своей дочери Блоцкой В. В., в мобильных приложениях «WatsApp» и Telegram обнаружила переписку интимного характера с контактом «Друг», в ходе которой несовершеннолетняя направляла собеседнику снимки интимного характера.

Данное сообщение по каналам быстрой связи было направлено в территориальный следственный отдел, в котором оно было зарегистрировано в порядке, предусмотренном статьями 144–145 УПК РФ.

По результатам проведённых следственных и оперативно-розыскных мероприятий удалось в кратчайшие сроки установить и задержать лицо, ведущее переписку с Блоцкой В. В., которым оказался гражданин Таджикистана.

Другим примером являеется одно из дел 2022 года, когда первым управлением по расследованию особо важных дел закончено расследование в отношении участников организованной преступной группы, члены которой на протяжении 2021 года, действуя от имени коллекторской организации, используя мобильную связь, вымогали денежные средства у родственников лиц, допустивших просрочку по выплате микро-займов, при этом угрожая потерпевшим применением физического и сексуального насилия, опасного для жизни и здоровья, а также сопровождая свои угрозы повреждением имущества последних. Данные действия преступников отличались особым цинизмом, так как преимущественно были направлены в отношении несовершеннолетних и женщин, которые не могли защитить себя. При активном взаимодействии органов предварительного следствия с оперативно-розыскными подразделениями органов внутренних дел было выявлено и доказано всего 15 эпизодов указанной преступной деятельности.

Таким образом, рассмотрев в примерах процесс организации и расследования уголовных дел Главным следственным управлением, можно прийти к выводу, что данное направление служебной деятельности органов Следственного комитета Российской Федерации по борьбе с «киберпреступностью» является одним из наиболее актуальных и динамично развивающихся. Органам

предварительного следствия необходимо постоянно и систематически заниматься вопросом повышения уровня своей профессиональной квалификации и подготовки.

Список литературы:

1. Батурин Ю. М., Полубинская С. В. Совершенствование законодательных норм уголовно-правового цикла в контексте высокотехнологического будущего // Преступность в XXI веке. Приоритетные направления противодействия: монография / под ред. А. Н. Савенкова. Москва: ЮНИТИ-ДАНА: Закон и право, 2020. С. 78.
2. Елин В. М. О подходах к криминологической характеристике лиц, совершающих преступления в сфере компьютерной информации // Российский следователь. 2022. № 7. С. 61–65.
3. Кучерков И. А. О понятии «киберпреступление» в законодательстве и научной доктрине // Юридическая наука. 2019. № 10. С. 78–81.

Ruslan S. Kadiev
Senior investigator-criminalist
Second department of the forensic support of the investigation
of the forensic department of the Main Investigation Department
of the Investigative Committee of the
Russian Federation for the city of St. Petersburg
(St. Petersburg, Russia)
r.s.kadiev@yandex.ru

Abstract. This article analyzes the experience in the work of the Main Investigation Department of the Investigative Committee of the Russian Federation for the city of St. Petersburg in the direction of disclosure and investigation of crimes committed using information and telecommunication technologies.

Keywords: criminal law, crime, criminal code, jurisprudence, law, preliminary investigation, crime detection, crime investigation, information technology.

УДК 378.14; 343.98

Каторгина Наталья Петровна
кандидат юридических наук,
доцент кафедры судебной экспертизы и криминалистики,
Белгородский государственный национальный исследовательский университет
(г. Белгород, Российская Федерация)
inyakova@bsu.edu.ru

ИСПОЛЬЗОВАНИЕ IT-ТЕХНОЛОГИЙ ПРИ ПОДГОТОВКЕ К ЗАНЯТИЮ ПРЕПОДАВАТЕЛЕМ ВЫСШЕЙ ШКОЛЫ

Аннотация. В статье рассмотрены теоретические аспекты подготовки преподавателя высшей школы к проведению занятий. Обращено внимание на организационную процедуру подготовки, а также развитие умений и навыков будущего специалиста. Особый интерес представляет подготовка преподавателя к проведению занятий в онлайн-формате. Приведён опыт Белгородского государственного национального исследовательского университета (далее – НИУ «БелГУ»). Предложены современные инструменты, используемые преподавателем с целью подготовки к занятию и успешному освоению дисциплины обучающимся. На основе проведенного анализа автором предложено собственное видение рассматриваемого вопроса.

Ключевые слова: высшее образование, подготовка к занятию, преподаватель высшей школы, студент, обучающийся, онлайн-формат.

Для цитирования:
Каторгина Н. П. Использование IT-технологий при подготовке к занятию преподавателем высшей школы // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 92–97.

Реформы, произошедшие в начале XXI века в сфере образования, способствуют повышению уровня подготовки преподавателя высшей школы к занятиям. Процесс подготовки должен включать не только решение организационных вопросов, но и анализ дискуссионных аспектов темы занятия, а также развитие умений и навыков будущего специалиста. Полная процедура подготовки является сложным и трудоёмким процессом, требующим от педагога концентрации внимания, достаточного объёма знаний и умений, наличия соответствующих личностных и профессиональных качеств, которые позволят провести подготовку к занятию.

Подготовка преподавателя к занятию начинается с анализа образовательного стандарта, основной профессиональной образовательной программы высшего образования по направлению / специальности, а также изучения учебного плана, карты компетенций и рабочей программы, размещенных в автоматизированной

системе «ИнфоБелГУ: Учебный процесс» на сайте НИУ «БелГУ»[1].

Образовательный стандарт высшего образования по специальности / направлению даст общее представление об области применения; о характеристике направления подготовки (специальности) и профессиональной деятельности специалиста; о требованиях, предъявляемых к результатам освоения, оценке качества освоения основных образовательных программ подготовки специалиста и т. д.

Изучая основную профессиональную образовательную программу высшего образования по направлению / специальности, представляется возможным установить назначение данной программы; нормативные документы, регламентирующие изучаемую сферу деятельности; перечень основных задач профессиональной деятельности выпускников; планируемые результаты освоения программы и многое другое.

На основе анализа учебного плана предполагается определить форму организации учебного процесса; вид занятий; общее количество часов, отводимых на лекционные, практические и лабораторные занятия, курсовую работу, самостоятельную работу студентов; форму завершения учебного курса; планируемые результаты освоения дисциплины.

Изучение карты компетенций позволит определить объём знаний, умений и навыков, которыми должен обладать будущий специалист. Исходя из сформулированных компетенций, преподаватель должен определить виды деятельности, которые выработают у студентов установленные компетенции.

Следующим процессом подготовки преподавателя к занятию является оценка рабочей программы дисциплины. Прежде всего, необходимо ознакомиться со структурой программы; определить место дисциплины в системе подготовки будущих специалистов; уяснить требования, предъявляемые к предварительной подготовке обучающегося; установить количество часов, отводимых на различные виды занятий; проанализировать содержание дисциплины и её разделы; выяснить перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине, основной и дополнительной учебной литературы, а также информационных технологий; определить типовые контрольные задания, используемые для оценки знаний, умений, навыков при формировании компетенций и другой информации, необходимой для подготовки преподавателя к занятию.

Обзор литературы, отмеченной в рабочей программе, подразумевает определение возможностей для развития нравственного, правового воспитания обучающихся, их гражданских и профессиональных качеств. Например, в рабочей программе дисциплины

[1] ИнфоБелГУ: Учебный процесс [Электронный ресурс]. URL: https://dekanat.bsu.edu.ru/blocks/bsu_nabor/nabor.php?facid=10100 (дата обращения: 10.04.2023).

«Криминалистика»[2] отмечена тема, посвящённая методике расследования преступлений, связанных с незаконным оборотом наркотических средств. Изучение данной темы позволяет получить общее представление о видах наркотических средств, видах ответственности за совершение противоправных деяний, типичной личности наркопреступника и наркопотребителя, способах совершения и сокрытия преступления, распространённых мотивах преступления, тактике следственных действий, последствиях преступных действий. Таким образом, действия преподавателя будут направлены, в том числе, и на профилактику наркомании и наркопреступности в образовательной среде. Преподаватель должен уметь проявить у студентов интерес к овладению соответствующих профессиональных знаний и навыков, а также оказать воспитательное и развивающее воздействие[3].

Знания преподавателя высшей школы не должны ограничиваться рамками узконаправленной дисциплины, необходимо знакомиться со смежными дисциплинами (уголовным правом, уголовно-процессуальным правом, криминологией, юридической психологией и др.), систематически пополнять объём имеющихся знаний, обмениваться опытом работы с другими преподавателями и практиками, проходить регулярные повышения квалификации.

Преподаватель высшей школы в ходе подготовки к занятию изучает и анализирует периодические источники, отечественный и зарубежный опыт для формирования у студентов научного мировоззрения. При этом необходимо учитывать развитие научно-технического прогресса, активно применять современные IT-технологии на очной и заочной формах обучения.

Российская Федерация ведёт планомерную работу по разработке и внедрению в образовательный процесс онлайн-курсов по учебным дисциплинам. В частности, с середины 1990-х годов наряду с традиционным образованием стали активно применять элементы IT-технологий в процессе освоения знаний и получения навыков на заочной форме обучения, а в настоящее время в связи с пандемией COVID-19 и специальной военной операцией применяют и на очной форме обучения. Например, в НИУ «БелГУ» с 2004 года используют систему электронного обучения «Пегас». Данная система базируется на основе модульной динамической учебной среды «Moodle», которая направлена на взаимодействие между обучающимися и преподавателем, а также предназначена для организации обучения с использованием Интернет-

[2] Логвинец Е. А., Каторгина Н. П. Рабочая программа дисциплины «Криминалистика» // [Электронный ресурс]. URL: https://pegas.bsu.edu.ru/course/view.php?id=3749 (дата обращения: 10.04.2023).

[3] Каторгина Н. П. Процесс подготовки преподавателя к занятию в бережливом вузе // Бережливое образование: сборник трудов Международной научно-практической конференции, 2021–2022 гг. / отв. ред. И. В. Чистникова. Белгород: ИД «Белгород» НИУ «БелГУ», 2022. С. 22.

технологий. В режиме удалённого обучения доступны рабочие программы, теоретические базы данных в виде лекций, дополнительные учебные материалы, практические, лабораторные и тестовые задания, терминологический словарь и т. д.[4]

Нарушение традиционной образовательной деятельности в виду наступления форс-мажорных обстоятельств побуждает преподавателя более тщательного готовиться к занятию с целью повышения эффективности образования в онлайн-формате. Так, преподавателю следует продумать виды интерактивной и групповой деятельности, что позволит компенсировать недостаток живого общения между всеми участниками образовательного процесса; ввести в дистанционный учебный процесс элементы игры, направленные на вовлечение обучающихся и поддержание их мотивации; подготовить и продемонстрировать учебные видеоролики и презентации, что позволит обучающимся выработать навыки и умения конструктивного мышления и анализа.

Способами наращивания мотивации обучающихся являются технологии виртуальной реальности. Их положительное значение отражается в самооценке навыков обучающихся, самоорганизации в период дистанционного обучения. Использование преподавателем в учебном процессе форумов для обсуждения актуальных вопросов, тренажеров виртуальной реальности, web-приложений для занятий в реальном времени, интерактивного обучения с помощью обучающей платформы, снизит уровень рутинности в обучении. Внедрение преподавателем в учебный процесс современных методов обучения позволит сформировать у обучающихся практические навыки, что только улучшит эффективность качества образования, получаемого в дистанционном формате.

Например, в рамках подготовки к практическому и лабораторному занятию по теме «Тактика осмотра места происшествия» по дисциплине «Криминалистика» преподавателю необходимо составить план занятия. В частности, вначале практического занятия рекомендовать обучающимся просмотреть учебный видеоролик осмотра места происшествия. После теоретического разбора предложить обучающимся решить кейс-задачу, используя методы интерактивной деятельности. Использование данного метода позволит научиться критически мыслить, определять проблемы на основе анализа имеющейся информации и принимать соответствующие решения, участвовать в дискуссиях, взаимодействовать друг с другом. По окончании, рассмотреть возможности

[4] Логвинец Е. А., Каторгина Н. П. Учебно-методический комплекс дисциплины «Криминалистика» // [Электронный ресурс]. URL: https://pegas.bsu.edu.ru/course/view.php?id=3749 (дата обращения: 10.04.2023); Логвинец Е. А., Каторгина Н. П. Учебно-методический комплекс дисциплины «Использование специальных знаний в судопроизводстве» [Электронный ресурс]. URL: https://pegas.bsu.edu.ru/course/view.php?id=17648 (дата обращения: 10.04.2023).

современных технических средств обнаружения, фиксации и изъятия криминалистически значимых объектов и следов, а также наиболее типовые ошибки, которые совершают следователи в ходе производства данного следственного действия[5].

Завершающим этапом подготовки преподавателя к занятию будут выступать построение логической структуры, формулирование чётких целей и задач, составление списка использованной литературы, выделение дискуссионных проблем, установление средств оценивания контрольных заданий, а также указание на применяемые актуальные технические средства и наглядные пособия, обеспечивающие современный уровень высшего образования.

Таким образом, подготовка преподавателя высшей школы к занятию в широком смысле включает не разовую организацию материалов к определённому занятию, а системную работу педагога (регулярные занятия по преподаваемой дисциплине, изучение теоретических и практических проблем, ознакомление с актуальными достижениями науки и техники, задействование творческого подхода). Кроме того, необходимо учитывать общую подготовленность студентов, наличие учебной и периодической литературы, аудитории, оснащённой необходимыми техническими средствами.

Список литературы

1. Каторгина Н. П. Процесс подготовки преподавателя к занятию в бережливом вузе // Бережливое образование: сборник трудов Международной научно-практической конференции, 2021–2022 гг. / отв.ред. И. В. Чистникова. Белгород: ИД «Белгород» НИУ «БелГУ», 2022. С. 21–23.

2. Логвинец Е. А., Каторгина Н. П. Цифровая трансформация образования: вызовы высшей школы в период пандемии COVID-19 // Общество: социология, психология, педагогика. 2022. № 8. С. 202–206.

Natalya P. Katorgina
PhD in Law,
lecturer of the Forensic Inquiry and Criminalistics Department,
Belgorod state national research university
(Belgorod, Russia)
inyakova@bsu.edu.ru

THE USE OF IT TECHNOLOGIES IN PREPARATION FOR THE LESSON BY A HIGH SCHOOL TEACHER

[5] Логвинец Е. А., Каторгина Н. П. Цифровая трансформация образования: вызовы высшей школы в период пандемии COVID-19 // Общество: социология, психология, педагогика. 2022. № 8. С. 205.

Abstract. The article discusses the theoretical aspects of the preparation of a high school teacher for conducting classes. Attention is paid to the organizational procedure of training, as well as the development of skills and abilities of the future specialist. Of particular interest is the teacher's preparation for conducting classes in an online format. The experience of the Belgorod State National Research University (next – NRU «BelSU»). The modern tools used by the teacher for the purpose of preparing for the lesson and the successful mastering of the discipline by students are proposed. Based on the analysis, the author offers his own vision of the issue under consideration.

Keywords: higher education, preparation for the lesson, high school teacher, student, student, online format.

УДК 340.130.4

Кодан Сергей Владимирович
Доктор юридических наук, профессор,
Заслуженный юрист Российской Федерации,
главный научный сотрудник Управления научных исследований,
профессор кафедры теории государства и права
Уральский государственный юридический университет имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
svk2005@yandex.ru

ИСТОЧНИКИ ПОЗНАНИЯ СОЦИАЛЬНЫХ ЯВЛЕНИЙ И ИНСТИТУТОВ КАК ИНФОРМАЦИОННЫЕ ЕДИНИЦЫ В ИСТОЧНИКОВЕДЕНИИ СОЦИОГУМАНИТАРИСТИКИ

Аннотация. В статье основное внимание акцентируется на проблеме характеристик источников познания государственно-правовых явлений и институтов в качестве информационных единиц. Опираясь на информационный подход, автор обращается к находящимся на пересечении информатики и социогуманитаристики вопросам: пониманию информационной единицы, информационного пространства и поля, дескриптора, информационной ячейки социальной памяти и др. В данном контексте рассматриваются основные вопросы понимания и возможностей использования информационных явлений в исследованиях в социально-гуманитарных науках.

Ключевые слова: информационные ресурсы научного исследования, социальная информация, социальная память, социальное наследие, источники познания социальных явлений и институтов, носители социальной информации, юридическое источниковедение.

Для цитирования:
Кодан С. В. Источники познания социальных явлений и институтов как информационные единицы в источниковедении социогуманитаристики // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2023. С. 98–108.

Информационные ресурсы в современной научно-познавательной деятельности учёного стали качественно новым исследовательским инструментом в работе с носителями социальной информации. Соответственно, для исследователей возникает и проблема чётких ориентиров в информационном пространстве, нахождения опоры на своеобразные «информационные образы», которые позволяют их связать с концептами предметной области исследования. В данном плане одним из актуальных направлений разработки проблем источниковедения в социогуманитаристике, как и в юридическом источниковедении,

выступает вопрос о позиционировании источников познания социальных явлений и институтов в исследовательских практиках как носителей информации в качестве информационных единиц.

Понимание информационной единицы и информационного поля в информатике формируется на основе изысканий в данной области науки. «Информационные единицы – это единицы, которые переносят порции информации безотносительно к содержанию или характеризуют содержание порции информации безотносительно к информационному объёму. <…> Информационные единицы служат основой построения сложных: языковых описаний, информационных конструкций или информационных объектов» – указывает В. Я. Цветков. Также им выделяются «информационные единицы сообщений», в которых «фраза (фразеологическая единица) – информационная единица, обладающая неделимостью по связанности предложений и выражающая законченную мысль», обладает максимальной смысловой содержательностью. Это «смысловое содержание» в совокупности с его контекстом и ассоциативными связями «с другими фразеологическими единицами или мыслимыми объектами… дополнительно наполняет данную информационную единицу ассоциативным смысловым содержанием», а «информационные единицы являются инструментом отображения внешнего мира и инструментом создания научной картины мира»[1].

Соответственно информационные единицы формируют *информационное поле*, выступающее как система, посредством которой осуществляется передача, обработка и хранение информации с использованием технических средств, информационных ресурсов и информационных каналов коммуникации. Одновременно важно учитывать и то, что в совокупности информационных единиц, составлявших информационно поле, для поиска информации используется *дескриптор* – конкретное слово, совокупность слов или словосочетание, которое отобрано из текста определённой области знаний и употребляется для описания основного смыслового содержания информационной единицы для поиска необходимой тематической информации при формулировке запроса в информационной среде. Уже на основе дескрипторов создаётся *информационно-поисковый тезаурус* как словарь терминов, который позволяет контролировать и обеспечивать эффективность информационного поиска. Задачи поиска сводится к необходимости ответа на три основных вопроса: какие источники информации искать (что искать?), к каким места размещения источников обращаться (где искать?) и

[1] Цветков В. Я. Информационные единицы сообщений // Фундаментальные исследования. 2007. № 12-1. С. 123-124; Цветков В. Я. Информационные единицы как средство построения картины мира // Международный журнал прикладных и фундаментальных исследований. 2014. № 8-4. С. 36-40.

на какой инструментарий опираться (как искать?). Именно тезаурус или дескрипторный словарь (упрощённый вариант тезауруса) обозначают упорядоченный список лексических единиц исследуемой предметной области с явным указанием на связи между ними и представляют предметную область в поисковой системе. При этом в работе по составлению тезауруса или дескрипторного словаря важным представляется привлечение специалистов в области отдельных наук, которые могут представить и обосновать включение терминов для использования в поисковых системах[2].

Цифровой поворот в науке на основе междисциплинарного взаимодействия информатики и социогуманитаристики в последние десятилетия качественно изменил исследовательское пространство, и на их пересечении появились и зарождаются новые междисциплинарные подходы, методы, методики и технологии, позволяющие на новом качественном уровне проводить научные исследования и получать качественно новые результаты. Также в социально-гуманитарных науках выделилось в отдельное направление – цифровые гуманитарные науки (Digital Humanities), в рамках которых оцифровываются книги и рукописи, создаются электронные архивы, библиотеки и музеи, базы заданных и т. п. В данном плане интерес представляют и постоянно возрастающие возможности расширяющегося набора инструментов, необходимых для получения и обработки информации, полученной из различного рода источников[3]. На стыке ряда естественных и социально-гуманитарных наук возникла и активно развивается в качестве нового междисциплинарного научного направления *социальная информатика,* ориентированная на изучение видов и форм проявления информации в обществе, информационных процессов, технологий, систем коммуникации, которые имеют значимость для жизнедеятельности человека и общества. В рамки данного направления также должны решаться и проблемы работы с различными носителями социальной информации, включая и источники познания государства и права.

Использование информационных единиц и информационного поля в социально-гуманитарных науках требует понимания их соотношения с другими явлениями познавательного характера и исследовательскими пространствами в плане работы с

[2] Ожерельева Т. А. Об отношении понятий информационное пространство, информационное поле, информационная среда и семантическое окружение // Международный журнал прикладных и фундаментальных исследований. 2014. № 10-2. С. 21–24; Рогова Н. А. Тезаурус как средство повышения эффективности современных информационно-поисковых систем // Труды Академии управления МВД России. 2011. № 1. С. 113–119.

[3] Digital Humanities: гуманитарные науки в цифровую эпоху / под ред. Г. В. Можаевой. Томск: Изд-во Томского гос. ун-та, 2016. 120 с.

социальной информацией. Эта проблематика может быть рассмотрена в ряде проекций и поэтому выделим основные из них.

Информационные единицы и информационный подход в социогуманитаристике

взаимосвязаны в плане того, что информационный подход выступает как «общая ориентация учёного на анализ информационного «среза» действительности и раскрытие в исследовательских практиках «специфически неповторимой информационной роли каждого конкретного феномена во всем его богатстве свойств и отношений» – отмечает Э. П. Семенюк[4]. Указанное нацеливает исследователя на изучение достаточно широкого спектра содержательных характеристик исследуемых социальных явлений и институтов, опираясь на семантическое ядро подхода – его обозначение как «информационного». Информационный подход направлен на изучение информационного поля и информационных единиц с позиционированием в нём носителей социальной информации во взаимосвязи с источниками познания социальных явлений, процессов, институтов и т. п. Информационные единицы, составляющие информационное поле и обозначенные их дескрипторами, позволяют исследователю посредством информационно-поискового тезауруса обрабатывать самые разнообразные массивы социальной информации (данных) в соответствии с предметной направленностью исследований в различных науках социально-гуманитарного профиля. При этом заметим, что в науке обоснованно ставится вопрос о дополнении концепции «трёх миров» Карла Поппера, который обращает внимание на то, что вместе с физическим миром, наблюдаемой природой («первый мир») и сферой человеческого познания, протекающих в мозгу людей психических процессов («второй мир») возникает «третий мир» именно «как продукт деятельности человека» – «человеческое творение»[5]. По мнению К. К. Колина, также существует и «информационный мир», который «служит своеобразным каналом информационного взаимодействия между физическим миром и миром сознания. Этот мир появляется в результате взаимодействия материальных объектов и представляет собой совокупность их взаимных отражений в процессе этого взаимодействия. Это так называемая первичная и вторичная информация, которую порождает мир физической реальности в результате действия всеобщего закона отражения». Автор также обращает внимание на то, что указанный мир «не только обеспечивает взаимодействие между физическим миром и миром сознания. Он также служит и ареной взаимодействия объектов физической реальности между собой. Если бы этого мира не существовало, то никакие взаимодействия

[4] Семенюк Э. П. Информационный подход к познанию действительности. Киев: Наукова думка, 1988. С. 8.

[5] Поппер К. Р. Объективное знание. Эволюционный подход. Пер. с англ. М: Эдиториал УРСС, 2002. С. 153–161.

материальных объектов между собой в природе вообще не были бы возможными. <…> Поскольку информация является всеобщим свойством реальности, то <…> она существует не только в сознании человека, но также и в физическом мире»[6]. Именно этот «информационный мир» – «четвёртый мир» – требует от исследователя понимания процессов передачи информации посредством информационных единиц и информационного поля во взаимосвязи с структурой изучаемого объекта и отражения последнего в получаемой исследователем информации.

Информационные единицы и когнитивное пространство исследователя изучаются в контексте информационного подхода и связаны в плане того, что учёный, как и всякий человек разумный, обладает способностью к умственному восприятию и переработке внешней информации – когнитивностью – и, познавая мир, приобретает и систематизирует полученные знания о нём, тем самым выступая как «когнитивный субъект»[7]. В данном контексте «информация есть субъективный образ или модель реальности» и «именно потому, что в основе информации об объективном мире лежит сам этот объективный мир, представление о нем у различных субъектов более или менее адекватное, то есть совпадающее с объективной реальностью» – отмечает Ю. Н. Столяров[8]. В результате научной деятельности появляются интеллектуальные продукты как информационные ресурсы, которые входят в число источников познания социальных явлений. В рамках информационной теории И. Д. Ковальченко (1970–е гг.) акцентировал внимание на соотношении информации и источников её получения и подчёркивал, что под информацией понимают совокупность сведений, содержащихся в источниках, а их возникновение в своём большинстве представляет «информационный процесс, в котором фигурируют объект – отражаемая реальность, субъект – творец источника и информация – результат отражения объекта субъектом. Этот процесс, как и всякий информационный, всегда имеет прагматический аспект, т. е. творец источника всегда преследует определённую цель, выявляя сведения об объективной действительности»[9]. Эта связанность информации с субъектом получила на принципиально новом уровне развитие в рамках *когнитивно-информационной теории* О. М. Медушевской, которая в центр внимания ставит проблему человека и человеческой деятельности,

[6] Колин К. К. Философия информации и структура реальности: концепция «четырех миров» // Знание. Понимание. Умение. 2013. № 2. С. 136–147.

[7] Егорова М. А. «Когнитивное пространство» и его соотношение с понятиями «Ментальное пространство», «Когнитивная база», «Концетосфера», «Картина мира» // Вестник Иркутского государственного лингвистического университета. 2012. № 3. С. 61–68.

[8] Столяров Ю. Н. Сущность информации. М.: ГПНТБ России, 2000. С. 52

[9] Ковальченко И. Д. Методы исторического исследования. М.: Наука, 2003. С. 127–128.

опосредованной и вводимой в информационное поле через интеллектуальные продукты. Тем самым в информационно-коммуникативном пространстве обеспечивается «связь между человеком и социумом через созданный одним и прочитанный «другими» интеллектуальный продукт <…> каждый созданный интеллектуальный продукт уже в момент своего создания пополняет совокупный ресурс человечества и может быть актуализирован теперь и всегда»[10]. Именно эти интеллектуальные продукты выступают информационными единицами в информационном поле и представлены источниками познания социальных явлений и институтов.

Информационные единицы и социальная память в плане их взаимодействия позволяют акцентировать внимание на механизмах и ресурсах передачи накопленного опыта как коммуникативно-информационных процессах. Социальная память в контексте информационного подхода выступает как «специфическая надындивидуальная система информации, обеспечивающая накопление, хранение, передачу существенно важной, программирующей поведение индивидов информации от поколения к поколению (вертикальный обмен информацией), а также обмен информацией между людьми одного поколения (горизонтальный обмен информацией)» – отмечает В. Г. Афанасьев[11]. Социальная память позволяет обратиться и актуализировать в настоящем массив информации о прошлом социальной системы, использовать её уже для решения насущных проблем[12]. Соответственно «хранилищем» социальной памяти» является *социальное наследие*, которое выступает как информационный массив результатов практического опыта и познавательной деятельности. Разновидностью социальной памяти является *научная память*, которая соединена с наукой и отражается в *научном наследии*. Относительно взаимодействия социальной памяти / социального наследия и научной памяти / научного наследия важно учитывать, что «науку можно рассматривать как механизм централизованной социальной памяти, которая аккумулирует практический и теоретический опыт человечества и делает его всеобщим достоянием» – отмечает М. А. Розов[13]. Одновременно следует обратить внимание на то, что

[10] Медушевская О. М. Теория и методология когнитивной истории // Медушевская О. М. Собрание сочинений: в 4 т. Т. 1. Философия истории и теория исторического познания. М.; Берлин: Директ-Медиа, 2017. С. 98–99.

[11] Афанасьев В. Г Социальная информация и управление обществом. М.: Политиздат, 1975. С. 45–46.

[12] Аникин Д. А. Социальная память в свете информационного подхода // Вестник Поволжской академии государственной службы им. П. А. Столыпина. 2007. № 12. С. 163–168; Миклина Л. И. Структура и содержание социальной памяти общества // Научное мнение. 2014. № 9-3. С. 71–74.

[13] Розов М. А. Наука как традиция // Стёпин В. С., Горохов В. Г., Розов М. А. Философия науки и техники. М.: Контакт-Альфа, 1995. С. 90.

современные информационные технологии создают уникальные возможности «актуализации» научного наследия для исследователя, связанные с возможностью оперативного и комплексного доступа к ранее территориально локализованным местам хранения носителей информации на уровне отдельных архивов, библиотек, музеев, галерей и др. Тем самым в распоряжении учёного имеется канал связи, который позволяет удовлетворить его запросы на необходимость информационного обеспечения работы с носителями информации и получение достоверных эмпирических данных. В указанных контекстах информационные единицы в преломлении социальной и научной памяти и отражения её в социальном и научном наследии позволяют исследователю проследить способы накопления, хранения и передачи информации и выделить соответствующий фрагмент информационного поля для получения соответствующей объекту / предмету работы необходимой информации для его изучения.

Информационные единицы и научное знание находятся во взаимодействии в плане понимания того, что информация выступает фундаментом знания, поскольку знание передаётся в форме научной информации в соответствующем предметно-закодированном виде посредством информационных единиц, что в совокупности образует фрагмент информационного поля – информацию о научном знании. При этом знание не сводится только к информации и представляет собой результат её анализа и синтеза, произведённых субъектом познания как получателем информации[14]. Знаниевая составляющая в указанных планах указывает не только на доминирующее положение знания относительно информации, но и на их взаимосвязь, поскольку субъект познания воспринимает информацию в виде информационных единиц на основе имеющихся в его распоряжении полученного и усвоенного знания[15]. Соответственно, наличие знаний об объекте / предмете исследования является предпосылкой как для выделения информационных единиц и создания тезаурусов для баз данных и поисковых систем, так и работы в информационном поле по поиску источников социальной информации и получения на их основе необходимого для работы фактического материала.

Информационные единицы и классификация источников познания взаимосвязаны в плане того, что классификация как средство упорядочения и поиска носителей информации опирается на создание классификационных схем для представления больших объёмов информации в сжатом и обозримом виде для поиска необходимых для исследования источников. Существующая в теоретическом

[14] Столяров Ю. Н. Сущность информации. М.: ГПНТБ России, 2000. С. 64–66.

[15] См.: Седякин В. П. Информация и знания // Научные ведомости Белгородского государственного университета. Сер. Философия. Социология. Право. 2009. № 8. С. 180-187.

источниковедении типо-видовая модель классификации опирается на информационный подход и выделяет соответствующие информационные единицы: тип, вид, разновидность источников. *Тип источника* отражает деление на основе синтаксической стороны социальной информации и характеризуется схожестью форм кодирования, хранения и передачи информации. Соответственно выделяются и типы источников – вещественные, фонетические, изобразительные. *Вид источника* выступает в качестве основной классификационной единицы и характеризует социальные функции, формы и содержательные особенности передачи информации. *Разновидность источника* рассматривается как внутривидовая классифицирующая единица, которая позволяет в рамках вида источников выделить носители информации с более узкими целевыми установками и функциями. При этом необходимо учитывать, что указанные характеристики источников позволяют выделить носители информации, которые становятся средством познания в рамках предметов отдельных социально-гуманитарных наук[16].

В итоге можно сделать вывод, что понимание процессов получения социальной информации исследователем требует не только предварительных знаний об объекте / предмете исследования, но и ориентации в информационном пространстве получения сведения о нём, иметь достаточные знания в информатике и развивать информационное мышление для эффективного использования информационных ресурсов при работе с источниками познания социальных явлений. Рассмотренные вопросы в полной мере относятся и к сфере юридического источниковедения как пространства работы с носителями юридической информации.

Список литературы

1. Аникин Д. А. Социальная память в свете информационного подхода // Вестник Поволжской академии государственной службы им. П. А. Столыпина. 2007. № 12. С. 163–168.

2. Афанасьев В. Г Социальная информация и управление обществом. М.: Политиздат, 1975. 408 с.

3. Егорова М. А. «Когнитивное пространство» и его соотношение с понятиями «Ментальное пространство», «Когнитивная база», «Концетосфера», «Картина мира» // Вестник Иркутского государственного лингвистического университета. 2012. № 3. С. 61–68.

[16] Кодан С. В. Классификация источников изучения истории государства и права России: теоретические подходы, классификационные основания, характеристика видов // Genesis: исторические исследования. 2018. № 11. С. 31-44.

4. Ковальченко И. Д. Методы исторического исследования. М.: Наука, 2003. 485 с.

5. Кодан С. В. Классификация источников изучения истории государства и права России: теоретические подходы, классификационные основания, характеристика видов // Genesis: исторические исследования. 2018. № 11. С. 31–44.

6. Колин К. К. Философия информации и структура реальности: концепция «четырех миров» // Знание. Понимание. Умение. 2013. № 2. С. 136–147.

7. Медушевская О. М. Собрание сочинений: в 4 т. Т. 1. Философия истории и теория исторического познания. М.; Берлин: Директ-Медиа, 2017. С. 820 с.

8. Миклина Л. И. Структура и содержание социальной памяти общества // Научное мнение. 2014. № 9–3. С. 71–74.

9. Ожерельева Т. А. Об отношении понятий информационное пространство, информационное поле, информационная среда и семантическое окружение // Международный журнал прикладных и фундаментальных исследований. 2014. № 10–2. С. 21–24.

10. Поппер К. Р. Объективное знание. Эволюционный подход. Пер. с англ. М.: Эдиториал УРСС, 2002. 381 с.

11. Рогова Н. А. Тезаурус как средство повышения эффективности современных информационно-поисковых систем // Труды Академии управления МВД России. 2011. № 1. С. 113–119.

12. Розов М. А. Наука как традиция // Стёпин В. С., Горохов В. Г., Розов М. А. Философия науки и техники. М.: Контакт-Альфа, 1995. С. 8–106.

13. Седякин В. П. Информация и знания // Научные ведомости Белгородского государственного университета. Серия: Философия. Социология. Право. 2009. № 8. С. 180–187.

14. Семенюк Э. П. Информационный подход к познанию действительности. Киев: Наукова думка, 1988. 238 с.

15. Столяров Ю. Н. Сущность информации. М.: ГПНТБ России, 2000. 106 с.

16. Цветков В. Я. Информационные единицы сообщений // Фундаментальные исследования. 2007. № 12–1. С. 123–124.

17. Цветков В. Я. Информационные единицы как средство построения картины мира // Международный журнал прикладных и фундаментальных исследований. 2014. № 8–4. С. 36–40.

18. Digital Humanities: гуманитарные науки в цифровую эпоху / под ред. Г. В. Можаевой. Томск: Изд-во Томского гос. ун-та, 2016. 120 с.

Sergey V. Kodan
Doctor of Law, Professor,
Honored Lawyer of the Russian Federation,
Chief Researcher of the Department of Scientific Research,
Professor of the Department of Theory of State and Law
Urals State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
svk2005@yandex.ru

SOURCES OF KNOWLEDGE OF SOCIAL PHENOMENA AND INSTITUTIONS AS INFORMATION UNITS IN SOCIOHUMANITARIAN SOURCE STUDIES

Abstract. The article focuses on the problem of characteristics of sources of cognition of state-legal phenomena and institutions as information units. Relying on the information approach, the author turns to the questions, which are at the crossroads of information science and sociohumanitarian studies: understanding of the information unit, information space and field, descriptor, information cell of social memory, etc. In this context, the main issues of understanding and possibilities of using information phenomena in research in socio-humanitarian sciences are considered.

Keywords: information resources of scientific research, social information, social memory, social heritage, sources of knowledge of social phenomena and institutions, carriers of social information, legal source study.

УДК 343.983

Кузнецов Пётр Семёнович
кандидат юридических наук, доцент, доцент кафедры криминалистики
Уральский государственный юридический университет имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
kuzn28@yandex.ru

Камышин Владимир Анатольевич
кандидат юридических наук, доцент, доцент кафедры криминалистики
Уральский государственный юридический университет имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
advocat99@mail.ru

ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ СПРАВОЧНИКА CRIMLIB.INFO (ОПИСАНИЕ СЛЕДОВ)

Аннотация. Настоящая статья посвящена технологии описания следов на месте происшествия, возможностям их использования в процессе доказывания. Показаны основные методы фиксации материальной обстановки в деятельности следователя. Дан алгоритм описания, основанный на зрительном восприятии следов.

Ключевые слова: следы, алгоритм описания, методы фиксации, следственный осмотр.

Для цитирования:
Кузнецов П. С., Камышин В. А. Вопросы совершенствования справочника CrimLib.info (Описание следов) // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 108–113.

Описание следов в процессуальных документах традиционно вызывает затруднения у лиц, производящих расследование преступлений. Автором этих строк совместно с И. О. Макушкиным был подготовлен и опубликован иллюстрированный справочник по криминалистическому описанию объектов[1], который в своё время являлся весьма востребованным среди практических работников. В настоящее время с развитием компьютерных технологий, многие из которых обладают огромной эффективностью в качестве источников знаний и советчиков, появляется гораздо больше возможностей в оказании помощи следователям. В частности, надо

[1] Кузнецов П. С., Макушкин И. О. Криминалистическое описание объектов. Екатеринбург: УрЮИ МВД РФ, 1998. 18 с.

решительно поддержать внедрение мобильного приложения «CrimLib.info – Справочник следователя» для устройств на операционных системах Android и iOS, разработанного Д. В. Бахтеевым[2]. Вместе с тем, как и любой творческий труд, Справочник нуждается в постоянном совершенствовании и развитии. Основное направление, по нашему мнению, состоит в том, чтобы информационные системы не только охватывали огромный массив справочного материала, но и, что важнее, создавали возможности для алгоритмизации описания и предпосылки для последующей идентификации следов, их систематизации, хранения и классификации. Это будет способствовать тому, что след, как сердцевина доказывания, не будет утрачен либо неверно истолкован, а послужит основополагающим целям правосудия.

Отметим, что в Справочнике даются весьма расплывчатые и многочисленные рекомендации: так, например, при описании следов рук указаны более двенадцати параметров, включающие состояние поверхности, способ обработки следа и даже тип папиллярного узора. Если следовать таким рекомендациям, то описание будет достаточно объёмным, а учитывая, что на месте происшествия всегда множество следов, то совершенно не реально следователю выполнить указанные методики. Также и в литературе можно встретить весьма расплывчатые рекомендации, ориентирующие на большое описание. Так, Кривихин А. А. советует подробно описать предмет, на котором обнаружен след, методы его обнаружения, индивидуальные признаки, состояние поверхности, тип папиллярного рисунка и многое другое[3]. При остром дефиците времени следователи при осмотре места происшествия зачастую ограничиваются стандартной фразой «следов не обнаружено». По нашему мнению, это реакция на такие усложнённые рекомендации.

Для того чтобы следы выполнили свою важнейшую роль в правовом поле и были максимально приближены к огромным возможностям современных технологий (в том числе системам искусственного интеллекта), по нашему мнению, необходимы два критерия: точность и краткость описания.

Точность описания связана с методологией познания следов непосредственно на месте их обнаружения, следовательно с теми техническими возможностями наблюдения и измерения, которые имеются в «полевых условиях». На

[2] Акт о внедрении мобильного приложения «CrimLib.info – Справочник следователя» для устройств на операционных системах Android и iOS, разработанного Бахтеевым Д. В., в практическую деятельности следственных органов Следственного комитета Российской Федерации от 15 апреля 2021 года;

[3] Кривихин А. А. Алгоритм описания следов в протоколе осмотра места происшествия // Сборник научных статей по итогам работы седьмого круглого стола со Всероссийским и международным участием «Юридическая наука в XXI веке: актуальные проблемы и перспективы их решений», 30–31 июля 2020 г. Шахты: ООО «Конверт», 2020. С. 42.

начальном этапе нет инструментальных возможностей углублённого изучения предметной сущности следа. Уместно вспомнить слова великого учёного Д. И. Менделева, когда судья Петербургского окружного суда показал ему пробирку и попросил сказать, яд ли в ней: «Для того, чтобы быть добросовестным экспертом и сказать правду, химик должен сделать научный опыт, а не судить по виду»[4]. При следственном осмотре мы можем судить только по виду. В протоколе не напишут «золотое кольцо», «свинцовая пуля», это кольцо из жёлтого металла, пуля из серого металла.

Всякое познание начинается с живого созерцания, что особенно важно для следственного осмотра, как исходной точки расследования, всё на этом этапе должно быть безупречным и достоверным. Зрительное восприятие, наблюдение глазами, или очами, даёт нам термин «очевидность» – то, что не требует доказательств. Только то, что человек видит, он может заносить в протокол: что вижу, то пишу. Другие технические средства используются уже на последующем познании.

Краткость описания связана так же с точностью, поскольку фиксируется лишь самое очевидное. Своими очами мы наблюдаем следы давления или скольжения, наслоения или отслоения, объёмные или поверхностные. Мы видим механизм образования следа, а чем он образован – это уже задачи последующего познания. В. Я. Колдин выделяет стадию предварительного исследования, предварительный анализ идентификационных признаков, как целостных систем, что характерно для следственного осмотра. В последующей стадии уже происходит аналитическое исследование[5]. Поэтому главная задача алгоритма описания состоит в обеспечении последующего исследования следов с применением более сложных технических средств и специальных знаний. А на этапе осмотра нет технических возможностей углублённого изучения следов, важна их точная и краткая фиксация в материальной обстановке с тем, чтобы показать: они существуют в этом мире объективно, независимо от воспринимающего субъекта.

Точное и краткое описание, выполненное по формуле «что вижу то и пишу» приближает наше субъективное восприятие к критериям объективности. Наши органы чувств, невооружённое зрение приближаются по своим функциям к техническому фиксированию подобно фотоаппарату. Опишем характерный пример. *Автор этих строк проводил транспортно-трасологическую экспертизу по ДТП, в основе которой были положены следы колёс на проезжей части дороги. Сторона защиты выдвинула аргумент о том, что на схеме к протоколу осмотра указаны не следы колёс транспортного средства, а траектория его движения. Судья был*

[4] Крылов И. Ф. Судебная экспертиза в уголовном процессе, Ленинград: Издтельство Ленинградского государственного университета. 1963. 214 с.

[5] Колдин В. Я. Судебная идентификация. М.: «ЛексЭст», 2002. 134 с.

вынужден вызвать в суд работника ГИБДД, который производил осмотр, и тот подтвердил, что описывает только то, что видит на месте происшествия, и на схеме указаны именно следы, а не рассуждения о траектории движения.

Описание должно охватывать только самое очевидное, наблюдаемое непосредственно глазами: форма следа, его размеры, цвет, видимый механизм образования. По нашему мнению, любой след, на любой поверхности должен описываться одинаково. В связи с чем предлагаем следующий алгоритм: «где, что, какой и как»[6].

Прежде всего необходимо зафиксировать пространственное расположение следа от двух неподвижных ориентиров, тем самым след закрепляется в конкретной материальной обстановке и становится аргументом в доказывании. Например: «*На внутренней стороне двери в 20 см. от замочной скважины и в 140 см. от пола...*». Далее указывается, что обнаружен след, который дополнительно описывается по механизму образования, указывается на вид давления или скольжения, наслоения или отслоения. При характеристике, какой след обнаружен, приводятся его форма и размеры. Многие авторы дают рекомендации по описанию типа папиллярного узора, но чаще всего такие детали слабо просматриваются на месте происшествия, и лучше эти данные получать в более благоприятных условиях.

Принцип обеспечения последующего познания ставит перед алгоритмом описания задачу последовательного всё более глубокого исследования, и каждый шаг должен быть безупречным, не вызывать сомнений и закладывать основу для дальнейшей работы. Алгоритм описания заканчивается сведениями о том, как зафиксирован и изъят след. Описываются технические средства обработки следа и все манипуляции по его изъятию.

Алгоритм точного и краткого описания приближает нас к возможностям искусственного интеллекта, хотя, конечно, в ближайшей перспективе компьютер не сможет заменить человека при осмотре места происшествия. По справедливому замечанию Д. В. Бахтеева, окончательная обработка и интерпретация информации остаётся за человеком[7]. Могут возникнуть опасения, что алгоритм описания приведёт к шаблонным автоматическим действиям, без процессов действительного осмысления и повлечёт за собой ошибки. При расследовании преступлений очень важны логические, эвристические и интуитивные механизмы мышления, особенно на этапе обнаружения следов[8]. А уже на этапе фиксации на

---

[6] Кузнецов П. С. Криминалистическое познание следов преступления: учебное пособие. Екатеринбург: Изд-во Екатеринбургской высшей школы МВД России, 1996. С. 34.

[7] Бахтеев Д. В. Компьютерное зрение и распознавание образов в криминалистике // Российское право: образование, практика, наука. 2019. № 3 (111). С. 68.

[8] Драпкин Л. Я. Логические, эвристические и интуитивные механизмы мышления

первый план выступает точность описания. Упорядоченное описание отличается от произвольного тем, что оно проводится полно, последовательно и с использованием устоявшейся, общепринятой терминологии. Здесь на первый план выступает технология, как система привычных, много раз повторяемых действий. И нельзя говорить, что это проходит без контроля мышления: всё и всегда проходит под контролем человеческого разума, только в этом случае даже многократно повторяемые действия, одинаковые термины, как бы подаваемые автоматически, будут осуществляться и использоваться грамотно, способствуя достижению целей правосудия. По нашему глубокому убеждению, в этом и проявляется настоящий профессионализм следователя, как бы автоматически, но всё под контролем.

Алгоритм описания создаёт предпосылки для выделения однозначно трактуемых элементов и признаков следов, подготовленных для машинной обработки. Соотношение человеческого разума и искусственного интеллекта наиболее ярко проявилось при создании дактилоскопических поисковых систем. До создания АДИС «Папилон» предпринимались многочисленные попытки идентификации папиллярных узоров, однако они не давали результатов поскольку кодировка узора производилась вручную людьми. Автор этих строк работал экспертом-криминалистом и получил задание руководства о введении следов рук в систему «След 2», когда уже были экспертами установлены подозреваемые, однако компьютер не смог установить тождество. Закодированные человеком папиллярные узоры несут ошибки субъективности. Только когда компьютер сам «увидел след», отсканировал его, система «Папилон» дала великолепные результаты.

Человеческий разум способен на размышления, пространные рассуждения, абстрактное мышление. Искусственный интеллект работает в миллиарды раз быстрее и уже обыгрывает человека в шахматы. Приблизить возможности техники и разума человека, по нашему мнению, поможет точное, краткое описание в виде единообразно понимаемого алгоритма.

Список литературы

1. Бахтеев Д. В. Компьютерное зрение и распознавание образов в криминалистике // Российское право: образование, практика, наука. 2019. № 3 (111). С. 66–74.

2. Драпкин Л. Я. Логические, эвристические и интуитивные механизмы мышления следователя в процессе раскрытия и расследования преступлений: монография. Екатеринбург: Издательский дом УрГЮУ, 2018. 101 с.

3. Колдин В. Я. Судебная идентификация. М.: «ЛексЭст», 2002. 528 с.

следователя в процессе раскрытия и расследования преступлений: моногр. Екатеринбург: Издательский дом УрГЮУ, 2018. 101 с.

4. Кривихин А. А. Алгоритм описания следов в протоколе осмотра места происшествия // Сборник научных статей по итогам работы седьмого круглого стола со Всероссийским и международным участием «Юридическая наука в XXI веке: актуальные проблемы и перспективы их решений», 30–31 июля 2020 г. Шахты: ООО «Конверт», 2020. С. 42–44.

5. Крылов И. Ф. Судебная экспертиза в уголовном процессе. Ленинград: Издтельство Ленинградского государственного университета, 1963. 214 с.

6. Кузнецов П. С., Макушкин И. О. Криминалистическое описание объектов. Екатеринбург: УрЮИ МВД РФ, 1998. 18 с.

7. Кузнецов П. С. Криминалистическое познание следов преступления: учебное пособие. Екатеринбург: Изд-во Екатеринбургской высшей школы МВД России, 1996. 92 с.

Peter S. Kuznetsov
PhD (in Law), Associate Professor,
Associate Professor of the Department of Criminalistics,
Ural state law university named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
kuzn28@yandex.ru

Vladimir A. Kamyshin
PhD (in Law), Associate Professor,
Associate Professor of the Department of Criminalistics,
Ural state law university named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
advocat99@mail.ru

ISSUES OF IMPROVING THE HANDBOOK CRIMLIB.INFO (DESCRIPTION OF THE TRACES)

Abstract. This article is devoted to the technology of describing traces at the scene of the incident, the possibilities of their use in the process of proof. The main methods of fixing the material situation in the investigator's activity are shown. The description algorithm based on the visual perception of traces is given.

Keywords: traces, description algorithm, fixation methods, investigative examination.

УДК 340

Коваленко Наталья Евгеньевна
Аспирант Юридического института,
Алтайский государственный университет
(г. Барнаул, Российская Федерация)
Kovalenkorub5@gmail.com

ЦИФРОВИЗАЦИЯ СУДЕБНОГО ПРОЦЕССА: ПРОБЛЕМЫ ТЕОРИИ

Аннотация. В статье рассматривается современная теория «цифровизации судебного процесса», анализируется вопрос об искусственном интеллекте как субъекте права и в целом, о его месте в современной правовой действительности. Сделан вывод о несоответсвии искуственного интеллекта критериям субъекта с точки зрения ценностного подхода к определению последнего.

Ключевые слова: искусственный интеллект, цифровизации судебного процесса, субъект права, субъект правоотношений, антропоцентричность права.

Для цитирования:
Коваленко Н. Е. Цифровизация судебного процесса: проблемы теории // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 114–116.

Рассмотрим современную теорию «цифровизации судебного процесса». Отдельные аспекты данной проблемы исследовались в юридической доктрине, однако до сих пор вопрос о допустимых видах субъектов права в судебном процессе остаётся не решённым. Система искусственного интеллекта (ИИ) не сможет дать оценку доказательствам, определить их относимость и допустимость. Однако, возможно следует разработать программы, облегчающие работу судье. Например, по отдельным категориям дел, например в части назначения пенсии. По ним возникает сложность в определении стажа, засчитанных сроках, подбора нормативно-правового акта, регулирующего трудовые отношения на тот период, в связи с чем должны применяться акты, действующие в прошлом, но утратившие силу в настоящее время. Программа попросту не сможет «протолковать» правовые нормы, поскольку она не является субъектом, не входит в состав суда.

В данном случае ИИ способен на унификацию и учёт данных, то есть может выступить в роли усовершенствованной Справочной правовой системы. Данной позиции придерживается профессор А. А. Васильев, в частности, он считает, что ИИ и его юниты не могут выступать в качестве субъекта права, субъекта правоотношения, независимо осуществляющих выбор решения при рассмотрении юридических казусов.

Так, в техническом плане будет верно ИИ отвести роль объекта или же средства – технологии, методики, позволяющей разгрузить юриста от волокиты[1].

Несмотря на недопустимость позиционирования систем ИИ в качестве полноправных субъектов права, неверным будет полностью их исключать из правовой действительности. Присутствие информационного пространства в обществе играет и положительную роль. Так, профессор О. А. Пучков отмечает, что информационные технологии, искусственный интеллект ускоряют процессы развития социальных институтов, создают прямые связи с государством, его органами, через системы Госуслуг, электронного правительства, а наличие электронного документооборота способствует увеличению скорости оказания государственных услуг, разгрузке в посещаемости государственных учреждений[2].

Таким образом, в период информационного общества ценности могут подменяться или исчезать под неконтролируемым потоком непроверенной, ложной информации. В этом случае роль социальных регуляторов, права, в первую очередь, многократно возрастает, прежде всего, для обеспечения безопасности государства и общества.

Список литературы

1. Печатнова Ю. В., Васильев А. А. Место искусственного интеллекта среди элементов состава правоотношения // Цифровое право. 2020. № 1 (4). С. 74–83.
2. Пучков О. А. Информационное общество и информационные процессы в современной России: векторы развития // Трансформация права в информационном обществе. Материалы II Всероссийского научно-практического форума молодых учёных и студентов. 2019. С. 503–513.

Natalia E. Kovalenko
Postgraduate student of Law Institute,
Altai State University
(Barnaul, Russian Federation)
Kovalenkorub5@gmail.com

DIGITALIZATION OF THE JUDICIAL PROCESS: PROBLEMS OF THEORY

[1] Печатнова Ю. В., Васильев А. А. Место искусственного интеллекта среди элементов состава правоотношения // Цифровое право. 2020. № 1 (4). С. 74–83.
[2] Пучков О. А. Информационное общество и информационные процессы в современной России: векторы развития // Трансформация права в информационном обществе. Материалы II Всероссийского научно-практического форума молодых учёных и студентов. 2019. С. 503–513.

Abstract. The article deals with the modern theory of «digitalization of the judicial process». The article analyzes the issue of artificial intelligence as a subject of law. The conclusion is made about the value aspects in the definition of the subject of law.

Keywords: artificial intelligence, digitalization of the judicial process, subject of law, subject of legal relations, anthropocentricity of law.

УДК 343.34

Кулаевский Андрей Витальевич
Аспирант кафедры уголовного процесса и криминалистки
Юридический институт
Алтайский государственный университет
(Барнаул, Российская Федерация).
andrei8888.98@mail.ru

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ УСТАНОВЛЕНИИ ЛИЦА, СОВЕРШИВШЕГО ПРЕСТУПЛЕНИЕ

Аннотация. В статье рассмотрены возможности использования технологий искусственного интеллекта при установлении лица, совершившего преступление. Автором анализируются качественные характеристики искусственного интеллекта на примере современных криминалистических средств идентификации преступника.

Ключевые слова: цифровизация криминалистики, искусственный интеллект, преступник, АИПС.

Для цитирования:
Кулаевский А. В. Использование искусственного интеллекта при установлении лица, совершившего преступление // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 117–122.

Четвёртая промышленная революция, активная цифровизация всех сфер человеческой деятельности, включая судопроизводство, влечёт необходимость обеспечения правоохранительных органов эффективными инструментами для расследования преступлений.

Использование цифровых устройств в повседневной жизни формирует технические компетенции, которые напрямую влияют на способ совершения преступления. Повсеместное распространение цифровых устройств и активное их применение предопределило развитие цифровой преступности.

Одной из причин цифровой трансформации правоохранительных органов РФ является активное противодействие цифровой преступности, обусловленной развитием цифровых технологий. Вышесказанное подтверждает статистика. Так, преступлений, совершаемых с помощью IT-технологий, только за 6 месяцев 2022 года зафиксировано 249 тыс. Такое число преступлений практически равно суммарному количеству преступлений в данной сфере за 2021 год – 271,1 тыс. преступлений. В свою очередь, за весь 2022 год наблюдается двукратное увеличение преступлений, совершённых с использованием

информационно-телекоммуникационных технологий – 522, 6 тыс.[1]

В настоящее время цифровые технологии используются при обработке криминалистически значимой информации. К примеру, использование базы данных ИБД-Ф «Дистанционное мошенничество» облегчает поиск установочных данных лица, совершившего преступление. Но всё же будущее автоматизированных цифровых криминалистических инструментов лежит в машинной обработке и искусственном интеллекте.

Понятие «искусственный интеллект» по-разному определяется учёными различных специальностей. Обратимся к понятию, которое сформулировал криминалист, специалист в области изучения искусственного интеллекта Д. В. Бахтеев. Автор указывает, что под искусственным интеллектом следует понимать компьютерные программы, программные комплексы, способные не просто действовать по заранее заданному алгоритму, но и реализовывать такие имманентные человеку творческие функции, как прогнозирование, оценка рисков, работа с неполными данными и т. д.[2]

Таким образом, работа искусственного интеллекта по заданному поиску заключается в анализе необходимой информации, с помощью которой и осуществляется поиск. При установлении лица, совершившего преступление, такой поиск необходимо выполнять, исходя из свойств личности.

В криминалистике структура личности преступника рассматривается во взаимодействии трёх свойств: биологических, к примеру, данные, характеризующие внешний облик; социальных, к примеру, персональные данные преступника и психологические, к примеру, данные об эмоциональных, волевых и интеллектуальных сферах личности преступника[3].

Соответственно, искусственный интеллект как программная система, имитирующая процесс мышления человека, для успешного поиска преступника должна учитывать свойства его личности.

Уникальность искусственного интеллекта заключается в том, что он способен рационализировать, автоматизировать, адаптировать, распознавать и классифицировать информацию о лице, совершившем преступление[4].

---

[1] Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2022 года // МВД.РФ [Электронный ресурс]. URL: https://мвд.рф/reports/item/35396677/.

[2] Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. №. 2. С. 43–49.

[3] Дяблова Ю. Л. Понятие и структура личности в криминалистике // Известия Тульского государственного университета. Экономические и юридические науки. 2016. №. 2-2. С. 99–110.

[4] Василова Д. И. Искусственный интеллект в криминалистике // Всероссийская научно-практическая конференция «Информационные технологии в науке и образовании» [Электронный ресурс]. URL: http://econf.rae.ru/article/11543 (дата обращения: 01.05.2023).

Рациональность искусственного интеллекта заключается в выборе наиболее правильных решений, способных развивать заданную область его работы. К примеру, автоматизированная биометрическая идентификация лиц может быть разработана на базе единой габитоскопической автоматизированной системы на базе АИПС «Портрет-Поиск». Такая АИПС способна взаимодействовать с различными криминалистическими учётам, обеспечивая хранение криминалистически значимой информации.

Автоматический характер искусственного интеллекта наглядно появляется в итогах тестирования указанной АИПС. Оно показало высокую результативность поиска лиц по конкретным образцам с различными исходными параметрами (возрастные изменения, наличие или отсутствие усов, бороды, очков, повороты головы, различные условия съёмки и т. д.).

Кроме того, указанная система не критична к возможностям определения графического изображения лица, зрачков глаз и может осуществлять идентификационные поиски по другим антропометрическим точкам. Такая особенность позволяет проводить сравнение по фотографиям трупов и фотороботам разыскиваемых лиц.

Для более точного определения личности преступника такая программа может работать синхронно с аппаратно-программным комплексом «Сегмент-С», который специализируется на определении места абонента. Так, в случае если у идентифицируемого лица в момент распознания АПС «Портрет-Поиск» имеются средства связи, то оно может подтверждать его нахождение в конкретном месте.

Также следует отметить, что Министерство внутренних дел Российской Федерации заключило контракт, согласно которому с 2022 г. ведомство использует программу «Зеркало», направленную на выявление признаков фальсификаций искусственными нейронными сетями видеоизображений людей (дипфейк)[5]. Использование подобных систем значительно облегчает производство видеотехнических экспертиз.

Адаптивность искусственного интеллекта заключается в его способности обрабатывать большое количество различной информации, предоставленной для обработки в различных видах: текст, рисунок, фото, видео. Таким образом, информация, с помощью которой можно осуществить криминалистическую идентификацию лица, совершившего преступление, и которая подлежит обработке искусственным интеллектом может быть:

1. Зафиксирована специальным средством фиксации, установленным в общественном месте;
2. Расположена в сети Интернет;
3. Сохранена в корпоративных базах данных операторов сотовой связи и т. д.

[5] МВД к концу 2022 года получит IT-разработку по распознаванию видео с заменой лиц // ТАСС [Электронный ресурс]. URL: https://tass.ru/obschestvo/11307705 (дата обращения: 01.05.2023).

Также искусственный интеллект способен классифицировать данные согласно заданным параметрам, в частности, при оценке достоверности информации в Интернете, определении способов подделок и подлогов.

К примеру, учёными Пермского государственного национального исследовательского института разработан алгоритм позволяющий установить лицо, склонное к совершению серийных преступлений. Такой алгоритм учитывает факторы, указывающие на особенности личности преступника. Авторами алгоритма были изучены различные параметры серийного преступника: пол, социальное положение, данные о перенесённом насилии в детстве, наличие родителей, семейный статус лица, склонность к алкоголизму у родителей, а также наличие или отсутствие у него детей[6]. Учёные изучали, какой из входных параметров в конкретной ситуации оказывает наибольшее влияние на склонность к насилию. Анализируя указанные параметры, авторам алгоритма удалось выявить исключительные параметры, по котором можно выявить серийного преступника.

Также криминалистическая идентификация лица, совершившего преступление возможна по клавиатурному почерку. Такой способ идентификации представляет собой анализ стиля ввода символов. Уникальность стиля определяет ряд параметров, таких как скорость набора текста, время удержания клавиш, сила нажима на клавиши[7]. При идентификации стиля обычно учитывается кодовая комбинация и на основе её ввода производится сравнение.

Это демонстрирует способность искусственного интеллекта осуществлять классификацию объектов по группам в соответствии с заранее заданным параметрами.

В качестве другого примера проявления указанного свойства можно указать на разработки кафедры криминалистики Уральского государственного юридического университета по внедрению искусственного интеллекта: учёные создают искусственную нейронную сеть, ориентированную на выявление признаков подлога подписей, выполненных без использования механических и компьютерных устройств[8].

В заключение необходимо отметить, что искусственный интеллект – это феномен современного

---

[6] Ясницкий Л. Н., Ваулева С. В., Сафонова Д. Н., Черепанов Ф. М. Использование методов искусственного интеллекта в изучении личности серийных убийц // Всероссийский криминологический журнал. 2015. Т. 9. № 3. С. 428. DOI 10.17150/1996-7756.2015.9(3).423-430.

[7] Полякова А. В. Использование при раскрытии и расследовании преступлений биометрических систем аутентификации пользователей в мобильных устройствах связи // I Минские криминалистические чтения: материалы Международной научно-практической конференции, (Минск, 20 декабря 2018 г.): в 2 ч. / УО «Академия Министерства внутренних дел Республики Беларусь». Минск, 2018. Ч. 1. С. 281–287.

[8] Бахтеев Д. В. Особенности распознавания подлога подписи человеком как первичные критерии для разработки системы искусственного интеллекта // Сибирское юридическое обозрение. 2020. Т. 17. №. 4. С. 514–522.

общества, ставящий перед криминалистикой новые задачи по изучению, применению его в качестве средства борьбы с преступностью. Моделирование искусственным интеллектом творческих и когнитивных способностей человека позволяет оценивать его как помощника при установлении лица, совершившего преступление.

Список литературы

1. Бахтеев Д. В. Особенности распознавания подлога подписи человеком как первичные критерии для разработки системы искусственного интеллекта // Сибирское юридическое обозрение. 2020. Т. 17. №. 4. С. 514–522.

2. Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. №. 2. С. 43–49.

3. Василова Д. И. Искусственный интеллект в криминалистике // Всероссийская научно-практическая конференция «Информационные технологии в науке и образовании» [Электронный ресурс]. URL: http://econf.rae.ru/article/11543.

4. Дяблова Ю. Л. Понятие и структура личности в криминалистике // Известия Тульского государственного университета. Экономические и юридические науки. 2016. №. 2-2. С. 99–110.

5. Полякова А. В. Использование при раскрытии и расследовании преступлений биометрических систем аутентификации пользователей в мобильных устройствах связи // I Минские криминалистические чтения: материалы Международной научно-практической конференции, (Минск, 20 декабря 2018 г.): в 2 ч. / УО «Академия Министерства внутренних дел Республики Беларусь». Минск, 2018. Ч. 1. С. 281–287.

6. Ясницкий Л. Н., Ваулева С. В., Сафонова Д. Н., Черепанов Ф. М. Использование методов искусственного интеллекта в изучении личности серийных убийц // Всероссийский криминологический журнал. 2015. Т. 9. № 3. С. 423–430. DOI 10.17150/1996-7756.2015.9(3).423-430.

Andrey V. Kulaevsky
Postgraduate student
of the Department of Criminal Procedure and Criminology
Law Institute
Altai State University
(Barnaul, Russian Federation)
andrei8888.98@mail.ru

THE USE OF ARTIFICIAL INTELLIGENCE IN IDENTIFYING THE PERSON WHO COMMITTED THE CRIME

Abstract. The article considers the possibilities of using artificial intelligence technologies in identifying a criminal. The author analyzes modern technologies capable of searching for the person who committed the crime.

Keywords: digitalization of criminalistics, artificial intelligence, the person who committed the crime, AIPS.

УДК 378.147

Лемешкин Алексей Михайлович
Заведующий отдела информационных технологий
Иркутский юридический институт (филиал)
Университета прокуратуры Российской Федерации
(г. Иркутск, Российская Федерация)
alexlm@mail.ru

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ДИСТАНЦИОННОГО ВЗАИМОДЕЙСТВИЯ В ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА В УСЛОВИЯХ ГЛОБАЛЬНЫХ ВЫЗОВОВ

Аннотация. В статье проводится обзор технологий дистанционного взаимодействия, их преимущества и недостатки, автор делится опытом использования технологий дистанционного взаимодействия на примере Иркутского юридического института (филиала) Университета прокуратуры Российской Федерации.

Ключевые слова: технологии дистанционного взаимодействия, цифровизация, цифровые технологии, цифровая трансформация.

Для цитирования:
Лемешкин А. М. Использование технологий дистанционного взаимодействия в организации учебного процесса в условиях глобальных вызовов // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 123–129.

Современный мир невозможно представить без цифровых технологий дистанционного взаимодействия в учебном процессе. Катализатором их бурного развития в последние годы послужили глобальные вызовы человечеству, такие как пандемия COVID-19. Пандемия закончилась, а технологии, навыки и умение работать с ними остались. Мы научились собирать огромные виртуальные аудитории, теперь расстояние для нас не имеет преграды. Мир изменился, он стал другим, благодаря цифровым технологиям.

Дистанционное обучение – это процесс обучения, который осуществляется удалённо с использованием различных технологий и инструментов. Существует множество технологий дистанционного взаимодействия, которые могут быть использованы для организации учебного процесса[1]. Некоторые из них включают в себя:

1. Видеоконференции (вебинары): технология, которая

[1] Уткина Т. И., Ряпина Н. Е. Оценка влияния дистанционного обучения на успешность изучения иностранного языка в неязыковом вузе // Вестник Томского государственного университета. 2021. № 473. С. 193.

позволяет участникам учебного процесса общаться между собой в режиме реального времени с помощью видео- и аудиосвязи.

2. Электронную почту: технология, которая позволяет участникам учебного процесса обмениваться сообщениями и файлами.

3. Системы управления обучением (LMS): программное обеспечение, которое позволяет организовать и проводить учебный процесс удалённо.

4. Социальные сети: технология, которая позволяет участникам учебного процесса общаться между собой и делиться информацией.

5. ЭИОС: электронная информационно-образовательная среда в образовательном учреждении высшего образования. ЭИОС должна обеспечивать эффективное использование информационных технологий в учебном процессе, в частности, она должна содержать информацию о курсах и учебных материалах, а также обеспечивать возможность удалённого доступа к ним.

Как и у любых технологий, существуют свои преимущества и недостатки использования у дистанционного взаимодействия в организации учебного процесса.

К преимуществам использования технологий дистанционного обучения можно отнести:

1. Гибкость: студенты могут изучать материалы и выполнять задания в удобное для них время.

2. Доступность: студенты могут получить доступ к материалам и заданиям из любой точки мира.

3. Экономия времени и денег: студенты не тратят время и деньги на поездки в учебные заведения.

4. Индивидуализация обучения: студенты могут изучать материалы в своём собственном темпе.

5. Улучшение навыков использования технологий: студенты могут получить опыт работы с различными программными продуктами и сервисами.

В числе недостатков использования технологий дистанционного обучения укажем:

1. Ограниченный контакт с преподавателем: студенты могут испытывать затруднения при получении помощи от преподавателя.

2. Ограниченный контакт с сокурсниками: студенты (слушатели) могут испытывать затруднения при общении с сокурсниками.

3. Необходимость самостоятельной работы: студентам может быть сложно организовать своё время и выполнить задания без постоянного контроля преподавателя.

4. Ограниченный доступ к оборудованию и программному обеспечению: студентам может потребоваться специальное оборудование или программное обеспечение для выполнения заданий.

5. Ограниченный доступ к библиотекам и другим ресурсам: студентам может быть сложно получить доступ к библиотекам и другим ресурсам, которые могут быть необходимы для выполнения заданий.

Хочется поделиться опытом использования технологий

дистанционного взаимодействия в организации учебного процесса в Иркутском юридическом институте (филиале) федерального государственного казённого образовательного учреждения высшего образования «Университета прокуратуры Российской Федерации» (далее – Институт) в условиях глобальных вызовов.

Институт является обособленным структурным подразделением федерального государственного казённого образовательного учреждения высшего образования «Университет прокуратуры Российской Федерации». Юридический факультет осуществляет подготовку студентов по направлению Юриспруденция только по очной форме и только на бюджетной основе. Факультет профессиональной переподготовки и повышения квалификации осуществляет реализацию дополнительных профессиональных программ повышения квалификации и профессиональной переподготовки для различных категорий прокурорских работников.

До 2020 года технологии дистанционного взаимодействия массово в организации учебного процесса не использовались. Для проведения отдельных мероприятий в виде конференций использовали Skype или сервер видеоконференцсвязи (TrueConf) Университета прокуратуры Российской Федерации. В начале 2020 года в связи с пандемией COVID-19 обучение слушателей факультета повышения квалификации и профессиональной переподготовки было перенесено на более поздний срок, а студенты юридического факультета переведены на удалённый формат обучения с использованием технологий дистанционного взаимодействия. Мне, как заведующему отделом информационных технологий, была поставлена задача в кратчайший срок найти и применить на практике технологии дистанционного взаимодействия для проведения занятий со студентами в режиме реального времени без изменения расписания. Задача осложнялась тем, что в институте не было опыта и навыков использования таких технологий. В первые дни занятий стали использовать Discord – платформу для общения и обмена информацией между людьми в режиме реального времени. Для каждой учебной группы создавали голосовой канал на сервере, а студенты и преподаватель подключались к нему. Точно так же создавали и работали с группами в VK. Но для эффективной работы со студентами в дистанционном режиме обучения требовалось нечто большее, а именно: возможность видеосвязи, показа презентаций, интерактивная доска, работа с группами в течении длительного времени, без перерыва. Пришло понимание того, что это должен быть свой собственный сервер видеоконференцсвязи, который бы обеспечивал одновременное подключение 230 студентов и 10–20 преподавателей. Для реализации этой задачи был выбран BigBlueButton – бесплатная и открытая платформа для видеоконференций с открытым исходным кодом. С помощью BigBlueButton была успешно

завершена весенняя сессия 2020 года и проведено обучение студентов в дистанционном формате в 2020/2021 учебном году. Расписание занятий не менялось под дистанционный формат, студенты точно по времени, с помощью BigBlueButton, заходили в свои учебные аудитории, только теперь виртуальные, и присутствовали на занятиях с помощью видеоконференцсвязи. Благодаря этой платформе студенты не только проходили обучение, но и сдавали экзамены, защищали свои дипломные работы. Интересен опыт проведения экзаменов в дистанционном формате. Взаимодействие с экзаменуемым осуществлялось посредством видеосвязи и подтверждённой электронной почты. Экзаменационные билеты случайным образом раскладывались в пронумерованные конверты, на интерактивной доске BigBlueButton вывешивалась таблица с номерами конвертов. Экзаменуемый называл номер конверта, перед видеокамерой конверт с этим номером вскрывали и извлекали из него экзаменационный билет с указанным номером, скан которого высылали на электронную почту экзаменуемого. Далее номер конверта вычёркивали из таблицы на интерактивной доске. Таким простым способом была реализована случайная выборка экзаменационных билетов. Всё происходило как на реальном экзамене, студенты включали камеру, заходили на экзамен, тянули билеты и готовились к ответу или заполняли специальный шаблон при письменном ответе. В процессе подготовки к ответу студент должен был постоянно находиться на видеосвязи, камера у него должна была быть установлена так, что в неё можно было видеть его и его рабочее пространство. Для проведения квалификационного экзамена у абитуриентов требовалось проводить процедуру идентификации по паспорту гражданина Российской Федерации. Паспорт в раскрытом виде демонстрировался на камеру, приёмная комиссия удостоверяла личность абитуриента.

Все учебно-методические материалы и учебная литература были размещены в электронной информационно-образовательной среде на сайте института.

В соответствии с «Концепцией цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2025 года»[2] в институте в 2020 году была создана единая защищённая сеть передачи данных, обеспечивающая потребности органов прокуратуры всех уровней по сбору и передаче данных граждан, бизнеса, государственных органов с учётом технических требований, предъявляемых цифровыми технологиями (включая IP-телефонию, видеоконференцсвязь, единую систему электронной почты).

С помощью системы видеоконференцсвязи органов

[2] Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года: приказ Генерального прокурора Российской Федерации от 14 сентября 2017 г. № 627 // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_278651/ (дата обращения: 12.05.2023).

прокуратуры было возобновлено обучение прокурорских работников.

В Институте 2020/21 году обучение на 7 потоках было организовано с использованием дистанционных образовательных технологий. Всего обучено 294 человека:

– по дополнительной профессиональной программе профессиональной переподготовки – 30 прокурорских работников, состоящих в резерве кадров для выдвижения на должности прокуроров городов, районов и приравненных к ним прокуроров специализированных прокуратур;

– по дополнительным профессиональным программам повышения квалификации – 264 прокурорских работника.

Слушатели 2020/2021 уч. года проходили обучение с использованием элементов дистанционных образовательных технологий. Лекционные занятия, все формы семинарских занятий проведены в единой защищённой сети передачи данных органов прокуратуры Российской Федерации с использованием ведомственной видеоконференцсвязи прокуратуры Российской Федерации. Что наложило определённые ограничения на проведение занятий. Обучающиеся находились на своих рабочих местах и были вынуждены решать текущие проблемы своей профессиональной деятельности, что не способствовало усвоению учебного материала. Учебно-методические материалы представлялись слушателям с использованием ЭИОС сайта института.

Следует подробнее остановиться на некоторых из описанных выше недостатков дистанционного обучения. Особенно остро проблема самостоятельного обучения стоит перед студентами первого курса. Студенческий коллективизм – особая форма взаимодействия, эффективно формируемая при совместной контактной деятельности. На базе уже сложившегося синхронного взаимодействия студентов и преподавателей организовать самостоятельную работу представляется менее проблематично, чем среди несформированного психологически коллектива студентов первого курса, у которых отсутствует опыт совместной работы с новым для них коллективом. В целом, в условиях дистанционного обучения усложняется выполнение воспитательных задач, которые эффективно реализуются в ходе совместных учебных занятий, дополнительных образовательных мероприятий, коллективной досуговой деятельности[3].

Другой проблемой при дистанционном обучении является восприятие преподавателя. Преподавателю сложно отслеживать обратную связь со студентами. В обычном формате это невербальный язык – глаза, жесты, поза и т. п. При дистанционном обучении – видео, на котором в лучшем случае видно лицо,

[3] Курьян М. Л., Воронина Е. А. Внеаудиторное общение студентов и преподавателей: восприятие и фактический опыт // Science for Education Today. 2019. Т. 9. № 3. С. 42–57. DOI: 10.15293/2658-6762.1903.03.

оно может быть дополнено комментариями в чате, показывающими эмоциональное и интеллектуальное отношение к обсуждаемым вопросам. Кроме этого, важно отметить, что область технологий дистанционного обучения быстро развивается и сегодняшние формы являются ранними и переходными. Обратная связь от учеников и преподавателей помогает разработчикам совершенствовать технологии и конкурировать друг с другом[4].

В рамках стратегии цифровой трансформации отрасли науки и высшего образования, определяющей основные подходы к достижению «цифровой зрелости» в России, было принято постановление Правительства Российской Федерации «О государственной информационной системе “Современная цифровая образовательная среда”»[5]. Наше государство прилагает все усилия для развития технологий дистанционного взаимодействия в организации учебного процесса. При государственной поддержке будут запущены грандиозные проекты, которые в будущем определят цифровую трансформацию высшего образования в Российской Федерации.

Список литературы

1. Курьян М. Л., Воронина Е. А. Внеаудиторное общение студентов и преподавателей: восприятие и фактический опыт // Science for Education Today. 2019. Т. 9. № 3. С. 42–57. DOI: 10.15293/2658-6762.1903.03.

2. Чанчаева Е. А., Куриленко Т. К., Недельский В. О., Кругликова Е. В., Гржибовский А. М. Сравнительный анализ эффективности обучения по естественнонаучным дисциплинам при дистанционном и традиционном формате // Science for Education Today. 2022. Т. 12. № 3. С. 149–168. DOI: 10.15293/2658-6762.2203.08.

Alexei M. Lemeshkin
Head of IT Department
Irkutsk Institute of Law (branch)
of the University of the Public Prosecutor's Office of the Russian Federation
(Irkutsk, Russian Federation)
alexlm@mail.ru

[4] Чанчаева Е. А., Куриленко Т. К., Недельский В. О., Кругликова Е. В., Гржибовский А. М. Сравнительный анализ эффективности обучения по естественнонаучным дисциплинам при дистанционном и традиционном формате // Science for Education Today. 2022. Т. 12. № 3. С. 149–168. DOI: 10.15293/2658-6762.2203.08.

[5] О государственной информационной системе «Современная цифровая образовательная среда» (вместе с «Положением о государственной информационной системе “Современная цифровая образовательная среда”»): постановление Правительства РФ от 16 ноября 2020 г. № 1836. // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_368202/ (дата обращения: 12.05.2023).

THE USE OF REMOTE INTERACTION TECHNOLOGIES IN EDUCATIONAL PROCESS ORGANIZATION UNDER THE CONDITIONS OF GLOBAL CHALLENGES

Abstract. The paper provides an overview of remote interaction technologies, their advantages and disadvantages. The author shares his experience in using remote interaction technologies on the example of Irkutsk Institute of Law (branch) of the Prosecutor's Office University of the Russian Federation.

Key words: remote interaction technologies, digitalization, digital technologies, digital transformation.

УДК 34.01

Лескина Элеонора Игоревна
Кандидат юридических наук, доцент кафедры
информационного права и цифровых технологий
Саратовская государственная юридическая академия,
(г. Саратов, Россия)
elli-m@mail.ru

ТЕХНОЛОГИИ МЕТАВСЕЛЕННОЙ В ОБРАЗОВАНИИ

Аннотация. Развитие технологий влияет на многие сферы общественных отношений и область образования здесь не является исключением. Метавселенная как особое, новое цифровое общество, объединяющее множество пользователей, предоставляет большие возможности в сферах здравоохранения, трудовых отношений, электронной коммерции, образования и др. Статья направлена на определение понятия, сущности, признаков, принципов метавселенной, анализ направлений внедрения сопутствующих технологий в различные области, особенно в образование.

Ключевые слова: информационное общество; цифровизация; сквозные технологии; метавселенная; современное образование; персональные данные; принципы метавселенной.

Для цитирования:
Лескина Э. И. Технологии метавселенной в образовании // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 130–137.

Широкое использование цифровых технологий привело к интеграции различных направлений науки, формированию новой технологической среды, социально-экономической, политической, юридической реальности, а также новому способу производства, цифровизации общественных отношений и права. Здесь цифровое пространство является инструментом, в том числе, и правового регулирования, что в свою очередь приводит к появлению новых социальных феноменов.

Развитие информационно-коммуникационных технологий, переход к обществу знаний предполагает развитие всех областей, значительное преобразования привычных представлений о возможностях коммуникации. Вместо того, чтобы быть наблюдателем контента, пассивной стороной, субъект превращается в непосредственного участника цифрового мира, который получил названия метавселенной.

Термин метавселенная образован от английского «meta» – трансцендентность и «verse» – мир. Под метавселенной понимают

коллективное виртуальное пространство, в котором объединяются физическая, дополненная и виртуальная реальность. Понимается метавселенная и в качестве парадигмы Интернета нового поколения, направленной на создание общего самоподдерживающегося виртуального социального пространства, характеризующегося признаками иммерсивности и многомерности[1]. Метавселенную понимают как суперэкосистему виртуальной реальности, сочетающую в себе функционирование различных технологий (искусственный интеллект, виртуальная и дополненная реальность, блокчейн, Интернет вещей и т. д.)[2]. Компоненты этой экосистемы взаимодействуют друг с другом, состоят в динамическом равновесии, создавая единый виртуальный мир.

Метавселенная отличается следующими признаками:

1) иммерсивность, то есть реалистичность созданного «машиной» виртуального пространства, в результате чего пользователи полностью погружаются в этот мир[3];

2) многомерность или гиперпространственно-временная реальность – в виртуальном мире временные ограничения, пространственные перемещения и другие аспекты не поддаются традиционным правилам;

3) устойчивость, под которой понимается основанность мира на определённых ценностях, наличие у него специфической структуры, что в совокупности позволяет ему противостоять угрозам как атак, так и в целом управления в централизованном порядке;

4) интероперабельность, позволяющая пользователям свободно перемещаться по так называемым субметавселенным[4];

5) масштабируемость, которая определяется исходя из большого количества одновременно задействованных пользователей, оптимального масштаба, типа аватара, уровня режимов взаимодействия пользователей, аватаров;

6) неоднородность, которая отражается в разнообразии субметавселенных, например, различные реализации виртуального пространства, интерфейсы, типы данных, режимы связи.

Отдельные элементы метавселенной присутствуют в играх, платформах для проведения конференций, виртуальных встреч. С учётом развития дистанционной занятости, удалённых форм получения

[1] Yuntao W., Zhou S., Ning Z., Dongxiao L., Rui X., Hao L. T., Xuemin S. A Survey on Metaverse: Fundamentals, Security, and Privacy. 2022. 23 p. DOI:10.36227/techrxiv.19255058.v1.

[2] Zhao R., Zhang Y., Zhu Y., Lan R., Hua Z. Metaverse: Security and Privacy Concerns // Journal of Latex Class Files. 2022. Vol. 14. № 8. Pp. 1–7.

[3] Dionisio J. D. N., Burns W. G., Gilbert R. 3D virtual worlds and the metaverse: Current status and future possibilities // ACM Computing Surveys (CSUR). 2013. Vol. 45. № 3. Pp. 1–38. DOI 10.1145/2480741.24807518.

[4] Lee L.-H., Braud T., Zhou P., Wang L., Xu D., Lin Z., Kumar A., Bermejo C., Hui P. All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda // arXiv preprint arXiv:2110.05352, 2021.

образования, метавселенная выводит на новый уровень такие отношения благодаря различным цифровым продуктам (например, Areena Virtual Space, Virbela, Project Starline, Azure и др.). Будь то научные конференции, семинарские занятия, рабочие совещания, по сравнению с известными площадками (Яндекс-мост, Zoom и т. п.) мероприятия, проводимые в метавселенной, способствуют большей вовлечённости участников, улучшению коммуникации, зрелищности, более позитивному впечатлению и другим положительным моментам. Это уже не просто игры в виртуальной реальности, а общение, отдельная цифровая вселенная, особенно при создании новых и объединении существующих платформ.

Среди перспективных направлений, где может быть использована технология метавселенной, следует отметить такие, как:

1) Организация труда, служебных отношений, политических институтов. Работникам предоставят возможности для выбора виртуального рабочего пространства, что может значительно повысить производительность труда. При этом сокращаются расходы на эксплуатацию рабочих помещений. Напрмиер, Барбадос является первым государством, которое открыло своё посольство в метавселенной.

2) Доступность социальной сферы. Метавселенная предоставляет возможности для лиц вне зависимости от места жительства, состояния здоровья получать образование, знакомиться с произведениями искусства, культурным наследием, посещать концерты, путешествовать и т. д.

3) Коммуникация. Сегодня зарождается новый тип коммуникации в отдельном цифровом мире. Кроме того, возможности 3D-сканирования объектов могут создавать аватаров, похожих на самих субъектов. Такие аватары будут копировать жесты, движения, мимику;

4) Коммерция. Появление новых видов товаров, услуг, профессий, развитие новых форм электронной коммерции, цифровых активов – такой процесс будет похожим на скачок в хозяйственных отношениях, который произошёл при зарождении Интернета.

Однако в данной работе хотелось бы подробнее остановиться на сфере образования.

Среди очевидных возможностей, которые предоставляет метавселенная в этой области, следует указать на развитие дистанционного обучения. Полное погружение в практические, семинарские занятия, когда действия, мимика, жесты в реальном мире влияют на содержание виртуального, вовлечённость в лекции, участие в виде аватара в научных конференциях – всё это способствует более активному эмоциональному отклику, формированию больших познавательных ответов, нежели в привычно применяемых в обучении в период пандемии коронавирусной инфекции технологиях. Так, запланированные в Zoom занятия заканчиваются, тогда как метавселенная существует всегда, позволяя создавать новые социальные связи со сверстниками, развиваться в

любое время, проходя обучение и получая новые знания альтернативными способами.

Однако возможности метавселенной более обширны. Так, Китайским университетом Гонконга в Шэньчжене была создана метавселенная кампуса, которую открывает Университет Таммасат в Таиланде. Это позволяет наглядно изучать историю, архитектуру, друге науки. При обучении пилотов уже достаточно давно применяются авиатренажёры, авиасимуляторы. Метавселенная позволит подобным образом обучать различной деятельности, например, в области сельского хозяйства, медицины. Это касается и отработки действий, реакций, навыков в чрезвычайных ситуациях. Помимо студентов, доступ к мета-кампусу получают различные представители публичного, частного сектора. В результате знания распространяются среди широкого круга лиц, создаётся среда для сотрудничества.

Таким образом, среди положительных явлений метавселенной в области образования можно отметить следующие:

1) Демократизация образования. Студенты, заходя в виртуальный мир, получают определённую свободу для общения со сверстниками, преподавателями, тьюторами, кураторами, консультантами и другими лицами в непринуждённой, психологически приятной обстановке. Также пространство метавселенной открыто для исследований, учёбы за счёт выделения библиотек и учебных блоков. Такой виртуальный мир может объединять людей независимо от физической удалённости, материального положения, ограничений в здоровье, стигм.

2) Развитие профессиональных навыков. В условиях метавселенной расширяются возможности формирования эмпирического опыта, после чего совершение ошибок в реальной профессиональной деятельности сокращается. Отработка различных вариантов посадок на самолете, многообразие дизайнерских решений, пожаротушение, хирургические операции, осмотр места происшествия и проведение иных следственных действий и т. д. – в таких процессах увеличивается вовлечённость учащихся, их уверенность в своих действиях, улучшаются практические навыки;

3) Развитие soft skills. Учитывая возможности коммуникации в метавселенной, у обучающихся формируются навыки взаимодействия в различных ситуациях, как в комфортной среде, так и в трудных беседах. В частности, можно симулировать беседы со «сложными» клиентами, формировать эмоциональный интеллект путём буквальной постановки себя на место другого человека, погружения в конфликтные ситуации. Лидерство, умение слушать, сочувствие, готовность к внештатным ситуациям, стрессоустойчивость – всё это можно формировать в безопасности путём погружения в виртуальный мир;

4) Развитие инклюзивного образования. Трудности организации инклюзивного образования становятся преодолимы в метавселенной. Обучающиеся с особенностями

здоровья, например, расстройством аутистического спектра, другими проблемами социального взаимодействия, могут улучшить своим навыки, посещая различные места, осуществляя там деятельность. При этом, у таких обучающихся может снижаться тревожность, беспокойство. Если привести в пример паллиативных больных, которые зачастую могут не иметь возможности даже выйти из больничной палаты, то мир метавселенной будет значительно увеличивать для них качество жизни. Они могут заниматься спортом с друзьями, путешествовать, и, конечно, получать образование;

5) Оптимизация учебного процесса посредством анализа данных об успеваемости, поведении обучающихся, прогрессе, вовлечённости, внимании.

Всё это оказывается верным и для юридического образования. Более того, рассматриваемая технология может позволить разрешить ряд традиционных проблем в этой сфере, в частности, обеспечить возможность действительной тренировки практических навыков (в части юридического консультирования, отстаивания позиции в суде, проведении расследования и т. д.), достичь междисциплинарности в учебном процессе.

Положительным моментом вовлечения технологий метавселенной в юриспруденцию является то, что наука юриспруденции будет более увлекательной для студентов. Отметим, что в настоящее время уже существует несколько курсов, на которых студенты учатся применять различные нормативные акты в условиях метавселенной.

Однако, как и в любой технологии, в метавселенной есть отдельные риски. Среди проблем, возникающих в сфере образования, следует обозначить:

1) Угрозы традиционной социализации, которая может потерпеть урон вследствие неограниченных ресурсов метавселенной. Особенно такая тенденция поглощения реального времени опасна для несовершеннолетних, и в целом для лиц, получающих образование. Школы, колледжи, университеты, иные образовательные учреждения – все они способствуют не только распространению знаний, обучению, но и формированию навыков социального общежития. Эта традиционная социальная жизнь может быть утрачена ввиду преобладания жизни виртуальной. Считаем, что в таком случае возможно введение ограничений, регламентирующих использование ресурсов метавселенной детьми. Неограниченная альтернативная реальность способна оказывать воздействие на сознание, прибегая к манипуляциям. Безусловно, ответственность за безопасность детей в этом случае должны нести родители (законные представители) либо иные лица, которые временно отвечают за вверенных несовершеннолетних (учителя, воспитатели дошкольных учреждений, учреждений дополнительного образования, вожатые и т. п.).

2) Угрозы конфиденциальности. В настоящее время создаются или

совершенствуются периферические устройства для подключения: очки, линзы, шлемы, наушники, перчатки, датчики, костюмы для сканирования движений и передачи их в виртуальное пространство. Эти устройства накапливают огромные массивы данных о пользователях. Эти данные многообразны, а возможности, связанные с несанкционированным получением персональной информации, постоянно развиваются. Управление массивными потоками данных, крупномасштабные объёмы профилирования пользователей, ошибки в алгоритмах искусственного интеллекта – всё это может возникать и в метавселенной, но в гораздо больших масштабах, нежели есть сейчас. Даже сами персональные данные в условиях метавселенной могут иметь более детализированный характер, распространяться более активно и широко, что само по себе создаёт новые угрозы для их неправомерного использования. Может иметь место отслеживание движений, мимики пользователей, их окружающего пространства, эмоциональных реакций, нейронных импульсов и т. д.[5] В целом, в эпоху метавселенной будут возникать новые данные в результате разработки современного оборудования и учёта ранее не собираемых показателей (например, движений глаз, мимики).

В связи с возрастающим использованием устройств в процессе обучения могут возникать вопросы об излишнем сборе и агрегировании персональных данных обучающихся. Закон о персональных данных устанавливает ограничение целей, минимизацию сбора данных показателей, последующее уничтожение их после использования, институт согласия, отвечающий признакам конкретности, предметности, информированности, сознательности. Однако возможны проблемы, связанные с осознанностью и информированностью обработки персональных данных в связи с внедрением в обучение метавселенной, необходимостью получения согласия законных представителей, если обучающийся является несовершеннолетним. Возможна кража персональных данных, в результате чего будут возникать проблемы при идентификации обучающихся во время проведения контрольных мероприятий или обычных занятий.

Ряд указанных проблем может быть решён посредством реформирования правовых режимов данных, в частности расширения института обезличивания по субъектному составу, выделение анонимизированных данных, на которых не распространялся бы правовой режим персональных данных, закрепление возможности получения согласие на несколько целей при обработке персональных данных.

3) Наконец, важной проблемой является цифровая грамотность как преподавателей, так и обучающихся. Зачастую проблемы в обучении студентов-юристов возникают даже на

[5] Falchuk B., Loeb S., Neff R. The social metaverse: Battle for privacy // IEEE Technology and Society Magazine. 2018. Vol. 37. № 2. Pp. 52–61.

этапе базовых курсов по информационном технологиям в профессиональной деятельности. Тем более, возможны проблемы, касающиеся активного применения технологий метавселенной со стороны как преподавателей, так и студентов. Решение данного вопроса видится в дополнительных курсах, посвящённых обучению субъектов образовательной деятельности использованию рассматриваемой технологии.

Считаем, что несмотря на все свои риски, технология метавселенной может поднять образование на кардинально более высокий уровень качества и общедоступности, что позволит выпускать настоящих профессионалов, готовых почти к любым трудностям практической деятельности.

Список литературы

1. Falchuk B., Loeb S., Neff R. The social metaverse: Battle for privacy // IEEE Technology and Society Magazine. 2018. Vol. 37. № 2. Pp. 52–61.

2. Dionisio J. D. N., Burns W. G., Gilbert R. 3D virtual worlds and the metaverse: Current status and future possibilities // ACM Computing Surveys (CSUR). 2013. Vol. 45. № 3. Pp. 1–38. DOI 10.1145/2480741.2480751

3. Lee L.-H., Braud T., Zhou P., Wang L., Xu D., Lin Z., Kumar A., Bermejo C., Hui P. All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda // arXiv preprint arXiv:2110.05352, 2021.

4. Zhao R., Zhang Y., Zhu Y., Lan R., Hua Z. Metaverse: Security and Privacy Concerns // Journal of Latex Class Files. 2022. Vol. 14. № 8. Pp. 1–7.

5. Yuntao W., Zhou S., Ning Z., Dongxiao L., Rui X., Hao L. T., Xuemin S. A Survey on Metaverse: Fundamentals, Security, and Privacy. 2022. 23 p. DOI:10.36227/techrxiv.19255058.v1.

Eleonora I. Leskina
PhD (Law), Associate Professor of the
Department of Information Law and Digital Technologies
Saratov State Law Academy
(Saratov, Russia)
elli-m@mail.ru

METAVERSE TECHNOLOGIES IN EDUCATION

Abstract. The development of technology affects many areas of social relations and the field of education is no exception. The Metaverse as a special, new digital society that unites many users provides great opportunities for healthcare, labor relations, e-commerce, education and other areas. The article is aimed at defining the concept, essence, features, principles of the metauniverse, analysis of the directions for the introduction of related technologies in various fields, especially in the field of education.

Keywords: information society; digitalization; end-to-end technologies; metaverse; data; education; Personal Information; principles of the metaverse.

УДК 343.98

Можаева Людмила Евгеньевна
Старший преподаватель кафедры теории и истории государства и права,
Гомельский государственный университет имени Франциска Скорины
(г. Гомель, Республика Беларусь)
luda666@yandex.ru

Савченко Дмитрий Геннадьевич
Студент 4 курса юридического факультета,
Гомельский государственный университет имени Франциска Скорины
(г. Гомель, Республика Беларусь)
savchenko_dmitryi@mail.ru

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. В статье рассматривается оперативно-розыскная деятельность, как основной инструмент выявления наиболее опасных и латентных преступлений, совершаемых посредством использования сети интернет, а также актуальные вопросы осуществления рассматриваемого вида деятельности. Авторами предлагаются новации правового и организационно-тактического характера.

Ключевые слова: оперативно-розыскная деятельность, информация, технологии, безопасность, IT-технологии.

Для цитирования:
Можаева Л. Е., Савченко Д. Г. Информационные технологии в оперативно-розыскной деятельности // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 138–142.

Преступность была и остается основной причиной большинства негативных явлений, имеющих место в общественной жизни, борьба с которой должна быть рациональной и эффективной. Согласно официальным статистическим данным[1] количественные показатели преступности неоднозначны, а качественные сигнализируют о стабильном росте преступлений в сфере IT-технологий[2].

[1] Правосудие и правонарушения // Национальный статистический комитет Республики Беларусь [Электронный ресурс]. 2022, 29 сентября. URL: http://dataportal.belstat.gov.by/Indicators/Preview?key=190785/ (дата обращения: 30.09.2022).

[2] Наривончик Д. Каждое четвертое преступление в Беларуси совершается в сфере информационных технологий // Экономическая газета [Электронный ресурс]. 2021, 14 мая. URL: https://neg.by/novosti/otkrytj/kazhdoe-chetvertoe-prestuplenie-v-belarusi-

Стоит отметить заинтересованность Республики Беларусь в обеспечении информационной безопасности, что отражено в соответствующей нормотворческой[3] и практикоприменительной деятельности, однако без осуществления негласной деятельности специальных подразделений государственных правоохранительных органов данные меры представляются малоэффективными. Любой вид преступлений целесообразно выявлять в среде его совершения. Как было упомянуто нами ранее, в настоящее время многие преступления перешли в интернет-пространство.

Так, например, дачу и получение взятки можно осуществить посредством перевода денежных средств, криптовалюты на электронный кошелек должностного лица. Ситуация в сфере незаконного оборота наркотиков и психотропов аналогична.

Подтверждением может служить следующая информация: «Доля наркотиков, продаваемых в Беларуси через интернет, в последние два года выросла до 95%. Большая часть наркотиков поступает в страну из России, сообщил временно исполняющий обязанности по должности заместителя начальника Главного управления по наркоконтролю и противодействию торговле людьми МВД Сергей Мелещик».

«Если в период 2016-2017 годов через виртуальное пространство осуществлялось порядка 60% сбыта наркотиков, то в 2021-2022 годах данный показатель вырос до 95%, – сказал Мелещик на пресс-конференции 11 августа. Он констатировал, что это обстоятельство увеличивает латентность таких преступлений»[4,5].

В связи с этим необходимо надлежащее упорядочение деятельности оперативных подразделений посредством оценки складывающейся оперативной обстановки, выстраивания эффективного взаимодействия сотрудников оперативных подразделений различных ведомств, избрание и планирование наиболее эффективных оперативно-розыскных мероприятий (далее – ОРМ) в рамках каждого конкретного факта.

---

sovershaetsya-v-sfere-informacionnyh-tehnologij/ (дата обращения: 01.10.2022).

[3] О Концепции информационной безопасности Республики Беларусь: Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. №1 // Национальный правовой интернет-портал Республики Беларусь pravo.by [Электронный ресурс]. URL: https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf/ (дата обращения: 01.10.2022).

[4] МВД: через интернет в Беларусь продается уже 95% всех наркотиков // Смартпресс [Электронный ресурс]. 2022, 11 августа.. URL: https://smartpress.by/news/27414/ (дата обращения: 03.10.2022).

[5] Наривончик Д. Каждое четвертое преступление в Беларуси совершается в сфере информационных технологий // Экономическая газета [Электронный ресурс]. 2021, 14 мая. URL: https://neg.by/novosti/otkrytj/kazhdoe-chetvertoe-prestuplenie-v-belarusi-sovershaetsya-v-sfere-informacionnyh-tehnologij/ (дата обращения: 01.10.2022).

Изучив национальное законодательство, структуру и полномочия государственных правоохранительных органов мы обратили внимание на тот факт, что вопреки существованию Департамента финансового мониторинга Комитета государственного контроля Республики Беларусь, относящего к субъектам ОРД, соответствующего законодательства, регулирующего вопросы деятельности названного субъекта, прямое определение понятия «мониторинг» либо «финансовый мониторинг» отсутствует.

В целях совершенствования законодательства, парвоприменительной практики, а также тактики и методики осуществления ОРД считаем целесообразным рассмотреть и в последующем внедрить в Закон Республики Беларусь от 15 июля 2015 г. № 307–З «Об оперативно-розыскной деятельности» положения, предложенные А. В. Кутузовым[6], С. А. Войтиховичем[7] касательно понятия «оперативно-розыскной мониторинг» с авторскими изменениями.

А именно, расширить перечень ОРМ и предусмотреть такое ОРМ как «Мониторинг» и изложить статью в следующей редакции:

«Мониторинг представляет собой систематическую деятельность по сбору, обобщению, изучению, анализу оперативно значимой информации посредством наблюдения за протекающими процессами в сети интернет, на торговых площадках, интернет-ресурсах, в средствах массовой информации в целях получения сведений, необходимых для выполнения задач оперативно-розыскной деятельности.

Мониторинг проводится по решению должностного лица органа, осуществляющего оперативно-розыскную деятельность.

При необходимости фиксации, копирования сведений, компьютерной информации, полученных в результате мониторинга, данные должны быть отражены в соответствующих оперативно-служебных документах.

Фиксация, копирование сведений, компьютерной информации, полученных в результате мониторинга не являются сбором образцов.».

Предложенная конструкция, на наш взгляд, целесообразна по причине того, что уже имеющиеся ОРМ в основном рассчитаны на проведение при наличии оперативно значимой информации, то есть при наличии объекта оперативного интереса либо события, а мониторинг позволяет

[6] Кутузов А. В. Оперативно-розыскной мониторинг сети Интернет как элемент противодействия преступлениям экстремистской направленности // Вестник Костромского государственного университета. 2020. Т. 26. № 2. С. 235-241.

[7] Войтихович В. А. Оперативно-розыскной мониторинг – элемент организации работы подразделений по борьбе с экономическими преступлениями органов внутренних дел // Проблемы оперативно-розыскного обеспечения уголовного процесса : тез. докл. респ. науч.-практ. конф. памяти первого начальника кафедры оператив.-розыскной деятельности фак. милиции Акад. МВД Респ. Беларусь Л. Н. Калинковича (Минск, 7 июня 2019 г.) / учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь»; редкол.: А. Н. Тукало (отв. ред.) [и др.]. Минск: Академия МВД, 2019. С. 21–23.

регламентировать деятельность по поиску информации о событии или лице, на основании которой будет приниматься решение о проведении иных ОРМ.

Например, по установлению лица, разместившего информацию деструктивного характера в открытом доступе либо лиц, организовавших и курирующих деятельность интернет-магазина по продаже психоативных веществ, после обнаружения такой информации или соответствующего интернет-магазина в процессе мониторинга.

Также лица, осуществляющие противоправную деятельность, зачастую осведомлены об основах проведения ОРМ в их отношении.

Например: наличие заявления от лица, обнаружение таких фактов в результате проверочных мероприятий, что позволяет им прогнозировать дальнейшие действия правоохранительных органов по их выявлению, поиску и собиранию доказательственной базы, последующему задержанию.

В результате существования и осуществления на практике мониторинга, лицам, ведущим противоправный образ жизни, будет сложнее, если вообще возможно выстроить логически обоснованную цепочку действий сотрудников оперативных подразделений, так как мониторинг подразумевает постоянную деятельность по изучению оперативной обстановки, в том числе, в сети интернет.

Резюмируя вышеизложенное:

1. ОРД продолжает оставаться наиболее эффективным инструментом в борьбе с преступностью, в особенности латентной.

2. Предложенная правовая конструкция позволит наиболее эффективно и масштабно предупреждать преступные посягательства, а также даст импульс для дальнейшего совершенствования законодательной базы, регулирующей осуществление ОРД, которая, на наш взгляд, является в значительной степени консервативной.

3. Считаем, что осуществление мониторинга позволит эффективно и своевременно собирать, обрабатывать и реализовывать оперативно значимую информацию, а также упреждать предпринимаемые попытки сокрытия следов преступлений, приготовления к их совершению, в особенности это актуально в отношении преступлений террористической, экстремисткой направленности, преступлений, связанных с незаконным оборотом наркотических средств, торговлей оружием и людьми.

Список литературы

1. Войтихович В. А. Оперативно-розыскной мониторинг – элемент организации работы подразделений по борьбе с экономическими преступлениями органов внутренних дел // Проблемы оперативно-розыскного обеспечения уголовного процесса : тез. докл. респ. науч.-практ. конф. памяти первого начальника кафедры оператив.-розыскной деятельности фак. милиции Акад. МВД Респ. Беларусь Л. Н. Калинковича (Минск, 7 июня 2019 г.) / учреждение

образования «Акад. М-ва внутр. дел Респ. Беларусь»; редкол.: А. Н. Тукало (отв. ред.) [и др.]. Минск: Академия МВД, 2019. С. 21–23.

2. Кутузов А. В. Оперативно-розыскной мониторинг сети Интернет как элемент противодействия преступлениям экстремистской направленности // Вестник Костромского государственного университета. 2020. Т. 26. № 2. С. 235–241.

Lyudmila E. Mozhayeva
Senior Lecturer of the Department of Theory and History of State and Law,
Gomel State University named after Francisk Skorina
(Gomel, Republic of Belarus)
luda666@yandex.ru

Dmitryi H. Savchenko
Student,
Gomel State University named after Francisk Skorina
(Gomel, Republic of Belarus)
savchenko_dmitryi@mail.ru

IT-TECHNOLOGIES IN THE OPERATIONAL SEARCH ACTIVITIES

Abstract. The article discusses: operational-search activity as the main tool for identifying the most dangerous and latent crimes committed through the use of the Internet, as well as topical issues of the implementation of the type of activity under consideration. The author proposes innovations of a legal, organizational and tactical nature.

Keywords: Operative-search activity, information, technologies, security, IT-technologies.

УДК 34.096

Можаева Людмила Евгеньевна
Старший преподаватель кафедры теории и истории государства и права,
Гомельский государственный университет имени Франциска Скорины
(г. Гомель, Республика Беларусь)
luda666@yandex.ru

Савченко Дмитрий Геннадьевич
Студент 4 курса юридического факультета,
Гомельский государственный университет имени Франциска Скорины
(г. Гомель, Республика Беларусь)
savchenko_dmitryi@mail.ru

ПРАВОПРИМЕНИТЕЛЬНЫЕ ПРОБЛЕМЫ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. Тенденции современного общества вынуждают переносить многие виды правоотношений в сферу информационных технологий, что требует принятия соответствующих мер по защите соответствующих данных. Одной из проблем эффективной защиты персональных данных является механизм правового регулирования процесса трансграничной передачи данных оператором, чему и посвящено данное исследование.

Ключевые слова: персональные данные, безопасность, передача, проблемы, механизм.

Для цитирования:
Можаева Л. Е., Савченко Д. Г. Правоприменительные проблемы трансграничной передачи персональных данных // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 143–149.

27 мая 2021 года был принят Закон Республики Беларусь № 99–З «О защите персональных данных»[1] (далее – Закон). Данный нормативный правовой акт, будучи новым, породил вопросы касательно его теоретического восприятия в соотношении с практической реализацией, в том числе в отношении трансграничной передачи данных.

В соответствии со ст. 1 Закона под трансграничной передачей данных понимается передача персональных данных на территорию иностранного государства.

[1] О защите персональных данных: Закон Респ. Беларусь от 7 мая 2021 г. № 99–З // Национальный правовой интернет-портал Республики Беларусь pravo.by [Электронный ресурс]. URL: https://pravo.by/upload/docs/op/H12100099_1620939600.pdf (дата обращения: 01.12.2022).

На наш взгляд, процесс передачи персональных данных, в особенности, если он приобретает трансграничный характер, является важнейшим с точки зрения как нормативного закрепления, так и практики применения, исходя из того, что вследствие указанного процесса затрагиваются права граждан, гарантируемые Конституцией. Несмотря на отсутствие комментариев по корректной реализации положений Закона, государственные органы, предприятия оперативно зафиксировали тождественные положения касательно политики обработки персональных данных сотрудников, клиентов:

1. Положение о порядке обработки и защите персональных данных в аппарате управления ГПО «Белэнерго» (утверждено Приказом ГПО «Белэнерго» от 3 декабря 2021 г. № 309)[2];

2. Постановление Министерства здравоохранения Республики Беларусь от 7 июня 2021 г. № 74 «О формах и порядке дачи и отзыва согласия на внесение и обработку персональных данных пациента»[3];

3. Политика обработки персональных данных в государственном предприятии «Минсктранс» (утверждена Приказом генерального директора государственного предприятия «Минсктранс» от 12 ноября 2021 г. № 786)[4].

Из содержания ст. 9 Закона можно предположить, что до осуществления передачи данных уполномоченный субъект передачи информации убеждается в том, что на территории государства, которому направляется информация, обеспечивается надлежащий уровень защиты прав субъектов персональных данных.

На наш взгляд, как у уполномоченного субъекта передачи информации (оператора), так и у лица, чьи данные подлежат передаче, могут возникнуть вопросы касательно определения «обеспечение надлежащего уровня защиты», а именно критериев «надлежащего

[2] Положение «О порядке обработки и защите персональных данных в аппарате управления ГПО “Белэнерго”», утв. приказом ГПО «Белэнерго» от 03.12.2021 № 309 // ГПО «Белэнерго» [Электронный ресурс]. URL: https://www.belenergo.by/upload/doc/%D0%9F%D1%80_309_%D0%9F%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B8%D0%B7%D0%BC.pdf (дата обращения: 22.12.2022).

[3] О формах и порядке дачи отзыва согласия на внесение и обработку персональных данных пациента: Постановление Министерства здравоохранения Респ. Беларусь от 07.06.2021 № 74 // Национальный правовой интернет-портал Республики Беларусь pravo.by [Электронный ресурс]. URL: http://minzdrav.gov.by/upload/dadvfiles/law/%D0%BF%D0%BE%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%9C%D0%97_2021_74.pdf (дата обращения: 23.12.2022).

[4] Политика обработки персональных данных в государственном предприятии «Минсктранс», утв. приказом генерального директора государственного предприятия «Минсктранс» от 12.11.2021 № 786 // Государственное предприятие «Минсктранс» [Электронный ресурс]. URL: https://minsktrans.by/wp-content/uploads/2021/11/politika-obrabotki-personalnyh-dannyh-v-gosudarstvennom-predpriyatii-minsktrans.pdf (дата обращения: 24.12.2022).

уровня». Законодательство Российской Федерации в области защиты персональных данных содержит термин «адекватная защита». В данном случае, на наш взгляд, отсутствует какая-либо необходимость разграничения понятий в виду предельной тождественности их смыслового наполнения.

В целом считаем, что наиболее универсальным критерием адекватности защиты или её надлежащим уровнем будет наличие соответствующего законодательства на территории государства, которому информация будет передана. Таким образом, возникает необходимость изучения со стороны должностных лиц оператора национального законодательства иностранного государства, наличия требований по обеспечению безопасности информации, уполномоченного государственного органа в сфере защиты информации. Вполне вероятно, что критерии определения «надлежащего уровня» могут определяться в международных соглашениях, но на данный момент упоминание об этом отсутствует.

Изучая мировой опыт в области трансграничной передачи данных, мы обратили внимание на некоторые положения существующей Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, принятой в Страсбурге 28 января 1981 г. (далее – Конвенция, Конвенция 108)[5]. В Конвенции отмечается следующее:

«1. В отношении передачи через национальные границы с помощью каких бы то ни было средств персональных данных, подвергающихся автоматизированной обработке или собранных с целью их автоматизированной обработки, применяются нижеследующие положения.

2. Сторона не должна запрещать или обусловливать специальным разрешением трансграничные потоки персональных данных, идущие на территорию другой Стороны, с единственной целью защиты частной жизни.

3. Тем не менее, каждая Сторона вправе отступать от положений пункта 2:

a) в той степени, в какой ее внутреннее законодательство включает специальные правила в отношении определенных категорий персональных данных или автоматизированных баз персональных данных в силу характера этих данных или этих файлов, за исключением случаев, когда нормы другой Стороны предусматривают такую же защиту;

b) когда передача осуществляется с ее территории на территорию Государства, не являющегося Стороной настоящей Конвенции, через территорию другой Стороны, в целях недопущения такой передачи, которая позволит обойти

[5] О защите физических лиц при автоматизированной обработке персональных данных: Конвенция от 28.01.1981. № 108 // Электронный фонд правовой и нормативно-технической документации [Электронный ресурс]. URL: https://docs.cntd.ru/document/8318842 (дата обращения: 24.12.2022).

законодательство Стороны, упомянутой в начале данного пункта».

Принимая во внимание вышеприведённые нормы, считаем, что Конвенция 108 рассматривает передачу данных в качестве как минимум двустороннего процесса взаимного обмена данными, а Закон закрепляет «трансграничную передачу данных» в качестве однонаправленного процесса. Также можно сделать вывод о том, что информационный обмен, в соответствии с Конвенцией, стабилен ввиду того, что защита частной жизни не является, по общему правилу, основанием для прекращения либо отмены обмена данными.

Считаем необходимым обратить внимание на то, что законодательство, а именно ст. 9 Закона, разрешает оператору трансграничную передачу данных в случае, если на территории иностранного государства не обеспечен «надлежащий уровень» защиты прав субъектов персональных данных, когда:

– дано согласие субъекта персональных данных при условии, что субъект персональных данных проинформирован о рисках, возникающих в связи с отсутствием надлежащего уровня их защиты;

– персональные данные получены на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором;

– персональные данные могут быть получены любым лицом посредством направления запроса в случаях и порядке, предусмотренных законодательством;

– такая передача необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно;

– обработка персональных данных осуществляется в рамках исполнения международных договоров Республики Беларусь;

– такая передача осуществляется органом финансового мониторинга в целях принятия мер по предотвращению легализации доходов, полученных преступным путём, финансирования террористической деятельности и финансирования распространения оружия массового поражения в соответствии с законодательством;

– получено соответствующее разрешение уполномоченного органа по защите прав субъектов персональных данных.

Видимо, предусмотрев проблему трансграничной передачи данных в случае, если на территории иностранного государства не обеспечен «надлежащий уровень» защиты прав субъектов персональных данных, 15 ноября 2021 года был издан Приказ Национального центра защиты персональных данных № 14 «О трансграничной передаче данных»[6] (далее – Приказ), которым

[6] О трансграничной передаче персональных данных: Приказ Национального центра защиты персональных данных Респ. Беларусь от 15.11.2021 № 14 // Информационно-правовая система ЭТАЛОН-ONLINE [Электронный ресурс]. URL: https://etalonline.by/document/?regnum=U621E3030 (дата обращения: 25.12.2022).

определяется порядок выдачи разрешения на трансграничную передачу персональных данных, если на территории иностранного государства не обеспечивается надлежащий уровень защиты прав субъектов персональных данных.

Несмотря на то, что Приказ определяет указание в заявлении способов защиты прав субъектов персональных данных в случае их нарушения, представляется, что такая защита, после выбытия информации из Республики Беларусь, будет осуществляться по дипломатическим каналам.

В законодательстве Республики Беларусь также окончательно не отражён вопрос защиты персональных данных непосредственно в момент их трансграничной передачи, когда информация, на наш взгляд, является наиболее уязвимой.

Вероятно, что защиту информации посредством защиты канала связи обеспечит либо «оператор электросвязи» либо «оператор универсального обслуживания», в качестве которых Закон Республики Беларусь от 19 июля 2005 г. № 45–З «Об электросвязи»[7] определяет юридических лиц или индивидуальных предпринимателей, оказывающих услуги электросвязи на основании специального разрешения (лицензии) на деятельность в области связи, операторов электросвязи, которым предоставлено право на оказание универсальных услуг электросвязи.

Также примечательно определение «оператор информационной системы», содержащееся в Законе Республики Беларусь от 10 ноября 2008 г. № 455–З «Об информации, информатизации и защите информации»[8]: «субъект информационных отношений, осуществляющий эксплуатацию информационной системы и (или) оказывающий посредством ее информационные услуги».

Таким образом, оператор в данных случаях является звеном защиты передаваемых персональных данных, однако остаётся неясным, может ли один субъект совмещать в себе оператора электросвязи универсального обслуживания и оператора информационной системы, а изучение сфер действия рассмотренных Законов показывает отсутствие принципиальных отличий между общественными отношениями, действиями, в результате которых создастся необходимость использования того или иного Закона.

В особенности это касается Закона Республики Беларусь от 27 мая 2021 г. № 99–З «О защите персональных данных», где смешиваются гражданские, публичные, уголовно-процессуальные

[7] Об электросвязи: Закон Респ. Беларусь от 19.07.2005 № 45–З // Национальный правовой интернет-портал Республики Беларусь pravo.by [Электронный ресурс]. URL: https://pravo.by/document/?guid=3871&p0=H10500045 (дата обращения: 26.12.2022).

[8] Об информации, информатизации и защите информации: Закон Респ. Беларусь от 10.11.2008 № 455–З // Национальный правовой интернет-портал Республики Беларусь pravo.by [Электронный ресурс]. URL: https://pravo.by/document/?guid=3871&p0=h10800455 (дата обращения: 27.12.2022).

отношения, а также отношения, возникающие при осуществлении оперативно-розыскной деятельности (далее – ОРД), так как прямого указания на то, что данные правоотношения находятся вне сферы действия рассматриваемого Закона, нет.

Однако, такую позицию по отношению к информации, передаваемой в рамках ОРД, считаем нецелесообразной по ряду причин:

– обязанность предоставления любой запрашиваемой информации органам, осуществляющим ОРД, уже закреплено отраслевым законодательством;

– сотрудники таких органов используют запрашиваемую информацию исключительно в рамках исполнения возложенных на низ задач, а информацию, к ней не относящуюся обязуются уничтожать / не использовать в иных целях;

– в рамках осуществления ОРД на территории иностранного государства, получение и передача оперативно значимой информации, содержащей персональные данные, осуществляется по закрытым каналам связи на основании уже существующих международных договоров, межведомственных соглашений;

– должностные лица несут персональную ответственность за неправомерное распространение личных данных физических лиц, полученных при осуществлении ОРД.

Исходя из факта существования отлаженного механизма обмена данными при осуществлении ОРД, распространение нового, недостаточно апробированного Закона, на данную сферу отношений считаем преждевременным и угрожающим национальной безопасности ввиду отсутствия окончательного толкования нового Закона, его достаточной апробации. Тем не менее, новации в законодательстве позволяют переосмыслить понятие защищённости информации в современном мире и выводят гражданско-правовые, семейные, некоторые отношения публично-правового характера на качественно новый уровень правовой регламентации и реализации.

Lyudmila E. Mozhayeva
Senior Lecturer at the Department of Theory and History of State and Law,
Francisk Skorina Gomel State University
(Gomel, Republic of Belarus)
luda666@yandex.ru

Dmitryi H. Savchenko
Student,
Francisk Skorina Gomel State University
(Gomel, Republic of Belarus)
savchenko_dmitryi@mail.ru

LAW ENFORCEMENT ISSUES OF CROSS-BORDER TRANSFER OF PERSONAL DATA

Abstract. The trends of modern society force the transfer of many types of legal relations to the field of information technology, which requires the adoption of appropriate measures to protect the relevant data. One of the problems of effective protection of personal data is the mechanism of legal regulation of the process of cross-border data transfer by the operator, to which this study is devoted.

Keywords: personal data, security, transfer, problems, mechanism.

УДК 347.6

Одегова Людмила Юрьевна
Кандидат юридических наук, и. о. заведующего кафедры
конституционного и международного права,
Донецкий национальный университет
(г. Донецк, Российская Федерация)
milaodegova17@mail.ru

Соловьёва Юлия Александровна
Кандидат юридических наук, доцент кафедры
конституционного и международного права,
Донецкий национальный университет
(г. Донецк, Российская Федерация)
soloveva5585@bk.ru

СУРРОГАТНОЕ МАТЕРИНСТВО В МЕЖДУНАРОДНОМ И НАЦИОНАЛЬНОМ ПРАВЕ

Аннотация. В статье дан краткий обзор международного и национального законодательства, регулирующего вопросы применения такого метода вспомогательных репродуктивных технологий, как суррогатное материнство; установлено, что в Российской Федерации нормативно закреплено право на применение гестационного суррогатного материнства, которое может быть как альтруистическим, так и коммерческим; подвергнута критике недостаточная правовая регламентация данного института в национальном праве.

Ключевые слова: вспомогательные репродуктивные технологии; суррогатное материнства; коммерческое суррогатное материнство; традиционное суррогатное материнство; гестационное суррогатное материнство; существенные условия договора о суррогатном материнстве.

Для цитирования:
Одегова Л. Ю., Соловьёва Ю. А. Суррогатное материнство в международном и национальном праве // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 150–155.

Сегодня во всем мире, наблюдается общее снижение уровня рождаемости, связанное, среди прочего, с проблемой бесплодия. Так, согласно официальным данным Всемирной организации здравоохранения, это касается от 48 миллионов пар до 186 миллионов

человек в мире[1]. Одним из способов «решения данной проблемы» является применение вспомогательных репродуктивных технологий, таких как экстракорпоральное оплодотворение (далее – ЭКО) и суррогатное материнство.

Согласно п. 5 ст. 55 Федерального закона РФ «Об основах охраны здоровья граждан в Российской Федерации»[2] суррогатное материнство представляет собой вспомогательную репродуктивную технологию, при которой вынашивание и рождение ребёнка в соответствии с договором о суррогатном материнстве, заключаемом между суррогатной матерью (женщиной, вынашивающей плод после переноса донорского эмбриона) и потенциальными родителями, половые клетки которых использовались для оплодотворения, для которых вынашивание и рождение ребёнка невозможны по медицинским показаниям и которые состоят в браке между собой, либо одинокой женщиной, половые клетки которой использовались для оплодотворения и для которой вынашивание и рождение ребёнка невозможны по медицинским показаниям. Кроме того, согласно п. 10 указанной статьи суррогатная мать не может одновременно быть донором яйцеклетки.

Таким образом, приведённая норма свидетельствует о том, что в РФ такой метод вспомогательной репродуктивной технологии как традиционное суррогатное материнство (когда ребёнок имеет связь с суррогатной материю вследствие использования её половых клеток) запрещён. Разрешённым методом является лишь гестационное суррогатное материнство. В связи с чем, присоединяясь к мнению В. В. Самойловой, считаем возможным суррогатное материнство в РФ определять как вспомогательную репродуктивную технологию, с помощью которого женщина на основании взаимной договоренности с лицами (лицом), обратившимися к ней за предоставлением указанной услуги, проходит процедуру имплантации эмбриона, созданного в результате ЭКО, и вынашивает ребёнка с целью родить и передать его указанным лицам (указанному лицу)[3].

Важно отметить, что проблема допустимости суррогатного материнства постоянно дискутируется, что связано, среди прочего, с её коммерциализацией. Так, например, Европейский Парламент в Годовом отчёте о правах человека и демократии в мире за 2014 год, указал, что он осуждает практику суррогатного материнства, которое подрывает

[1] Бесплодие // Оф. сайт Всемирной организации здравоохранения [Электронный ресурс]. URL: https://www.who.int/ru/news-room/fact-sheets/detail/infertility (дата обращения: 26.01.2023).

[2] Об основах охраны здоровья граждан в Российской Федерации (с изм. и доп., вступ. в силу с 11.01.2023): Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 28.12.2022) // Информационно-правовой портал «ГАРАНТ» [Электронный ресур]. URL: https://base.garant.ru/12191967/0dacf58504c4847f1a1635db72279562/ (дата обращения: 26.01.2023).

[3] Самойлова В. В. Суррогатное материнство как правовой институт // Теория и практика общественного развития. 2014. № 4. С. 234.

человеческое достоинство женщины, поскольку её тело и репродуктивные функции используют как товар, а также то, что гестационное суррогатное материнство предусматривает репродуктивную эксплуатацию и использование человеческого тела с целью получения финансовой или иной выгоды и должно быть запрещено[4]. В ст. 21 Конвенции по правам человека в биомедицине (Овьедо, 4 апреля 1997 года) ещё ранее был закреплён запрет на использование тела человека и его частей для извлечения финансовой выгоды (т. е. коммерческого суррогатного материнства)[5]. Судом Европейского Союза в 2013 году, в деле C-167/12 C. D. / S.T. и C-363/12 Z. / A Government Department and the Board of Management of a Community School было вынесено решение, что «…право Союза не предусматривает для суррогатных матерей право на оплачиваемый отпуск, эквивалентное отпуску по беременности и родам или отпуску в связи с усыновлением»[6].

Действительно, с точки зрения норм международного права коммерческое суррогатное материнство нарушает п. «а» ст. 2 Факультативного протокола 2000 г. к Конвенции о правах ребёнка, где закреплено, что торговля детьми представляет собой любой акт или сделку, посредством которых ребёнок передаётся любым лицом или любой группой лиц другому лицу или группе лиц за вознаграждение или любое иное возмещение[7]. Ст. 20 Декларации о социальных и правовых принципах, касающихся защиты и благополучия детей, особенно при передаче детей на воспитание и их усыновлении на национальном и международном уровнях также устанавливает, что усыновление не должно приводить к получению сторонами, принимающими участие в усыновлении, неоправданных финансовых выгод[8]. В связи с чем в

[4] Львофф Л. Суррогатное материнство. Вспомогательные репродуктивные технологии // Совет Европы. Блок биоэтики [Электронный ресурс]. URL: https://rm.coe.int/168070b6d9 (дата обращения: 26.01.2023).

[5] Конвенция о защите прав и достоинства человека в связи с применением достижений биологии и медицины: Конвенция о правах человека и биомедицине (Овьедо, 4 апреля 1997 года) // Совет Европы [Электронный ресур]. URL: https://rm.coe.int/168007d004 (дата обращения: 26.01.2023).

[6] Львофф Л. Суррогатное материнство. Вспомогательные репродуктивные технологии // Совет Европы. Блок биоэтики [Электронный ресурс]. URL: https://rm.coe.int/168070b6d9 (дата обращения: 26.01.2023).

[7] Факультативный протокол к Конвенции о правах ребёнка, касающийся торговли детьми, детской проституции и детской порнографии: Резолюция 54/263 Генеральной Ассамблеи ООН от 25 мая 2000 года // ООН. Конвенциии и соглашения [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/conventions/rightschild_protocol2.shtml (дата обращения: 26.01.2023).

[8] Декларация о социальных и правовых принципах, касающихся защиты и благополучия детей, особенно при передаче детей на воспитание и их усыновлении на национальном и международном уровнях: Резолюция 41/85 Генеральной Ассамблеи ООН от 3 декабря 1986 года // ООН. Конвенциии и соглашения [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/de

ряде государств мира коммерческое суррогатное материнство запрещено (Нидерланды, Португалия, Греция, Канада, Австралия).

В РФ суррогатное материнство может осуществляется как на возмездной, так и на безвозмездной основе. При этом по справедливому замечанию Данельян А. А. сложность правового регулирования суррогатного материнства в РФ заключается в том, что по сути услуги по оказанию суррогатного материнства напрямую зависят от частно-правовых отношений, отражённых в соответствующем гражданском договоре[9]. Кроме того, законодательство РФ не содержит перечня прав и обязанностей участников программы суррогатного материнства, не предусматривает ответственности за нарушения в сфере суррогатного материнства и пр.

Важно также отметить, что правовое регулирование по договору суррогатного материнства в РФ характеризуется приоритетом прав суррогатной матери, что, по нашему убеждению, является неоправданным. Так, согласно ч. 4 ст. 51 Семейного Кодекса РФ[10] и п. 5 ст. 16 Федерального закона «Об актах гражданского состояния»[11] при регистрации ребёнка, рождённого суррогатной матерью, необходимым является её согласие.

В отличие от подхода российского законодателя к обозначенному вопросу, Кодексом Республики Беларусь о браке и семье (ст. 52) закреплено, что «матерью ребёнка, рождённого суррогатной матерью, признаётся женщина, заключившая с суррогатной матерью договор суррогатного материнства. Отцом ребёнка, рождённого суррогатной матерью, признаётся супруг женщины, заключившей с суррогатной матерью договор суррогатного материнства»[12]. Кроме того, законодательством Республики Беларусь в Законе «О вспомогательных репродуктивных технологиях» от 7 января 2012 г. № 341-З[13] достаточно полно регламентирована процедура

clarations/childpri.shtml (дата обращения: 26.01.2023).

[9] Данельян А. А. Международно-правовые аспекты суррогатного материнства // Электронное сетевое издание «Международный правовой курьер» [Электронный ресурс]. URL: http://inter-legal.ru/mezhdunarodno-pravovye-aspekty-surrogatnogo-materinstva (дата обращения: 26.01.2023).

[10] Семейный кодекс Российской Федерации от 29.12.1995 № 223-ФЗ (ред. от 19.12.2022) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_8982/ (дата обращения: 26.01.2023).

[11] Об актах гражданского состояния: Федеральный закон от 15.11.1997 № 143-ФЗ (последняя редакция) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_16758/ (дата обращения: 26.01.2023).

[12] Кодекс Республики Беларусь о Браке и Семье от 9.07.1999 г. № 278-З // Kodeksy-by [Электронный ресурс]. URL: https://kodeksy-by.com/kodeks_rb_o_brake_i_semje.htm (дата обращения: 26.01.2023).

[13] О вспомогательных репродуктивных технологиях: Закон Республики Беларусь от 7 января 2012 г. № 341-З // Kodeksy-by [Электронный ресурс]. URL: https://kodeksy-by.com/zakon_rb_o_vspomogatel_nyh_reproduktivnyh_tehnologiyah.htm (дата обращения: 26.01.2023).

суррогатного материнства (закреплены порядок применения вспомогательных репродуктивных технологий, права доноров и реципиентов, условия и порядок суррогатного материнства, существенные условия договора суррогатного материнства и пр.), что, бесспорно, заслуживает внимания и одобрения.

Важно также отметить, что сегодня существенные отличия правопорядков разных государств привели к возникновению такого явления, как «репродуктивный туризм», когда граждане страны, где запрещено суррогатное материнство, направляются в те страны, где последнее разрешено. В связи с чем для предотвращения торговли детьми, их защиты от «попадания» в однополые пары, недопущения ситуация, когда дети становятся жертвами преступлений (например, продажа на органы) Федеральным законом от 19 декабря 2022 г. № 538-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»[14], среди прочего закреплено, что иностранцам и лицам без гражданства запрещено использовать институт суррогатного материнства в России.

Таким образом, проведённое исследование позволяет сделать ряд выводов. Во-первых, на международном уровне практика коммерческого суррогатного материнства осуждается в силу того, что последнее нарушает международные нормы о запрете на торговлю детьми. Во-вторых, в РФ разрешённым методом вспомогательных репродуктивных технологий является гестационное суррогатное материнство, которое может быть как альтруистическим, так и коммерческим. В-третьих, институт суррогатного материнства в РФ характеризуется недостаточной правовой регламентацией (отсутствием отдельного нормативно-правового акта, регулирующего отношения в сфере суррогатного материнства). В связи с чем считаем возможным использовать опыт законодателя Республики Беларусь при регламентации обозначенной сферы правоотношений.

Список литературы

1. Данельян А. А. Международно-правовые аспекты суррогатного материнства // Электронное сетевое издание «Международный правовой курьер» [Электронный ресурс]. URL: http://inter-legal.ru/mezhdunarodno-pravovye-aspekty-surrogatnogo-materinstva (дата обращения: 26.01.2023).

2. Самойлова В. В. Суррогатное материнство как правовой институт // Теория и практика общественного развития. 2014. № 4. С. 234–236.

[14] О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 19 декабря 2022 г. № 538-ФЗ // Информационно-правовой портал «ГАРАНТ» [Электронный ресурс]. URL: https://www.garant.ru/hotlaw/federal/1591683/ (дата обращения: 26.01.2023).

Ludmila Y. Odegova
PhD (Law), acting head of the department of
constitutional and international law,
Donetsk National University
(Donetsk, Russian Federation)
milaodegova17@mail.ru

Yulia A. Solovyova
PhD (Law), associate professor of the department of
constitutional and international law,
Donetsk National University
(Donetsk, Russian Federation)
soloveva5585@bk.ru

SURROGACY IN INTERNATIONAL AND NATIONAL LAW

Abstract. The article provides a brief overview of international and national legislation governing the use of such a method of assisted reproductive technologies as surrogate motherhood; it has been established that in the Russian Federation the right to use gestational surrogacy, which can be both altruistic and commercial, is legally fixed; insufficient legal regulation of this institution in national law has been criticized.

Keywords: assisted reproductive technologies; surrogate motherhood; commercial surrogacy; traditional surrogacy; gestational surrogacy; essential terms of the contract on surrogate motherhood.

УДК 347.9

Покаместов Пётр Викторович
Ведущий эксперт ООО «СиЭсАй груп»,
(г. Москва, Российская Федерация)
Petr.pokamestov@csi.group

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ EDISCOVERY В ЮРИСПРУДЕНЦИИ НА ПРИМЕРЕ ДЕЛ О БАНКРОТСТВЕ

Аннотация. Настоящая статья призвана исследовать применимость eDiscovery в рамках российского законодательства, на примере сферы банкротства. Внедрение eDiscovery в судебную систему обсуждается уже довольно давно. Прогрессивное развитие цифровых технологий и растущий объём цифровых данных вносят изменения в привычные процессы, включая область правосудия. eDiscovery, или электронное раскрытие, является одним из инновационных инструментов, находящим применение в судопроизводстве по всему миру, и может эффективно использоваться в Российском. Однако, использование eDiscovery может привести не только к процессуальным, но и к ценностным изменениям в правовой системе.

Ключевые слова: eDiscovery, электронная информация, коммерческие споры, уголовные дела, банкротство, релевантная информация, судебный процесс, финансовый анализ, судебные расходы; корпоративная электронная почта, корпоративные смартфоны, компьютерно-технические исследования.

Для цитирования:
Покаместов П. В. Использование технологии eDiscovery в юриспруденции на примере дел о банкротстве // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 156–161.

EDiscovery – это процесс поиска, сбора, анализа и представления электронной информации в целях использования в судебном процессе[1].

Поддерживая сквозной процесс электронного обнаружения, eDiscovery помогает организациям снизить риски и обеспечить соответствие требованиям при сборе данных и разнообразных следов. Единая, полностью интегрированная платформа для поиска, сбора, обработки, оценки данных, их юридического анализа. eDiscovery предоставляет инструмент управления сквозным электронным обнаружением, результаты которого можно использовать в гражданских и уголовных судебных процессах.

Свойственные eDiscovery методы включают в себя обширный поиск по ключевым словам, аналитику

[1] The Sedona Conference, «Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery», 2017.

большого количества данных и машинное обучение, что позволяет быстро обрабатывать и анализировать большое количество информации, значительно ускоряя процесс и увеличивая точность результатов.

В международных судах eDiscovery уже давно является стандартной практикой и применяется в различных типах судопроизводства, включая коммерческие споры, уголовные дела и дела о банкротстве. eDiscovery помогает сторонам быстро и точно найти релевантную информацию, что в итоге способствует справедливому решению дела в более короткие сроки[2].

В России применение eDiscovery ещё находится в начальной стадии. Однако, существует значительный потенциал для использования данно технологии, особенно в делах о банкротстве. В таких делах, где может быть множество участников и огромное количество документов, этот инструмент может быть особенно полезным.

Прежде всего, eDiscovery может ускорить процесс поиска и анализа информации. Вместо того, чтобы вручную просматривать каждый документ, юристы могут использовать инструменты eDiscovery для быстрого поиска нужной информации. Это не только экономит время, но и может привести к более точным результатам, поскольку риск пропуска важной информации снижается. Степень влияния человеческого фактора ниже, чем при ручном анализе документов.

Второй момент, где eDiscovery может быть полезным, – это анализ больших объёмов данных. В делах о банкротстве может быть вовлечено множество участников и транзакций. С помощью него предполагается анализировать эти данные с целью выявления скрытых взаимосвязей, потенциальных злоупотреблений и других факторов, которые могут повлиять на исход дела.

В-третьих, eDiscovery может быть использован для автоматического отслеживания изменений в документах и базах данных, что позволит своевременно реагировать на любые изменения в ситуации.

Несмотря на отсутствие точных статистических данных по России, исследования, проведённые в других странах, показывают, что eDiscovery значительно повышает эффективность судебного процесса.

По результатам одного исследования, использование eDiscovery может сократить время анализа документов на 60–80 %[3], что позволяет значительно сократить затраты на юридические услуги, а также уменьшить нагрузку на судебную систему.

Применение eDiscovery в делах о банкротстве может быть не только полезным, но и необходимым инструментом. В эпоху цифровизации, когда объёмы данных растут с каждым днём, традиционные методы анализа документов становятся всё менее эффективными. eDiscovery предлагает решение этой проблемы, позволяя

[2] Federal Judicial Center, «Managing Discovery of Electronic Information: A Pocket Guide for Judges», 2007.

[3] Grossman D. C., Frieder O. Information Retrieval: Implementing and Evaluating Search Engines. MIT Press, 2016. DOI: https://doi.org/10.1007/978-1-4020-3005-5

обрабатывать большие объёмы информации быстро и точно.

Основным нормативным источником, дающим представление о том, как и в каких целях составляется финансовый анализ должника в делах о банкротстве (несостоятельности), является Постановление Правительства РФ от 25.06.2003 № 367 «Об утверждении Правил проведения арбитражным управляющим финансового анализа»[4] (далее – «Правила проведения арбитражным управляющим финансового анализа», «Правила»). Данный правовой акт регламентирует принципы и условия проведения арбитражным управляющим финансового анализа и используемые им сведения.

Правила не выделяют отдельно такую цель, как выявление точки объективного банкротства должника. Пункт 2 Правил определяет, что финансовый анализ проводится в целях:

1. Подготовки предложения о возможности (невозможности) восстановления платёжеспособности должника и обоснования целесообразности введения в отношении должника соответствующей процедуры банкротства;

2. Определения возможности покрытия за счёт имущества должника судебных расходов;

3. Подготовки плана внешнего управления;

4. Подготовки предложения об обращении в суд с ходатайством о прекращении процедуры финансового оздоровления (внешнего управления) и переходе к конкурсному производству;

5. Подготовки предложения об обращении в суд с ходатайством о прекращении конкурсного производства и переходе к внешнему управлению.

Для осуществления этих целей может быть необходимо проанализировать огромный массив данных. Объектами анализа могут являться:

1. Документация нескольких организаций и (или) физических лиц;

2. Сообщения корпоративной электронной почты;

3. Данные с корпоративных смартфонов и персональных компьютеров.

Соответственно, ручной анализ таких объёмов информации будет требовать больших временных затрат. Вероятность ошибки, вызванной человеческим фактором, в процессе анализа прямо пропорционально растёт объёму анализируемой информации. Однако при использовании инструмента eDiscovery все эти данные будут храниться в одном месте, текст документов будет распознан, и специалисты смогут в автоматизированном режиме работать сразу со всем массивом информации.

Однако необходимо учитывать несколько моментов.

Во-первых, для сбора данных необходимо привлекать специалистов, которые имеют компетенции в

[4] Постановление Правительства РФ от 25.06.2003 № 367 «Об утверждении Правил проведения арбитражным управляющим финансового анализа» // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_42901/ (дата обращения: 14.05.2023).

компьютерно-технических исследованиях. Это обусловлено требованиями российского законодательства к обеспечению неизменности цифровых устройств и объектов. То есть задачей данного специалиста будет снять данные с устройств так, чтобы не внести изменений в их информационную структуру.

В таком случае если какой-либо орган или сторона спора будут не согласны с результатами, они смогут проверить, что никакая информация не удалялась с объектов или не была добавлена, что обеспечит принцип повторяемости. Также необходимо учитывать необходимость соблюдения принципов законности, соблюдения прав и свобод человека и гражданина, прав юридического лица.

Для большей прозрачности использования инструмента eDiscovery и возможности проверки совершаемых действий, необходимо составление и использование следующих документов:

1. Журнал передачи устройств;
2. Журнал сбора данных.

Журнал передачи устройств обеспечит возможность проверки, кто и какие устройства передавал техническим специалистам для сбора информации. А Журнал сбора данных необходим для максимально подробного описания техническими специалистами того, как, с каких устройств и при помощи чего проводился сбор данных.

Любые данные, которые хранятся в электронной форме, могут быть обработаны в соответствии с общими правилами eDiscovery. Этот тип данных исторически включал электронную почту и офисные документы, но также поддерживает фотографии, видео, базы данных и другие типы файлов.

В электронное обнаружение также включены «необработанные данные», которые могут просматриваться на предмет скрытых доказательств. Исходный формат файла известен как «собственный» формат[5].

Судебные органы могут просматривать материалы из электронного открытия в одном из нескольких форматов: печатная бумага, «исходный файл» или в окаменелом, похожем на бумагу формате, таком как файлы PDF или изображения TIFF. Современные платформы просмотра документов допускают использование собственных файлов и позволяют конвертировать их в формат TIFF и штамп Бейтса для использования в суде.

Таким образом, в целом, eDiscovery предлагает новые возможности для улучшения эффективности и объективности в судебном процессе. В контексте дел о банкротстве это может означать быстрый и точный поиск по документам, анализ больших объёмов данных и автоматизированный анализ,

[5] Иванова А. П. Искусственный интеллект в осуществлении правосудия: новые возможности и новые проблемы // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право: Реферативный журнал. 2022. № 3. С. 89–98.

которые могут иметь значительное значение для исхода дела.

Однако, чтобы в полной мере использовать потенциал eDiscovery, требуется не только соответствующее техническое оборудование и программное обеспечение, но и подготовка юридических специалистов. Только в этом случае возможно достижение максимальной эффективности при использовании данного подхода.

Таким образом, мы видим, как мир приближается к официальной информационной эре, индустрия eDiscovery будет продолжать активно расти. В цифровом виде создаётся больше информации, чем когда-либо прежде, а это означает, что потребность в процессе обнаружения электронных данных возрастает с каждым годом.

Список литературы

1. Артюшина Л. А. Управление ИТ-сервисами и контентом: учеб. пособие / Под ред. Л. А. Артюшиной, Е. А. Троицкой; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. Владимир: ВлГУ, 2021. 280 с.

2. Иванова А. П. Искусственный интеллект в осуществлении правосудия: новые возможности и новые проблемы // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право: Реферативный журнал. 2022. № 3. С. 89–98.

3. Mulder W. D., Valcke P., Vanderstichele G., Baeck J. Are judges more transparent than black boxes? A scheme to improve judicial decision-making by establishing a relationship with mathematical function maximization // Law and contemporary problems. Durham, 2021. Vol. 84. № 3. Pp. 46–67.

4. Grossman D. C., Frieder O. Information Retrieval: Implementing and Evaluating Search Engines. MIT Press, 2016. DOI: https://doi.org/10.1007/978-1-4020-3005-5

5. Kasap G. H. Can artificial intelligence («AI») replace human arbitrators? Technological concerns and legal implications // Journal of dispute resolution. Columbia. 2021. № 2. Pp. 1–46.

6. Re R. M., Solow-Niederman A. Developing artificially intelligent justice // Stanford technology law review. Stanford, 2019. Vol. 22. № 2. P. 242–289.

7. Reiling A. D. Courts and artificial intelligence // International journal for court administration. Williamsburg, 2020. Vol. 11. № 2. Pp. 1–10.

Petr V. Pokamestov
Leading Expert of LLC «CSI Group»
(Moscow, Russian Federation)
Petr.pokamestov@csi.group

THE USE OF EDISCOVERY TECHNOLOGY IN LEGAL PRACTICE, FOR EXAMPLE BANKRUPTCY CASES

Abstract. This article is intended to investigate the applicability of eDiscovery within the framework of Russian legislation, using the example of the sphere of bankruptcy. The introduction of eDiscovery into the judicial system has been discussed for quite some time. The progressive development of digital technologies and the growing volume of digital data are making changes in the usual processes, including the field of justice. eDiscovery, or electronic disclosure, is one of the innovative tools that finds application in legal proceedings around the world and can be effectively used in Russian. However, the use of eDiscovery can lead not only to procedural, but also to value changes in the legal system.

Keywords: eDiscovery, electronic information, commercial disputes, criminal cases, bankruptcy, relevant information, litigation, legal services, judicial system, financial analysis, court costs; corporate email, corporate smartphones, personal computers, computer and technical research.

УДК 347.963

Покуль Анастасия Анатольевна
Научный сотрудник отдела информационных технологий
Иркутский юридический институт (филиал)
Университета прокуратуры Российской Федерации
(г. Иркутск, Россия)
pokul79@mail.ru

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ПРОКУРАТУРЫ

Аннотация. В статье проводится анализ применения искусственного интеллекта в органах прокуратуры. Прокуратура Российской Федерации играет особую правозащитную роль. Использование нейронных сетей в прокурорской деятельности позволит активно добиваться устранения нарушений закона и восстановления нарушенных прав.

Ключевые слова: цифровизация, цифровые технологии, деятельность органов прокуратуры, цифровая трансформация, искусственный интеллект, прокуратура, нейронные связи.

Для цитирования:
Покуль А. А. Возможности использования технологии искусственного интеллекта в деятельности органов прокуратуры // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 162–169.

Современный мир невозможно представить без цифровых технологий. Они востребованы во всех сферах жизни человека, в том числе и в работе государственных органов. Цифровые технологии стали частью современных управленческих систем в отраслях экономики, права, обороны страны, сферах государственного управления, безопасности государства и обеспечения правопорядка. Развитие информационных технологий повышает эффективность управления в этих отраслях.

Цифровизация органов прокуратуры РФ является частью национальной программы «Цифровая экономика Российской Федерации», утвержденной распоряжением Правительства РФ от 28.07.2017 № 1632-р[1]. Для реализации данной программы Генеральной прокуратурой Российской Федерации была утверждена Концепция цифровой

[1] Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение правительства РФ от 28 июля 2017 года № 1632-р // СПС «КонсультантПлюс». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_221756/ (Дата обращения: 10.05.2023).

трансформации органов и организаций прокуратуры до 2025 года[2]. Сегодня мы находимся на завершающем этапе реализации Концепции, который включает в себя «создание аналитической платформы баз данных органов прокуратуры с применением стандартов обработки массивов больших данных в облачных и иных системах, а также технологий искусственного интеллекта».

Цифровая трансформация органов прокуратуры направлена на высокотехнологичный прокурорский надзор, электронный документооборот, разработку и внедрение вновь создаваемых компонентов цифровой среды, создание системы взаимодействия с гражданами, обществом и организациями, разработку и внедрение систему мониторинга, повышение удовлетворённости граждан, открытости и прозрачности информационного сопровождения процессов надзорной деятельности.

В Концепции содержатся ожидаемые результаты и основные показатели её реализации. Предполагается, что к 2025 г. доля граждан и юридических лиц, удовлетворённых качеством взаимодействия с органами прокуратуры, составит не менее 90 %, а время прохождения обращений до исполнителя сократится на 50 %.

Приоритетные направления развития и использования технологий искусственного интеллекта определяются с учётом национальных целей и стратегических задач, определённых Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»[3].

Первые сведения о внедрении искусственного интеллекта в деятельность органов прокуратуры появились 2018 году, когда НИИ «Восход» разместило тендер на выполнение работ по созданию, развитию и поддержке информационных систем и ресурсов Генеральной прокуратуры Российской Федерации. Внедрение искусственного интеллекта в деятельность органов прокуратуры – это весьма интересный и перспективный проект. Из информации, размещённой на сайте государственных закупок[4], следует,

[2] Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года: приказ Генерального прокурора Российской Федерации от 14 сентября 2017 г. № 627 // СПС «КонсультантПлюс». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_278651/ (Дата обращения: 10.05.2023).

[3] О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года» : указ Президента РФ от 10 октября 2019 г. № 490 // СПС «КонсультантПлюс». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_335184/ (Дата обращения: 10.05.2023).

[4] Закупка № 31807017413 // Единая информационная система в сфере закупок. [Электронный ресурс]. URL: https://zakupki.gov.ru/223/purchase/public/purchase/info/common-info.html?lotId=9618345&purchaseId=7233622&purchaseMethodType=EP (дата обращения: 09.10.2022).

что к 2025 году Генеральная прокуратура Российской Федерации планирует ввести в прокурорскую деятельность «высокотехнологичный надзор», подразумевающий под собой совокупность организационных и технических мер прокурорского надзора и иных функций органов прокуратуры с использованием современных технологических инструментов, которые включают в себя «автоматизированное выявление нарушений, дистанционного доступа в информационные системы надзорных органов, использование инструментов на базе «мягкого искусственного интеллекта» (soft AI) и больших данных (big data)».

До недавнего времени искусственный интеллект считался программным решением, заложенным в памяти, действующим по заданным алгоритмам. Впоследствии, с развитием цифровых технологий, искусственная интеллектуальная система стала программно-аппаратным комплексом, умеющим выполнять творческие задания, относящиеся к конкретным предметным областям, знания о которых хранятся в памяти интеллектуальной системы. Такая система свидетельствует о разумном поведение при сборе и анализе обстановки и реализации с некоторой степенью автономии действий по достижению конкретных целей.

Необходимо отметить, что специалисты в области разработки и внедрения нейронных сетей дифференцируют несколько смежных понятий искусственного интеллекта. В частности, выделяется прикладной искусственный интеллект (Artificial Narrow Intelligence) – слабый, узкий искусственный интеллект; общий или сильный искусственный интеллект (Artificial General Intelligence), являющийся универсальным, он находится на одном уровне с человеческим интеллектом и способен выполнять разнообразный круг задач и искусственный сверхинтеллект (Artificial Superintelligence), превосходящий уровень отдельного человека или всего человечества.

Исходя из анализа документов, приведённых на сайте государственных закупок, можно говорить о том, что Генеральная прокуратура Российской Федерации внедряет в прокурорскую деятельность именно прикладной (слабый) искусственный интеллект. В связи с этим возникает вопрос о необходимости реализации указанных предложений в практической деятельности прокурорских работников, а также о проблемах, которые могут возникнуть в ходе их выполнения.

На сегодняшний день имеются сложности, с которыми ежедневно сталкиваются работники прокуратуры при выполнении своих служебных обязанностей. Попробуем обобщить и осветить некоторые из них. С этой целью нами проведено исследование, в рамках которого были проанкетированы прокурорские работники из Сибирского и Дальневосточного федеральных округов, проходивших обучение в Иркутском юридическом институте (филиале) Университета прокуратуры Российской Федерации в 2022–2023 уч. году. Результаты анкетирования позволили сделать предварительные

выводы о возможности использования искусственного интеллекта в органах прокуратуры.

Так, по мнению прокурорских работников, применение искусственного интеллекта может осуществляться с целью освобождения их от монотонной работы в такой информационной системе, как портал государственной автоматизированной системы правовой статистики (далее – ГАС ПС). 69 % респондентов высказались об использовании искусственного интеллекта при формировании показателей статистической отчётности в ГАС ПС.

Основные сложности, с которыми сталкиваются прокурорские работники при использовании ГАС ПС:

– большие временные затраты на внесение в программу данных;

– необходимость внесения большого количества информации, сканирования значительного объёма документов;

– сложность в освоении ГАС ПС, недостаточная адаптированность к работе прокурора.

По своей сути ГАС ПС представляет собой специальное программное обеспечение, предназначенное для сбора, ввода, обработки, хранения и использования статистической информации. Основной его смысл состоит в создании и ведении учётных карточек по основным направлениям прокурорской деятельности. Преимущество данной технологии заключается в том, что «создается единое хранилище данных на федеральном уровне, что повышает степень контроля за обеспечением достоверности правовой статистики»[5].

ГАС ПС была создана для упрощения работы прокуроров с различными данными, включая статистические. Она также заменяет бумажный документооборот на электронный, что позволяет участникам информационного взаимодействия обмениваться данными быстрее и эффективнее. ГАС ПС также позволяет отслеживать ход событий любого дела или материала, а также выполнять другие важные функции. Эта система была создана для улучшения работы прокурорских органов и повышения эффективности их работы.

В рамках цифровой трансформации в деятельность органов прокуратуры Российской Федерации поэтапно устанавливался поисково-аналитический интерфейс, отдельные элементы которого построены были на работе нейронных сетей.

Основной сложностью, возникающей при применении нейронных сетей в прокурорской деятельности, в том числе в рамках Портала ГАС ПС, является отсутствие подхода к определению лица, обязанного нести ответственность за неправильное формирование статистической отчётности в органах прокуратуры. Правовая статистика является важной составляющей прокурорского надзора. Информация, излагаемая в статистической

[5] Яцуценко В. В. Проблемы и перспективы внедрения цифровых технологий в деятельность органов прокуратуры // Актуальные проблемы российского права. 2021. № 11. С. 187–193.

отчётности, является отражением результатов надзорной деятельности органов прокуратуры РФ, показателем эффективности их работы в рамках проведения анализа состояния законности. Ошибочное внесение статистических показателей может привести к искажению реальных сведений по борьбе с преступностью и правонарушениями непреступного характера, что, в свою очередь, может повлиять на правильность определения политики государства в указанной сфере[6] .

Кроме того, возникают сложности при вводе вручную показателей при составлении статистических отчётов. Современные нейронные сети способны анализировать текст отдельно, извлекать из него необходимые данные и размещать в различные формах юридических документов. Такую нейронную сеть можно было развернуть в прокуратуре для генерации собственных и статистических данных из документов. Отсканированные прокурором документы загружались бы на портал ГАС ПС.

Считается, что с использованием технологий искусственного интеллекта для формирования статистической отчётности, необходимо изменить подход прокуратуры Российской Федерации к определению ответственных лиц за искажение статистических данных, которые отражены в отчётах.

В связи с этим возникает необходимость в правовом регулировании использования искусственного интеллекта в деятельности прокуратуры Российской Федерации.

В целях совершенствования модернизированного специального программного обеспечения государственной автоматизированной системы правовой статистики на территории Российской Федерации временно приостановлена опытная эксплуатация ГАС ПС с 01 января 2023 года[7].

Возможно, в дальнейшем данный Портал будет работать с учётом анализа проблем и сложностей, с которыми сталкиваются работники прокуратуры при использовании ГАС ПС.

Кроме того, прокурорские работники (60 %) положительно высказались о применении нейронных связей в прогнозировании и отслеживании изменений в области законодательства и судебной практики.

Мониторинг законодательства и правоприменительной практики является важным инструментом для

[6] Быстров Д. С. Вопросы применения технологий искусственного интеллекта в прокурорской деятельности // Проблемы совершенствования прокурорской деятельности и правоприменительной практики: сборник статей. Иркутск: Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2021. Выпуск 11. С. 199.

[7] О временном приостановлении опытной эксплуатации государственной автоматизированной системы правовой статистики : приказ Генерального прокурора Российской Федерации от 10 января 2023 г. № 3. Доступ из справочно-правовой системы «КонсультантПлюс».

обеспечения сбалансированного регулирования общественных правоотношений и формирования системности в оценке практики применения законодательства. Он позволяет выявлять недостатки в законодательстве и его применении, а также помогает в разработке новых законов и улучшении существующих.

Использование технологий искусственного интеллекта в целях мониторинга изменений законодательства связано с участием машинного обучения на основе нейросетей, работающих с большими массивами данных. В будущем это позволит создать автоматизированную систему, представляющую собой комплекс решений для анализа законодательства, эффективного обнаружения изменений, что привело бы к оптимизации рабочего времени прокурорского работника. Данная система должна быть самообучаемой.

Также хочется обратить внимание на ещё одно из главных направлений прокуратуры – работа с обращениями граждан, которая занимает значительную часть общей нагрузки органов прокуратуры. Прокуратура – это орган государственной власти, который занимается надзором за соблюдением закона и защитой прав и свобод граждан. Каждый год работники прокуратуры рассматривают сотни тысяч жалоб и заявлений от граждан. В последние годы число жалоб и заявлений, поступающих в органы прокуратуры, постоянно увеличивается. Граждане используют своё право на обращение, чтобы защитить нарушенные права и свободы.

Так, 60 % опрошенных прокурорских работников высказались о внедрении искусственного интеллекта при работе с обращениями граждан.

Система могла бы быть эффективной и для выявления мошеннических схем – посредством фиксации однотипных заявлений граждан из различных районов или регионов такие схемы распознать несложно.

Использование современных технологий даёт нам возможность улучшить доступ к правосудию, чем мы обязательно должны воспользоваться.

Кроме того, одна из главных задач будущей нейросети – ускорение бюрократических правовых процедур путём классификации преступлений по категориям и создания реестра судебных дел, которые будут оцифрованы. В настоящее время мы находимся на пути развития и внедрения электронного уголовного дела. Цифровая трансформация уголовного судопроизводства обеспечивает быстроту и качество предварительного расследования, является дополнительной гарантией соблюдения разумных сроков, а также усиления прокурорского надзора и судебного контроля. Это поможет ускорить судебные процессы и сделать их более эффективными.

В разных странах мира, таких как Германия, США, Канада, Великобритания, Австрия, КНР, Сингапур и другие, уже успешно используются электронные уголовные дела. В России также появляются соответствующие предложения. Внедрение электронной системы

уголовного процесса имеет множество преимуществ, таких как сокращение времени расследования, удобство судебного процесса и другие. Однако, есть и риски, такие как возможность хакерских атак, утечки персональных данных и незаконного вмешательства в уголовное дело. Кроме того, электронные уголовные дела могут быть более доступными для людей с ограниченными возможностями, такими как слабовидящие или глухие. Они могут использовать специальные программы и технологии для получения доступа к информации и участия в судебном процессе. Однако, необходимо обеспечить соответствующую поддержку и обучение для таких людей, чтобы они могли эффективно использовать электронные уголовные дела.

По мнению работников прокуратуры, искусственные нейронные сети могут быть применены в следующих направлениях деятельности:

- составление исковых заявлений;
- анализ состояния законности;
- правовое просвещение;
- подготовка актов прокурорского реагирования;
- аналитическая деятельность.

Таким образом, мы видим потребность прокурорских работников во внедрении искусственного интеллекта в служебную деятельность, нейронная сеть может стать незаменимым помощником в решении различных задач.

Вместе с тем, технологии искусственного интеллекта основываются на модели искусственного нейрона головного мозга человека, который представляет собой математическую формулу, в которую подставляются точные величины. Несмотря на это, ни одна нейронная сеть не является идеальной и может допускать ошибки и погрешности в своей работе. В настоящее время не решён вопрос о статусе искусственного интеллекта, его ответственности за принимаемые решения и других вопросах, связанных с правовым регулированием. Искусственный интеллект – это одна из наиболее быстро развивающихся областей в науке и технологиях. Он используется в различных сферах, таких как медицина, финансы, транспорт и многие другие. Однако, с развитием искусственного интеллекта возникают новые этические и правовые вопросы, которые требуют серьёзного обсуждения и регулирования. Кто несёт ответственность за ошибки, допущенные искусственным интеллектом? Как обеспечить безопасность и конфиденциальность данных, обрабатываемых искусственным интеллектом? Как регулировать использование искусственного интеллекта в различных областях жизни? Эти вопросы требуют дальнейшего изучения и разработки соответствующих правовых норм и стандартов не только в различных сферах жизни общества и государства, но и в прокурорской деятельности. Если эти проблемы будут решены, то внедрение искусственного интеллекта в деятельность органов прокуратуры может стать важным шагом на пути к более эффективной борьбе с преступностью и защите прав граждан.

Список литературы

1. Быстров Д. С. Вопросы применения технологий искусственного интеллекта в прокурорской деятельности // Проблемы совершенствования прокурорской деятельности и правоприменительной практики: сборник статей. Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2021. Выпуск 11. С. 199–201.

2. Яцуценко В. В. Проблемы и перспективы внедрения цифровых технологий в деятельность органов прокуратуры // Актуальные проблемы российского права. 2021. № 11. С. 187–193.

Anastasia A. Pokul
Researcher in the Department of Information Technology
Irkutsk Institute of Law (branch)
of the University of the Public Prosecutor's Office of the Russian Federation
(Irkutsk, Russia)
pokul79@mail.ru

POSSIBILITIES OF USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE ACTIVITY OF PROSECUTOR'S OFFICES

Abstract. The article analyzes the use of artificial intelligence in the prosecutor's office. The Prosecutor's Office of the Russian Federation plays a special human rights role. The use of neural networks in prosecutorial activities will allow us to actively seek the elimination of violations of the law and the restoration of violated rights.

Keywords: digitalization, digital technologies, activities of the prosecutor's office, digital transformation, artificial intelligence, prosecutor's office, neural connections.

УДК 343.97

Ржанникова Светлана Сергеевна
старший преподаватель кафедры криминалистики
Уральский юридический институт МВД России
(г. Екатеринбург, Россия)
ssr80@mail.ru

К ВОПРОСУ О ПРАВОВОМ РЕГУЛИРОВАНИИ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. В статье рассмотрены особенности правовой регламентации применения технологий искусственного интеллекта в работе экспертно-криминалистических подразделений МВД России, проанализированы положения действующих нормативных правовых актов, на основе которых сформулированы выводы о необходимости совершенствования существующего законодательства.

Ключевые слова: искусственный интеллект, алгоритм, машинное обучение, правовая регламентация, экспертно-криминалистическая деятельность.

Для цитирования:
Ржанникова С. С. К вопросу о правовом регулировании использования искусственного интеллекта в экспертно-криминалистической деятельности // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 170–174.

В настоящее время ведутся активные научные дискуссии на тему возможностей использования технологий искусственного интеллекта в различных сферах правоприменительной деятельности.

Анализ современного законодательства в данной сфере показал, что на сегодняшний день наблюдается некое замедление в вопросах разработки нормативно-правовых актов, регламентирующих использование технологий искусственного интеллекта в деятельности правоохранительных органов в целом и в экспертной деятельности в частности. К тому же нормативно-правовые акты, содержащие данные положения, можно подразделить на два типа: первые регламентируют понятийный аппарат технологий, связанных с искусственным интеллектом; вторые содержат алгоритм и рекомендации по их использованию в правоохранительной деятельности.

Ещё в 2016 году в Указе Президента переход к технологиям машинного обучения и искусственного интеллекта назван приоритетной задачей развития науки и техники в России[1]. При этом в данном документе

[1] О стратегии научно-технического развития Российской Федерации: указ Президента РФ от 01.12.2016 № 642 // Президент России: официальный сайт. [Электронный ресурс].

обработка больших объёмов данных, машинное обучение и искусственный интеллект именуются через запятую как самостоятельные технологии, если и обладающие взаимосвязью, то лишь косвенной.

В 2019 году в развитие идеи перехода российской науки и техники к исследованию, созданию и внедрению в практическую деятельность технологий искусственного интеллекта утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года (далее – Стратегия)[2]. В Стратегии указано, что её положения должны учитываться при реализации проектов, обеспечивающих достижение целей и показателей деятельности органов исполнительной власти. Одной из целей развития искусственного интеллекта в России названо обеспечение национальной безопасности и правопорядка.

Кроме того, в Стратегии впервые на законодательном уровне даётся определение таким понятиям, как: «искусственный интеллект», «технологии искусственного интеллекта», «архитектура вычислительной системы» и др.

Приказом Минэкономразвития утверждены Критерии принадлежности проектов к проектам в сфере искусственного интеллекта. Данный документ не только устанавливает требования для получения бюджетного финансирования на создание, развитие или внедрение проектов в сфере искусственного интеллекта, но и определяет виды технологий и методов искусственного интеллекта, среди которых законодатель кратко раскрывает понятие нейросети, как «автоматизированное машинное обучение, включая эволюционные алгоритмы»[3].

Таким образом, в настоящий момент существует три нормативных акта общего характера, из которых только Стратегия является непосредственно применимой к рассматриваемому вопросу. В Стратегии встречается словосочетание «экспертная система», однако, это никакого отношения к экспертно-криминалистической деятельности не имеет, а подразумевает под собой алгоритм по выбору заранее определённого решения, в зависимости от установленных условий. Указ Президента № 642 в большей части носит декларативный характер, а приказ Минэкономразвития не имеет отношения к экспертно-криминалистической деятельности МВД России.

Федеральный закон от 31.05.2001 г. №73-ФЗ «О

URL: http://www.kremlin.ru/acts/bank/41449 (Дата обращения 29.04.2023).

[2] О развитии искусственного интеллекта в Российской Федерации: указ Президента РФ от 10.10.2019 № 490 // Президент России: официальный сайт. [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/44731 (Дата обращения 29.04.2023).

[3] Об утверждении критериев определения принадлежности проектов к проектам в сфере искусственного интеллекта: Приказ Минэкономразвития России от 29.06.2021 № 392 // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_391797/ (Дата обращения 29.04.2023).

государственной судебно-экспертной деятельности в Российской Федерации» не отражает всей специфики работы экспертных учреждений, предоставляя ведомствам самим решать многие вопросы, в том числе связанные с применением программных продуктов при выполнении исследований. Проект Федерального закона № 306504-6 «О судебно-экспертной деятельности в Российской Федерации»[4] раскрывает содержание деятельности экспертных подразделений более широко, включая в неё не только организацию и производство экспертиз, но также научную деятельность, кадровое обеспечение и повышение квалификации действующих сотрудников.

Одним из направлений учётно-регистрационной деятельности является ведение экспертно-криминалистических учётов. В соответствии с положениями приказа № 70, это деятельность по систематизации и размещению в информационной системе экспертно-криминалистической информации об объектах учёта. Помимо этого, указано, что ведение учётов может быть «автоматизировано с использованием технических средств и автоматизированных информационных систем» [5].

В Стратегии закреплено, что искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма), поэтому положения приказа № 70 в существующем виде не позволяют применять технологии искусственного интеллекта в регистрационной деятельности ЭКП.

К тому же, к информационным системам, применяемым для формирования, ведения и использования криминалистических учётов предъявляется требование: они должны быть апробированы и рекомендованы к использованию экспертно-криминалистическим центром МВД России.

Возможность реализовать проекты в области искусственного интеллекта на базе уже имеющихся массивов информации нашла своё отражение в Программах цифровой трансформации МВД России в 2020 и 2022 годах, разработанных в соответствии с требованиями Правительства РФ[6]. Действующая программа цифровой трансформации

[4] О государственной судебно-экспертной деятельности в Российской Федерации: проект федерального закона № 306504-6 // Система обеспечения законодательной деятельности Государственной думы Федерального Собрания Российской Федерации: официальный сайт. [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/306504-6 (Дата обращения 05.05.2023).

[5] Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации: приказ МВД России № 70 от 10.02.2006 г. // ИПС «Гарант» [Электронный ресурс]. URL: https://base.garant.ru/72222630/ (Дата обращения 29.04.2023)

[6] О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных

МВД России на 2022–2024 год[7] предусматривает создание информационной системы определения фенотипических признаков человека на основе анализа биологического материала, изъятого с мест преступлений. Сама Программа не вводит каких-либо понятий или определений, используя ранее рассмотренную терминологию, и не только посвящена внедрению технологий искусственного интеллекта в деятельность МВД России, но и предусматривает их разработку и апробацию. Полагаем, обоснованно считать, что приведённая в Программе информационная система может быть отнесена к технологиям искусственного интеллекта, поскольку для её разработки предполагается создание датасета, а следовательно, система должна быть способна к осуществлению машинного обучения, чтобы освоить его.

Если рассматривать основной вид деятельности ЭКП – производство судебных экспертиз и исследований, то законодательством установлено, что судебные экспертизы должны производиться на основе единого научно-методического подхода к экспертной практике[8] с применением рекомендованных экспертных методик для полного, объективного и научно обоснованного[9] ответа на поставленные инициатором экспертизы вопросы.

Заключение эксперта является одним из доказательств по уголовному делу, и к нему, как и к другим видам доказательств, применяются требования относимости, допустимости, достоверности и достаточности.

Д. В. Бахтеев справедливо отмечает, что процесс обучения искусственной нейронной сети происходит на уровне скрытого слоя, в связи с чем проследить путь принятия ею решения от результата до исходных данных не представляется возможным[10]. По этой причине выводы, полученные на основе исследования с использованием

органов исполнительной власти и органов управления государственными внебюджетными фондами: постановление Правительства РФ от 10.10.2020 № 1646 // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_364874/ (Дата обращения 29.04.2023).

[7] Об утверждении ведомственной программы цифровой трансформации: распоряжение МВД России от 11.01.2022 г. № 1/37 // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_414300/f62ee45faefd8e2a11d6d88941ac66824f848bc2/ (Дата обращения 29.04.2023).

[8] О государственной судебно-экспертной деятельности: федеральный закон от 31.05.2011 № 73-ФЗ // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_31871/ (Дата обращения 05.05.2023).

[9] Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации: приказ МВД России № 511 от 29.06.2005 г. // СПС «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_55315/ (Дата обращения 05.05.2023).

[10] Бахтеев Д. В. Искусственный интеллект в следственной деятельности: задачи и проблемы // Российский следователь. 2020. № 9. С. 5.

технологий искусственного интеллекта и изложенные в заключении эксперта, нельзя считать соответствующими критерию достоверности. Результаты деятельности искусственного интеллекта могут содержать только ориентирующую, но не доказательственную информацию.

Учитывая, что ни в ФЗ № 73, ни в Приказе № 511, ни в Наставлении по организации экспертно-криминалистической деятельности в системе МВД России не содержится положений, допускающих применение технологий искусственного интеллекта в производстве экспертиз, можно заключить, что на текущий момент отсутствуют не только правовые, но и методические основы для их применения.

Таким образом, правовые основания использования искусственного интеллекта в деятельности экспертно-криминалистических подразделений МВД России содержатся в нескольких нормативно-правовых актах: Указах Президента и Стратегии. Что касается существующих ведомственных приказов, то прямой запрет либо разрешение на использование технологий искусственного интеллекта в ЭКП МВД России отсутствует. Учитывая, что в ближайшем будущем данные технологии могут быть внедрены в организационную, консультационную и образовательную деятельность экспертно-криминалистических центров, требуется корректировка действующих нормативно-правовых актов с целью приведения в соответствие существующих технологических возможностей и допустимости их использования в различных направлениях деятельности ЭКП.

Список литературы

1. Бахтеев Д. В. Искусственный интеллект в следственной деятельности: задачи и проблемы // Российский следователь. 2020. № 9. С. 3–6.

Svetlana S. Rzhannikova
Senior Lecturer of the Department of Criminalistics
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russia)
ssr80@mail.ru

ON THE ISSUE OF LEGAL REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE IN FORENSIC ACTIVITIES

Abstract. The article considers the features of the legal regulation of the use of artificial intelligence technologies in the work of the forensic units of the Ministry of Internal Affairs of Russia, analyzes the provisions of existing regulatory legal acts, on the basis of which conclusions are formulated about the need to improve existing legislation.

Keywords: artificial intelligence, algorithm, machine learning, legal regulation, forensic activity.

УДК 343.9

Рыбалкин Никита Андреевич
государственный судебный эксперт
ФБУ Тульская ЛСЭ Минюста России,
ассистент кафедры СЭиТД
Тульский государственный университет
(г. Тула, Россия)
nikitarybalkin@rambler.ru

АКТУАЛЬНЫЕ ПРОБЛЕМЫ СУДЕБНОЙ ЭКСПЕРТИЗЫ ПРИ ВЫЯВЛЕНИИ ДОКУМЕНТОВ, ВЫПОЛНЕННЫХ С ПОМОЩЬЮ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Аннотация. Автором рассматривается актуальный вопрос судебно-почерковедческой экспертизы и судебной технической экспертизы документов – выполнение реквизитов документов с помощью современных технических средств (графопостроительной техники). В предлагаемой статье анализируются основные методы выявления данных почерковых объектов, описываются экспериментальные исследования их выполнения, изучаются и характеризуются основные современные технические средства, с помощью которых возможно выполнение почерковых объектов. Следует отметить, что данная работа является одной из попыток обобщения судебно-экспертной практики по вопросам выполнения почерковых объектов с помощью современных технических средств, в ней озвучиваются рекомендации экспертам при работе с подобными объектами, а также затрагиваются вопросы, связанные с тем, что подобного рода объекты являются предметом возможного комплексного исследования экспертов-почерковедов и экспертов-техников. Считаем, что впоследствии эти рекомендации должны повлиять на подготовку будущих экспертов указанных специальностей.

Ключевые слова: судебно-почерковедческая экспертиза, судебно-техническая экспертиза документов, технические средства изготовления документов, плоттер, судебная экспертиза, таможенная экспертиза, таможенные документы.

Для цитирования:
Рыбалкин Н. А. Актуальные проблемы судебной экспертизы при выявлении документов, выполненных с помощью современных технических средств // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 176–183.

В рамках выполнения своих профессиональных обязанностей сотрудниками правоохранительных органов нередко выявляются различного рода документы, выполненные с помощью современных технических средств. Судебно-почерковедческая и судебно-техническая экспертиза документов обеспечивают установление

объективной истины по делам, связанным, в частности, с фальсификацией различных таможенных документов. В силу изменений, произошедших в науке и технике за последние 20 лет, значительно повысились требования к эффективности судебно-почерковедческих и судебно-технических экспертиз документов.

Укажем, что, по мнению Т. В. Толстухиной и И. В. Устиновой, «последнее десятилетие вследствие глобальной цифровизации общественной жизни, породившей аналогичное направление преступной деятельности, отмечено появлением в научной литературе в рамках криминалистики «новых криминалистических» направлений – «компьютерной криминалистики», «электронной криминалистики», «цифровой криминалистики», «медицинской криминалистики», «экономической криминалистики», «лингвокриминалистики»[1].

Следует отметить, что цифровые технологии также могут использоваться при фальсификации различного рода документов. Причиной этому послужил переход к безбумажным технологиям составления документов, в результате чего объекты почерковедческой и технической экспертизы становятся всё чаще малообъёмными, что вызывает дополнительные трудности при производстве судебной экспертизы. В этих случаях традиционные методики исследования документов в большинстве случаев не дают возможности однозначного решения задач, поставленных перед экспертом.

Т. В. Толстухина, А. А. Светличный и Д. В. Панарина отмечают в этой связи, что «применяемые методики должны быть общепризнанными и общеизвестными. Такая ситуация может стать реальной при создании и утверждении на соответствующем уровне каталогов экспертных методик. Необходимость стандартизации экспертных методик учеными отмечается уже на протяжении 30 лет… По новым и формирующимся родам (видам) экспертиз методики могут на первом этапе заимствоваться из материнской науки и без надлежащей модификации использоваться для решения простых прямых задач исследования объектов судебной экспертизы. Однако неизбежно практика судебно-экспертной деятельности заставляет модифицировать и оптимизировать такие методики, адаптируя их к специфике судебно-экспертного исследования, а также к возможному изменению законодательства»[2]. Таким

[1] Толстухина Т. В., Устинова И. В. Формализация научного криминалистического и судебно-экспертного знания в условиях цифровизации // Криминалистика и судебная экспертиза: наука, практика, опыт: Всероссийский форум, 27–28 апреля 2021 г. М.: Московский университет МВД России имени В. Я. Кикотя, 2021. С. 109–113.

[2] Толстухина Т. В., Светличный А. А., Панарина Д. В. Актуальные проблемы совершенствования методического обеспечения судебно-экспертной деятельности // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) Сборник статей Международной научно-практической конференции. 2018. С. 288–292.

образом, согласимся с необходимостью стандартизации и модификации уже существующих методик судебно-экспертной деятельности, а также создания новых, в связи с появлением объектов, выполненных с помощью современных технических средств.

Не случайно в XXI веке всё больше внимания уделяется созданию экспертных методик, связанных с применением современной оргтехники. В общей теории судебной экспертизы и практической судебно-экспертной деятельности наблюдается серьёзный пробел в виде неразработанности методики исследования почерковых объектов, выполненных с помощью современных технических средств, системы теоретических знаний о предмете, объекте, целях, задачах данной методики, что негативно сказывается на структуре и разработанности общей теории науки.

Следует отметить, что в связи с бурным развитием офисной техники компетентная фальсификация различных видов документов становится более доступной. Всё чаще стали выявляться документы, выполненные с помощью современных технических средств. Развитие компьютерной техники и прикладных навыков сделали эту технологию доступной даже для людей с небольшим опытом и навыками использования компьютерной техники. Сравнительно невысокая себестоимость цифровой фальсификации и её оперативность определяют рентабельность и эффективность для подделки различного рода документов. Например, в практике экспертов ФБУ ТЛСЭ Минюста России в договорах были выявлены фальсификации подписей генеральных директоров юридических лиц[3]. Данные подписи, предположительно, по совокупности выявленных признаков, были выполнены с помощью графопостроительной техники (плоттер, 3D-принтер, роботизированная рука).

Оговоримся, что под технических средством понимается «совокупность технических устройств средств вычислительной техники либо их частей»[4]. К таким устройствам можно отнести плоттер (графопостроитель), 3D-принтер, роботизированную руку, станок с числовым программным управлением (далее – ЧПУ).

Отметим, что первым примером выявления данного рода объектов в российской литературе можно считать статью Т. О. Пановой, О. Ю. Миловидовой и Е. С. Карпухиной[5]. В данном исследовании был описан случай из экспертной практики, когда

[3] Архив ФБУ ТЛСЭ Минюста России за 2017, 2019, 2023 годы (заключение эксперта О. № 673 от 21 апреля 2017 года, заключение экспертов К. и Г. № 1392-1581 от 2019 г., заключения К. и Р. 2023 года).

[4] Судебная компьютерно-техническая экспертиза. Термины и определения: Национальный стандарт РФ. Москва: Стандартинформ, 2018. 12 с.

[5] Панова Т. О., Миловидова О. Ю., Карпухина Е. С. Комплексное исследование имитации рукописных реквизитов (случай из экспертной практики) // Теория и практика судебной экспертизы. 2008. № 3 (11). С. 118–121.

удалось установить признаки выполнения почерковых объектов с помощью графопостроителя (плоттера).

В зарубежной практике одним из первых случаев использования техники вместо человеческой руки был зафиксирован в 2004 году, когда известная канадская писательница, Маргарет Этвуд, обратилась к одной из известных канадских фирм в области робототехники Quanser Consulting Inc. и впоследствии в сентябре 2006 года организовала презентацию онлайновой дистанционной подписи экземпляров книг с использованием устройства, которое было зарегистрировано под торговой маркой LongPenTM, т. е. роботизированная рука.

Отметим, что роботизированная рука изначально разрабатывалась и выпускается до сих пор для вполне легальных целей, например, для подписания неофициальных документов, открыток, поздравлений и т. п. Но, как это неоднократно случалось со многими достижениями научно-технического прогресса, она начинает активно использоваться в криминальных целях. Необходимо отметить, что если сегодня злоумышленник воспользуется для рисовки почеркового объекта одним из вышеописанных устройств, которые могут имитировать распределение нажима, то мы можем полагать, что эксперты только исходя из личного опыта и предельной внимательности к деталям смогут установить факт использования подобной технологии подделки, поскольку они не располагают методиками выявления следов их применения.

Для того, чтобы вооружить экспертов методическими рекомендациями по установлению фактов компьютерной технологии подделки рукописного почерка и подписей, необходимо проведение серьёзных исследований, требующих определённых финансовых затрат, прежде всего связанных с приобретением современных роботизированной руки, плоттеров, 3D-принтеров, станков с ЧПУ и иной графопостроительной техники для проведения исследований данных технологий, а также возможностью проведения комплексных исследований экспертом-почерковедом и экспертом-техником данного рода объектов.

Также необходимо отметить, что исследованию диагностирования признаков выполнения почерковых объектов с помощью технических средств посвятили свои труды Е. Н. Белова[6], Н. Ф. Бодров[7], М. Л. Подкатилина[8], В. Н. Пронин, П. Г.

---

[6] Белова Е. Н. Развитие криминалистической идентификации в судебно-почерковедческой экспертизе // Научно-практический журнал. 2015. № 3 (39). С. 172–175.

[7] Бодров Н. Ф. Судебно-экспертное исследование записей, выполненных аппаратами имитации рукописных реквизитов // Теория и практика судебной экспертизы в современных условиях. Материалы VI Международной научно-практической конференции, посвященной памяти заслуженного юриста РФ, доктора юридических наук, профессора Юрия Кузьмича Орлова. Москва, 2017. С. 56–59.

[8] Подкатилина М. Л. Проблемы назначения и производства судебных почерковедческих экспертиз // Вестник Университета имени О.Е. Кутафина. 2015. № 12. С. 116–121.

Лесникова[9], Т. В. Толстухина, Н. А. Рыбалкин[10], Н. А. Трушакова[11], Д. А. Шлыков[12], И. А. Ярощук, К. В. Гриневич[13], D. Kruger[14] и другие учёные. Таким образом, с учётом выхода статей указанных выше авторов, данная проблема уже долгое время является актуальной и требует дальнейшего более глубокого изучения.

Технические достижения последних лет в отношении офисной оргтехники привели к тому, что также и с помощью 3D-принтера, станка с ЧПУ и специального программного обеспечения возможно выполнить нажимные характеристики и рефлекторные штрихи, что может доставить дополнительные сложности при исследовании подобного рода объектов экспертами.

Отметим, что нами в порядке нескольких рабочих экспериментов были произведены попытки воспроизведения подписей с помощью различных моделей 3D-принтеров, плоттеров, станка с ЧПУ: Tarantula, Anycubic i3 mega, Ender 3 pro, робот-художник MR Painty FRP-01, благодаря чему нам удалось воссоздать почерковый объект, который, однако, сохранил признаки технического выполнения, такие как различие в нажиме, замедленный темп выполнения, усиленный нажим, фрагментарность выполнения некоторых элементов подписей (рис. 1).

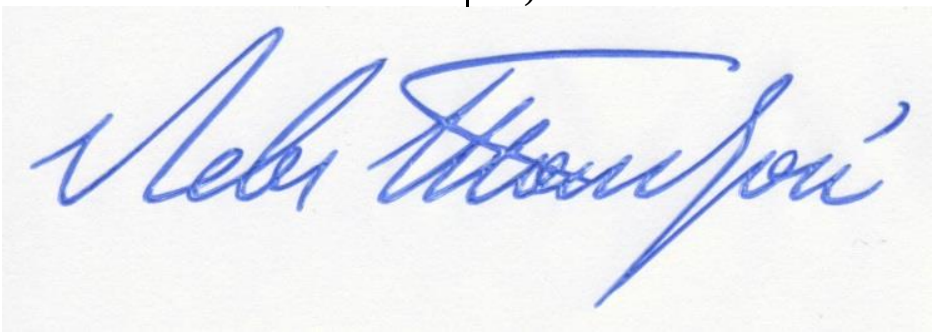

Рис. 1. Подпись Льва Толстого, выполненная с помощью 3D-принтера.

[9] Пронин В. Н., Лесникова П. Г. Исследование подписи с целью установления факта ее выполнения с помощью технического средства – плоттера (случай из экспертной практики) // Вестник Нижегородского университета им. Н. И. Лобачевского. 2015. № 4. С. 162–165.

[10] Толстухина Т. В., Рыбалкин Н. А. Проблемы производства судебно-почерковедческой экспертизы малообъёмных почерковых объектов по электрофотографическим копиям // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 2. С. 52–60.

[11] Трушакова Н. А. Судебно-почерковедческая экспертиза на современном этапе: проблемные вопросы и пути их решения // Вестник Московского университета МВД России. 2018. С. 103–105.

[12] Шлыков Д. А. Установление фактов нерукописного воспроизведения почерковых объектов: современное состояние и перспективы развития // Энциклопедия судебной экспертизы: науч.-практ. журнал: сетевое электронное издание. 2016. № 4 (11). С. 14–25.

[13] Ярощук И. А., Гриневич К. В. Проблемные вопросы экспертизы подписи как малообъемного почеркового объекта // Актуальные проблемы российского права. 2021. № 8 (129). С.141–150.

[14] Kruger D. The LongPenTM – The World's First Original Remote Signing Device // Journal of Forensic Sciences. 2010. Vol. 55. Issue 3. Pp. 795–800.

При улучшении данной технологии (что уже встречается на практике), указанные выше признаки будут утрачены и выявить фальсификацию реквизитов документов будет возможно только при очень внимательном исследовании экспертом всех элементов почерковых объектов и тщательном сличении нажимных характеристик.

Таким образом, в связи с применением графопостроительной техники, к которой можно отнести плоттер, 3D-принтер, роботизированную руку и станок с ЧПУ, как отмечено выше, в литературе стали появляться публикации на эту тему, однако данных работ явно недостаточно, что обусловливает большой интерес к полному изучению указанной проблемы, в том числе практикующими экспертами, и подтверждает необходимость разработки методики исследования почерковых объектов, выполненных с помощью современных технических устройств.

Список литературы

1. Белова Е. Н. Развитие криминалистической идентификации в судебно-почерковедческой экспертизе // Научно-практический журнал. 2015. № 3 (39). С. 172–175.

2. Бодров Н. Ф. Судебно-экспертное исследование записей, выполненных аппаратами имитации рукописных реквизитов // Теория и практика судебной экспертизы в современных условиях. Материалы VI Международной научно-практической конференции, посвященной памяти заслуженного юриста РФ, доктора юридических наук, профессора Юрия Кузьмича Орлова. Москва, 2017. С. 56–59.

3. Волчецкая Т. С. Криминалистическая ситуалогия. М., 1997. 248 с.

4. Панова Т. О., Миловидова О. Ю., Карпухина Е. С. Комплексное исследование имитации рукописных реквизитов (случай из экспертной практики) // Теория и практика судебной экспертизы. 2008. № 3 (11). С. 118–121.

5. Подкатилина М. Л. Проблемы назначения и производства судебных почерковедческих экспертиз // Вестник Университета имени О.Е. Кутафина. 2015. № 12. С. 116–121.

6. Пронин В. Н., Лесникова П. Г. Исследование подписи с целью установления факта ее выполнения с помощью технического средства – плоттера (случай из экспертной практики) // Вестник Нижегородского университета им. Н. И. Лобачевского. 2015. № 4. С. 162–165.

7. Светличный А. А. Использование метода моделирования для анализа терминологического аппарата криминалистики и общей теории судебной экспертизы // Национальные и международные тенденции и перспективы развития судебной экспертизы: сборник докладов Научно-практической конференции с международным участием, г. Нижний Новгород, 19–20 мая 2022 г. Нижний Новгород: ННГУ, 2022. С. 238–243.

8. Толстухина Т. В., Рыбалкин Н. А. Проблемы производства судебно-почерковедческой экспертизы малообъёмных почерковых объектов по электрофотографическим копиям // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 2. С. 52–60.

9. Толстухина Т. В., Светличный А. А., Панарина Д. В. Актуальные проблемы совершенствования методического обеспечения судебно-экспертной деятельности // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения) Сборник статей Международной научно-практической конференции. 2018. С. 288–292.

10. Толстухина Т. В., Устинова И. В. Формализация научного криминалистического и судебно-экспертного знания в условиях цифровизации // Криминалистика и судебная экспертиза: наука, практика, опыт: Всероссийский форум, 27–28 апреля 2021 г. М.: Московский университет МВД России имени В. Я. Кикотя, 2021. С. 109–113.

11. Трушакова Н. А. Судебно-почерковедческая экспертиза на современном этапе: проблемные вопросы и пути их решения // Вестник Московского университета МВД России. 2018. С. 103–105.

12. Шлыков Д. А. Установление фактов нерукописного воспроизведения почерковых объектов: современное состояние и перспективы развития // Энциклопедия судебной экспертизы: науч.-практ. журнал: сетевое электронное издание. 2016. № 4 (11). С. 14–25.

13. Ярощук И. А., Гриневич К. В. Проблемные вопросы экспертизы подписи как малообъемного почеркового объекта // Актуальные проблемы российского права. 2021. № 8 (129). С.141–150.

14. Kruger D. The LongPenTM – The World's First Original Remote Signing Device // Journal of Forensic Sciences. 2010. Vol. 55. Issue 3. Pp. 795–800.

Nikita A. Rybalkin
State Forensic Expert
Federal State Budgetary Institution Tula LSE
of the Ministry of Justice of Russia,
Assistant of the SEiTD Department
Tula State University
(Tula, Russia)
nikitarybalkin@rambler.ru

ACTUAL PROBLEMS OF FORENSIC EXAMINATION IN THE IDENTIFICATION OF DOCUMENTS MADE WITH THE HELP OF MODERN TECHNICAL MEANS

Abstract. The author considers topical issues of forensic handwriting expertise and forensic technical examination of documents – the execution of document details using modern technical means (graph-building equipment). The proposed article analyzes the main methods of identifying these handwriting objects, describes experimental studies of

their implementation, studies and characterizes the main modern technical means by which it is possible to perform handwriting objects. It should be noted that this work is one of the attempts to generalize forensic expert practice on the implementation of handwriting objects with the help of modern technical means, recommendations are made to experts when working with such objects, as well as issues related to the fact that such objects are the subject of a possible comprehensive study of handwriting experts and expert technicians. Subsequently, we believe that these recommendations should influence the training of future experts in these specialties.

Keywords: forensic handwriting examination, forensic technical examination of documents, technical means of document production, plotter, forensic examination, customs examination, customs documents.

УДК 340

Саргсян Аделина Арменовна
Кандидат юридических наук
преподаватель кафедры уголовного права и уголовно-процессуального права,
Институт права и политики,
Российско-Армянский университет
(г. Ереван, Республика Армения)
adelina-sargsyan@mail.ru

ИННОВАЦИОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ В ЮРИСПРУДЕНЦИИ

Аннотация. Одним из показателей успешной образовательной политики государства и залогом его процветания в настоящее время выступает раскрытие и использование инновационного потенциала системы высшего образования. Изменение вектора образовательного процесса с подхода, основанного на знаниях, на практико-ориентированный подход к результатам образовательного процесса, неизбежно привело к постановке проблемы технологий и методов обучения, которыми эта практикоориентированность будет достигаться. Эффективность современного образования зависит от сочетания классчического и инновационного подхода и его реализации в учебном процессе.

Цифровая трансформация социально-политической, экономической сферы государства неизбежно отражается и на образовательном процессе, требуя активное применение возможностей и достижений, в частности, электронных образовательных технологий. Создание единой образовательной платформы в дополнение к классическим методам обучения в системе высшего образования будет способствовать наиболее эффективному усвоению и восприятию учебного материала, повышению заинтересованности и активности студентов и наиболее полноценному усвоению компетенций, предусмотренных федеральными государственными образовательными стандартами и столь необходимых непосредственно в профессиональной деятельности. Отрыв обучающихся от практической деятельности, наличие преддипломной и образовательной практики, предусмотренных соответствующими стандартами и учебными планами, не позволяют в должной мере достигнуть наивысшей степени эффективности юридического образования, в то время как отмеченное успешно может быть восполнено посредством использования инновационных образовательных (цифровых) технологий, таких как внедрение цифровой реальности в учебный процесс, моделирование, проектирование, виртуальные юридические клиники. Интересным представляется использование в образовательном процессе видеороликов обучающего характера, предполагающих развитие аналитического и критического мышления студентов. Отмеченные направления развития в своей совокупности способствуют развитию потенциала обучающихся и совершенствованию системы высшего образования. Новейшие образовательные

технологии (в том числе, электронные), требуют и соответствующей подготовки специалистов, обладающих познаниями и способностью отвечать реалиям потребности и организовывать свою профессиональную преподавательскую деятельность с использование электронных образовательных технологий.

Ключевые слова: образование, образовательная политика, цифровизация, инновационные технологии, интерактивные методы обучения, виртуальная реальность, практико-ориентированный подход, компетенции.

Для цитирования:
Саргсян А. А. Инновационные образовательные технологии в юриспруденции // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 185–190.

В условиях нынешних реалий, стремления государств к постепенному переходу на цифровую трансформацию экономики, права, здравоохранения и иных сфер жизнедеятельности, закономерным является и подготовка образовательного пространства к процессам информатизации и цифровизации, созданию цифрового образовательного пространства и внедрению новейших технологий в образовательный процесс. Безусловно, речь идёт о сочетании традиционных и новейших (в том числе, цифровых) образовательных технологий, поскольку только лишь в этом случае можно достигнуть наибольшего уровня процветания высшей школы.

На этапе цифровизации образования важное значение приобретает применение в учебном процессе электронных образовательных технологий, особенностью которых является, в частности, их интерактивный характер, способствующий наиболее эффективной реализации предусмотренных образовательными стандартами компетенций. Таким образом, на пути к цифровой трансформации образования важное значение приобретают именно электронные образовательные технологии.

В научной литературе электронные образовательные технологии (ресурсы) трактуются по-разному: «образовательные, представленные в электронно-цифровой форме и включающие в себя структуру, предметное содержание и метаданные о них»[1]; «совокупность электронных учебных средств, необходимых и достаточных для обеспечения учебного процесса в пределах методической системы обучения»[2]; «полноценные и наиболее

[1] Вайндорф-Сысоева М. Е., Грязнова Т. С. Педагогические аспекты разработки электронного образовательного ресурса практикующим педагогом: краткий путеводитель: учеб.-метод. пособие М. : ИИУ МГОУ, 2014. С. 6.

[2] Макаров С. И. Методические основы создания и применения образовательных электронных изданий (на примере курса математики) : автореф. дис. ... д-ра пед. наук : 13.00.02. Ин-т общего среднего образования Рос. акад. образования. М., 2003. С. 14.

значимые средства информатизации образования»[3]. Цифровая трансформация образования предполагает активную вовлечённость всех участников образовательного процесса в работу с цифровыми технологиями.

Стратегическими задачами цифровой трансформации образования высшей школы является: создание современной и безопасной цифровой образовательной среды, обеспечивающей высокое качество и доступность образования, внедрение в рамках высшего образования новых методов обучения и воспитания, обеспечивающих вовлечённость обучающихся в образовательный процесс, разработка адаптивных, практико-ориентированных и гибких образовательных программ[4]. Таким образом, цифровая трансформация современного юридического образования предполагает создание цифрового пространства, сочетающего в себе классические подходы к обучению и цифровые образовательные инструменты, разработку электронных учебных курсов и др.

Что же касается методик повышения качества образования путём электронных технологий, то здесь необходимо выделить некоторые важные особенности:

– электронные технологии помогают реализовывать инновационные педагогические технологии;

– электронные технологии способствуют полноценному развитию личности в индивидуальном аспекте;

– появляется возможность организации эффективной коллективной образовательной деятельности;

– благодаря электронному обучению, происходит расширение информационного пространства;

– повышается свободный доступ к информационным потокам;

– появляется возможность создания инновационного средства оценки результатов образовательной деятельности[5].

Своеобразной электронной образовательной технологией, способствующей усвоению теоретического материала, развитию профессиональных навыков обучающихся является создание единой образовательной платформы, на которой, в частности, преподаватели будут размещать разработанные ими учебные онлайн-курсы по той или иной дисциплине либо спецкурсу. Электронные образовательные ресурсы способны повысить результативность и качество учебного процесса, эффективность

[3] Гриншкун В. В. Развитие интегративных подходов к созданию средств информатизации образования: автореф. дис. ... д-ра пед. наук: 13.00.02. Московский городской пед. ун-т. М., 2004. С. 3.

[4] Гафиатулина Н. Х., Самыгин С. И. Вектор разработки образовательнойпарадигмы в контексте персонифицированного образования в эпоху развитияцифровыхтехнологий // Образование и молодежь в условиях цифровой экономики будущего. Материалы. 2020. С. 17–21.

[5] Евтушенко К. Д. Дидактические требования к современному электронному обучению в вузе // Известия Тульского государственного университета. Педагогика. 2015. Вып. 1. С. 51–55.

усвоения студентами преподносимого материала.

Необходимо указать также на возможность внедрения в учебный процесс цифрового образовательного видеоресурса, представляющего собой современную электронную образовательную технологию интерактивного характера. Сюда следует отнести как разработку научно-педагогическими кадрами авторских онлайн-курсов, коротких видеороликов обучающего характера, способствующих закреплению студентами пройденного материала. «Ожидается, что основным форматом подачи информации в курсах станет видеолекция. Идеологи онлайн-обучения подчеркивают: современного студента сложно замотивировать на прочтение больших объемов текста, да и качество восприятия такой информации оставляет желать лучшего»[6].

Следующим видом электронных образовательных технологий, представляющий собой инновации в юридическом образовании, являются такие категории, как «виртуальная реальность», «интерактивные симуляторы», «виртуальные тренажеры», «диалоговые тренажеры», внедрение которых также заслуживает внимания передовых высших учебных заведений. Создание виртуальной реальности в образовательных организациях позволит обучающимся погрузиться в атмосферу действительной профессиональной деятельности, что позитивным образом скажется на уровне и качестве их подготовки. Посредством данной образовательной технологии становится возможным применить методы моделирования и проектирования, что в своей совокупности активизирует эффективность учебного процесса. На сказанное подталкивает и имеющийся положительный зарубежный опыт. Термин «симуляционное обучение» пришел в юриспруденцию из таких отраслей, как медицина и авиация[7]. М. А. Горшков и А. Л. Колыш указывают, что симуляционное медицинское обучение в период новейшей истории опиралось на успехи симуляционного тренинга в других отраслях, связанных с риском для жизни практического обучения в реальных условиях, прежде всего – в авиации[8]. Отмеченное, в особенности, применимо к дисциплинам уголовно-правовой направленности.

Таким образом, разработки в сфере виртуальной реальности как стремительными темпами развивающейся новейшей компьютерной технологии, оказывают благоприятное воздействие на

[6] Миляева Е. Зачёт онлайн (УрФУ вошёл в национальную платформу открытого образования) // Российская газета [Электронный ресурс]. 2015, 7 июля. URL: http://www.rg.ru/2015/07/16/regurfo/zachet.html

[7] Сейтаева Ж. С., Балашов Р. С. Симуляционное обучение в практической подготовке сотрудников правоохранительных органов: учебно-практическое пособие. Косшы: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2020. С. 6.

[8] Симуляционное обучение в медицине / РОСОМЕД – Российское о-во симуляционного обучения в медицине; сост. Горшков М. Д.; под ред. Свистунова А. А., М.: Изд-во Первого МГМУ им. И. М. Сеченова, 2013. С. 189.

образовательный процесс. Речь может идти о виртуальном юридическом пространстве, виртуальных юридических лабораториях. Подобный опыт уже давно имеется и практикуется в медицинском образовании при создании виртуальных симуляторов для обследования пациентов и проведения с ними различных хирургических манипуляций.

Использование возможностей виртуальной реальности на юридических факультетах имеет такие преимущества, как предоставление возможности моделирования криминалистических полигонов, виртуальных мест совершения преступлений (преимуществом является моделирование того или иного места совершения преступления в зависимости от изучаемой и отрабатываемой студентами темы), с последующим производством ряда следственных действий, что в своей совокупности будет способствовать систематической отработке студентами практических навыков профессиональной деятельности. Даже в процессе прохождения студентами производственной и преддипломной практики в Следственных органах России и Армении, маловероятным представляется участие студентов при расследовании таких преступлений (и, соответственно, присутствие на местах преступления), как террористические акты, взрывы, авиационные катастрофы и т. д., в то время как в рамках виртуальной реальности такая возможность имеется. Наличие таких виртуальных полигонов, как место совершения убийства, место дорожно-транспортного происшествия, место авиакатастрофы, место террористического акта позволит студентам отработать на практике ряд разделов криминалистической методики, техники и тактики, в особенности, трасологии (в частности отработки тактики поиска оставленных на месте преступления следов). Помимо отмеченного, в случае максимальной «оснащённости» виртуальной криминалистической площадки, имеется также возможность брать, осматривать имеющиеся предметы. Таким образом, подобные виртуальные криминалистические пространства предоставляют широкие возможности для поиска следов преступления, отработки студентами навыков выдвижения следственных версий.

Создание всевозможных ситуаций, имитирующих приближенные к натуральным условиям, написание специальных симуляционных сценариев открывают новые горизонты для практической подготовки и повышения квалификации сотрудников правоохранительных органов[9].

Идея о проведении подобного тренинга по моделированию борьбы с торговлей людьми была озвучена руководством Генеральной прокуратуры Республики Казахстан на встрече с Генеральным секретарем ОБСЕ в 2017 году, после показа

9 Сейтаева Ж. С., Балашов Р. С. Симуляционное обучение в практической подготовке сотрудников правоохранительных органов: учебно-практическое пособие. Косшы: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2020. С. 5.

видеоролика, созданного Центром передового опыта для подготовки итальянских полицейских карабинеров, расположенного в г. Виченце (Италия), который первым инсценировал преступления о рабстве. После этого Академия правоохранительных органов и ОБСЕ инициировала организацию симуляционных тренингов по борьбе с торговлей людьми с привлечением представителей 17 стран Европы и Азии.

Подводя итоги, следует отметить, что внедрение электронных новейших образовательных технологий в учебный процесс, оперативное использование современных возможностей, инновационных технологий – являются требованиями современного качественного образования и залогом подготовки действительно профессиональных юридических кадров.

Список литературы

1. Вайндорф-Сысоева М. Е., Грязнова Т. С. Педагогические аспекты разработки электронного образовательного ресурса практикующим педагогом: краткий путеводитель: учеб.-метод. пособие М.: ИИУ МГОУ, 2014. 64 с.

2. Гафиатулина Н. Х., Самыгин С. И. Вектор разработки образовательнойпарадигмы в контексте персонифицированного образования в эпоху развития цифровых технологий // Образование и молодежь в условиях цифровой экономики будущего. Материалы. 2020. С. 17–21.

3. Гриншкун В. В. Развитие интегративных подходов к созданию средств информатизации образования: автореф. дис. ... д-ра пед. наук: 13.00.02. Московский городской пед. ун-т. М., 2004. 48 с.

4. Евтушенко К. Д. Дидактические требования к современному электронному обучению в вузе // Известия Тульского государственного университета. Педагогика. 2015. Вып. 1. С. 51–55.

5. Макаров С. И. Методические основы создания и применения образовательных электронных изданий (на примере курса математики) : автореф. дис. ... д-ра пед. наук: 13.00.02. Ин-т общего среднего образования Рос. акад. образования. М., 2003. 39 с.

6. Сейтаева Ж. С., Балашов Р. С. Симуляционное обучение в практической подготовке сотрудников правоохранительных органов: учебно-практическое пособие. Косшы: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2020. 90 с.

7. Симуляционное обучение в медицине / РОСОМЕД – Российское о-во симуляционного обучения в медицине; сост. Горшков М. Д.; под ред. Свистунова А. А., М.: Изд-во Первого МГМУ им. И. М. Сеченова, 2013. 287 с.

Adelina A. Sargsyan
Candidate of Law Sciences
Lecturer of Chair of Criminal Law and Criminal Procedure
of Institute of Law and Politics
Russian-Armenian University
(Yerevan, Republic of Armenia)
adelina-sargsyan@mail.ru

INNOVATIVE EDUCATIONAL TECHNOLOGIES IN JURISPRUDENCE

Abstract. One of the indicators of successful educational policy of the state and the guarantee of its prosperity at the present time is the disclosure and use of the innovative potential of the higher education system. Changing the vector of the educational process from knowledge-based approach to practice-oriented approach to the results of the educational process inevitably led to the statement of the problem of technologies and teaching methods, which will achieve this practice-oriented approach. The effectiveness of modern education depends on the combination of the classroom and innovative approach and its implementation in the educational process.

Digital transformation of socio-political, economic sphere of the state is inevitably reflected in the educational process, requiring the active use of opportunities and achievements, in particular, electronic educational technologies. Creation of a single educational platform in addition to classical teaching methods in the system of higher education will contribute to the most effective assimilation and perception of educational material, increase students' interest and activity and the fullest assimilation of competencies provided by the federal state educational standards and so necessary directly in professional activity. The separation of students from practical activity, the presence of pre-degree and educational practice, provided by the relevant standards and curricula do not allow to achieve the highest degree of effectiveness of legal education, while the noted can be successfully made up through the use of innovative educational (digital) technologies, such as the introduction of digital reality in the learning process, modeling, design, virtual legal clinics. Interesting is the use of educational videos in the educational process, involving the development of analytical and critical thinking of students. The above-mentioned areas of development in their entirety contribute to the development of students' potential and improvement of higher education system. The latest educational technologies (including electronic), require appropriate training of specialists with the knowledge and ability to meet the realities of the needs and organize their professional teaching activities with the use of electronic educational technologies.

Keywords: education, education policy, digitalization, innovative technologies, interactive teaching methods, virtual reality, practice-oriented approach, competencies.

УДК 347.965

Сентябова Анна Владимировна
Ассистент кафедры теории и истории государства и права
Удмуртский государственный университет
(г. Ижевск, Российская Федерация)
sentyabovaanna@yandex.ru

РАЗВИТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В АДВОКАТСКОЙ ДЕЯТЕЛЬНОСТИ ПРИ РЕШЕНИИ НАСУЩНЫХ ПРОБЛЕМ

Аннотация. В статье рассмотрено практическое использование информационных технологий для решения проблем адвокатской деятельности, а также положительные и отрицательные стороны внедрения цифровых технологий. Обосновывается неизбежность их применения в адвокатском сообществе.

Ключевые слова: информационные технологии, цифровые технологии, права граждан, конфиденциальность, цифровая среда.

Для цитирования:
Сентябова А. В. Развитие информационных технологий в адвокатской деятельности при решении насущных проблем // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 191–194.

В России после опубликования Указа Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[1] и программы «Цифровая экономика Российской Федерации»[2] наступила эпоха информационных технологий, что не могло не отразиться на деятельности адвокатов. Юридическая общественность стала активно обсуждать вопросы применения информационных технологий. Так в настоящий момент запущена в работу Комплексная информационная система адвокатуры России (КИС АР – далее Система), которая была создана для усиления гарантии защиты прав граждан с помощью автоматического режима распределения дел между адвокатами; обмена документами со

[1] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_216363/ (дата обращения: 14.05.2023).

[2] Постановление Правительства РФ от 02.03.2019 № 234 (ред. от 13.05.2022) «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации» (вместе с «Положением о системе управления реализацией национальной программы “Цифровая экономика Российской Федерации”»)» // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_319701/ (дата обращения: 14.05.2023).

следствием и судом; сбора информации в электронном виде; участия в судебных заседаниях онлайн; обеспечения возможности конфиденциального общения с доверителем. Помимо этого, система способна:

– исключить человеческий фактор при распределении адвокатам поручений на оказание квалифицированной юридической помощи по назначению;

– препятствовать «угодным» адвокатам;

– сократить время от принятия органом решения до назначения определённого защитника;

– без выходных и круглосуточно заменить адвоката за 1–3 минуты;

– обеспечить равноправие адвокатов при распределении поручений на оказание юридической помощи по назначению (при «ручном» распределении заявок органов о назначении защитника нарушался принцип равноправия адвокатов, т. к. на практике встречались случаи использования отдельными адвокатами личных связей с работниками судебных и правоохранительных органов для привлечения их к участию по делам по назначению, что не соответствовало ст. 50, 51 УПК РФ[3], а также приводило к системным нарушениям прав граждан на получение квалифицированной юридической помощи);

– обеспечить получение достоверных статистических сведений;

– реализовать принцип равномерности распределения поручений (система распределяет поручение в первую очередь тому дежурному адвокату, у которого имеется наименьший показатель ранее полученных дел).

Безусловно, система позволяет взаимодействовать в цифровой среде со всеми государственными органами Российской Федерации и имеет множество положительных моментов, но стоит отметить, что также имеются и риски, связанные с использованием цифровых ресурсов[4]. Например, разный уровень компетентности владения и использования информационных технологий среди адвокатского сообщества; необходимость обеспечения и применения дополнительных способов защиты персональных и конфиденциальных данных в рамках информационных систем; трудности при переходе на системы электронного взаимодействия между государственными системами и адвокатскими палатами.

Также следует отметить, что стабильный Интернет имеется не везде, что может негативно сказываться на реализации прав

[3] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 28.04.2023) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 14.05.2023).

[4] Тарасов А. В., Джаримок В. В. Процессуальные и организационные аспекты использования цифровых технологий в деятельности адвоката: проблемы и перспективы // Молодой ученый. 2022. № 25 (420). С. 148–151.

граждан на получение квалифицированной юридической помощи.

Помимо этого, немаловажно отметить, что с развитием цифровых технологий возрастает и число мошеннических действий, заключающихся в использования персональных данных в корыстных целях. На сегодняшний день имеется ФЗ «О персональных данных»[5], который закрепляет, что обработка персональных данных возможна только лишь с согласия субъекта персональных данных. При оформлении адвокатского запроса в целях оказания юридической помощи доверителю адвокат обязан взять письменное согласие с подзащитного. Также закон позволяет отозвать согласие на обработку персональных данных в любое время, но также и предусмотрены случаи, когда оператор может продолжить работу с личными инфоматериалами субъекта даже при отзыве своего согласия. Как мы видим юридическая незащищенность индивидуума остается очевидной.

На основании вышеизложенного можно сделать вывод о том, что процесс внедрения цифровых технологий в адвокатскую деятельность закономерен, но требует значительных доработок. Думается, что необходима разработка концепции развития системы законодательства в области защиты прав человека в сфере цифровых технологий, а также ужесточение ответственности для лиц, имеющих доступ к персональным данным, и закрепление на законодательном уровне требований к хранению персональных данных и работе с ними в информационных системах адвокатуры.

Список литературы

1. Тарасов А. В., Джаримок В. В. Процессуальные и организационные аспекты использования цифровых технологий в деятельности адвоката: проблемы и перспективы // Молодой учёный. 2022. № 25 (420). С. 148–151.

Anna V. Sentyabova
Assistant of the Department of Theory and History of State and Law
Udmurt State University
(Izhevsk, Russian Federation)
sentyabovaanna@yandex.ru

DEVELOPMENT OF INFORMATION TECHNOLOGIES IN ADVOCACY IN SOLVING CURRENT PROBLEMS

[5] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 14.05.2023).

Abstract. The article discusses the practical use of information technology to solve the problems of advocacy, as well as the positive and negative aspects of the introduction of digital technologies and the inevitability of their use in the legal community.

Key words: information technologies, digital technologies, citizens' rights, privacy, digital environment.

УДК 343.98

Смахтин Евгений Владимирович
Доктор юридических наук, профессор,
профессор кафедры криминалистики
Уральский государственный юридический университет имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
smaxt@yandex.ru

Льянов Муса Микаилович
Преподаватель кафедры организации расследования
преступлений и судебных экспертиз
Тюменский институт повышения квалификации сотрудников МВД России
(г. Тюмень, Российская Федерация)
musa-lyanov@mail.ru

СОКРЫТИЕ ЭЛЕКТРОННО-ЦИФРОВЫХ СЛЕДОВ КАК СПОСОБ ПРОТИВОДЕЙСТВИЯ РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЯ

Аннотация. Одним из актуальных вопросов расследования преступлений в сфере информационных технологий является установление скрытых электронно-цифровых следов. Как показывает анализ теоретических положений и правоприменительной практики, существует множество вариантов противодействия расследованию преступления соответствующим образом. В рамках данной научной статьи были выявлены основные способы сокрытия электронно-цифровых следов, к числу которых отнесены искажение, уничтожение и маскировка. Предложены оптимальные варианты по установлению фактов применения каждого из рассмотренных видов сокрытия.

Ключевые слова: электронно-цифровой след, электронный носитель информации, информационные технологии, сокрытие следов, маскировка, искажение, уничтожение.

Для цитирования:
Смахтин Е. В., Льянов М. М. Сокрытие электронно-цифровых следов как способ противодействия расследованию преступлений // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 195–203.

Согласно докладу Президента России В. В. Путина на Расширенном заседании коллегии МВД России 20 марта 2023 года, одним из приоритетных направлений работы правоохранительных органов является борьба с преступлениями с использованием информационных

технологий[1]. В связи с распространённостью информационных технологий появляются новые способы совершения преступлений, обеспечивающие анонимность их исполнителей и иных участников. При этом особое значение приобретает установление (обнаружение) способов сокрытия таких преступлений, а также лиц их совершивших.

В теории криминалистики выделяют множество способов сокрытия следов. Для примера можно привести утаивание, уничтожение, маскировку, фальсификацию, искажение информации и её носителей, а также смешанные способы[2]. Анализ правоприменительной практики показывает, что сокрытие электронно-цифровых следов в деятельности заинтересованных лиц, как правило, совершается при помощи искажения, уничтожения и маскировки информации, содержащейся в электронных носителях и имеющей значение для раскрытия и расследования уголовного дела. Исходя из особенностей способов сокрытия электронно-цифровых следов, можно установить фактические обстоятельства соответствующих действий, а также предложить пути преодоления указанного противодействия расследованию преступлений.

Рассмотрим выделенные способы сокрытия электронно-цифровых следов более подробно.

1) Искажение информации, содержащейся в электронно-цифровых следах, заключается в таком умышленном изменении информации о преступной деятельности в электронных носителях, которое не позволяет установить изначальный смысл обнаруженной информации. Данный способ сокрытия электронно-цифровых следов проявляется в применении участниками преступлений всевозможных редакторов текстовых, графических, аудио- и видеофайлов. Так, к примеру, могут быть использованы программы для искажения голоса при совершении мошенничества с использованием средств связи, при пересылке аудиосообщений. Могут вноситься изменения в графические и видеофайлы, например, для искажения информации о времени, месте совершения преступления и т. п.[3] Как отмечается в исследовании А. Л. Осипенко, искажение электронно-цифровых следов

[1] Расширенное заседание коллегии МВД // Президент России: официальный сайт [Электронный ресурс]. 2023, 20 марта. URL: http://kremlin.ru/events/president/transcripts/70744 (дата обращения 27.03.2023)

[2] Белкин Р. С. Курс советской криминалистики в 3-х томах. Т. 3 М.: Изд-во Академии МВД СССР, 1979. 407 с.; Бибиков А. А. Способы сокрытия следов преступлений, связанных с нарушением правил дорожного движения и эксплуатации транспортных средств // Известия ТулГУ. Экономические и юридические науки. 2016. №4–2. С. 61–71; Карагодин В. Н. Способы сокрытия преступления, их криминалистическое значение, методы распознавания и преодоления: автореф. дис. ... канд. юрид. наук. Свердловск, 1982. 19 с.

[3] Малышкин П. В. Способы сокрытия преступлений, совершаемых с применением информационных компьютерных технологий // Вестник МГУ. 2014. Т. 24. № 4. С. 42–47. DOI 10.15507/VMU.024.201403.042.

возможно и путём дистанционного подключения к компьютерным сетям, которое осуществляется во время хакерских атак[4].

На распространённость применения данного способа сокрытия электронно-цифровых следов указывает, в частности, и анализ судебной практики. Так, к примеру, в Приговоре Сызранского городского суда Самарской области от 9 февраля 2015 г. в целях конспирации и сокрытия фактов сбыта наркотических средств, подозреваемая использовала функции программного обеспечения сотового телефона, предусматривающего искажение голоса с женского на мужской[5]. В Приговоре Сургутского городского суда Ханты-Мансийского автономного округа – Югра от 10 декабря 2019 г. указывается, что подозреваемым использовалось специальное программное обеспечение, с помощью которого он менял свой голос на женский при связи с потерпевшим[6].

На наш взгляд, преодоление подобного способа сокрытия электронно-цифровых следов возможно путём фиксации сведений о последних изменениях файлов, а также перечня программного обеспечения на осматриваемых аппаратно-программных технических средствах, которые имеют в своём функционале возможность редактирования информации. Зафиксированные в протоколе осмотра сведения необходимо соотносить с другими имеющимися доказательствами по уголовному делу, что позволит установить факт искажения электронно-цифровых следов.

2) Второй способ сокрытия информации, содержащейся в электронно-цифровых следах, заключается в её уничтожении. Он предполагает множество вариантов своего исполнения. Так, в научной статье А. А. Белякова и В. Ю. Иванова указывается, что электронно-цифровые следы могут быть уничтожены под воздействием вредоносного программного обеспечения[7]. В исследовании А. В. Ширяева, помимо уничтожения информации при помощи вредоносных программ, обозначена возможность достижения такого же эффекта путём внесения изменений непосредственно в электронное устройство либо посредством физического уничтожения электронного носителя информации[8]. На наш взгляд, данный способ сокрытия электронно-цифровых следов можно разделить на

[4] Осипенко А. Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс // Научный вестник Омской академии МВД России. 2009. № 4 (35). С. 31–34.

[5] Приговор Сызранского городского суда Самарской области от 9 февраля 2015 г. по делу № 1-55/2015 (1-742/2014).

[6] Приговор Сургутского городского суда Ханты-Мансийского автономного округа-Югра от 10 декабря 2019 г. по делу № 1-1223/2019.

[7] Беляков А. А., Иванов В. Ю. Тактические особенности работы с электронно-цифровыми следами на месте происшествия // Криминалистика: вчера, сегодня, завтра. 2021. № 4 (20). С. 17–26. DOI 10.24412/2587-9820-2021-4-17-26.

[8] Ширяев А. В. Способы сокрытия следов мошенничества в сфере компьютерной информации // Проблемы правовой и технической защиты информации. 2020. № 8. С. 119–127.

следующие категории: физическое и программное уничтожение.

К примеру, возможно удаление файлов, содержащих информацию, имеющую значение для расследования уголовного дела, форматирование электронного носителя информации, на котором содержится электронно-цифровой след, физическое уничтожение электронного носителя информации и (или) аппаратно-программного технического средства, уничтожение электронно-цифровых следов в электронных сетях и т. д. Одновременно с этим, лицо, совершающее либо совершившее преступление, может не понимать принципы работы электронных носителей информации, записи и хранения данных. В связи с этим им может быть избран неэффективный способ сокрытия электронно-цифровых следов, в том числе и под воздействием внезапно возникших факторов, например появления при совершении преступления сотрудников правоохранительных органов.

Так, физическое уничтожение электронного носителя информации или аппаратно-программных технических средств является весьма эффективным способом сокрытия электронно-цифровых следов, однако уничтожение, например, мобильного телефона с содержащейся на нём информацией может не привести к ожидаемому эффекту в связи с сохранностью встроенного в него электронного носителя. Удаление файлов также может быть неэффективным в случае, если при сокрытии электронно-цифрового следа не были учтены особенности записи и хранения отдельно взятого электронного носителя информации. Например, на магнитных носителях информации в отдельных случаях удалённые файлы могут быть восстановлены, если на их ферромагнитное покрытие не была записана иная информация.

В указанных случаях у следователя имеется возможность восстановить криминалистически важную информацию при помощи назначения различных видов судебной компьютерной экспертизы. К примеру, в приговоре Клинцовского городского суда Брянской области от 10 июля 2020 г. указывается, что при проведении экспертизы на карте памяти флеш-накопителя были обнаружены в удалённом виде 4 видеофайла, которые содержали в себе информацию об обстоятельствах уголовного дела[9]. В Приговоре Железнодорожного районного суда г. Пензы Пензенской области от 6 ноября 2019 г. имеется указание на восстановление в памяти ноутбука графических и текстовых файлов, которые содержали сведения об эпизодах сбыта наркотических средств[10].

3) Маскировка электронно-цифровых следов связана с возможностями, предлагаемыми стеганографией, то есть способом сокрытия самого факта существования и передачи информации, и криптографии, то есть сокрытия содержания передаваемой либо

[9] Приговор Клинцовского городского суда Брянской области от 10 июля 2020 г. по делу № 1-27/2020.

[10] Приговор Железнодорожного районного суда г. Пензы Пензенской области от 6 ноября 2019 г. по делу № 1-383/2019.

хранящейся информации. Способ криптографии в условиях развития компьютерных технологий получил широкое распространение в противоправной деятельности. Он используется при совершении широкого круга преступлений общеуголовной, экономической и террористической направленности[11]. При использовании криптографии могут быть задействованы возможности кодирования аппаратно-программных технических средств, шифрование переносных электронных носителей информации, например, ограничение возможности воспроизведения информации на электронном носителе при помощи других аппаратно-программных технических средств, использование шифрования, встроенного в мессенджеры и т. п.[12] Использование криптографических методов при совершении преступлений значительно усложняет процесс расследования и получения доступа к криминалистически значимой информации. В отдельных случаях, при установлении фактов применения криптографии по уголовному делу могут быть использованы возможности различных судебных экспертиз, так как для расшифровки подобной информации требуется задействование специальных познаний в области компьютерных технологий и информационной безопасности.

Ещё одним вариантом реализации маскировки электронно-цифровых следов является стеганография. Стеганография может применяться для сокрытия следов преступлений, когда подозреваемому необходимо утаить сам факт существования электронно-цифрового следа[13]. Так, информация может быть спрятана, на первый взгляд, в абсолютно обыкновенных файлах, так называемых «контейнерах»[14]. На актуальность данного способа сокрытия преступлений отмечает А. Б. Смушкин в работе «Концепция «электронных» следственных действий», указывая на необходимость участия в следственных действиях специалиста, имеющего в своём распоряжении программно-аппаратные комплексы, что, на наш взгляд, позволит выявить скрытые электронно-цифровые следы и информацию о преступлении[15].

Выделяют такие типы стеганографии как лингвистическая, предполагающая сокрытие информации в тексте, сообщениях и т.

---

[11] Зиновьева Н. С. Криминалистическое значение диагностики криптографически защищенных объектов // Юристъ-Правоведъ. 2019. № 3 (90). С. 142–146.

[12] Рудых А. А. Криптография и криминалистика: современные проблемы и возможные пути решения // Вестник Восточно-Сибирского института МВД России. №2 (89). 2019. С. 203–212.

[13] Зиновьева Н. С. К вопросу о месте криптографии и стеганографии в криминалистической науке // Гуманитарные, социально-экономические и общественные науки. 2019. № 2. С. 87–89. DOI 10.23672/SAE.2019.2.26715.

[14] Компьютерная стеганография / В. Г. Грибунин [и др.]. М: Солон-Р, 2002. 240 с.

[15] Смушкин А. Б. Концепция «электронных» следственных действий // Криминалистика: вчера, сегодня, завтра. 2021. № 3 (19). С. 165–172.

п.[16]; цифровая[17], то есть скрытное внедрение информации в графические, аудио- и видеофайлы. При этом наиболее эффективным форматом для целей стеганографии, согласно исследованию, проведённому А. В. Питолиным, Ю. П. Преображенским и О. Н. Чопоровым, являются цифровые изображения[18]. Данный способ сокрытия информации о совершённом преступлении с использованием информационных технологий является наиболее результативным, так как электронно-цифровые следы в этом случае незаметны без подробного осмотра предметов. Зачастую, для следователя может быть неожиданным использование данного способа сокрытия следов преступления и, в итоге, он может не обратить внимания на важную для расследования информацию.

А. А. Кривцов и В. Н. Будко в своём исследовании также отмечают эффективность данного способа сокрытия следов преступлений[19]. При этом авторы обращают внимание на то, что для большей защищённости информации от несанкционированного доступа стеганография используется не в каждом изображении, а выборочно, по определённой последовательности. Для стороннего наблюдателя такой выбор изображений может выглядеть как устроенный в случайном порядке. В связи с этим, при подготовке к следственным действиям необходимо учитывать личность подозреваемого, наличие у него навыков и знаний в области стеганографии, а также его профессиональную деятельность, предшествующую совершению преступления. При наличии информации о навыках подозреваемого в области стеганографии следует обращать внимание, например, на размеры осматриваемых на электронных носителях информации файлов, наличие лишних пробелов, повторяющейся последовательности символов в текстовых документах и т. п. Кроме того, следует учитывать возможность выборочной стеганографии, факт которой необходимо проверять путём выявления закономерностей в обнаруженной информации для каждого конкретного случая.

Подводя итоги рассмотренной в настоящей статье проблеме, отметим, что исследование особенностей сокрытия электронно-цифровых следов имеет большое значение для совершенствования процесса их обнаружения. В связи с этим считаем, что способы сокрытия электронно-цифровых следов возможно классифицировать по механизму

[16] Priya K. Steganography Techniques Used to Hide the Information // Journal of Computer Engineering. 2018. Pp. 16–19.

[17] Абазина Е. С., Ерунов А. А. Цифровая стеганография: состояние и перспективы // Системы управления, связи и безопасности. 2016. № 2. С. 182–201

[18] Питолин А. В., Преображенский Ю. П., Чопоров О. Н. Исследование возможностей использования стеганографических способов защиты информации // Моделирование, оптимизация и информационные технологии. 2018. Т. 6. № 2 (21). С. 336–353.

[19] Кривцов А. А., Будко В. Н. Повышение стойкости стеганографических систем путем встраивания информации в существенные элементы изображений // Защита информации. Инсайд. 2006. № 4 (10). С. 81–83.

воздействия на них:

1) Искажение информации, содержащейся в электронно-цифровых следах.

2) Уничтожение информации, содержащейся в электронно-цифровых следах:

– физическое уничтожение электронного носителя информации или электронного устройства;

– программное уничтожение информации без повреждения электронного носителя, в том числе, при помощи вредоносного программного обеспечения.

3) Маскировка информации, содержащейся в электронно-цифровых следах:

– криптография;

– стеганография.

Во всех случаях при осмотре электронно-цифрового следа принимает участие специалист. После фиксации результатов осмотра в протоколе и получения заключения специалиста, следователь принимает решение о назначении различных судебных компьютерных и иных экспертиз, позволяющих установить факт противодействия расследованию путём искажения, уничтожения или маскировки информации, имеющей значение для расследования.

Список литературы

1. Абазина Е. С., Ерунов А. А. Цифровая стеганография: состояние и перспективы // Системы управления, связи и безопасности. 2016. № 2. С. 182–201.

2. Белкин Р. С. Курс советской криминалистики в 3-х томах. Т. 3 М.: Изд-во Академии МВД СССР, 1979. 407 с.

3. Беляков А. А., Иванов В. Ю. Тактические особенности работы с электронно-цифровыми следами на месте происшествия // Криминалистика: вчера, сегодня, завтра. 2021. № 4 (20). С. 17–26. DOI 10.24412/2587-9820-2021-4-17-26.

4. Бибиков А. А. Способы сокрытия следов преступлений, связанных с нарушением правил дорожного движения и эксплуатации транспортных средств // Известия ТулГУ. Экономические и юридические науки. 2016. №4–2. С. 61–71.

5. Зиновьева Н. С. К вопросу о месте криптографии и стеганографии в криминалистической науке // Гуманитарные, социально-экономические и общественные науки. 2019. № 2. С. 87–89. DOI 10.23672/SAE.2019.2.26715.

6. Зиновьева Н. С. Криминалистическое значение диагностики криптографически защищенных объектов // Юристъ-Правоведъ. 2019. № 3 (90). С. 142–146.

7. Карагодин В. Н. Способы сокрытия преступления, их криминалистическое значение, методы распознавания и преодоления: автореф. дис. ... канд. юрид. наук: 12.00.09. Свердловск, 1982. 19 с.

8. Компьютерная стеганография / В. Г. Грибунин [и др.]. М: Солон-Р, 2002. 240 с.

9. Кривцов А. А., Будко В. Н. Повышение стойкости стеганографических систем путем встраивания информации в существенные элементы изображений // Защита информации. Инсайд. 2006. № 4 (10). С. 81–83.

10. Малышкин П. В. Способы сокрытия преступлений, совершаемых с применением информационных компьютерных технологий // Вестник МГУ. 2014. Т. 24. № 4. С. 42–47. DOI 10.15507/VMU.024.201403.042.

11. Осипенко А. Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс // Научный вестник Омской академии МВД России. 2009. № 4 (35). С. 31–34.

12. Питолин А. В., Преображенский Ю. П., Чопоров О. Н. Исследование возможностей использования стеганографических способов защиты информации // Моделирование, оптимизация и информационные технологии. 2018. Т. 6. № 2 (21). С. 336–353.

13. Рудых А. А. Криптография и криминалистика: современные проблемы и возможные пути решения // Вестник Восточно-Сибирского института МВД России. №2 (89). 2019. С. 203–212.

14. Смушкин А. Б. Концепция «электронных» следственных действий // Криминалистика: вчера, сегодня, завтра. 2021. № 3 (19). С. 165–172.

15. Ширяев А. В. Способы сокрытия следов мошенничества в сфере компьютерной информации // Проблемы правовой и технической защиты информации. 2020. № 8. С. 119–127.

16. Priya K. Steganography Techniques Used to Hide the Information // Journal of Computer Engineering. 2018. Pp. 16–19.

Evgeny V. Smakhtin
PhD (Law), Professor, Professor of the Department of Criminology
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
smaxt@yandex.ru

Musa M. Lyanov
Teacher of the Department of Organization of
Crime Investigation and Forensic Examinations
Tyumen Institute for Advanced Training of Employees
of the Ministry of Internal Affairs of Russia
(Tyumen, Russian Federation)
musa-lyanov@mail.ru

CONCEALMENT OF ELECTRONIC-DIGITAL TRACES AS A WAY TO COUNTERACT THE INVESTIGATION OF A CRIME

Abstract. One of the topical issues in the investigation of IT crime is the establishment of hidden electronic digital traces. As the analysis of theoretical provisions and law enforcement practice shows, there are many options to counteract the investigation of a crime in an appropriate way. In the framework of this research paper, the main ways of concealment of digital traces, which include distortion, destruction and disguise, were identified. The best options for identifying the use of each of these

concealment methods have been proposed.

Keywords: electronic-digital trace, electronic data carrier, information technology, concealment of traces, masking, distortion, destruction.

УДК 343

Таджибов Зейнудин Рамазанович
Аспирант
Российский университет дружбы народов имени П. Лумумбы
(г. Москва, Российская Федерация)
zeka3009@mail.ru

ВНЕДРЕНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ В УГОЛОВНО-ПРОЦЕССУАЛЬНУЮ ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Аннотация. В данной статье рассматриваются вопросы о развитии технологий и последующем их внедрении в уголовное судопроизводство. Данный вопрос актуален в связи с изменениями в обществе и государстве, которые являются своего рода вызовом для правоотношений и их регулирования. Уровню современных технологий должно соответствовать и уголовное судопроизводство, поскольку является одним из авангардов отраслей российского права. В этой связи рассматриваются основные аспекты развития и возможное влияние на уголовный процесс технологий. Исследуется, насколько сами правоохранительные органы, участвующие в данных правоотношениях, готовы к такому роду изменениям, и насколько изменятся их роль и процессуальный статус. Так же рассматриваются вопросы о качестве работы технологий, их отрицательные и положительные стороны, и пределы, а также целесообразность их внедрения.

Ключевые слова: уголовное судопроизводство, электронные документы, предварительное расследование.

Для цитирования:
Таджибов З. Р. Внедрение современных технологий в уголовно-процессуальную деятельность правоохранительных органов // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 204–208.

Безусловно, человек и его стремление совершенствоваться приводят к развитию определённых факторов в жизнедеятельности, имеющих за собой такие качества как удобство, комфорт и практичность, а технологии являются ведущим катализатором для последующего скачка вперёд как в развитии человека, так и в его конкретной профессиональной деятельности.

За последние несколько десятков лет появилось огромное количество гаджетов, аппаратуры, специальных технических средств и прочего, что может облегчить нашу жизнь. Технологии на сегодняшний день можно считать одним из быстро развивающихся явлений. С каждым днём появляется большое количество патентов и новых подходов к созданию чего-либо. Без технологий трудно представить продвижение работы и

деятельность человека в той или иной сфере. Технологии в зависимости от их назначения могут дать свой результат. Но не стоит и забывать вопросе: «а какого характера будет результат?», то есть на сколько целесообразно и полезно будет внедрение технологий для решения конкретных задач. Мы же будем говорить о технологиях в контексте деятельности правоохранительных органов в уголовном судопроизводстве.

Для многих не является секретом, что в работе правоохранительных органов, в том числе, органов предварительного расследования с точки зрения уголовного процесса было множество проблем с осуществлением тех или иных процессуальных действий, поскольку вызывали ряд сложностей как с практической стороны, так с теоретической. Тем более, если в качестве примера мы обратимся к советской эпохе и советскому уголовному процессу, тогда многие процессуальные действия происходили с некоторыми сложностями и ошибками, да и в целом имели за собой множество пробелов на законодательном уровне. Например, в советской практике допроса никто не думал, что можно использовать приборы аудио- и видео фиксации, тогда и сами технологии мало что могли предложить в этом плане.

С развитием технологий, их стали применять повсеместно в правоохранительных органах. Со временем это стали утверждать на законодательном уровне с последующим внесением поправок в уголовно-процессуальный кодекс России. Сегодня применение разного рода технологий и всего, что с ними связано, является своего рода нормой, и, что немаловажно, законодательной нормой. Возникает другой вопрос возникает: «к чему может привести большое количество внедрения таких технологий и как это будет влиять на качество расследования уголовных дел?»

Начнём с того, что ранее был принят Указ Президента Российской Федерации «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», где уже указывается конкретное нацеливание на цифровизацию и внедрение технологий в целом в повседневную жизнь государства и граждан.

В рамках уголовного судопроизводства мы можем рассмотреть вопрос использования ВКС (видео-конференц-связи), которая стала активно развиваться, в том числе, в условиях коронавируса, поменявшего правили работы и поведения людей, где исключением не стало и уголовное судопроизводство. Для примера, ВКС упоминается в ст. 241.1 УПК РФ, где закрепляется само понятие видео-конференц-связи, описываются условия примененя технологии: в частности, наличие возможности использовать специально подготовленное оборудование в зале судебного заседания. Ст. 278.1 УПК РФ регулирует конкретную ситуацию применения рассматриваемой технологии: допрос свидетеля или потерпевшего посредством системы видео-конференц-связи.

«В ряде государств на постсоветском пространстве (Грузия, Беларусь, Казахстан, Эстония) и в

других государствах модернизация и совершенствование, в частности досудебного производства, происходит путем более активного внедрения электронных технических средств в деятельность органов и должностных лиц, осуществляющих предварительное расследование»[1].

Здесь можно наблюдать развитие и права, и технологий. Если говорить про недавнее время: 15–20 лет назад не существовало такого понятия, как электронные документы, но с последующим развитием тех же технологий их внедрение стало возможным, в частности, в сфере подачи обращений граждан в правоохранительные органы. Так, например, Федеральным законом от 23 июня 2016 г. № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти» УПК РФ дополнен статьёй 474.1 «Порядок использования электронных документов в уголовном судопроизводстве»[2]. Законодательно закреплена возможность подачи процессуальных документов в суд в электронной форме при подписании электронной подписью, изготовления судебных решений в форме электронного документа и направления через сеть Интернет участнику уголовного судопроизводства.

В современном обществе практически у каждого имеется мобильный телефон, что, в свою очередь, не преминуло сказаться на применяемых судом способах вызова в судебный процесс лиц – участников судебных заседаний. Так, вызов осуществляется посредством направления на номер мобильного телефона СМС-уведомлений (SMS – Shot Message Service – служба коротких сообщений). Обязательным условием отправки подобных уведомлений является подключение адресата к сети мобильной связи[3].

К сожалению, вопрос о последствиях внедрения технологий в работу правоохранительных органов и в уголовный процесс в целом ставят реже, так как здесь присутствует и негативная сторона. Некоторые сотрудники правоохранительных органов и учёный высказывают предположения о потенциальной замене судьи в процессе искусственным интеллектом. Данную позицию мы категорически не поддерживаем, поскольку искусственному интеллекту не даны морально-нравственные качества и

[1] Клещина Е. Н., Григорьев Д. А. К вопросу о внедрении цифровых технологий в российский уголовный процесс // Государственная служба и кадры. 2021. № 4. 218–222. DOI 10.24411/2312-0444-2021-4-218-222.

[2] Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти» от 23.06.2016 № 220-ФЗ (последняя редакция) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_200008/ (дата обращения: 16.05.2023).

[3] Долгов А. М. Правовые основы применения цифровых технологий в уголовном процессе России // Теория и практика общественного развития. 2020. № 12 (154). С. 72–74. DOI 10.24158/tipor.2020.12.13.

чувства, которые присущи человеку, а некоторые принципы уголовного судопроизводства, в свою очередь, основываются на этих человеческих свойствах.

Ещё одной проблемой для полного охвата технологиями уголовного процесса, является структура как уголовного судопроизводства, так и уголовно-процессуального законодательства. Этот вопрос возникает в связи со строгостью и консервативностью УПК РФ как основного закона, регулирующего данные правоотношения, хотя модернизация требуется из-за современных реалий

Также следует отметить, что не всегда законодательство успевает нагнать темпы развития технологий, чтобы можно было сразу итегрировать их практике, а также предотвраить умышленные нарушения при использовании данных технологий для личной выгоды со стороны должностных лиц. «В действующем уголовно-процессуальном законодательстве не сформировался единый принцип использования понятий, относящихся к техническим средствам, применяемым в сфере уголовного судопроизводства. На практике часто возникают процессуальные проблемы применения результатов использования технических средств в качестве доказательства, поскольку не представляется возможным исключить вероятность фальсификации результатов. С развитием научнотехнического прогресса расширяются возможности монтажа, подделки, подлога, и других способов фальсификации доказательств, имеющих значений для рассмотрения дела. Все это усложняется тем, что возможности компьютерного монтажа позволяют делать это без оставления следов вмешательства в осуществленную запись, предоставляют возможность создавать доказательства с помощью мультипликации, инсценировки, имитации и др., что не всегда может быть выявлено даже экспертом»[4].

Исходя из вышесказанного можно прийти к выводу о том, что внедрение технологий в контексте закона и правоприменения может служить на пользу в уголовном судопроизводстве, но лишь в умеренном виде, ведь остальное должно опираться на человеческие факторы и только за человеком может оставаться исход расследования уголовного дела и придание виновного лица суду, который тоже должен объективно дать оценку преступным событиям и вынести соответствующее решение о виновности или невиновности лица.

[4] Аджимагомедова С. К., Турилов Г. Г. Проблемы применения современных технологий в уголовном судопроизводстве // Нацразвитие. Наука и образование. 2021. № 2 (2). С. 22–23. DOI 10.37539/2782-375.2021.2.2.004.

Список литературы

1. Аджимагомедова С. К., Турилов Г. Г. Проблемы применения современных технологий в уголовном судопроизводстве // Нацразвитие. Наука и образование. 2021. № 2 (2). С. 22–23. DOI 10.37539/2782-375.2021.2.2.004.

2. Долгов А. М. Правовые основы применения цифровых технологий в уголовном процессе России // Теория и практика общественного развития. 2020. № 12 (154). С. 72–74. DOI 10.24158/tipor.2020.12.13.

3. Клещина Е. Н., Григорьев Д. А. К вопросу о внедрении цифровых технологий в российский уголовный процесс // Государственная служба и кадры. 2021. № 4. 218–222. DOI 10.24411/2312-0444-2021-4-218-222.

Zeynudin R. Tajibov
Postgraduate student
Russian Peoples' Friendship University
named after P. Lumumba
(Moscow, Russian Federation)
zeka3009@mail.ru

INTRODUCTION OF MODERN TECHNOLOGIES INTO THE CRIMINAL PROCEDURAL ACTIVITIES OF LAW ENFORCEMENT AGENCIES

Abstract. This article discusses the development of technologies and their subsequent introduction into criminal proceedings. This issue is relevant in connection with the realities and changes in society and the state, which are a kind of challenge for legal relations and their regulation. In the current realities, criminal justice should also correspond, since it is one of the vanguards of the branches of Russian law and it should be at the same pace of development with modern conditions. In this regard, the main aspects of the development and possible impact on the criminal process of technology are considered. To what extent are the law enforcement agencies themselves involved in these legal relations ready for such changes, and to what extent will their role and procedural status change. Questions about the quality of technology, their negative and positive sides, and the limits of technology implementation and their expediency in general are also considered.

Keywords: Technology, criminal proceedings, electronic documents, preliminary investigation, judge, evidence.

УДК 343.14

Тарнавский Олег Александрович
Кандидат юридических наук, доцент,
заместитель генерального директора ООО «Газпром энерго»
(г. Москва, Российская Федерация)
mellert@bk.ru

МЕСТО ЦИФРОВОЙ ИНФОРМАЦИИ СРЕДИ ИСТОЧНИКОВ ДОКАЗЫВАНИЯ ПО УГОЛОВНОМУ ДЕЛУ

Аннотация. В статье рассматривается вопрос о месте цифровых источников информации в системе доказательств, анализируются существующие критерии определения и возможности вхождения «электронного доказательства» в действующую систему доказательственного права через призму действующей нормативно-правовой регламентации, потребности практических работников и суждений процессуалистов.

Ключевые слова: уголовный процесс, доказывание, источники, доказательства, цифровая информация.

Для цитирования:
Тарнавский О. А. Место цифровой информации среди источников доказывания по уголовному делу // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 209–215.

По данным Главного информационно-аналитического центра МВД России, в 2022 преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, было зарегистрировано на 12 % больше, чем в предыдущем периоде, а в сравнении с статистическими данными за пятилетний срок увеличение произошло в десятки раз[1]. И это за вычетом иных составов преступлений, в которых способом совершения преступления являются цифровые технологии. Таковых, конечно же, многократно больше. Выявление и раскрытие подобных преступных посягательств возможно при наличии соответствующего ресурса (технологического, кадрового). Однако статистика также свидетельствует о наличии проблем с процессом доказывания по рассматриваемой категории уголовных дел.

Правоохранительными органами для раскрытия преступления часто используются фотографии и

[1] Результаты деятельности МВД России в 2022 году // Официальный сайт МВД России [Электронный ресурс]. URL: https://мвд.рф/dejatelnost/results/annual_reports (дата обращения: 13.05.2023).

видеозаписи, сделанные с помощью цифровых фото- и видеокамер, установленных в помещениях банков, магазинов, а также на городских улицах. В следственно-криминалистической практике всё чаще применяются цифровые способы фиксации следов преступления, моделирования внешности преступника и поиска информации, относящейся к событию преступления[2].

Отечественными учёными-правоведами выделяются две точки зрения в восприятии компьютерной информации в уголовном процессе[3]. Одними электронные материалы расцениваются как самостоятельные доказательства, другие относят их к иным документам. Первая точка зрения представляется более верной, поскольку, исходя из современных реалий, компьютерную информацию необходимо рассматривать в качестве нового самостоятельного вида доказательств[4]. При этом комплексного монографического исследования, посвящённого специфике компьютерной информации как самостоятельного вида доказательств в уголовном судопроизводстве, требующего специального подхода к его собиранию, проверке и оценке в отечественной литературе на сегодняшний день не существует.

По данной проблеме учёными высказано мнение, что традиционные документы, хотя и не с той скоростью, с которой требуют современные реалии, постепенно вытесняются так называемыми электронными документами (далее – ЭД) – файлами, созданными с помощью аппаратно-программных средств компьютерной техники, содержащими документную информацию в виде текста, изображения или их сочетания[5].

В условиях использования ЭД в официальном документообороте они также могут представляться в качестве письменных или иных доказательств в административном, арбитражном, гражданском и уголовном процессах, и точно также, как и в отношении баз данных, судом должны решаться вопросы об их достоверности [6].

Немаловажными для использования компьютерной информации в качестве надлежащего доказательства в уголовном судопроизводстве являются основания и условия изъятия такой информации при производстве обыска в рамках неотложных следственных действий

---

[2] Капустина Л. К. Оценка допустимости и достоверности доказательств в уголовном судопроизводстве // Вестник Санкт-Петербургского университета МВД России. 2020. № 1 (85). С. 115.

[3] Ишмаева Т. П. К вопросу о юридических свойствах доказательств в уголовном процессе // Вестник Челябинского государственного университета. 2015. № 23 (378). С. 133.

[4] Зажицкий В. И. О нетрадиционных свойствах доказательств по уголовному делу // Российская юстиция. 2018. № 2. С. 20.

[5] Доля Е. А. Происхождение доказательств в уголовном судопроизводстве // Законность. 2016. № 10. С. 66.

[6] Бахтаров С. Х.-П. Проблема понимания свойств доказательств в уголовном судопроизводстве // FORMAT.Юриспруденция. 2019. № 2 (2). С. 12.

по уголовному делу, предусмотренные п. 9.1 ст. 182 УПК РФ[7].

Допустимость доказательств представляет больший интерес как для учёных, так и для практических работников, при этом наибольшие трудности вызывает определение соответствия сведений конкретному свойству. Применительно к цифровой информации, представляющей интерес с точки зрения познавательной ценности об обстоятельствах по уголовному делу, следует указать следующее.

При производстве следственных действий необходимо помнить, что электронные носители информации изымаются с участием специалиста. По ходатайству законного владельца осуществляется копирование информации на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей. При производстве обыска не допускается копирование информации, если это может воспрепятствовать расследованию преступления либо, по заявлению специалиста, повлечь за собой утрату или изменение информации. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе делается запись[8].

При производстве предварительного расследования с компьютерной информацией допускаются ошибки, способные повлечь утрату сведений, которые могут оказать помощь в раскрытии преступления. Научное прогнозирование развития новых видов доказательств позволит ускорить процесс их практического использования[9], а также выработать подходы, позволяющие избежать проявление указанных ошибок. Вопросы понимания роли и места компьютерной информации в уголовном процессе приобретают в современных условиях всё большую актуальность и требуют оперативного их разрешения.

Практическим примером использования компьютерной информации в качестве доказательства в современном уголовном процессе могут служить уголовные дела, рассмотренные за 2021 год и 10 месяцев 2022 года Оренбургским районным судом. Речь идёт о преступлениях в области нарушения

[7] Давлетов А. А. Основы уголовно-процессуального познания. Екатеринбург: Издательство Гуманитарного университета, 1997. С. 56.

[8] Лютынский А. М. О процедуре признания доказательства недопустимым в российском уголовном судопроизводстве // Современные исследования социальных проблем. 2015. № 7 (51). С. 231.

[9] Татаров Л. А. Свойства доказательств в уголовном судопроизводстве: правовые и гносеологические проблемы // Глобальный научный потенциал. 2013. № 10 (31). С. 152.

авторских прав, неправомерного доступа к охраняемой законом компьютерной информации, сопряжённого с копированием компьютерной информации, а также использования компьютерных программ, заведомо предназначенных для нейтрализации средств защиты компьютерной информации. При этом, о динамике роста преступлений данной категории, можно судить, сравнив количество уголовных дел в указанной сфере, рассмотренных Оренбургским районным судом в 2019–2020 годах (2 уголовных дела) и в 2021 году за аналогичный с 2022 годом период в 10 месяцев (6 уголовных дел)[10].

Компьютерная информация по таким делам, являющаяся контрафактным экземпляром программного обеспечения для ЭВМ, изъятая при обыске (выемке) или в результате ОРМ контрольной закупки, исследуется в судебном заседании в ходе судебного следствия посредством обозрения с учётом выводов эксперта, а после вынесения приговора по делу, в результате определения дальнейшей судьбы вещественных доказательств по делу, в соответствии со ст. 81–82 УПК РФ, как правило уничтожается, а электронные носители, после её уничтожения, возвращаются законным владельцам по принадлежности[11].

Некоторые учёные, анализируя практику судов относительно применения ст. 75 УПК РФ, приходят к выводу о необходимости уточнения перечня оснований для признания доказательств недопустимыми. В. В. Соткова предлагает законодательно предусмотреть перечень существенных нарушений, в связи с которыми доказательства признаются недопустимыми[12].

Полагаем необходимым отрегулировать вопросы, связанные с поиском, обнаружением, фиксацией компьютерной информации и её закреплением, приобщением к делу в качестве доказательств, в связи с чем высказана необходимость ее дополнительного закрепления в главе 10 УПК РФ и оценена целесообразность внесения изменений в главу 25 УПК РФ (часть 9.1 ст. 182 введена Федеральным законом от 28.07.2012 № 143-ФЗ, в редакции Федерального закона от 29.11.2012 № 207-ФЗ)[13].

Приемлемым вариантом соответствия реалиям времени может стать редакция норм статей 84^1 «Компьютерная информация», 84^2 «Процессуальный порядок

[10] Статистические данные Оренбургского областного суда по рассмотрению уголовных дел за 2015–2019 годы // Оренбургский областной суд: официальный сайт [Электронный ресурс]. URL: http://oblsud.orb.sudrf.ru/modules.php?name=docum_sud&id=615 (дата обращения: 13.05.2023).

[11] Барыгина А. А. Доказывание в уголовном процессе: оценка отдельных видов доказательств. Москва: Издательство Юрайт, 2019. С. 113.

[12] Соткова В. В. Основания для признания доказательств недопустимыми // Материалы научной конференции XLVII Огаревские чтения. Саранск: Национальный исследовательский Мордовский государственный университет им. Н. П. Огарева, 2019. С. 464.

[13] Баранова М. А. Признание доказательств недопустимыми в судебных решениях по уголовным делам: поиск критериев // Юридическая наука и правоохранительная практика. 2016. № 1 (35). С. 127.

приобщения к делу компьютерной информации в качестве доказательства», 84[3]. «Представление доказательств в виде компьютерной информации участниками процесса или иными лицами» [14].

Отечественной практикой систематизированы и отражены основные аспекты общепринятых видов доказательств в уголовном судопроизводстве, а также виды компьютерных преступлений и анализ мер противодействия им.

Так, Мещанским районным судом города Москвы 2 октября 2018 года было рассмотрено дело № 01-0123/2018, согласно материалам которого бывшие сотрудники правоохранительных органов были признаны виновными в совершении преступления, предусмотренного п. «в» ч. 3. ст. 286 УК РФ (превышение должностных полномочий, повлекшее наступление тяжких последствий). Суть нарушений, допущенных сотрудниками, сводится к фальсификации доказательств с использованием новых цифровых возможностей: контекстное компилирование из мессенджеров частей разговоров и сообщений, осуществлённое в отношении потерпевших. Постановление президиума Московского городского суда[15] отменило ранее вынесенное решение по данному делу. Рассмотрение подобного вопроса в московском суде стало возможным благодаря проведению установления достоверности (подлинности) полученной информации, что стало предметом исследования в рамках судебной компьютерно-технической экспертизы[16]. При этом анализу подлежали и машинопечатные тексты, в целом подобное исследование всегда комплексное и соединяет в себе как традиционные формы экспертных методик, так методики аппаратных, программных систем. Однако приведенный пример скорее исключение из общего правила, нежели часто используемый приём проверки доказательств[17].

Подводя итог, следует отметить, что электронные носители информации были включены в УПК РФ как новый вид вещественных доказательств. Об этом свидетельствует содержание статьи 474.1, регулирующей порядок использования электронных документов в уголовном судопроизводстве, а судебная практика, например, положительно оценивает вручение копии обвинительного заключения в электронной форме. А значит данное

[14] Капустина Л. К. Соотношение допустимости и достоверности доказательств в уголовном судопроизводстве // Вестник Казанского Юридического института МВД России.2019. № 3 (37). С. 387.

[15] Дело № 01-0123/2018 от 2 октября 2018 года, рассмотренное Мещанским районным судом г. Москва // КонсультантПлюс: Высшая Школа: правовые док. для студентов юрид., финансовых и экон. специальностей [Электронный ресурс]. Москва, 2023.

[16] Терехин В. В. Стандарты допустимости доказательств в уголовном процессе // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 1 (33). С. 190.

[17] Левченко О. В. Система средств познавательной деятельности в доказывании по уголовным делам и ее совершенствование: автореф. дис. … канд. юрид. наук. Краснодар, 2004. С. 31.

направление необходимо расширять, вводить в законодательство новый источник получения доказательства – электронное доказательство.

Список литературы

1. Баранова М. А. Признание доказательств недопустимыми в судебных решениях по уголовным делам: поиск критериев // Юридическая наука и правоохранительная практика. 2016. № 1 (35). С. 122–127.
2. Барыгина А. А. Доказывание в уголовном процессе: оценка отдельных видов доказательств. Москва: Издательство Юрайт, 2019. 277 с.
3. Бахтаров С. Х.-П. Проблема понимания свойств доказательств в уголовном судопроизводстве // FORMAT.Юриспруденция. 2019. № 2 (2). С. 12–16.
4. Давлетов А. А. Основы уголовно-процессуального познания. Екатеринбург: Издательство Гуманитарного университета, 1997. 190 с.
5. Доля Е. А. Происхождение доказательств в уголовном судопроизводстве // Законность. 2016. № 10. С. 65–70.
6. Зажицкий В. И. О нетрадиционных свойствах доказательств по уголовному делу // Российская юстиция. 2018. № 2. С. 20–23.
7. Ишмаева Т. П. К вопросу о юридических свойствах доказательств в уголовном процессе // Вестник Челябинского государственного университета. 2015. № 23 (378). С. 133–136.
8. Капустина Л. К. Оценка допустимости и достоверности доказательств в уголовном судопроизводстве // Вестник Санкт-Петербургского университета МВД России. 2020. № 1 (85). С. 113–118.
9. Капустина Л. К. Соотношение допустимости и достоверности доказательств в уголовном судопроизводстве // Вестник Казанского Юридического института МВД России. 2019. № 3 (37). С. 386–390.
10. Левченко О. В. Система средств познавательной деятельности в доказывании по уголовным делам и ее совершенствование: автореф. дис. … канд. юрид. наук. Краснодар, 2004. 55 с.
11. Лютынский А. М. О процедуре признания доказательства недопустимым в российском уголовном судопроизводстве // Современные исследования социальных проблем. 2015. № 7 (51). С. 225–233.
12. Соткова В. В. Основания для признания доказательств недопустимыми // Материалы научной конференции XLVII Огаревские чтения. Саранск: Национальный исследовательский Мордовский государственный университет им. Н. П. Огарева, 2019. С. 463–465.
13. Татаров Л. А. Свойства доказательств в уголовном судопроизводстве: правовые и гносеологические проблемы / Л. А. Татаров // Глобальный научный потенциал. 2013. № 10 (31). С. 152–155.
14. Терехин В. В. Стандарты допустимости доказательств в уголовном процессе // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 1 (33). С. 188–193.

Oleg A. Tarnavsky
PhD in Law, Associate Professor,
Deputy General Director of Gazprom energo LLC
(Moscow, Russian Federation)
mellert@bk.ru

PLACE OF DIGITAL INFORMATION AMONG SOURCES OF EVIDENCE IN A CRIMINAL CASE

Abstract. The article considers the question of the place of digital sources of information in the evidence system existing criteria and the possibility of entering «electronic evidence» into the current system of evidence law through the prism of the current regulatory regulation, the needs of practitioners and judgments of procedural experts.

Keywords: criminal process, proof, sources, evidence, digital information.

УДК 343.98

Титов Павел Михайлович
Кандидат юридических наук,
старший преподаватель кафедры ОРД ОВД
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
titov1995@ya.ru

ОПЕРАТИВНО-РОЗЫСКНЫЕ МЕРОПРИЯТИЯ, ПРОВОДИМЫЕ ОПЕРАТИВНЫМИ СОТРУДНИКАМИ ПРИ ВЫЯВЛЕНИИ И РАСКРЫТИИ ПРЕСТУПЛЕНИЙ В ЭКОНОМИЧЕСКОЙ СФЕРЕ

Аннотация. В данной статье проведён анализ оперативно-розыскных мероприятий, проводимых при выявлении и раскрытии преступлений в сфере экономики. Данная сфера представляет повышенный интерес как для государства, так и для преступников, в связи с чем требует особого внимания сос стороны правоохранительных органов.

Ключевые слова: экономические преступления, оперативно-розыскные мероприятия, оперативно-розыскная деятельность, экономическая безопасность.

Для цитирования:
Титов П. М. Оперативно-розыскные мероприятия, проводимые оперативными сотрудниками при выявлении и раскрытии преступлений в экономической сфере // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 216–220.

Экономические преступления по своим социальным и экономическим последствиям представляют реальную угрозу как для личности и общества отдельно, так и для государства в целом, так как данные преступления напрямую влияют на бюджет государства и на авторитет страны на мировой арене. На сегодняшний день преступления в сфере экономики имеют большое распространение наряду с мошенничеством, о котором ранее автором отмечалось[1].

Далеко не по всем экономическим преступлениям имеется возможность выявить субъектов, их совершивших. Это может быть связано с несколькими факторами:

1. Злоумышленники не отстают от развития технологий, то есть развиваются параллельно вместе с ними, что позволяет им использовать специальные программы, системы для сокрытия следов преступлений и анонимизации собственной личности.

[1] Титов П. М. Оперативно-розыскные мероприятия, осуществляемые при расследовании мошенничества в сфере компьютерной информации // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2023. № 23-1. С. 32–33

2. Правоохранительные органы, занимающиеся раскрытием и расследованием данных видов преступлений, не взаимодействуют должным образом между собой и с другими субъектами, на что автором также неоднократно обращалось внимание[2].

3. Правоохранительные органы, в частности оперативные подразделения экономической безопасности и противодействия коррупции, проводят неполный комплекс оперативно-розыскных мероприятий.

4. Отдельные оперативно-розыскные мероприятия проводятся несвоевременно и т. д.

При этом ущерб, наносимый от совершения экономических преступлений значителен, что напрямую сказывается на национальной безопасности Российской Федерации.

Как правило, экономические преступления совершают не по одному человеку, а хорошо замаскированной организованной группой, именно поэтому оперативным подразделениям нужно своевременно проводить комплекс мер по выявлению и раскрытию преступлений в экономической сфере.

Проанализировав все оперативно-розыскные мероприятия, которые закреплены в статье 6 Федерального закона от 12.08.1995 №144-ФЗ «Об оперативно-розыскной деятельности» (далее – ФЗ «Об ОРД»), мы пришли к выводу, что все они могут использоваться при выявлении и раскрытии преступлений экономической направленности. Рассмотрим их более подробно.

Опрос. Данное оперативно-розыскное мероприятие предполагает общение самостоятельно или через третьих лиц с опрашиваемым с целью получения оперативно-значимой информации. Опрос является универсальным и применяется при выявлении и раскрытии преступлений во всех сферах. В экономической сфере опросу подлежат, чаще всего, лица, которые могли стать свидетелями преступления; лица, находящиеся в окружении интересуемого субъекта и так далее. Опрос в данной сфере может проводиться как гласно и негласно, так и легендированно.

Следующим, наиболее специфичным оперативно-розыскным мероприятием для экономической

[2] Титов П. М. Взаимодействие органов внутренних дел и Федеральной налоговой службы России при расследовании налоговых преступлений // Актуальные проблемы использования специальных знаний при выявлении и доказывании экономических преступлений: Сборник научных статей по итогам межвузовской научно-практической конференции, Нижний Новгород, 25 октября 2022 года. Нижний Новгород: ООО «Стимул-СТ», 2023. С. 347–349; Титов П. М. взаимодействие при расследовании преступлений, совершенных с использованием IT-технологий // Актуальные проблемы международного сотрудничества в борьбе с преступностью: Международная научно-практическая конференция, приуроченная к 20-летию образования Московского университета МВД России имени В. Я. Кикотя: сборник научных трудов, Москва, 25 февраля 2022 года. Москва: Московский университет Министерства внутренних дел Российской Федерации им. В. Я. Кикотя, 2022. С. 174–176.

сферы, является наведение справок. Его особенность заключается в том, что оно проводится практически в 100 % случаев при выявлении и раскрытии преступлений в экономической сфере.

Ещё одним оперативно-розыскным мероприятием является сбор образцов для сравнительного исследования. Данное мероприятие проводится при выявлении преступлений в сфере потребительского рынка. Оно проводится с целью выявления контрафактной продукции, товаров и т. д. Также при выявлении преступлений в сфере потребительского рынка может проводиться проверочная закупка, осуществляемая как самим оперативным сотрудником, так и с помощью лиц, оказывающих содействие оперативным подразделениям, согласно ст. 17 ФЗ «Об ОРД».

После проверочной закупки, обычно проводится исследование предметов и документов. Для данного оперативно-розыскного мероприятия могут привлекаться эксперты из экспертно-криминалистических центров. Помимо потребительского рынка, оно может проводиться по бухгалтерскими налоговым документам для выявления и раскрытия преступлений.

Наблюдение, также как и опрос, является универсальным оперативно-розыскным мероприятием, которое может применяться во всех сферах. Примером проведения данного оперативно-розыскного мероприятия может служить выявления признаков преступления, предусмотренного статьёй 171.2 Уголовного кодекса Российской Федерации (далее – УК РФ) «Незаконные организация и проведение азартных игр». Оно проводится с целью выявления субъектов, совершающих данное деяние.

Обследование помещений, зданий, сооружений, участков местности и транспортных средств. Данное мероприятие может проводиться в отношении как юридических лиц и индивидуальных предпринимателей, так и физических лиц. Цель проведения данного оперативно-розыскного мероприятия – выявление оперативно-значимой информации, которая может содержаться в бухгалтерской и налоговой отчётности, а также в иных документах.

Контроль почтовых отправлений, телеграфных и иных сообщений. Проводится оперативным сотрудником при получении им судебного разрешения. Данное оперативно-розыскное мероприятие может проводиться при выявлении и раскрытии следующих видов экономических преступлений: ст. 175 УК РФ при том условии, что в статистической карточке имеется отметка о его коррупционной направленности, ч. 3 ст. 228.1 УК РФ при том условии, что в карточке имеется отметка о совершении данного преступления должностным лицом, ст. 290 УК РФ, ст. 291 УК РФ и так далее.

Прослушивание телефонных переговоров также является оперативно-розыскным мероприятием судебного санкционирования. Данное оперативно-розыскное мероприятие чаще всего в сфере экономики применяется в отношении лиц,

совершающих преступления коррупционной направленности.

Снятие информации с технических каналов связи, оно же СИТКС, также является оперативно-розыскным мероприятием судебного санкционирования, так как при его проведении могут ограничиваться конституционные права граждан. Чаще всего проводится при выявлении признаков преступлений, связанных с отчётностью, которая предоставляется в контролирующие органы.

И заключительным оперативно-розыскным мероприятием является получение компьютерной информации. Оно схоже с предыдущим мероприятием. Может применяться для сопоставления результатов из программы 1С и результатов на бумажных носителях.

Таким образом, практически все пятнадцать оперативно-розыскных мероприятий применяются при выявлении и раскрытии преступлений экономической направленности. Оперативным сотрудникам необходимо своевременно, наиболее полно и правильно составить комплекс мероприятий, направленных на решение задач оперативно-розыскной деятельности.

Список литературы

1. Титов П. М. Взаимодействие органов внутренних дел и Федеральной налоговой службы России при расследовании налоговых преступлений // Актуальные проблемы использования специальных знаний при выявлении и доказывании экономических преступлений: Сборник научных статей по итогам межвузовской научно-практической конференции, Нижний Новгород, 25 октября 2022 года. Нижний Новгород: ООО «Стимул-СТ», 2023. С. 347–349.

2. Титов П. М. Взаимодействие при расследовании преступлений, совершенных с использованием IT-технологий // Актуальные проблемы международного сотрудничества в борьбе с преступностью: Международная научно-практическая конференция, приуроченная к 20-летию образования Московского университета МВД России имени В. Я. Кикотя: сборник научных трудов, Москва, 25 февраля 2022 года. Москва: Московский университет Министерства внутренних дел Российской Федерации им. В. Я. Кикотя, 2022. С. 174–176.

3. Титов П. М. Оперативно-розыскные мероприятия, осуществляемые при расследовании мошенничества в сфере компьютерной информации // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2023. № 23-1. С. 32–33.

4.

Pavel M. Titov
PhD in Law,
Senior Lecturer of the Department of Internal Affairs,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
titov1995@ya.ru

OPERATIONAL INVESTIGATIVE MEASURES CARRIED OUT BY OPERATIONAL OFFICERS IN THE DETECTION AND DISCLOSURE OF CRIMES IN THE ECONOMIC SPHERE

Abstract. This article analyzes the operational investigative measures carried out in the detection and disclosure of crimes in the field of economics. This area is of increased interest to both the state and criminals. The collegiums of the Ministry of Internal Affairs of the Russian Federation and the Prosecutor's Office of the Russian Federation in 2023 showed the relevance and sensitive attention of the President of the Russian Federation V.V. Putin to this topic and served as a starting point for a coordinated change of departmental approaches to combating crimes in the economic sphere. Turning to statistics, you can see certain "peak values" for some economic crimes both at the highest point and at the lowest.

Keywords: economy, economic crimes, operational investigative measures, operational investigative activities, operational staff, economic security.

УДК 343.985

Тозик Ирина Витальевна
Старший преподаватель кафедры уголовно-правовых дисциплин и криминалистики Донецкого филиала Волгоградской академии МВД России
(г. Донецк, Российская Федерация)
tozenka@mail.ru

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ОСУЩЕСТВЛЕНИЯ ДОПРОСА НЕСОВЕРШЕННОЛЕНИХ ПОСРЕДСТВОМ ВИДЕО-КОФЕРЕНЦ-СВЯЗИ

Аннотация. Статья посвящена специфике производства допроса несовершеннолетних путём видео-конференц-связи, в частности рассмотрены особенности взаимного расположения участников, проблемы привлечения третьих лиц к производству следственного действия и пути их решения, предложена классификация тактических приёмов в зависимости от их результативности при дистанционном допросе несовершеннолетних.

Ключевые слова: допрос несовершеннолетнего, видео-конференц-связь, тактические приёмы, дистанционный допрос, психологические особенности.

Для цитирования:
Тозик И. В. Тактические особенности осуществления допроса несовершеннолетних посредством видео-конференц-связи // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 221–227.

В ответ на развитие научно-технических средств связи, а также практические потребности предварительного расследования, законодатель Федеральным законом от 30.12.2021 № 501-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» закрепил возможность производства ряда вербальных следственных действий путём использования систем видео-конференц-связи. Несмотря на то, что необходимость нововведений и их характер становились предметом изучения многих учёных, внимание уделялось, как правило, проблемам организационного характера и материально-технического обеспечения следственного действия[1], оставляя в стороне его

1 См., например, Афанасьева А. А. Дистанционный допрос: состояние и перспективы // Вестник Казанского юридического института МВД России. 2021. № 3 (45). С. 370–374; Антонович Е. К. Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств) // Актуальные проблемы российского права. 2019. № 6 (103). С. 125–136.

психологические и тактические стороны.

Вместе с тем, очевидно, что использование средств видео-конференц-связи значительно ограничивает возможность личного взаимодействия с допрашиваемым, формализует общение и деперсонализирует его. А следовательно, такие следственные действия должны иметь свои психологические и тактические особенности производства. Тем более, если речь идёт о несовершеннолетних участниках уголовного процесса.

Законодательно установлено, что при производстве следственных действий с использованием видео-конференц-связи задействованы два следователя (дознавателя): непосредственно осуществляющий производство предварительного расследования, а также тот, которому поручена организация участия допрашиваемого в следственном действии, расположенный по месту нахождения последнего. При этом конкретное распределение обязанностей между указанными должностными лицами не обозначено. Однако очевидно, что инициатива и руководство следственным действием принадлежат следователю, в производстве которого находится уголовное дело. Другой же выполняет вспомогательную роль, которая ограничивается обеспечением участия допрашиваемого, и ни в коем случае не должен подменять функции основного следователя, т. е. не имеет права самостоятельно задавать вопросы, дублировать вопросы и ответы в случае плохого аудио-сигнала, комментировать происходящее или любым другим образом воздействовать на содержательную сторону следственных действий. Вместе с тем остаются открытыми вопросы, должен ли такой следователь обращать внимание допрашивающего следователя на случаи нарушения процедуры допроса (например, при оказании воздействия на несовершеннолетнего законным представителем), должен ли он находиться в кабинете в ходе всего следственного действия или после налаживания конференц-связи обязан покинуть кабинет?

Стоит отметить, что специфика несовершеннолетних участников уголовного процесса заключается в том, что на установление психологического контакта и общую атмосферу следственного действия значительное влияние оказывают первое впечатление от должностного лица, его поза, жесты, мимика. В этом аспекте не вызывает сомнения, что следователь, которому поручена организация участия несовершеннолетнего в следственных действиях посредством видео-конференц-связи, должен предпринять меры к обеспечению психологически комфортной атмосферы, но при этом соблюдать баланс, не перехватывая инициативу у основного следователя, чтобы у несовершеннолетнего не сложилось ложное впечатление относительно их подчинённости друг другу.

При обеспечении допроса несовершеннолетних посредством видео-конференц-связи угол обзора видеокамеры, направленный на допрашивающего следователя, должен фиксировать официальную

обстановку, не отягощённую посторонними предметами. Не рекомендуется обращать камеру в сторону окон или дверей. Оптимальным является расположение следователя напротив стены, при использовании видеокамеры рабочего компьютера, фиксирующей следователя за своим рабочим столом по пояс. В случае если в кабинете допрашивающего следователя находятся другие участники текущего следственного действия, угол обзора видеокамеры должен захватывать и их.

Свои особенности при дистанционном допросе несовершеннолетнего накладывает и присутствие третьих лиц: законных представителей, педагогов (психологов), которыми отягощено данное следственное действие. Такие участники могут оказывать существенное влияние на обстановку допроса, в том числе и негативное. Так, явное пренебрежительное отношение к процессу со стороны педагога (например, использование телефона во время производства следственного действия) может спровоцировать реакцию отторжения у несовершеннолетнего, существенно снизить оценку им значения дачи показаний и их качество. Законные же представители могут значительно корректировать показания несовершеннолетнего, пользуясь при этом невербальными сигналами (качая головой, дотрагиваясь, или даже просто взглядом выражая неодобрение сказанному). При дистанционном допросе следователю тяжело отслеживать и контролировать данные проявления в полной мере, учитывая, что такие участники располагаются по месту нахождения допрашиваемого[2]. По общему правилу, специалисты рекомендуют проводить дистанционные допросы без присутствия посторонних лиц со стороны допрашиваемого. Но если избежать этого невозможно, необходимо постараться минимизировать воздействие на несовершеннолетнего. Законного представителя следует разместить в положении сидя в пределах угла обозрения так, чтобы он не имел возможности незаметно дотрагиваться до ребёнка, а все участники следственного действия были бы обращены лицом к видеокамере. Отдельные специалисты предлагают справа-сзади от допрашиваемого расположить повернутое под 45 градусов к плоскости объектива зеркало, так, чтобы в кадр входили не только лицо и фигура допрашиваемого, но и прилегающее пространство[3], другие – организовать систему прокторинга (контрольного видеонаблюдения)[4], третьи –

[2] Мещеряков В. А., Цурлуй О. Ю. Допрос в свете изменений, внесённых в уголовнопроцессуальное законодательство в декабре 2021 года // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 34.

3 Ахмедшин Р. Л. Тактика коммуникативных следственных действий / науч. ред. Н. Т. Ведерников. Томск: Издательский Дом ТГУ, 2014. С. 280.

4 Шереметьев И. И. Использование современных цифровых технологий при

дублировать видеозапись экрана двумя независимыми камерами[5].

При подготовке к следственному действию рекомендуется заранее удостовериться в качестве транслируемого интернет-сигнала. Но на наш взгляд, момент подключения к видео-конференц-связи непосредственно лица, показания которого фиксируются, должен осуществляться уже после размещения всех участников следственного действия на своих местах.

Поскольку задачи идентификации личности несовершеннолетнего лежат на том следователе, который обеспечивает его участие в следственном действии, дополнительного уточнения анкетных данных по конференц-связи не требуется. В начале беседы нужно удостовериться в возможности несовершеннолетнего воспринимать информацию путём интернет-соединения. С этой целью задаётся ряд вопросов, касающихся технической стороны обеспечения следственного действия: «Хорошо ли меня слышно, видно? Стоит ли повернуть камеру, включить свет? Не мешают ли посторонние шумы, предметы?». Учитывая ограниченные возможности интернет-общения для установления психологического контакта, рационально будет увеличить по времени стадию знакомства и личностного разговора. Справедливым является мнение относительно важности поддержания постоянного зрительного контакта с несовершеннолетним[6], при необходимости следователю отлучиться из угла обзора используемой камеры (за дополнительными материалами, для исправления помех соединения и пр.), необходимо заранее уведомлять об этом допрашиваемого несовершеннолетнего.

До начала непосредственного допроса посредством видео-конференции-связи всем участникам (в том числе третьим лицам) должны быть разъяснены особенности порядка проведения данного следственного действия: невозможность до окончания следственного действия покидать своё место, перемещаться по кабинету, использовать какие-либо материалы или технические средства без сообщения об этом следователю. Дополнительное внимание несовершеннолетнего, на наш взгляд, должно быть обращено также и на то, что в случае, если он плохо расслышал вопрос следователя, он должен сообщить об этом и попросить повторить вопрос. Здесь же следует

судебном разбирательстве уголовных дел в дистанционном режиме. // Вестник Университета имени О. Е. Кутафина (МГЮА). 2020. № 10. С. 106.

5 Плахота К. С. Особенности производства допроса посредством использования видео-конференц-связи // Сборник материалов криминалистических чтений. 2021. № 18. С. 53–55.

6 Мещеряков В. А., Цурлуй О. Ю. Тактические особенности допроса с использованием видеоконференцсвязи // Актуальные проблемы криминалистического обеспечения раскрытия, расследования и предупреждения преступлений: Материалы Всероссийской научно-практической конференции, посвященной памяти доктора юридических наук, профессора В. И. Шиканова, Иркутск, 10 декабря 2021 года. Иркутск: Байкальский государственный университет, 2021. С. 107.

отметить несовершеннолетнему, что если следователь не расслышит его ответ, то скажет об этом и попросит повторить. При этом, сталкиваясь с подобной ситуацией и принимая во внимание повышенную внушаемость несовершеннолетних лиц, стоит каждый раз отмечать, что просьба повторить ответ связана с особенностями интернет-соединения, а не содержанием показаний.

По общему правилу, на стадии свободного рассказа следователь должен выслушивать показания, не перебивая и не задавая вопросов, кроме уточняющих. Вместе с тем, в ходе видео-конференц-связи возможна потеря интернет-соединения, что влечёт за собой необходимость дублирования рассказа. До настоящего времени специалисты не пришли к единому мнению относительно последствий прерывания интернет-сигнала для проведения дистанционного следственного действия, в том числе и тактических особенностей продолжения допроса после такого прерывания. На наш взгляд, инициатива повторного интернет-соединения лежит на следователе, проводящем следственное действие. После восстановления связи следователю необходимо обозначить момент, когда интернет-соединение было потеряно, а также последнюю зафиксированную часть показаний несовершеннолетнего. В случаях же нестабильного интернет-соединения (длительного прерывания сигнала, множественных отключений) целесообразно отложить производство следственного действия или перенести его.

Следует отметить также особенности использования отдельных тактических приёмов при производстве дистанционного допроса несовершеннолетнего. Часть из них может быть использована во время видео-конференц-связи без изменений. Например, стимулирование положительных качеств допрашиваемого, актуализация забытого или максимальная детализация показаний. Часть требует корректировки с учётом особенностей интернет-соединения, например, демонстрация доказательств или форсирование темпов допроса. Уголовно-процессуальное законодательство не несёт конкретизации, каким образом осуществлять предъявление доказательств при видео-конференц-связи: через интернет или при помощи следователя, обеспечивающего участие допрашиваемого в следственном действии. Вызывает сомнение эффективность демонстрации, например, рукописного текста, материалов уголовного дела через объектив видеокамеры. Форсирование темпа допроса также значительно усложняется при видео-конференц-связи, поскольку основой данного тактического приёма является необходимость подстраивания под темп беседы, которая обуславливает снижение уровня защиты лжи и установление правдивой информации. При интернет-общении темп беседы в значительной степени определяется скоростью транслируемого сигнала, что приводит к малой эффективности рассматриваемого приёма.

Безусловно, в случае допроса несовершеннолетних потерпевших и

свидетелей чаще всего реализуются бесконфликтные ситуации, где внимание следователя сосредоточено, в основном, на установлении контакта, создании комфортной психологической атмосферы, актуализации забытого и максимальной детализации показаний. На наш взгляд, ряд проблем допросов несовершеннолетних посредством видео-конференц-связи возможно решить путём их проведения в специальных помещениях для производства следственных действий с участием несовершеннолетних[7]. Указанные помещения оборудованы необходимыми средствами двойной видеофиксации, а также предусматривают помощь специалиста-психолога, способствующего установлению психологического контакта и использованию отдельных тактических приёмов с учётом особенностей видео-конференции.

Список литературы

1. Антонович Е. К. Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств) // Актуальные проблемы российского права. 2019. № 6 (103). С. 125–136.

2. Афанасьева А. А. Дистанционный допрос: состояние и перспективы // Вестник Казанского юридического института МВД России. 2021. № 3 (45). С. 370–374.

3. Ахмедшин Р. Л. Тактика коммуникативных следственных действий / науч. ред. Н. Т. Ведерников. Томск: Издательский Дом ТГУ, 2014. 294 с.

4. Мещеряков В. А., Цурлуй О. Ю. Допрос в свете изменений, внесённых в уголовно-процессуальное законодательство в декабре 2021 года // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 31–38.

5. Мещеряков В. А., Цурлуй О. Ю. Тактические особенности допроса с использованием видеоконференцсвязи // Актуальные проблемы криминалистического обеспечения раскрытия, расследования и предупреждения преступлений: Материалы Всероссийской научно-практической конференции, посвященной памяти доктора юридических наук, профессора В. И. Шиканова, Иркутск, 10 декабря 2021 года. Иркутск: Байкальский государственный университет, 2021. С. 104–109.

[7] Об оборудовании специальных помещений для производства в Следственном комитете Российской Федерации следственных и иных процессуальных следственных действий с участием несовершеннолетних: Приказ СК России от 03 марта 2015 г. № 19. // URL: https://ukrfkod.ru/zakonodatelstvo/prikaz-sk-rossii-ot-03032015-n-19/ (дата обращения: 23.03.2023).

6. Плахота К. С. Особенности производства допроса посредством использования видео-конференц-связи // Сборник материалов криминалистических чтений. 2021. № 18. С. 53–55.

7. Шереметьев И. И. Использование современных цифровых технологий при судебном разбирательстве уголовных дел в дистанционном режиме. // Вестник Университета имени О. Е. Кутафина (МГЮА). 2020. № 10. С. 97–107.

Irina V. Tozik
Senior Lecturer of the Department of Criminal Law Disciplines and Criminalistics
Donetsk Branch of the Volgograd Academy
of the Ministry of the Interior of Russia
(Donetsk, Russian Federation)
tozenka@mail.ru

TACTICAL FEATURES OF INTERROGATION OF MINORS VIA VIDEO-COFERENCE COMMUNICATION

Abstract. The article is devoted to the specifics of the interrogation of minors by video conferencing, in particular, the features of the relative position of the participants, the problems of involving third parties in the production of an investigative action and ways to solve them are considered, a classification of tactics is proposed depending on their effectiveness in remote interrogation of minors.

Keywords: interrogation of a minor, video conferencing, tactics, remote interrogation, psychological features.

УДК 343.98

Хамидуллин Руслан Сибагатуллович
кандидат юридических наук
Начальник кафедры оперативно-разыскной деятельности
органов внутренних дел
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
sledgsugu@mail.ru

Чуб Дмитрий Сергеевич
Слушатель
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
ural-yui@mvd.ru

КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННОМ ОБРАЗОВАНИИ

Аннотация. Предметом исследования является деятельность правоохранительных органов в борьбе с киберпреступностью. Объектом исследования выступают общественные отношения, возникающие в сфере образования в ходе реализации программ по борьбе с киберпреступностью в России. Автор рассматривает вопросы преступлений совершённых с помощью информационных технологий или в киберпространстве, а также организацию противодействия их совершению, деятельность, направленную на охрану здоровья граждан, обеспечение государственной и общественной безопасности; изучает процесс использования современных способов и методов криминалистики в выявлении, раскрытии преступлений совершаемых с использованием информационно-телекоммуникационных технологий. Особое внимание уделяется стратегии цифровой трансформации образования школьников и студентов, по которой обучающиеся в рамках занятий смогут овладевать знаниями, необходимыми для защиты себя и своих данных при работе с техническими средствами связи.

Ключевые слова: Кибербезопасность, киберпреступления, национальная безопасность, школьное образование, цифровая трансформация образования, проверка подлинности сайта, международные отношения, сеть Интернет, профилактика, обучение.

Для цитирования:
Хамидуллин Р. С., Чуб Д. С. Криминалистическое обеспечение кибербезопасности в современном образовании // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 228–234.

В век развития постиндустриального общества сотовая связь и сеть Интернет стали неотъемлемой частью в повседневной деятельности более ста миллионов людей в России и более семи миллиардов – в мире. Каждый человек нашей необъятной планеты имеет у себя в личном пользовании информационно-телекоммуникационные технологии (IT-технологии), которые не только получили широкое применение не только в этой области, но и оптимизировали сферу государственных и частных услуг. Помимо звонков с помощью мобильных телефонов или смартфонов, сеть Интернет позволила населению общаться между собой через мессенджеры в социальных сетях, находить нужную информацию в один «клик» с использованием поисковой строки в браузере, совершать покупки продуктов, одежды, техники и много другого с использованием Интернет-сайтов или специальных приложений, получать государственные, банковские и другие услуги не выходя из дома и т. д. Перечень возможностей, которые осуществляются с помощью сети Интернет, очень большой и развивается по сей день, что упрощает жизнь людям и сокращает временные издержки.

В современной теории криминалистики словосочетание «криминалистическое обеспечение» получило весьма широкое распространение[1]. Анализ литературы показал, что оно используется при характеристике не только всей криминалистической деятельности, но и отдельных её направлений, а в некоторых случаях и с целью обобщения отдельных частных вопросов криминалистики.

Система криминалистического обеспечения деятельности оперативного сотрудника по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий (ИТТ), – это особая организационно-функциональная система, направленная на формирование и поддержание на определённом уровне постоянной готовности оперативного работника к систематическому использованию в практической деятельности криминалистического арсенала средств борьбы с преступностью (макроуровень, научно-дидактический уровень), а также на реализацию этой готовности в каждом случае выявления, раскрытия и расследования преступлений, обусловливаемой конкретной оперативно-розыскной или следственной ситуацией (микроуровень, исполнительский уровень).

Применительно к противодействию преступлениям, совершаемым с использованием IT-технологий, криминалистическое

[1] Хамидуллин Р. С. Криминалистическое обеспечение противодействия незаконному обороту наркотических средств и психотропных веществ, осуществляемому в криптовалюте с использованием технологий «blockchain» // Технологии XXI века в юриспруденции. Материалы четвёртой международной научно-практической конференции. отв. редактор: Д. В. Бахтеев. Екатеринбург, 2022. С. 52–58.

обеспечение представляет собой комплекс мер, ориентированных на обеспечение субъектов уголовного преследования знаниями о наиболее эффективных и рациональных криминалистических средствах, приёмах и методах в целях установления обстоятельств, имеющих значение для полного и всестороннего раскрытия и расследования преступления, совершаемого с использованием информационно-телекоммуникационных технологи, а также создание оптимальных условий для их практической реализации в различных оперативно-розыскных и следственных ситуациях.

К криминалистическому обеспечению деятельности оперуполномоченного относится и деятельность по профилактике киберпреступлений среди несовершеннолетних.

Киберпреступления являются одной из самых серьёзных угроз для современных людей и организаций. По мере развития технологий кибербезопасности злоумышленники только усложняют свои атаки, используя новые данные. Поэтому каждой отрасли нужны эксперты по кибербезопасности, чтобы остановить хакеров на их пути и защитить конфиденциальные данные компании. Благодаря такому высокому спросу ожидается, что число рабочих мест для специалистов по кибербезопасности вырастет на 33 % в период с 2020 по 2030 годы [2].

На Международном конгрессе по кибербезопасности в Москве (2019 г.) Владимир Путин озвучил список мер по киберзащите страны, которые намерено принять правительство[3]. В список вошли международное сотрудничество, создание системы обмена информацией о кибератаках, использование отечественного ПО и подготовка квалифицированных кадров.

Реформируемая под процессы цифровизации общества и экономики система образования должна создать условия для содействия гражданам в формировании цифровых компетенций, для достижения массовой цифровой грамотности и возможности персонализации образовательной траектории в форме индивидуальной образовательной траектории формирования компетенций[4].

Для решения этих задач осуществляется ряд проектов, и к 2024 г. ожидается создание такой системы образования, которая могла бы выявлять талантливую молодёжь, особенно в ИТ-сфере, обеспечивать подготовку высококвалифицированных кадров,

[2] Inouye J. Top 10 Online Cyber Security Degree Options for 2023 // Hakr.io [Электронный ресурс]. 2023, 5 апреля. URL: https://hackr.io/blog/online-cyber-security-degree (дата обращения: 05.04.2023).

[3] Пленарное заседание Международного конгресса по кибербезопасности // Официальные сетевые ресурсы президента России (kremlin.ru). Раздел: Новости, выступления и стенограммы [Электронный ресурс: текстовая версия]. 2018, 6 июля. URL: http://www.kremlin.ru/events/president/news/57957 (дата обращения: 04.04.2023).

[4] Константинова Д. С., Кудаева М. М. Цифровые компетенции как основа трансформации профессионального образования // Экономика труда. 2020. Т. 7. № 11. С. 1055–1072. DOI: 10.18334/et.7.11.111073.

востребованных в условиях Индустрии 4.0, а также масштабную реализацию программ переподготовки и повышения квалификации в более узких профессиональных областях с учётом достижений цифровизации. В рамках данного направления важным является и то, что построение любой цифровой инфраструктуры очень тесно взаимосвязано с деятельностью, основанной на инновационном подходе.

В сложившихся условиях предусмотренные процессы цифровой трансформации отрасли выступают необходимым фундаментом для решения поставленных перед системой науки и образования задач.

Процессы цифровой трансформации широко представлены в стратегии цифровой трансформации отрасли науки и высшего образования, принятой распоряжением Правительства РФ «Об утверждении стратегического направления в области цифровой трансформации науки и высшего образования» от 21 декабря 2021 г. № 3759-р.

Согласно стратегии, школьники должны изучать основы кибербезопасности на уроках ОБЖ и технологии. По согласованию с Министерство просвещения почти половина учебной программы предмета ОБЖ будет посвящена изучению основ безопасности в интернете. На уроках технологии школьников будут учить навыкам безопасного использования различных цифровых сервисов. Минцифры считает, что занятия по информатике для этого не предназначены, так как на них преподаются информационные технологии и принципы их применения[5].

С 2022 года ученикам 8–11 классов будут доступны в удалённом режиме специальные двухгодичные курсы программирования. Дополнительное бесплатное профессиональное обучение программированию поможет школьникам определиться с будущей профессией и сформировать навыки, востребованные в цифровой экономике[6].

Во многих ВУЗах страны была введена новая дисциплина, которая так и называется «Кибербезопасность». Эти новшества должны помочь нашим гражданам справиться с угрозами, возникающими при работе с электронной средой.

Самые обыденные проблемы, с которыми может столкнуться пользователь электронной среды, это фальшивые сайты в ресурсе Интернет: ложные магазины, берущие оплату, но не доставляющие товар; страницы, необоснованно требующие паспортные данные, данные банковских карт и многие другие. Далеко не каждый человек сможет отличить сайт оригинала от сайта мошенников без наличия определённых знаний в этой сфере, а

[5] Денис. Российские школьники будут изучать основы кибербезопасности на уроках ОБЖ и технологии // Хабра [Электронный ресурс]. 2021, 5 сентября. URL: https://habr.com/ru/news/t/576394/ (дата обращения 04.04.2023).

[6] Крайнов В. Школьники смогут бесплатно учиться программированию с 2022 года // Информационное агентство ТАСС [Электронный ресурс]. 2021, 5 августа. URL: https://tass.ru/obschestvo/12214121 (дата обращения: 05.04.2023).

страницы мошенников появляются в интернете прямо как гидра – закрывается один сайт, на его месте создаются два новых.

Конечно, существуют определённые алгоритмы действий и специальные подразделения, которые занимаются поиском и закрытием вредоносных электронных страниц, большинство из которых, это сайты-клоны, посредством которых совершается мошенничество с помощью фишинга. Фишинг (fishing – рыбная ловля) – это противоправное действие, с помощью которого мошенники пытаются заставить лицо сообщить им конфиденциальную информацию.

Проведя исследование данной темы, предлагаем совершенствовать программу обучения школьников таким образом, чтобы в ней обучали навыкам отличия безопасных и небезопасных интернет-страниц, а программу обучения студентов так, чтобы они могли дополнительно отличать, запрещённый это сайт или нет и соответствует ли он правилам работы в той сфере, в которой студент получает образование. Например, представители юридических специальностей могут определить разрешена ли продажа товара, расположенного на сайте в России. Считаем также полезным, чтобы в процессе такого обучения образовательные организации предоставляли обучающимся возможность сообщать о таких сайтах специальному работнику, стимулировали их к этому.

Для достижения работоспособности данного предложения необходимо усовершенствовать материально-техническую базу в образовательных организациях, которая будет соответствовать условиям новых стандартов обучения.

Необходимо отметить, что программа по комплектации учреждений новыми технологиями уже проводится. Но во многих образовательных организациях нашей страны оснащённость современными техническими устройствами, используемыми в процессе обучения, оставляет желать лучшего. Кроме того, учебные заведения, которые имеют большое количество современных технических средств, зачастую не используют их в процессе обучения.

Для достижения цели необходимы дополнения к учебным пособиям или их полная переработка. Школьники и студенты должны иметь хорошо проработанную, актуальную информацию для обучения. Также необходима подготовка сотрудников оперативных подразделений и педагогических кадров, способных грамотно объяснять обучающимся все аспекты действий по обнаружению и ликвидации вредоносных программ и мошеннических сайтов. Кроме того, в обязанности педагога, преподающего соответствующий предмет, должны входить обязанности по приёму и проверке информации от обучающихся о вредоносных сайтах и программах. В результате чего, анализируя полученную информацию, они смогут предоставлять её в правоохранительные органы для дальнейшей проверки. Что, в свою очередь, также требует наладить взаимодействие между органами

правопорядка и сферой образования в данном направлении

Список литературы

1. Хамидуллин Р. С. Криминалистическое обеспечение противодействия незаконному обороту наркотических средств и психотропных веществ, осуществляемому в криптовалюте с использованием технологий «blockchain» // Технологии XXI века в юриспруденции. Материалы четвёртой международной научно-практической конференции. отв. редактор: Д. В. Бахтеев. Екатеринбург, 2022. С. 52–58.

2. Константинова Д. С., Кудаева М. М. Цифровые компетенции как основа трансформации профессионального образования // Экономика труда. 2020. Т. 7. № 11. С. 1055–1072. DOI: 10.18334/et.7.11.111073.

Ruslan S. Khamidullin
PhD in Law
Head of the Department of Operative and Investigative Activities
internal affairs bodies
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
sledgsugu@mail.ru

Dmitry S. Chub
Trainee
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
ural-yui@mvd.ru

FORENSIC SUPPORT OF CYBER SECURITY IN MODERN EDUCATION

Abstract. The subject of the research is the activities of law enforcement agencies in the fight against cybercrime. The object of the study is the social relations that arise in the field of education in the course of implementing programs to combat cybercrime in Russia. The author considers the issues of crimes committed with the help of information technology or in cyberspace, as well as the organization of counteraction to their commission, activities aimed at protecting the health of citizens, ensuring state and public security. She studies the process of using modern methods and methods of forensic science in identifying and solving crimes committed using information and telecommunication technologies. Particular attention is paid to the strategy of digital transformation of the education of schoolchildren and students: according to which students, within the framework of classes, will be able to acquire the knowledge necessary to protect themselves and their data when working with technical means of communication.

Keywords: Cybersecurity, cybercrime, national security, school education, digital transformation of education, site authentication, international relations, Internet, prevention, education.

УДК 343.98.06

Хорошева Анна Евгеньевна
Кандидат юридических наук, доцент,
юрисконсульт группы логистических компаний
(г. Барнаул, Российская Федерация)
khorosheva.defence@gmail.com

МЕТОД ТРЁХМЕРНОГО КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ И ЕГО КРИМИНАЛИСТИЧЕСКОЕ ЗНАЧЕНИЕ В СУДЕБНОМ РАЗБИРАТЕЛЬСТВЕ УГОЛОВНЫХ ДЕЛ

Аннотация. Реализация принципа наглядности в судебном разбирательстве уголовных дел при своей востребованности нуждается во взвешенном подходе. Помимо очевидного положительного эффекта, оказываемого средствами визуальной реконструкции на судебное исследование преступлений, имеют место риски, вызванные игнорированием влияния, которое такие средства способны оказать на принятие итогового решения по делу. Необходимость нейтрализации рисков, главным из которых является опасность вынесения несправедливого приговора под воздействием зрительных образов, заставляет обратить внимание на проблему представления в суде визуальной информации. Автор отмечает, что в рамках развития криминалистического направления, связанного с применением трёхмерного компьютерного моделирования, важно не только совершенствовать научную классификацию методов и технологий визуальной реконструкции, но и разрабатывать рекомендации по их надлежащему использованию в процессе судебного рассмотрения и разрешения уголовных дел.

Ключевые слова: визуальная реконструкция, криминалистический метод, компьютерное моделирование, 3D-модель.

Для цитирования:
Хорошева А. Е. Метод трёхмерного компьютерного моделирования и его криминалистическое значение в судебном разбирательстве уголовных дел // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 235–243

Проблема влияния визуальных образов на процедуру судебного исследования преступлений мало освещена в современной криминалистической литературе. О том, что такие технологии эффективны и полезны, особенно при рассмотрении уголовных дел повышенной сложности, сопряжённых с большим массивом данных, с неясным механизмом происшествия и т. д., не приходится говорить отдельно. Вопросы изучения в судах визуальных моделей выходят далеко за рамки оснащённости залов заседаний. Велико их влияние при производстве судебных

экспертиз, а также представлении моделей, замещающих объекты биологической природы и соответствующих при должной верификации вещественным доказательствам. Демонстрация объектов биологического происхождения в натуре по делам о преступлениях, связанных с причинением смерти, чаще всего невозможна в связи с рядом причин:

1) значимая часть проблемы сопряжена с шокирующим эффектом, помноженным на угрозу причинения страданий родственникам погибшего, вызванных невозможностью захоронить тело полностью;

2) исследование объектов биологической природы повышает риск их порчи и разрушения, который в некоторых случаях можно минимизировать лишь посредством использования защитной упаковки;

3) нельзя игнорировать этический и религиозный аспекты, актуализированные необходимостью «работы» с фрагментами и частями тел и способные оказать серьёзное влияние на внутреннее убеждение, вызывая предвзятое отношение к участникам судебного процесса и преступлению в целом.

Как показывает сложившаяся практика, потребность в представлении объектов биологического происхождения возникает в ситуации, когда вопрос об идентификации орудия преступления по отобразившимся ранениям, зафиксированным при помощи компьютерной томографии, приобретает первостепенное значение, позволяя, например, доказать совершение преступления определённым способом или конкретным лицом, особенно если речь идёт о соучастии. В условиях коллизионной защиты исследование перечисленных обстоятельств наполняется дополнительным смыслом. Тем не менее, все перечисленные факторы, препятствующие демонстрации объектов биологической природы в натуре, возможно нейтрализовать посредством массированного вовлечения в судебное исследование преступлений, связанных с причинением смерти, технологий 3D-моделирования.

Р. А. Коныгин и Л. А. Шестакова определяют трёхмерное компьютерное моделирование как «процедуру разработки 3D-модели (или же каркасной модели в виде трёхмерного объекта – воодушевлённого или невоодушевлённого) с использованием специализированного программного обеспечения. Трёхмерная модель создаётся посредством множества точек (Points), соединённых между собой линиями (Lines) и изогнутыми поверхностями (Curved Surfaces)»[1]. Модель имеет ряд преимуществ перед фото- и графическими изображениями повреждений, являющихся частью заключения судебно-медицинской экспертизы. Исследователи утверждают, что последние способны оказывать более сильное эмоциональное воздействие на принимающих юридические решения

[1] Коныгин Р. А., Шестакова Л. А. Использование компьютерного трехмерного моделирования в уголовном судопроизводстве Российской Федерации // Юридический вестник Самарского университета. 2017. № 3. Том 3. С. 99.

лиц (профессиональных судей и присяжных заседателей), тогда как изготовленная при помощи 3D-принтера модель может представлять собой реконструированный фрагмент или участок определённой части тела, не распознаваемый сам по себе. Но одновременно с этим потенциальная возможность использования в судебном исследовании 3D-модели инициирует ряд требующих разрешения вопросов, ответы на которые ещё крайне «слабо» представлены в науке и в судопроизводственной практике стран общего права, и ещё менее – в России: 1) адекватно ли конкретному случаю применение технологии трёхмерного моделирования? 2) при помощи каких технологий изготавливалась 3D-модель? 3) каким образом модель должна быть представлена в суде?

Неотъемлемым условием достоверности 3D-модели выступает точность, измеряемая уровнем её соответствия оригиналу. Допустимость модели связывается с надёжностью методов, используемых при её создании. По мнению зарубежных и российских исследователей, оценивать допустимость и достоверность 3D-модели в ходе судебного разбирательства необходимо, руководствуясь следующими критериями:

1. Актуальностью применённой при создании 3D-модели методики, которая находится на стадии разработки и основывается на действии компьютерной программы «ContexCapture». Установлено, что «при статистической обработке метрических характеристик трёхмерных моделей, создаваемых с учётом разработанных требований, максимальная относительная погрешность измерений составила 0,25 %. Существующий процент ошибки обусловлен «человеческим фактором», поскольку перенос размеров на объект осуществляется вручную и зависит от точности расстановки точек на цифровых фотографиях. В случае точной расстановки ориентиров процент ошибки может быть сведён практически к нулевому результату, ограниченному размером пикселя матрицы фотографирующего устройства»[2].

2. Полнотой и своевременностью выполнения действий по вызову и допросу в судебном разбирательстве специалиста, привлечённого к участию в сканировании объекта. Британские учёные полагают, что таким специалистом может выступать эксперт по метрологии и измерительным системам[3]. Его основная задача в судебном процессе включает дачу пояснений относительно методов и методик, при помощи которых изготавливалась модель, а также критериев, позволяющих определить соответствие модели оригиналу. Как отмечают исследователи, к таковым

[2] Шакирьянова Ю. П. Трехмерное моделирование в судебной медицине: визуализация, идентификация, реконструкция: дис. … д-ра. мед. наук. Москва, 2021. С. 18–19.

[3] Baier W., Warnett J. M., Payne M., Williams M. A. Introducing 3D Printed Models as Demonstrative Evidence at Criminal Trials // Journal Forensic Sciences. 2018. Vol. 63. Issue 4. P. 1301.

относятся: «конгруэнтность поверхностей, метрическая оценка, адекватность цветопередачи, возможность оценки исходной информации, ведение протокола создания модели, соответствие количественных и качественных характеристик оригинального и виртуального объектов, оценка возможности изменения (монтажа) объекта»[4]. Выяснение данных обстоятельств должно охватывать содержание вопросов и составлять предмет судебного допроса специалиста.

Положительные факторы, позволяющие визуализировать процесс судебного исследования, всё же не исключают тех негативных последствий, которые гипотетически могут наступить вследствие применения компьютерных технологий по реконструкции преступного события и его отдельных компонентов. Теории зрительного восприятия, разработанные представителями когнитивных наук и объединённые идеей ограниченности зрительных способностей человека, заставляют критически относиться к любым наглядным формам, демонстрируемым в судах. Кроме того, искусственно созданная модель реальности, независимо от качества заложенных в неё данных, всегда будет подвержена действию субъективного фактора, позволяющего оказывать разное по степени силы воздействие на аудиторию. И речь идёт не только об информации, вкладываемой в основу модели, но и о положении объектов в пространстве и возможностях его корректировки, освещённости, хронологической последовательности изложения и временных интервалах, а также о точке, с которой была произведена фиксация и осуществляется повествование. Конечно, современное программное обеспечение способно создавать сложные динамические 3D-модели, дающие возможность «взглянуть на событие преступления глазами свидетеля, потерпевшего, преступника и сопоставить увиденное с их показаниями»[5], как, например, программа 3D EyeWitness, но сущностной проблемы это всё равно не снимает, и связана она с возможностью либо невозможностью осуществлять контроль над эмоцией, которую несут исследованные в судебном процессе фотография, видео или виртуальная 3D-модель. Конструкция визуального доказательства[6] такова, что в её основе всегда отмечается присутствие эмоционального элемента, представляющего собой вербальное повествование, воплощённое в форму образов. Одновременно с этим все

[4] Шакирьянова Ю. П. Трехмерное моделирование в судебной медицине: визуализация, идентификация, реконструкция: дис. … д-ра. мед. наук. Москва, 2021. С. 22.

[5] Холопов А. В. Компьютерные программы 3D-визуализации события преступления // Криминалистъ. 2021. № 3 (36). С. 74.

[6] Автор настоящей статьи использует термин «визуальные доказательства» для обозначения общей совокупной группы всех источников и средств доказывания, которые могут восприниматься визуально, но с оговоркой, что данное словосочетание имеет процессуальную природу. Для целей же криминалистического исследования оптимальным видится употребление таких словосочетаний, как «средства и формы визуализации», «источники визуальной информации», «виртуальная модель».

источники, формы и модели зрительного восприятия, демонстрируемые в судебном разбирательстве, содержат визуальную информацию, которая может носить как доказательственный, так и ориентирующий, вспомогательный характер. При этом без ответа пока остаётся вопрос о научной классификации визуальных средств и форм, а также источников информации. Упорядочивание вышеупомянутых групп позволит в дальнейшем разрабатывать комплексные тактические рекомендации, учитывающие особенности положенных в основу классификации критериев.

Все источники визуальной информации можно разделить на две большие группы: 1) источники, являющиеся объектами живой и неживой природы, и их производные; 2) источники, полученные при помощи цифровых средств визуализации.

Остановимся подробнее на источниках, составляющих вторую группу. В криминалистической литературе проведена классификация средств, с помощью которых возможно создавать те или иные формы визуализации. Л. В. Бертовский, И. А. Кучерков и А. Л. Лисовецкий выделяют статические и динамические средства визуализации.

Статические средства, отображающие последствия, позволяют осматривать обстановку происшествия или объект происшествия при невозможности менять местоположение в пространстве или же, напротив, позволяют осматривать обстановку места происшествия или объект при наличии возможности виртуально перемещаться в пространстве. К первому подвиду авторы относят такие формы, как фото- и видеоизображения, рисунки и планы-схемы, предметы-аналоги, рентгеновские изображения объектов и т. д. Второй подвид включает в себя панорамные изображения обстановки места происшествия, полученные при помощи 3D-сканеров. Отмечается, что модель, относящаяся ко второму виду объективна, однако не характеризуется гибкостью, так как в ней содержатся объекты как относящиеся, так и не относящиеся к происшествию, вследствие чего может возникнуть необходимость в изменении её фактического содержания.

Динамические средства визуализации создают анимационные модели, визуализирующие происшествие целиком, включая отображение материальных объектов относительно друг друга[7].

Приведённая авторами классификация не представляется безупречной и упускает из виду несколько важных моментов. Прежде всего, не учитывается уровень развития новейших технологий, применяемых в технических областях и взятых на вооружение судебно-медицинскими экспертами. Публикации последних лет являются хорошим тому подтверждением. Сегодня экспертами с успехом осваивается технология

[7] Бертовский Л. В., Кучерков И. А., Лисовецкий А. Л. Криминалистический рендеринг: основные положения // Евразийский юридический журнал. 2015. № 7 (86). С. 250–251.

информационного моделирования (building information modeling или BIM-технология), позволяющая создавать 4D-модели, объединяющие все архитектурно-планировочные, конструктивные и инженерные решения с отражением всех технико-экономических показателей. Взятое за основу программное обеспечение позволило судебно-медицинским экспертам создавать BIM-модели криминального события, которые могут дополняться в условиях реального времени.

Так, группой судебно-медицинских экспертов в ходе проведённой ситуационной медико-криминалистической экспертизы с помощью совокупности 3D-технологий был создан информационный комплекс по уголовному делу об убийстве, совершённому с применением огнестрельного оружия. Экспертами были применены следующие технологии:

– реконструкция повреждений костей черепа по данным КТ;

– реконструкция траекторий полёта брызг крови по данным фототаблиц осмотра места происшествия;

– реконструкция траекторий полётов огнестрельных снарядов и их элементов на основе проведённой баллистической экспертизы;

– позиционирование источника кровотечения в пространстве с учётом анатомических особенностей жертвы, оригинального ранения и траекторий выстрелов на основе фотографии трупа;

– позиционирование модели на месте происшествия, определение положения стрелявшего, полученных методом фотограмметрии при помощи облёта места происшествия имеющимся в распоряжении экспертов квадрокоптером Fantom 4;

– прогнозирование разрушения пулями созданной информационной экспертной модели лобового стекла автомобиля в рамках определения характера деформации исследуемого объекта с использованием метода конечных элементов и специализированной компьютерной программы «Autodesk Inventor»[8].

Анализ приведённых данных инициирует ряд вопросов, нуждающихся в разрешении. Например, к какой классификационной группе относится упомянутая 4D-модель, учитывая, что BIM-технология позволяет пополнять такую модель новой информацией, и является ли модель, полученная при помощи традиционных средств фиксации, статической моделью первого подвида? Сегодня набирает популярность метод осмотра с использованием фототехники и беспилотных летательных аппаратов, позволяющий получать визуальную информацию с мест, «нахождение в которых либо затруднено, либо представляет опасность для эксперта»[9]. Можно ли предположить,

[8] Леонов С. В., Шакирьянова Ю. П., Пинчук П. В. Перспективы развития трехмерного моделирования для решения судебно-медицинских экспертных задач: BIM-технология и 4D-моделирование // Судебная медицина. 2020. Том 6. № 1. С. 7–10.

[9] Колесников И. И., Бульбачева А. А. Инновационный подход к проведению осмотра места происшествия с

что полученная таким образом 3D-модель, воспроизводящая обстановку места происшествия с возможностью осуществлять измерения, будет статической моделью комбинированного типа?

Обращает на себя внимание, что группа динамических средств Л. В. Бертовским, И. А. Кучерковым и А. Л. Лисовецким сужена до одного их производного – «анимационных моделей, визуализирующих происшествие целиком». Видимо, под данным словосочетанием авторы подразумевают созданную при помощи мультипликации виртуальную среду, внутри которой разворачивается преступное событие или его часть. При этом анимационная модель на языке программирования включает создание анимированных персонажей – аватаров. Куда же в таком случае отнести интерактивные виртуальные симуляторы, входящие в группу симуляторов виртуальной реальности и характеризующиеся реакцией виртуальной среды на активность пользователя?

Так, в рамках расследования громкого уголовного дела об убийстве двух молодых женщин, случайным образом попавших под перекрёстный огонь в Бирмингеме, была создана масштабная интерактивная модель. В виртуальной среде были воспроизведены более шестидесяти движущихся объектов – людей и транспортных средств. За основу были взяты данные с записей камер видеонаблюдения, полученные при осмотре места происшествия, и допросах свидетелей. Модель позволяла пользователю просматривать место происшествия с разных позиций и отслеживать хронологию событий в интерактивном режиме, обновляя её по мере появления новой информации. Окончательная версия интерактивной модели была использована в суде и позволила доказать виновность четырёх мужчин, открывших стрельбу[10].

Представляется оптимальным все модели, полученные посредством применения метода компьютерного моделирования, классифицировать по их целевому назначению на следующие виды:

1) виртуальная модель обстановки места происшествия, демонстрирующая в режиме виртуального времени доказательства;

2) виртуальная модель, созданная в процессе производства судебной экспертизы и способствующая решению ряда задач, например, установлению местоположения стрелявшего, механизма следообразования и т. п.;

3) виртуальная модель, позволяющая создать анимационное изображение версии одной из сторон;

4) виртуальные модели, применяемые в связи с проведением вербального процессуального действия, разделяемые на:

– виртуальную модель, созданную на основе показаний

использованием передовых технологий // Академическая мысль. 2018. № 4 (5). С. 86.

[10] Schofield D., Fowle K. Technology corner: Visualising forensic data: Evidence guidelines (Part 2) //Journal of Digital Forensics, Security and Law. 2013. Vol. 8 (2). P. 95–96.

свидетеля, потерпевшего, обвиняемого;

– виртуальную модель, созданную для решения тактических задач (симулятор для свидетеля, запускающий процесс «припоминания»; модель-реконструкция для обвиняемого, демонстрирующая уровень осведомлённости следственных органов о преступлении и образованных в ходе его совершения следах, и т. д.).

Список литературы

1. Бертовский Л. В., Кучерков И. А., Лисовецкий А. Л. Криминалистический рендеринг: основные положения // Евразийский юридический журнал. 2015. № 7 (86). С. 250–253.

2. Колесников И. И., Бульбачева А. А. Инновационный подход к проведению осмотра места происшествия с использованием передовых технологий // Академическая мысль. 2018. № 4 (5). С. 84–88.

3. Коныгин Р. А., Шестакова Л. А. Использование компьютерного трехмерного моделирования в уголовном судопроизводстве Российской Федерации // Юридический вестник Самарского университета. 2017. № 3. Том 3. С. 99–106.

4. Леонов С. В., Шакирьянова Ю. П., Пинчук П. В. Перспективы развития трехмерного моделирования для решения судебно-медицинских экспертных задач: BIM-технология и 4D-моделирование // Судебная медицина. 2020. Том 6. № 1. С. 4–13.

5. Холопов А. В. Компьютерные программы 3D-визуализации события преступления // Криминалистъ. 2021. № 3 (36). С. 70–76.

6. Шакирьянова Ю. П. Трехмерное моделирование в судебной медицине: визуализация, идентификация, реконструкция: дисс. … д-ра. мед. наук. Москва, 2021. 317 с.

7. Baier W., Warnett J. M., Payne M., Williams M. A. Introducing 3D Printed Models as Demonstrative Evidence at Criminal Trials // Journal Forensic Sciences. 2018. Vol. 63. Issue 4. Pp. 1298–1302.

8. Schofield D., Fowle K. Technology corner: Visualising forensic data: Evidence guidelines (Part 2) // Journal of Digital Forensics, Security and Law. 2013. Vol. 8 (2). Pp. 93–114.

Anna E. Khorosheva
PhD in Law, Associate Professor,
Corporate Lawyer of a Group of Logistics Companies,
(Barnaul, the Russian Federation)
khorosheva.defence@gmail.com

THE METHOD OF THE 3D- MODELING AND IT'S FORENSIC SIGNIFICANCE IN

JUDICIAL PROCEEDINGS OF CRIMINAL CASES

Abstract. The implementation of the principle of visibility in the trial of criminal cases, when in demand, needs a balanced approach. In addition to the obvious positive effect of visual reconstruction tools on the judicial investigation of crimes, there are risks caused by ignoring the impact that such tools can have on the adoption of the final decision on the case. The need to neutralize the risks, the main one of which is the danger of an unfair verdict under the influence of visual images, makes us pay attention to the problem of presenting visual information in court. The author notes that as part of the development of the criminalistic direction associated with the use of three-dimensional computer modeling, it is important not only to improve the scientific classification of methods and technologies of visual reconstruction, but also to develop recommendations for their proper application in the process of judicial review and resolution of criminal cases.

Keywords: visual reconstruction, forensic method, computer modeling, 3D model.

УДК 343.13

Черкасова Анастасия Максимовна
Адъюнкт
Нижегородская академия МВД России,
(г. Нижний Новгород, Российская Федерация)
Nastye4a@mail.ru

ЦИФРОВИЗАЦИЯ СТАДИИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА

Аннотация. В рамках исследования проанализировано законодательство Республики Казахстан, регулирующее правоотношения на стадии возбуждения уголовных заявлений и сообщений, поступающих в правоохранительные органы. Автором выявлены положительные тенденции использования автоматизированной системы и цифровых инструментов при приёме и регистрации сообщений и заявлений о происшествиях и предложено перенять положительный опыт правоприменительной практики Республики Казахстан, внедрив в уголовно-процессуальное законодательство использование цифровых технологий на стадии возбуждения уголовного дела, а именно регламентацию порядка приёма и регистрации заявлений и сообщений.

Ключевые слова: автоматизированная система, цифровые инструменты, сокращение срока расследования, защита прав и свобод.

Для цитирования:
Черкасова А. М. Цифровизация стадии возбуждения уголовного дела // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 244–249.

Существование современного человека уже трудно представить без цифровых технологий. С каждым днём всё больше аспектов нашей жизни переносятся в онлайн-сферу: от образования до работы, от развлечений до законодательства. Уголовно-процессуальные правоотношения не стали исключением: всё чаще процессуалисты обсуждают вопросы эффективности внедрения цифровых технологий в правоприменительную практику. Стоит отметить, что цифровизация касается всех стадий уголовного судопроизводства: от возбуждения уголовного дела до исполнения судебных решений и возобновления производства по делу.

Возбуждение уголовного дела характеризуется установлением наличия или отсутствия признаков состава преступления. Эта стадия служит своеобразным «фильтром» поступающей информации в правоохранительные органы: возбудить уголовное дело для последующего его расследования и раскрытия или отказать в таковом. В Российской Федерации деятельность по приёму, регистрации и разрешению

заявлений и сообщений в МВД России регламентируется Приказом МВД РФ от 29 августа 2014 года № 736[1], который утверждает соответствующую Инструкцию (далее – Инструкция). Согласно указанному документу, приём заявлений и сообщений о преступлениях осуществляются при помощи письменного или устного обращения граждан, также посредством электронной формы, направляемых через официальные сайты. Стоит отметить, что при принятии электронного обращения, оно должно быть распечатано на бумажном носителе и дальнейшая работа ведётся как с письменными заявлениями.

Официальным сайтом, через который можно подать заявление, сообщение в полицию, является сайт МВД России[2]. На нём в разделе «приём обращений» указано, что обращение в электронной форме рассматривается в соответствии с федеральным законом от 2 мая 2006 года № 59-ФЗ, регламентирующим порядок рассмотрения обращений[3], и приказом МВД России от 12 сентября 2013 года № 707, утверждающим инструкцию организации рассмотрения обращений в МВД РФ[4]. Кроме того, указано, что обращения регистрируются в срок, составляющий 3 дня, а рассматриваются – 30 дней. На наш взгляд, эта информация может ввести людей, подающих заявление о преступлении (особенно не обладающих юридическими познаниями), в сомнение. Во-первых, на сайте не указана Инструкция, во-вторых, сроки рассмотрения заявления о преступлении отличаются от представленных на сайте.

Отметим, что более пяти лет назад, в пилотном режиме функционировал модуль «Безопасность и охрана правопорядка» на справочно-информационном портале, при помощи которого граждане могли обратиться в правоохранительные органы с заявлением о преступлении[5]. Впоследствии осталась возможность только для подачи обращения в органы прокуратуры[6]. Мы разделяем мнения А. М. Долгова и А. А. Собенина о том, что портал государственных услуг РФ

[1] Приказ МВД РФ от 29 августа 2014 года № 736 «Об утверждении инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» // Российская газета, 2014. № 260.

[2] Официальный сайт МВД России. [Электронный ресурс]. URL: https://мвд.рф/request_main (дата обращения: 01.05.2023).

[3] Федеральный закон от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» // СЗРФ. 2006. № 19. Ст. 2060.

[4] Приказ МВД России от 12 сентября 2013 года № 707 «Об утверждении инструкции об организации рассмотрения обращений граждан в системе министерства внутренних дел Российской Федерации» // Российская газета, 2014. № 9.

[5] Андреева О. И, Зайцева О. А. Перспективы ведения российского уголовного судопроизводства в электронном формате // Уголовная юстиция. 2018. № 12. С. 58

[6] Портал государственных услуг Российской Федерации. [Электронный ресурс]. URL: https://www.gosuslugi.ru/352356/1 (дата обращения: 10.05.2023).

нуждается в поддержке в качестве «универсального инструмента в сфере электронно-цифровых услуг» для подачи заявления, сообщения о преступлении[7].

Считаем необходимым уделить внимание опыту применения цифровых инструментов для приёма и регистрации сообщений о преступлениях, которые используют сотрудники правоохранительных органов Республики Казахстан. Порядок принятия решения по поступающей информации в правоохранительные органы регламентируется в соответствии с Приказом Генерального Прокурора Республики Казахстан от 19 сентября 2014 года № 89[8] (далее – Приказ № 89). Согласно указанному документу, заявления могут быть поданы в письменном или электронном виде. С целью подачи онлайн-заявления в Республике Казахстан был разработан специальный модуль на сайте Комитета. Поданные сообщения в режиме реального времени поступают в автоматизированные системы правоохранительных органов и заносятся в электронную книгу учета заявлений и сообщений[9]. Такой алгоритм примечателен тем, что у сотрудников отсутствует возможность удалить, изменить информацию или вовсе её не регистрировать. Это исключает возможность укрытия поступающей информации от регистрации, обеспечивая эффективную защиту прав и свобод граждан. Все заявления и сообщения регистрируются в книге учёта информации (далее – КУИ) – автоматизированной системе. Все поступившие сведения становятся доступными для сотрудников правоохранительных органов, а также прокуратуры, что позволяет сократить время на проверку и выявления недочётов (у прокурора нет необходимости выезжать в каждый территориальный орган).

В соответствии с Приказом № 89 предусмотрена выдача отрывного талона-уведомления заявителю с идентифицирующим номером и оставление корешка талона-уведомления в органе уголовного преследования. На обороте талона-уведомления указаны адрес Интернет-ресурса, номера телефона, при помощи

[7] Долгов А. М. Электронное уголовное дело в досудебных стадиях уголовного процесса в России // Общество: политика, экономика, право. 2018. № 9 (62). С. 57; Собенин А. А. Актуальные вопросы регистрации заявлений и сообщений о преступлениях в условиях развития цифровых технологий // Вестник Воронежского государственного университета. Серия: Право. 2019. № 4 (39). С. 269.

[8] Приказ Генерального Прокурора Республики Казахстан от 19 сентября 2014 года № 89 «Об утверждении Правил приема и регистрации заявления, сообщения или рапорта об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований» // Информационно-правовая система нормативных правовых актов Республики Казахстан. [Электронный ресурс]. URL: https://adilet.zan.kz/rus/docs/V14W0009744 (дата обращения: 05.05.2023).

[9] Собенин А. А. Актуальные вопросы регистрации заявлений и сообщений о преступлениях в условиях развития цифровых технологий // Вестник Воронежского государственного университета. Серия: Право. 2019. № 4 (39). С. 269.

которых заявитель может получить информацию по поданному им заявлению, сообщению. Кроме того, приказом № 89 предусмотрена возможность уведомления участников уголовного процесса посредством модуля SMS-оповещения.

Законодатель Казахстана предусмотрел действия сотрудников в ходе нештатных ситуаций, в том числе отсутствии доступа в информационную систему. В таком случае уполномоченным сотрудником заполняются соответствующие документы на бумажном носителе и в течение 24 часов направляются в специальный орган для внесения сведений в информационную базу.

Анализ ведомственного нормативного акта Республики Казахстан, регулирующего уголовно-процессуальные правоотношения по приёму, регистрации сообщений и заявлений о правонарушениях, а также порядку введения государственного единого учёта заявлений и сообщений о преступлениях, позволил сделать следующие выводы о положительных эффектах использования автоматизированной базы:

1) упрощается процедура подачи заявлений, сообщений для граждан (они могут это осуществить при помощи Интернета, не затрачивая временные и финансовые ресурсы для непосредственного обращения в территориальные органы);

2) устраняется возможность волокиты при приёме и регистрации преступления;

3) минимизируется укрытие преступлений (вся поступающая онлайн-информация регистрируется и не подлежит изменению или удалению сотрудниками правоохранительной системы), что позволяет создать реальную картину преступности в стране;

4) появляется эффективный оперативный контроль за принятым решениям по поступившей информации (уполномоченные лица, в том числе прокуроры, в любой момент могут отследить в какой стадии находится зарегистрированная информация, не осуществляя выезд непосредственно в территориальный орган, что позволяет сократить временные затраты).

Понятна позиция скептиков-процессуалистов, которые утверждают, что внедрение цифровых технологий может нанести вред уголовному судопроизводству России. Они оперируют и угрозами обеспечения информации, и возможностью фальсификации, и стиранием грани между доказательствами и простой информации[10]. Однако россияне продолжают активно использовать различные мессенджеры, сайт государственных услуг РФ и ряд иных цифровых инструментов, не боясь вводить свои персональные данные и

[10] Зуев С. В. Электронное уголовное дело: за и против // Правопорядок: история, теория, практика. 2018. № 4 (19). С. 7–10; Чурикова А. Ю. Проблемы цифровизации российского уголовного процесса // Вестник СГЮА. 2021. № 6 (143). С. 212; Миронова Е. Ю. Нравственные начала уголовного процесса в условиях цифровизации: принципиальная незыблемость или неизбежная трансформация // Актуальные проблемы российского права. 2023. №1 (146). С. 138–139.

не задумываясь о негативных последствиях.

Резюмируя вышесказанное, мы считаем, что необходимо перенять положительный опыт постсоветских государств (в частности Казахстана) по внедрению автоматизированных цифровых систем в уголовный процесс России, что позволит ускорить всё судопроизводство, обеспечив процессуальные гарантии в виде защиты прав и свобод граждан.

Цифровизация уголовного процесса – необходимый шаг в развитии правоохранительной системы. Она позволяет значительно повысить эффективность работы всех участников уголовного процесса, обеспечить более быстрое рассмотрение уголовных дел и принятия по ним решений. При этом необходимо помнить, что при использовании с цифровыми технологиями необходимо соблюдать правила безопасности при обращении с информацией, относиться с максимальной ответственностью к применяемым данным.

Список литературы

1. Андреева О. И, Зайцева О. А. Перспективы ведения российского уголовного судопроизводства в электронном формате // Уголовная юстиция. 2018. № 12. С. 57–61.

2. Долгов А. М. Электронное уголовное дело в досудебных стадиях уголовного процесса в России // Общество: политика, экономика, право. 2018. № 9 (62). С. 55–57.

3. Зуев С. В. Электронное уголовное дело: за и против // Правопорядок: история, теория, практика. 2018. № 4 (19). С. 6–12.

4. Миронова Е. Ю. Нравственные начала уголовного процесса в условиях цифровизации: принципиальная незыблемость или неизбежная трансформация / Е. Ю. Миронова // Актуальные проблемы российского права. 2023. № 1 (146). С. 136–148.

5. Собенин А. А. Актуальные вопросы регистрации заявлений и сообщений о преступлениях в условиях развития цифровых технологий // Вестник Воронежского государственного университета. Серия: Право. 2019. № 4 (39). С. 266–273.

6. Чурикова А. Ю. Проблемы цифровизации российского уголовного процесса // Вестник СГЮА. 2021. № 6 (143). С. 209–216.

Anastasia M. Cherkasova
Adjunct postgraduate,
Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia,
(Nizhny Novgorod, Russian Federation)
Nastye4a@mail.ru

DIGITALIZATION OF THE STAGE OF INITIATING A CRIMINAL CASE

Abstract. Within the framework of the research analyzed the legislation of the Republic of Kazakhstan, which regulates legal relations at the stage of initiating of criminal applications and reports received by law enforcement agencies. The author identified positive trends in the use of an automated system and digital instruments, when receiving and registering messages and statements about incidents and proposed to adopt the positive experience of law enforcement practice of the Republic of Kazakhstan by introducing the use of digital technologies into the criminal procedure legislation at the stage of initiating a criminal case, namely the regulation of the procedure for admission and registration.

Keywords: automated system, digital instruments, reduction of the investigation terms, protection of rights and freedoms.

УДК 343.13; 004.85

Чурикова Анна Юрьевна
Кандидат юридических наук, доцент,
доцент кафедры административного и уголовного права
Поволжский институт управления – филиал РАНХиГС
(г. Саратов, Российская Федерация)
a_tschurikova@bk.ru

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЦЕЛЯХ УПРАВЛЕНИЯ РИСКАМИ УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Аннотация. Риск является неотъемлемой частью уголовно-процессуальной деятельности. В статье приводится перечень рисков, возникающих в деятельности правоохранительных органов, а также авторские определения риск-ориентированного подхода и системы управления рисками в уголовном судопроизводстве. Анализируются возможности использования искусственного интеллекта для управления рисками в деятельности правоохранительных органов. Рассматриваются механизмы обучения искусственного интеллекта и эффект «чёрного ящика» при принятии им решений. По итогам исследования сделан вывод о необходимости комплексного специального правового регулирования использования искусственного интеллекта правоохранительными органами.

Ключевые слова: уголовно-процессуальные риски, управление рисками, уголовный процесс, обучение искусственного интеллекта, прогнозирование рисков.

Для цитирования:
Чурикова А. Ю. Использование искусственного интеллекта в целях управления рисками уголовно-процессуальной деятельности правоохранительных органов // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 250–256.

Правоохранительные органы, в том числе в осуществляющие деятельность в сфере уголовного судопроизводства, зачастую действуют в условиях неопределённости. Непредсказуемость и сложность уголовно-процессуальной деятельности в самом своём понимании допускают возможность возникновения риска, о которых можно говорить в ситуациях, когда подразумеваются такие условия, как вариативность поведения и событийная вариативность.

Прогнозирование и учёт рисков в правоохранительной и уголовно-процессуальной деятельности является ключевым фактором выстраивания эффективной модели уголовного судопроизводства. При этом под риск-ориентированным подходом в уголовном процессе предлагаем

понимать выбор видов осуществляемых действий, объёмов затрачиваемых ресурсов (трудовых, материальных, временных и т. д.), содержания осуществляемых процессуальных действий (в том числе объёмы проверки, например, проверка уголовного дела полностью или в определённой части), интенсивности осуществляемых действий, а также перечня решений, которые могут быть приняты, в зависимости от категории риска. В связи с этим, управление рисками в уголовном процессе – это такое применение риск-ориентированного подхода, которое позволяет влиять на управляемые риски наступления неблагоприятных последствий, минимизируя их.

Активное технологическое развитие, появление аналитики больших данных, машинного обучения и программ искусственного интеллекта (далее «ИИ») оказывают колоссальное влияние на развитие современного общества и государства, в том числе и в сфере борьбы с преступностью, и способствуют возможности управления рисками уголовно-процессуальной деятельности.

В качестве одного из наиболее перспективных направлений цифровой трансформации правоохранительной деятельности и правосудия в науке активно обсуждается возможность использования искусственного интеллекта (далее – ИИ) в сфере уголовного судопроизводства[1]. Для большинства технологически развитых государств решение вопросов, связанных с внедрением систем на базе ИИ в уголовный процесс, представляется приоритетным.

Во многих научных исследованиях, посвящённых применению искусственного интеллекта в области юриспруденции, можно встретить предложения о принятии данными программами решений за профессиональных участников (судей, прокуроров, следователей)[2]. При этом авторы подобных предложений не рассматривают и не принимают во внимание особенности обучения искусственного интеллекта, для которого задействуются следующе методы, основанные на примерах или интеллектуальном анализе данных:

1) логические (эмпирическая индукция – TDIDT, AQ-алгоритм,

[1] Noriega M. The application of artificial intelligence in police interrogations: An analysis addressing the proposed effect AI has on racial and gender bias, cooperation, and false confessions // Futures. 2020. Vol. 117. DOI: 10.1016/j.futures.2019.102510; Суходолов А. П., Бычкова А. М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. № 6. С. 753–766; Использование искусственного интеллекта при выявлении, раскрытии, расследовании преступлений и рассмотрении уголовных дел в суде / Д. В. Бахтеев, Е. А. Буглаева, А. И. Зазулин [и др.]. Москва: Издательство «Юрлитинформ», 2022. 216 с.

[2] Поляков С. Б. Наше мнение: только искусственный интеллект принудит судью к справедливости // Вестник Московского университета МВД России. 2021. № 3. С. 213–218 DOI: 10.24412/2073-0454-2021-3-213-218; Колоколов Н. А. Искусственный интеллект в правосудии – будущее неотвратимо // Вестник Московского университета МВД России. 2021. №. 3. С. 201–212.

алгоритм FOIL, конструктивная индукция – CIA);

2) статистические (например, регрессия, PCA и т. д.);

3) вычислительные (анализ данных в динамических системах – BACON, LAGRANGE);

4) графы вычислений (т. н. искусственные нейронные сети).

То есть используются логические и математические алгоритмы, требующие, как правило, анализа большого массива данных (big-data).

Причём существующие механизмы обучения ИИ, как справедливо отмечают многие учёные, провоцируют эффект «чёрного ящика»[3], то есть непрозрачность и непонятность цепочек, которые приводят к выводам, представляемым ИИ.

Кроме того, в сфере судопроизводства для обучения соответствующей программы искусственного интеллекта необходимо, чтобы данной программой был проанализирован значительный объём принимаемых по различным делам решений. Однако никто не застрахован от ошибок правоприменителей, допускаемых ими при принятии решений. Эти ошибки при их систематическом характере будут накапливаться и имитироваться программами искусственного интеллекта. Обучение же программы искусственного интеллекта в «идеальных условиях» также может привести к возникновению в дальнейшем ошибок, связанных с невозможностью принятия и прогнозирования такими программами решений в реальной жизненной ситуации.

При обучении ИИ в сфере юриспруденции можно выделить ещё одну существенную проблему: довольно быстрые изменения законодательства. Искусственный интеллект принимает и прогнозирует решения, руководствуясь определёнными методами автоматизации рассуждений. Рассуждения ИИ основаны на эмпирических зависимостях в данных, либо связях между действиями и результатами этих действий, либо Байесовской вероятности[4]. В такой ситуации обучение искусственного интеллекта принятию решений в рамках правового поля представляется нецелесообразным. Однако, его использование для планирования или прогнозирования фактической ситуации представляется обоснованным и целесообразным, так как программы ИИ способны выявлять широкий спектр причинно-следственных связей.

Прогнозирование наступления неблагоприятных последствий и организация работы правоохранительных органов в соответствии с возможностью наступления того или иного события –

[3] Pasquale F. The black box society: The secret algorithms that control money and information. Harvard University Press, 2015. 310 p.; Završnik A. Criminal justice, artificial intelligence systems, and human rights // ERA Forum. Berlin, Heidelberg: Springer Berlin Heidelberg, 2020. Vol. 20. №. 4. Pp. 567–583.

[4] Вьюгин В. Математические основы машинного обучения и прогнозирования. Электронное издание. М.: МЦНМО, 2014. 304 с.

это фактически и есть управление рисками или риск-ориентированный подход в уголовно-процессуальной деятельности соответствующих органов. Считаем возможным, таким образом, говорить о перспективах использования программы искусственного интеллекта для оптимизации данных процессов. В связи с этим оценка риска совершения преступления, а также действий по выявлению и расследованию преступных деяний становятся всё более технологически сложными.

Для определения основных направлений применения ИИ по управлению рисками в уголовно-процессуальной деятельности правоохранительных органов, следует в начале обозначить, какие существуют основные риски при осуществлении данной деятельности:

1. Риски, связанные с субъектами, осуществляющими данную деятельность (недостаточный уровень компетентности, высокая загруженность, личностные объективные и субъективные качества отдельных субъектов и т. д.);

2. Риски, связанные с объектами, на которые направлено осуществление данной деятельности (объекты, требующие специальных познаний, объёмные, сложные в исследовании и анализе объекты и т. д.);

3. Риски, связанные с противодействием осуществлению уголовно-процессуальной деятельности;

4. Риски, связанные с нарушением установленного законом порядка осуществления уголовно-процессуальной деятельности.

Учитывая данные группы рисков, можно выделить следующие основные направления применения ИИ в деятельности по управлению рисками уголовно-процессуальной деятельности правоохранительных органов:

1) Помощь в выстраивании алгоритмов производства следственных и иных процессуальных действий. Например, анализ следственной ситуации и планирование следственных и иных действий; подготовка рекомендаций по фактическому порядку осуществления действий исходя из конкретной ситуации и т. д.

2) Распределение нагрузки в зависимости от компетентности и загруженности конкретного сотрудника.

3) Применение функций компьютерного зрения и распознания естественной речи.

4) Выявление причинно-следственных связей и анализ большого массива данных.

5) Прогнозирование ситуаций.

6) Отслеживание соответствия фактических действий и решений действующему законодательству, выявление индикаторов, которые могут указывать на нарушения уголовно-процессуального законодательства.

В настоящее время в работе правоохранительных органов уже активно применяются различные государственные информационные,

поисковые и экспертные системы[5]. Например, система «ФОРВЕР»[6], которая формирует наиболее вероятные версии о личности преступника либо информационная система «Посейдон»[7], применение которой должно способствовать противодействию коррупции. Кроме того, также функционируют ГИС «Зеркало», информационно-аналитические системы «Октопус», «ПСКОВ», программный комплекс «Биокон», экспертные системы «Наркоэкс», «Балэкс», «Кортик», «Мясо» и «Полюс», автоматизированная дактилоскопическая информационная система «Папилон» и другие. Все они помогают упростить процесс расследования и повысить эффективность работы правоохранительных органов благодаря быстрой и эффективной обработке больших объёмов информации и проведению анализа данных[8].

Государство предпринимает достаточно много действий для развития информационных систем и внедрения платформенных решений в сфере государственного управления. Однако этого недостаточно. Уже сейчас мы существенно отстаём в разработке и обучении программ ИИ для нужд уголовного судопроизводства. Отсутствует единая, проработанная концепция развития искусственного интеллекта в уголовно-процессуальной сфере. В Указе Президента Российской Федерации от 10.10.2019 г. № 490 применение ИИ в работе правоохранительных органов и уголовном судопроизводстве не рассматриваются как отдельные направления, требующие специфического регулирования и самостоятельных программ развития.

---

[5] См., например: Бессонов А. А. Использование алгоритмов искусственного интеллекта в криминалистическом изучении преступной деятельности (на примере серийных преступлений) // Вестник Университета имени О. Е. Кутафина (МГЮА). 2021. № 2. С 45–53. DOI: 10.17803/2311-5998.2021.78.2.045-053; Брушковский К. Б., Алмаганбетов П. А. Использование и перспективы автоматизированных информационно-поисковых систем в борьбе с преступностью // Вестник Института законодательства и правовой информации Республики Казахстан. 2020. №1 (59). С. 203–208; Толоконников В. К. Применение автоматизированных поисковых систем (АИПС) в следственной практике // Вестник Самарской гуманитарной академии. Серия: Право. 2015. №1-2 (17). С. 122–127

[6] Толстолуцкий В. Ю., Фесик П. Ю. Криминалистические значимые признаки, позволяющие определить пол преступника, при раскрытии убийств с помощью программы «ФОРВЕР» // Черные дыры в Российском законодательстве. 2009. № 4. С. 129–132.

[7] Указ Президента РФ от 25.04.2022 № 232 «О государственной информационной системе в области противодействия коррупции «Посейдон» и внесении изменений в некоторые акты Президента Российской Федерации» (вместе с «Положением о государственной информационной системе в области противодействия коррупции “Посейдон”»)» // СПС «КонсультантПлюс». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_415707/ (дата обращения 07.05.2023).

[8] Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Уголовный процесс и криминалистика. 2018. № 2. С. 43–49

В такой ситуации одной из ключевых проблем становится разрозненность правового регулирования использования информационных, поисковых, экспертных систем и ИИ в уголовно-процессуальной деятельности правоохранительных органов. Кроме того, отсутствуют стандартизированные требования к базам для обучения и самому обучению ИИ в этой области, что в целом может негативно сказаться на дальнейшей правоприменительной деятельности.

Таким образом, существует объективная необходимость проработки специального правового регулирования использования ИИ в уголовно-процессуальной деятельности правоохранительных органов, а также активизация политики, направленной на разработку и внедрение ИИ для управления рисками, возникающими в данной деятельности.

Список литературы

1. Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Уголовный процесс и криминалистика. 2018. № 2. С. 43–49.
2. Бессонов А. А. Использование алгоритмов искусственного интеллекта в криминалистическом изучении преступной деятельности (на примере серийных преступлений) // Вестник Университета имени О. Е. Кутафина (МГЮА). 2021. № 2. С 45–53. DOI: 10.17803/2311-5998.2021.78.2.045-053.
3. Брушковский К. Б., Алмаганбетов П. А. Использование и перспективы автоматизированных информационно-поисковых систем в борьбе с преступностью // Вестник Института законодательства и правовой информации Республики Казахстан. 2020. № 1 (59). С. 203–208.
4. Вьюгин В. Математические основы машинного обучения и прогнозирования. Электронное издание. М.: МЦНМО, 2014. 304 с.
5. Использование искусственного интеллекта при выявлении, раскрытии, расследовании преступлений и рассмотрении уголовных дел в суде / Д. В. Бахтеев, Е. А. Буглаева, А. И. Зазулин [и др.]. Москва: Издательство «Юрлитинформ», 2022. 216 с.
6. Колоколов Н. А. Искусственный интеллект в правосудии – будущее неотвратимо // Вестник Московского университета МВД России. 2021. №. 3. С. 201–212.
7. Поляков С. Б. Наше мнение: только искусственный интеллект принудит судью к справедливости // Вестник Московского университета МВД России. 2021. № 3. С. 213–218. DOI: 10.24412/2073-0454-2021-3-213-218.
8. Суходолов А. П., Бычкова А. М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. № 6. С. 753–766.

9. Толоконников В. К. Применение автоматизированных поисковых систем (АИПС) в следственной практике // Вестник Самарской гуманитарной академии. Серия: Право. 2015. №1-2 (17). С. 122–127.

10. Толстолуцкий В. Ю., Фесик П. Ю. Криминалистические значимые признаки, позволяющие определить пол преступника, при раскрытии убийств с помощью программы «ФОРВЕР» // Чёрные дыры в Российском законодательстве. 2009. № 4. С. 129–132.

11. Noriega M. The application of artificial intelligence in police interrogations: An analysis addressing the proposed effect AI has on racial and gender bias, cooperation, and false confessions // Futures. 2020. Vol. 117. DOI: 10.1016/j.futures.2019.102510

12. Pasquale F. The black box society: The secret algorithms that control money and information. Harvard University Press, 2015. 310 p.

13. Završnik A. Criminal justice, artificial intelligence systems, and human rights // ERA Forum. Berlin, Heidelberg: Springer Berlin Heidelberg. 2020. Vol. 20. №. 4. Pp. 567–583.

Anna Y. Churikova
PhD (Law), Associate Professor,
Associate Professor of Administrative and Criminal Law
Volga Institute of Management – Branch of Russian Presidential Academy of National Economy and Public Administration
(Saratov, Russian Federation)
a_tschurikova@bk.ru

ARTIFICIAL INTELLIGENCE APPLICATION FOR RISK MANAGEMENT IN CRIMINAL PROCEDURE ACTIVITIES OF LAW ENFORCEMENT AGENCIES

Abstract. Risk is an integral part of criminal procedure activity. The article provides a list of risks arising in the activities of law enforcement agencies, as well as the author's definition of the risk-based approach and risk management system in criminal proceedings. The possibilities of using artificial intelligence for risk management in the activity of law enforcement agencies are analysed. The mechanisms of artificial intelligence training and "black box" effect in decision-making by artificial intelligence are considered. As a result of research the conclusion about necessity of complex special legal regulation of use of artificial intelligence by law enforcement bodies is made.

Keywords: criminal procedure risks, risk management, criminal procedure, artificial intelligence training, risk prediction.

УДК 343.98

Шаталов Александр Семёнович
доктор юридических наук, профессор кафедры уголовного процесса
Московская академия Следственного комитета РФ
(г. Москва, Российская Федерация)
asshatalov@rambler.ru

АКТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ ОТ ПРЕСТУПНЫХ ПОСЯГАТЕЛЬСТВ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СФЕРЕ

Аннотация. В статье рассматриваются вопросы обеспечения защиты прав и законных интересов российских граждан в информационно-коммуникационной сфере от разного рода преступных посягательств. На фоне характерных примеров хищения их персональных данных и некоторых статистических обобщений автор предпринял попытку выяснить, почему прогресс в деле борьбы с киберпреступностью пока остаётся малозаметным. Он стремиться доказать, что меры по предотвращению, выявлению, раскрытию и расследованию киберпреступлений вообще, и онлайн-мошенничества, в частности, могут быть результативными не столько в национальном, сколько в международном масштабе, в силу транснационального характера самой сети «Интернет» и постоянного увеличения количества её пользователей.

Ключевые слова: искусственный интеллект, киберпреступность, персональные данные, электронно-цифровые доказательства, интернет-мошенничество.

Для цитирования:
Шаталов А. С. Актуальные вопросы защиты от преступных посягательств в информационно-коммуникационной сфере // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 257–263.

Направления развития информационного общества и подходы к его формированию в Российской Федерации, определены в соответствующей государственной Стратегии, рассчитанной на период с 2017 по 2030 гг.[1] Именно в ней в своё время было официально одобрено повсеместное и интенсивное использование органами государственной власти Российской Федерации, бизнесом и гражданами современных цифровых технологий. Более того, в ней впервые было

[1] Указ Президента Российской Федерации от 09. 05. 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_216363/ (дата обращения: 12.05.2023).

сформулирована принципиальная задача обеспечения защиты интересов российских граждан в информационно-коммуникационной сфере, в том числе от разного рода преступных посягательств. С некоторых пор решению этой задачи в нашей стране стало уделяться особое внимание, поскольку всё большее и большее влияние на практику защиты прав и законных интересов граждан стали оказывать стремительно меняющиеся способы анализа, передачи, получения и хранения данных, появившихся благодаря развитию современных информационно-коммуникационных технологий (Big Data, Blockchain и др.). Вместе с тем, с их появлением общие задачи российского уголовно-процессуального права и криминалистики не изменились. По большому счёту, они как и раньше призваны «…создать такие универсальные механизмы, которые, во-первых, отражали бы общечеловеческие ценности; во-вторых, предлагали бы универсальные правовые способы разрешения социальных конфликтов (основная функция права), независимые от сугубо политических или иных соображений целесообразности; и, наконец, переходя на иной уровень обобщения, способствовали бы сохранению мира и человечности, то есть нашей *цивилизации права»*[2].

Объём оцифрованных данных возрастает постоянно и с огромной скоростью. Целенаправленное исследование их многочисленных наборов при помощи стремительно ворвавшегося в нашу жизнь искусственного интеллекта позволяет обнаруживать новые корреляции, в т. ч. для целей всестороннего предварительного расследования преступлений и справедливого судебного рассмотрения уголовных дел. Фактически это становится не чем иным, как новым и весьма востребованным направлением процессуальной коммуникации, осуществляемой для получения, передачи и использования разнообразной криминалистически значимой информации. Её новизна нам видится отнюдь не в изменении сути процесса доказывания по уголовным делам, а в появившихся возможностях обогащения его содержания, вызванного принципиальным обновлением самих средств получения и передачи такой информации. Включившись в процесс глобальной цифровизации, российское уголовно-процессуальное право и отечественная криминалистика должны активно и своевременно рефлексировать на происходящие изменения общественной жизни. В противном случае, одобряемые ими процессуальные процедуры и научно обоснованные практические рекомендации, постепенно утратят своё рациональное содержание, а значит и признание в следственной и судебной практике. Более того, стремительные и постоянно возрастающие требования к цифровым навыкам участников уголовного

[2] Зорькин В. Д. Право будущего в эпоху цифр. Индивидуальная свобода или сильное государство? // Российская газета. Федеральный выпуск. 2020, 16 апр. № 83 (8137). С. 6.

судопроизводства могут привести к непониманию языка, предназначенного для поддержания устойчивой социальной связи между ними.

Для того, чтобы этого не случилось, на государственном уровне всё больше и больше внимания уделяется обеспечению цифровых прав граждан, особенно в части защиты их персональных данных и предоставления им самых широких возможностей отстаивать свои интересы в рамках национального правового пространства. На этом фоне особую тревогу вызывает непрекращающийся рост преступности в IT-сфере, где, например, в 2021 году преступлений было совершено на треть больше, чем за аналогичный предыдущий период[3]. Общее число имевших место уголовно наказуемых деяний, в которых использовались мобильные устройства, выросло на 32 % (т. е. более чем на треть), а с использованием информационных ресурсов всемирной паутины – почти наполовину (около 49 %). В сложившейся к настоящему времени ситуации стало очевидно, что на данном этапе цифровизации всех сфер общественной жизни искоренить киберпреступность вряд ли получится. Но это не препятствует разработке и созданию действенных механизмов для продолжительной и эффективной борьбы с нею. Правоохранительным органам государства сейчас, в частности, важно заниматься не только и не столько блокировкой тех или иных интернет-ресурсов, сколько выявлением создателей и популяризаторов разного рода мошеннических схем. Нужно последовательно добиваться и того, чтобы сами граждане вели себя в максимальной степени ответственно и умело реагировали на мошеннические проявления в своих аккаунтах и на посещаемых ими интернет-площадках. Данные официальной судебной статистики свидетельствуют о том, что в скорейшем совершенствовании нуждаются инструменты предотвращения утечек и хищений персональных данных, поскольку подавляющее большинство актов онлайн-мошенничества совершается в социальных сетях (примерно 60 %), через фейковые сайты (около 23 %) и мобильные приложения (около 6 %).

Мошенническими действиями ежегодно сопровождается примерно три четверти преступлений, совершаемых в IT-сфере. В их числе преобладают разнообразные проекты, с заведомо высоким риском потери собственных денежных средств и раскрытием персональных данных (т. н. скам) и получение доступа к конфиденциальным данным пользователей, в т. ч. логинам и паролям (т. н. фишинг). В качестве характерного примера можно привести случай, когда мошенники по поддельной нотариальной доверенности от имени журналистки, публиковавшей в региональных средствах массовой информации статьи на криминальные темы, смогли получить в салоне сотовой связи

[3] Мошенничество в сети: судебная практика и ключевые аспекты // RTM Group [Электронный ресурс]. 2023, 20 апреля. URL: https://rtmtech.ru/research/online-fraud-research/#anchor5 (дата обращения: 12.05.23).

детализацию её звонков и SMS-сообщений за два последних года. Её мобильный телефон и аккаунты в мессенджерах они также пытались взломать, но сделать это не удалось из-за их надёжной защиты. Узнав об этом, сама журналистка сразу же обратилась в полицию с заявлением о мошенничестве и незаконном использовании своих персональных данных. В другом случае, имевшем место в 2021 году во Владивостоке, жертвой шантажа стал молодой сотрудник салона одного из известных операторов мобильной связи. В социальной сети он общался на провокационные темы с девушкой, которая через непродолжительное время стала угрожать рассылкой их переписки его родным и знакомым. Впоследствии выяснилось, что «девушка» оказалась мужчиной, занимавшимся шантажом в сети. За своё молчание он требовал выкуп, но потерпевший заплатить его не смог. Узнав место, где последний работает, шантажист периодически стал просить его выяснить данные тех или иных абонентов и пароли для входа в их электронные личные кабинеты. Проникая в них, он настраивал переадресацию вызова на свой номер, получая таким образом пароли от аккаунтов в социальных сетях, а затем вымогал деньги у их владельцев.

Говоря о потерпевших от мошеннических действий такого рода важно понимать, что большинство из них – обычные люди, часто не знающие даже самых простых способов защиты своих прав в киберпространстве. Если их персональные данные были похищены (в т. ч. по халатности сотрудников онлайн-платформ или из-за несовершенства их защитных функций), то привлечение к уголовной ответственности самих мошенников, становится весьма и весьма проблематичным. Другими значимыми факторами, препятствующими их разоблачению, является масштабный характер утечек персональных данных и множественность каналов утечки информации, которыми обычно пользуются киберпреступники. В их числе:

– комплексы аппаратных и программных средств, предназначенные для хранения и оперативной обработки информации, серверы, персональные компьютеры, ноутбуки и др. (т. е. компьютерное оборудование);

– смартфоны, планшеты (т. е. мобильные устройства);

– CD, USB, карты памяти (т. е. съёмные носители);

– сетевые каналы, используемые для отправки данных через веб-интерфейс;

– электронная почта (личная и корпоративная);

– IM – сервисы мгновенных сообщений, предназначенные для передачи текстовой, аудио- и видеоинформации с использованием мессенджеров;

– документы на бумажном носителе и др.

По данным российского экспертно-аналитического центра InfoWatch, только за 2020 год российскими правоохранителями было выявлено 2722 факта утечек информации, в которых они фигурировали. Крупнейшими стали утечки баз данных москвичей,

переболевших коронавирусом, клиентов «РЖД Бонус», портала «SuperJob.ru», школы английского языка «Skyeng», заёмщиков микрофинансовых организаций и сервиса «Премиум бонус». Все они по разным причинам не смогли исключить незаконные доступы к собственной клиентской базе. Отрицательным последствием таких утечек стало то, что количество несанкционированных электронных операций выросло на 34 % (до 773 008)[4]. Следовательно, ещё одной острой проблемой, нуждающейся в скорейшем решении в деле борьбы с киберпреступностью вообще и с онлайн-мошенничеством в частности, является локализация корпоративных баз данных о россиянах в пределах национальной юрисдикции. Необходимость этого вызвана множеством факторов, среди которых следует выделить:

– увеличение объёмов информации, обрабатываемой и хранимой в киберпространстве;

– её «привлекательность» для преступников;

– нестандартность, сложность и постоянное обновление способов хищения персональных данных;

– длительную неосведомлённость потерпевших о факте их совершения;

– повышенную скрытность совершения преступных действий и отсутствие их связи с определённой территориальной локацией;

– существование объективных сложностей выявления, раскрытия и расследования преступлений, совершаемых в киберпространстве;

– отсутствие возможности «… предотвращения и пресечения преступлений данного вида традиционными средствами»[5].

Всё сказанное подтверждает правильность позиции, доминирующей среди российских криминалистов, о том, что борьба с киберпреступностью может стать эффективной только при условии, если она приобретёт международный масштаб. Дополнительным подтверждением этому является тот факт, что все современные девайсы, интернет-сервисы, теле -, радиотехника, транспорт, связь, промышленные, производственные комплексы не только прочно связаны с «Интернетом», но и управляются извне. Следовательно, всё большее и большее значение в доказывании по уголовным делам приобретают цифровые следы, предопределяя, таким образом, необходимость преумножения и применения сотрудниками российских правоохранительных органов комплекса компетенций из сферы компьютерных и сетевых технологий, в т. ч. основанных на использовании методов искусственного интеллекта.

Сам процесс выявления, раскрытия и предварительного расследования преступлений, совершённых с использованием

[4] Исследование судебной практики по преступлениям, связанным с неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации в 2021 году // Экспертно-Аналитический центр InfoWatch. 2022. С. 11.

[5] Осипенко А. Л. Сетевая компьютерная преступность. Монография. Омск: Омская акад. МВД России, 2009. С. 109–110.

современных информационных технологий, имеет множество характерных особенностей. Ошибки, допускаемые при этом следователями и дознавателями, нередко являются следствием их неудовлетворительной профессиональной подготовки, именно для этого сегмента познавательной деятельности. Одной из наиболее существенных причин низкого качества предварительного расследования преступлений, совершаемых в киберпространстве, следует признать отсутствие таких методических разработок, где был бы в полной мере задействован искусственный интеллект. В таких условиях объективные сложности обнаружения, фиксации и изъятия криминалистически значимой информации с целью её дальнейшего использования в качестве доказательств по уголовному делу нередко становятся непреодолимыми. Более того, здесь как нигде высока вероятность того, что те доказательства, что всё же были обнаружены, могут быть непреднамеренно изменены и даже утрачены, как в результате допущенных ошибок при их фиксации или, например, изъятии, так и в ходе их исследования. Подготовка в ходе досудебного производства по уголовному делу доказательств такого рода для дальнейшего представления их в суде требует обязательного наличия не только основательной профессиональной подготовки, но и регулярного обновления имеющихся знаний у лиц, ответственных за ход и исход производства по уголовному делу.

Список литературы

1. Зорькин В. Д. Право будущего в эпоху цифр. Индивидуальная свобода или сильное государство? // Российская газета. Федеральный выпуск. 2020. 16 апр. №83 (8137). С. 6.

2. Осипенко А. Л. Сетевая компьютерная преступность. Монография. Омск: Омская акад. МВД России, 2009. 479 с.

Alexander S. Shatalov
Doctor of Law, Professor of the Department of Criminal Procedure
Moscow Academy of the Investigative Committee of the Russian Federation
(Moscow, Russian Federation)
e-mail: asshatalov@rambler.ru

CURRENT ISSUES OF PROTECTION AGAINST CRIMINAL ATTACKS IN THE INFORMATION AND COMMUNICATION SPHERE

Abstract. The article deals with the issues of ensuring the protection of the rights and legitimate interests of Russian citizens in the information and communication sphere from various kinds of criminal encroachments. Against the background of typical examples of the theft of their personal data and some statistical generalizations, the author

made an attempt to find out why progress in the fight against cybercrime has so far remained little noticeable. He strives to prove that measures to prevent, detect, detect and investigate cybercrime in general, and online fraud in particular, can be effective not so much on a national as on an international scale, due to the transnational nature of the Internet itself and the constant increase the number of its users.

Keywords: artificial intelligence, cybercrime, forensics, personal data, crime investigation, criminal procedure, digital technologies, digital evidence.

УДК 347.963

Яровой Александр Валерьевич
декан факультета, кандидат юридических наук, доцент
Иркутский юридический институт (филиал)
Университета прокуратуры Российской Федерации
(г. Иркутск, Россия)
jam98@yandex.ru

ВОПРОСЫ ПРАВОВОГО РЕЖИМА ОБЪЕКТА ГРАЖДАНСКИХ ПРАВ, СОЗДАННОГО С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В статье на основе анализа разграничения понятий искусственный интеллект и нейронная сеть рассматриваются подходы к определению места искусственного интеллекта в гражданском правоотношении. Обосновывается несостоятельность подхода по его отнесению к субъекту права. На основе анализа действующего законодательства и сущностных признаков обосновывается необходимость специального правового регулирования создания новых нейронных сетей. Предлагаются формы договорных связей создания нейросети.

Ключевые слова: искусственный интеллект, нейронные связи, гражданское правоотношение, воля, интерес.

Для цитирования:
Яровой А. В. Вопросы правового режима объекта гражданских прав, созданного с использованием технологий искусственного интеллекта // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 264–269.

Искусственный интеллект (далее – ИИ) может использоваться для благих целей: диагностики заболевания и поиска лекарства от рака, развивать возобновляемую энергетику, – но участие ИИ в создании текстов произведений литературы, науки, музыки, объектов изобразительного искусства влечёт угрозу человеческой цивилизации из-за вмешательства в сферу творческой деятельности авторов. Многие дискутируют о применении нейросети в написании ученических работ, но есть более вредоносные и общественно опасные сферы: политика, мораль, религия, пропаганда, изготовление фейковых новостей. Применение ИИ может оказывать «разрушительное» влияние на человеческий интеллект, устои человечества. С сотворения мира бок о бок существует добро и зло, так и результаты применения ИИ создают «новую реальность» человеческого бытия, но с теми же морально-этическими категориями и проблемами.

ИИ должен являться инструментом в руках человека, а не его конкурентом. Сокращаются циклы

проектирования, с помощью ИИ более быстрыми темпами ведутся разработки лекарств, медицинского оборудования, создаются геномные и клеточные технологии, развивается синтетическая биология. Человечество получило уникальную возможность избавиться от рутинных процессов, не соответствующих творческим возможностям личности.

Основоположником понятия «искусственный интеллект» принято считать Д. Маккарти, который впервые использовал его во время своего выступления с докладом на конференции Дартмутского университета в 1956 году в значении «науки и технологии создания интеллектуальных машин, в частности, интеллектуальных компьютерных программ»[1]. С момента появления ИИ не утихают споры о его месте в гражданском правоотношении.

1. Отнесение к субъекту гражданского правоотношения: концепция «электронного лица»[2], «квазисубъекта гражданского правоотношения – робота»[3], «аналогия юридического лица»[4].

Такое решение не отражает сущности ИИ в общем и нейронной сети, в частности. Использование математического подхода, отражающего упрощённый подход к процессу функционирования головного мозга человека, не позволяет проводить подобные аналогии. При характеристике субъекта гражданского права используются категории **«воля»** и **«интерес»**. Человек как участник гражданских отношений обладает волей. Согласно устоявшимся взглядам, воля является внутренним сформированным желанием лица стать участником гражданских правоотношений, порождать юридические последствия путём возникновения, изменения и прекращения гражданских прав и обязанностей. Субъект, действуя в отношениях, изъявляет свою волю. Осуществление гражданских прав и исполнение обязанностей позволяет реализовывать законные интересы лица. Несомненно, в отдельных отношениях он может действовать в чужом интересе, но это возникает на основе закона или обязательства, при этом волевой характер поведения сохраняется.

Нейросеть выполняет установки, заложенные её создателем. Принятие волевого (инициативного) решения, направленного на реализацию собственного интереса исключено.

---

[1] Селезнёв М. Как искусственный интеллект становится эффективным бизнес-инструментом // РБК Тренды. [Электронный ресурс]. 2021, 10 февраля. URL: https://trends.rbc.ru/trends/industry/cmrm/60224ec09a79475d351c0503 (дата обращения: 17.05.2022).

[2] Мохат П. М. Концепт электронного лица в классификации субъектного состава лиц в гражданском праве // Пермский юридический альманах. 2019. № 2. С. 273–282.

[3] Ирискина Е. Н., Беляков К. О. Правовые аспекты гражданско-правовой ответственности за причинение вреда действиями робота как квазисубъекта гражданско-правовых отношений // Гуманитарная информатика 2016. № 10. С. 63–72.

[4] Бегишев И. Р. Искусственный интеллект и робот как правовые категории // Безопасность бизнеса. 2020. № 6. С. 32–36.

При всём развитии ИИ, созданные им результаты носят прикладной характер, и их самостоятельность ограничена. Отсутствует «божья искра» на самостоятельное познание мира, и такой подход должен сохраниться в дальнейшем. Возможности самообучения не представляют угрозы для человечества, так как дальнейшее развитие ИИ не приводит к появлению собственной воли и своих интересов.

Применение аналогии с конструкцией юридического лица невозможно к ИИ, так как несмотря на искусственный характер такого субъекта волеобразующим и волеизъявляющим органом юридического лица всегда выступает человек.

Вызывает сомнение необходимость применения «субъектной» природы ИИ с точки зрения правовых результатов. Субъекты гражданского права обладают юридическим равенством, автономией воли, имущественной самостоятельностью. Невозможно создать нового субъекта гражданского права «с исключениями», например, наделив его только самостоятельной ответственностью.

2. Признание ИИ объектом гражданского правоотношения: робот (ИИ) как разновидность вещей, с применением правил о плодах, продукции и доходах[5], как разновидность программ для ЭВМ[6], в качестве топологии интегральных микросхем.

Представляется, что в «объектном» подходе происходит отождествление процесса (ИИ), его результата (созданного продукта, например, отдельной нейросети) и его применения (использование в механизме, технологии).

ИИ следует рассматривать как направление развития научно-технического прогресса в области разработки и применения математических методов в интеллектуальных системах на основе использования научных достижений человечества. ИИ – это область научных разработок, создание новых сфер применения. В настоящий момент создаются новые матрицы ИИ, которые призваны кардинальным образом изменить человеческую цивилизацию. Необходимо сохранить прикладной характер, проводимых исследований. Ограничить (запретить) разработки в определённых вредоносных сферах. Мировому сообществу необходимо определить основные общие подходы к ИИ на основе представлений о гуманности и морали.

Нейронная сеть является одним из математических методов ИИ, и строится на представлениях о работе головного мозга человека. Соответственно, являясь частью ИИ, создаваемые новые сети выступают в качестве результатов интеллектуальной деятельности

[5] Гурко А. В. Искусственный интеллект и авторское право: взгляд в будущее // Интеллектуальная собственность. Авторское право и смежные права. 2017. № 12. С. 7–18.

[6] Дурнева П. Н. Искусственный интеллект: анализ с точки зрения классической теории правосубъектности // Гражданское право. 2019. № 5. С. 30–34.

(нейронная сеть первого рода). В рамках действующего законодательства выделяются:

– Объекты патентного права: изобретения, полезные модели, промышленные образцы. Общей чертой объектов патентного права является их повторимость, то есть возможность создания результата разными лицами независимо друг от друга. В связи с чем проверка новизны результата зависит от даты обращения с заявкой в патентное ведомство. Нейросеть может быть содержательно отнесена к такому виду изобретения, как способу. Однако характеристикой новизны выступает оригинальность решения. Использование признака промышленной применимости для созданной нейросети представляется нецелесообразным так как её применение возможно в абсолютно разных сферах жизнедеятельности.

– Программы ЭВМ и базы данных. Нейросеть по способу создания не является линейным алгоритмом. Нейронная сеть – это более сложный механизм, основное отличие которого от программы для ЭВМ заключается в том, что последняя не может обучаться и сопоставлять предоставленные ей данные, тогда как нейросеть может развиваться, анализировать алгоритм выполнения установленной цели и изменять его в зависимости от полученного результата, а значит выполнять более сложные задачи. Говоря простым языком, у программы для ЭВМ всегда есть «исходный план», которого она придерживается, а у нейросети есть цель, которую он пытается достичь посредством изменения входных данных до тех пор, пока не добьётся наиболее точного результата.

– Топологии интегральных микросхем. В соответствии со статьёй 1448 ГК РФ топология интегральных микросхем представляет собой «зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы и связей между ними». Посредством отдельных элементов интегральной микросхемы происходит преобразование аналогового сигнала в цифровую форму. Принцип формирования материального носителя (кристалла) заключается в соединении одной интегральной микросхемы с другой, что позволяет реализовать быстродействие и количество выполняемых задач. Далее интегральная микросхема обрабатывает полученную информацию и выполняет определённые команды, необходимые пользователю. Принцип работы интегральной микросхемы напоминает устройство нейросети, когда поступающая информация передаёт импульсы с одного искусственного нейрона на другой, в результате чего также происходит выполнение определённой задачи. Однако моделирование искусственного нейрона по принципу работы головного мозга человека – это больше программное установление взаимодействия, нежели передача информации с одной интегральной микросхемы на другую.

На основании изложенного можно сделать вывод, что создание матрицы нейронной сети является результатом интеллектуальной

деятельности, если обладает признаками новизны и оригинальности. Сеть не относится ни к одному из закреплённых действующим законодательством результату интеллектуальной деятельности. Прослеживается необходимость отдельного регулирования данного объекта в рамках общих подходов, заложенных частью 4 ГК РФ, к регулированию результатов интеллектуальной деятельности. Закрепление в национальном законодательстве регламентации отношений по созданию и использованию новых нейронных сетей позволит выработать позицию Российской Федерации по определению подходов в рамках конвенционального регулирования.

Создание нейронных сетей для выполнения какой-либо функции на основе имеющейся математической матрицы (нейронная сеть второго рода), следует отнести к продукции как разновидности вещей. Создание нейросети возможно на основе договора о выполнении научно-исследовательских работ или ином договоре подрядного типа.

Представляется целесообразным установление международного и национального механизма верификации нейронных сетей (как первого, так и второго рода). Если верификация нейронных сетей первого рода позволит защищать права авторов на результаты интеллектуальной деятельности (с соблюдением баланса интересов автора и общества), то верификация нейронных сетей второго рода необходима для отражения соответствия сети нормам морали и нравственности, а также идентификации создателя, прохождение верификации должно быть необходимым условием для применения нейронной сети в различных товарах (механизмах, роботах, устройствах, технологиях), а также системах.

И последнее, можно ли отнести созданные нейросетью объекты к результатам интеллектуальной деятельности?

Необходимо отметить, что гражданское законодательство не закрепляет понятия «творчество», предоставляя любому автору возможность создания охраняемых результатов интеллектуальной деятельности. Основной критерий, отличающий творчество от изготовления (производства), – уникальность его результата, то есть создание нового, ранее неизвестного.

Нейронная сеть генерирует результаты своей деятельности на основе уже существующих, ранее известных объектов в той или иной области искусства, в то время как процесс творчества предполагает создание нового, уникального результата интеллектуальной деятельности. По своей сути, результат деятельности нейросети – это простая компоновка ранее существовавших объектов авторского права, которая не отличается новизной, уникальностью, неповторимостью или оригинальностью.

В связи с этим можно говорить о том, что творческий результат не прослеживается в объектах, создаваемых искусственным интеллектом. По тем же причинам наличие творческой деятельности не видится и в ситуациях, когда

искусственный интеллект при создании объектов самообучался независимо от разработчика при помощи сторонних программ.

Список литературы

1. Бегишев И. Р. Искусственный интеллект и робот как правовые категории // Безопасность бизнеса. 2020. № 6. С. 32–36.
2. Гурко А. В. Искусственный интеллект и авторское право: взгляд в будущее // Интеллектуальная собственность. Авторское право и смежные права. 2017. № 12. С. 7–18.
3. Дурнева П. Н. Искусственный интеллект: анализ с точки зрения классической теории правосубъектности // Гражданское право. 2019. № 5. С. 30–34.
5. Ирискина Е. Н., Беляков К. О. Правовые аспекты гражданско-правовой ответственности за причинение вреда действиями робота как квазисубъекта гражданско-правовых отношений // Гуманитарная информатика 2016. № 10. С. 63–72.
6. Морхат П. М. Концепт электронного лица в классификации субъектного состава лиц в гражданском праве // Пермский юридический альманах. 2019. № 2. С. 273–282.

Alexander V. Yarovoy
Dean of the Faculty, PhD in Law, Associate Professor
Irkutsk Institute of Law (branch) of the University of Public Prosecutor's Office of the Russian Federation
(Irkutsk, Russia)
e-mail: jam98@yandex.ru

ISSUES OF LEGAL REGIME OF CIVIL RIGHTS OBJECTS CREATED WITH THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGY

Abstract. The article based on the analysis of the differentiation of the concepts of artificial intelligence and neural network, the article discusses approaches to determining the place of artificial intelligence in civil law relations. The inconsistency of the approach to its attribution to the subject of law is substantiated. Based on the analysis of the current legislation and essential features, the necessity of special legal regulation of the creation of new neural networks is substantiated. The forms of contractual connections for creating a neural network are proposed.

Keywords: artificial intelligence, neural connections, civil legal relationship, will, interest.

УДК 343.98

Яшин Александр Александрович
Старший преподаватель кафедры криминалистики
Саратовская государственная юридическая академия
(г. Саратов, Российская Федерация)
alek1811@rambler.ru

Шутова Виктория Алексеевна
Студент Института юстиции,
Саратовская государственная юридическая академия
(г. Саратов, Российская Федерация)
vika.shutova.02@bk.ru

К ВОПРОСУ О НЕОБХОДИМОСТИ ПРИМЕНЕНИЯ КРИМИНАЛИСТИЧЕСКОГО ПРОФАЙЛИНГА В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Аннотация. В статье рассматривается понятие криминалистического профайлинга, анализируется зарубежная и отечественная практика применения психологического профилирования, раскрывается методика составления психологического портрета предполагаемого преступника, изучается возможность обучения сотрудников правоохранительных органов использованию методики профилирования.

Ключевые слова: криминалистическое профилирование, профайлинг, виктимологическое профилирование, географическое профилирование, психологический портрет преступника.

Для цитирования:
Яшин А. А., Шутова В. А. К вопросу о необходимости применения криминалистического профайлинга в деятельности правоохранительных органов // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 270–277.

Развитие науки и техники затрагивает все сферы человеческой жизни, в том числе и такую специфическую её область как расследование преступлений. Ежегодно в практику должностных лиц, осуществляющих производство по уголовному делу, внедряются новые технологии, средства и методы ведения следственных действий, помогающие в раскрытии самых сложных и запутанных преступлений. Одним из закономерных шагов в процессе модернизации криминалистических средств является широкое применение способов раскрытия преступлений, непосредственно связанных с человеком, особенностями его личности и поведения, которые не

всегда возможно изучить путём применения традиционных и наиболее популярных методов криминалистического исследования, в частности профайлинга.

Для производства дальнейшего исследования необходимо дать определение понятию «профайлинг». Итак, профайлинг определяется специалистами как совокупность психологических методов прогнозирования и оценки поведения человека на основе анализа его наиболее информативных частных признаков, характеристик внешности, вербального и невербального поведения[1]. Сущность криминалистического профайлинга заключается в определении личности преступника исходя из способа, характера, обстановки и условий совершения преступления. Говоря простыми словами, специалист-профайлер составляет психолого-криминалистический портрет предполагаемого преступника, в котором указывает пол, возраст, уровень образования и предполагаемое место работы злоумышленника, его отличительные личностные характеристики, на которые следователю необходимо обратить внимание при его поимке, задержании, а также при проведении с его участием различных следственных действий.

Практическая эффективность метода криминалистического профилирования была доказана ещё в 1956 году: благодаря профилю, составленному американским психиатром Джеймсом Брасселом, следственные органы смогли вычислить и задержать серийного бомбиста, подорвавшего в Нью-Йорке более 50 взрывных устройств. Специалист изучил предоставленные ему материалы розыскного дела и предоставил правоохранителям следующие данные: преступником предположительно является мужчина славянской внешности, средних лет, аккуратный, религиозный, субъект проживает совместно с женщиной старше себя, хорошо разбирается в механике и электронике, мотивом преступления по мнению психиатра, явился недавний стресс, например, увольнение с работы. Арестованным преступником оказался 54-летний поляк, электрик по специальности, еженедельно посещавший церковь и проживавший в одной квартире со своими старшими сёстрами. В ходе проведения допроса полиции удалось выяснить, что подозреваемый, действительно, в последнее время был сильно подвержен стрессу из-за увольнения с работы, что и побудило его к совершению преступления[2].

Обращаясь к исследователям XX века, нельзя не отметить достижения в области психологического профилирования (разработку термина «серийный убийца», типологии серийных убийц, детализацию метода профилирования и т. д.) американского криминолога и специального агента ФБР Роберта Ресслера. Пользуясь

[1] Профайлинг в деятельности органов внутренних дел : учебное пособие / В. В. Вахнина и др. М.: Академия управления МВД России, 2018. С. 23.

[2] Brussel J. Casebook of a Crime Psychiatrist. Bernard Geis Associates, 1968.

своими знаниями в области психологии и методикой профилирования, Ресслер исследовал и участвовал в раскрытии преступлений таких серийных убийц как Ричард Чейз (Убийца-вампир), Джеффри Дамер, Девид Берковиц и т. д. Методика Ресслера заключалась в тщательном исследовании места происшествия, следов преступления, тела жертвы, а также обстоятельств совершения противоправного деяния. На основе выявленных фактов учёный находил закономерности в поведении убийцы, которые указывали на его пол, возраст, социальное положение и в итоге помогали правоохранителям вычислить и задержать преступника[3]. Метод Ресслера высоко оценили в США, о чём свидетельствует создание в структуре ФБР такого подразделения как Отдел анализа поведения, который занимается психологическим профилированием преступников.

Активное внедрение профайлинга в деятельность следственных органов не является чем-то уникальным и присущим только американской юрисдикции, о необходимости широкого применения данного криминалистического метода уже не один год рассуждают правоведы. В российской практике профайлинг появился в середине XX века, анализируя зарубежный опыт, исследователи пришли к выводу, что в отечественную практику расследования преступлений необходимо внедрить относительно молодой криминалистический метод – профайлинг. Криминалистическое профилирование было раскрыто в трудах таких советских учёных как В. М. Бехтерев, И. П. Павлов, А. Н. Леонтьев и др.[4] Таким образом, уже в XX веке советскими, а затем и российскими теоретиками была отмечена высокая эффективность криминалистического профилирования, начались разговоры о возможности его применения на практике.

Позитивные результаты советского опыта использования криминалистического профилирования в деятельности органов правопорядка не остались незамеченными современными теоретиками и практиками. На сегодняшний день в России профайлинг применяется в качестве одного из средств защиты личности, общества и государства от террористических угроз[5]: методы психологического профилирования для реализации указанной цели применяются на крупных железнодорожных станциях, а также в сфере авиаперевозок. Таким образом методика профайлинга способствует обеспечению в нашей стране транспортной безопасности:

[3] Ressler R., Burgess A., Douglas J. Criminal Profiling Research on Homicide. New York: Unpublished Research Report, 1982. 70 p.

[4] Ветрова Т. В., Яковлев Е. В., Гневышев Е. Н., Смирнов А. А., Леонтьев О. В. Психофизиологические и морфофункциональные основы профайлинга: Учебное пособие. СПб.: Изд-во Университета при МПА ЕврАзЭС, 2021. С. 7.

[5] Ветрова Т. В., Яковлев Е. В., Гневышев Е. Н., Смирнов А. А., Леонтьев О. В. Психофизиологические и морфофункциональные основы профайлинга: Учебное пособие. СПб.: Изд-во Университета при МПА ЕврАзЭС, 2021. С. 13.

сотрудники полиции, обеспечивающие безопасность на транспорте, должны обладать развитыми навыками наблюдения и оперативного определения типа, находящегося перед ними пассажира (является ли данный пассажир потенциально не опасным или потенциально опасным, т. е. подозрительным, представляющим угрозу). В данном случае профилирование помогает органам внутренних дел своевременно выявить подозрительных личностей в районе транспортных узлов и предотвратить готовящийся террористический акт.

В качестве ещё одного перспективного и востребованного в Российской Федерации направления криминалистического профилирования можно выделить профайлинг при проведении массовых мероприятий. Сложность в данном случае заключается в необходимости оценить поведение большого числа людей (например, при обеспечении безопасности различного рода спортивных соревнований), естественно, в таких условиях сотрудники органов правопорядка не обладают возможностью находить в непосредственном контакте с наблюдаемыми лицами, поэтому существенную роль в обеспечении безопасности играет система видеонаблюдения. Сотрудников органов внутренних дел обучают навыкам отслеживания с помощью видеокамер, передающих на специальные мониторы изображение с массовых мероприятий, подозрительных лиц, которые могут нести потенциальную угрозу. Исследователями отмечается, что одновременная работа нескольких специалистов-профайлеров по наблюдению за проведением мероприятий способствует оперативному и эффективному выявлению правонарушителей[6].

В отечественной практике психологическое профилирование зарекомендовало себя как прогрессивный и эффективный криминалистический метод, оказывающий значительное содействие в раскрытии личности преступника. Приведём несколько наглядных примеров: расследование уголовного дела по факту убийства сотрудника ДПС в Калужской области в 2009 году[7]. Преступление было совершено с поражающей жестокостью: инспектору были нанесены множественные проникающие ножевые ранения в область шеи и грудной клетки. Долгое время у следствия не было информации о личности подозреваемого, вещественных доказательств (крови, слюны, личных вещей или фрагментов одежды преступника) на месте происшествия обнаружено не было. Позднее следователем было принято решение о привлечении к данному делу в качестве специалистов профайлеров,

[6] Кудин В. А., Статный В. М. Профайлинг в деятельности органов внутренних дел: от теории и методологии к практике // Вестник Санкт-Петербургского университета МВД России. № 3. 2013. С. 4–15.

[7] Возбуждено дело по факту убийства автоинспектора в Калуге // СКП [Электронный ресурс]. URL: https://ria.ru/20091201/196411166.html (Дата обращения 22.02.2023).

чтобы последние с помощью своих специальных знаний проанализировали место совершения преступления, характер нанесённых жертве ранений и составили психологический портрет преступника, который позволил бы сузить круг подозреваемых или определить траекторию поисков. Специалисты дали следующее заключение: преступником является мужчина в возрасте от 25 до 30 лет, физически хорошо развитый, имеющий среднее специальное образование, он часто меняет место работы и ранее уже был судим за совершение насильственного преступления, является сельским жителем и владеет навыком забоя скота. Примечательно, что в ходе дальнейшего расследования (с учётом характеристик портрета) была установлена личность преступника: им оказался 27-летний мужчина, проживающий в частном доме, ранее работавший разнорабочим, будучи несовершеннолетним молодой человек убил своего отца топором[8]. Данный пример иллюстрирует эффективность применения криминалистического профилирования при расследовании сложных уголовных дел.

Ещё одним знаковым примером необходимости использования профайлинга в правоохранительной деятельности можно считать сотрудничество органов следствия и психиатра А. О. Бухановского во время расследования череды громких серийных убийств (дела А. Р. Чикатило и Ю. Л. Цюмана)[9]. Врач изучал материалы уголовных дел: протоколы осмотра мест происшествий и приложения к ним, акты вскрытий, свидетельские показания; это помогло психиатру в обоих случаях достаточно чётко составить портеры маньяков. В частности, А. О. Бухановский смог установить примерный возраст Чикатило, а также указал на особенность личности – возможность получения сексуального удовлетворения только в обстановке абсолютного господства над жертвой.

Указанные примеры как из зарубежной, так и из отечественной практики являются наглядной демонстрацией того, что метод криминалистического профилирования, зародившийся ещё в XIX веке и получивший значительное развитие в XX, в современных реалиях всё чаще применяется правоохранительными органами как для пресечения готовящихся преступлений, так и для расследования уже совершённых. Данный факт может свидетельствовать о признании органами правопорядка эффективности профайлинга как криминалистического метода.

[8] Криминальный профайлинг: следственная и экспертная практика составления поискового психологического портрета (профиля) неизвестного лица по уликовым признакам и совокупности обстоятельств совершённого преступления // Академия Детекции Лжи [Электронный ресурс]. URL: https://akademy-dl.ru/press-centr/publikacii-nashih-ekspertov/kriminalnyj-profajling-sledstvennaya-i-ekspertnaya-praktika-sostavleniya-poiskovogo-psihologicheskog (Дата обращения 22.02.2023).

[9] Попов В. В., Тройченко Ю. Ю. Психологический портрет как способ идентификации личности // Юристъ-Правоведъ. 2019. № 3. С. 137–141.

Отвечая на вопрос «Для чего сотрудникам правоохранительных органов нужно знать методику профайлинга и уметь применять её в своей практической деятельности?», необходимо дать следующие разъяснения.

Во-первых, сотрудник органа охраны и защиты правопорядка ограничен законом сроками проведения расследования, знание же основ и методов психологического профилирования, а также понимание способов его применения позволит должностным лицам сузить круг подозреваемых по уголовному делу, в более короткий срок разыскать преступника.

Во-вторых, профайлинг позволяет следователю оперативно определить личностные особенности участника уголовного процесса, разработать стратегию проведения допроса, как говорится «найти подход», что особо важно при допросе подозреваемого.

В-третьих, применение метода психологического профилирования при поимке преступника помогает сузить район поиска предполагаемого подозреваемого. Оценка места преступления, его местоположения, характер оставленных следов позволяет определить, каким типом преступников было совершено деяние, а зная характеристики каждого из типов, следователь или дознаватель может сделать вывод о размере радиуса поиска предполагаемого преступника.

В-четвёртых, одним из видов криминалистического профилирования является виктимологическое профилирование. Говоря простым языком, сотрудники правоохранительных органов должны фокусировать своё внимание не только на преступнике, но и на жертве преступления, при помощи профайлинга определять её личностные характеристики. В ходе работы над уголовным делом должностному лицу необходимо поставить перед собой вопрос «Почему именно это лицо стало жертвой преступления?» и найти на него ответ. Подобная практика способствует уточнению профиля преступника, его детализации и лучшему пониманию мотивов совершения преступления, что позволит спрогнозировать поведение злоумышленника, предотвратить совершение новых противоправных деяний.

В настоящее время в России криминалистический профайлинг активно развивается, методика его применения модернизируется. Учёные считают, что необходимо регламентировать в законодательстве методические рекомендации по составлению психологических портретов[10], поскольку в зарубежной практике и в некоторых областях российского правоприменения криминалистическое профилирование зарекомендовало себя как один из эффективных методов борьбы с преступностью, а также средство

[10] Карпенко О. А. Криминалистический профайлинг: проблемы и пути решения // Вестник Восточно-Сибирского института МВД России. 2019. № 4. С. 176–183.

предотвращения и пресечения правонарушений[11].

Криминалистический профайлинг не может и не должен заменять иные криминалистические методы в арсенале следователя или дознавателя, осуществляющих расследование, однако владение методикой профилирования в перспективе способствует повышению эффективности работы должностного лица. Профайлинг – это не универсальный ответ на все вопросы, интересующие следствие или дознание, но важный и нужный инструмент необходимый для понимания поведения преступника и его мотивов, что положительно сказывается на ходе расследования, помогает отыскать потенциального злодея в более короткий и срок и, вполне возможно, пресечь совершение им новых противоправных деяний. Методу криминалистического профилирования преступников необходимо уделять внимание при подготовке студентов-юристов – потенциальных кадров правоохранительных органов, разрабатывать и поддерживать программы повышения квалификации уже действующих сотрудников не только в сфере профилирования, но и в части изучения основ психологии; осуществлять внедрение в систему обучения сотрудников выездных школ и семинаров по основам профайлинга, на которых у следователей появится реальная возможность освоить данный набор средств, задать возникающие вопросы специалистам в указанной области.

Данные знания и умение их применять способны вывести эффективность работы органов следствия и дознания на принципиально новый уровень.

Список литературы:

1. Профайлинг в деятельности органов внутренних дел: учебное пособие / В. В. Вахнина и др. М.: Академия управления МВД России, 2018. 100 с.

2. Ветрова Т. В., Яковлев Е. В., Гневышев Е. Н., Смирнов А. А., Леонтьев О. В. Психофизиологические и морфофункциональные основы профайлинга: Учебное пособие. СПб.: Изд-во Университета при МПА ЕврАзЭС, 2021. 226 с.

3. Пирогова Л. К. Профайлинг. Превентивные методы обеспечения авиационной безопасности: учебно-наглядное пособие. М.: ДГСК МВД России, 2014. 72 с.

4. Карпенко О. А. Криминалистический профайлинг: проблемы и пути решения // Вестник Восточно-Сибирского института МВД России. 2019. № 4. С. 176–183.

5. Кудин В. А., Статный В. М. Профайлинг в деятельности органов внутренних дел: от теории и методологии к практике // Вестник Санкт-Петербургского университета МВД России. № 3. 2013. С. 4–15.

[11] Пирогова Л. К. Профайлинг. Превентивные методы обеспечения авиационной безопасности: учебно-наглядное пособие. М.: ДГСК МВД России, 2014. С. 26.

6. Попов В. В., Тройченко Ю. Ю. Психологический портрет как способ идентификации личности // Юристъ-Правоведъ. № 3. 2019. С. 137–141.

7. Brussel J. Casebook of a Crime Psychiatrist. Bernard Geis Associates, 1968.

8. Ressler R., Burgess A., Douglas J. Criminal Profiling Research on Homicide // New York: Unpublished Research Report, 1982.

Alexander A. Yashin
Senior lecturer of the Department of Criminology
Saratov State Law Academy
(Saratov, Russian Federation)
alek1811@rambler.ru

Victoria A. Shutova
Student of the
Saratov State Law Academy
(Saratov, Russian Federation)
vika.shutova.02@bk.ru

TO THE QUESTION OF THE NEED FOR THE USE OF FORENSIC PROFILING IN THE ACTIVITIES OF LAW ENFORCEMENT AGENCIES

Abstract. The article discusses the concept of criminalistic profiling, analyzes foreign and domestic practice of psychological profiling, reveals the methodology of compiling a psychological portrait of an alleged criminal, examines the possibility of training law enforcement officers to use profiling techniques.

Keywords: criminalistic profiling, profiling, victimological profiling, geographical profiling, psychological portrait of the criminal.

ТРИБУНА НАЧИНАЮЩИХ ИССЛЕДОВАТЕЛЕЙ

УДК 342.565

Арефинкина Серафима Геральдовна
Магистрант
Сочинский институт (филиал)
«Российского университета дружбы народов имени Патриса Лумумбы»
(г. Сочи, Российская Федерация)
Arefinkina82@mail.ru

Научный руководитель: Павличенко Николай Владимирович
доктор юридических наук, профессор
Сочинский институт (филиал)
«Российского университета дружбы народов имени Патриса Лумумбы»
(г. Сочи, Российская Федерация)
pavlichenko.pro@mail.ru

ЦИФРОВИЗАЦИЯ ПРАВОСУДИЯ: ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

Аннотация. В работе рассматривается процесс цифровизации правовой сферы как неотъемлемый элемент современного мира. Отдельно разбираются различные подходы к определению таких широко распространённых, но по-разному трактуемых сегодня понятий, как «цифровое правосудие», «электронное правосудие». Обращается внимание на то, какие концепции к толкованию данных терминов можно считать сложившимися. Рассмотрены в работе коротко и сложности, связанные не только с повсеместным внедрением цифровых технологий в процесс отправления правосудия, но и с обучением соответствующих кадров навыкам работы с информационно-коммуникационными технологиями. Изучены положительные последствия цифровой трансформации в сфере электронного судопроизводства. Также обозначены проблемы, без решения которых дальнейшая цифровизация правосудия будет затруднена. В заключение автором предлагаются варианты решения указанных проблем.

Ключевые слова: цифровизация правосудия; цифровизация судопроизводства; электронное судопроизводство.

Для цитирования:
Арефинкина С. Г. Цифровизация правосудия: проблемы и пути их решения // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 279–285.

Развитие информационных технологий влияет на все сферы общественной жизни. Построение электронного государства, элементами которого является электронное правительство, электронный парламент, электронное правосудие стало неотъемлемой частью бытия

современного информационного общества. Первоочерёдной задачей государства является не просто повышение уровня технического оснащения судов, улучшение документооборота внутри них, но и переход на новый уровень принятия решений за счёт внедрения новых способов сбора, обработки, передачи и распространения информации.

В 2018 г. в Послании Президента РФ Федеральному Собранию были подчёркнуты важность цифровой трансформации и преодоления технологического отставания России, а также необходимость укрепления институтов демократии, в том числе судов[1]. Так, с 2017 г. существует возможность подавать заявления в суд в электронном виде; в 2019 г. в судах нескольких субъектов России начали работу системы автоматического стенографирования[2]. К 2020 г. повсеместно обеспечена возможность электронного обращения в суд и возможность участия в судебных заседаниях посредством видеоконференцсвязи. На современном этапе развития электронного правосудия в России уже широко применяются следующие его элементы:

– видеоконференцсвязь, позволяющая дистанционно участвовать в судебном заседании;

– электронная подача документов, т. е. с помощью систем ГАС «Правосудие» и «Мой арбитр» появилась возможность электронной подачи документов в судебные органы, отслеживать движение дела и т. д.

Таким образом, старт процессу цифровизации дан, но правосудие нуждается в дальнейшем реформировании в сторону большего удобства и доступности как для граждан и организаций, так и для судей. Сегодня это означает прежде всего перевод всех возможных процессов в цифровую форму, так как именно это даёт максимальные возможности для интерактивной коммуникации.

Помимо стремительной технологизации жизни общим вектором развития правоотношений является их усложнение, что влечёт увеличение и усложнение законодательной базы, в связи с чем растёт и количество дел, поступающих на рассмотрение судов вследствие возникновения новых видов споров в результате применения в жизни новых технологий, вовлечение в судебную деятельность новых типов информации, создаваемой или передаваемой с помощью цифровых технологий и т. д.

Действительно, в последние несколько лет правосудие по различным категориям дел претерпело колоссальные изменения, связанные с активным введением цифровизации в правовую среду. Однако необходимо

[1] Послание Президента Российской Федерации Федеральному Собранию 01.03.2018 // Президент России: официальный сайт [Электронный ресурс]. 2018, 1 марта. URL: http://kremlin.ru/events/president/news/56957 (дата обращения: 13.04.2023).

[2] В судах автоматизируют протоколирование судебных заседаний // Информационно-аналитический центр поддержки ГАС «Правосудие» [Электронное правосудие]. 2018, 8 августа. URL: http://iac.cdep.ru/index.php?id=9&item=207 (дата обращения: 09.04.2022).

отметить, что зачастую как у обывателей, так и у профессиональных юристов наблюдается смешение терминов «электронное правосудие», «цифровое судопроизводство» и пр. Поэтому первоочерёдная задача состоит в том, чтобы сформулировать на законодательном уровне точные и ёмкие определения указанных понятий, чтобы достичь единообразия в понимании и применении данных терминов.

В соответствии с Приказом Судебного департамента при Верховном Суде РФ № 362 от 26.11.2015 г. под электронным правосудием понимается способ и форма осуществления предусмотренных законом процессуальных действий, основанные на использовании информационных технологий в деятельности судов, включая взаимодействие судов, физических и юридических лиц в электронном (цифровом) виде[3]. Действительно, электронные инструменты обеспечивают абсолютную открытость и доступность судов, улучшение качества судейской работы, сокращение издержек и максимальное удобство для участников судопроизводства. Можно сказать, что термин «электронное правосудие» (e-justice) уже в принципе устоялся, под ним традиционно понимается способ осуществления правосудия, основанный на использовании современных информационно-коммуникационных технологий и имеющий своей целью обеспечение гласности, открытости и доступности судопроизводства[4], а потому есть все основания для закрепления его толкования на законодательном уровне.

При этом понятие «электронное правосудие» необходимо чётко отграничивать от понятия «цифровое правосудие»: в первом случае речь идёт о свойствах носителя информации, во втором – о форме существования данных[5].

Ряд существующих терминологических пробелов в сфере цифровизации связан не только с отсутствием в юридическом языке тех или иных понятий, но и с тем, что сами явления, отражаемые такими

[3] Приказ Судебного департамента при Верховном Суде РФ от 26.11.2015 № 362 «Об утверждении Перечня основных понятий и терминов, применяемых в нормативных правовых актах Судебного департамента, регламентирующих использование информационно-телекоммуникационных технологий в деятельности судов, управлений Судебного департамента в субъектах Российской Федерации и учреждениях Судебного департамента» // Бюллетень актов по судебной системе. 2016. № 2.

[4] Сухаренко А. Электронное правосудие // Мудрый юрист [Электронный ресурс]. URL: https://wiselawyer.ru/poleznoe/81087-ehlektronnoe-pravosudie (дата обращения: 09.04.2023); Электронное правосудие: итоги и перспективы: интернет-интервью Председателя Арбитражного суда Калужской области С. Ю. Шараева // Информационно-правовой портал ГАРАНТ.РУ [Электронный ресурс]. 2010, 21 июля. URL: https://www.garant.ru/company/cooperation/gov/action/regional/271319/ (дата обращения: 09.04.2023).

[5] Козырев А. Н. Цифровая экономика и цифровизация в исторической ретроспективе // Medium [Электронный ресурс]. URL: https://medium.com/cemi-ras/цифровая-экономика-и-цифровизация-в-исторической ретроспективе-1ad034c16373 (дата обращения: 25.03.2023).

понятиями, не сложились окончательно. Если давать определение термину «цифровизация правосудия», то здесь нам наиболее близка точка зрения, в соответствии с которой, под ним понимается средство обеспечения перехода к системе электронной подачи обращений в суд и автоматизированного распределения дел между судьями; внедрения средств информатизации судебного разбирательства (от использования видеоконференцсвязи и электронных доказательств до применения искусственного интеллекта в оценке доказательств и вынесения решений); а также онлайн-взаимодействия и электронного оборота между всеми участниками судебного судопроизводства на базе личных кабинетов (судьи, стороны и иные участники судебного процесса)[6]. В частности, цифровое правосудие предполагает переход большей части коммуникаций в цифровую среду[7], тогда как электронное правосудие предполагает в основном осуществление судами разрешения правовых конфликтов посредством информационно-коммуникационных технологий, прежде всего электронного документооборота и системы видеоконференцсвязи, результаты которых отображаются в информационной системе[8].

Представляется, что электронное правосудие – важный шаг на пути к цифровому. Полагаем, что в ближайшей перспективе с учётом сегодняшних тенденций развития науки, техники и права правосудие должно приобрести цифровую форму. Информатизация и автоматизация судебной системы и её цифровизация это два разных, но при этом тесно взаимосвязанных процесса.

Поимо сложностей, связанных с недостаточно чётким на данный момент толкованием терминов «электронное правосудие», «цифровизация судопроизводства» и ряда других, необходимо отметить и такую проблему, как недостаточный уровень подготовки юридических кадров. Новейшие технологии развиваются настолько быстро, что по меткому замечанию Т. Я. Хабриевой ответы на многие вопросы, возникающие при «обеспечении правового регулирования необходимым высокотехнологическим инструментарием», юристы дать самостоятельно не смогут, а значит, нужно ориентироваться на сотрудничество со специалистами в области информационных технологий (IT-специалистами)[9]. Однако всеобщая цифровизация ставит перед юридической наукой и новый серьёзный вызов. Юриспруденция –

[6] Шатковская Т. В., Гончаров Е. И. Электронный документооборот в судебной системе Российской Федерации: проблемы и перспективы // Северо-Кавказский юридический вестник. 2021. № 2. С. 135–139.

[7] Колга О. В., Калашникова Е. Б. «Цифровое» направление развития правосудия в России // Актуальные проблемы юриспруденции: сб. ст. по матер. XVI Междунар. науч.-практ. конф. (Новосибирск). 2018. № 11 (15). С. 51–57.

[8] Тищенко А. В. Электронное правосудие: судебное реформирование к 2020 году // Правопорядок: история, теория, практика. 2018. № 4. С. 65–69.

[9] Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9. С. 11.

традиционно гуманитарная специальность. Однако уже сегодня информационное право перенасыщено сложными к пониманию для «гуманитариев» техническими терминами и понятиями. Юристы и IT-специалисты, порой, говорят об одном и том же, но на разных языках, иногда абсолютно не понимая друг друга. Таким образом, назрела потребность в серьёзной реформе юридического образования в России (с учётом необходимости углублённого изучения информационных дисциплин), иначе все начинания в деле регулирования информационного пространства будут недостаточно эффективными. Безусловно, это работа на будущее, но начинать движение в этом направлении надо уже сейчас, поскольку, учитывая быстрые темпы цифровизации, требуется действовать на упреждение будущих проблем в этой сфере и высвобождения со временем большого количество специалистов, знающих право, но не понимающих и не имеющих возможности его применения в условиях нового цифрового общества.

Мнение квалифицированных юристов важно и при принятии законов, регулирующих информационную сферу, иначе последние не принесут практической пользы, вызовут сложности в правоприменительной деятельности и неизбежные многочисленные поправки в нормативно-правовые акты, что отнюдь не способствует стабильности законодательства, а значит его эффективности. Цифровая трансформация – это лишь один из аспектов судебной реформы, она должна идти параллельно с решением имеющихся глобальных вопросов другими, не цифровыми, средствами, например, с обеспечением реального, а не номинального доступа всех граждан к новым технологиям. Замена человека искусственным интеллектом будет полезна, особенно там, где речь идёт о рутинной работе, но тут существует и перспектива замены неравенства между людьми на неравенство между человеком и машиной. В правовом поле такая ситуация неприемлема, поэтому действовать нужно на упреждение, понимая, что опасны в равной степени как недооценка, так и переоценка возможностей цифровой среды[10].

Таким образом, можно констатировать, что сложностей в сфере цифрового правосудия наметилось уже не мало. Но только лишь наметить проблемы – недостаточно. Сформулируем предложения по их решению. На наш взгляд, первоочерёдной задачей государства в лице соответствующих органов является упреждающий характер нормотворчества, определяющего правовой статус информационных технологий. Немаловажным является и скорейшая реформа юридического образования, расширение количества изучаемых юристами информационных дисциплин, появление новых специализаций правоведов в условиях тотальной цифровизации.

[10] Брянцева О. В., Солдаткина О. Л. Электронное правосудие в России: проблемы и пути решения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 12. С. 97–104.

Список литературы

1. Брянцева О. В., Солдаткина О. Л. Электронное правосудие в России: проблемы и пути решения // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 12. С. 97–104.

2. Колга О. В., Калашникова Е. Б. «Цифровое» направление развития правосудия в России // Актуальные проблемы юриспруденции: сб. ст. по матер. XVI Междунар. науч.-практ. конф. (Новосибирск). 2018. № 11 (15). С. 51–57.

3. Козырев А. Н. Цифровая экономика и цифровизация в исторической ретроспективе // Цифровая экономика. 2018. № 1. С. 5–19.

4. Тищенко А. В. Электронное правосудие: судебное реформирование к 2020 году // Правопорядок: история, теория, практика. 2018. № 4. С. 65–69.

5. Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9. С. 5–16.

6. Шатковская Т. В., Гончаров Е. И. Электронный документооборот в судебной системе Российской Федерации: проблемы и перспективы // Северо-Кавказский юридический вестник. 2021. № 2. С. 135–139.

Serafima G. Arefinkina
Graduate student
Sochi Institute (branch) of the
Peoples' Friendship University of Russia named after Patrice Lumumba
(Sochi, Russia)
Arefinkina82@mail.ru

Scientific Supervisor: Nikolay V. Pavlichenko
PhD in Law, Professor
Sochi Institute (branch) of the
Peoples' Friendship University of Russia named after Patrice Lumumba
(Sochi, Russia)
pavlichenko.pro@mail.ru

DIGITALIZATION OF JUSTICE: PROBLEMS AND SOLUTIONS

Abstract. The article considers the process of digitalization of the legal sphere as an integral element of the modern world. Different approaches to the definition of such widespread, but differently interpreted concepts as «digital justice», «electronic justice» are separately analyzed, attention is drawn to what concepts for the interpretation of these terms can be considered established. The article briefly discusses the difficulties associated not only with the widespread introduction of digital technologies in the process of administration of justice, but also with the training of relevant personnel in the skills of working with information and communication competencies. The positive consequences of digital transformation in the field of electronic legal proceedings are

studied. The problems are also identified, without solving which further digitalization of justice will be difficult. In conclusion, the author suggests solutions to these problems.

Keywords: digitalization of justice; digitalization of legal proceedings; electronic court proceedings.

УДК 343.98

Винокурова Ника Сергеевна
Слушатель факультета подготовки следователей
Уральский юридический институт МВД России,
(г. Екатеринбург, Россия)
nikusavinokurova@mail.ru

Научный руководитель: Ржанникова Светлана Сергеевна
старший преподаватель кафедры криминалистики
Уральский юридический институт МВД России
(г. Екатеринбург, Россия)
ssr80@mail.ru

ТЕХНОЛОГИИ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ: КРИМИНАЛИСТИЧЕСКИЙ И ПРАВОВОЙ АСПЕКТЫ

Аннотация. В статье рассмотрены виды и принципы функционирования существующих технологий биометрической идентификации. Проанализированы особенности их применения в различных сферах жизни общества, а также в работе правоохранительных органов Российской Федерации и других стран, оценена результативность их использования в раскрытии и расследовании преступлений и перспективы их дальнейшего внедрения в правоохранительную деятельность. Рассмотрена нормативно-правовая регламентация применения технологий биометрической идентификации, сделаны предложения по совершенствованию правового регулирования использования биометрических технологий.

Ключевые слова: биометрия, алгоритм, технологии биометрической идентификации, биометрические данные, распознавание.

Для цитирования:
Винокурова Н. С. Технологии биометрической идентификации в расследовании преступлении: криминалистический и правовой аспекты // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 286–291.

В настоящее время происходят огромные изменения в различных сферах жизни общества, связанные с повсеместной цифровизацией. За счёт использования инновационных методов развивается и совершенствуется человеческая деятельность. На сегодня спектр применения биометрических технологий довольно велик и с каждым днём расширяется, технологическая сфера биометрии стремительно интегрируется в нашу жизнь и в деятельность многих предприятий и организаций. Практически каждый человек так или иначе соприкоснулся с

биометрией, например, при доступе к смартфону с помощью изображения лица или отпечатка пальца.

Одновременно с этим, одним из главных направлений деятельности правоохранительных органов является полное, всестороннее и объективное расследование преступлений, что представляет собой сложный процесс установления истины и определённых обстоятельств по уголовному делу, включающий в себя разнообразные тактические приёмы и методы. На сегодняшний день с использованием технологий биометрической идентификации не только выясняются конкретные обстоятельства уголовного дела, но и идентифицируются личности участников правонарушений и преступлений. Основой современных технологий идентификации является биометрия. Биометрия – это система измерений характеристик человека с целью его идентификации на основе уникальных физических параметров. Среди биометрических параметров выделяют 2 типа:

1) статические, к которым можно отнести папиллярные узоры пальцев и ладоней рук, радужную оболочку глаза, элементы лица и т. п.;

2) динамические: речь, походка, жестикуляция, почерк (в том числе и клавиатурный).

Как правило, все биометрические технологии имеют одинаковый алгоритм работы. Для начала система должна запомнить образец одной или нескольких, в зависимости от настроек, биометрических характеристик, например, лицо или папиллярный узор. Это необходимо для обеспечения в последующем возможности наиболее точного составления изображения биометрической характеристики, которую следует проверить. Затем то, что было получено, обрабатывается и преобразовывается в определённый код с помощью встроенных математических программ. Полученный код сравнивается с базой имеющихся данных, и в результате устанавливается сходство или различие полученной информации. Таким образом, работу биометрических технологий можно представить в четырёх стадиях:

1) запись – тот или иной образец, статическая или динамическая биометрическая характеристика сканируется и запоминается программой;

2) выделение или кодирование – полученный образец преобразовывается в математический код;

3) сравнение – сохраненная и закодированная биометрическая характеристика сравнивается с имеющейся информацией в определённой базе данных;

4) получение результата – установление сходства или различия.

На перспективность использования в расследовании преступлений технологий биометрической идентификации указывают статистические данные. В России лидером в области распознавания лиц является комплексная система «Безопасный город». Так, с её использованием только в Москве за 2022 год раскрыто

9,1 тыс. преступлений[1].

Помимо автоматизированной системы «Безопасный город», для идентификации личности человека применяется АДИС «Папилон», которая обладает возможностями не просто ведения базы данных отпечатков пальцев и ладоней рук и осуществления поиска по ней, но и мультибиометрической идентификации по папиллярным узорам пальцев (ладоней) рук, радужной оболочке глаз, изображению лица[2].

В Казахстане с 2020 года разработан проект новой технологии оплаты проезда, установленной в общественном транспорте, которая считывает биометрические данные лица, сравнивает с базой данных, имеющихся в полиции, и идентифицирует человека. Данная система позволяет выявить уже известных «карманников». Как только «карманник» войдёт в автобус, то система сразу же его распознает. Точность распознавания лица составляет 95 %. С помощью биометрических технологий в Казахстане решили бороться и с коррупцией[3].

В США разработана система речевой идентификации человека «CSL», которая применяется при расследовании вымогательств, банковских мошенничеств и телефонных сообщений о терактах[4].

Помимо камер применяются и инновационные очки со встроенной «умной» камерой, разработанные китайской компанией LLVision Technology Co. С помощью таких очков в течение двух минут можно распознать лицо, благодаря алгоритму сверки лица с базой данных. Такие очки применяются и в деятельности полиции. Замечая правонарушителя, или лицо, находящееся в розыске, очки «уведомляют» об этом сотрудника. В ходе тестирования лишь за полторы недели с помощью данных очков удалось задержать более 300 человек[5].

Следует отметить, что, безусловно, перспективы развития

---

[1] В Москве за прошлый год благодаря камерам раскрыто 9,1 тыс. преступлений // ТАСС. 2023, 20 января. [Электронный ресурс]. URL: https://tass.ru/obschestvo/16849671?ysclid=lhherlmxlz944504583 (Дата обращения 01.05.2023).

[2] Ржанникова С. С. Совершенствование деятельности экспертно-криминалистических подразделений МВД России в условиях цифровизации // Правоохранительные органы: теория и практика. 2022. № 2 (43). С. 34.

[3] Новый биометрический формат оплаты проезда в автобусах протестировали в Казахстане // ИАЦ. 2019, 18 октября. [Электронный ресурс]. URL: https://ia-centr.ru/publications/novyy-biometricheskiy-format-oplaty-proezda-v-avtobusakh-protestirovali-v-kazakhstane/?ysclid=lgn9monllv630362208 (Дата обращения 10.05.2023).

[4] Ксендзов Ю. Ю. Актуальное состояние и перспективы технико-криминалистического обеспечения расследования преступлений // Право и государство: теория и практика. 2022. № 6 (210). С. 135.

[5] В чем польза технологий распознавания лиц: ответ эксперта // МИ-7. Мир новостей. 2021, 29 октября. [Электронный ресурс]. URL: https://mynewslent.com/obshestvo/publication/v-chem-polza-tehnologijraspoznavaniya-lic-otvet-eksperta-2415192 (Дата обращения 05.05.2023).

технологий биометрической идентификации довольны велики. С каждым годом в различных регионах страны данные технологии внедряются в подразделения органов внутренних дел, тем самым повышая эффективность их работы и скорость реагирования на противоправные деяния. Поэтому можно считать биометрию одной из инновационных технологий, которая приведёт к снижению роста преступности и высокому темпу раскрываемости совершаемых преступлений.

Что касается вопроса, который заключается в спорах граждан об использовании их персональных данных, то существует ряд нормативных актов, которые фрагментарно регулируют деятельность правоохранительных органов при сборе и использовании биометрических персональных данных, а именно – дают право на их использование при применении технологий биометрической идентификации в ходе расследования и раскрытия преступлений. Например, федеральный закон от 29.12.2022 № 572-ФЗ[6]и ФЗ от 27.07.2006 № 152-ФЗ[7], которые разрешают в отдельных случаях осуществлять сбор и использование биометрических персональных данных граждан без их согласия. Правоохранительным органам разрешено осуществлять сбор и использование персональных данных в следующих случаях:

– в связи с осуществлением правосудия;

– при оперативно-розыскных и следственных действиях;

– в рамках судебного производства.

ФЗ № 572 также регулирует и те отношения, которые связаны с изъятием фото- и видеоизображения лица из толпы и с его идентификацией с помощью биометрических данных. Также отмечено, что биометрические персональные данные лица могут собираться, храниться и использоваться органами государственной власти в исключительных случаях, в том числе в случаях, связанных с осуществлением правосудия.

Все нюансы, связанные с применением изображения лица с камер видеонаблюдения правоохранительными органами, требуют законодательного урегулирования, чтобы мог соблюдаться справедливый баланс между правом человека на тайну личной жизни, персональных данных и интересами общества и государства, а также иных коммерческих субъектов

[6] Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации: федеральный закон от 29.12.2022 № 572-ФЗ // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_436110/ (дата обращения: 01.05.2023).

[7] О персональных данных: федеральный закон от 27.07.2006 г. № 152-ФЗ // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 01.04.2023).

на обработку такой информации при помощи интеллектуальных систем.

Учитывая также, что современные технологии распознавания личности используют нейросетевые алгоритмы, относящиеся к искусственному интеллекту, вопрос законодательного регулирования их применения стоит особенно остро. В большинстве развитых и развивающихся стран уже начаты работы по созданию нормативно-правовых подходов к регулированию этой технологии[8].

На наш взгляд, применение технологии распознавания личности по признакам внешнего облика должно быть законодательно урегулировано и применяться в соответствии с нормами права, в том числе защищающими гражданские и конституционные права. Использование такой системы правоохранительными органами могло бы контролироваться специальными подразделениями, которые следили бы за соблюдением гражданских прав. Также мы считаем, что в местах, где используются технологии распознавания лиц, должны быть размещены соответствующие информационные стенды, чтобы надлежащим образом уведомить всех граждан.

Подводя итог, следует отметить, что дальнейшее внедрение технологий биометрической идентификации в работу правоохранительных органов будет способствовать повышению эффективности раскрытия и расследования преступлений. Возможность оперативной идентификации лиц, подозреваемых в совершении преступлений, повысит шансы их задержания, тем самым обеспечит не только эффективность расследования, но и защиту прав, свобод и законных интересов граждан, при этом использование таких технологий должно быть законодательно урегулировано.

Список литературы

1. Бахтеев Д. В. Этические кодексы как основание нормативного регулирования технологий искусственного интеллекта // Цифровые технологии и право: Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года / Под редакцией И. Р. Бегишева [и др.]. Том 3. Казань: Издательство «Познание», 2022. С. 342–350.

2. Ксендзов Ю. Ю. Актуальное состояние и перспективы технико-криминалистического обеспечения расследования преступлений // Право и государство: теория и практика. 2022. № 6 (210). С. 134–137.

3. Ржанникова С. С. Совершенствование деятельности экспертно-криминалистических подразделений МВД России в условиях цифровизации //

[8] Бахтеев Д. В. Этические кодексы как основание нормативного регулирования технологий искусственного интеллекта // Цифровые технологии и право: Сборник научных трудов I Международной научно-практической конференции. В 6-ти томах, Казань, 23 сентября 2022 года / Под редакцией И. Р. Бегишева [и др.]. Том 3. Казань: Издательство «Познание», 2022. С. 342.

Правоохранительные органы: теория и практика. 2022. № 2 (43). С. 33–36.

Nika S. Vinokurova
Student of the Faculty of Training investigators
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russia)
nikusavinokurova@mail.ru

Scientific Supervisor: Svetlana S. Rzhannikova
Senior Lecturer of the Department of Criminalistics
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russia)
ssr80@mail.ru

BIOMETRIC IDENTIFICATION TECHNOLOGIES IN CRIME INVESTIGATION: CRIMINALISTIC AND LEGAL ASPECT

Abstract. The article discusses the types and principles of functioning of existing biometric identification technologies. The features of their application in various spheres of society, as well as in the work of law enforcement agencies of the Russian Federation and other countries are analyzed, the effectiveness of their use in the detection and investigation of crimes and the prospects for their further implementation in law enforcement are evaluated. The regulatory and legal regulation of the use of biometric identification technologies is considered, proposals are made to improve the legal regulation of the use of biometric technologies.

Keywords: biometrics, algorithm, biometric identification technologies, biometric data, recognition.

УДК 342.9

Водопьянова Арина Николаевна
Студент Института юстиции
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
vodoarina@yandex.ru

Научный руководитель: Антонова Екатерина Евгеньевна
кандидат юридических наук, доцент,
доцент кафедры информационного права
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
ee-antonova@yandex.ru

НАЦИОНАЛЬНАЯ СИСТЕМА МАРКИРОВКИ И ПРОСЛЕЖИВАЕМОСТИ ТОВАРОВ «ЧЕСТНЫЙ ЗНАК»

Аннотация. В статье раскрываются понятие и содержание национальной системы цифровой маркировки и прослеживаемости товаров «Честный ЗНАК». Описывается режим её правового регулирования, а также анализируется необходимость внедрения. Особое внимание уделяется преимуществам использования системы «Честный ЗНАК».

Ключевые слова: маркировка товаров, код марки, контрафакт, «Честный ЗНАК».

Для цитирования:
Водопьянова А. Н. Национальная система маркировки и прослеживаемости товаров «Честный ЗНАК»// Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 292–297.

На сегодняшний день большой проблемой для потребителей и производителей является увеличение масштабов распространения некачественной и контрафактной продукции. Контрафакт означает подделку продукции известных брендов без соответствующего на то разрешения и согласия от владельца интеллектуальной собственности на производство и распространение товаров его бренда. В итоге это приводит к уменьшению прибыли производителя, портит его репутацию, а также наносит моральный ущерб потребителю.

Федеральная таможенная служба России в 2021 г. выявила более 7 млн единиц контрафактных товаров и не допустила их введения в гражданский оборот. Было возбуждено более 800 дел об административных

правонарушениях по ст. 14.10 КоАП РФ за незаконное использование товарного знака и по ч. 1 ст. 7.12 КоАП РФ за нарушение авторских и смежных прав[1].

Система цифровой маркировки и прослеживаемости товаров «Честный ЗНАК» (далее также – «Честный ЗНАК», система маркировки) играет большую роль в выявлении и ликвидации контрафакта.

Основными её задачами являются обеспечение безопасности граждан РФ за счёт гарантии подлинности и заявленного качества приобретаемой продукции, борьба с контрафактной и некачественной продукцией. Рассмотрим подробнее вопросы её функционирования.

Система цифровой маркировки и прослеживаемости товаров «Честный ЗНАК» закреплена в Федеральном законе 28 декабря 2009 г. № 381-ФЗ как государственная информационная система мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации (информационная система мониторинга)[2].

В соответствии с ч. 1 ст. 20.1 данного Федерального закона единая национальная система маркировки и прослеживаемости товаров «“Честный ЗНАК” – это государственная информационная система, создаваемая в целях автоматизации процессов сбора и обработки информации об обороте товаров, подлежащих обязательной маркировке средствами идентификации, хранения такой информации, обеспечения доступа к ней, её предоставления и распространения, повышения эффективности обмена информацией об обороте таких товаров и обеспечения их прослеживаемости, а также в иных предусмотренных законодательством РФ целях».

Согласно ч. 3 ст. 20.1 того же Федерального закона и Распоряжению Правительства РФ от 03 апреля 2019 г. № 620-р [3] оператором государственной информационной системы мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации, является ООО «Оператор-ЦРПТ» – Центр развития перспективных технологий, который создан с целью реализации проектов в цифровой экономике. Центр осуществляет свою деятельность на основе государственно-частного партнёрства.

В соответствии с пунктом 3.1 части 1 статьи 5 Федерального закона «Об основах государственного регулирования торговой деятельности в Российской Федерации», Правительство РФ имеет полномочие по утверждению перечня отдельных

[1] ФТС выявила в 2021 году контрафактные товары на 7,2 млрд рублей // Рамблер. Финансы [Электронный ресурс]. 2022, 9 февраля. URL: https://finance.rambler.ru/economics/48097498-fts-vyyavila-v-2021-godu-kontrafaktnye-tovary-na-7-2-mlrd-rubley/ (дата обращения: 07.05.2023).

[2] Об основах государственного регулирования торговой деятельности в Российской Федерации: Федер. закон Рос. Федерации от 28 декабря 2009 г. N 381-ФЗ (ред. от 06.02.2023) // СЗ РФ. 2010. № 1. Ст. 2.

[3] Об операторе государственной информационной системы мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации: распоряжение Правительства РФ от 03 апреля 2019 г. № 620-р // СЗ РФ. 2019. № 15 (часть IV). Ст. 1790.

товаров, которые подлежат обязательной маркировке средствами идентификации. В Распоряжении Правительства от 28.04.2018 № 792-р[4] закреплён перечень товаров, подлежащих обязательной маркировке. В него включены:

– табачные изделия;
– духи и туалетная вода;
– шины и покрышки;
– предметы одежды, включая рабочую одежду, изготовленные из натуральной или композиционной кожи;
– блузки трикотажные;
– пальто, полупальто, накидки, плащи, куртки (включая лыжные), ветровки, штормовки и аналогичные изделия мужские или для мальчиков, женские или для девочек;
– бельё постельное, столовое, туалетное и кухонное;
– обувные товары;
– фотокамеры;
– сыры, мороженое и прочие виды пищевого льда, не содержащие или содержащие какао (за исключением мороженого и десертов без содержания молочных жиров и (или) молочного белка в составе);
– молочная продукция со сроком хранения до 40 суток (включительно) и более 40 суток, за исключением сыров, мороженого и прочих видов пищевого льда, не содержащих или содержащих какао;
– велосипеды;
– упакованная вода (в том числе газированные воды, не содержащие сахара, подсластителей, ароматизаторов и других пищевых веществ);
– кресла-коляски;
– пиво солодовое и напитки, изготавливаемые на основе пива; безалкогольное пиво;
– сидр и грушевый сидр;
– прочие напитки, сброженные, игристые и неигристые, с фактической концентрацией спирта не более 7 об.%.

По данным группам товаров чаще всего встречается контрафакт, поэтому и возникла необходимость в маркировке.

Таким образом, правовое регулирование системы «Честный ЗНАК» осуществляется следующими нормативными правовыми актами:

1) Федеральный закон от 28 декабря 2009 г. № 381-ФЗ «Об основах государственного регулирования торговой деятельности в Российской Федерации»;

2) Распоряжение Правительства Российской Федерации от 28 апреля 2018 г. № 792-р «Об утверждении перечня отдельных товаров, подлежащих обязательной маркировке средствами идентификации»;

3) Распоряжение Правительства Российской Федерации от 3 апреля 2019 г. № 620-р «Об операторе государственной информационной системы мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации»;

4) Постановление Правительства РФ от 19.03.2020 № 303

[4] Об утверждении перечня отдельных товаров, подлежащих обязательной маркировке средствами идентификации: распоряжение Правительства РФ от 28.04.2018 № 792-р (ред. от 28.02.2023) // СЗ РФ. 2018. № 19. Ст. 2773.

«Об утверждении требований к техническим средствам, используемым участниками оборота товаров, подлежащих обязательной маркировке средствами идентификации, для обмена информацией с государственной информационной системой мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации, в том числе к техническим средствам проверки кода проверки»;

5) Постановление Правительства Российской Федерации от 8 мая 2019 г. № 577 «Об утверждении размера платы за оказание услуг по предоставлению кодов маркировки, необходимых для формирования средств идентификации и обеспечения мониторинга движения товаров, подлежащих обязательной маркировке средствами идентификации, а также о порядке ее взимания»;

6) Постановление Правительства РФ от 31.12.2019 № 1955 «Об обеспечении доступа к информации, содержащейся в государственной информационной системе мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации»;

7) Постановление Правительства РФ от 11.04.2019 №420 «Требования к порядку создания, развития ввода в эксплуатацию государственных информационных систем»;

8) Федеральный закон от 22 мая 2003 г. № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации»;

9) Постановление Правительства Российской Федерации от 21 февраля 2019 г. № 174 «Об установлении дополнительного обязательного реквизита кассового чека и бланка строгой отчетности»;

10) Постановление Правительства Российской Федерации от 26 апреля 2019 № 515 «О системе маркировки товаров средствами идентификации и прослеживаемости движения товаров»;

11) Приказ Минпромторга России от 27.06.2019 № 2296 «Об утверждении требований к обезличиванию информации, содержащейся в государственной информационной системе мониторинга за оборотом товаров, подлежащих обязательной маркировке средствами идентификации, и методов обезличивания такой информации»;

12) Распоряжение Правительства Российской Федерации от 28 апреля 2018 г. № 791-р «Об утверждении модели функционирования системы маркировки товаров средствами идентификации в Российской Федерации»;

13) Распоряжение Правительства РФ от 28.12.2018 № 2963-р «Об утверждении Концепции создания и функционирования в Российской Федерации системы маркировки товаров средствами идентификации и прослеживаемости движения товаров» и многими другими.

Остановимся подробнее на технической стороне вопроса маркировки, состоящей из нескольких этапов. Сначала оператор ЦРПТ присваивает каждой единице товара

уникальный специальный код (Data Matrix) и вносит его в базу данных. Затем производитель или импортёр размещает этот код на упаковке товара. Далее весь путь перемещения товара фиксируется по логистической цепи с помощью присвоенного кода. Когда товар непосредственно доставлен от завода-производителя к продавцу, то лица, осуществляющие торговую деятельность, сканируют код товара и размещают его на полке, витрине. При этом возможность подделки исключена, так как все действия с товаром фиксируются. Последней стадией маркировки является реализация товара: при его продаже код выходит из оборота.

Выгоду от внедрения данной системы получают потребители, бизнес и государство. Для потребителя можно выделить следующие преимущества:

– Возможность проверки легальности товара[5]. С помощью мобильного приложения «Честный ЗНАК», установленного на смартфон, потребитель может отсканировать код и получить информацию о товаре, а именно данные о производителе.

– Сохранение здоровья за счёт уверенности в качестве товара. Посредством того же приложения потребитель может узнать дату, место изготовления продукции, срок годности, условия хранения и т. п. Таким образом, у него появляется возможность обезопасить себя от потребления некачественных товаров и избежать проблем со здоровьем;

– Защита прав потребителей. Система «Честный ЗНАК» делает рынок прозрачным и действует в интересах потребителя в том числе, поэтому в случае получения некачественного или контрафактного товара, человек на основе информации, занесённой в систему «Честный ЗНАК», может обратиться в Роспотребнадзор, прокуратуру и правоохранительные органы, чтобы защитить свои права.

Бизнесу это система выгодна, так как обеспечивает:

– повышение прибыли[6];

– рост конкурентоспособности;

– снижение издержек;

– возможность контроля движения товара[7];

– оптимизацию процессов продаж.

Для государства можно выделить следующие положительные последствия внедрения системы:

– уменьшение масштабов чёрного рынка;

– увеличение поступаемых налоговых и таможенных сборов;

– сокращение бюджетных расходов на обеспечение товарного контроля.

Таким образом, система цифровой маркировки и

[5] Дубровина Л. В. Честный знак – это национальная система маркировки // Тенденции развития науки и образования. 2022. № 83–3. С. 21–23.

[6] Курганская О. В., Махмудов В. В. Изменение эластичности спроса НА товары в условиях введения маркировки «Честный ЗНАК» // Бизнес-образование в экономике знаний. 2023. № 2 (25). С. 40–46.

[7] Махмудов В. В., Салтыкова Ю. А. Внедрение системы обязательной маркировки товаров «Честный ЗНАК» // Бизнес-образование в экономике знаний. 2023. № 2 (25). С. 54–56.

прослеживаемости товаров «Честный ЗНАК» имеет большую значимость для торговой деятельности и в ближайшем будущем, скорее всего, будет распространена на все виды товаров широкого потребления.

Список литературы

1. Дубровина Л. В. Честный знак – это национальная система маркировки // Тенденции развития науки и образования. 2022. № 83–3. С. 21–23.
2. Махмудов В. В., Салтыкова Ю. А. Внедрение системы обязательной маркировки товаров «Честный ЗНАК» // Бизнес-образование в экономике знаний. 2023. № 2 (25). С. 54–56.
3. Курганская О. В., Махмудов В. В. Изменение эластичности спроса НА товары в условиях введения маркировки «Честный ЗНАК» // Бизнес-образование в экономике знаний. 2023. № 2 (25). С. 40–46.

Arina N. Vodopyanova
First-year student of the Institute of Justice,
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
vodoarina@yandex.ru

Scientific Supervisor: Ekaterina E. Antonova
PhD in Law, Associate Professor,
Associate Professor of the Department of Information law
Ural State Law University
named after V. F. Yakovlev
(Ekaterinburg, Russian Federation)
ee-antonova@yandex.ru

NATIONAL TRACK & TRACE DIGITAL SYSTEM CHESTNY ZNAK

Abstract. The article reveals the concept and content of the national system of digital marking and traceability of goods "CHESTNY ZNAK". It describes the regime of its legal regulation, as well as analyzes the need for its implementation. Particular attention is paid to the advantages of using the "CHESTNY ZNAK" system.

Keywords: marking, product, code, counterfeit, quality, consumer, manufacturer.

УДК 343.3.7

Гарькуша Анастасия Геннадьевна
Студент
Сочинский институт (филиал)
Российского университета дружбы народов имени Патриса Лумумбы
(г. Сочи, Россия)
anastasia.garkusha.29@mail.ru

Научный руководитель: Арефинкина Екатерина Геральдовна,
кандидат юридических наук
заведующий кафедрой уголовного права и процесса
Сочинский институт (филиал)
Российского университета дружбы народов имени Патриса Лумумбы
(г. Сочи, Россия)
arefinkina@mail.ru

О НЕКОТОРЫХ ОСОБЕННОСТЯХ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация. В статье рассматриваются некоторые вопросы правильной квалификации преступлений в сфере компьютерной информации. Приводятся основные для данных составов понятия и выдвигается предложение по совершенствованию российского уголовного законодательства в области определения ответственности за преступления, связанные с компьютерной информацией.

Ключевые слова: компьютерная информация, информационные технологии, уголовное законодательство, совершенствование уголовного законодательства, проблемы квалификации.

Для цитирования:
Гарькуша А. Г. О некоторых особенностях квалификации преступлений в сфере компьютерной информации // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 298–304.

Развитие информационных технологий и увеличение аудитории, пользующейся глобальной сетью «Интернет», на современном этапе способствовало генезису преступной деятельности, связанной с указанной сферой. Так, в соответствии с данными Международного союза электросвязи на 2022 год, интернетом пользуются около 5,3 млрд человек во всём мире. По состоянию на 2021 год в России

насчитывалось около 88 % интернет-пользователей среди населения[1].

Система законодательства несовершенна, она постоянно развивается для того, чтобы соответствовать прогрессивному обществу и регулировать все новые виды возникающих общественных отношений, оставаясь всегда на шаг позади их. В ещё большей степени указанное относится к уголовной сфере. Здесь законодатель отстаёт уже на несколько шагов, не успевая за стремительно видоизменяющимися существующими видами преступлений, закреплёнными в уголовном законе, а также появляющимися новыми видами и формами противоправных общественно опасных деяний, связанных с информационными технологиями.

В подтверждение актуальности темы следует отметить рост преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Так, в соответствии с данными, представленными на сайте Министерства внутренних дел РФ, о состоянии преступности за январь-декабрь 2022 года: было зарегистрировано 522,1 тыс. преступлений, совершённых с использованием информационно–телекоммуникационных технологий или в сфере компьютерной информации, что на 0,8 % больше, чем за отчётный период 2021 года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 25,8 % до 26,5 %[2]. Проанализировав данные о совершении преступлений данной категории за последние 6 лет, можно проследить стойкую тенденцию на увеличение.

Определимся с кругом составов преступлений, о которых идёт речь. Это составы, закреплённые в главе 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации», которая включает в себя: статью 272 «Неправомерный доступ к компьютерной информации»; статью 273 «Создание, использование и распространение вредоносных компьютерных программ»; статью 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей»; статью 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»[3].

Предметом составов преступлений, предусмотренных статьями 272–274.1 УК РФ являются охраняемая законом компьютерная

[1] Официальный сайт международного союза электросвязи. [Электронный ресурс]. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (дата обращения: 26.02.2023).

[2] Официальный сайт Министерства внутренних дел Российской Федерации. [Электронный ресурс]. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 26.02.2023).

[3] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.02.2021) // СПС «КонсультантПлюс». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 26.02.2023).

информация; вредоносные компьютерные программы либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации; средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и оконченное оборудование; критическая информационная инфраструктура Российской Федерации.

Объектом этой группы преступных деяний являются общественные отношения, обеспечивающие безопасность в сфере компьютерной информации, а также безопасность в сфере критической информационной инфраструктуры Российской Федерации.

Примечание 1 к статье 272 УК РФ даёт определение термина компьютерная информация – это сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В соответствии с пунктом 2 Постановления Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершённых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”», сведения, о которых идёт речь в примечании к статье 272 УК РФ, могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах либо на любых внешних электронных носителях (дисках, в том числе жёстких дисках – накопителях, флеш-картах и т. п.) в форме, доступной восприятию с помощью компьютерного устройства, и (или) передаваться по каналам электрической связи.

При этом к числу компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приёму, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащённые встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведённые или переделанные промышленным либо кустарным способом[4].

[4] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных

Неправомерным, в соответствии с комментарием к Уголовному кодексу РФ в редакции председателя Верховного суда РФ, признаётся доступ к компьютерной информации лица, не обладающего правами на получение и работу с данной информацией либо компьютерной системой, в отношении которых приняты специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ[5].

Стоит отметить, что не все составы, которые связаны с информационно-телекоммуникационными технологиями или компьютерной информацией содержатся в упомянутой ранее главе 28 УК РФ. Ряд из них находится в других разделах УК РФ.

К подобным составам можно отнести, например, мошенничество в сфере компьютерной информации – статья 159.6 УК РФ. Для корректной квалификации совершённого необходимо понимать и отличать такие составы от преступлений в сфере компьютерной информации, предусмотренные главой 28 УК РФ. Действия, совершаемые с компьютерной информацией, закреплённые в диспозиции статьи 159.6 УК РФ выступают способом совершения преступления. В свою очередь, в составах статей 272–274.1 УК РФ, указанные действия (неправомерный доступ, создание вредоносных программ и т. д.) выступают самим деянием, на совершение которого направлен умысел. Тем не менее, данное разграничение не препятствуют применению правил о совокупности преступлений, предусмотренных статьёй 159.6 УК РФ и составами, закреплёнными в главе 28 УК РФ[6].

Так, в соответствии с пунктом 20 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» есть указание на то, что мошенничество в сфере компьютерной информации, совершённое посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ[7].

Присутствуют спорные моменты при квалификации по статье 272 УК РФ «Неправомерный доступ к компьютерной информации» и статье

сетей, включая сеть "Интернет"» // СПС «КонсультантПлюс». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 27.02.2023).

[5] Комментарий к Уголовному кодексу РФ в 4 т. Том 3. Особенная часть. Раздел IX / В. М. Лебедев [и др.]. М.: Издательство Юрайт, 2023. С. 287.

[6] Ермакова О. В. Проблемы квалификации мошенничества в сфере компьютерной информации, связанные с отграничением от смежных составов преступлений // Вестник барнаульского юридического института МВД России. 2017. № 1 (32). С. 181.

[7] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «КонсультантПлюс». [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 27.02.2023).

146 УК РФ «Нарушение авторских и смежных прав». Проблема заключается в том, что в ряде преступлений, во время его совершения злоумышленник получает доступ к компьютерной программе, которая является объектом авторского права и осуществляет её использование в своих целях. Для правильной квалификации стоит отметить, объективная сторона состава статьи 146 УК РФ предусматривает в качестве обязательного обстоятельства причинение ущерба автору в виде упущенной выгоды или морального вреда. Объективная сторона состава статьи 272 УК РФ такого обязательного признака не имеет. Более того, важным, при квалификации, является то, что нарушение авторских прав сопровождается присвоением либо незаконным использованием объектов, а при неправомерном доступе дальнейшее использование ненужно.

Например, в случаях, когда виновный, сначала копирует компьютерную программу, являющуюся объектом авторского права, а в последующем данные копии незаконно использует в своих преступных интересах, совершённое следует квалифицировать по совокупности статей 146 и 272 УК РФ, при условии причинения автору значительного ущерба как последствия совершённого преступления.

Таким образом, с целю совершенствования законодательства в сфере борьбы с компьютерными преступлениями было бы целесообразно в состав статьи 146 УК РФ «Нарушение авторских и смежных прав» ввести квалифицирующий признак, определяющий способ совершения преступления: «с применением компьютерных средств» либо «с применением компьютерной информации».

Похожим образом законодатель уже поступил со статьёй 159.6 УК РФ «Мошенничество в сфере компьютерной информации», которая предусматривает уголовную ответственность за хищение чужого имущества или приобретение права на чужое имущество путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно–телекоммуникационных сетей. С момента принятия УК РФ существовал состав статьи 159 УК РФ «Мошенничество», который предусматривал уголовную ответственность за хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием, однако с развитием преступности в сфере кибермошенничества появилась необходимость во введении в УК РФ соответствующей статьи, специальных норм регулирующих уголовную ответственность в этой специфической области.

Представляется, что для борьбы с преступлениями в сфере компьютерной информации нужны значительные изменения в основном источнике уголовного права – Уголовном Кодексе РФ. Перечень преступлений указанной направленности, закрепленный в главе

28 УК РФ в количестве 4 составов, объективно не может охватить всего многообразия данных специфических противоправных деяний, даже с учётом тех норм, которые находятся вне главы 28 УК РФ. Изменения могут быть осуществлены как путём внесения новых составов (как это произошло со статьёй 159.6 УК РФ), так и дополнением существующих составов квалифицирующим признаком – совершения преступления с применением компьютерных средств, в сфере компьютерной информации и т. п., в зависимости от особенностей каждого состава. Целесообразным в этом отношении выглядит расширение количества составов преступлений, входящих в главу 28 УК «Преступления в сфере компьютерной информации».

Стоит сказать, что проработка потенциальных новых составов уголовно наказуемых деяний, в том числе в области киберпреступности, видится не желательной, а необходимой на современном этапе. Киберпреступность в современных условиях, являет собой серьезную угрозу как для информационной безопасности государства, так и для его экономического развития, и ключевую роль в киберпреступности настоящего времени играют преступления, совершаемые с использованием искусственного интеллекта. Использование данного инструмента предопределяет новый уровень угрозы информационной безопасности, что требует от законодателя в обозримом будущем готовности противостоять ей. Начать необходимо с комплексной работы не только правоведов, но и IT-специалистов, поскольку перед введением новых составов в УК РФ надлежит разработать чёткий понятийный аппарат. В перспективе требуется разработка федеральных законов, определяющих понятие «искусственного интеллекта», а затем и дальнейшая работа с элементами уголовно-правовой нормы.

Подводя итог, хочется отметить, что развитие технологического уровня государства и общества, совершенствование информационных технологий во всех сферах жизни имеет не только положительные моменты, но и несёт в себе ряд отрицательных аспектов, так как растёт уязвимость к киберугрозам, организованной преступности и терроризму. Любое революционное развитие не только открывает возможности для прогресса, но и порождает новые угрозы объектам уголовно-правовой охраны, наделяет преступников новыми способами и средствами совершения преступлений. Киберпреступность принимает разные формы, поэтому бороться с ней сложно. Уже сейчас становится очевидным тот факт, что четырёх составов преступлений в сфере компьютерной информации, которые содержатся в УК РФ, недостаточно для противодействия ей и для профилактики. Киберпреступность развивается, и, если её не контролировать, она может трансформироваться в очень опасную проблему национальной безопасности с потенциально катастрофическими последствиями.

Список литературы

1. Комментарий к Уголовному кодексу РФ в 4 т. Том 3. Особенная часть. Раздел IX / В. М. Лебедев [и др.]. Москва: Издательство Юрайт, 2023. 298 с.

2. Ермакова О. В. Проблемы квалификации мошенничества в сфере компьютерной информации, связанные с отграничением от смежных составов преступлений // Вестник барнаульского юридического института МВД России. 2017. № 1 (32). С. 180–181.

Anastasia G. Garkusha
Student
Sochi Institute (branch)
Peoples' Friendship University of Russia
named after Patrice Lumumba
(Sochi, Russia)
anastasia.garkusha.29@mail.ru

Scientific Supervisor: Ekaterina G. Arefinkina,
PhD in law
Head of the Department of Criminal Law and Procedure
Sochi Institute (branch)
Peoples' Friendship University of Russia
named after Patrice Lumumba
(Sochi, Russia)
arefinkina@mail.ru

ON SOME FEATURES OF QUALIFYING CRIMES IN THE SPHERE OF COMPUTER INFORMATION

Abstract. The article discusses some issues of correct qualification of crimes in the field of computer information. The main concepts for these compositions are given and a proposal is put forward to improve the Russian criminal legislation in the field of crimes related to computer information.

Keywords: computer information, information technologies, criminal legislation, improvement of criminal legislation, qualification problems.

УДК 343.98

Замятин Евгений Романович
Слушатель факультета подготовки следователей,
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
zhenya.zamyatin.00@mail.ru

Научный руководитель: Хамидуллин Руслан Сибагатуллович
кандидат юридических наук,
начальник кафедры оперативно-разыскной деятельности
органов внутренних дел
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
46006@bk.ru

ОСНОВНОЙ СПОСОБ КОММУНИКАЦИИ НАРКОПРЕСТУПНИКОВ

Аннотация. В статье рассмотрены способы взаимодействия преступников, осуществляющих свою противоправную деятельность в сфере незаконного оборота наркотических средств. Проанализированы часто используемые наркопреступниками средства коммуникации (мессенджеры). В качестве предмета исследования рассмотрен функционал мессенджера «Telegram». Соотнесены особенности функций мессенджера «Telegram» и способы их использования наркопреступниками в своей незаконной деятельности.

Ключевые слова: мессенджер, информационные технологии, наркотические средства, Telegram-канал.

Для цитирования:
Замятин Е. Р. Основной способ коммуникации наркопреступников // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 256–265.

На современном этапе развития общества существование и процветание большинства сфер жизнедеятельности невозможно без информационных технологий. Определяющую роль в становлении информационного общества, стоит отнести развитию всемирной сети «Интернет», которая является основным средством коммуникации. Безусловно, это ведёт к ускорению развития экономической сферы, формированию социума, что положительно сказывается на становлении общества и государства. Однако это же и является источником угроз, так как преступность, в свою очередь, тоже «идёт в ногу» с современным развитием.

Очень ярко процесс информатизации отразился на сфере незаконного оборота наркотических средств. На сегодняшний день технология распространения наркотиков полностью видоизменилась и практически вся наркоторговля ушла в интернет. Появился бесконтактный способ распространения наркотиков, суть которого заключается в том, что между сбытчиком и приобретателем не происходит непосредственного контакта, а передача наркотиков осуществляется через системы тайников и закладок. Этот способ позволяет преступникам на всех этапах своей деятельности оставаться анонимными, используя для связи различного рода мессенджеры электронные средства платежа, в которых скрываются истинные или указываются ложные персональные данные.

Основной принцип киберпреступников это анонимная и безопасная переписка, в двухтысячных этому служил ICQ, потом Jabber, некоторые же использовали шифрование OTR, перебрасывали весь трафик через браузер Tor. В последнее же время очень популярным средством коммуникации наркоторговцев за счёт своей политики конфиденциальности стал мессенджер Telegram[1].

Зачастую, рекламы о деятельности некоторых Telegram-каналов по распространению наркотических средств размещаются с соответсвующими ссылками на стенах зданий во многих российских городах, а также в социальных сетях. Эта открытая информирующая деятельность свидетельствует о том, что основной массив торговли запрещёнными веществами осуществляется через мессенджер Telegram.

Telegram – это гибкая и простая в использовании платформа, которая позволяет администраторам создавать и управлять каналами со всего мира, а также легко добавлять и удалять подписчиков.

Telegram имеет функцию «секретного чата», которая обеспечивает конфиденциальность сообщений, сообщения удаляются автоматически в зависимости от времени, установленного пользователем. В этом режиме сообщения не хранятся на серверах Telegram и шифруются, что уберегает их от прослушивания и взлома. Таким образом, информация, передаваемая между соучастниками незаконного оборота наркотиков бесконтактным способом надежно защищена и недоступна для правоохранительных органов. В 2018 году в Telegram появились «коммерческие» наркоблоги, созданные специально для размещения рекламы, и каналы кладменов. Одновременно стало больше каналов о наркополитике и наркокультуре («Наркофобия», «Наркпросвет», DrugStat)[2].

[1] Бертовский Л. В. Понятие киберпреступлений // Расследование преступлений: проблемы и пути их решения. 2020. № 4 (30). С. 85.

[2] Суходолов А. П., Бычкова А. М. Цифровые технологии и наркопреступность: проблемы противодействия использованию мессенджера «Телеграм» в распространении наркотиков // Всероссийский

На сайте «Судебные и нормативные акты РФ» слово «Telegram» упоминается почти в 5124 документах, из которых около 4831 также содержат слово «наркотическое»[3]. Большинство уголовных дел, со словом «Telegram» очень похожи и имеют два варианта развития событий, которые от города к городу идентичны. Первый вариант, когда лицо оплачивает покупку через бота в «Telegram», едет за закладкой, успешно её находит и забирает, а далее, по пути домой или через некоторое время, его задерживают сотрудники полиции. Второй вариант случается, когда человек устраивается кладменом, коммуницирует с дилером через «Telegram» и делает закладки до тех пор, пока его не задержат сотрудники полиции.

Бот в Telegram – это программа, которая автоматически выполняет заданные пользователем команды или отвечает на сообщения с предопределёнными шаблонами. Боты могут выполнять множество разных функций: от автоматической рассылки новостей до проведения опросов пользователей. Создателями этого специального аккаунта (бота) на платформу загружается вся необходимая информация о наркотическом средстве, психотропном веществе. Они позволяют реальному пользователю автоматически выбрать товар, вес и его примерное местонахождение[4].

Почти в каждом деле, где упомянут «Telegram» есть формулировки «переписка с неустановленным лицом». В наркоторговле «Телеграма» есть целая иерархия, сотрудники низшего звена и «уважаемые» люди, о которых известен только никнейм, то есть их сетевое имя. Однако, зачастую на практике эта схема шире и более функционально развита. Как правило, у нарко-магазина есть главный, его владелец, которого в своих кругах называют «seller», но никто из других участников системы его не знает. Под его руководством работают «бухгалтеры», «кураторы», «химики», «складмены», «операторы», «администраторы групп», «курьеры», каждый из которых выполняет свою роль, оставляя других участников системы незамеченными.

Раскроем более детально типичные роли соучастников в сообществах, занимающихся незаконным сбытом наркотических средств:

– организатор и руководитель – это лицо / лица, осуществляющие организационные и управленческие функции в преступной группе, координирующие её действия, разрешающие те или иные споры и т. д.;

криминологический журнал. 2019. № 1. С. 5–17. DOI: 10.17150/2500-4255.2019.13(1).5-17.

[3] Судебные и нормативные акты РФ [Электронный ресурс]. URL: https://sudact.ru (Дата обращения 10.05.2023).

[4] Бычкова, А. М. Трансграничный интернет и его роль в распространении глобальной угрозы наркотизма // Евразийский интеграционный проект: цивилизационная идентичность и глобальное позиционирование: Материалы Международного Байкальского форума, Иркутск, 20–21 сентября 2018 года / Под научной редакцией Е. Р. Метелевой. Иркутск: Байкальский государственный университет, 2018. С. 247–252.

– оператор – лицо, принимающее заказы и оплату от приобретателей наркотических средств посредством электронных платёжных систем, сообщающее о местах тайников с приобретаемым незаконным товаром;

– курьер – лицо, непосредственно доставляющее заказ из места незаконного хранения до тайника;

– «региональные склады» – лица, осуществляющие незаконное хранение партии наркотиков на той или иной территории, их расфасовку;

– закладчики – представители низшего структурного звена преступной группы, которые непосредственно по указанию оператора размещают наркотические средства в тайниковые закладки для незаконного сбыта приобретателям[5].

Однако, в описанной выше иерархии не выделен ещё один из наиболее значимых участников преступной группы – администратор Telegram-канала. Как и любой другой администратор, он отвечает за управление и моделирование канала, включая:

1) создание и публикацию контента на канале (вид и размер наркотика);

2) привлечение новых подписчиков и поддержание уровня активности на канале;

3) организацию конкурсов, опросов и других активностей на канале для поддержания интереса подписчиков;

4) ответы на вопросы и обратную связь от подписчиков;

5) управление командой модераторов для улучшения качества контента на канале и поддержания порядка.

Помимо этого, он публикует информацию о вакансиях, включая условия работы, требования к соискателям и контактную информацию для связи, что совершается в целях привлечения лиц для дальнейшей работы по распространению запрещённых веществ. Также важно понимать, что администратор является соучастником в совершении преступления и будет привлечён к ответственности по соответствующей статье Уголовного кодекса РФ.

Рассмотрим теперь типичную схему деятельности описанной преступной группировки. Первым делом создаётся канал, который будет выступать в роли интернет-магазина. На канале всё систематизировано: прайс-лист с ценами на наркотик; чат, на котором потребители могут делиться впечатлениями; объявления о вакантных местах для тех, кто ищет подработку, а также информациях о различных розыгрышах и акциях, бонусах. В объявлениях о вакансиях на должность закладчика или курьера, как правило, указан контакт, к которому можно обращаться по трудоустройству. Этот «ноунейм» присылает шаблон с информацией о зарплате, сути и условиях работы – сообщение следующего содержания: «Работа: тебе кидают адрес, ты идешь

[5]Овчинникова О. В. Особенности расследования сбыта наркотических средств, совершенных с использованием сети Интернет // Правопорядок: история, теория, практика. 2018. № 1 (16). С. 94–98.

и забираешь большую посылку, делишь ее на несколько посылок, а далее раскидываешь эти мелкие посылки в своем городе в любых местах, но в определенных районах. Фиксируешь координаты посылки, делаешь фотки места и присылаешь человеку, который будет тебя курировать. Один раз в неделю забрал большую посылку, поделил и раскидал ее по городу. Зарплата от 60 тысяч рублей, смотря как работать будешь». Чаще всего об истинном содержании посылки не говорят, уверяя, что придётся раскладывать полулегальный табак.

Для работодателя, то есть основателя наркомагазина, идеальным закладчиком считается лицо, которое к наркотикам не имеет никакого отношения, что является гарантией целостности переданного вещества. Также в целях гарантии целостности товара, курьерам выдвигается условие: им необходимо предоставить фотографии с паспортом у лица или же внести залог в денежном эквиваленте, обычно это сумма в размере 5 тысяч рублей. Но, в свою очередь, нужно понимать, что, оставляя фотографии с паспортом, лицо передаёт свои персональные данные и, по сути, становится зависим от преступников. В таком случае, о противоправной деятельности закладчика его же работодатели в любой момент могут проинформировать сотрудников правоохранительных органов, что заставляет начинающего закладчика выполнять все условия, выдвинутые куратором.

Также, существует и иной способ привлечения лиц для работы в этой противозаконной сфере – это массовые рассылки в других социальных сетях типа «Вконтакте» или «Instagram». Рассылка обычно содержит сообщение следующего содержания: «Доступный и хороший заработок. Курьер, водитель. Зп от 70 тысяч рублей в месяц. Выплаты еженедельно. Возраст 17+. Опыт не важен. Мы рады сделать Вам предложение о работе, пожалуйста, установите Telegram и напишите нам введя в поиск ***».

Также для привлечения внимания потенциальных работников и потребителей в Telegram активно используются функции рассылки для отправки существующим контактам и подписчикам канала приглашений на вакансию курьера и информации о наличии для приобретения конкретного вида наркотика определённой массы.

Так, именно Telegram, имея свои программные особенности, помогает злоумышленникам провести рекламную кампанию, чтобы привлечь больше людей в сферу своей преступной деятельности по распространению запрещённых веществ.

Подводя итог вышесказанному, ещё раз отметим, что личность пользователя в мессенджере Telegram установить довольно трудно, это позволяет преступникам, в частности торговцам наркотиками, практически безбоязненно вести свою деятельность через «Интернет».

Стоит отметить, что Правительство РФ установило новые правила идентификации пользователей сети «Интернет» организатором сервиса обмена мгновенными

сообщениями по номеру телефона[6]. Обязанность по проведению такой идентификации предусмотрена п. 1 ч. 4.2. ст. 10.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[7]. Однако, установление администраторов каналов в мессенджере Telegram до сих пор представляет собой задачу максимальной сложности, поскольку идентификатор любого канала никак не связан с идентификатором пользователя, который его создал. Большинство успешных деанонимизаций Telegram-каналов носят случайный характер и связаны с идентификацией личностей администраторов, контакты которых были указаны в описании самого канала.

Также задача идентификации Telegram-каналов осложнена тем, что мессенджер не имеет никаких представительств на территории России и не отвечает на запросы наших правоохранительных органов. Соответственно, идентификация пользователей или администраторов каналов по запросу полиции невозможна. Каналы в Telegram не имеют априорной формы обратной связи с администратором, т. е. сотрудники полиции не смогут в целях их деанонимизациии осуществить даже банальный сниффинг (изучение части интернет-трафика).

В итоге никаких имён или контактной информации – только изображение наркотика и его стоимость. Наконец, к оплате принимаются только криптовалюты, преимущественно биткоины, что делает практически невозможным для сотрудников правоохранительных органов выявить и установить наркопреступников.

Список литературы

1. Бертовский Л. В. К вопросу о понятии киберпреступлений // Расследование преступлений: проблемы и пути их решения. 2020. № 4 (30). С. 84–88.

2. Бычкова А. М. Трансграничный интернет и его роль в распространении глобальной угрозы наркотизма // Евразийский интеграционный проект: цивилизационная идентичность и глобальное позиционирование: Материалы Международного Байкальского форума, Иркутск, 20–21 сентября 2018 года / Под

[6]Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями: Постановление Правительства Российской Федерации от 20 октября 2021 г. №1801 // Официальный интернет-портал правовой информации pravo.gov [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202110210009 (Дата обращения: 10.05.2023).

[7] Об информации, информационных технологиях и о защите информации: федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ // Официальный интернет-портал правовой информации pravo.gov [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264 (Дата обращения 10.05.2023).

научной редакцией Е. Р. Метелевой. Иркутск: Байкальский государственный университет, 2018. С. 247–252.

3. Овчинникова О. В. Особенности расследования сбыта наркотических средств, совершенных с использованием сети Интернет // Правопорядок: история, теория, практика. 2018. № 1 (16). С. 94–98.

4. Суходолов А. П., Бычкова А. М. Цифровые технологии и наркопреступность: проблемы противодействия использованию мессенджера «Телеграм» в распространении наркотиков // Всероссийский криминологический журнал. 2019. Том 13. № 1. С. 5–17. DOI: 10.17150/2500-4255.2019.13(1).5-17.

Evgeny R. Zamyatin
Student
Ural Law Institute of the Ministry of Internal Affairs of the Russian Federation
(Yekaterinburg, Russian Federation)
zhenya.zamyatin.00@mail.ru

Scientific Supervisor: Ruslan S. Khamidullin
PhD in Law,
Head of the Department of operative-investigative activity
internal affairs bodies
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Ekaterinburg, Russian Federation)
46006@bk.ru

THE MAIN WAY OF COMMUNICATION OF DRUG CRIMINALS

Abstract: in the article: the ways of interaction of criminals carrying out their illegal activities in the field of illicit drug trafficking are considered. The means of communication (messengers) frequently used by drug criminals are analyzed. The functionality of the Telegram messenger is considered as the subject of the study. The features of the functions of the Telegram messenger and the ways of their use by drug criminals in their illegal activities are correlated.

Keywords: messenger, information technology, narcotic drugs, Telegram channel.

УДК 343.98

Красноперова Людмила Николаевна
Студент кафедры судебной экспертизы и криминалистики,
Белгородский государственный национальный
исследовательский университет
(г. Белгород, Российская Федерация)
krasnoluda13@gmail.com

Научный руководитель: Ярощук Инна Александровна,
кандидат филологических наук, доцент,
доцент кафедры судебной экспертизы и криминалистики
юридический институт Белгородского государственного национального
исследовательского университета
(г. Белгород, Российская Федерация)
yaroshchuk@bsu.edu.ru

ПРОФАЙЛИНГ В СОВРЕМЕННЫХ РЕАЛИЯХ

Аннотация. В статье рассматриваются понятие, сущность и задачи профайлинга как новой технологии в современных реалиях. Определены признаки неконгруэнтности партнёра, а также отмечена необходимость совершенствования образовательных программ по подготовке специалистов «криминалистический профайлер».

Ключевые слова: профайлинг, неконгруэтность, конгруэнтность, авиационный профайлинг, методика, технология.

Для цитирования:
Красноперова Л. Н. Профайлинг в современных реалиях // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 312–315.

Профайлинг, как новая технология, используется для выявления лиц, склонных к совершению преступлений и иных противоправных действий. Данная технология появилась относительно недавно, благодаря ей является возможным расшифровывать невербальные компоненты, которые проявляются в межличностном общении.

Суть профайлинга заключается в установлении личности в соответствии с характером и способом совершения преступления. Профайлинг как средство расследования уголовных преступлений направлен на использование сложных методов психологического профилирования для оптимизации следственных и процессуальных действий.

«Профайлинг – это комплекс методов и методик оценки и

прогнозирования поведения человека на основе анализа наиболее информативных признаков, характеристик внешности и поведения»[1].

Профайлинг в сфере криминалистики, так называемый «криминалистический» профайлинг, возник благодаря совместному развитию таких дисциплин, как психология, социология, криминология, судебная экспертиза, и согласованному действию соответствующих специалистов, преследующих цель определить личность преступника, специфика выбора жертв, их мотивы и цели.

Умение «просчитывать» психологическое состояние партнера по общению по внешним его проявлениям является важнейшим условием достижения целей по обеспечению безопасности в рамках задач правоохранительных органов.

Тело человека и его психика тесно взаимосвязаны. Таким образом, всё, что происходит внутри человека, влияет на него и внутренне: так, эмоциональные переживания отражаются в мимике, жестах и т. д. Больше всего информации во время общения передаёт именно лицо партнера. Поэтому люди, чтобы скрыть свои истинные намерения, мысли относительно совершения противоправных деяний, стараются изменить выражение лица, чтобы обмануть наблюдателя и таким образом ввести его в заблуждение.

Определить нечестность, неискренность, попытку обмануть партнера по общению в профайлинге можно с помощью такого понятия как «неконгруэтность». Так, в своих работах В. Л. Цветков определил конгруэнтность как «оценочное понятие, всегда оценка извне, и всегда интерпретация. Другая ситуация возникает, когда наблюдателю кажется, что в человеке есть что-то, противоречащее в его словах, вовсе не соответствующее его намерениям, то тогда можно говорить о неконгруэнтности»[2].

В современных условиях выделяют большое количество проверенных приёмов профайлинга, с помощью которых можно с максимальной точностью обнаружить признаки неконгруэнтности партнера по общению. Например, среди таких, выделяют:

– допущение логических ошибок;

– расхождение между словами и эмоциями;

– использование структурирования информации;

– использование так называемых жестов лжи;

– чрезмерное / полное отсутствие жестикуляции;

– нахождение в эмоционально дискомфортном состоянии.

Этот перечень не является исчерпывающим, выделяют множество других признаков, с помощью которых становится возможным начать подозревать человека в готовности совершить преступление, выявить его волнение, а также неуверенность. Однако следует

[1] Вахнина В. В. Профайлинг в деятельности органов внутренних дел. Москва: Академия управления МВД России, 2018. С. 5.

[2] Цветков В. Л. Профайлинг в деятельности органов внутренних дел. Москва: Юнити-Дана, 2014. С. 87.

помнить о том, что не всегда перечисленные признаки являются очевидными. В случаях, когда они не видны «невооружённым глазом» используют дополнительные способы, например, устанавливают незаметные признаки с помощью замедленной съёмки.

Одной из главной задач, реализуемой в настоящее время, для эффективного использования профайлинга в системе безопасности является подготовка специалистов в осуществлении требуемых программ. Так как именно от уровня подготовки, опыта работы сотрудников будет зависеть эффективность технологий профайлинга. Для успешной подготовки специалистов в этой сфере необходимо сочетать теоретическую основу и практический опыт сотрудников полиции, а также других силовых ведомств.

Профайлинг – один из эффективных способов обеспечения безопасности. С его помощью предоставляются такие возможности, как предотвращение противоправного действия, терроризма посредством выявления потенциально опасных ситуаций и лиц.

Пожалуй, самым большим и главным преимуществом профайлинга является гибкость и универсальность, что позволяет применять его не только на определённом объекте, но и на всех объектах, образующих массовое скопление людей.

В настоящее время профайлинг активно используется за рубежом практически во всех авиакомпаниях для обеспечения безопасности в аэропортах. Не является исключением и Российская Федерация. В аэропортах Пулково, Домодедово, Шереметьево, Внуково, активно используют профайлинг для обеспечения безопасности и предотвращения терактов. В российских аэропортах проводят выборочную проверку, а не каждого пассажира. Для выборной проверки используют два основных метода:

1) метод наблюдения (данный метод осуществляется с помощью осмотра и выявления несоответствий);

2) метод опроса (осуществляется с помощью наблюдения за реакцией партнера по общению в результате поставленного ему вопроса).

Таким образом, подводя итог всему вышесказанному, следует отметить, что в настоящее время профайлинг активно используется для обеспечения безопасности. Полученные положительные результаты подтверждают его практическую полезность. Благодаря чему становится возможным точно и правильно оценивать опасность субъекта, прогнозировать противоправное деяние, готовящееся преступление и своевременно его предупреждать. Сегодня использование профайлинга достаточно широко распространено в аэропортах, а также на железнодорожных вокзалах и в иных местах большого скопления людей как в России, так и за рубежом. Во всех перечисленных случаях профайлинг с большой степенью результативностью применяется в целях предупреждения терроризма.

Список литературы

1. Вахина В. В. [и др.] Профайлинг в деятельности органов внутренних дел: учебное пособие. Москва: Академия управления МВД России, 2018. 100 с.
2. Цветков В. Л. Профайлинг в деятельности органов внутренних дел: учебное пособие. Москва: Юнити-Дана, 2014. 254 с.

Lyudmila N. Krasnoperova
Student, Department of Forensic Examination and Criminalistics,
Belgorod State National Research University
(Belgorod, Russian Federation)
krasnoluda13@gmail.com

Scientific Supervisor: Inna A. Yaroshchuk,
PhD in Philology, Associate Professor,
Associate Professor of the Department of forensic expertise and criminalistics
Law Institute of Belgorod State National Research University
(Belgorod, Russian Federation)
yaroshchuk@bsu.edu.ru

PROFILING IN MODERN REALITIES

Abstract. The article discusses the concept, essence and tasks of profiling as a new technology in modern realities. The signs of incongruence of the partner are identified, and the need to improve educational programs for the training of specialists «forensic profiler» is also noted.

Keywords: profiling, incongruence, congruence, aviation profiling, methodology, technology.

УДК 347.786, 347.78.031.2

Калоша Егор Дмитриевич
Студент
Минский филиал
Российского Государственного Социального Университета
(г. Минск, Республика Беларусь)
yegor.kalosha@bk.ru

Научный руководитель: Бочарова Ольга Станиславовна,
кандидат юридических наук, доцент кафедры правовых дисциплин,
Минский филиал
Российского Государственного Социального Университета
(г. Минск, Республика Беларусь)
nihil13@mail.ru

ОХРАНА РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ КИНОПРОИЗВОДСТВА

Аннотация. Цель исследования заключается в изучении проблем, возникающих при создании аудиовизуального произведения, а именно: связанных с авторским правом на произведение и его охраной. Уделяется внимание способам защиты авторского права, а также коллизиям в законодательстве.

Ключевые слова: аудиовизуальное произведение, объект авторского права, интеллектуальная собственность, результат творческой деятельности.

Для цитирования:
Калоша Е. Д. Охрана результатов интеллектуальной деятельности в сфере кинопроизводства // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 316–324.

Аудиовизуальные произведения являются одной из важнейших с культурной и экономической точек зрения категорий объектов авторских прав, занимая доминирующее положение на современном рынке авторских прав. Как отмечал А. Луцкер, «аудиовизуальные произведения на протяжении последних десятилетий являются причиной многих серьёзных, широко обсуждавшихся конфликтов в сфере авторского права»[1].

Техническое развитие создаёт всё больше предпосылок для широкой востребованности аудиовизуальной продукции, включая художественные и телевизионные фильмы, сериалы,

[1] Луцкер А. П. Авторское право в цифровых технологиях и СМИ: товар. знаки, телевидение, интернет, образование, мультимедиа, радио / с науч. коммент. А. Серго. М.: КУДИЦ-Образ, 2005. С. 330

музыкальные и рекламные видеоролики и многие другие виды произведений, основанных на создании эффекта движущихся изображений, которые могут быть охарактеризованы в качестве аудиовизуальных произведений при условии их соответствия определению ст. 1263 Гражданского кодекса Российской Федерации (далее – ГК РФ).

В соответствии со ст. 1263 ГК РФ, аудиовизуальное произведение – это произведение, «…состоящее из зафиксированной серии связанных между собой изображений (с сопровождением или без сопровождения звуком) и предназначенное для зрительного и слухового (в случае сопровождения звуком) восприятия с помощью соответствующих технических устройств»[2]. Самая «типичная» категория аудиовизуальных произведений – это кинофильмы, а также «все произведения, выраженные средствами, аналогичными кинематографическим» (телепрограммы, видеоклипы и др.)

Сегодня авторское право является наиболее актуальной отраслью права, а создание аудиовизуального произведения требует использования результатов творческой деятельности широкого круга авторов и значительных затрат. В связи с чем, как отмечает в своей диссертационной работе Э. С. Ромашин, возникают две основные группы правовых проблем: «Первая группа проблем связана с постоянным расширением круга авторов и правообладателей, результаты творческой деятельности которых могут входить в аудиовизуальное произведение <…> Использование в современных аудиовизуальных произведениях значительного числа результатов творческой деятельности, а также непосредственное участие в их создании значительного числа авторов и специализированных компаний правообладателей приводят к возможности возникновения неурегулированных или конфликтных ситуаций <…> Вторая группа проблем обусловлена массовым характером использования аудиовизуальных произведений в современном мире, в значительной части случаев совершаемого с нарушениями требований законодательства об авторском праве, при отсутствии возможности осуществления эффективного контроля и принятия своевременных и достаточных мер для пресечения нарушений»[3].

Рассмотрим, как охраняются результаты интеллектуальной деятельности в сфере кино- и видеоиндустрии, как наиболее типичных и массовых. На каждое такое аудиовизуальное произведение (далее – фильм) существует т. н.

[2] Гражданский кодекс Российской Федерации (часть четвертая), № 318-ФЗ, 24 ноября 2006 (ред. от 11.06.2022) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_64629 (дата обращения: 08.05.2023).

[3] Ромашин Э. С. Особенности правовой охраны аудиовизуального произведения как сложного комплексного объекта интеллектуальной собственности: автореф. ... канд. юрид. наук. Москва, 2016. С. 3–4.

«двухуровневое авторство»[4]. Поясним на примере. В соответствии с правилами ст. 1263 ГК РФ, авторами любого аудиовизуального произведения являются три лица: режиссёр (постановщик), сценарист (автор сценария) и композитор, являющийся автором музыки, специально созданной для кинофильма. Режиссёр руководит постановкой аудиовизуального произведения и игрой актёров, сценарист создаёт сценарий фильма, композитор пишет для него музыку. Если в фильме звучат песни, то к числу авторов может примкнуть и автор слов. К тому же у фильма всегда в число авторов входят операторы, художники (постановщики, по гриму, по костюмам), сами актёры, чья игра и делает фильм. Не следует забывать и о том, что в основу данного произведения может быть положено уже ранее изданное литературное произведение, причём правами на него могут обладать не только сам писатель, но и его потомки. В соответствие с нормами части четвёртой ГК РФ все авторы обладают правом авторства и иными личными (неимущественными) правами в отношении аудиовизуального произведения.

Поэтому у такого аудиовизуального произведения как фильм есть и второй «уровень» авторства: в соответствии с п. 5 ст. 1263 ГК РФ, «…каждый автор произведения, вошедшего составной частью в аудиовизуальное произведение, как существовавшего ранее (автор произведения, положенного в основу сценария, и другие), так и созданного в процессе работы над ним (оператор-постановщик, художник-постановщик и другие), сохраняет исключительное право на свое произведение, за исключением случаев, когда это исключительное право было передано изготовителю или другим лицам либо перешло к изготовителю или другим лицам по иным основаниям, предусмотренным законом»[5]. У такого произведения как кинофильм всегда достаточно большое число различных по степени вклада в конечный результат авторов, чьи права и интересы необходимо учитывать.

Среди всех прав интеллектуальной собственности авторское право является основой всего производства в киноиндустрии. Защита авторов, а также правообладателей от несанкционированного использования их произведения третьими лицами – основная задача указанного института.

Авторское право регулирует и те отношения, которые возникают в результате производства и распространения результатов интеллектуальной деятельности вне трудовых процессов. При этом создаваемые произведения неразрывно

[4] Права на аудиовизуальное произведение: законодательство и практика // Зуйков и партнёры [Электронный ресурс]. 2015, 22 декабря. URL: https://zuykov.com/ru/about/articles/prava-na-audiovizualnoe-proizvedenie/ (дата обращения: 08.05.2023)

[5] Гражданский кодекс Российской Федерации (часть четвертая), № 318-ФЗ от 24.11.2006 (ред. от 11.06.2022) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_64629 (дата обращения: 08.05.2023).

связаны с авторами, именно поэтому данные права носят исключительный характер. Данные обстоятельства оказывают значительное влияние на регулирование правоотношений, определяя нормы авторского права в достаточно самостоятельное подразделение.

При разработке и принятии части четвёртой ГК РФ была предпринята попытка решения возникших проблем за счёт отнесения аудиовизуальных произведений к числу сложных объектов интеллектуальных прав, включающих в себя несколько результатов интеллектуальной деятельности, в отношении которых ст. 1240 ГК РФ предусмотрено специальное правовое регулирование вопросов принадлежности прав на произведения, создаваемые для использования в составе сложного объекта. Однако практика применения данных положений до настоящего времени носит ограниченный характер. Кроме того, положения о сложном объекте позволяют решить лишь часть проблем правовой регламентации создания и использования аудиовизуальных произведений, так как действие предусматриваемых ими презумпций распространяется только на произведения, специально созданные или создаваемые для включения в аудиовизуальное произведение.

Случаи нарушения авторских прав в России не редкость. Это связанно с неосведомлённостью правообладателей о способах защиты своих произведений, недостаточностью опыта и знания законодательства. Оказывает влияние и небольшое количество наработанной судебной практики по этому вопросу.

Есть несколько основных методов защиты авторских прав. Первый – это признание авторства, иными словами: определение принадлежности к конкретному лицу. Если какое-либо произведение было опубликовано анонимно, то сначала автору придётся подтвердить сам факт авторства, и только потом предъявлять претензии нарушителю. Подтверждением могут служить различные документы, черновики, фрагменты переписок, свидетельские показания и другие материалы. В некоторых случаях могут потребоваться экспертизы. Наиболее ярким примером является долгое установление авторства романа «Тихий Дон». Подтвердить авторство М. А. Шолохова получилось только после обнаружения оригинальной рукописи и её подробного исследования в 1999 году.

Второй метод – это полное восстановление положения, которое существовало до момента нарушения. Если в произведение были внесены правки без согласования с автором, он вправе требовать отмены этих правок (ст. 1251 ГК РФ).

И третий метод – пресечение действий, нарушающих авторское право. Как пример по данной теме можно привести судебные разбирательства с продолжением мультфильма «Простоквашино». Автор оригинала – Эдуард Успенский при жизни не раз обращался в суд и прокуратуру, с требованиями о запрете продолжения. На последнем заседании было установлено, что права на мультфильм также имеются и у

«Союзмультфильма»[6].

Все фильмы относятся к аудиовизуальным произведениям, которые ст. 1263 ГК РФ определяет, как «произведение, состоящее из зафиксированной серии связанных между собой изображений (с сопровождением или без сопровождения звуком)». Поэтому авторское право распространяется на любой фильм. В данную категорию входит большое количество объектов интеллектуальной собственности: видео-, телевизионные и кинофильмы; слайд-фильмы; короткометражки; мультфильмы; видеоклипы и др. Все эти объекты охраняются авторским правом.

Чаще всего аудиовизуальное произведение – это сложный, многоэлементный объект, в создании которого принимают участие большое количество лиц, в этом и заключается сложность защиты авторских прав.

С точки зрения права, это достаточно специфический объект интеллектуальной собственности, у которого обычно изначально имеется сразу несколько авторов, о чём было сказано выше. Но во главе всех стоит продюсер или заказчик – лица, которые несут ответственность за большинство рисков. Изготовителем (продюсером, заказчиком) может быть как физическое, так и юридическое лицо и оно же является особым субъектом прав, которому принадлежат исключительные права на весь фильм. Возможно, конечно, и иное распределение, но в этом случае конкретные условия должны быть прописаны в договоре.

Как правило, изготовитель фильма становится правообладателем по соответствующему договору. Так он подтверждает права на фильм, но бывают ситуации, когда автор и продюсер – одно лицо. В данном случае зафиксировать права на произведение можно несколькими способами. Во-первых, стоит сделать копии нескольких кадров, описать идею, сюжет фильма и заверить у нотариуса. Второй, и не менее распространённый способ, – это отправить самому себе посылку с текстом сценария, фрагментами фильма на материальном носителе и не вскрывать пакет до момента, когда потребуется подтверждение авторства.

Ещё один из способов – депонирование. В России действует презумпция авторства. Это значит, что автору произведения не требуется проходить какие-то установленные законом процедуры, чтобы закрепить за собой статус автора. Достаточно указать себя автором на оригинале или экземпляре произведения.

Депонирование произведения – один из способов защиты, который фиксирует: наличие объекта, его существование на конкретный момент времени, авторство конкретного лица. Депонирование схоже с регистрацией объекта авторского права. Регистрация права – один из наиболее надёжных способов защиты, но ст. 1259 ГК РФ не предусматривает регистрацию авторских прав. Проблема заключается в том, что депонирование не является юридическим фактом. Данную услугу

[6] Решение Суда по интеллектуальным правам г. Москва от 11 июля 2017 г. по делу № СИП-150/2017 // Судебные и нормативные акты РФ [Электронный ресурс]. URL: https://sudact.ru/arbitral/doc/E0UwT99ooAlN/ (дата обращения: 08.05.2023).

оказывают различные организации-депозитарии, а с недавнего времени стало возможно произвести депонирование онлайн. Процедуру регулируют внутренние правила организации-депозитария. В законах о таком способе защиты нет ни слова. Его часто используют, он относительно надёжен, но гарантировать, что суд встанет на сторону автора, такой вариант не в силах. В юридическом смысле депонирование представляет собой процесс организованного хранения объектов интеллектуальной собственности для последующей защиты законных интересов правообладателя. Результат депонирования авторских прав заключается в получении специального свидетельства, которое подтверждает, что на определённую дату объект авторского права существовал в конкретной форме[7]. Поэтому депонировать фильм рекомендуется до его обнародования – выпуска в прокат, публичного показа или размещения на сайте в Интернете.

В Российской Федерации срок действия авторского права равен продолжительности жизни автора, а также действует ещё 70 лет после его смерти. Свидетельство о депонировании будет действовать на протяжении всего этого времени.

Аудиовизуальные произведения занимают особое место среди объектов авторского права. Особенности предоставления правовой охраны таким произведениям, в целом, и их отдельным элементам закрепляются в российском законодательстве, в законодательстве иностранных государств, а также в большинстве международных соглашений.

К сожалению, в Российской Федерации законодательство и судебная практика находятся на разном уровне. Есть много неучтённых моментов. К примеру: согласно законодательству Российской Федерации, авторское право является неприкосновенным. Запрещается публиковать произведение с искажениями, но в то же время закон позволяет переработку произведения. Например, книгу можно экранизировать и это будет новым самостоятельным объектом интеллектуальной собственности, принадлежащим лицу, которое произвело переработку. Но как отличить искажение произведения от его переработки? Ответ на этот вопрос пока не нашли. В этой связи весьма известны иски детского писателя Эдуарда Успенского к правообладателям мультфильмов, созданных по его книжкам. Успенский требовал с «Союзмультфильма» отчисления за использование своих героев в мультфильмах. Киностудия отказалась, объяснив, что в результате переработки литературного источника были созданы новые художественные образы. То есть Матроскин Успенского и Матроскин «Союзмультфильма» – это разные персонажи. Суд поддержал позицию киностудии. «Союзмультфильм» не теряет надежды

[7] Сазонова М. Является ли депонирование презумпцией авторства? Мнения экспертов и обзор судебной практики // Информационно-правовой портал «ГАРАНТ.РУ» [Электронный ресурс]. 2021, 11 октября. URL: https://www.garant.ru/news/1489064/ (дата обращения: 08.05.2023).

выкупить у писателя его права, чтобы положить конец спору. Успенский собирается подавать в суд иск по поводу выпуска сериала по мотивам книги «Дядя Федор, пес и кот», первая серия которого вышла в феврале 2018 года[8].

Исключительное право на фильм как аудиовизуальное произведение существенным образом отличается по своему содержанию от исключительного права на иные виды произведений. При этом «использование любого результата интеллектуальной деятельности, вошедшего в аудиовизуальное произведение, отдельно от такого произведения, а также переработка аудиовизуального произведения могут осуществляться только на основании договора, заключенного с автором или иным правообладателем соответствующего результата интеллектуальной деятельности, и в установленных таким договором пределах»[9]. Данный вывод следует также из пункта 2 статьи 14 Бернской конвенции об охране литературных и художественных произведений, предусматривающего, что «…переделка в любую другую художественную форму кинематографических постановок, созданных на основе литературных или художественных произведений, требует разрешения авторов оригинальных произведений, вне зависимости от наличия разрешения авторов кинематографических постановок…», и пункта 1 статьи 14 bis Бернской конвенции, в соответствии с которым кинематографическое произведение подлежит охране в качестве оригинального «…без ущерба авторским правам…» на использованные при его создании произведения[10]. Бернская конвенция не предусматривает презумпции передачи авторами исключительных прав изготовителю аудиовизуального произведения, ограничиваясь установлением диспозитивной нормы о предоставлении авторами согласия на последующее беспрепятственное использование создаваемого произведения (подпункт (b) пункта 2 статьи 14 bis Бернской конвенции). В терминологии ГК РФ речь идёт только о предоставлении неисключительной лицензии в отношении основных видов использования созданного фильма, не охватывающей действия по его переработке или использованию результата творческой деятельности автора, участвовавшего в создании фильма, отдельно от созданного при его участии аудиовизуального произведения.

Проблемы выявления среди лиц, внёсших творческий вклад в создание

[8] 9 случаев, когда закон об интеллектуальной собственности вам не поможет // Юридическое агентство Санкт-Петербурга [Электронный ресурс]. URL: https://la-advokat.ru/blog/problemy-intellektualnoj-sobstvennosti/ (дата обращения: 08.05.2023).

[9] Ромашин Э. С. Особенности правовой охраны аудиовизуального произведения как сложного комплексного объекта интеллектуальной собственности: автореф. ... канд. юрид. наук. Москва, 2016. С. 10.

[10] Бернская Конвенция по охране литературных и художественных произведений от 09.09.1886 (ред. от 28.09.1979). // СПС «КонсультантПлюс» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_5112/ (дата обращения: 08.05.2023).

фильма, тех авторов, которые должны рассматриваться именно в качестве авторов фильма, а также определение принадлежащих таким авторам прав и порядка их перехода к изготовителю фильма, до настоящего времени не нашли единообразного решения в национальных законодательствах стран-участниц Бернской конвенции. В результате объединения разных элементов в фильме возникает единый объект, которое «растворяет» в себе вошедшие в него иные произведения, представляющие собой результат творческого вклада многих лиц – авторов, однако не сводится к простой совокупности таких вкладов, а выводит общий творческий результат на совершенно новый уровень. При этом аудиовизуальные произведения, как правило, обладают большой ценностью с экономической точки зрения, а правовое регулирование представляется достаточно противоречивым, и должно дополняться последовательной и согласованной судебной практикой[11].

В заключение следует отметить, что институт интеллектуальной собственности представляет собой ядро современной глобальной экономики и появление новых результатов интеллектуальной, творческой деятельности предполагает наличие их правовой охраны. При этом сами объекты права являются товаром. Роль интеллектуальной собственности станет ключевым фактором, определяющим социально-экономический рост в стране и её влияние в мире. Предпосылки для этого созданы развитием глобальных цифровых сетей, более 70 % трафика которых составляет движение объектов интеллектуальной собственности[12], а основной объём этого трафика связан с передачей различных аудиовизуальных произведений.

Список литературы

1. Луцкер А. П. Авторское право в цифровых технологиях и СМИ: товар. знаки, телевидение, интернет, образование, мультимедиа, радио / с науч. коммент. А. Серго. М.: КУДИЦ-Образ, 2005. 416 с.

2. Коротковская Е. С. Эффективное использование интеллектуальной собственности в современных российских социально-экономических условиях // Изв. Сарат. ун-та Нов. сер. Сер. Социология. Политология. 2018. Т. 18. Вып. 2. С. 162–168.

3. Ромашин Э. С. Особенности правовой охраны аудиовизуального произведения как сложного комплексного объекта интеллектуальной

[11] Права на аудиовизуальное произведение: законодательство и практика // Зуйков и партнёры [Электронный ресурс]. 2015, 22 декабря. URL: https://zuykov.com/ru/about/articles/prava-na-audiovizualnoe-proizvedenie/ (дата обращения: 08.05.2023)

[12] Коротковская Е. С. Эффективное использование интеллектуальной собственности в современных российских социально-экономических условиях // Изв. Сарат. ун-та. Нов. сер. Сер. Социология. Политология. 2018. Т. 18. Вып. 2. С. 163.

собственности: автореф. … канд. юрид. наук: Москва, 2016. 30 с.

Egor D. Kalosha
Student,
Russian State Social University branch in Minsk
(Minsk, Republic of Belarus)
yegor.kalosha@bk.ru

Scientific Supervisor: Olga S. Bocharova
PhD (Law), Associate Professor of the Department of Legal Disciplines of Russian State Social University branch in Minsk
(Minsk, Republic of Belarus)
nihil13@mail.ru

PROTECTION OF THE RESULTS OF INTELLECTUAL ACTIVITY IN THE FIELD OF FILM PRODUCTION

Abstract. The purpose of the study is to study the problems that arise when creating an audiovisual work, namely: related to copyright on the work and its protection. Attention is paid to the methods of copyright protection, as well as conflicts in legislation.

Keywords: an audiovisual work, an object of copyright, intellectual property, the result of creative activity.

УДК 343.98

Князева Александра Сергеевна
Студентка
Уральский государственный юридический университет
имени В.Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
aleks.knyazeva2016@yandex.ru

Научный руководитель: Матвеев Максим Михайлович
старший преподаватель кафедры криминалистики
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Россия)
matveevmaks@mail.ru

СУДЕБНАЯ ЭКСПЕРТИЗА В ОБЛАСТИ ЦИФРОВОГО ИСКУССТВА

Аннотация. В статье рассмотрены вопросы проведения судебной компьютерно-технологической экспертизы применительно к произведениям искусства в цифровом пространстве. Автором отмечены вариации проведения компьютерно-технологической экспертизы для произведений цифрового искусства в формате NFT. Сделан вывод о возможности применения искусственного интеллекта для данных судебных экспертиз.

Ключевые слова: судебная экспертиза, блокчейн, NFT-токен, пост-фотография, компьютерно-технологическая экспертиза.

Для цитирования:
Князева А. С. Судебная экспертиза в области цифрового искусства // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 325–329.

Судебные экспертизы многогранны в своих разновидностях: имеется значительная вариативность в зависимости от методики экспертного исследования или разрешаемых экспертизой вопросов.

Цифровые технологии блокчейна позволяют создавать различные изображения, интегрируемые затем на торговые площадки в формате NFT-токенов. Например, на аукционе Christie’s работа художника Beeple «Первые пять тысяч дней» была продана за рекордные $69 млн[1]. Несмотря на защищённость блокчейна подделки в

[1] Селизарова В. Как стартап россиян по выявлению NFT-подделок привлек $11 млн от инвестора Google // Forbes [Электронный ресурс]. 2022, 1 августа. URL: https://www.forbes.ru/svoi-biznes/473081-kak-startap-rossian-po-vyavleniu-nft-poddelok-

сфере NFT всё же встречаются, а следовательно, требуют и новых подходов к методике экспертиз.

Цифровые технологии в рамках проведения судебной экспертизы в настоящее время могут применяться и в случае с пост-фотографиями. Пост-фотография представляет собой новый способ создания изображений, который сочетает в себе методы аналоговой фотографии и искусственного интеллекта[2]. Подобные произведения интегрируются в NFT, а затем выставляются на маркетплейсах или в аукционных домах. Например, работа Рупа Райнисто «Полет лебедя» выставлялась на аукционе Christie's в апреле 2023 года.

Актуальность темы сохраняется и в случае предварительного использования плоттеров для создания изображения. Плоттер создаёт линейный рисунок, который затем дорабатывается самим художником. Примером этого может служить работа «Fidenza #163» Тайлера Хоббса. Художник использовал программируемого робота для создания рисунка, а затем собственноручно закрасил рисунок гуашью и интегрировал готовую работу в NFT-формат[3].

Блокчейн может рассматриваться как распределённая база данных, у которой устройства хранения не подключены к общему серверу. В случае назначения экспертизы судебно-экспертному учреждению эксперт получает доступ к системе посредством закрытого ключа[4], а затем исследует совокупность представленных в реестре данных – дорожку электронно-цифровых следов[5].

Экспертное исследование в рамках расследования преступлений, связанных с подделкой NFT, возможно с помощью технологий искусственного интеллекта. В частности, может иметь место применение компьютерно-технической экспертизы. Эксперт в данном случае должен обладать специальными компетенциями, а именно: понимать принципы работы информационной системы, в которой существуют NFT, уметь анализировать

---

privlek-11-mln-ot-investora-google?gallery=450565 (дата обращения: 03.04.2023).

[2] A collector's guide to AI and generative art // Christie's [Электронный ресурс]. 2023, 12 апреля. URL: https://www.christies.com/features/ai-and-generative-art-collecting-guide-12707-1.aspx?sc_lang=en#fid-12707 (дата обращения: 07.05.2023).

[3] A collector's guide to AI and generative art // Christie's [Электронный ресурс]. 2023, 12 апреля. URL: https://www.christies.com/features/ai-and-generative-art-collecting-guide-12707-1.aspx?sc_lang=en#fid-12707 (дата обращения: 07.05.2023).

[4] Бертовский Л. В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. № 6. С. 228.

[5] Карепанов Н. В. Особенности технологии агрегирования, исследования и использования электронно-цифровых следов преступления // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 87.

записи, отражённые в информационной системе[6], уметь пользоваться большим количеством операционных систем, уметь разворачивать сложные системы, включающие сетевую компоненту на тестовых компьютерах, разбираться в вопросах программирования в различных программных средах и на различных языках, а также программном реинжиниринге, видеть логику работы компьютерных сетей как на локальном, так и на глобальном уровне[7], владеть навыками создания и анализа технической документации по компьютерным средствам и системам, разбираться в нормативной базе, сопровождающей создание, эксплуатацию, внедрение, утилизацию элементов в распределённых реестрах.

Использование блокчейн-технологий в судебной экспертизе позволит достигнуть высокой степени надёжности и достоверности[8]. Технологическая экспертиза применительно к NFT-токенам может проводиться при помощи специальной методики автоматической верификации существующих NFT-художников и работ, выставленных на NFT-маркетплейсах. Кроме того, новые приложения позволяют проводить верификацию с авторами и работами, существующими в Интернете, но не представленными на маркетплейсах[9]. Верификацию возможно проводить также в случае с использованием Art Blocks на базе Ethereum, где художники используют систему для создания основы серии работ, а затем Art Blocks добавляет случайных элементов в созданный художником алгоритм. Таким образом, уникальные блоки будут запускаться для каждого конкретного покупателя, а на оригинальность в ходе компьютерно-технологической экспертизы может проверяться исходный код художника, положенный в основу набора работ.

Данные, полученные в рамках судебной экспертизы предметов искусства, могут быть использованы при расследовании преступлений, связанных с изготовлением контрафактных экземпляров произведений (ст. 146 УК РФ[10]). Использование компьютерных

[6] Колотов С. М. Компетенция судебных экспертов при производстве судебных экономических экспертиз в отношении операций с цифровыми активами, созданными с использованием технологии блокчейн // Законы России: опыт, анализ, практика. 2021. № 3. С. 35.

[7] Семикаленова А. И. Судебная компьютерно-техническая экспертиза: проблемы компетенций экспертов // Вестник криминалистики. 2020. № 2 (74). С. 72.

[8] Дондукова Т. Б., Кузбагаров М. Н., Кузбагарова Е. В. Судебная компьютерно-техническая экспертиза блокчейн-технологии // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 2. Казань: Изд-во «Познание» Казанского инновационного университета, 2022. С. 114–119.

[9] Колотов С. М. Практические аспекты производства судебных экономических экспертиз в отношении операций с цифровыми активами, созданными на основе технологии блокчейн // Вопросы экспертной практики. Март 2019. С. 316.

[10] Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. // Российская газета 1996. 18 июня.

технологий не только облегчит деятельность правоохранительных органов, но и будет способствовать более эффективному раскрытию и расследованию преступлений[11], что можно считать оптимизацией определённых аспектов профессиональной деятельности следователей[12].

Таким образом, с учётом развития цифровых технологий представляется возможным расширение области применения судебных компьютерно-технологических экспертиз предметов искусства. Вероятно использование искусственного интеллекта для анализа подлинности произведений на NFT-маркетплейсах.

Список литературы

1. Бахтеев Д. В. Тактика использования дронов при осмотре места происшествия // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 47–51.

2. Бертовский Л. В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. № 6. С. 226–230.

3. Долинин В. Н., Пермяков Е. К., Ровнушкин В. Е. Использование компьютерных технологий в правоохранительной деятельности // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 65–75.

4. Дондукова Т. Б., Кузбагаров М. Н., Кузбагарова Е. В. Судебная компьютерно-техническая экспертиза блокчейн-технологии // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 2. Казань: Изд-во «Познание» Казанского инновационного университета, 2022. С. 114–119.

5. Карепанов Н. В. Особенности технологии агрегирования, исследования и использования электронно-цифровых следов преступления // Технологии XXI века

[11] Долинин В. Н., Пермяков Е. К., Ровнушкин В. Е. Использование компьютерных технологий в правоохранительной деятельности // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 69.

[12] Бахтеев Д. В. Тактика использования дронов при осмотре места происшествия // Технологии XXI века в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 48/

в юриспруденции: мат-лы Четвёртой междунар. науч.-практ. конф. (Екатеринбург, 20 мая 2022 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В. Ф. Яковлева, 2022. С. 86–104.

6. Колотов С. М. Практические аспекты производства судебных экономических экспертиз в отношении операций с цифровыми активами, созданными на основе технологии блокчейн // Вопросы экспертной практики. Март 2019. С. 315–318.

7. Колотов С. М. Компетенция судебных экспертов при производстве судебных экономических экспертиз в отношении операций с цифровыми активами, созданными с использованием технологии блокчейн // Законы России: опыт, анализ, практика. 2021. № 3. С. 34–38.

8. Семикаленова А. И. Судебная компьютерно-техническая экспертиза: проблемы компетенций экспертов // Вестник криминалистики. 2020. № 2 (74). С. 70–74.

Aleksandra S. Kniazeva
Student
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
aleks.knyazeva2016@yandex.ru

Scientific Supervisor: Maxim M. Matveev
Senior Lecturer of Criminalistics Department
Deputy Director of the Institute of State and International Law
Ural State Law University
named after V. F. Yakovlev
(Ekaterinburg, Russia)
Matveevmaks@mail.ru

THE FORENSIC EXAMINATION IN DIGITAL ART

Abstract. The article deals with the issues of conducting forensic computer-technological expertise in relation to works of art in the digital space. The author notes the variations of computer-technological expertise for works of digital art in the NFT. The conclusion is made about the possibility of using artificial intelligence for these forensic examinations.

Keywords: forensic examination, blockchain, NFT token, art objects, post-photography, computer-technological expertise.

УДК 343.98

Кузнецова Елизавета Николаевна
Студент Института прокуратуры,
Уральский государственный юридический университет
имени В. Ф. Яковлева,
(г. Екатеринбург, Россия)
kuznetsova.elizaveta.nikolaevna@gmail.com

Научный руководитель: Матвеев Максим Михайлович
старший преподаватель кафедры криминалистики
заместитель директора Института государственного и международного права
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Россия)
Matveevmaks@mail.ru

ОСОБЕННОСТИ РАБОТЫ С ЦИФРОВЫМИ СЛЕДАМИ ПРИ ОСМОТРЕ МЕСТА ПРОИСШЕСТВИЯ

Аннотация. Статья посвящена особенностям осмотра места происшествия по делам о преступлениях в сфере компьютерной информации. Рассмотрены тактические особенности производства данного следственного действия с учётом специфики цифровых следов, проанализированы возможности специализированных технических средств, используемых следователями с целью обнаружения, фиксации и изъятия цифровых следов.

Ключевые слова: цифровые доказательства**,** цифровые данные, компьютерные преступления, компьютерная информация, изъятие цифровых следов.

Для цитирования:
Кузнецова Е. Н. Особенности работы с цифровыми следами при осмотре места происшествия // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 330–335.

Современное общество не может существовать без «цифры»: мы всё время находимся в цифровом пространстве. Именно это неосязаемое цифровое пространство в 21 веке для криминалистики и для борьбы с преступностью в целом является основным источником «следовой картины» последствий преступного деяния.

Цифровой след – сложное и многоаспектное понятие, в научной литературе на этот счёт нет единого мнения. Цифровой след – любая криминалистически значимая компьютерная информация, то есть

сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов[1]. Данная позиция неоднозначна, поскольку исследуемая категория следов отображается не только в компьютерных, но и в цифровых устройствах (смартфоны, фотокамеры, мобильные телефоны, планшеты и т. д.). Можно также согласиться с точкой зрения В. Ю. Агибалова, который указывает на то, что «в результате электронно-цифрового отображения на материальном носителе фиксируется лишь образ, состоящий из цифровых значений параметров формальной математической модели наблюдаемого реального физического явления»[2].

Представляется, что цифровые следы не могут быть отнесены к идеальным, а также не в полной мере соответствуют характеристикам материальных следов. Они представляют третью специфическую разновидность следовой информации, используемой в доказывании по уголовным делам[3].

Как показывают практика расследования и теория криминалистики, цифровые технологии могут рассматриваться как способ или средство совершения преступлений.

При совершении преступлений в сети Интернет непосредственный контакт преступника и потерпевшего в большинстве случаев исключается. Полностью уничтожить следы пребывания в коммуникационной сети невозможно, но существуют современные способы их маскировки. Поэтому с каждым годом возрастает количество преступлений в сфере компьютерной информации. Согласно статистике МВД о состоянии преступности за январь-декабрь 2022 года зарегистрировано 522065 преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (распространение экстремистской и иной запрещённой информации по средствам сети Интернет, «взлом» защиты компьютерных сетей и программ, Интернет и SMS-мошенничества, участие в группах смерти и т. д.). Однако криминалистика не стоит на месте и находит новые приёмы и способы, предназначенные для сбора, исследования и использования доказательств в целях раскрытия и расследования преступлений. В частности, появляются новые методики исследования электронных носителей информации, реализация

[1] Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки: монография. Волгоград: Волгоградская акад. МВД России, 2008. С. 89–92.

[2] Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе: дис. … канд. юрид. наук. Воронеж: ГОУ ВПО «Воронежский государственный университет», 2010. С. 13, 30.

[3] Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. 2019. № 6 (129). С. 68.

которых уместна при изучении содержимого того или иного флеш-накопителя, жёсткого диска и других носителей информации, а также восстановления удалённых данных.

Заслуживают внимание и вопросы, касающиеся повышения эффективности следственного осмотра, в том числе осмотра места происшествия, по делам о компьютерных преступлениях.

Осмотр и предварительное исследование компьютерных средств и систем, на месте происшествия, а также цифровых данных, которые передаются по компьютерным сетям, значительно расширяют возможности процесса доказывания по уголовным делам, так как позволяют собирать криминалистически значимую компьютерную информацию о событиях или действиях, отражённую в материальной среде в процессе её возникновения, обработки, хранения и передачи и представляющую собой цифровые следы[4].

Осмотр места происшествия – наиболее распространённое и значимое следственное мероприятие в ходе расследовании компьютерных преступлений. Поскольку данные действия производятся в достаточно сжатые промежутки времени, а значит выделяется мало времени на подготовку, то сложность заключается в неотложности. Однако необходимо провести ряд подготовительных действий, в противном случае, прибыв на место происшествия для его осмотра, следователь с большой долей вероятности столкнётся с некоторыми проблемными ситуациями[5]. Например, не сможет обнаружить видимые материальные признаки совершённого деяния, цифровые следы в жилых или офисных помещениях, где находятся средства вычислительной техники (компьютеры, мобильные устройства, серверы, маршрутизаторы). В ряде случаев компьютерное оборудование связанно в локальную сеть и размещено в разных частях здания. Кроме того, установить связь между преступлением и осматриваемым местом происшествия при подобных обстоятельствах возможно только с использованием специальных знаний и технико-криминалистических средств.

Более качественному и быстрому изъятию следов преступной деятельности могут способствовать аппаратно-программные комплексы («Мобильный криминалист», UFED, SecureView 3, Magnet, MicroSystemation, XRY и др.). В рамках проведения оперативно-розыскных мероприятий и следственных действий их применение позволяет извлечь необходимую информацию с технических устройств, имеющую значение для расследования уголовного дела[6]. В настоящее время

[4] Россинская Е. Р., Семикаленова А. И. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. Т. 11. Вып. 3. 2020. С. 745–759.

[5] Перевалов В. Д. Теоретические и исторические аспекты российского юридического образования// Российское право: образование, практика, наука. 2009. № 2 (55). С.113.

[6] Баркова Т. В. К вопросу использования криминалистических экспертиз для решения

более чем актуальным становится вопрос разработки и внедрения аппаратно-программных комплексов отечественного производства, совершенствование уже используемой в данной области криминалистической техники.

Так, например, криминалистическое программное обеспечение «Мобильный криминалист» (Оксиджин Софтвер) предоставляет возможность изъять информацию, хранящуюся в мобильном телефоне, компьютерном устройстве, а также в облачном хранилище (iCloud, Microsoft OneDrive, Amazon Drive и др.), даже если устройство является заблокированным[7].

Применение аналогичных аппаратно-программных комплексов позволит эффективно решать задачи не только следственного осмотра, но и ряда судебных исследований, проводимых в условиях применения специальных знаний сведующих лиц.

Другая, не менее функциональная программа UFED также позволяет извлекать криминалистически значимую информацию с различных компьютерных устройств. Данное программное обеспечение способно работать практически со всеми видами мобильных устройств[8]. Существенным достоинством указанного комплекса является возможность исследования нерабочего телефона (например, в результате технической поломки или долгое время находящегося в воде). Помимо устройств, работающих на IOS и Android, программа поддерживает менее популярные операционные системы, такие как Windows Phone, SIRIN OS и др. Несомненным преимуществом является тот факт, что приложение обладает способностью к декодированию пароля любой сложности, установленного на телефоне.

Специальная программа для исследования компьютерной информации Belkasoft способствует поиску, анализу, изъятию и копированию цифровых следов, находящихся на техническом устройстве. Программа анализирует жёсткие диски, образы, облачные хранилища, резервные копии iOS, Android, Blackerry и chip-off-дампы.

Говоря о проблемных вопросах изъятия цифровых следов, стоит отметить, что процедура их фиксации и изъятия из социальных сетей и мессенджеров требует определённого порядка (который автором подробно не рассматривается в рамках настоящей статьи), связанного со спецификой данных объектов. Несоблюдение правил работы с такими доказательствами может привести к признанию полученных цифровых данных из сети Интернет или

вопросов по «новым составам» преступлений // Дневник науки. 2020. № 10 (46). С. 33–39.

[7] Программно-аппаратный комплекс «Мобильный Криминалист» [Электронный ресурс]. URL: https://www.oxygensoftware.ru/ru/products/ mk (дата обращения: 30.04.2023).

[8] Ханов Т. А., Нуркеев А. Ж. Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений // Известия Алтайского государственного университета. 2017. № 6 (98). С. 105–111.

электронных носителей информации недостоверными и, как следствие, недопустимыми доказательствами по делу.

В заключении хотелось бы повторно акцентировать внимание на острую необходимость в нынешних условиях актуализации ведущихся разработок в данной области российскими научно-исследовательскими объединениями, обеспечивающими технико-криминалистическое сопровождение процесса расследования.

Список литературы

1. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе: дис. … канд. юрид. наук. Воронеж: ГОУ ВПО «Воронежский государственный университет», 2010. 198 с.

2. Баркова Т. В. К вопросу использования криминалистических экспертиз для решения вопросов по «новым составам» преступлений // Дневник науки. 2020. № 10 (46). С. 33–39.

3. Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. 2019. № 6 (129). С. 61–68.

4. Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки: монография. Волгоград: Волгоградская акад. МВД России, 2008. 401 с.

5. Перевалов В. Д. Теоретические и исторические аспекты российского юридического образования // Российское право: образование, практика, наука. 2009. № 2 (55). С. 112–114.

6. Россинская Е. Р., Семикаленова А. И. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. 2020. Т. 11. Вып. 3. С. 745–759.

7. Ханов Т. А., Нуркеев А. Ж. Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений // Известия Алтайского государственного университета. 2017. № 6 (98). С. 105–111.

Elizaveta N. Kuznetsova
Student of the Prosecutor's Office
Ural State Law University
named after V.F. Yakovlev,
(Ekaterinburg, Russia)
kuznetsova.elizaveta.nikolaevna@gmail.com

Scientific Supervisor: Maxim M. Matveev
Senior Lecturer of Criminalistics Department
Deputy Director of the Institute of State and International Law

Ural State Law University
named after V. F. Yakovlev
(Ekaterinburg, Russia)
Matveevmaks@mail.ru

FEATURES OF WORKING WITH DIGITAL TRACES WHEN EXAMINING THE CRIME SCENE

Abstract. The article is devoted to the peculiarities of the examination of the scene of incident in cases of crimes in the field of computer information. The tactical peculiarities of this investigative action are considered, taking into account the specifics of digital traces, the possibilities of specialized technical means used by investigators to detect, record and seize digital traces are analysed.

Keywords: digital evidence, digital data, computer crimes, computer information, seizure of digital (electronic-digital) traces.

УДК 336.74

Курилов Максим Николаевич
Студент Института юстиции
ФГБОУ ВО «Саратовская государственная юридическая академия»
(г. Саратов, Российская Федерация)
kurilovm525@gmail.com

Ермолович Василина Сергеевна
Студент Института юстиции
ФГБОУ ВО «Саратовская государственная юридическая академия»
(г. Саратов, Российская Федерация)
vasilina.e02@mail.ru

Научный руководитель: Быкова Тамара Анатольевна
кандидат юридических наук, доцент,
профессор кафедры гражданского права
Саратовская государственная юридическая академия
(г. Саратов, Российская Федерация)
d.grachev@yandex.ru

КРИПТОВАЛЮТА КАК СРЕДСТВО БЕЗНАЛИЧНЫХ РАСЧЁТОВ В ГРАЖДАНСКОМ ПРАВЕ РФ

Аннотация. В статье поднимается вопрос об использовании криптовалюты в качестве средства безналичных расчётов по гражданско-правовым сделкам. Посредством анализа нормативно-правовой базы российского законодательства делается анализ криптовалюты как платежного средства в Российской Федерации.

Ключевые слова: криптовалюта, гражданско-правовые сделки, безналичный расчёт, цифровая валюта, виртуальная валюта, цивилистика, гражданское право.

Для цитирования:
Курилов М. Н., Ермолович В. С. Криптовалюта как средство безналичных расчётов в гражданском праве РФ // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 336–340.

На современном этапе развития общество испытывает постоянную необходимость во внедрении и использовании цифровых технологий в различных областях. Примером тому может служить криптовалюта как один из способов безналичных расчётов. Криптовалюта рассматривается как объект правоотношений различными отраслями права. С позиций уголовного, налогового права «Отсутствие полного регулирования в этой сфере приводит не только к проблемам во взаимоотношениях с

юридической точки зрения, и не только к проблемам с классификацией как преступления и как объекта вмешательства, но и к налоговым потерям. Чем популярнее становится технология, тем больше людей вовлечены в нее и получают от нее выгоду, и тем больше отсутствие регулирования открывает возможности для незаконной деятельности»[1]. Для цивилистики криптовалюта представляет интерес как средство расчёта по гражданско-правовым сделкам. В этой связи представляется актуальным проанализировать правовые нормы российского законодательства и выяснить, возможно ли использовать криптовалюту как основное средство оплаты в рамках гражданско-паровых сделок.

В первую очередь обратимся к ч. 3 ст. 1 Федерального закона от 31 июля 2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», которая закрепляет следующее положение: «Цифровой валютой признается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам»[2].

Из данного определения, следует, что российским законодательством допускается использование криптовалюты в качестве средства платежа. Однако, проанализировав нормативно-правовые акты, можно сделать вывод, что процитированная ранее правовая норма относится к числу неисполняемых и неисполнимых, поскольку не имеет дополнительного закрепления во многих отраслях российского законодательства, в том числе и гражданском праве.

Так, в ст. 140 Гражданского кодекса РФ (далее – ГК РФ) закреплено положение о том, что, во-первых, «рубль является законным платежным средством, обязательным к приему по нарицательной стоимости на всей

[1] Вяжева Д. Ю., Тищенко О. В. Криптовалюта как объект гражданско-правового регулирования // Проблемы социально-экономического развития Сибири. 2022. № 2. С. 37.

[2] Федеральный закон от 31 июля 2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (ред. от 14 июля 2022) // Собрание законодательства РФ. 2020. № 31 (часть I). Ст. 5018; 2022. № 29 (часть III). Ст. 5298.

территории Российской Федерации»[3], во-вторых, «платежи на территории Российской Федерации осуществляются путем наличных и безналичных расчетов» и в-третьих, «случаи, порядок и условия использования иностранной валюты на территории Российской Федерации определяются законом или в установленном им порядке». То есть, последняя редакция ГК РФ в качества основного средства расчёта по гражданско-правовым сделкам видит только рубль и иностранную валюту, использование которых допускает как в наличной, так и безналичной форме. О возможности использования криптовалюты в данном случае речи не идёт.

Можно предположить, что такая ситуация вызвана ранее сложившимся отношением Банка России к использованию «виртуальных валют» на территории России. Так, ещё в 2014 году в своём информационном сообщении «Информация об использовании при совершении сделок «виртуальных валют», в частности, Биткойн» было высказано, следующее: «Банк России отмечает, что в последнее время в мире получили определенное распространение так называемые «виртуальные валюты», в частности, Биткойн. По «виртуальным валютам» отсутствуют обеспечение и юридически обязанные по ним субъекты. Операции по ним носят спекулятивный характер, осуществляются на так называемых «виртуальных биржах» и несут высокий риск потери стоимости»[4]. Несмотря на то, что с момента издания данного и информационного письма прошло уже 10 лет, доверия к использованию криптовалюты у государства так и не появилось. В подтверждение тому можно привести достаточно свежую информацию, опубликованную на официальном сайте Федеральной нотариальной палаты. Так, в одной из актуальных статей подчёркивается ранее упомянутый факт о том, что «…законным платежным средством на территории РФ является российский рубль. Соответственно, любые денежные обязательства должны быть выражены в рублях»[5]. При этом, вторая сложность урегулирования данного вопроса также кроется в понятийном аппарате: «…если рассматривать в качестве платежного средства не криптовалюту, а отчасти урегулированную российским законодательством цифровую валюту. Прежде всего, барьером для совершения платежа выступает тот факт, что цифровая валюта признается имуществом. Соответственно, идея приобрести за имущество другое

[3] Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 № 51-ФЗ (ред. от 16 апреля 2022) // Собрание законодательства РФ. 1994. № 32. Ст. 3301; 2022. № 16. Ст. 2601.

[4] Информация об использовании при совершении сделок «виртуальных валют», в частности, Биткойн // Вестник Банка России. 2014. № 11. URL: https://cbr.ru/Queries/XsltBlock/File/86262/-1/1489 (дата обращения: 27.03.2023).

[5] Цифровая нереальность: что можно и что нельзя делать с криптовалютой // Информационно-правовой портал «Нотариат.рф». [Электронный ресурс]. URL: https://notariat.ru/ru-ru/news/cifrovaya-nerealnost-chto-mozhno-i-chto-nelzya-delat-s-kriptovalyutoj-2205 (дата обращения: 27.03.2023).

имущество, например, недвижимое, противоречит самому понятию сделки купли-продажи»[6].

Таким образом, на основе анализа норм российского законодательства представляется, что вопрос применение криптовалюты в качестве средства расчёта по гражданско-правовым сделкам на данный момент не находит своего законодательного закрепления. В этой связи, использование подобного «денежного эквивалента» с учётом большим пробелов законодательного регулирования в области цифровых активов на данный момент является достаточно спорной процедурой. Выходом из этого положения может стать принятие на законодательном уровне своей собственной официальной цифровой валюты, использовать которую будет возможно в качестве законного платёжного средства, а следовательно, и в качестве средства расчёта по гражданско-правовым сделкам. Однако полный отказ от возможности использования криптовалюты будет не оправдан по той причине, что мировое сообщество, учитывая состояние экономики и нестабильность доллара США, выступающего ключевой валютой международной финансовой системы, всерьёз предпринимает усилия по внедрению данной цифровой валюты в качестве средства платежа по заключаемым сделкам и договорам. Так, «…один австралийский блокчейн-проект, носящий название TravelbyBit, претендует в обозримом будущем превратиться в глобальную платежную платформу, осуществляющую мультивалютные безналичные платежи в аэропортах мировых столиц, в том числе оплату в наиболее популярных криптовалютах. Вскоре путешественники смогут расплачиваться криптовалютами в крупнейших аэропортах мира, не заботясь о наличии местной валюты зарубежной страны, экономя на потерях в виде курсовых разницах при обмене иностранных валют. Примечательно, что TravelbyBit разрабатывает для туристов разнообразные маршруты в различных уголках мира, посещая которые они могут бронировать и оплачивать посредством криптовалют»[7].

[6] Цифровая нереальность: что можно и что нельзя делать с криптовалютой // Информационно-правовой портал «Нотариат.рф». [Электронный ресурс]. URL: https://notariat.ru/ru-ru/news/cifrovaya-nerealnost-chto-mozhno-i-chto-nelzya-delat-s-kriptovalyutoj-2205 (дата обращения: 27.03.2023).

[7] Австралийская блокчейн-сеть Red Belly Blockchain способна обрабатывать до 30 000 трансграничных платежей в секунду. // Блокчейн. [Электронный ресурс]. URL: https://blockchain.ru/posts/avstralijskaya-blokchejn-set-red-beUy-blockchain-sposobna-obrabatyvat-do-30-000-transgranichnyh-platezhej-v-sekundu (дата обращения: 19.04.2023)

Список литературы

1. Вяжева Д. Ю., Тищенко О. В. Криптовалюта как объект гражданско-правового регулирования // Проблемы социально-экономического развития Сибири. 2022. № 2. С. 35–38.

Kurilov Maxim Nikolaevich
Student of the Institute of Justice
Saratov State Law Academy
(Saratov, Russian Federation)
kurilovm525@gmail.com

Ermolovich Vasilina Sergeevna
Student of the Institute of Justice
Saratov State Law Academy
(Saratov, Russian Federation)
vasilina.e02@mail.ru

Scientific Supervisor: Tamara A. Bykova
PhD in Law, Associate Professor,
professor of the civil law department
Saratov State Law Academy
(Saratov, Russian Federation)
d.grachev@yandex.ru

CRYPTOCURRENCY AS A MEANS OF NON-CASH PAYMENTS IN THE CIVIL LAW OF THE RUSSIAN FEDERATION

Abstract. the article raises the question of using cryptocurrency as a means of non-cash payments for civil transactions. Through the analysis of the regulatory framework of Russian legislation, the analysis of cryptocurrency as a means of payment in the Russian Federation is made.

Keywords: cryptocurrency, civil transactions, cashless settlement, digital currency, virtual currency, civil law, civil law.

УДК 347

Кушнарёв Александр Сергеевич
Студент Института прокуратуры
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
kushnarev-02@list.ru

Научный руководитель: Калистратова Наталия Сергеевна,
заместитель директора Института прокуратуры
УрГЮУ имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
kns003@usla.ru

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ АВТОРСКИХ ПРАВ НА КОД И ИНТЕРФЕЙС ПРОГРАММЫ В СЕТИ ИНТЕРНЕТ

Аннотация. Проблема совершенствования законодательства в сфере защиты авторских прав – одна из наиболее актуальных в России. Обусловлена она тем, что в связи с резким развитием информационных и коммуникационных технологий у недобросовестных пользователей появляется возможность незаконно обладать кодом программы или же её интерфейсом.

Ключевые слова: авторское право, код программы, интерфейс программы, IT-технологии, ЭВМ.

Для цитирования:
Кушнарёв А. С. Актуальные проблемы защиты авторских прав на код и интерфейс программы в сети Интернет // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 341–346.

В условиях формирования высоких технологий и градационного перехода рыночной экономики к инновационной правовое регулирование интеллектуальных авторских прав становится одним из значимых направлений работы государства. В связи с чем одной из актуальных проблем, стоящих сегодня перед российской правовой системой, является проблема защиты авторских прав, в том числе в сети «Интернет»[1].

Говоря о сети «Интернет», следует отметить, что сфера IT-технологий, непосредственно связанная с всемирной паутиной, является на данный момент одной из самых престижных и

[1] Осипов М. Ю. Защита авторских прав в сети «Интернет»: основные особенности и проблемы // Актуальные проблемы российского права. 2018. № 12 (97). С. 116–122.

быстроразвивающихся сфер, что в свою очередь порождает и определённые правовые проблемы.

Так или иначе каждый разработчик задаётся вопросом: как защитить технологию, идею, продукт? В IT-сфере практическим вопросом становится защита права на технологию (код) программы, интерфейс.

Существует суждение, что в сети «Интернет» нереально гарантировать законную защиту авторских прав из-за недоступности ограничений на свободное дублирование и трудности контроля за копированием и применением произведений. Но все без исключения компоненты интернет-сайтов, которые в соответствии с законодательством признаются объектами авторских прав, можно и, что наиболее важно, нужно защищать.

Начнём с того, что перечисленные объекты охраняются авторским правом, которое возникает у их создателя. В юридическом пространстве под таким термином как «код» предполагается «программа для ЭВМ». В соответствии с законодательством РФ дефиниция программы для ЭВМ как объекта авторского права определена в ст. 1261 Гражданского кодекса Российской Федерации (далее – ГК РФ) – это представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определённого результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения (здесь и далее – программа для ЭВМ, программное обеспечение). Некоторые авторы приводят свои определения программы для ЭВМ, например, представляя её как «совокупность детальных команд и инструкций, написанная на одном из машинных языков, которая указывает, что делать компьютеру»[2]. По мнению С. П. Гришаева, программа для ЭВМ – текст, объективированный любым образом – на бумаге, в памяти ЭВМ, в виде изображения на экране монитора. При этом автор отмечает, что каждое аудиовизуальное произведение, взятое в отдельности (например, заставка к игровой программе), может рассматриваться и как часть программы, и как художественное произведение, в связи с чем должна охраняться как отдельный объект авторского права[3].

Такие программы могут быть созданы на любом языке и в любой форме, но они всегда включают себя исходный текст и объектный код.

Исходный текст – это код, который понятен программисту, а объектный код – это код, понятный компьютеру. По этой причине программа для ЭВМ среди объектов авторского права приравнивается к литературным произведениям.

В свою очередь, при защите авторского права на код законодатель сталкивается с первой проблемой, которая выражена в том, что языки

[2] Маккланг К. Дж., Герриери Д. А., Маккланг К. А. Микрокомпьютеры для юристов. М.: Юридическая литература, 1988. С. 144.

[3] Гришаев С. П. Интеллектуальная собственность: учебное пособие. М.: Юристъ, 2004. С. 288.

программирования являются компилируемыми, так как получить исходный текст чужой программы невозможно, если его не передал сам программист-разработчик. А поскольку интерфейс программы (аудиовизуальные отображения) есть у каждой компьютерной программы, то интерфейс должен включаться в программу для ЭВМ, т. е. это не нечто отдельное, а наоборот, часть программы. В свою очередь, существует и противоположная точка зрения: ряд авторов считают[4], что аудиовизуальные отображения есть нечто иное как художественные произведения, что опосредует другую насущную проблему – не все правообладатели могут сразу разграничить такие понятия, что приводит дело в суд, поскольку стороны не оформляют должным образом договорные отношения; не все понимают важность процедуры патентования объектов авторских прав, регистрации товарного знака, регистрации программы для ЭВМ в Роспатенте, Минкомсвязи. Как показывает практика, только когда права уже нарушены третьими лицами или же работниками (программистами), правообладатели обращаются к юристам и оформляют авторское право по закону.

Одним из вариантов решения проблемы может быть «осуществление гражданских прав и исполнение обязательств по договору исходным кодом программы ЭВМ»[5]. Подтверждением заявленного тезиса служит Постановление Суда по интеллектуальным правам от 25.02.2019 г. по делу № А72-7169/2017. Так, согласно фактическим обстоятельствам дела, истец обратился с требованием о признании исключительного права на программу для ЭВМ, однако ответчик отказал подписывать акт передачи исключительного права. По договору оказания услуг по разработке программного обеспечения, заключённому между сторонами, истцу (заказчику) должны были быть переданы исключительные права. Суды первой и апелляционной инстанции исковые требования удовлетворили. Суд по интеллектуальным правам поддержал выводы судов нижестоящих инстанций: отказ ответчика от подписания акта передачи исключительного права, предусмотренного заключённым между истцом и ответчиком договором, а также регистрация программы для ЭВМ в Роспатенте оценены судами как обстоятельства, свидетельствующие об оспаривании наличия у истца исключительного права на указанный объект авторского права с учётом нормы подпункта 1

[4] Алисова Е. В. Актуальные проблемы защиты авторского права в сети Internet // Наука, образование и культура. 2016. № 7 (10). С. 55–62.

[5] Адельшин Р. Н. Роль правовой инфраструктуры договорных отношений с участием потребителей в свете новеллизации объектов гражданских прав // Современные тенденции развития гражданского и гражданского процессуального законодательства и практики его применения. 2020. № 6. С. 8–16.

пункта 1 статьи 1252 ГК РФ[6].

Не менее интересный тезис был сформулирован и Научно-консультативным советом при Суде по интеллектуальным правам: «Государственная регистрация программы для ЭВМ не носит правоустанавливающий характер, порождённая ею презумпция может быть опровергнута в том числе при рассмотрении дела о нарушении исключительного права»[7]. За основу был взят спор, связанный с требованием о взыскании компенсации за нарушение исключительного права на программу для ЭВМ. Ответчик в данном деле оспаривал наличие у истца исключительного права на программу для ЭВМ и исходил из того, что факт государственной регистрации не является достаточным и безусловным доказательством, кроме того, при государственной регистрации программы для ЭВМ проводится лишь формальная экспертиза (п. 1 ст. 1262 ГК РФ). Суд по интеллектуальным правам отменил судебные акты нижестоящих инстанций, потому что в них не было отражено, каким образом и на каком основании судами был установлен факт принадлежности истцу исключительного права на программу для ЭВМ. Помимо этого, суд кассационной инстанции отметил, что довод ответчика касаемо наличия у него исключительного права на программу не может подтверждаться лишь ссылкой на государственную регистрацию программы для ЭВМ.

«По смыслу положений статьи 1262 ГК РФ государственная регистрация программы для ЭВМ не является правообразующим фактом, а следовательно, порождённая ею презумпция (п. 6 ст. 1262 ГК РФ, пункт 109 постановления Пленума Верховного Суда Российской Федерации от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации») может быть опровергнута, в том числе при рассмотрении дела о нарушении исключительного права»[8]. Следовательно, документация на передачу исключительных прав должна быть оформлена надлежащим

[6] Постановление Суда по интеллектуальным правам от 25.02.2019 № С01-128/2018 по делу № А72-7169/2017.

[7] Обзор практики Суда по интеллектуальным правам по вопросам, возникающим при применении норм Гражданского кодекса Российской Федерации о правовой охране программ для ЭВМ и баз данных // Журнал Суда по интеллектуальным правам. [Электронный ресурс]. URL: http://ipcmagazine.ru/official-cronicle/review-of-the-practice-of-the-intellectual-property-rights-court-on-issues-arising-from-the-application-of-the-norms-of-the-civil-code-of-the-russian-federation-on-the-legal-protection-of-computer-programs-and-databases (дата обращения 01.03.2023 г.)

[8] Обзор практики Суда по интеллектуальным правам по вопросам, возникающим при применении норм Гражданского кодекса Российской Федерации о правовой охране программ для ЭВМ и баз данных // Журнал Суда по интеллектуальным правам. [Электронный ресурс]. URL: http://ipcmagazine.ru/official-cronicle/review-of-the-practice-of-the-intellectual-property-rights-court-on-issues-arising-from-the-application-of-the-norms-of-the-civil-code-of-the-russian-federation-on-the-legal-protection-of-computer-programs-and-databases (дата обращения 01.03.2023 г.)

образом, чтобы избежать осложнений.

Существующая система защиты авторских прав в сети «Интернет» справедливо нуждается в совершенствовании. В целях усиления защиты авторских и смежных прав следует сформировать целостную муниципальную и государственную политику, которая бы гарантировала действительную защиту прав и законных интересов равно как самих авторов, так и обычных пользователей. Основным направлением в данной области должно быть усовершенствование законодательства о защите авторских прав и практики его применения. Более того, для всесторонней правовой защиты программы для ЭВМ и её элементов представляется верным рассматривать в качестве объекта авторского права не только саму программу для ЭВМ, но и её отдельные составляющие. В свою очередь, дабы нивелировать упоминаемые в тексте работы проблемы, предлагается патентовать алгоритмы работы программы, но законодательство не указывает на такой способ защиты прав напрямую, так как в соответствии с ГК РФ программа для ЭВМ не является изобретением (ст. 1350 ГК РФ).

Список литературы

1. Адельшин Р. Н. Роль правовой инфраструктуры договорных отношений с участием потребителей в свете новеллизации объектов гражданских прав // Современные тенденции развития гражданского и гражданского процессуального законодательства и практики его применения. 2020. № 6. С. 8–16.

2. Алисова Е. В. Актуальные проблемы защиты авторского права в сети Internet // Наука, образование и культура. 2016. № 7 (10). С. 55–62.

3. Гришаев С. П. Интеллектуальная собственность: учебное пособие. М.: Юристъ, 2004. С. 288.

4. Маккланг К. Дж., Герриери Д. А., Маккланг К. А. Микрокомпьютеры для юристов. М.: Юридическая литература, 1988. С. 144.

5. Осипов М. Ю. Защита авторских прав в сети «Интернет»: основные особенности и проблемы // Актуальные проблемы российского права. 2018. № 12 (97). С. 116–122.

Alexander S. Kushnarev
Student of the Institute of the Prosecutor's Office,
Ural State Law University
named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
kushnarev-02@list.ru

Scientific Supervisor: Natalia S. Kalistratova,
Deputy Director of the Institute of Prosecutor's Office
Ural State Law University named after V. F. Yakovlev
(Ekaterinburg, Russian Federation)

kns003@usla.ru

ACTUAL PROBLEMS OF COPYRIGHT PROTECTION ON PROGRAM CODE AND INTERFACE ON INTERNET

Abstract. The problem of improvement of legislation in the sphere of copyright protection is one of the most urgent in Russia. It is conditioned by the fact that due to rapid development of information and communication technologies unscrupulous users have an opportunity to illegally obtain the code of a program or its interface.

Keywords: copyright, program code, program interface, IT-technologies, PC.

УДК 343.98

Олифиренко Артем Алексеевич
Студент
Саратовская государственная юридическая академия
(г. Саратов, Российская Федерация)
artol2002@mail.ru

Научный руководитель: Лавнов Михаил Александрович,
кандидат юридических наук,
доцент кафедры уголовного процесса
Саратовская государственная юридическая академия
(г. Саратов, Российская Федерация)
m-lavnov@rambler.ru

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ ПРОЦЕССЕ: ТЕОРЕТИЧЕСКИЙ АСПЕКТ

Аннотация. Настоящая научная работа посвящена актуальной проблеме использования электронных доказательств в уголовном процессе. В свете современного цифрового развития, вопрос эффективного использования электронных доказательств становится всё более важным. Однако в уголовно-процессуальном законодательстве РФ до сих пор отсутствуют чёткие регламенты по данному вопросу. В работе обсуждаются основные проблемы и сложности, связанные с внедрением электронных доказательств в уголовный процесс, а также влияние электронных доказательств на сам процесс и его участников. Исследование базируется на анализе зарубежного опыта, в частности, практики Европейского Союза. В заключение предлагаются пути и механизмы решения проблем внедрения электронных доказательств в УПК РФ, включая предложения по изменению законодательства, развитию технической инфраструктуры и обучению участников процесса.

Ключевые слова: электронные доказательства, цифровые технологии, Уголовно-процессуальный кодекс РФ.

Для цитирования:
Олифиренко А. А. Использование электронных доказательств в уголовном процессе: теоретический аспект // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 347–355.

Современное развитие информационных технологий привело к существенным изменениям во многих сферах жизни общества, включая юриспруденцию. Электронные доказательства, как элемент уголовного процесса, стали активно использоваться в

правоохранительной практике. В то же время, нормативное регулирование использования электронных доказательств в Уголовно-процессуальном кодексе Российской Федерации (УПК РФ) остаётся неопределённым и требует детального изучения и доработки. Именно поэтому данная тема является актуальной и важной для научного исследования.

Целью настоящей работы является анализ проблематики внедрения и использования электронных доказательств в уголовный процесс РФ и разработка предложений по совершенствованию нормативного регулирования данного вопроса.

Электронные доказательства представляют собой относительно новую категорию в уголовном процессе, поэтому их понятие и характеристики ещё не полностью закреплены в нормативно-правовых актах, прямое их определение в УПК отсутствует.

Тем не менее, исходя из общего понимания доказательства как информации, на основе которой устанавливаются наличие или отсутствие обстоятельств, предусмотренных уголовным законодательством (ст. 74 УПК РФ), можно предложить следующее определение: электронные доказательства – это информация в электронной форме, которая может быть использована для подтверждения или опровержения фактов, имеющих значение для уголовного дела[1].

В зарубежной научной литературе термин «электронные доказательства» также активно обсуждается. Одно из самых часто встречающихся определений: электронные доказательства – это любые данные, сохранённые или переданные в электронной форме, которые стороны могут представить в суд в качестве доказательства[2].

Среди основных характеристик электронных доказательств можно выделить следующие:

1. Форма представления. Электронные доказательства представлены в цифровой форме и хранятся на электронных носителях.

2. Мобильность. Благодаря цифровому формату, электронные доказательства легко передаваемы и доступны из различных точек мира.

3. Уязвимость. Электронные доказательства подвержены риску искажения, уничтожения или подделки.

4. Сложность идентификации источника. Из-за особенностей цифровой среды, идентификация источника электронных доказательств может быть затруднена.

Существует значительная необходимость в дальнейшем уточнении понятия и характеристик электронных доказательств, их классификации и стандартов

[1] Меркулова М. С., Калентьева Т. А. Электронные доказательства в уголовном процессе: проблемы допустимости // Международный журнал гуманитарных и естественных наук. 2022. № 5-3. С. 139–143. DOI 10.24412/2500-1000-2022-5-3-139-143.

[2] Morrissy J. D. Digital forensic evidence in the courtroom: Understanding content and quality // Northwestern Journal of Technology and Intellectual Property. 2014. № 12 (2). Pp. 121–128.

обработки в рамках уголовного процесса.

УПК РФ определяет доказательства в уголовном деле как любую информацию, которая помогает установить наличие или отсутствие обстоятельств, требующих доказывания в уголовном процессе, а также других обстоятельств, имеющих значение для уголовного дела. Кодекс включает в себя их полный список, в котором присутствует категория «иные документы». Однако, в ст. 81.1 УПК РФ упоминаются лишь электронные носители информации, которые признаются вещественными доказательствами и приобщаются к материалам уголовного дела по постановлению следователя. Электронные документы, включая электронные записи транзакций, контрактов, отчётов и других материалов, могут быть признаны вещественными доказательствами, если они относятся к делу и их подлинность подтверждена.

В юридическом сообществе существуют два противостоящих взгляда на необходимость включения концепции «электронное доказательство» в УПК РФ. Некоторые учёные утверждают, что такое включение необходимо, так как в его отсутствие теория и практика сталкиваются с множеством споров[3]. Этот взгляд, как кажется, связан с относительной новизной такого типа информации. Однако в условиях цифрового развития мирового общества и всё большей адаптации граждан и правоприменителей к электронной информации, текущие проблемы и недопонимания скоро должны исчезнуть.

Другие учёные, в свою очередь, считают, что такое включение не является обязательным. Они указывают на то, что использование электронных доказательств не вносит кардинальных изменений в процедуру и метод доказывания в уголовном процессе[4].

С точки зрения доктринального учения, электронные доказательства не привносят нового в классическую систему судебных доказательств. Основой этой системы является принцип, согласно которому судья оценивает любую информацию по своему внутреннему убеждению, независимо от формы и вида её представления. Хранимая электронно информация может быть представлена и воспринята в форме одного из традиционных видов доказательств, таких как вещественное доказательство или документ.

Однако данный вопрос необходимо рассматривать под «иным углом» – электронные доказательства это не электронные документы, а компьютерная информация, которую необходимо рассматривать как «иные документы» в ст. 74 УПК РФ, они включают в себя логи, метаданные, IP-

[3] Зигура Н. А, Кудрявцева А. В. Компьютерная информация как вид доказательства в уголовном процессе России: монография. Москва: Юрлитинформ, 2011. 173 с.

[4] Пастухов П. С. Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества: монография / под. ред. О. А. Зайцева. М.: Юрлитинформ, 2015. 347 с.

адреса, зафиксированные протоколы передачи данных (TCP, UDP и т. д.).

В этом контексте, при определении концепций «вещественное доказательство» и «иные документы» следует ясно указать, что электронные сведения могут быть представлены в обеих из этих форм. Например, электронная копия договора может быть рассмотрена как «иные документы», в то время как жёсткий диск, содержащий такую копию, может быть рассмотрен как «вещественное доказательство».

Взаимосвязь между электронными доказательствами и существующими категориями доказательств в уголовном процессе стоит рассматривать более детально.

Обращаясь к опыту других стран, отметим, что Европейский Союз (ЕС) в последнее десятилетие активно работает над унификацией подходов к использованию электронных доказательств в рамках уголовного судопроизводства.

Одним из ключевых документов, регулирующих данный вопрос, является регламент о Европейском ордере на сохранение и передачу электронных доказательств в рамках уголовных дел[5]. Этот регламент устанавливает процедуры для доступа правоохранительных органов к электронным доказательствам в рамках уголовного процесса.

Согласно регламенту, Европейский ордер на сохранение может быть выдан для обеспечения сохранения любых данных, которые хранятся в компьютерной системе и которые могут служить в качестве электронных доказательств. Данные могут быть сохранены в течение определённого периода времени до их передачи.

Европейский ордер на передачу может быть выдан для получения сохранённых данных. Принимающая сторона обязана передать сохранённые данные выдающей стороне не позднее, чем через 10 дней с даты получения ордера[6].

США являются одной из стран, которые активно применяют электронные доказательства в уголовном судопроизводстве, в связи с чем имеются несколько нормативно-правовых актов.

Федеральные правила уголовного судопроизводства предусматривают возможность использования электронных доказательств. В частности, они устанавливают правила относительно получения информации от электронных и коммуникационных систем[7].

Федеральные правила судебных доказательств содержат положения о

[5] Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders // Official Journal of the European Union L 303/1 [Electronic resource]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1805 (дата обращения: 12.05.2023).

[6] Бирюков П. Н. О цифровых доказательствах в зарубежном уголовном процессе // Вестник ВГУ. Серия: Право. 2022. № 1 (48). С. 275–286. DOI 10.17308/vsu.proc.law.2022.1/9043.

[7] Federal Rules of Criminal Procedure // Legal Information Institute [Electronic resuerce]. URL: https://www.law.cornell.edu/rules/frcrmp (дата обращения: 12.05.2023).

признании и применении электронных документов как доказательств при условии подтверждения их достоверности[8].

Более того, США внесли значительный вклад в развитие концепции «электронного открытия» (e-discovery), которая предполагает предоставление сторонами друг другу электронной информации, которая может служить доказательствами в суде[9]. Это позволяет использовать большое количество цифровых данных в качестве потенциальных доказательств.

В нашем государстве, согласно УПК РФ, доказательства должны быть истинными, относящимися к уголовному делу и допустимыми. В то же время, вопрос о допустимости электронных доказательств в уголовном процессе является предметом дискуссий в научной литературе. Электронные доказательства представляют собой информацию, сохранённую или переданную в цифровой форме, которая используется в уголовном судопроизводстве для подтверждения или опровержения обстоятельств, имеющих значение для уголовного дела. Это могут быть электронные документы, электронная переписка, информация из социальных сетей, аудио- и видеозаписи и другие данные.

Согласно зарубежному опыту, в частности, в США и странах ЕС, электронные доказательства признаются допустимыми, если они получены законным образом и их подлинность может быть подтверждена. При этом существуют специальные процедуры для сбора, сохранения и представления электронных доказательств в суде.

Основными критериями достоверности доказательств в уголовном процессе являются их релевантность, приемлемость и достоверность. Эти критерии применимы и к электронным доказательствам, однако они выступают в новом свете из-за особенностей этого вида доказательств.

Важной проблемой при оценке достоверности электронных доказательств является их уязвимость к манипуляциям. В отличие от традиционных доказательств, электронные доказательства легко поддаются изменению, удалению или подделке без видимых следов. В связи с этим, важно обеспечить их сохранность и целостность, а также прозрачность процесса их сбора и хранения. Это может включать в себя использование цифровых подписей, хэширования и других технологий защиты информации.

Так, в США в соответствии с Федеральными правилами уголовного судопроизводства, электронные доказательства должны быть приемлемыми и достоверными, чтобы быть допущенными к рассмотрению в суде.

С учётом международного опыта и доктрины уголовного процесса, можно предложить

[8] Federal Rules of Evidence // Legal Information Institute [Electronic resuerce]. URL: https://www.law.cornell.edu/rules/fre (дата обращения: 12.05.2023).

[9] Prater D. D., Capra D. J., Saltzburg S. A., Arguello H. Ch. M. Evidence: The Objection Method. Fifth Edition. Carolina Academic Press, LLC, 2016. 33 p.

следующие критерии достоверности электронных доказательств:

1. Авторство: Идентификация источника электронного доказательства. Это может включать в себя проверку подлинности электронной подписи, IP-адреса, учётных данных пользователя и т. д.

2. Целостность: Электронное доказательство не было изменено или повреждено после его получения. Технологии, такие как хеширование и блокчейн, могут использоваться для подтверждения целостности электронных данных.

3. Своевременность: Электронное доказательство было получено или создано в определённое время. Метаданные и цифровые свидетельства могут подтвердить временные метки и даты создания.

4. Доступность: Электронное доказательство может быть доступно для проверки и анализа судом и защитой. Это включает в себя возможность просмотра, копирования и анализа электронных данных.

5. Соответствие правилам: Сбор и использование электронного доказательства должны соответствовать принципам справедливости, законности и уважения к частной жизни. Это может включать в себя соблюдение процедур поиска и изъятия, а также согласие на доступ к частной информации.

Важно отметить, что эти критерии должны использоваться в сочетании и в соответствии с принципами оценки доказательств в каждой конкретной юрисдикции.

Для успешного внедрения электронных доказательств в уголовный процесс РФ необходима комплексная стратегия, включающая правовые, технологические и образовательные элементы.

1. Законодательные изменения: Необходимо внести изменения в УПК РФ, чтобы учесть особенности электронных доказательств.

2. Техническая инфраструктура: Необходимо создать техническую инфраструктуру для обработки и хранения электронных доказательств. Это включает специализированное оборудование, программное обеспечение и надёжные методы защиты информации.

3. Обучение и подготовка: Все участники уголовного процесса должны быть обучены основам работы с электронными доказательствами. Это включает обучение юридического персонала и судей основам информационных технологий, а также обучение IT-специалистов особенностям уголовного процесса.

4. Роль экспертов: Важной ролью в процессе использования электронных доказательств должны играть эксперты в области IT. Они могут помочь в оценке достоверности электронных доказательств и могут дать суду необходимые объяснения по техническим аспектам этих доказательств.

По итогам работы в УПК РФ можно внести следующие изменения:

1. В статье 74 УПК РФ после слов «любые документы» добавить слова «включая электронные документы и данные, хранящиеся в электронной форме».

2. После статьи 81.1 УПК РФ добавить новую статью 81.2 следующего содержания:

«Статья 81.2. Электронные доказательства

1. Электронными доказательствами признаются любые сведения, представленные в электронной форме и хранящиеся на электронных носителях информации, которые могут быть использованы для подтверждения или опровержения обстоятельств, подлежащих доказыванию в уголовном судопроизводстве.

2. Электронные доказательства должны удовлетворять критериям релевантности, допустимости, достоверности и своевременности. Оценка достоверности электронных доказательств производится с учётом их происхождения, целостности, непрерывности цепи управления данными и отсутствия признаков подделки или искажения.

3. При истребовании электронных доказательств следователь, прокурор, следственный орган, суд обязаны соблюдать законодательство о защите персональных данных и принципы международного сотрудничества в области обмена электронной информацией.

4. При работе с электронными доказательствами необходимо привлечение специалистов в области информационных технологий для гарантирования правильности сбора, сохранения, анализа и презентации таких доказательств».

Электронные доказательства становятся всё более актуальными в уголовном процессе в свете современных технологий. Они представляют собой информацию, сохранённую или переданную в электронной форме, которая может быть использована в суде для подтверждения или опровержения фактов, имеющих значение для дела.

Несмотря на растущую актуальность электронных доказательств, в уголовном процессе РФ до сих пор нет чёткого законодательного регулирования данного вопроса. Это создаёт ряд проблем, включая неопределённость в вопросе их использования и оценки достоверности.

Опыт зарубежных стран показывает, что для эффективного использования электронных доказательств необходима комплексная стратегия, включающая изменения в законодательстве, развитие технической инфраструктуры и обучение участников процесса.

Внедрение электронных доказательств в уголовный процесс может значительно повлиять на его ход и результаты, предоставляя новые возможности для сбора доказательств и ускоряя процесс судопроизводства.

Несмотря на вызовы, связанные с внедрением электронных доказательств, их использование является неизбежным в свете современного развития технологий. Поэтому важно начать работу по их интеграции в уголовный процесс в России как можно скорее, используя положительный опыт зарубежных стран.

Список литературы

1. Бирюков П. Н. О цифровых доказательствах в зарубежном уголовном процессе // Вестник ВГУ. Серия: Право. 2022. № 1 (48). С. 275–286. DOI 10.17308/vsu.proc.law.2022.1/9043.

2. Зигура Н. А, Кудрявцева А. В. Компьютерная информация как вид доказательства в уголовном процессе России: монография. Москва: Юрлитинформ, 2011. 173 с.

3. Меркулова М. С., Калентьева Т. А. Электронные доказательства в уголовном процессе: проблемы допустимости // Международный журнал гуманитарных и естественных наук. 2022. № 5-3. С. 139–143. DOI 10.24412/2500-1000-2022-5-3-139-143.

4. Пастухов П. С. Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества: монография / под. ред. О. А. Зайцева. М.: Юрлитинформ, 2015. 347 с.

5. Prater D. D., Capra D. J., Saltzburg S. A., Arguello H. Ch. M. Evidence: The Objection Method. Fifth Edition. Carolina Academic Press, LLC, 2016. 33 p.

6. Morrissy J. D. Digital forensic evidence in the courtroom: Understanding content and quality // Northwestern Journal of Technology and Intellectual Property. 2014. № 12 (2). Pp. 121–128.

Artem A. Olifirenko
Student
Saratov State Law Academy
(Saratov, Russian Federation)
panolifer@gmail.com

Scientific Supervisor: Mikhail A. Lavnov,
PhD in Law,
Associate Professor of the Department of Criminal Procedure
Saratov State Law Academy
(Saratov, Russian Federation)
m-lavnov@rambler.ru

USE OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: THEORETICAL ASPECT

Abstract. This scientific work is devoted to the actual problem of the use of electronic evidence in criminal proceedings. In the light of modern digital development, the issue of effective use of electronic evidence is becoming increasingly important. However, the criminal procedure legislation of the Russian Federation still lacks clear regulations on this issue. The paper discusses the main problems and difficulties associated with the introduction of electronic evidence in criminal proceedings, as well as the impact of electronic evidence on the process itself and its participants. The study is based on the analysis of foreign experience, in particular, the practice of the European Union. In conclusion, the ways and mechanisms of solving the problems of introducing

electronic evidence in the Criminal Procedure Code of the Russian Federation are proposed, including proposals for changing legislation, developing technical infrastructure and training participants in the process.

Keywords: electronic evidence, criminal procedure, digital technologies, legislation, Criminal Procedure Code of the Russian Federation.

УДК 347.7

Пащук Елена Олеговна
Студент,
Уральский государственный экономический университет
(Г. Екатеринбург, Российская Федерация)
elenaand807@gmail.com

Научный руководитель: Шалаумова Татьяна Владимировна
старший преподаватель кафедры гражданского права
Уральский государственный экономический университет
(Г. Екатеринбург, Российская Федерация)
gizn.67@mail.ru

ПРАВОВОЙ АСПЕКТ ИСПОЛЬЗОВАНИЯ НЕЙРОННЫХ СЕТЕЙ ДЛЯ БИЗНЕСА

Аннотация: В данной научной работе рассмотрен правовой аспект использования нейронных сетей в предпринимательской деятельности. Изучены проблемы правового характера при генерации нейросетями различных произведений. Рассмотрены варианты использования нейросетей в бизнесе. Предложены решения выявленных проблем. Проанализировано развитие нейронных сетей с целью автоматизации различных процессов в бизнесе.

Ключевые слова: цифровизация, предпринимательское право, гражданское право, нейронные сети, искусственный интеллект.

Для цитирования:
Пащук Е. О. Правовой аспект использования нейронных сетей для бизнеса // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 256–265.

Эпоха цифровых технологий открывает новые возможности для реализации различных проектов, продуктов и произведений. То, что раньше создавалось только посредством использования человеческих ресурсов сейчас легко и быстро исполнимо с помощью информационно-коммуникационных технологий. Именно современные технологии стали незаменимым компонентом жизни современного человека. В последнее время одним из самых передовых трендов являются нейронные сети или как принято их ещё называть нейросети.

Под нейросетью принято понимать математическую модель, работающую по принципам живого организма и способную к

самообучению[1]. Другими словами, нейросеть – это программа, работающая по принцам машинного обучения, используя при этом нейронные связи[2]. То, что раньше могло показаться нам кадрами из фантастического фильма, сейчас является обычным явлением. Создание различных музыкальных произведений, написание картин, раскрашивание изображений, создание прозы и стихотворений – всё это стало возможно получить в считанные секунды благодаря нейросети.

В настоящее время всё больше предпринимателей в целях реализации своих товаров и услуг прибегают к помощи нейронных сетей, так как они являются не только удобным, но и эффективным инструментом для развития бизнеса. Важно отметить, что на данном этапе развития информационно-коммуникационных технологий нейросеть не способна полностью заменить различных специалистов, например дизайнеров. Однако уже сейчас общедоступные генеративные нейросети помогают бизнесменам существенно сэкономить время и средства на создании изображений. Например, одна из российских дизайнерских компаний уже начала использовать данную технологию для создания уникальных логотипов[3].

Функции нейросети довольно обширны. Представляется возможным использование нейронных сетей для написания сценариев публикаций и видеороликов, а также в целях генерации контента[4]. Например, на это способна нейросеть Gerwin AI. Многие крупные компании уже внедрили нейронные сети в свой бизнес. Так сервис ДомКлик, который специализируется на недвижимости, активно использует их для оценки стоимости объектов недвижимости. Введение такой бизнес-идеи существенно сократило затраты компании на привлечение сторонних организаций. Помимо этого, именно нейросети могут помочь бизнесу существенно повысить уровень качества обслуживания клиентов, заранее прогнозируя их потребности.

В связи с этим необходимо отметить, что нейросети имеют существенное количество плюсов для предпринимателей. Можно выделить два основных положительных аспекта: сокращение затрат на производство и, как следствие, экономия материальных ресурсов предпринимателя, а также существенная экономия времени на выполнение различных функций.

Потенциал нейронных сетей является практически безграничным, и со временем он будет только

[1] Шмыгарева В. С. Разработка и обучение нейросетей // Молодой ученый. 2022. № 24 (419). С. 79–87.

[2] Гареева Г. А., Григорьева Д. Р., Гилязеев Т. В. Применение нейронных сетей в экономике // Молодой ученый. 2018. № 18 (204). С. 306–309.

[3] Матюшко М. «Студия Артемия Лебедева» рассказала о своей нейросети, которая генерирует логотипы для «экспресс-дизайна» // VC.ru [Электронный ресурс]. 2020, 26 июня. URL: https://vc.ru/design/137397-studiya-artemiya-lebedeva-rasskazala-o-svoey-neyroseti-kotoraya-generiruet-logotipy-dlya-ekspress-dizayna (дата обращения 23.05.2023).

[4] Подкладкин А. С., Пособилов Н. Е. Использование нейронных сетей глубокого обучения с целью формирования комментариев к видео // Труды НГТУ им. Р. Е. Алексеева. 2017. № 3 (118). С. 51–57.

увеличиваться[5]. Однако необходимо понимать, как именно устроена данная технология и на основании чего она способна генерировать новые объекты.

Одна из популярных нейросетей LEXICA, представляет собой галерею произведений искусства, созданных с помощью такой художественной модели как Stable Diffusion. Она может стать помощником для дизайнеров и других специалистов в сфере дизайна и искусства. Основной её функцией является создание, как утверждают её авторы, уникальных изображений[6]. Однако фрагменты сгенерированных картин можно найти в сети Интернет, так как они заимствованы с работ как художников с мировым именем, так и авторов известных лишь в узких кругах. При этом, истинные авторы произведений, лежащих в основе объекта, полученного с помощью нейросети, нигде не указаны и никак об этом не уведомляются.

В качестве другого, но очень схожего примера, можно привести нейросеть Gerwin AI. Она используется некоторыми предпринимателями в целях написания текстов для рекламных блогов и публикаций в социальных сетях, на видеохостингах, создания описаний товаров и услуг для различных объявлений. Отдельные части текста, либо полностью дублируют строки каких-либо авторов, либо просто переформулируют их. В связи с этим возникает ряд правовых проблем, связанных не только с использованием и распоряжением такого рода произведениями, но и с определением авторства на них.

Согласно ст. 1257 Гражданского кодекса Российской Федерации, автором является то лицо, творческим трудом которого создано произведение[7]. Важным признаком при этом выступает творческий характер, который отсутствует при создании работ нейросетью, так в их основе лежат множество произведений, созданных людьми. Также, согласно действующему законодательству Российской Федерации, нейросеть является объектом гражданского права, а не его субъектом, в связи с чем не может выступать в качестве автора сгенерированного произведения.

Изображение, текст или музыкальное произведение создаётся посредством использования нейросетью такого процесса, как компиляция, когда осуществляется сбор сотен или даже тысяч произведений, которые преобразовываются в одно. В соответствии с пп. 1 п. 2 ст. 1259 ГК РФ, к объектам авторских прав относятся производные произведения, то есть произведения, представляющие собой переработку другого

[5] Ладоша Е. Н., Коструб М. И. Искусственный интеллект: потенциал развития на пути создания нового цифрового искусства // Молодой ученый. 2022. № 48 (443). С. 1–4.

[6] Нейросеть Lexica: обзор нейросети рисующей по словам // Neuroseti.ru [Электронный ресурс]. 2023, 24 февраля. URL: https://neuroseti.ru/nejroset-lexica-risuyushchaya-po-slovam/ (дата обращения 23.05.2023).

[7] Гражданский кодекс Российской Федерации часть 4 от 18 декабря 2006 года № 230-ФЗ // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_64629/ (дата обращения: 24.05.2023).

произведения. Согласно пп. 9 п. 2 ст. 1270 ГК РФ, перевод или другая переработка произведений относится к использованию произведения. При этом использование произведения возможно только при наличии согласия автора и при заключении с ним определённого договора. В настоящее время также существуют позиции специалистов по рассмотрению в качестве авторов таких произведений либо самих разработчиков нейросети, либо компаний, которые используют такую нейросеть.

Определённые проблемы могут возникать и при использовании нейронных сетей в целях создания рекламы[8]. Так, рассматриваемая технология может брать за основу изображения известных персонажей, реальных людей или голоса популярных личностей. В этом случае предпринимателям, использующим нейронные сети в целях создания рекламного контента, необходимо получить согласие субъектов, чьи персональные данные будут использованы.

Важно отметить, что не во всех случаях при использовании какого-либо изображения авторское право будет нарушено, однако генерация нейронными сетями изображений может повлечь новые правовые риски.

Несмотря на то, что законодательство Российской Федерации достаточно полно регламентирует вопросы защиты прав авторов и устанавливает ответственность за их нарушение, в настоящее время существует ряд проблемных вопросов, препятствующих развитию нейронных сетей в бизнесе. Стоит отметить, что сама категория рассматриваемых систем является новой для отечественной нормативно-правовой базы, в связи с чем отсутствует законодательное закрепление понятия нейронных сетей.

В связи с вышеизложенными аспектами, представляется возможным внесение точечных поправок с целью решения данных проблем. Необходимо урегулирование правового статуса искусственного интеллекта, а именно определение его правовой природы и сущности, решение вопроса ответственности за действия, совершаемые искусственным интеллектом[9]. Пока нейронные сети берут за основу «творчества» и обучаются на чужих произведениях реальных авторов, использование результатов их деятельности в предпринимательской деятельности будет считаться не совсем правомерным. При этом, если с автором, чьи произведения использовала нейросеть, не было заключено специального договора, разработчиков нейросети или предпринимателя, если он знал об отсутствии таких соглашений с авторами, можно привлечь к ответственности.

[8] Букаева А. Р. Использование технологий нейронных сетей в современной видео рекламе на примере рекламного ролика сбербанка // Молодой исследователь Дона. 2021. №4 (31). С. 355–356.

[9] Ишутин А. В., Косаримов С. В., Чикирка Е. В. «Нейронное искусство» как объект авторского права // Социальные новации и социальные науки. 2021. № 1 (3). С. 133–144.

Подводя итог, важно отметить, что стремительное развитие цифровых технологий способствует не только появлению новых возможней для развития бизнеса, но и формированию новых вызовов, в том числе и для правового регулирования. При использовании нейронных сетей предпринимателям важно соблюдать как авторские права на произведения, сгенерированные нейросетью, так и нормы других отраслей права, например законодательства о защите персональных данных. Кроме того, важно, чтобы произведения, созданные нейронными сетями, не вводили в заблуждение потребителей, на которых направлено, например, описание того или иного товара. Предприниматели, которые будут соблюдать действующее законодательство и учитывать риски использования нейронных сетей, смогут быть конкурентоспособными на быстро меняющимся рынке. Стоит отметить, что развитие цифровых технологий всегда опережало, и будет опережать процесс их законодательного регулирования, однако именно право является тем инструментом, без которого невозможно дальнейшее социально-экономическое развитие общества и государства в целом.

Список литературы

1. Букаева А. Р. Использование технологий нейронных сетей в современной видео рекламе на примере рекламного ролика сбербанка // Молодой исследователь Дона. 2021. №4 (31). С. 355–356.
2. Гареева Г. А., Григорьева Д. Р., Гилязеев Т. В. Применение нейронных сетей в экономике // Молодой ученый. 2018. № 18 (204). С. 306–309.
3. Ишутин А. В., Косаримов С. В., Чикирка Е. В. «Нейронное искусство» как объект авторского права // Социальные новации и социальные науки. 2021. № 1 (3). С. 133–144.
4. Ладоша Е. Н., Коструб М. И. Искусственный интеллект: потенциал развития на пути создания нового цифрового искусства // Молодой ученый. 2022. № 48 (443). С. 1–4.
5. Подкладкин А. С., Пособилов Н. Е. Использование нейронных сетей глубокого обучения с целью формирования комментариев к видео // Труды НГТУ им. Р. Е. Алексеева. 2017. № 3 (118). С. 51–57.
6. Шмыгарева В. С. Разработка и обучение нейросетей // Молодой ученый. 2022. № 24 (419). С. 79–87.

Elena O. Paschuk
Student,
Ural State University of Economics
(Yekaterinburg, Russian Federation)
elenaand807@gmail.com

Scientific supervisor: Tatiana V. Shalamova

Senior Lecturer of the Department of Civil Law
Ural State University of Economics
(Yekaterinburg, Russian Federation)
gizn.67@mail.ru

LEGAL ASPECT OF USING NEURAL NETWORKS FOR BUSINESS

Abstract: In this scientific work, the legal aspect of the use of neural networks in business is considered. The problems of a legal nature in the generation of various works by neural networks are studied. The options for using neural networks in business are considered. Solutions to the identified problems are proposed. The development of neural networks in order to automate various business processes is analyzed.

Keywords: digitalization, business law, civil law, neural networks, artificial intelligence, legal regulation.

УДК 343.98

Полежаева Виктория Романовна
Слушатель факультета подготовки следователей
Санкт-Петербургская академия Следственного комитета
(г. Санкт-Петербург, Российская Федерация)
viktoria.polejaeva@yandex.ru

Научный руководитель: Кондаков Александр Владимирович,
кандидат юридических наук, доцент, заведующий кафедрой криминалистики,
судебно-экспертной и оперативно-розыскной деятельности,
Санкт-Петербургская академия Следственного комитета
(г. Санкт-Петербург, Российская Федерация)
kondakov.av@skspba.ru

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ СЛЕДОВАТЕЛЯМИ СЛЕДСТВЕННОГО КОМИТЕТА

Аннотация. В статье рассматриваются формы использования специальных знаний следственными органами Следственного комитета Российской Федерации. Особое внимание автор обращает на судебную экспертизу – наиболее распространённую форму использования специальных знаний в уголовном процессе. Рассмотрена деятельность Следственного комитета по расследованию преступлений с использованием цифровых технологий, предложено внедрить подготовку специалистов в области компьютерно-технической экспертизы на базе высших образовательных учреждений ведомства.

Ключевые слова: специальные знания, киберпреступления, судебная экспертиза, специалист, цифровые доказательства.

Для цитирования:
Полежаева В. Р. Использование специальных знаний при расследовании киберпреступлений следователями Следственного комитета // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 362–366.

В век развития компьютеризации и информационных технологий достаточно актуальным вопросом для следственных органов является применение специальных знаний при расследовании преступлений, совершаемых с применением электронной информации, информационных технологий, а также информационно-телекоммуникационной сети Интернет. Так, согласно статистическим данным: из числа киберпреступлений в первом полугодии 2021 года 212,8 тысячи совершены с использованием

Интернет-ресурсов, 103,7 тысячи – банковских карт, 21,8 тысячи – компьютерной техники[1]. Количество киберпреступлений в России в 2022 году увеличилось на 0,8 %, и стало составлять 522 065 тысяч преступлений[2], в перечень которых входят мошенничества через телефонные звонки, кардинг, фишинг и другие.

Специфика источников доказательственной информации обуславливает определённые трудности, возникающие при расследовании киберпреступлений. Следователю, в чьём производстве находится уголовное дело, приходится изымать, осматривать и приобщать в качестве вещественных доказательств огромный массив информации, содержащийся в электронных сообщениях, интернет-сообществах, сайтах, файлах на электронных устройствах. Для расследования этой группы преступлений от следователя требуется знание и применение не только законодательных норм, но и тактики производства отдельных следственных действий, специфики постановки вопросов при назначении судебной экспертизы, повышение квалификации в области внедрения усовершенствованных методов работы с цифровыми объектами с учётом современных достижений техники и науки. В образовательных учреждениях Следственного комитета на сегодняшний день существуют дополнительные профессиональные программы повышения квалификации действующих сотрудников ведомства, посвящённые расследованию преступлений в сфере информационных, телекоммуникационных и высоких технологий, реализация которых была начата в октябре 2021 года[3].

В связи со спецификой указанных нами ранее объектов, которые подлежат изъятию, осмотру и направлению на экспертное исследование, целесообразно вести разговор об использовании следователями возможностей специальных знаний при расследовании киберпреступлений. На протяжении уже многих лет одной из самых распространённых форм специальных знаний выступает судебная экспертиза. В июле 2020 года в Следственном комитете Российской Федерации был создан Судебно-экспертный центр, высокая квалификация и техническая

[1] Комитет Госдумы привёл данные статистики о киберпреступлениях // DiRUSSIA.RU. 2021, 17 ноября. [Электронный ресурс]. URL: https://d-russia.ru/komitet-gosdumy-privjol-dannye-statistiki-o-kiberprestuplenijah.html (дата обращения: 01.05.2023).

[2] Материалы к заседанию коллегии Следственного комитета Российской Федерации «Об итогах работы следственных органов Следственного комитета Российской Федерации за 2022 год и задачах на 2023 год» // Следственный комитет РФ [Электронный ресурс]. 2023, 3 марта. URL: https://sledcom.ru/press/events/item/1771051/ (дата обращения: 13.05.2023).

[3] Козлова Н. СК РФ начинает подготовку специалистов по расследованию киберпреступлений // Российская газета [Электронный ресурс]. 2021, 30 сентября. URL: https://rg.ru/2021/09/30/sk-rf-nachinaet-podgotovku-specialistov-po-rassledovaniiu-kiberprestupnosti.html (дата обращения: 07.05.2023).

оснащённость экспертов которого сегодня позволяют проводить уникальные компьютерно-технические исследования, информационно-аналитические экспертизы даже самых сложных объектов и получать результаты в самых сложных случаях. Сами эксперты Судебно-экспертного центра в этой области отмечают значительный рост указанных исследований, сложность работы с цифровыми следами, необходимость внимательного подхода к их изъятию и сохранению со стороны следователей[4]. Об особом внимании к киберпреступлениям со стороны Следственного комитета России свидетельствует создание в ведомстве в 2019 году **отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий, работа сотрудников которого** помогает оперативно раскрывать преступления в сфере информационных технологий, восстанавливать нарушенные права и законные интересы потерпевших, способствовать предупреждению их совершения.

Особое внимание следует уделить правильной формулировке вопросов, которые ставятся следователем на разрешение эксперта: необходимость избегать тех вопросов, которые могут быть решены и без проведения экспертного исследования, например, *«имеются ли на представленном электронном носителе файлы и каков их формат?»* Также необходимо отказаться от тех вопросов, которые носят правовой характер и по объективным причинам не могут быть решены экспертом, например, *«каким образом можно квалифицировать действия лица, совершённые с компьютерной программой, представленной на исследование?»*

Достаточно важной формой применения специальных знаний при расследовании преступлений в рассматриваемой нами сфере является привлечение к участию в следственных действиях сведущего лица, а именно специалиста. Следственные действия могут проводиться как с работающей, так и с неработающей техникой, например, при задержании подозреваемого лица с поличным можно проводить осмотр с работающий техникой, а с неработающей – уже непосредственно в момент фиксации доказательственной информации. В подавляющем большинстве случаев применение специальных познаний специалиста требуется при производстве осмотра места происшествия и иных видов осмотра. В 2022 году следователями Следственного комитета России расследовано свыше 15 500 преступных деяний, совершённых с применением компьютерных технологий, что составило на 29 % больше, чем в 2021 году. На основании изложенного следует констатировать, что успешное расследование киберпреступлений и преступлений в сфере высоких технологий во многом

[4] Интервью и. о. директора Судебно-экспертного центра СК России Андрея Маркова // Следственный комитет РФ [Электронный ресурс]. 2020, 20 июля. URL: https://sledcom.ru/press/interview/item/1485206/?print=1 (дата обращения: 12.05.2023).

обусловлено не только проведением качественного исследования объектов компьютерно-технической экспертизы, но и активным участием специалиста, обладающего специальными знаниями в указанной сфере при проведении различных следственных действий.

На сегодняшний день Следственный комитет Российской Федерации уделяет большое внимание расследованию, предупреждению киберпреступлений и преступлений в сфере высоких технологий. Одним из шагов в данном направлении можно считать создание в 2021 году на базе академий ведомства кафедр информационных технологий и организации расследования киберпреступлений.

Как справедливо отмечает Председатель Следственного комитета А. И. Бастрыкин: «Если для законопослушных граждан цифровизация – хороший инструмент для саморазвития, то злоумышленники используют научно-технический прогресс в целях личного незаконного заработка. И их жертвами становятся простые граждане, в том числе дети и пенсионеры. Именно поэтому создание специализированных кафедр обусловлено вызовом времени»[5].

Подводя итог, необходимо констатировать, что эффективности работы по расследованию преступлений рассматриваемой категории могло бы способствовать и осуществление подготовки на базе ведомственных академий Следственного комитета не только следователей, но и лиц, обладающих специальными познаниями в области компьютерно-технической экспертизы.

Victoria R. Polezhaeva
Trainee at the Faculty of Investigative Training
St. Petersburg Academy of the Investigative Committee
(Saint Petersburg, Russian Federation)
viktoria.polejaeva@yandex.ru

Scientific Supervisor: Alexander V. Kondakov,
PhD in Law, Associate Professor,
Head of Forensic Science, Forensic and Investigative Activity Department
St. Petersburg Academy of the Investigative Committee
kondakov.av@skspba.ru

USE OF SPECIAL KNOWLEDGE DURING CYBERCRIME INVESTIGATIONS BY INVESTIGATORS OF INVESTIGATORY COMMITTEE

[5] По поручению Председателя СК России на базе ведомственных академий создаются кафедры по организации расследования киберпреступлений // Следственный комитет Российской Федерации. [Электронный ресурс]. 2021, 30 сентября. URL: http://sledcom.ru/press/events/item/1614956/ (дата обращения: 07.05.2023).

Abstract. The article deals with forms of use of special knowledge by investigators of the Investigative Committee of the Russian Federation. The author focuses on forensic examination – the most common form of special knowledge application in criminal proceedings. It also considers activities of the Investigative Committee in investigating crimes using digital technologies and suggests training specialists in the field of computer forensics on the basis of higher educational institutions of the department.

Keywords: special knowledge, cybercrime, forensic examination, specialist, digital evidence.

УДК 343.98

Половинкина Ольга Дмитриевна
Студент Института прокуратуры,
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
olgapolovinkina24907@gmail.com

Научный руководитель: Рачева Нелли Витальевна
кандидат юридических наук, доцент,
доцент кафедры криминалистики
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
ekaterinburgg@mail.ru

ПРОБЛЕМА КРИМИНАЛИЗАЦИИ СОЦИАЛЬНЫХ СЕТЕЙ

Аннотация. В статье рассматривается социальная сеть, являющаяся не только местом проявления социальной активности, но и местом, где сосредотачивается значительный объём следов такой активности, в том числе и криминальной. Предлагается понятие социальной сети, раскрываемое в аспекте криминалистической науки, которое может быть использовано при разработке криминалистических методик по расследованию преступлений, совершаемых с помощью социальных сетей.

Ключевые слова: социальная сеть, киберпреступность.

Для цитирования:
Половинкина О. Д. Проблема криминализации социальных сетей // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 367–375.

В настоящее время, в период активной информатизации, всемирная сеть Интернет является неотъемлемой частью жизни как отдельного человека, так и всего общества в целом. Доступ к глобальной сети получило более 4,5 миллиардов человек со всего мира, в России это число достигает 116 миллионов человек. Необходимо отметить, что и в дальнейшем это число будет расти, ведь обусловлен такой рост активно развивающимися компьютерными технологиями, а также их всё более широкой доступностью.

Такое распространение сети Интернет в современной жизни не могло не спровоцировать появление принципиально новой формы взаимодействия между людьми. Так, использование результатов научно-технического прогресса для

объединения людей в новые формы социального взаимодействия привело к появлению такой интернет-платформы как социальная сеть. На сегодняшний день существует множество социальных сетей, наиболее популярными среди которых являются: Facebook (официально запрещена на территории Российской Федерации), ВКонтакте, Twitter, Одноклассники, YouTube, Мой Мир, WhatsApp, Viber, MySpace, Pinterest, Tik Tok, Instagram (официально запрещена на территории Российской Федерации) и многие другие. В частности, количество активных пользователей «ВКонтакте», одной из наиболее популярных социальных сетей в России, в 2023 году составляет 101.7 млн пользователей. Почти 54 % населения России используют ВКонтакте каждый месяц при том, что число сообщений в сутки на ресурсе превышает 10 млрд[1]. Безусловно, такие значения во многом отражают активное использование социальных сетей повсеместно.

Важно отметить, что само понятие «социальная сеть» появилось задолго до сети Интернет. Термин «социальная сеть» (ориг. «social field of this kind as a network») впервые был использован в 1954 г. в работе Джона Барнса «Классы и собрания в норвежском островном приходе»[2]. Данное определение «социальная сеть» включает в себя не только круг знакомых человека, но и взаимные социальные связи между ними. Соответственно, пользователь выступает не только в качестве потребителя приложения, но и как активный его участник, ведь социальная сеть как онлайн-платформа предназначена для общения и формирования социальных связей через списки друзей, подписчиков и т. д.

Социальная сеть как Интернет-ресурс может быть рассмотрена с самых различных аспектов, от философии до маркетинга, однако необходимо обратить внимание на следующее определение социальной сети как виртуализированной социальной среды, где человек занимается построением, расширением и углублением социальных связей, формируя тем самым специфическую структуру отношений, а также самореализуется, социализируется, генерирует и потребляет любую, интересующую его информацию[3]. Такой подход прежде всего позволяет акцентировать внимание на широком взаимодействии людей в социальных сетях, определить функциональное значение таковых, а также факторы, которые способны повлиять на распространенность социальных сетей, в том числе и для преступников.

В связи с этим особое внимание социальным сетям уделяется и в криминалистической науке. Ввиду того, что сеть Интернет не имеет

[1] Бегин А. Статистика ВКонтакте в 2023 году // Инклиент [Электронный ресурс]. 2023, 9 апреля. URL: https://inclient.ru/vk-stats/ (дата обращения: 15.05.2023).

[2] Barnes J. A. Class and committees in a Norwegian island parish // Hum. Relat. 1954. Vol. 7. Pp. 39–54.

[3] Безбогова М. С. Социальные сети как фактор формирования социальных установок современной молодежи: автореферат дис. ... канд. психолог. наук. Москва, 2017. 25 с.

определённого информационного центра, позволяющего контролировать потоки информации, открываются весьма обширные перспективы для преступной деятельности, благодаря чему и происходит активное использование новейших технологий сетевой коммуникации для совершения преступлений. Важно отметить, что преступность в сети Интернет не может быть ограничена исключительно преступлениями в сфере компьютерной информации. В настоящий момент широкий перечень деяний, включающих экстремизм, мошенничество, оборот порнографических материалов, доведение до самоубийства, склонение к употреблению наркотических веществ, клевету, вымогательство и т. п. могут совершаться путём использования социальных сетей через сеть Интернет[4].

Проблемы криминализации социальных сетей в Интернет-пространстве связаны с предоставлением злоумышленникам широких возможностей для совершения преступлений при минимальных затратах, ведь необходимыми в такой ситуации являются лишь компьютерное устройство, программное обеспечение и возможность выхода в сеть. Более того, постоянная автоматизация работы с программным обеспечением снижает требование к наличию тех или иных специальных знаний, необходимых для совершения преступлений с использованием социальных сетей. Еще одним фактором является возможность действовать в условиях использования выдуманных имен, псевдонимов (так называемые «аккаунты-фейки»), то есть «под прикрытием» своей реальной личности, выдавая себя за иное лицо. В таком случае социальные сети выступают в качестве удобного средства совершения преступлений.

Интернет-пространство создаёт новую сферу для человеческой интеракции, отличающееся нетипичным доверием к самой информации и непосредственно лицам, действующим в сети[5]. Проблемой в новых условиях становится то, что Интернет-пространство человеком на подсознательном уровне не воспринимается как источник опасности, оно нематериально, а соответственно, по мнению многих, и не может нанести прямой вред. Такое чувство «ложной безопасности» предоставляет преступнику широчайшие возможности для подготовки, совершения и сокрытия преступлений, совершаемых с использованием социальных сетей.

В случае поступления информации о совершённом преступлении осмотр места происшествия традиционно приобретает основополагающее значение как наиболее важное следственное действие, проводимое на первоначальном этапе расследования. Качество осмотра и его полнота во

[4] Григорьев А. Н., Серых А. Б., Маханек А. Б. Некоторые проблемы раскрытия и расследования преступлений, связанных с распространением детской порнографии в сети интернет // Право и практика. 2017. № 1. С. 37–43.

[5] Гладышев В. В. Социальные сети как инструмент для пропаганды экстремизма // Обзор.НЦПТИ. 2013. № 2. С. 28–31.

многом влияют на качество расследования. Однако ситуация существенно меняется, если преступление, совершаемое в форме действия, реализуется в виртуальном пространстве социальной сети, поскольку определение фактического места совершения преступления представляется довольно сложным.

В криминалистической науке достаточно распространённым является подход, где под местом совершения преступления понимается как помещение или территория, где происходило противоправное деяние, так и место, где были обнаружены связанные с преступным деянием вредные последствия[6]. Такой подход, тем не менее, не учитывает проблему определения фактического места совершения преступления с использованием социальной сети, так называемой «распределительной инстанцией», главной задачей функционирования которой должен стать контроль информационных потоков сети Интернет. В связи с широкой рассредоточенностью современных социальных сетей представляется весьма сложным определить место преступления в информационном пространстве, где было совершено противозаконное деяние с использованием социальной сети. Местом преступления может являться часть информационного пространства (домен, сайт), в котором было совершено преступление активным пользователем. Здесь необходимо учитывать два фактора: фактическое место преступления (сайт, который зарегистрирован на сервере, имеющем фактическое местоположение на определённой территории) и лицо, являющееся активным пользователем сети Интернет в момент совершения преступления. Такой подход поможет облегчить идентификацию преступника, поскольку современные методы не дают высокой точности по отдельности, а предлагаемая формулировка позволяет правоохранительным органам применять их в совокупности[7].

Дуализм виртуальной социальной сети, выступающей «одновременно и средством связи, и уникальной социальной средой»[8], приводит к тому, что социальная сеть становится в том числе «местом», где лицо осуществляет социальную активность и, соответственно, оставляет следы своего пребывания. В связи с этим возникает необходимость расширения традиционного подхода к определению места совершения преступления, куда представляется целесообразным включать и виртуальное пространство, в том числе социальных сетей[9], где будет находиться интересующая следствие

[6] Неупокоева Л. С., Кочерова Л. А., Шеховцова Л. С. Осмотр места происшествия как информационная основа расследования преступления // Закон и право. 2018. № 6. С.136–139.

[7] Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально экономические явления и процессы. 2017. № 12. С. 200.

[8] Тихонова С. В. Социальные сети: проблемы социализации Интернета. // Полис. Политические исследования. 2016. № 3. С. 138–152.

[9] Болвачев М. А. К вопросу о понятии места совершения преступления в пространстве

информация и с чего целесообразно начинать процесс расследования преступлений, совершаемых с использованием социальных сетей.

Социальная сеть может быть рассмотрена и в качестве части нового пространства социальной деятельности человека. Именно в ней, как отмечалось ранее, из всего пространства всемирной сети эта активность проявляется в полной мере, следовательно, она будет содержать следы такой активности, в частности: фотографии, видеозаписи, аудиозаписи, голосовые сообщения, видеосообщения и др.

В криминалистической науке такие следы исследуются в качестве цифровых, актуальной задачей при работе с которыми является уточнение порядка работы с ними в процессе собирания доказательств. К работе со следами криминалисты, как правило, относят их обнаружение, фиксацию, изъятие и исследование. Применительно к цифровым следам особую значимость приобретают также вопросы их хранения и копирования.

По мнению Д. В. Бахтеева и Е. В. Смахтина, в ходе производства любого следственного действия лицо, его производящее, должно отчётливо представлять, с какой разновидностью цифровых следов оно столкнулось. Соответственно, одним из основных вопросов, требующих научного обсуждения и решения, является вопрос о сущности и классификации цифровых следов.

Цифровые следы как форма существования электронной информации могут быть классифицированы по различным основаниям. Так, в зависимости от характера происхождения они дифференцируются на оставленные человеком непосредственно (электронные документы, записи в социальных сетях и т. п.) и опосредованно (данные телеметрии, файлы регистрации, атрибуты создаваемых файлов и т. п.). Следы первой группы могут быть исследованы в ходе производства следственных действий (например, в ходе осмотра места происшествия), исследование же следов второй группы требует использования специальных знаний (как правило, производства компьютерно-технических исследований).

Следует учитывать, что доказывание связи цифровых следов с конкретным лицом всегда зависит от типа технического устройства и в некоторых случаях может быть осложнено. Так, подозреваемый может заявить, что доступ к его персональному компьютеру имела группа людей; им также может быть выдвинута версия о том, что его учётная запись в социальной сети была взломана третьими лицами и т. д.[10]

Так, приговором Вологодского областного суда от 17.11.2016 г. Анферьев И. М. был признан

социальных сетей // Уголовно-процессуальные и криминалистические чтения на Алтае. 2018. Вып. 15. С. 39–43.

[10] Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. 2019. № 6 (129). С. 61–68.

виновным в совершении преступлений, предусмотренных ч. 1 ст. 137, ч. 1 ст. 138, ч. 1 ст. 272 УК РФ за распространение фотографий интимного характера лица без его согласия, совершённое с использованием социальной сети «ВКонтакте» путём получения несанкционированного доступа к аккаунту потерпевшей, что, в частности, подтверждалось такими доказательствами как протоколы осмотра предметов, согласно которым объектами осмотра являлись аккаунты пользователей данной социальной сети, в ходе чего устанавливались факты осуществления переписок со страниц таких пользователей, которые, по своей сути, и являлись следами совершения данного преступления. Более того, по данному делу следами явились и фотографии, размещённые преступником на странице в социальной сети «Вконтакте», на которых была изображена потерпевшая в обнажённом виде, что подтверждается протоколом обыска, проведённого в квартире Анферьева И. М. посредством которого был изъят, в том числе, ноутбук, в ходе осмотра которого и были обнаружены фотографии потерпевшей[11].

Соответственно, в качестве следов совершения преступления с использованием социальной сети могут выступать не только фотографии, видеозаписи, аудиозаписи, голосовые сообщения, видеосообщения и др., но и переписки, звонки, отдельные сообщения, удалённые сообщения (применительно к отдельным социальным сетям, например, WhatsApp, они также оставляют следы), время последнего посещения социальной сети (в случае, если оно не скрыто пользователем) и т. д. Однако следует отметить, что далеко не всегда указанные следы остаются, поскольку, как правило, злоумышленники предпринимают все меры к удалению подобной информации, её сокрытию и уничтожению, что порождает определённые трудности в обнаружении следов совершения преступлений с использованием социальных сетей.

Особенностью социальной сети является также и самостоятельное её наполнение контентом самими пользователями, то есть аккаунт в социальной сети выступает отражением личности человека в виртуальном пространстве, соответственно, он приобретает именно личный характер: информация в виде фотографий, аудиозаписей, видеозаписей, текста или других формах и комбинациях будет отражать индивидуальные особенности самого пользователя, что в значительной степени отличает социальную сеть от других Интернет-платформ.

В связи с этим в рамках криминалистического исследования под социальной сетью следует понимать единое цифровое средство и место человеческой деятельности (в том числе преступной) в глобальной сети Интернет, где и с помощью чего

[11] Приговор Вологодского областного суда по уголовному делу № 1-914/2016 по обвинению Анферьева И. М. по ч. 1 ст. 137 УК РФ. // Справочная система «СудАкт» [Электронный ресурс]. URL: https://sudact.ru/regular/doc/hwzIJ69MfXmR/ (дата обращения: 10.05.2023).

лицо формирует взаимоотношения с другими пользователями, общается, а также создаёт и/или использует различного рода информацию. При этом социальная сеть, как и любая другая среда человеческой деятельности, обладает способностью хранить в себе информацию о человеке, его следы, которые вполне могут быть использованы в целях противодействия преступности.

Введение понятия социальной сети в криминалистическую науку имеет фундаментальное значение для разработки криминалистических методик, направленных на противодействие преступности в виртуальной сфере, поскольку специфика социальной сети как элемента глобальной сети Интернет позволяет выделить её среди остальных составляющих.

Отдельно необходимо отметить значение социальной сети как источника ориентирующей информации: в зависимости от наполнения аккаунта можно получить сведения: о местоположении лица (по геопозиции фотографий); определить маршруты перемещений (по соотнесению времени и места фотографий); определить интересы, предрасположенности, социальные связи; текущее эмоциональное состояние (по статусу, текстовым, аудио- или видеосообщениям); место работы или учёбы; другой информации, нашедшей отражение в профиле сети. Кроме того, источником информации могут выступать и другие профили, где имела место публикация материалов, связанных с интересующим лицом или событием[12].

Вместе с тем, важно также учитывать, что поведение личности в социальной сети отличается стремлением показать себя с лучшей стороны, предстать в наиболее выгодном свете перед окружающими, обратить их внимание именно на те стороны и качества, которые человек считает или хочет считать своими достоинствами, что требует особого подхода к верификации полученной информации и устранению ложных сведений.

Таким образом, на основании изложенного представляется, что с информатизацией общества социальные сети стали неотъемлемой частью его жизнедеятельности. Характерные особенности социальных сетей привели к их выделению среди остальных Интернет-платформ, а также поразительным темпам роста аудитории пользователей. Такое их проникновение в повседневную и профессиональную жизнь человека и общества привело к закономерной криминализации социальных сетей, что связано с виртуализацией определённой доли человеческой деятельности. Социальная сеть стала выступать в качестве нового пространства человеческого взаимодействия, в том числе и преступного. В связи с этим, для решения задач криминалистики на современном этапе развития общества необходима разработка методик расследования преступлений, совершаемых в социальных сетях.

[12] Болвачев М. А. Использование социальных сетей при расследовании преступлений экстремистской направленности: дисс. … канд. юрид. наук. Калининград, 2022. 206 с.

Список литературы

1. Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. 2019. № 6 (129). С. 61–68.

2. Безбогова М. С. Социальные сети как фактор формирования социальных установок современной молодежи: автореферат дис. ... канд. психолог. наук. Москва, 2017. 25 с.

3. Болвачев М. А. Использование социальных сетей при расследовании преступлений экстремистской направленности: дисс. … канд. юорид. наук. Калининград, 2022. 206 с.

4. Болвачев М. А. К вопросу о понятии места совершения преступления в пространстве социальных сетей // Уголовно-процессуальные и криминалистические чтения на Алтае. 2018. Вып. 15. С. 39–43.

5. Гладышев В. В. Социальные сети как инструмент для пропаганды экстремизма // Обзор.НЦПТИ. 2013. № 2. С. 28–31.

6. Григорьев А. Н., Серых А. Б., Маханек А. Б. Некоторые проблемы раскрытия и расследования преступлений, связанных с распространением детской порнографии в сети интернет // Право и практика. 2017. № 1. С. 37–43.

7. Неупокоева Л. С., Кочерова Л. А., Шехцова Л. С. Осмотр места происшествия как информационная основа расследования преступления // Закон и право. 2018. № 6. С.136–139.

8. Тихонова С. В. Социальные сети: проблемы социализации Интернета. // Полис. Политические исследования. 2016. № 3. С. 138–152.

9. Чернышов В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств // Социально экономические явления и процессы. 2017. № 12. С. 199–203.

10. Barnes J. A. Class and committees in a Norwegian island parish // Hum. Relat. 1954. Vol. 7. Pp. 39–54.

Olga D. Polovinkina
Student at the Institute of Public Prosecutor's Office,
Ural State Law University
named after V.F. Yakovlev
(Yekaterinburg, Russian Federation)
olgapolovinkina24907@gmail.com

Scientific Supervisor: Nelly V. Racheva
PhD in Law, Associate Professor,
Associate Professor at the Depertvent of Criminalistics
Ural State Law University
named after V.F. Yakovlev
(Ekaterinburg, Russian Federation)

ekaterinburgg@mail.ru

THE PROBLEM OF CRIMINALIZATION OF SOCIAL NETWORKS

Abstract. The article deals with social network, which is not only a place of social activity, but also a place where significant volume of traces of such activity is concentrated, including criminal ones. In the article we propose the concept of social network, disclosed in the aspect of criminology, which can be used in developing criminological techniques to investigate crimes committed with the help of social networks.

Keywords: social network, cybercrime.

УДК 343.985

Проскурина Дарья Александровна
Студент
Юго-Западный государственный университет
(г. Курск, Российская Федерация)
darya.proskurina@rambler.ru

Научный руководитель: Ряполова Ярослава Петровна
кандидат юридических наук, доцент,
доцент кафедры уголовного процесса и криминалистики
Юго-Западный государственный университет
(г. Курск, Российская Федерация)
yarosslava@mail.ru

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОИЗВОДСТВА ДОПРОСА С ИСПОЛЬЗОВАНИЕМ ВИДЕО-КОНФЕРЕНЦ-СВЯЗИ

Аннотация. В статье рассматриваются дискуссионные вопросы, связанные с производством допроса с использованием видео-конференц-связи. Автор исследует теоретические и прикладные проблемы при производстве допроса в дистанционном формате, рассматривает основания для выбора рассматриваемой формы допроса, круг возможных участников данного следственного действия, обеспечение присутствия защитника (адвоката), определяет перспективы применения дистанционных технологий на этапе проверки сообщений о преступлении.

Ключевые слова: допрос, видео-конференц-связь, следственное действие, предварительное расследование, участники допроса.

Для цитирования:
Проскурина Д. А. Актуальные проблемы производства допроса с использованием видео-конференц-связи // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 376–381.

В 2020 году, когда началась пандемия коронавируса, практически все сферы жизнедеятельности перешли на дистанционные технологии. Не осталась без внимания и сфера уголовного судопроизводства. Так, 30 декабря 2021 г. был принят Федеральный закон № 501-ФЗ, в соответствии с которым были внесены изменения в УПК РФ, определяющие порядок проведения допроса, очной ставки и опознания посредством видео-конференц-связи (далее – ВКС) на стадии предварительного расследования. Хотим заметить, что запрос со стороны научного сообщества и практических

работников[1] на введение дистанционного формата производства следственных действий существовал довольно продолжительное время, при этом до конца 2021 г. использование систем ВКС являлось прерогативой только суда в ходе судебного следствия.

Под видео-конференц-связью подразумевается технология, позволяющая одновременно передавать видео и звук между двумя и более субъектами посредством аппаратно-программных средств коммуникации[2].

Долгое время возможность применения средств ВКС у правоохранительных органов на стадии предварительного расследования полностью отсутствовала. Эта ситуация была обусловлена и тем, что расследование уголовного дела представляет собой длительный трудоёмкий процесс с вовлечением большого количества участников, обладающих разным процессуальным статусом. Как правило, обеспечить соблюдение прав и законных интересов каждого из них при производстве следственных действий в дистанционном режиме не всегда возможно, что, безусловно, можно считать недостатком использования дистанционных технологий[3]. Однако применение систем ВКС в ходе досудебного производства, в том числе при проведении отдельных следственных действий, помогает не только улучшить качество получаемого при этом доказательства, но и сократить сроки проведения предварительного расследования, что приводит к повышению эффективности расследования[4]; призвано сэкономить финансовые средства, которые тратятся в настоящее время на возмещение процессуальных издержек отдельным участникам уголовного процесса, что в данном случае выступает положительным моментом; может способствовать большей откровенности лиц, опасающихся посткриминального воздействия[5]. Также в числе плюсов выделяют обеспечение безопасности свидетелей, которые испытывают давление со стороны других участников уголовного процесса, а также сокращение финансовых затрат на производство следственных действий. Данное положение понятно: государству, например, не придётся

[1] Овчинникова О. В. Перспективы применения видеоконференцсвязи при производстве дознания // Вестник Уральского юридического института МВД России. 2019. №. 1. С. 28.

[2] Казакова А. А. Возможности применения видеоконференцсвязи в уголовном процессе // Сибирские уголовно-процессуальные и криминалистические чтения. 2019. № 3. С. 48.

[3] Киселева К. А., Зыков Д. А. Актуальные вопросы использования видеоконференцсвязи при производстве допроса // StudNet. 2022. № 4. С. 2790.

[4] Толмачев О. В. О некоторых проблемных вопросах организации взаимодействия следователя и органа дознания при проведении следственных действий путем использования систем видео-конференц-связи //Академическая мысль. 2023. №. 1 (22). С. 114.

[5] Новиков С. А. Допрос с использованием систем видеоконференц-связи: завтрашний день российского предварительного расследования // Российский следователь. 2014. №. 1. С. 3.

оплачивать командировку следователю.

При этом вопрос допустимости результатов проводимых следственных действий с использованием ВКС по праву признается дискуссионным и проблемным в некоторых аспектах.

Прежде всего, актуальной проблемой видится техническое оснащение органов следствия и дознания видео-конференц-связью. Не во всех регионах и не на всех уровнях имеет место оснащение высокоскоростным Интернетом и аппаратурой, очевидно, в связи с дороговизной данной технологии. Помещения для ВКС должны располагать сертифицированным по международным стандартам техническим оснащением, т. е. аудио- и видеооборудованием, телекоммуникационными сетями, позволяющими передавать видеоинформацию в режиме реального времени. Техническим средствам, используемым для ВКС, надлежит обеспечивать необходимое качество изображения и звука, а также информационную безопасность.

Поскольку все соединения возможны исключительно через ведомственную связь и с использованием специальных каналов и аппаратуры, сам процесс проведения и подключения является затратным и трудоёмким. Более того, некоторые отдалённые местности либо вовсе не имеют связи, либо связь ненадлежащего для проведения допросов качества. В связи с чем постоянные обрывы, плохая слышимость и иные сопутствующие технические сбои не способствуют качеству проведения того или иного следственного действия, что напрямую влияет на перспективы включения полученных результатов в доказательственную базу уголовного дела. Как видится, решение указанной проблемы возможно путём закладывания достаточного бюджета на техническое оснащение органов предварительного расследования, штатную укомплектованность органов расследования техническими исполнителями и специалистами.

В законодательстве нечётко обозначены пути решения технических проблем, при которых нет возможности продолжать проведение допроса в дистанционном формате (перерыв, завершение или перенос следственного действия), если в видео-конференц-связи нет нормального звука и изображения по аналогии с возможными проблемами, которые имеют место в ходе судебного производства[6]. Считаем необходимым закрепить порядок действий дознавателя и следователя в таком случае, а также конкретные требования к видео-конференц-связи.

Ещё один проблемный аспект нового формата допроса связан с перечнем участников уголовного судопроизводства, с которыми возможно провести допрос по ВКС. Буквальное толкование нормы закона позволяет правоприменителю делать вывод о возможности проведения

[6] Пономаренко Ю. Н. Особенности проведения допроса, очной ставки, опознания путем использования систем видео-конференц-связи: актуальные проблемы и пути их решения // Вестник науки. 2022. № 6. С. 260.

таких следственных действий в отношении потерпевшего, свидетеля, подозреваемого, обвиняемого, специалиста, эксперта. Исследователи справедливо опасаются перспективы утраты психологического контакта между следователем и допрашиваемым лицом, столь необходимого для получения всей интересующей следствие информации, особенно в условиях жесткого противодействия со стороны защиты[7]. Поймать на лжи, убедить сознаться под неопровержимым грузом собранных доказательств, использовать тактические приёмы – все это может быть нивелировано несовершенством технических возможностей, помехами, нестойким соединением Интернета[8].

Кроме того, пристального внимания со стороны законодателя требует вопрос обеспечения участия защитника в ходе проводимого следственного действия в дистанционной формате. На наш взгляд, учитывая процессуальную роль защитника, он должен быть приглашён дознавателем, органом дознания или следователем по месту нахождения обвиняемого (подозреваемого), аналогично – в отношении адвоката свидетеля.

Стоит также указать на то, что законодатель предусмотрел широкие дискреционные полномочия следователя при определении оснований для производства допроса в дистанционном формате, закрепляя оборот «при необходимости», что повлекло активное обсуждение среди исследователей предложений о распространении этих правил на широкий спектр следственных ситуаций, в том числе и не связанных с невозможностью проведения следственных действий в обычном порядке[9].

Также стоит ожидать в будущем, что возможность дистанционного допроса будет распространена и на стадию возбуждения уголовного дела при получении объяснений, что также во многом упростило порядок рассмотрения сообщений о преступлениях в рамках доследственой проверки[10].

Подводя итог вышесказанному, хотим отметить, что производство допроса с использованием дистанционных технологий могло бы оптимизировать процесс расследования уголовного дела при условии соблюдении прав и законных интересов участников производства. Вместе с тем рассмотренные вопросы,

[7] Росовская Е. В. Влияние использования видео-конференц-связи при допросе свидетеля на достоверность его показаний // Вестник Волгоградской академии МВД России. 2022. №. 4 (63). С. 60.

[8] Ушаков А. Ю., Кирянина И. А. О введенной в уголовно-процессуальный закон норме, позволяющей проводить отдельные следственные действия посредством дистанционных ресурсов // Вестник Белгородского юридического института МВД России. 2023. №. 1. С. 58.

[9] Афанасьева С. И., Добровлянина О. В. Правовое регулирование производства следственных действий с использованием видео-конференц-связи по действующему УПК РФ // Ex jure. 2022. №. 4. С. 112.

[10] Рябинина Т. К., Ряполова Я. П. Сохранение стадии возбуждения уголовного процесса: новые аргументы в старой дискуссии // В сборнике: Уголовный процесс: от прошлого к будущему. Материалы Международной научно-практической конференции. 2014. С. 274.

возникающие в правоприменительной деятельности в связи с реализацией новых правил, требуют дальнейшего теоретического осмысления и надлежащей законодательной регламентации.

Список литературы

1. Афанасьева С. И., Добровлянина О. В. Правовое регулирование производства следственных действий с использованием видео-конференц-связи по действующему УПК РФ // Ex jure. 2022. №. 4. С. 101–117.

2. Казакова А. А. Возможности применения видеоконференцсвязи в уголовном процессе // Сибирские уголовно-процессуальные и криминалистические чтения. 2019. №3. С. 48–53.

3. Киселева К. А., Зыков Д. А. Актуальные вопросы использования видеоконференцсвязи при производстве допроса // StudNet. 2022. №4. С. 2789–2796.

4. Новиков С. А. Допрос с использованием систем видеоконференц-связи: завтрашний день российского предварительного расследования // Российский следователь. 2014. №. 1. С. 2–6.

5. Овчинникова О. В. Перспективы применения видеоконференцсвязи при производстве дознания // Вестник Уральского юридического института МВД России. 2019. №. 1. С. 28–31.

6. Пономаренко Ю. Н. Особенности проведения допроса, очной ставки, опознания путем использования систем видео-конференц-связи: актуальные проблемы и пути их решения // Вестник науки. 2022. №6. С. 257–263.

7. Росовская Е. В. Влияние использования видео-конференц-связи при допросе свидетеля на достоверность его показаний // Вестник Волгоградской академии МВД России. 2022. №. 4 (63). С. 59–64.

8. Рябинина Т. К., Ряполова Я. П. Сохранение стадии возбуждения уголовного процесса: новые аргументы в старой дискуссии // В сборнике: Уголовный процесс: от прошлого к будущему. Материалы Международной научно-практической конференции. 2014. С. 273–278.

9. Ряполова Я. П., Рябинина Т. К. Уголовно-процессуальное доказывание в стадии возбуждения уголовного дела: анализ научных воззрений // Известия Юго-Западного государственного университета. Серия: История и право. 2012. № 1–1. С. 160–164.

10. Толмачев О. В. О некоторых проблемных вопросах организации взаимодействия следователя и органа дознания при проведении следственных действий путем использования систем видео-конференц-связи //Академическая мысль. 2023. №. 1 (22). С. 113–115.

11. Ушаков А. Ю., Кирянина И. А. О введенной в уголовно-процессуальный закон норме, позволяющей проводить отдельные следственные действия

посредством дистанционных ресурсов // Вестник Белгородского юридического института МВД России. 2023. №. 1. С. 57–62.

Daria A. Proskurina
Student
Southwestern State University
(Kursk, Russian Federation)
darya.proskurina@rambler.ru

Scientific Supervisor: Ryapolova Yaroslava Petrovna
PhD in Law, Associate Professor,
Associate Professor of Criminal Procedure and Criminalistics Department
South-Western State University
(Kursk, Russian Federation)
yarosslava@mail.ru

CURRENT PROBLEMS OF INTERROGATION USING VIDEO CONFERENCE COMMUNICATION

Abstract. The article discusses debatable issues related to the production of interrogation using videoconferencing, the author explores theoretical and applied problems in the production of interrogation in a remote format, considers the grounds for choosing the considered form of interrogation, the circle of possible participants in this investigative action, ensuring the presence defender (lawyer), determines the prospects for the use of remote technologies at the stage of checking reports of a crime.

Keywords: interrogation, videoconferencing, investigative action, preliminary investigation, participant, problem, technologies, court.

УДК 343.2/.7

Ремнева Татьяна Александровна
Магистрант
Поволжский институт управления – филиал РАНХиГС
(г. Саратов, Российская Федерация)
RemnevaTA@yandex.ru

Научный руководитель: Чурикова Анна Юрьевна
кандидат юридических наук, доцент,
доцент кафедры административного и уголовного права
Поволжского института управления – филиал РАНХиГС
(г. Саратов, Российская Федерация)
a_tschurikova@bk.ru

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ ПРИ ПОМОЩИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В статье рассмотрена проблема использования информационных технологий для совершения преступлений. Автором проанализирована статистика преступлений, совершённых в сфере информационной безопасности, а также способы противодействия таким преступлениям. На основе анализа сложившейся ситуации выявлена необходимость изменения ряда нормативных документов, а также создания механизма обмена информацией правоохранительных органов с банковскими учреждениями, операторами связи и другими учреждениями.

Ключевые слова: информационные технологии, информационные преступления, механизм обмена информацией, защита от киберпреступлений.

Для цитирования:
Ремнева Т. А. Противодействие преступлениям, совершаемым при помощи информационных технологий // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 382–387.

Стремительное развитие технологий современного мира не только предоставляет много возможностей, но и порождает ряд проблем. Стремительное развитие цифровизации с одной стороны способствует развитию общества и государства, с другой же позволяет преступникам использовать более современные и совершенные методы совершения преступлений.

Согласно статистике, ежегодно количество преступлений, совершаемых с использование информационных технологий только растёт. Эти преступления не только направлены против собственности и материального благосостояния

граждан и организаций, но и всё чаще стали затрагивать конституционные права и свободы человека. При совершении данного вида преступлений злоумышленники в первую очередь преследуют именно корыстные мотивы, используя для обогащения информационно-телекоммуникационные сети, компьютерную информацию и электронные (цифровые) технологии. Также целью злоумышленников могут стать дискредитация граждан и организаций, распространение в сети запрещённой законом информации, поддержание и продвижение идей терроризма и экстремизма. Сильный рост числа преступлений, совершаемых с использованием информационных технологий, произошёл по причине перехода на дистанционный формат в период 2020–2021 гг., и сейчас это является глобальной тенденцией. Согласно статистике, каждое четвёртое преступление, совершаемое в России, затрагивает именно информационную безопасность[1].

Для таких преступлений в Уголовном кодексе Российской Федерации (далее УК РФ) выделена отдельная глава – Глава 28. Преступления в сфере компьютерной информации[2]. Но стоит отметить, что перечень преступных деяний, совершаемых с использованием информационных технологий, только ей не ограничивается. Так, например, ст. 159.6. УК РФ (мошенничество в сфере компьютерной информации) также рассматривает экономическое преступление, совершённое с использованием информационных технологий.

Согласно статистике Судебного департамента при Верховном Суде Российской Федерации в 2021 г. число осуждённых по статьям главы 28 УК РФ составило 225 человек, тогда как в 2020 году их было 137, в 2019 – 165. Самое большое количество осуждённых привлечены по ч. 3 ст. 272 УК РФ, т. е. неправомерный доступ к охраняемой законом компьютерной информации[3].

Очевидно, что необходимо постоянно искать и совершенствовать способы противодействия данным видам преступлений. Анализируя имеющиеся проблемы, связанные с выявлением и пресечением подобных преступлений, а также необходимостью предотвращения их совершения, учёные и практики предлагают различные варианты решения. Например, в своей статье А. В. Бойкова, опираясь на мнения экспертов, предлагает следующие способы борьбы с информационными преступлениями:

[1] Статистика Судебного департамента при Верховном суде Российской Федерации // Судебный департамент при Верховном суде Российской Федерации [Электронный ресурс] URL: http://www.cdep.ru/index.php?id=5&item=35 (дата обращения 12.03.2023).

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2022) // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 10.03.2023).

[3] Статистика Судебного департамента при Верховном суде Российской Федерации // Судебный департамент при Верховном суде Российской Федерации [Электронный ресурс]. URL: http://www.cdep.ru/index.php?id=5&item=35 (дата обращения 12.03.2023).

– пользоваться менеджером паролей;

– обязательно использовать программное обеспечение, защищающее от вредоносных программ;

– скрывать IP-адрес и создавать безопасное онлайн-соединение с помощью использования VPN;

– регулярно обновлять используемое в организации программное обеспечение;

– повышать информационную грамотность в отношении используемых цифровых источников, к которым можно отнести электронную почту и текстовые сообщения;

– не передавать свои персональные данные или данные других сотрудников третьим лицам, придерживаясь правила нулевого доверия[4].

С одной стороны, эти меры позволят обезопасить себя от преступлений, совершаемых с использованием информационных технологий. Но, с другой стороны, данные меры способны помочь лишь при противодействии очень узкому кругу угроз. Посредством указанных средств можно обезопасить свой персональный компьютер, сеть компьютеров в организации, но не стоит забывать, что не только мошенничество или похищение информации является целью преступлений. С помощью информационных ресурсов могут совершаться и такие преступления как публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2 УК РФ); незаконные организация и проведение азартных игр (ст. 171.2 УК РФ). От этих преступлений данные меры не будут эффективны.

К тому же предлагаемые А. В. Бойковой способы фактически можно отнести к мерам профилактики, а не противодействия. Аналогично и некоторые другие авторы в большей степени акцентируют внимание исключительно на профилактических мероприятиях. Так, П. Н. Кобец указывает, что основными субъектами противодействия данному виду преступлений могли бы выступать СМИ и общество[5]. Но не по всем видам преступлений, совершаемых с использованием информационных технологий, достаточно повышения информированности населения.

Для выработки эффективных мер противодействия обозначенным видам преступлений, на наш взгляд, необходимо, в первую очередь, определиться с механизмом их совершения и субъектами. Например, А. Ю. Чурикова в своей работе

[4] Бойкова А. В. Анализ преступлений с использованием информационных технологий и мер противодействиям им // Индустриальная экономика. 2021. Т. 12. №. 5. С. 1160.

[5] Кобец П. Н. Причины, условия и особенности предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий в современном цифровом пространстве // Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XIII Международной научно-практической конференции, Москва, 15 августа 2022 года., Москва: Печатный цех, 2022. С. 565.

предлагает делить все преступления, совершаемые с использованием информационных технологий, на две обобщённые группы: те, для совершения которых требуется наличие специальных знаний в области информационных технологий, и те, совершение которых не требует наличия специальных познаний. И уже в зависимости от группы А. Ю. Чурикова предлагает разделять способы противодействия преступлениям, совершаемым с использованием информационных технологий[6].

Действительно, с целью профилактики и противодействия киберпреступлениям, для совершения которых фактически не требуется специальных познаний в IT-сфере, подойдут предлагаемые многими учёными меры профилактического характера и работы с населением. В связи с этим, можно отдельно отметить предлагаемый А. Ю. Чуриковой риск-ориентированный подход в организации работы прокуроров и органов расследования[7]. В настоящее время правоохранительные органы перегружены работой и не могут полноценно заниматься эффективной профилактикой преступлений. Распределение усилий с учётом риск-ориентированного подхода, позволило бы им высвободить необходимое для организации профилактической работы время.

На наш взгляд, чтобы противодействовать преступлениям, совершаемым с использованием информационных технологий, требуется провести комплекс мер не только в законодательной сфере, но и в технической области. МВД России давно настаивает на создании новой системы взаимодействия и обмена информацией между правоохранительными органами, банками и операторами связи. Для создания этой системы необходимо изменить существующее законодательство, регулирующее данную сферу деятельности, а также создать специализированное подразделение в правоохранительных органах, которое будет за это отвечать. Данное изменение позволит получать необходимую в ходе расследования информацию в режиме реального времени.

Следует также отметить, что за рубежом давно существует такая система, способствуя повышению оперативности раскрытия дел, а также предотвращению новых преступлений. Ведь не стоит забывать, что целью деятельности правоохранительных органов является не только выявление уже совершенных преступлений и привлечение к ответственности за их совершение, но и предупреждение

[6] Чурикова А. Ю. Противодействие киберпреступности: роль прокурора (уголовно-процессуальный аспект) // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXIV международной научно-практической конференции, Красноярск, 08–09 апреля 2021 года. Том Часть 1. Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2021. С. 210.

[7] Чурикова, А. Ю. Риск-ориентированный подход в уголовно-процессуальной деятельности прокурора // Законность. 2022. № 8 (1054). С. 49.

совершения новых преступлений. Существующая система сотрудничества органов МВД, банковских учреждений и операторов связи не отличается особой оперативностью. Каждый запрос очень долго обрабатывается, что в свою очередь усложняет ведение уголовных дел.

Таким образом, можно сказать, что стремительное развитие информационных технологий стало основой для появления и развития нового вида совершения преступлений. Преступники очень быстро подстраиваются и используют в своих целях результаты научно-технического прогресса. Это становится серьёзной угрозой не только для граждан, но и для всех сфер деятельности государства, которые функционируют в информационном поле. Это происходит из-за того, что на данном этапе развития киберпространство и общество уже неотделимы. В связи с этим, предложение правоохранительных органов о создании объединенной базы будет способствовать повышению информационной безопасности. Данная система позволит банкам и мобильным операторам проводить системную работу по профилактике и пресечению потенциальных преступлений[8], а также позволит органам МВД более оперативно реагировать на преступления и ускорит их раскрываемость.

Список литературы

1. Бойкова А. В. Анализ преступлений с использованием информационных технологий и мер противодействиям им // Индустриальная экономика. 2021. Т. 12. №. 5. С. 1158–1161.

2. Кобец П. Н. Причины, условия и особенности предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий в современном цифровом пространстве // Актуальные проблемы науки и образования в условиях современных вызовов: Сборник материалов XIII Международной научно-практической конференции, Москва, 15 августа 2022 года., Москва: Печатный цех, 2022. С. 560–566.

3. Чурикова А. Ю. Противодействие киберпреступности: роль прокурора (уголовно-процессуальный аспект) // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXIV международной научно-практической конференции, Красноярск, 08–09 апреля 2021 года. Том Часть 1. Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2021. С. 209–211. DOI 10.51980/2021_1_209.

4. Чурикова А. Ю. Риск-ориентированный подход в уголовно-процессуальной деятельности прокурора // Законность. 2022. № 8 (1054). С. 48–50.

[8] Киберпреступность 2022: отчет МВД. // TelecomTimes [Электронный ресурс]. 2022, 7 апреля. URL: https://telecomtimes.ru/2022/04/kiber-2022/ (Дата обращения 14.04.2023)

Tatiana A. Remneva
Master's student.
Volga Region Institute of Management – Branch of Russian Academy of National Economy and Public Administration
(Saratov, Russian Federation)
RemnevaTA@yandex.ru

Scientific Supervisor: Anna Y. Churikova
PhD in Law, Associate Professor,
Associate Professor at the Department of Administrative and Criminal Law
Volga Region Institute of Management – Branch of Russian Academy of National Economy and Public Administration
(Saratov, Russian Federation)
a_tschurikova@bk.ru

COUNTERACTION TO CRIMES COMMITTED WITH THE HELP OF INFORMATION TECHNOLOGIES

Abstract. The paper deals with the problem of using information technologies for committing crimes. The author analyses statistics of crimes committed in the field of information security, as well as ways to counteract such crimes. On the basis of the analysis of this situation the necessity of changes in a number of normative documents, and also creation of the mechanism of information exchange of law enforcement bodies with banking institutions, communication operators and other establishments has been revealed.

Keywords: information technologies, information crimes, information exchange mechanism, criminal law, criminal procedure, cybercrime protection.

УДК 343.13

Савченко Пётр Сергеевич
Студент
Поволжский институт управления – филиал РАНХиГС
(г. Саратов, Российская Федерация)
gangstervegas3000@gmail.com

Шамсетдинов Дамир Данилович
Студент
Поволжский институт управления – филиал РАНХиГС
(г. Саратов, Российская Федерация)
damir.shamsietdinov98855@mail.ru

Научный руководитель: Чурикова Анна Юрьевна
кандидат юридических наук, доцент,
доцент кафедры административного и уголовного права
Поволжский институт управления – филиал РАНХиГС
(г. Саратов, Российская Федерация)
a_tschurikova@bk.ru

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТЫ

Аннотация. В статье анализируются вопросы расследования преступлений, связанных с использованием криптовалюты. Обозначены существенные проблемы расследования криптовалютных преступлений: отсутствие полноценного нормативного регулирования и недостаточная цифровая грамотность следователей. Предлагаются меры для улучшения работы правоохранительных органов по расследованию криптовалютных преступлений.

Ключевые слова: криптовалюта, криптовалютные преступления, расследование криптовалютных преступлений.

Для цитирования:
Савченко П. С., Шамсетдинов Д. Д. Особенности расследования преступлений, совершаемых с использованием криптовалюты // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 388–393.

В современном мире криптовалюта стала новым объектом пристального внимания со стороны преступников. Это обусловлено развитием интернет-технологий, которые позволяют обходить законы и спрятаться за анонимностью криптовалютных транзакций. Вместе с тем, рост популярности криптовалюты

вызвал необходимость расследования преступлений в этой сфере.

Сам по себе термин «криптовалюта» хотя и является повсеместно употребляемым, в том числе и в научной литературе, но не имеет нормативного закрепления и полноценного регулирования. В связи с этим, вопрос понятия криптовалюты относится к дискуссионным. Например, П. Л. Мащенко, М. О. Пилипенко предлагают понимать под криптовалютой «разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах»[1]. В свою очередь М. А. Егорова и Л. Г. Ефимова обращают внимание на то, что данный термин является многоаспектным и можно предложить несколько определений криптовалюты (техническое, экономическое и правовое)[2].

Понятие виртуальных денег также дано в отчёте группы разработки финансовых мер по борьбе с отмыванием денег (ФАТФ). Согласно данному отчёту, виртуальная валюта – это средство выражения стоимости, которым можно торговать в цифровой форме и которое функционирует в качестве средства обмена, и/или расчётной денежной единицы, и/или средства хранения стоимости, но не обладает статусом законного платёжного средства ни в одной юрисдикции[3]. Данное понятие можно расценивать как очень широкое и обобщённое, что также, на наш взгляд, не способствует внесению ясности в определение криптовалюты.

Проблема с нормативным регулированием понятия криптовалюты не была решена и принятием Федерального закона от 31 июля 2020 г. № 259-ФЗ[4]. Хотя данный закон и закрепляет понятие цифровой валюты, но оно подвергается существенной критике как среди учёных, так и среди практиков[5].

Кроме того, одной из главных проблем расследования криптовалютных преступлений является отсутствие регулирования и прозрачности этой сферы. Криптовалюты не подчиняются традиционным правилам банковской системы, и их использование не всегда связано с фактическими транзакциями или услугами. Это делает их использование в качестве инструмента обмана или отмывания денег ещё более привлекательным для преступников.

Понятие криптовалютных преступлений также нормативно не закреплено. Фактически с

[1] Мащенко П. Л., Пилипенко М. О. Технология Блокчейн и ее практическое применение // Наука, техника, образование. Олимп, 2017. № 32. С. 61.

[2] Егорова М. А., Ефимова Л. Г. Понятие криптовалют в контексте совершенствования российского законодательства // Lex Russica. 2019. №7 (152). С. 133

[3] Отчёт ФАТФ Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ июнь 2014 г. / FATF/OECD; АНО «МУМЦФМ», 2014. 28 с.

[4] Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ (последняя редакция) // Российская газета. 2020. № 173 (8227).

[5] Молостова В. Е. Анализ понятия цифровых прав в России // Символ науки. 2022. №. 6-1. С. 53–58.

использованием криптовалюты может быть совершён широкий спектр преступных деяний, в котором криптовалюта может выступать как объектом, так и способом совершения преступления (мошенничеств, отмывания денежных средств, краж, грабежей, разбоев, финансирования террористических и экстремистских организаций и т. д.). Это вызывает потребность в урегулировании вопросов, связанных с использованием криптовалюты в преступной деятельности.

Например, в Пленуме Верховного суда отдельно был рассмотрен вопрос об отмывании доходов с помощью криптовалют. Согласно Постановлению Пленума ВС РФ предметом преступлений, предусмотренных ст. 174 и 174.1 Уголовного кодекса Российской Федерации, также следует считать денежные средства, преобразованные из виртуальных активов (криптовалюты), которые получены в результате преступной деятельности[6].

Следующей заслуживающей внимания проблемой расследования криптовалютных преступлений является сложность их отслеживания. Криптовалюту можно хранить на компьютерах и устройствах, доступных только их владельцам, и использовать их для перевода денег в любой точке мира, обратившись к услугам интернет-бирж и кошельков. Из-за этого сбор и анализ информации о транзакциях может быть затруднён.

Э. Х. Недысева обоснованно указывает на тот факт, что для расследования преступлений, связанных с криптовалютой, необходимо обладать специальными познаниями, понимать – что это такое, порядок хранения, использования и оборота данной валюты[7].

Расследование криптовалютных преступлений требует новых знаний и навыков от сотрудников правоохранительных органов. Это связано с тем, что для раскрытия таких преступлений необходимо понимать технические особенности блокчейна и использования специализированного программного обеспечения для анализа криптовалютных транзакций. Недостаточная цифровая грамотность сотрудников правоохранительных органов, как указывает в своём исследовании А. Ю. Чурикова, является одной из ключевых проблем цифровизации уголовного судопроизводства[8], что в целом негативно сказывается на расследовании всех преступлений, связанных с цифровыми технологиями. На наш взгляд, для эффективного расследования преступлений, совершаемых с

[6] Постановление Пленума Верховного Суда РФ от 26 февраля 2019 г. № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» // Российская газета. 2019. № 51.

[7] Надысева Э. Х. Проблемы расследования преступлений в сфере оборота криптовалют // Вестник экономической безопасности. 2019. № 3. С. 225

[8] Чурикова А. Ю. Проблемы цифровизации российского уголовного процесса // Вестник Саратовской государственной юридической академии. 2021. № 6 (143). С. 214

использованием криптовалюты, недостаточно просто привлечь специалиста, необходимо также, чтобы следователь сам понимал, с чем он имеет дело. В связи с этим предлагаем ввести для следователей обязательное прохождение курсов повышения квалификации в данной области, где им подробно объяснялось бы, что такое криптовалюта и какие существуют механизмы работы с ней.

Кроме того, отсутствие достаточного уровня информированности сотрудников правоохранительных органов о криптовалюте влечёт, зачастую, нарушения действующего законодательства, прав и законных интересов граждан и организаций. Например, незаконные отказы в возбуждении уголовных дел по заявлениям о хищениях криптовалюты, основанные лишь на отсутствии полноценного нормативного регулирования понятия такой валюты[9]. В связи с этим, полагаем обоснованным предложение по внедрению модели деятельности прокурора, ориентированной на профилактику нарушений в сфере уголовного судопроизводства[10], так как это позволит более эффективно организовать деятельность правоохранительных органов по борьбе с преступлениями, совершаемыми с использованием криптовалюты.

При всём указанном выше для успешного расследования преступлений, связанных с криптовалютой, правоохранительным органам необходимо придерживаться следующей последовательности дейтсвий:

1) Сбор данных о транзакциях. Очень важно установить, какие транзакции были совершены, когда и куда они направлялись. Использование специализированных программ и аналитических инструментов для сбора данных может помочь установить достаточный объём информации для успешного расследования.

2) Анализ данных. Правоохранительным органам необходимо определить, какие данные являются важными и какие нужны для проведения дальнейшего расследования.

3) Изучение связей между различными транзакциями. Это может помочь правоохранительным органам выявить связь между различными субъектами и раскрыть организованную группу преступников.

4) Сотрудничество с криптобиржами. Криптобиржи могут помочь правоохранительным органам выявить идентичность владельца кошелька, через который были произведены незаконные операции, а также предоставить иную полезную

[9] Крицына А. Криптовалюта как предмет преступления. Проблемы уголовно-правовой защиты прав собственности на криптовалюту // ЭЖ-Юрист. 2022. № 05 (1206). [Электронный ресурс] URL: https://www.eg-online.ru/article/450687/ (дата обращения: 03.05.2023).

[10] Чурикова А. Ю. Модель деятельности прокурора, ориентированная на профилактику нарушений уголовно-процессуального законодательства // Вестник Саратовской государственной юридической академии. 2020. № 4 (135). С. 130–133

информацию для успешного расследования.

5) Международное сотрудничество. Криптовалюты не имеют границ, что означает, что они могут использоваться для совершения преступлений в любой стране. Правоохранительные органы должны сотрудничать с международными коллегами, чтобы раскрыть преступления, совершённые с использованием криптовалюты в других странах.

В целом, расследование криптовалютных преступлений представляет собой сложную задачу, требующую совместных усилий представителей правоохранительных органов, специалистов по криптографии и соответствующих экспертов. Успех расследования преступлений, связанных с криптовалютой, зависит от того, насколько правоохранительные органы могут собрать и проанализировать информацию, а также обобщить результаты, полученные во время расследования для раскрытия преступления. Тем не менее, отсутствие эффективных мер регулирования и контроля в этой сфере может привести к усилению криптовалютной преступности и опасностей, связанных с её использованием.

Список литературы

1. Егорова М. А., Ефимова Л. Г. Понятие криптовалют в контексте совершенствования российского законодательства // Lex Russica. 2019. № 7 (152). С. 130–140

2. Крицына А. Криптовалюта как предмет преступления. Проблемы уголовно-правовой защиты прав собственности на криптовалюту // ЭЖ-Юрист. 2022. № 05 (1206). [Электронный ресурс]. URL: https://www.eg-online.ru/article/450687/ (дата обращения: 03.05.2023).

3. Мащенко П. Л., Пилипенко М. О. Технология Блокчейн и ее практическое применение // Наука, техника, образование. Олимп, 2017. № 32. С. 61–64.

4. Молостова В. Е. Анализ понятия цифровых прав в России // Символ науки. 2022. №. 6-1. С. 53–58.

5. Надысева Э. Х. Проблемы расследования преступлений в сфере оборота криптовалют // Вестник экономической безопасности. 2019. № 3. С. 223–227. DOI 10.24411/2414-3995-2019-10167.

6. Чурикова А. Ю. Проблемы цифровизации российского уголовного процесса // Вестник Саратовской государственной юридической академии. 2021. № 6 (143). С. 209–216. DOI 10.24412/2227-7315-2021-6-209-216.

7. Чурикова А. Ю. Модель деятельности прокурора, ориентированная на профилактику нарушений уголовно-процессуального законодательства // Вестник Саратовской государственной юридической академии. 2020. № 4 (135). С. 128–134. DOI 10.24411/2227-7315-2020-10109.

Petr S. Savchenko,
Student
Volga Institute of Management – Branch of Russian Presidential Academy of National Economy and Public Administration
(Saratov, Russian Federation)

Damir D. Shamsetdinov
Student
Volga Institute of Management – Branch of Russian Presidential Academy of National Economy and Public Administration
(Saratov, Russian Federation)
damir.shamsietdinov98855@mail.ru

Scientific Supervisor: Anna Y. Churikova
PhD in Law, Associate Professor,
Associate Professor at the Department of Administrative and Criminal Law
Volga Institute of Management – Branch of Russian Academy of National Economy and Public Administration
(Saratov, Russian Federation)
a_tschurikova@bk.ru

SPECIFICS OF THE INVESTIGATION OF OFFENCES INVOLVING CRYPTOCURRENCIES

Abstract. The article analyses the issues of investigation of crimes involving the use of cryptocurrency. Significant problems in the investigation of cryptocurrency crimes are highlighted: lack of full-fledged regulatory framework and insufficient digital literacy of investigators. Measures to improve the work of law enforcement agencies to investigate cryptocurrency crimes are proposed.

Keywords: cryptocurrency, cryptocurrency crimes, law enforcement agencies, crime investigation, transaction, crime.

УДК 343.98

Сапожникова Елизавета Сергеевна
Студент,
Национальный исследовательский
Нижегородский государственный университет
имени Н. И. Лобачевского
(г. Нижний Новгород, Россия)
heyelizabeth13@gmail.com

Научный руководитель: Полякова Анастасия Васильевна
старший преподаватель кафедры судебной экспертизы,
Национальный исследовательский
Нижегородский государственный университет
имени Н. И. Лобачевского
(г. Нижний Новгород, Россия)
anastasia.poliakova811@yandex.ru

СУДЕБНО-ПОРТРЕТНАЯ ИДЕНТИФИКАЦИЯ ЧЕЛОВЕКА ПО ПРИЗНАКАМ ПОХОДКИ

Аннотация. Статья посвящена наиболее эффективным методам современной идентификации человека по признакам походки, которые изучены автором посредством сравнительного метода исследования. Особое внимание уделено возможностям использования искусственного интеллекта и нейронных сетей для решения указанной задачи, а также рассмотрены конкретные разработки, направленные на идентификацию человека по признакам походки.

Ключевые слова: идентификация по признакам походки, временные и пространственные характеристики, нейронные сети, искусственный интеллект, программа распознавания.

Для цитирования:
Сапожникова Е. С. Судебно-портретная идентификация человека по признакам походки // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 394–398.

Идентификация человека по разнообразным признакам является одним из самых востребованных направлений в современной криминалистической науке. Исходя из исследований статистических данных, в период с 01.01.2022 г. по 24.11.2022 г. количество нераскрытых преступлений достигло отметки

700207[1], что несомненно повышает возможность возникновения рецидивов, так как преступники не были привлечены к юридической ответственности. Данные факты свидетельствуют о недостаточной эффективности привычных способов идентификации личности, таких как: исследование внешнего облика человека по статическим признакам, составление «словесного портрета» и т. д. Судебно-портретная идентификация человека по походке позволит расширить возможности поиска преступника за счёт использования информации о его функционально-динамических свойствах. Однако всё ещё существует ограниченное количество методов идентификации, каждый из которых представляет собой уникальный способ достижения поставленной задачи. Исходя из этого, авторы поставили перед собой задачу определить наиболее эффективный способ идентификации человека по признакам походки.

В настоящее время широко применимо компьютерное исследование признаков походки человека, которое может быть осуществимо контактным и бесконтактным методом. Первый представляет собой использование определённых устройств, которые при соприкосновении с двигательной частью человека считывают отдельные особенности походки, постановку и функционирование стопы, устойчивость положения человека и т. д.

Однако подробнее мы рассмотрим именно бесконтактный метод исследования, который представляет собой систему отслеживания признаков походки по видеоизображениям и является более распространённым и доступным для изучения. Так, один из методов с помощью комплекса определённых показателей составляет единую картину функционирования опорно-двигательного аппарата человека, что позволяет выделить характерные особенности походки, необходимые при сравнительном анализе исследования видеозаписей. Судебная экспертиза видеозаписей с целью идентификации личности включает анализ общей модели движения и кинематики суставов, временных и пространственных характеристик движения, анализ статических или динамических поз, анализ антропометрических показателей. Временные характеристики отображаются посредством исследования так называемого цикла шага, то есть времени от начала контакта ноги с опорой до следующего аналогичного контакта этой же ноги. Цикл состоит из семи стадий, в которых выделяются периоды опоры и переноса. В совокупности, исследование данного цикла шага, длительности различных его стадий, позволяет изучить фазы подъёма, падения, передачи, ускорения, продвижения и торможения, что является индивидуальными особенностями, слабозаметными при визуальном восприятии видеозаписи.

[1] Краткая характеристика состояния преступности в Российской Федерации // МВД России [Электронный ресурс]. URL: https://мвд.рф/reports/item/28021552/ (дата обращения: 10.02.2023).

Пространственные характеристики содержат в себе такие показатели, как: длина правого и левого шага и угол разворота стоп. Для исследования и сопоставления данных показателей, необходимо проводить видеозапись с различных ракурсов и точек съемки, для определения масштаба в кадре должен присутствовать предмет, с приблизительно известными размерными характеристиками. Не менее важными при исследовании являются кинематические характеристики движений в суставах. Подлежат изучению голеностопный, коленный и тазобедренный суставы. Особое внимание уделяется сгибательным и разгибательным движениям, общей подвижности суставов, данные характеристики при сравнительном анализе позволяют идентифицировать человека по походке, отображённой на видеозаписи. Также, существуют иные характеристики, которые в совокупности с описанными выше, устанавливают полноценную, детальную картину состояния походки идентифицируемого человека[2]. По нашему мнению, данный метод в совокупности различных показателей и характеристик представляется эффективным, однако при наличии различных факторов, данные по одному или нескольким показателем могут быть искажены, из-за чего полученный результат будет сильно отличаться от истины.

Далее, рассмотрим нейросетевые подходы, которые базируются на характеристиках, описанных нами выше. Также важно, при аналитике данного метода рассмотреть еще одну важную характеристику, называемую оптическим потоком, который представляет собой векторное поле видимого движения точек сцены. По мере использования данных этой характеристики, при обработке видеоматериала, программа не учитывает цвет, контрастность, яркость исследуемых фрагментов. Это необходимо для того, чтобы отвлекающие факторы, которые могут так или иначе изменять походку либо движение человека, такие как одежда и освещение, не позволяли искажать результаты исследования. Одним из источников обучения сетей являются бинарные маски силуэтов. При данном подходе сверточная архитектура обучается по отдельным силуэтам предсказывать человека, которому этот силуэт принадлежит. В дальнейшей работе сеть используется для извлечения необходимых идентификационных признаков, причем переход от отдельных кадров к целому видео происходит путем выбора максимального отклика по циклу походки. Преимущество данного метода состоит в отсутствии дополнительной предварительной обработки при наличии необходимых данных характеристик силуэта. Для успешной идентификации человека, широко применяются рекуррентные нейронные сети, что позволяет при простейших данных получать информативные динамические признаки походки. Также, рекуррентные слои могут быть

[2] Петров С.М. Судебно-экспертное исследование походки // Теория и практика судебной экспертизы. 2022. Т. 17. № 3. С. 26-39.

применимы к скелету человека, то есть к тепловым картам суставов, что позволяет получить более общую картину, не делая акцент на фигуру и силуэт, а анализировать лишь изменения позы человека[3]. По нашему мнению, данный метод позволяет распознавать основные признаки походки человека, игнорируя более изменчивые показатели, которые могут затруднить анализ.

Далее рассмотрим современные разработки, ведущей из которых представляется программа NTECH LAB, которая построена на использовании алгоритма детектирования и распознавания по силуэту. Алгоритм данной программы с помощью нейронных сетей определяет характерные черты походки человека. Каждая сеть определяет одну черту, при этом все задействованные сети работают параллельно. Система распознавания по силуэту выполняет точный и быстрый подсчет масс людей в видеопотоке, а также осуществляет межкамерный трекинг силуэтов. Данная разработка направлена на предотвращение кибер-атак путем интеграции системы распознавания живого человека от изображения. Программа NTECH LAB успешно внедряется в российскую систему городской безопасности. Видеоаналитика с использованием системы распознавания позволила разыскать и принять своевременные меры к задержанию почти 100 человек из розыскных баз с 50 000 фотографий правонарушителей на FIFA 2018[4]. По состоянию на 2021 год система, установленная в Москве, позволила за полгода задержать более девятисот преступников в метрополитене. По нашему мнению, программа NTECH LAB позволяет за короткий промежуток времени идентифицировать человека по его силуэту, походке, что значительно упрощает дальнейший поиск правонарушителей для правоохранительных органов. Однако нельзя не отметить, что реализация алгоритма проблематична. Различное расположение камер, их низкое либо высокое качество, цветное или черно-белое изображение создает определенные проблемы для межкамерного трекинга силуэтов, что в последствии затрудняет поиск правонарушителей.

Исходя из перечисленных выше современных методов, искусственный интеллект постепенно внедряется в российскую систему безопасности, однако существует необходимость расширения использования программ на основе нейронных сетей на всю территорию Российской Федерации. В перспективе использования в настоящий момент проводятся тестирования умных очков с встроенной технологией распознавания лиц от NTECH LAB, которыми в будущем планируется оснащать полицию, что позволит мгновенно распознавать правонарушителей по походке и силуэту, а также осуществлять

[3] Соколова А.И., Конушин А.С. Методы идентификации человека по походке в видео // Труды ИСП РАН. 2019. №1. С. 69-82.

[4] Система идентификации и верификации лиц [Электронный ресурс] // Программа NTECH LAB. URL: https://ntechlab.ru/technology/ (дата обращения: 27.01.2023).

своевременное задержание данных лиц. Система отслеживания признаков походки по видеоизображениям результативна, однако требует определенного комплекса характеристик для полноты образа идентифицируемого, высокого качества видеофрагментов и различных углов съемки, что представляет собой более кропотливую работу для экспертов. Таким образом, проблема определения наиболее эффективного способа идентификации человека по признакам походки остается актуальной на данный момент, требует дальнейшего изучения и внедрения современных разработок.

Список литературы

1. Петров С.М. Судебно-экспертное исследование походки // Теория и практика судебной экспертизы. 2022. Т. 17. № 3. С. 26-39.

2. Соколова А.И., Конушин А.С. Методы идентификации человека по походке в видео // Труды ИСП РАН. 2019. №1. С. 69-82.

Elizaveta S. Sapozhnikova
Student,
National Research State University of Nizhny Novgorod
named after N. I. Lobachevsky
(Nizhny Novgorod, Russia)
E-mail: heyelizabeth13@gmail.com

Scientific supervisor: Anastasia V. Polyakova
Senior Lecturer of the Department of Forensic Expertise,
National Research State University of Nizhny Novgorod
named after N. I. Lobachevsky
(Nizhny Novgorod, Russia)
anastasia.poliakova811@yandex.ru

FORENSIC PORTRAIT IDENTIFICATION OF A PERSON BY SIGNS OF GAIT

Abstract. The article is devoted to the most effective methods of modern human identification by gait signs. The author has conducted a comparative study of modern methods of human identification by gait signs. Particular attention is paid to the possibility of using artificial intelligence and neural networks to solve this problem, and also considered specific developments aimed at human identification by gait signs.

Keywords: gait identification, temporal and spatial characteristics, neural networks, artificial intelligence, recognition program.

УДК: 004.8

Сикач Артём Сергеевич
Студент Юридической школы,
Дальневосточный федеральный университет
(г. Владивосток, Российская Федерация)
sikach.as@students.dvfu.ru

Научный руководитель: Князева Наталья Анатольевна
кандидат юридических наук, доцент,
доцент кафедры уголовного права и криминологии Юридической школы
Дальневосточный федеральный университет
knyazeva.na@dvfu.ru

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УЛУЧШЕНИИ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ПРОКУРАТУРЫ

Аннотация. Целью данной статьи является анализ возможности применения искусственного интеллекта в деятельности органов прокуратуры. В статье описываются основные области применения искусственного интеллекта, такие как автоматизация правоприменительных процессов, анализ данных, подбор наилучшей стратегии и оптимизация работы прокурорских органов. Также обсуждаются преимущества и недостатки применения искусственного интеллекта в деятельности органов прокуратуры.

Ключевые слова: искусственный интеллект, органы прокуратуры, автоматизация, анализ данных, оптимизация, применение.

Для цитирования:
Сикач А. С. Использование искусственного интеллекта в улучшении деятельности органов прокуратуры // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 399–403.

Искусственный интеллект широко применяется в разных сферах жизни, таких как торговля, медицина, военное дело, промышленность, управление движением и другие. Его использование в уголовном судопроизводстве также активно исследуется. Прогнозы показывают, что применение ИИ будет только расти, а доходы от этого – увеличиваться[1].

Внедрение ИИ в общество – процесс с чёткими приоритетами и параметрами, заданными в

[1] Сикач А. С. Искусственный интеллект в российском уголовном праве: студенческая научная работа. Владивосток, 2021. С. 3.

программных документах. Он неизбежен и продвигается на основе общественных потребностей[2]. В декабре 2016 года Президент РФ В. В. Путин высказал важность цифровизации государства и необходимость сосредоточиться на направлениях, связанных с цифровыми и технологическими разработками, которые определяют облик всех сфер жизни[3]. В стратегии развития информационного общества в РФ на 2017–2030 гг. искусственный интеллект признан одним из важнейших направлений развития российских ИКТ[4]. 10 октября 2019 г. Президент РФ утвердил Национальную стратегию развития искусственного интеллекта до 2030 г. В документе отмечается, что ключевым свойством ИИ является возможность имитации когнитивных функций человека и достижения результатов, сравнимых с результатами человеческой интеллектуальной деятельности[5]. Искусственный интеллект стал незаменимым в борьбе с пандемией COVID-19, доказав свою значимость и эффективность, когда скорость распространения угрозы не давала шансов традиционным методам борьбы[6].

В. В. Путин заявил на AI Journey, что нельзя игнорировать прогресс в области искусственного интеллекта и важно научиться им управлять. Нам нужно быть смелыми и компетентными, чтобы подчинить себе эту технологию и смотреть в будущее[7]. В экспертном сообществе отмечается, что в будущем технологии искусственного интеллекта станут более социальными, а их агенты будут использоваться для решения задач в среде человеческих взаимодействий[8].

---

[2] Заметина Т. В., Комбарова Е. В., Искусственный интеллект и конституционные вопросы его внедрения в современной России // Правовая политика и правовая жизнь. 2021. № 1. С. 183–187.

[3] Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://minsvyaz.ru/ru/activity/directions/779/ (дата обращения: 10.03.2021).

[4] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента Российской Федерации от 9 мая 2017 г. № 203 // СЗРФ. 2017. № 41. Ст. 5700.

[5] О развитии искусственного интеллекта в Российской Федерации: указ Президента РФ от 10 октября 2019 г. № 490 (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) // СЗРФ. 2019. № 20. Ст. 2901.

[6] Кашкин С. Ю., Тищенко С. Ю., Алтухов А. В. Правовое регулирование искусственного интеллекта в условиях пандемии и инфодемии: монография / под общ. ред. В. В. Блажеева, М. А. Егоровой. М.: Проспект, 2020. 240 с.; Кашкин С. Ю., Тищенко С. Ю., Алтухов А. В. Правовое регулирование применения искусственного интеллекта для борьбы с распространением COVID-19: проблемы и перспективы с учетом мирового опыта // Lex Russica (Русский закон). 2020. Т. 73. № 7. С. 107–112.

[7] Конференция Artificial Intelligence Journey (AI Journey 2020) на тему «Искусственный интеллект – главная технология XXI века». // Президент России. 2020. 5 декабря. [Электронный ресурс]. URL: http:// kremlin.ru/events/president/news/64545 (дата обращения: 09.05.2023).

[8] Резаев А. В., Трегубова Н. Д. Искусственный интеллект и искусственная социальность: новые явления и проблемы для развития медицинских наук // Эпистемология и философия науки. 2019. Т. 56. № 4. С. 187–195.

Искусственный интеллект всё более популярен в различных сферах общества, включая органы власти, правоохранительные органы и органы прокуратуры. Цифровизация прокуратуры является частью «Цифровой экономики РФ», утверждённой Правительством в 2017 году, а в 2018 году была принята «Концепция цифровой трансформации органов и организаций прокуратуры до 2025»[9]. Генеральная прокуратура РФ планирует внедрить инструменты мягкого искусственного интеллекта к 2025 году для обработки больших массивов данных, что позволит увидеть закономерности, невидимые гражданам.

Примером использования таких инструментов является проект Окружной прокуратуры в Сан-Франциско, который позволяет снизить предвзятость в подготовке обвинительных заключений, исключив из документов информацию о расовой принадлежности обвиняемого[10].

Стэндфордская лаборатория создала программы искусственного интеллекта для автоматического выявления серийных моделей преступлений и редактирования полицейских отчётов.

Аргентинский сервис Prometea использует искусственный интеллект для оптимизации работы прокуратуры, вынося вердикты в 33 из 33 случаев за десять секунд. Технология позволяет сотрудникам прокуратуры уделять больше времени сложным делам, а сервис обрабатывает административные дела на испанском и английском языках[11].

В Китае также разработали искусственный интеллект, который может предъявлять обвинения с точностью в 97 % на основе устного описания дела[12]. В Пудуне (Шанхай, Китай) успешно протестирован ИИ, способный заменить прокуроров в рутинных делах и помочь им в составлении обвинительных заключений. Система обучилась на 17 тысячах рассмотренных судебных дел и способна выдвигать обвинения по 8 распространённым преступлениям. В ближайшем будущем ИИ сможет работать и со сложными делами. Китай является первой страной, применяющей технологии ИИ в работе прокуратуры.

---

[9] Приказ Генеральной прокуратуры РФ № 627 от 14 сентября 2017 г. «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» // СПС «Гарант». [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71670972 (дата обращения: 09.05.2023).

[10] Избавит ли искусственный интеллект от «предвзятости» прокуроров? // Умная безопасность. Яндекс.Дзен. 2019, 14 июня. [Электронный ресурс]. URL: https://zen.yandex.ru/media/id/5c88926728941b00b4b27d1a/izbavit-li-iskusstvennyi-intellektot-predvziatosti-prokurorov-5d034b6e2ec4b60e6db4ce5d/(дата обращения: 09.05.2023).

[11] Искусственный интеллект изучил 300 000 документов и стал помогать прокуратуре. // Институт судебных экспертиз и криминалистики. 2018, 30 октября. [Электронный ресурс]. URL: https://ceur.ru/news/921/item351285/(дата обращения: 09.05.2023).

[12] Совина М. В Китае разработали цифрового прокурора // Lenta.ru. 2021, 27 декабря. [Электронный ресурс]. URL: https://lenta.ru/news/2021/12/27/ai_prosecutor/ (дата обращения: 09.05.2023).

В Казахстане создали информационную систему «Зандылык», которая помогает проверять проекты актов на соответствие законам и получать статистику по регионам[13].

Таким образом, искусственный интеллект является эффективным электронным помощником, упрощающим нагрузку на сотрудников органов прокуратуры, полностью правоохранительных органов, благодаря чему идут показательные успехи в этом.

Список литературы:

1. Заметина Т. В., Комбарова Е. В., Искусственный интеллект и конституционные вопросы его внедрения в современной России // Правовая политика и правовая жизнь. 2021. № 1. С. 183–187.

2. Кашкин С. Ю., Тищенко С. Ю., Алтухов А. В. Правовое регулирование искусственного интеллекта в условиях пандемии и инфодемии: монография / под общ. ред. В. В. Блажеева, М. А. Егоровой. М.: Проспект, 2020. 240 с.

3. Кашкин, С. Ю., Тищенко С. Ю., Алтухов А. В. Правовое регулирование применения искусственного интеллекта для борьбы с распространением COVID-19: проблемы и перспективы с учетом мирового опыта // Lex Russica (Русский закон). 2020. Т. 73. № 7. С. 107–112.

4. Резаев А. В., Трегубова Н. Д. Искусственный интеллект и искусственная социальность: новые явления и проблемы для развития медицинских наук // Эпистемология и философия науки. 2019. Т. 56. № 4. С. 187–195.

5. Сикач А. С. Искусственный интеллект в российском уголовном праве: студенческая научная работа. Владивосток, 2021. 37 с.

Artem S. Sikach
Student of the Law School,
Far Eastern Federal University
(Vladivostok, Russian Federation)
sikach.as@students.dvfu.ru

Scientific Supervisor: Natalya A. Knyazeva
PhD in Law, Associate Professor,
Associate Professor of the Department of Criminal Law
and Criminology of the Law School
Far Eastern Federal University

[13] Концепция развития технологий машиночитаемого права: утверждена Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 15 сентября 2021 г. № 31) // СПС КонсультантПлюс. [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_396491/ (дата обращения: 09.05.2023).

knyazeva.na@dvfu.ru

THE USE OF ARTIFICIAL INTELLIGENCE IN IMPROVING THE ACTIVITIES OF THE PROSECUTOR'S OFFICE

Abstract. The purpose of this article is to analyze the possibility of using artificial intelligence in the activities of the prosecutor's office. The article describes the main areas of application of artificial intelligence, such as automation of law enforcement processes, data analysis, selection of the best strategy and optimization of the work of prosecutorial bodies. The advantages and disadvantages of using artificial intelligence in the activities of the prosecutor's office are also discussed.

Keywords: artificial intelligence, prosecution authorities, automation, data analysis, optimization, application.

УДК 343.98

Сикач Артём Сергеевич
Студент Юридической школы,
Дальневосточный федеральный университет
(г. Владивосток, Российская Федерация)
sikach.as@students.dvfu.ru

Научный руководитель: Князева Наталья Анатольевна
кандидат юридических наук, доцент,
доцент кафедры уголовного права и криминологии Юридической школы
Дальневосточный федеральный университет
knyazeva.na@dvfu.ru

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Аннотация. В данной статье рассматривается роль цифровых технологий и, в частности, искусственного интеллекта в расследовании преступлений. Приводятся примеры зарубежных стран: США, Британии, Турции, Голландии, ОАЭ, Японии и т. д., – в которых успешно реализуются отдельные проекты по внедрению искусственных интеллектуальных систем в правоохранительную деятельность.

Ключевые слова: искусственный интеллект, предсказание преступления, робот – полицейский, искоренение преступности, Япония, США, Турция, Индия.

Для цитирования:
Сикач А. С. Роль искусственного интеллекта в расследовании преступлений // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 404–413.

С каждым годом наука развивается все быстрее, и цифровые технологии становятся неотъемлемой частью жизни общества. Сферы их применения находится в различных областях: медицине, бизнесе, образовании (где разрабатываются роботы, способные преподавать в высших учебных заведениях). Цифровые помощники, созданные с помощью этих технологий, могут стать друзьями человека в различных ситуациях. Однако, вместе с позитивными сторонами цифровых технологий связаны и негативные. Использование их для совершения противоправных действий против граждан и пользователей Интернета становится всё более распространённым, и киберпреступность набирает обороты. В частности, хакеры, обладающие углублёнными знаниями в области компьютеризации и информатизации,

могут использовать разработанные ими компьютерные программы для хищения денежных средств и других противоправных действий в отношении организаций и частных лиц. Они также могут управлять чужим транспортным средством, чтобы совершить покушение на владельца. Таким образом, хотя цифровые технологии открывают перед обществом множество новых возможностей, необходимо помнить о существующих рисках, связанных с их применением. Необходимо всеми силами бороться с киберпреступностью и защищать права граждан и пользователей Интернета, в чём также могут помочь цифровые технологии.

Использование искусственного интеллекта и анализа больших данных может значительно ускорить расследование дел и способствовать выявлению связей между преступниками, сокращая тем самым возможность новых преступлений. Однако, необходимо помнить о том, что применение новых технологий в сфере правоохранительной деятельности требует комплексного подхода, в том числе с позиций этики. Важно соблюдать конфиденциальность персональных данных граждан и убедиться, что алгоритмы и модели обучаемости искусственного интеллекта не содержат дискриминационных элементов. Высказывания Президента РФ В. В. Путина на международной конференции по искусственному интеллекту подчеркивают, что цифровые технологии имеют огромный потенциал для развития общества. Применение искусственного интеллекта и анализа больших данных может облегчить работу в различных сферах, поэтому внедрение технологий искусственного интеллекта должно стать одним из приоритетов государства. Тем не менее, важно не забывать о том, что все новые технологии должны применяться с соблюдением этических норм и учитывать защиту интересов граждан и пользователей[1]. Применение цифровых технологий в правоохранительной деятельности может значительно ускорить расследование уголовных дел, в том числе и сложных, благодаря анализу больших данных и использованию искусственного интеллекта. Уже в 2019 году на Ежегодной встрече полицейских экспертов ОБСЕ была обсуждена тема использования искусственного интеллекта в правоохранительных органах, что свидетельствует о том, что интеграция цифровых технологий в эту сферу находится на повестке дня и является важным шагом для повышения эффективности деятельности правоохранительных органов и снижения процента преступности в обществе[2].

[1] Владимир Путин в режиме видеоконференции принял участие в основной дискуссии конференции по искусственному интеллекту Artificial Intelligence Journey (AI Journey 2020) на тему «Искусственный интеллект – главная технология XXI века» // Президент России. 2020, 4 декабря. [Электронный ресурс]. URL: http://www.kremlin.ru/events/president/news/64545 (дата обращения: 01.05.2023).

[2] Овчинский В. С., Маслов А. А., Бабушкин А. А. О перспективах использования

Одним из основных аспектов, вынесенных для обсуждения участниками Ежегодной встречи полицейских экспертов ОБСЕ, является потенциал искусственного интеллекта для внедрения в правоохранительную деятельность. Существует два основных направления развития искусственного интеллекта: «сильный» и «слабый». Сильный ИИ, способный заменить человека, требует дальнейших исследований, в то время как слабый ИИ, на основе которого создаются автоматизированные системы, развивается очень быстро. Использование искусственного интеллекта в правоохранительной деятельности может быть направлено на следующие задачи: сбор, обработка и хранение информации, прогностические и аналитические модели, цифровое расследование и обеспечение коммуникаций и взаимодействия.

Учитывая быстрый прогресс науки и цифровых технологий, внедрение искусственного интеллекта в профессиональную деятельность лиц, осуществляющих следствие по уголовным делам, становится всё более актуальным. Это связано с тем, что «преступный мир» также показал интерес к использованию цифровых технологий с противоправными целями, а также с растущей популярностью использования искусственного интеллекта в разных странах, в том числе и в России. Однако использование искусственного интеллекта не предполагает полного отказа от работы следователей, но лишь. призвано повысить эффективность их работы. Считается, что сохранение накопленного опыта и корректности действий сотрудников правоохранительных органов в ходе применения новых информационных технологий является особенно важным аспектом. Это предотвратит возможные негативные последствия в процессе улучшения работы следователей с использованием искусственного интеллекта. Поэтому надо тщательно продумывать действия в процессе использования ИИ и сохранять баланс между использованием технологии и опытом следователей. В связи с этим нельзя не согласиться с А. Ю. Афанасьевым, который отмечает, что «потенциал искусственного интеллекта должен использоваться в той степени, которая позволит успешно реализовывать возложенные функции, а не в противовес имеющейся системе»[3].

Следует отметить, что с появлением и совершенствованием цифровых технологий, работа правоохранителей в расследовании уголовных дел стала более эффективной, особенно в условиях присутствия преступлений в цифровой среде. Искусственный интеллект помогает правоохранительным органам оценить информацию по уголовному делу и выдвинуть следственные версии. Цифровые технологии построены на модели

технологий искусственного интеллекта в оперативно-розыскной деятельности органов внутренних дел: Научный доклад. Москва: ВНИИ МВД России. 2020.

[3] Афанасьев А. Ю. Искусственный интеллект или интеллект субъектов выявления, раскрытия и расследования преступлений: что победит? // Библиотека криминалиста. Научный журнал. 2018. №3 (38). С. 30.

противоправных действий, которые сформулированы в криминалистических методиках. Искусственный интеллект на их основе создаёт свои методики расследования преступлений[4].

Одной из главных функций искусственного интеллекта является обработка больших объёмов данных с целью выявления важной информации для расследования преступлений. Однако для эффективного использования возможностей ИИ необходима обширная база данных. В то же время существует этический аспект в формировании таких баз данных, при котором принудительное получение информации о личной жизни граждан может противоречить нормам Конституции, например, защите частной жизни, тайне переписки, и так далее. Поэтому, чтобы найти законный компромисс в этой ситуации, необходимо тщательно рассмотреть и оценить возможные риски и найти способы по защите личных данных граждан.

В этом смысле интересно высказывание Д. А. Кравцова: «Обеспечение приемлемого уровня безопасности является приоритетным направлением в функционировании государства в целом, в связи с чем способность искусственного интеллекта собирать, отслеживать и анализировать такой огромный поток всевозможных данных для деятельности в целях предупреждения преступности, является весьма эффективной, хоть и может вызывать вопросы о конфиденциальности и т. п.»[5]. На наш взгляд, вынесение таких этических проблем является необходимой мерой хорошего развития цифровых технологий, оказывающий положительное влияние на деятельность человека во всех отраслях жизни общества.

Следует также обратиться к мнению Президента РФ В. В. Путина, согласно которому «… нужно дать искусственному интеллекту больше данных, последовательно снимать подчас надуманные преграды для их использования, но при этом необходимо гарантировать безопасность, соблюдение интересов и прав граждан»[6].

Сейчас искусственный интеллект внедряют ещё и в видеонаблюдение для искоренения и пресечения правонарушений, а также обнаружения потенциальных и «состоявшихся» правонарушителей. МВД России уже проводило тестирование интеллектуальных видеосистем, которые помогают бороться с противоправными действиями. Кроме того, в 2017 году были получены положительные результаты такого тестирования. В 2019 году также был достигнут успех

[4] Вехов В. Б. Автоматизированные методики расследования преступлений как новое направление в криминалистической технике // Известия тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 10.

[5] Кравцов Д. А. Искусственный разум: предупреждение и прогнозирование преступности. Вестник Московского университета МВД России. 2018. № 3. С. 109.

[6] Конференция по искусственному интеллекту // Официальный сайт Президента России. 2020, 7 июня. [Электронный ресурс]. URL: http://www.kremlin.ru/events/president/news/62003 (дата обращения: 01.05.2023).

при использовании системы видеонаблюдения, которая применяла биометрическую идентификацию в рамках программного комплекса «Безопасный город». Таким образом, было раскрыто более 3 тысяч противоправных действий[7]. С использованием интеллектуальных видеокамер и их усовершенствованием возможности поимки преступников увеличиваются каждый год. Интеллектуальные видеокамеры распознавания лиц работают путём сравнения лица гражданина, снятого на видео, с имеющимися изображениями разыскиваемых лиц, хранящимися в соответствующей базе данных. В случае положительного совпадения, находящиеся поблизости сотрудники правоохранительных органов получают уведомление, что упрощает дальнейшее расследование преступлений и помогает отыскать скрывающихся от государства личностей.

Эффективность интеллектуальных систем видеонаблюдения в борьбе с преступностью породила идею внедрения подобных технологий на улицах Москвы и в метрополитене, о чём заявил мэр города в 2020 году. Система умного видеонаблюдения должна была начать работать с 1 сентября 2020 года. В феврале 2020 года МВД России заявило о совершенствовании системы, позволяющей выявлять злоумышленников не только по изображению лица, но и по радужной оболочке глаза, татуировкам, а также голосу. Планировалось, что данный функционал будет внедрён в интеллектуальную систему видеонаблюдения к концу 2021 года[8].

Создание интеллектуальных систем видеонаблюдения с использованием искусственного интеллекта вызвало большой интерес учёных и разработчиков в сфере цифровых технологий. Компания «Промобот», специализирующаяся на производстве сервисных роботов, создала робота-полицейского, который может не только распознавать лица и речь автономно, но и содействовать правоохранительным органам в оказании помощи на местах массового скопления людей. Он способен сканировать отпечатки пальцев и выводить информацию о конкретном человеке, если тот находится в базе данных ведомства. Робот также обладает нейронной сетью, позволяющей ему распознавать различные типы оружия. Однако, роботы до сих пор не способны проводить оперативные действия, а только помогают живым полицейским в местах повышенного скопления людей, например, в метро, аэропортах и на массовых мероприятиях.

[7] Система распознавания лиц в Москве помогла раскрыть 3 тысячи преступлений. // Российская газета. 2020, 6 июля. [Электронный ресурс]. URL: https://rg.ru/2019/11/04/reg-cfo/sistema-raspoznavania-lic-v-moskve-pomogla-raskryt-3-tysiachi-prestuplenij.html (дата обращения: 01.05.2023).

[8] МВД при помощи камер начнёт искать преступников по татуировкам и походке. // РБК. 2020, 7 июня. [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/24/02/2020/5e4fb5af9a7947cfdfd5e1e3 (дата обращения: 01.05.2023).

Получается, что такие технологии помогают улучшить эффективность патрулирования на улицах и повышают уровень безопасности населения[9]. Роботы-полицейские выполняют множество задач, среди которых патрулирование, видеонаблюдение и поддержание порядка на объектах.

Вместе с Россией, и другие страны продвигаются в области искусственного интеллекта. Например, в Чикагском университете разработан алгоритм ИИ, который с точностью до 90 % может предсказывать возможность совершения различных преступлений в городе на неделю вперед. Алгоритм делит город на секторы площадью около 300 метров, в процессе анализируя время и место прошлых преступлений и выявляя закономерности, которые позволяют предсказывать будущие события. Созданный цифровой двойник позволяет прогнозировать возможные преступления и изучать возможные последствия, которые могут произойти при изменении в различных районах города. Благодаря таким разработкам местные правоохранительные органы могут повысить эффективность своей работы и обеспечить безопасность жителей[10].

В Великобритании полиция привлекает искусственный интеллект для расследования преступлений, что позволяет более эффективно обрабатывать огромный объём информации при сборе доказательств. Благодаря ИИ полицейские могут быстрее находить нужную информацию среди тысяч сообщений и упрощать работу, связанную с разоблачением самых сложных дел, связанных с коррупцией. Один из примеров – искусственный интеллект, разработанный компанией Rovn и помогавший в работе 7 следователям. За считанные дни ИИ смог обработать более 30 млн документов, просматривая в день около 600 тысяч сообщений. Это облегчило задачу следователям в несколько раз и сократило время, которое они должны были бы потратить на обработку информации, на несколько месяцев[11].

Турецкие инженеры создали искусственный интеллект ASENA для работы в области борьбы с наркотиками. Программа интегрирована с базами данных электронного правительства и Министерства внутренних дел и юстиции, а также с UYAP. ASENA использует тысячи данных, включая методы, разработанные

[9] В РФ создали робота – полицейского, способного говорить на двух языках // Аргументы и факты AIF.RU. 2021, 23 ноября. [Электронный ресурс]. URL: https://aif.ru/techno/v_rf_sozdali_robota-policeyskogo_sposobnogo_govorit_na_dvuh_yazykah (дата обращения: 01.05.2023).

[10] Учёные из Чикагского университета разработали новый алгоритм, который с точностью около 90 процентов прогнозирует в городе на неделю вперед возможность совершения различных преступлений // Российская газета. 2022, 1 июля. [Электронный ресурс]. URL: https://rg.ru/2022/07/01/iskusstvennyj-intellekt-predskazhet-prestupleniia.html (дата обращения: 01.05.2023).

[11] Британская полиция привлекла ИИ для помощи в раскрытии преступлений // Хабр. Сообщество IT-специалистов. 2019, 6 сентября. [Электронный ресурс]. URL: https://habr.com/ru/news/t/466471/ (дата обращения: 01.05.2023).

злоумышленниками, что позволяет выявлять преступников и раскрывать преступления в сфере наркотиков. За 14 месяцев работы программа помогла раскрыть более 3,7 тысячи преступлений в данной области. Программа ASENA также обладает высокой степенью безопасности, так как использует замкнутую систему связи POLNET, которая является защищённой от кибератак[12].

Голландские правоохранительные органы начали использовать искусственный интеллект для решения сложных преступлений. Система оцифровывает больше 1500 отчётов и 30 млн страниц материалов, связанных с нераскрытыми делами, начиная с 1988 года, когда преступление оставалось не раскрытым не менее 3 лет и злоумышленник был приговорён больше, чем к 12 годам лишения свободы. После оцифровки система искусственного интеллекта подключится к системе машинного обучения, которая позволит анализировать записи и определять, какие доказательства являются наиболее достоверными. Таким образом, система сократит время обработки дел и раскрытия преступлений от нескольких недель до одного дня. Система искусственного интеллекта также будет делить дела по их вероятности разрешения и укажет на возможные результаты экспертизы ДНК. В будущем система может автоматизировать анализ в других областях судебной экспертизы и охватывать данные в таких областях, как общественные науки и свидетельские показания. Ключевой разработчик системы, Джерун Хаммер, подчеркнул возможность запуска API-функций для партнеров, которые могут исправить существующие проблемы и ускорить процесс работы в области правосудия[13].

В Дубае, Объединённых Арабских Эмиратах, тестируется SIME (Space Imaging Middle East), искусственный интеллект, который использует данные о происшествиях за последние годы, чтобы предсказывать места совершения преступлений. Нейронная сеть анализирует архивные данные и выдаёт прогнозы о вероятности преступлений в различных районах города. Полицейские используют эти данные для усиления патрулирования проблемных районов[14].

В 2019 году в Японии начался эксперимент по использованию искусственного интеллекта в полиции. Эксперимент включает в себя несколько этапов: идентификацию модели автомобиля по изображению с камеры наблюдения, анализ

[12] Искусственный интеллект ASENA отслеживает наркотики // ADANAMERSIN. 2022, 3 июня. [Электронный ресурс]. URL: https://ru.rayhaber.com/2022/06/Асена-с-искусственным-интеллектом-отслеживает-наркотики/ (дата обращения: 01.05.2023).

[13] 2018: Применение ИИ голландской полицией для расследования сложных преступлений // TADVISER. Государство. Бизнес. Технологии. 2022, 30 августа. [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_криминалистике (дата обращения: 01.05.2023).

[14] Искусственный интеллект будет предугадывать преступления в городе Дубай // NAKED SCIENCE. 2016, 26 декабря. [Электронный ресурс.]. URL: https://naked-science.ru/article/concept/iskusstvennyy-intellekt-budet (дата обращения: 01.05.2023).

транзакций, считающихся подозрительными, и блокировку подозрительных лиц или предметов. Эта инициатива проводится Японским национальным полицейским управлением. В дальнейшем будет рассмотрен вопрос о применении искусственного интеллекта в других областях работы полиции, таких как предупреждение о возможных преступлениях на основе результатов экспериментов[15].

В Индии была создана система искусственного интеллекта PAIS (Punjab Artificial Intelligence System), предназначенная для распознавания лиц подозреваемых на фоне толпы. Система использует алгоритмы распознавания лиц с использованием искусственного интеллекта, чтобы сравнить их с базой данных национальной полиции, содержащей более 100 000 криминальных записей. Она разработана с целью улучшения качества работы полиции и ускорения процесса поиска преступников. При успешной реализации этого проекта система PAIS может быть внедрена в других частях индийской полиции для достижения более высоких результатов в борьбе с преступностью[16]. Недавно отдел по борьбе с организованной преступностью полиции Пенджаба использовал эту систему для раскрытия дела о торговле наркотиками, когда подозреваемый сбежал. Телефонные фотографии с места происшествия позволили быстро привлечь правонарушителя к ответственности. Однако Пенджаб не единственный регион, в котором используют технологии искусственного интеллекта в полицейских участках. Такой подход применяется также в Раджастхане, Махараштре, Бихаре, Телангане и других регионах. Например, Андхра-Прадеш сотрудничает с несколькими департаментами для создания системы видеонаблюдения во всем регионе.

Кроме того, Индия разработала множество программных систем с использованием искусственного интеллекта, которые позволяют расследовать и прогнозировать преступления. Например, разработан искусственный интеллект под названием ABHED (Artificial Intelligence Based Human Efface Detection) для обнаружения и распознавания человеческих лиц на видеозаписях[17], который помогает правоохранительным органам в оцифровывании криминальных отчётов и анализе информации в

---

[15] Япония начала тестирование искусственного интеллекта для раскрытия преступлений в 2019 году, сможет ли полиция с искусственным интеллектом стать детективом // Русские Блоги. 2019, 20 апреля. [Электронный ресурс]. URL: https://russianblogs.com/article/23001451216/ (дата обращения: 01.05.2023).

[16] Япония начала тестирование искусственного интеллекта для раскрытия преступлений в 2019 году, сможет ли полиция с искусственным интеллектом стать детективом // Русские Блоги. 2019, 20 апреля. [Электронный ресурс]. URL: https://russianblogs.com/article/23001451216/ (дата обращения: 01.05.2023).

[17] «Индийский» искусственный интеллект для расследования преступлений // Дзен. 2019, 27 июня. [Электронный ресурс.] URL: https://dzen.ru/media/id/5c88926728941b00b4b27d1a/indiiskii-iskusstvennyi-intellekt-dlia-rassledovaniia-prestuplenii-5d1461cd0119dd00aee5c087 (дата обращения: 01.05.2023).

режиме реального времени. Компания также предоставляет решения для государственных заказчиков, включая систему обнаружения человеческого фактора на основе искусственного интеллекта и умные очки с технологией распознавания лиц. Системы помогли раскрыть более 1100 противоправных действий. Компания работает с базой данных более чем 1 млн преступников. Ещё одна система – «GAUT» – распознаёт лиц в режиме реального времени, используя не только черты лица, но и походку, жесты.

Система «GANG Analysis» помогает полиции вычислять банды преступников. Анализ «горячих точек» и «геозон» используются для определения закономерностей в местах преступлений. Компания «STAQU» применяет ИИ для поиска пропавших людей. Родственники предоставляют фотографии пропавших, которые загружаются в базу данных. Приложение «STAQU» использует данную базу для сопоставления с фотографиями беспризорных детей или трупов, найденных полицией. Компания планирует сделать систему доступной для всех граждан, чтобы они могли помогать в поиске пропавших людей.

Искусственный интеллект применяется в РФ и зарубежных странах для расследования преступлений и помощи сотрудникам правоохранительных органов. Уровень преступности постепенно падает, но ИИ не является панацеей от преступности – он лишь инструмент. Искусственный интеллект может стать полноценным помощником только тогда, когда будет обладать сознательностью, правами и обязанностями, а также сможет отдавать себе отчёт в своих действиях.

Список литературы:

1. Афанасьев А. Ю. Искусственный интеллект или интеллект субъектов выявления, раскрытия и расследования преступлений: что победит? // Библиотека криминалиста. Научный журнал. 2018. № 3 (38). С. 28–34.

2. Вехов В. Б. Автоматизированные методики расследования преступлений как новое направление в криминалистической технике // Известия тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 8–11.

3. Кравцов Д. А. Искусственный разум: предупреждение и прогнозирование преступности. Вестник Московского университета МВД России. 2018. № 3. С. 108–110.

4. Овчинский В. С., Маслов А. А., Бабушкин А. А. О перспективах использования технологий искусственного интеллекта в оперативно-розыскной деятельности органов внутренних дел: Научный доклад. Москва: ВНИИ МВД России. 2020.

Artem S. Sikach
Student of the Law School,

Far Eastern Federal University
(Vladivostok, Russian Federation)
sikach.as@students.dvfu.ru

Scientific Supervisor: Natalya A. Knyazeva
PhD in Law, Associate Professor,
Associate Professor of the Department of Criminal Law
and Criminology of the Law School
Far Eastern Federal University
knyazeva.na@dvfu.ru

THE ROLE OF ARTIFICIAL INTELLIGENCE IN CRIME INVESTIGATION

Abstract. This article examines the role of digital technology and, in particular, artificial intelligence in the investigation of crime. Examples are given of foreign countries: USA, Britain, Turkey, Holland, UAE, Japan, etc., where there are successful projects of implementing artificial intelligence systems in law enforcement.

Keywords: Artificial intelligence, crime prediction, police robot, crime eradication, Japan, USA, Turkey, India.

УДК 328.185

Станогина Валерия Николаевна
Студент Института прокуратуры
Саратовская государственная юридическая академия
(г. Саратов, Российская Федерация)
valeriastanogina@gmail.com

Научный руководитель: Гарига Ольга Анатольевна
Кандидат юридических наук, доцент,
доцент кафедры криминалистики,
Саратовская государственная юридическая академия
ogariga@yandex.ru

РАССЛЕДОВАНИЕ КОРРУПЦИОННЫХ ПРЕСТУПЛЕНИЙ ПРИ РЕАЛИЗАЦИИ НАЦИОНАЛЬНЫХ ПРОЕКТОВ

Аннотация. В статье рассматриваются проблемы расследования коррупционных преступлений и предлагаются оптимальные способы для осуществления настоящей деятельности. При этом, автором учитываются круг лиц, участвующих в совершении преступлений, служебное положение субъекта, время осуществления коррупционной деятельности, предмет преступного посягательства.

Ключевые слова: коррупционные преступления, национальные проекты, оперативно-розыскная деятельность.

Для цитирования:
Станогина В. Н. Расследование коррупционных преступлений при реализации национальных проектов // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 414–417.

В современном мире развиваются различные проекты, спонсируемые государством и позволяющие улучшить важнейшие сферы жизни общества. Но зачастую, граждане путём обмана и злоупотребления доверием совершают деяния, связанные с хищением денежных средств из федерального бюджета, что противоречит установленным уголовным законодательством нормам. Наиболее распространёнными в настоящее время являются коррупционные преступления при реализации национальных проектов. Важное значение для квалификации таких деяний имеют лица, совершающие противоправные действия. Ими могут выступать как недобросовестные подрядчики, так и должностные лица, использующее своё служебное положение в корыстных целях. На этапе расследования данных преступлений возникает ряд вопросов: каким образом необходимо

организовать такое расследование, какие следственные действия оптимально произвести, какую криминалистическую технику использовать и др.

Исходя из отчётов, представленных на координационном совещании, проведённом Генеральной прокуратурой РФ[1], можно сделать вывод, что эффективность раскрытия и расследования преступлений очень низкая, поскольку показатели совершения деяний в данной сфере достаточно большие. Анализируя преступления, совершённые за 2021 год, было выявлено 432 расследованных случая посягательств на законный порядок осуществления деятельности в сфере реализации нацпроектов, совершённых более 314 людьми. При этом, в большинстве дел фигурантами являлись сотрудники государственных учреждений, использующие своё служебное положение.

Трудности, связанные с расследованием преступлений, объясняются тем, что деяния совершаются скрытыми методами, а также связаны с упущениями в совместной работе надзорных, правоохранительных органов и недостаточной координации оперативных служб. Важной задачей правоохранительных органов при расследовании коррупционных преступлений в связи с реализацией национальных проектов является обладание специальными знаниями в области государственного финансирования и функционирования бюджетной системы.

Зачастую уголовные дела о коррупционных преступлениях возбуждаются по материалам оперативно-розыскной деятельности. Поэтому слаженное и скоординированное проведение оперативно-розыскных мероприятий, а также правильная фиксация их результатов является основой для формирования доказательственной базы по делам о коррупционных преступлениях. Самым быстрым способом выявления субъекта преступной деятельности при обнаружении признаков хищения бюджетных средств является использование источников, содержащих конфиденциальные сведения. Поскольку такие средства позволяют спланировать более конкретные действия с учётом специфики полученной оперативной информации.

Важно понимать, что информация, необходимая для доказывания при расследовании хищений денежных средств из федерального бюджета, выявляется в ходе производства различных видов следственных действий (осмотр документов, допрос, обыск и т. д.).

Стоить иметь в виду, что при проведении расследования следователю необходимо изучить не

[1] Под председательством Генпрокурора России Игоря Краснова состоялось координационное совещание по вопросам выявления, раскрытия и расследования преступлений, связанных с хищением средств при исполнении нацпроектов // Генеральная прокуратура Российской Федерации: официальный сайт. Новости. 2021, 25 ноября. [Электронный ресурс]. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=66960784 (дата обращения: 26.03.2023).

только правила предоставления субсидий, льгот, а также иных гарантий, позволяющих претендовать на получение денежных средств из федерального бюджета, но и иные документы, подтверждающие финансирование расходов на реализацию национального проекта, порядок предоставления отчётов соответствующими ведомствами, являющимися распределителями или пользователями бюджетных средств, нормативно-правовые акты, регламентирующие деятельность данных органов. Данная деятельность требует привлечения специалистов соответствующего уровня и знаний. Также в формировании доказательственной базы по коррупционным преступлениям при реализации нацпроектов играет большую роль проведение экспертных исследований.

Важно отметить, что значительную роль при проведении различных следственных действий по данной категории преступлений играет участие специалиста, к выбору которого следователь должен подходить внимательно. Так, в большинстве случаев при расследовании преступлений коррупционной направленности проводится выемка документов, а также носителей компьютерной информации (жёстких дисков). Роль специалиста в данном случае заключается в том, чтобы разъяснить содержание финансовых документов. Трудно переоценить роль специалиста в поиске следов данных деяний, скрытых в компьютерах и облачных хранилищах, так как подпольная бухгалтерия часто хранится в скрытых папках, зашифрована и закрыта сложными паролями[2].

Важно отметить, что по данной категории дел назначают разные экспертизы такие, как судебно-экономическая, судебно-бухгалтерская, фоноскопическая, видео-техническая, компьютерно-техническая, а также комплексные экспертизы повышенной сложности с большим количеством объектов и др.[3]

Таким образом, взаимодействие следователя с оперативными работниками и экспертами является основой эффективного расследования коррупционных преступлений не только при реализации национальных проектов, но у других деяний, связанных с хищением бюджетных средств. Также деятельность оперативного работника по поиску криминалистически значимых фактов в ходе расследования зависит от способа совершения преступления, требует специальных знаний о характере хищения и функционировании финансовой системы государства, имеющей центральное значение для формирования доказательственной базы.

[2] Караева А. А., Столбоушкин А. В. Проблемные аспекты расследования преступлений коррупционной направленности // Вопросы науки и образования. 2020. №. 13 (97). С. 26–33.

[3] Шапиро Л. Г. Судебно-экономические экспертизы в борьбе с преступностью в сфере экономики: процессуальные и криминалистические проблемы // Вестник Саратовской государственной юридической академии. 2016. № 8. С. 35–40.

Считаем, что для повышения эффективности расследования такого рода преступлений необходимо создать отдельную автоматическую информационную поисковую систему, которая бы включала в себя данные о лицах, совершивших коррупционные преступления, что позволило бы сократить время на поиск виновных.

Список литературы

1. Караева А. А., Столбоушкин А. В. Проблемные аспекты расследования преступлений коррупционной направленности // Вопросы науки и образования. 2020. №. 13 (97). С. 26–33.

2. Шапиро Л. Г. Судебно-экономические экспертизы в борьбе с преступностью в сфере экономики: процессуальные и криминалистические проблемы // Вестник Саратовской государственной юридической академии. 2016. № 8. С. 35–40.

Valeria N. Stanogina
Student of the Institute of Prosecutor's Office
Saratov State Law Academy
(Saratov, Russian Federation)
valeriastanogina@gmail.com

Scientific Supervisor: Olga A. Gariga
PhD in Law, Associate Professor,
Associate Professor of the Department of Criminalistics,
Saratov State Law Academy
ogariga@yandex.ru

INVESTIGATION OF CORRUPTION CRIMES IN THE IMPLEMENTATION OF NATIONAL PROJECTS

Abstract. The article examines the problems of corruption offences investigation and proposes the best ways to carry out this activity. In doing so, the author takes into account the range of persons involved in the commission of the crime, the official position of the subject, the timing of corrupt activities, the subject of the criminal offense.

Keywords: corruption crimes, national projects, operational investigative activities.

УДК 347.77

Смирнова Лидия Алексеевна
Студент юридического факультета
Национальный исследовательский Нижегородский
государственный университет имени Н. И. Лобачевского
(г. Нижний Новгород, Российская Федерация)
lida_smirnova_a@mail.ru

Научный руководитель: Балдин Александр Константинович
кандидат юридических наук, доцент,
доцент кафедры гражданского права и процесса
Юридический факультет Национального исследовательского
Нижегородского государственного университета имени Н. И. Лобачевского
(г. Нижний Новгород, Российская Федерация)
akbaldin@unn.ru

ПРАВОВАЯ ОХРАНА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ, СОЗДАННОЙ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Аннотация. в статье исследуется правовая охрана результатов интеллектуальной деятельности, созданных интеллектуальными системами. Автором проведён анализ интеллектуальных прав, их основных особенностей, а также рассмотрены режимы правового регулирования прав интеллектуальной собственности и подходы к определению правосубъектности искусственного интеллекта. В рамках статьи вносятся предложения по совершенствованию правовой защиты результатов интеллектуальной деятельности, созданных юнитами искусственного интеллекта.

Ключевые слова: Гражданский кодекс Российской Федерации, искусственный интеллект, правосубъектность, результаты интеллектуальной деятельности, интеллектуальная собственность.

Для цитирования:
Смирнова Л. А. Правовая охрана интеллектуальной собственности, созданной искусственным интеллектом // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 418–423.

В Российской Федерации происходит постепенное становление информационного общества. В ходе цифровизации всё большее распространение получают сквозные информационные технологии, среди которых: искусственный интеллект (далее – ИИ), нейротехнологии, системы распределённого реестра, виртуальная и дополнения реальность и др. Особую популярность приобретают интеллектуальные системы, активно внедряемые во многие сферы деятельности человека.

В науке и правоприменительной практике всё более актуальной становится проблема определения авторства на объекты интеллектуальной собственности, созданной исключительно искусственным интеллектом, без какого-либо вклада человека.

Согласно статье 1226 Гражданского Кодекса Российской Федерации (далее ГК РФ), под интеллектуальными правами понимаются права «на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации, которые включают исключительное право, являющееся имущественным правом, также личные неимущественные и иные права»[1].

Говоря об объектах интеллектуальных прав, необходимо обозначить их основные признаки:

– *нематериальность* (представляет собой результат умственного труда человека, его интеллектуальной деятельности);

– *возможность объективированного выражения* (объекты нематериального мира должны существовать в реальном материальном мире, а не в идеальном);

– *защищённость со стороны государства* (интеллектуальной собственностью является только результат интеллектуальной деятельности, охраняемый законодателем);

– *уникальность* (право владения объектом интеллектуальных прав принадлежит только правообладателю, новизна результата интеллектуальной деятельности)[2].

Статья 1225 ГК РФ закрепляет объекты интеллектуальной собственности. Указанный перечень периодически конкретизируется и уточняется, что свидетельствует о стремлении соответствовать тенденциям изменяющихся общественных отношений.

В свою очередь, под искусственным интеллектом понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при их реализации результаты, сопоставимые с его деятельностью[3].

По утверждению П. М. Морхата, в целом существует несколько режимов правового регулирования прав интеллектуальной собственности с использованием ИИ:

1) *машиноцентрический концепт*, согласно которому ИИ представляет собой субъект интеллектуального права;

2) *концепт гибридного авторства*, согласно которому ИИ выступает в качестве соавтора;

3) *концепт служебного произведения*, в соответствии с которым технология ИИ является наёмным работником;

[1] Гражданский кодекс Российской Федерации (часть четвертая): Федеральный закон от 18.12.2006 № 230-ФЗ // СЗ РФ. 2006. № 52. Ст. 5496.

[2] Джикаева Ф. А., Лолаева А. С. Понятие и признаки интеллектуальной собственности // Аграрное и земельное право. 2020. № 9 (189). С. 16–17.

[3] Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства РФ. 2019. № 41. Ст. 5700.

4) *антропоцентричный концепт*, согласно которому ИИ выступает в качестве инструмента в руках человека;

5) *концепт «исчезающего» авторства*, предполагающий переход произведения в общественное достояние[4].

В силу статьи 1257 ГК РФ автором произведения признается лицо, указанное в качестве автора на оригинале или экземпляре произведения. Важно отметить, что субъектом авторского права выступает физическое лицо, наделённое конкретным объёмом правоспособности.

Очевидно, что правовая защита интеллектуальной собственности, созданной искусственным интеллектом, напрямую зависит от правового статуса юнитов ИИ. В науке сформулировано несколько концепций, определяющих место интеллектуальных систем в системе общественных правоотношений:

1) *ИИ как объект права.* Концепция предполагает рассмотрение юнитов искусственного интеллекта как «вещи, источника повышенной опасности», «вещи, требующей особого рода регулирования»[5].

2) *ИИ как физическое лицо.* Концепция предполагает наделение интеллектуальной системы правами, схожими с правами физических лиц[6], таких как:

– право на функционирование,

– право на самообучение,

– право на неприкосновенность,

– право на взаимодействие с человеком и др.

3) *ИИ как юридическое лицо.* В соответствии с данной концепцией интеллектуальные системы фактически представляют собой субъекты, обособленные от создателя-учредителя, но за действия которых он отвечает в рамках доли участия[7]. Авторами подхода предлагается применение к ИИ законодательства о юридических лицах.

4) *ИИ как животное.* В соответствии с данным подходом предлагается применять к интеллектуальной системе законодательство, которое применяется к животным[8].

5) *ИИ как электронное лицо.* Резолюция Европарламента от 16

[4]Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: дисс. … д-ра юрид. наук. Москва, 2019. С. 181.

[5] Роботов предложили наделить статусом «электронной личности» // Российская газета. [Электронный ресурс]. URL: https://rg.ru/2017/01/24/robotov-predlozhili-nadelit-statusom-elektronnoj-lichnosti.html (дата обращения: 06.05.2023).

[6] Крысанова Н. В. К вопросу о правосубъектности и правовом развитии искусственного интеллекта // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4. Государство и право: Реферативный журнал. 2021. С. 25.

[7] Роботы в законе. Должен ли искусственный интеллект отвечать за свои проступки // Официальный сайт НИУ «Высшая школа экономики». [Электронный ресурс]. URL: https://issek.hse.ru/news/227178200.html (дата обращения: 11.05.2023).

[8] Роботы в законе. Должен ли искусственный интеллект отвечать за свои проступки // Официальный сайт НИУ «Высшая школа экономики». [Электронный ресурс]. URL: https://issek.hse.ru/news/227178200.html (дата обращения: 11.05.2023).

февраля 2017 года № 2015/2103 «Нормы гражданского права о робототехнике» заключает, что «наиболее сложно организованные автономные работы могут наделяться статусом электронных лиц и нести ответственность за причинённый ими ущерб»[9]. Концепция «электронного лица» является принципиально новым пониманием, в связи с чем в науке ещё не сформулирован единый подход к такому правовому статусу. Наиболее верным представляется понимание «электронного лица» как юридической фикции, предполагающей наделение технологии ИИ специфическими правами, обязанностями, гарантиями, не свойственными для правовых статусов физических и юридических лиц.

Полагаем, что интеллектуальные системы необходимо рассматривать исключительно в качестве объекта правоотношений. Остальные подходы представляются нам нецелесообразными и недопустимыми в условиях современного развития общественных отношений.

Вопрос определения правовой охраны объектов интеллектуальной деятельности, созданных интеллектуальными системами, не может быть разрешён без рассмотрения деликтоспособности ИИ.

П. М. Морхат отмечает, что существует два подхода к установлению ответственности юнитов искусственного интеллекта:

– установление непосредственной ответственности за свои действия,

– установление ответственности третьих лиц за их действия[10].

На сегодняшний день уровень развития интеллектуальных систем не позволяет говорить о том, что они принимают решения самостоятельно, так как наделены ограниченными правами для достижения конкретных целей, установленных разработчиком программного обеспечения. Опираясь на это обстоятельство, обозначим, что российское законодательство и правоприменительная практика на данном этапе основывается на втором подходе.

Учитывая вышеуказанные обстоятельства, представляется, что машиноцентричный концепт на сегодняшний день не может быть выбран в качестве основополагающего для обеспечения защиты интеллектуальной собственности, созданной юнитами искусственного интеллекта.

Несмотря на то, что право интеллектуальной собственности направлено на защиту результатов интеллектуальной деятельности человека, а юниты ИИ не признаются

[9] European Parliament. REPORT with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL)). Debates, 15 February 2017. // European Parliament. [Электронный ресурс]. URL: http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20170215&secondRef=ITEM-014&language=EN&ring =A8– 2017–0005 (дата обращения: 11.05.2023).

[10] Морхат П. М. Правосубъектность юнитов искусственного интеллекта и ответственность за их действия // Право и государство: теория и практика. 2017. № 11 (155). С. 33–34.

субъектами в привычном понимании, современные методы анализа и машинного обучения позволяют создать программы, функционирующие автономно от разработчика. В таком случае применение концепта служебного произведения и концепта гибридного авторства недопустимо: объекты создаются не по заданию пользователя, совместный вклад отсутствует.

Говоря о концепции «нулевого авторства», следует вспомнить об основном назначении интеллектуальных прав – получение экономической выгоды для правообладателей произведений. Переход таких объектов в общественное достояние не позволит достичь указанной цели, а также станет причиной торможения в технологическом развитии общества и государства в целом, ввиду потери компаниями-разработчиками материального интереса к осуществляемой новаторской деятельности.

Наиболее подходящим представляется антропоцентричный концепт, в соответствии с которым правообладателем произведения, созданного интеллектуальной системой, является третье лицо – пользователь, разработчик или владелец.

По нашему мнению, исключительное право на результат интеллектуальной деятельности должно принадлежать владельцу или пользователю такой машинной технологии. Как отмечается в профессиональном сообществе[11], даже совершенному ИИ необходим человек для надлежащего обеспечения деятельности, координации действий и регулярного технического и программного обслуживания. Такой подход позволит не только надлежащим образом защитить интеллектуальную собственность, созданную искусственным интеллектом, но и обеспечить развитие инноваций, а, значит, и экономический рост государства.

В заключение необходимо подчеркнуть, что в условиях цифровизации многие сферы деятельности человека трансформируются, изменения затрагивают в том числе и право интеллектуальной собственности. В связи со стремительным развитием общественных отношений в гражданском законодательстве существует пробел, связанный с определением правообладателя объекта, созданного исключительно интеллектуальной системой. Принимая во внимание обстоятельства, обозначаемые в теории и практике права интеллектуальной собственности, нам представляется важным внести изменение в ГК РФ – признать правообладателем владельца или пользователя интеллектуальной системы. Рассматриваемый подход является универсальным, при этом обеспечивая достаточную свободу участникам гражданских правоотношений и стимулируя развитие новейших технологий.

[11] Борьба за ИИ-кадры: сложности поиска специалистов в России // Ict.Moscow. [Электронный ресурс]. URL: https://ict.moscow/news/ai-talents/ (дата обращения: 11.05.2023).

Список литературы

1. Джикаева Ф. А., Лолаева А. С. Понятие и признаки интеллектуальной собственности // Аграрное и земельное право. 2020. № 9 (189). С. 14–18.

2. Крысанова Н. В. К вопросу о правосубъектности и правовом развитии искусственного интеллекта // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4. Государство и право: Реферативный журнал. 2021. С. 23–31.

3. Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: дисс. … д-ра юрид. наук. Москва, 2019. 420 с.

4. Морхат П. М. Правосубъектность юнитов искусственного интеллекта и ответственность за их действия // Право и государство: теория и практика. 2017. № 11 (155). С. 30–36.

Lidia A. Smirnova
Student of the Faculty of Law,
National Research University of Nizhny Novgorod
named after N. I. Lobachevsky
(Nizhny Novgorod, Russian Federation)
lida_smirnova_a@mail.ru

Scientific Supervisor: Alexander K. Baldin
PhD in Law, Associate Professor,
Associate Professor of the Department of Civil Law and Procedure,
Faculty of Law of the National Research University of Nizhny Novgorod
named after N. I. Lobachevsky
(Nizhny Novgorod, Russian Federation)
akbaldin@unn.ru

LEGAL PROTECTION OF INTELLECTUAL PROPERTY CREATED BY ARTIFICIAL INTELLIGENCE

Abstract. the article explores the legal protection of the results of intellectual activity created by intelligent systems. The author analyzes intellectual rights, their main features, and also considers regimes of legal regulation of intellectual property rights and approaches to the definition of legal personality of artificial intelligence. Proposals for improving the legal protection of the results of intellectual activity, created by artificial intelligence units are made in the framework of the article.

Keywords: Civil Code of the Russian Federation, artificial intelligence, legal personality, results of intellectual activity, intellectual property.

УДК 340

Тимофеева Римма Ивановна
Студент Института Юстиции
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
rimmatimofeeva2003@mail.ru

Научный руководитель: Окулич Анастасия Ивановна,
ассистент кафедры конституционного права
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
a.i.okulich@usla.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РОЛИ СУДЬИ: УТОПИЯ ИЛИ СПОСОБ ДОСТИЖЕНИЯ КОНСТИТУЦИОННОГО ПРИНЦИПА СПРАВЕДЛИВОСТИ?

Аннотация. В данной статье рассматриваются различные точки зрения как отечественных, так и зарубежных учёных по поводу возможности замены искусственным интеллектом судьи-человека. В итоге своих рассуждений автор статьи приходит к выводу, что судебные решения, вынесенные машиной, будут лишены человеческой составляющей, поэтому данная идея будет являться утопией и уж точно не поспособствует достижению справедливости.

Ключевые слова: искусственный интеллект, судья, судебные решения, справедливость.

Для цитирования:
Тимофеева Р. И. Искусственный интеллект в роли судьи: утопия или способ достижения конституционного принципа справедливости // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 424–429.

В наше время показатели уважения и доверия к судебной системе со стороны граждан РФ находятся на достаточно низком уровне[1]. В глазах народа судьи должны олицетворять справедливость, но на деле это отнюдь не всегда происходит. Для того, чтобы поднять авторитет судебной власти в стране, необходимо обеспечить реальные гарантии

[1] Отношение россиян к судебной системе (по материалам всероссийского опроса 2020) // Независимый исследовательский центр [Электронный ресурс]. 2020, 17 февраля. URL: http://исследовательский-центр.рф/otnoshenie-rossiyan-k-sudebnoj-sisteme-po-materialam-vserossijskogo-oprosa/ (дата обращения: 11.05.2023).

судебной защиты для граждан. Но возможно ли достижение принципа справедливости при реализации данного права посредством внедрения искусственного интеллекта в судебную систему РФ вместо судьи-человека?

Для начала, хотелось бы обозначить, что включает в себя понятие “искусственный интеллект”. В российском праве его легальное определение закреплено в Указе Президента РФ от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации"[2]. Согласно подп. ”а” п. 5 данного Указа, под искусственным интеллектом понимается “комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека”. То есть, исходя из данного определения, мы видим, что искусственный интеллект по своей сути призван заменить человека в определённых сферах деятельности, а значит, рассуждения о нём в судебной сфере будут также уместны, поскольку и по сей день ведутся различные научные дискуссии по данной теме.

Среди учёных-исследователей нет общего мнения о возможности замены искусственным интеллектом судью-человека. К примеру, Н. В. Антонова, С. Б. Бальхаева, Ж. А. Гаунова считают, что роботизация судейского корпуса, помощников судей и секретарей судебных заседаний считается одной из тенденций цифровизации судебной системы[3]. Однако в науке есть и противоположная точка зрения. В частности, В. В. Котлярова считает, что искусственный интеллект не сможет по своему внутреннему убеждению объективно, беспристрастно и полно оценивать доказательства, чтобы вынести справедливое решение, как это сделает живой судья[4].

По мнению Судьи Конституционного Суда РФ Г. А. Гаджиева, “роботы не способны принимать решения, которые принимает суд. Ведь в суде происходит не только применение правовых норм, но и во многих случаях большее влияние имеет экономическая эффективность или этическая составляющая»[5]. Действительно, заложить в машину то, что по своей социальной природе свойственно

---

[2] О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10 октября 2019 г. № 490 // Собрание законодательства РФ. 2019. №41. Ст. 5700.

[3] Тихомиров Ю. А., Антонова Н. В., Бальхаева С. Б., Гаунова Ж. А. Юридическая концепция роботизации: монография. М.: Проспект. 2019, 240 с.

[4] Котлярова В. В. К вопросу о цифровизации процесса отправления правосудия // Арбитражный и гражданский процесс. 2019. № 12. С. 46–49.

[5] Гаджиев Г. Судья КС предсказал будущее роботов в юриспруденции // Лента.ру [Электронный ресурс]. 2017, 15 мая. URL: https://m.lenta.ru/news/2017/05/15/robojudge/?utm_source=lentatw&utm_medium=social&utm camзaign=sudya-ks-predskazal-buduschee-robotov-v-yur (дата обращения: 05.05.2023).

только человеку, наверное, невозможно.

Кроме того, у искусственного интеллекта не может быть таких качеств, как сочувствие, милосердие, мудрость, справедливость, эмпатия. Однако, с другой стороны, данная черта может также вызвать у людей доверие, поскольку они будут уверены, что суд останется максимально объективным, не станет отдавать предпочтение той стороне, на которой окажется его приятель, товарищ или друг, более привлекательной внешности человек или человек, относительно пола, расы, нации или религии которого у судьи будут сформированы стереотипы. Сторонники использования искусственного интеллекта отмечают, что, в отличие от людей, машине не присущи предубеждения. Однако учёный А. Моррисон, вместе с тем, описывает ряд примеров того, как действия алгоритмов приводили к результату, отражающему необъективность создавших их людей[6].

Действительно, способность машины мгновенно находить и применять нормы права позволяет сделать процесс правосудия более быстрым и эффективным за счёт автоматизации судопроизводства. В свою очередь, чем быстрее правосудие, тем оно более доступно для граждан, поскольку стороны судебного процесса смогут своевременно получить компенсации по своим искам. Это действительно большой плюс, поскольку всем нам известно, какая нагрузка возлагается на судей.

Многие люди ошибочно считают, что при автоматизированном рассмотрении дел ответственность за принятые судебные решения будет нести машина, а не человек, поскольку искусственный интеллект обладает чем-то вроде разума. Однако это далеко не так. Произведения человеческого разума остаются собственностью того, кто их придумал[7]. А значит, и ответственность за принятые решения будут нести те люди, которые запрограммировали эту машину. И тогда возникает вопрос: целесообразно ли будет привлекать программистов к ответственности за вынесенные искусственным интеллектом судебные решения? Мы считаем, что нет: в противном случае, нужно искать судью-программиста, а в наше время найти компетентных в данной области людей, которые бы обладали существенным багажом знаний как в юриспруденции, так и в сфере IT, очень затруднительно.

Также, говоря о плюсах, использование искусственного интеллекта сможет поспособствовать снижению уровня коррупции в судебной системе. Однако важно понимать, что программы создаются такими же людьми, которые могут быть и корыстными, и пристрастными,

[6] Morrison A. Artificial intelligence in the courtroom. Increasing or decreasing access to justice? // International Journal of Online Dispute Resolution. 2020. Vol. 6. № 1. Pp. 76–93.

[7] Кравчук Н. В. Искусственный интеллект как судья: Перспективы и опасения // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4: Государство и право. 2021. № 1. С. 115–122.

так что создатели искусственных интеллектуальных систем также подвержены коррупции, как и обычные судьи, поскольку они тоже люди. Поэтому созданные ими программы с точки зрения справедливости нельзя с уверенностью назвать эффективными.

Также хотелось бы отметить, что искусственный интеллект не способен учитывать человеческие ценности в процессе принятия решений по делу. Судебные решения, созданные машиной, возможно, и будут максимально объективными и беспристрастными, однако они будут лишены человечности. Для наглядности, обратимся к сфере гражданского права: вопрос определения судом размера компенсации морального вреда носит оценочный характер. Так, согласно п. 2 ст. 1101 ГК РФ, при определении размера компенсации морального вреда должны учитываться требования разумности и справедливости. Характер физических и нравственных страданий оценивается судом с учётом фактических обстоятельств, при которых был причинён моральный вред, и индивидуальных особенностей потерпевшего[8]. Уже исходя из содержания данной нормы, можно увидеть, насколько проблематично это будет осуществить искусственному интеллекту.

С другой стороны, если алгоритм отражает ценности тех, кто его создаёт, то он будет отражать и его положительные черты. Встаёт вопрос, кто будет тем человеком, чьи ценности будут реализованы компьютером. Если это судья, то, вероятно, каждый судья должен участвовать в программировании, поскольку речь идёт в том числе о толковании права, индивидуальном процессе, в котором общий алгоритм неприемлем[6].

Также важно отметить, что в компьютере отсутствует гибкость, присущая человеческому сознанию, разрешение им дел возможно только в той степени, в которой разработчик предусмотрел и заложил в алгоритм дело со схожими фактами. Предусмотреть и запрограммировать всё многообразие дел, которое может возникнуть в реальности, будет крайне сложно, если в принципе возможно.

При бесспорности преимуществ искусственного интеллекта в разных сферах, его использование в качестве судьи должно рассматриваться с осторожностью. При всей своей уязвимости, именно человек обладает уникальной способностью выносить решения. На наш взгляд, целесообразнее будет говорить об использовании элементов искусственного интеллекта, что сможет помочь судье повысить эффективность в отправлении правосудия, то есть он должен использоваться в качестве вспомогательного инструмента. Такого рода программы, наделённые искусственным интеллектом, могут составлять судебные акты, осуществлять проверку и обеспечение представления надлежащим образом претензий сторон, осуществлять оценку хода дела, автоматически

[8] Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 01.07.2021, с изм. от 08.07.2021) // Собрание законодательства РФ. 1996. № 5. Ст. 1101.

проверять доказательства и ходатайства сторон.

То есть внедрение искусственного интеллекта именно в судебное делопроизводство было бы очень хорошей идеей, но именно в качестве помощника судьи. Функции судьи, как мы считаем, всё-таки должны осуществляться человеком, поскольку судьбу человека не должна решать машина, которая не способна к эмпатии, сочувствию, пониманию и сопереживанию.

Для наглядности приведём пример из сферы уголовного права. Перед тем, как суд назначает наказание подсудимому, он анализирует его поведение и образ жизни, положение потерпевшего, внимательно слушает свидетелей, обращает внимание на их поведение, на взаимоотношения между участниками судебного процесса. В конце концов, для того, чтобы судья индивидуализировал наказание подсудимому, он должен учесть его семейное, материальное положение, возраст, здоровье и другие факторы.

Искусственный интеллект действительно способен оперировать достаточно большими (нежели судья-человек) объёмами данных из архивов судебных дел и справочных правовых систем, может быстро обрабатывать информацию и учитывать значительно больше факторов, чем судья-человек[9].

Программы искусственного интеллекта действительно могут применяться в качестве вспомогательного элемента в судебной системе, но не более того. Поэтому использование искусственного интеллекта вместо профессионального судьи-человека, скорее всего, будет являться утопией, нежели достижением конституционного принципа справедливости.

Список литературы

1. Колесникова Л. В. Перспективы внедрения электронного судьи и электронного помощника судьи в уголовное судопроизводство // Развитие правосудия и современные технологии (наука и практика). К 15-летию Четвёртого арбитражного апелляционного суда: Сборник материалов национальной научно-практической конференции, Чита, 22 сентября 2021 года. Чита: Забайкальский государственный университет, 2021. С. 34–37.

2. Котлярова В. В. К вопросу о цифровизации процесса отправления правосудия // Арбитражный и гражданский процесс. 2019. № 12. С. 46–49.

3. Кравчук Н. В. Искусственный интеллект как судья: Перспективы и опасения // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4: Государство и право. 2021. № 1. С. 115–122.

[9] Колесникова Л. В. Перспективы внедрения электронного судьи и электронного помощника судьи в уголовное судопроизводство // Развитие правосудия и современные технологии (наука и практика). К 15-летию Четвертого арбитражного апелляционного суда: Сборник материалов национальной научно-практической конференции, Чита, 22 сентября 2021 года. Чита: Забайкальский государственный университет, 2021. С. 34–37.

4. Тихомиров Ю. А., Антонова Н. В., Бальхаева С. Б., Гаунова Ж. А. Юридическая концепция роботизации: монография. М.: Проспект. 2019, 240 с.

5. Morrison A. Artificial intelligence in the courtroom. Increasing or decreasing access to justice? // International Journal of Online Dispute Resolution. 2020. Vol. 6. № 1. Pp. 76–93.

Rimma I. Timofeeva
2nd year undergraduate student of the Institute of Justice
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
rimmatimofeeva2003@mail.ru

Scientific Supervisor: Anastasia I. Okulich,
Assistant of the Constitutional Law Department
Ural State Law University
named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
a.i.okulich@usla.ru

ARTIFICIAL INTELLIGENCE AS A JUDGE: UTOPIA OR A WAY TO ACHIVE THE CONSTITUTIONAL PRINCIPLE OF JUSTICE?

Abstract. This article discusses various points of view of both domestic and foreign scientists about the possibility of replacing a human judge with artificial intelligence. As a result of his reasoning, the author of the article comes to the conclusion that judicial decisions made by a machine will be devoid of a human component, therefore this idea will be a utopia and certainly will not contribute to achieving justice.

Keywords: artificial intelligence, judge, machine, human, judicial decisions, justice.

УДК 343.98

Туркина Диана Андреевна
Студент Института государственного и международного права,
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
turkina.di@mail.ru

Сафронова Екатерина Владимировна
Студент Института государственного и международного права,
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
Katia.safronowa@yandex.ru

Научный руководитель: Рачева Нелли Витальевна,
кандидат юридических наук, доцент,
доцент кафедры криминалистики
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
ekaterinburgg@mail.ru

К ВОПРОСУ О ЦИФРОВОМ АЛИБИ В КРИМИНАЛИСТИКЕ

Аннотация. В статье рассматривается понятие «цифровое алиби», особенности его проверки при расследовании преступлений. Анализируется сложность работы с цифровыми доказательствами, а также возможности фальсификации цифрового алиби, выявленные зарубежными исследователями. Дана оценка перспективам развития цифрового алиби в Российской Федерации.

Ключевые слова: цифровое алиби, цифровые доказательства, проверка цифрового алиби, цифровая информация, цифровые следы.

Для цитирования:
Туркина Д. А., Сафронова Е. В. К вопросу о цифровом алиби в криминалистике // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 430–438.

Информатизация является глобальным процессом во всём мире, проникая в различные сферы жизнедеятельности человека. Данный процесс не обошёл стороной и деятельность правоохранительных органов. Появилось достаточно много различных направлений информатизации следственной деятельности, к примеру,

компьютерная экспертиза, использование систем видео-конференц-связи, использование автоматизированных систем[1] (АИРС «ПОРТРЕТ», «Бинар-3», «САУД-М»). В данной статье исследуется цифровое алиби – одно из новых направлений информатизации, статус которого ещё не определён до конца.

При расследовании преступлений субъекты нередко выдвигают алиби. Данное понятие получило закрепление в статье 5 Уголовно-процессуального кодекса Российской Федерации[2] (далее – УПК РФ), где под ним понимается «нахождение подозреваемого или обвиняемого в момент совершения преступления в другом месте». Однако многие учёные, одним из которых является О. Н. Алексиенко, считают, что законодательная дефиниция «алиби» даётся в узком смысле слова[3], и предлагают свою интерпретацию данного понятия, которую, по мнению учёного, нужно внести в часть 1 статьи 5 УПК РФ, изложив её в следующей редакции: «алиби – факт, влекущий отказ от уголовного преследования невиновного лица, которое в момент совершения преступления находилось в другом месте». М. И. Николаева под алиби понимает «подлежащий проверке довод либо факт, который установлен следствием или судом, свидетельствующий о нахождении подозреваемого или обвиняемого во время совершения преступления в ином месте, что может доказывать его невиновность»[4]. А. Т. Тимербаев в учебном пособии «Тактика проверки заявления об алиби на предварительном следствии» писал: «Заявление об алиби – это подлежащий проверке довод подозреваемого или обвиняемого (подсудимого) о том, что данное лицо во время совершения преступления находилось в другом месте и поэтому оно не причастно к расследуемому преступлению»[5].

В настоящее время появилось новое понятие – цифровое алиби. Как пишет И. П. Пономарёв, под термином «цифровое алиби следует понимать факт непосредственного взаимодействия подозреваемого (обвиняемого) в момент совершения преступления с электронной системой, находящейся в другом месте»[6]. В таких ситуациях деятельность субъекта

---

[1] Бычкова В. А. Элементы информатизации следственной деятельности // Электронный сборник трудов молодых специалистов Полоцкого государственного университета / Полоцкий государственный университет; ред. кол.: Д. Н. Лазовский (пред.). 2018. Вып. 22 (92): Юридические науки. С. 276.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Российская газета. 2001. № 249.

[3] Алексиенко О. Н. Криминалистические методы разоблачения ложного алиби по делам о преступлениях против жизни и здоровья: автореферат дис. ... канд. юрид. наук. Ростов-на-Дону, 2009. С. 8.

[4] Николаева М. И. Алиби: уголовно-процессуальный и криминалистический аспекты: автореф. дис. ... канд. юрид. Наук. М., 2005. С. 14

[5] Тимербаев А. Т., Сердюк Л. В. Тактика проверки заявления об алиби на предварительном следствии: Учебное пособие. Хабаровск: Хабаровская высшая школа МВД СССР, 1987. С. 5.

[6] Пономарев И. П. Цифровое алиби и его проверка // Вестник Воронежского государственного университета. Серия: право. 2011. № 3. С. 444.

непосредственно связана с использованием какого-либо устройства в интересующее следствие время, а основным источником доказательств с позиции субъекта преступления будет выступать информация, записанная в цифровой форме на машинном носителе[7].

Digital alibi (цифровое алиби) впервые появилось за рубежом и пользуется популярностью в западных странах. Так, 13 августа 2007 года в коммуне Италии – Гарласко была убита Кьяра Поджи. Подозреваемым по делу был признан её парень – Альберто Стази. Подозреваемый утверждал, что в ночь убийства он был у себя дома и работал над дипломным проектом за ноутбуком. На следующий день после убийства Альберто добровольно передал свой ноутбук полиции для проверки своего алиби. После проверки полицией выяснилось, что 13 августа 2007 года ноутбук был включён 7 раз, вставлялось несколько USB-дисков, файлы с дипломным проектом открывались много раз. Следует отметить, что сотрудники полиции, которые занимались проверкой алиби подозреваемого, не были экспертами и не располагали специальными знаниями в области информационных технологий. После проведения проверки, подозрения с Альберто Стази были сняты. Однако данным делом в 2011 году заинтересовались специалисты по цифровым доказательствам – доктор Порт и доктор Окетти. Они провели экспертизу, в результате которой была выявлена совершенно другая информация: произведён доступ к более чем 39 000 документам, изменено более 500 файлов, изменены метаданные дипломного проекта, создано более 500 новых файлов[8]. Альберто, прежде чем отдать ноутбук на проверку полиции, изменил все данные, вследствие этого первоначальная проверка сотрудниками полиции являлась ошибочной. Таким образом, «дело Гарласко» послужило толчком для многих учёных в области исследования цифрового алиби. Судебный процесс по данному делу выявил проблему границы между надлежащим образом полученными неизменёнными цифровыми данными как средством доказательства.

Ещё одним примером использования цифрового алиби за рубежом является дело об ограблении, произошедшем в 2009 году в Нью-Йорке. Родни Брэдфорду было предъявлено обвинение в вооружённом ограблении. Но дело прекратили, поскольку цифровые доказательства показали, что он активно использовал свою учётную запись Facebook во время преступления. В 11:49 утра в субботу, 17 октября 2009 года, когда Брэдфорд обновлял свой статус в Facebook в доме своего отца, в 12 милях от его местонахождения, двое мужчин были ограблены. Адвокат отметил, что цифровые доказательства обеспечили

[7] Иванов Н. А. Применение специальных познаний при проверке «цифрового алиби» // Информационное право. 2006. № 4. С. 32.

[8] Colombo E. The Garlasco case and the digital alibi evidence: a difficult relationship between law and informatics // Digital evidence and electronic signature law review. 2017. Vol. 14. Pp. 31–38 DOI 10.14296/deeslr.v14i0.2452.

Брэдфорду «непревзойдённое алиби»[9]. Однако не было доказано, что именно Родни пользовался своей учётной записью, поскольку компьютером могли пользоваться также и другие члены его семьи.

Возникает вопрос о том, насколько допустимо рассматривать цифровое алиби в качестве цифрового доказательства. Понятие «доказательство» дано в статье 74 УПК РФ, где под ним понимаются любые сведения, на основе которых уполномоченные лица устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию, а также иных обстоятельств, имеющих значение для уголовного дела.

С понятием «цифровые доказательства» коррелирует понятие «цифровая информация». Цифровая информация – информация в цифровой форме, которая записывается, обрабатывается (изменяется), сохраняется и (или) передаётся через электронные носители. Д. В. Бахтеев считает, что название информации «цифровой» вполне оправданно в силу особенностей её хранения, которое осуществляется в зашифрованном, т. е. цифровом, виде[10]. В части 2 статьи 74 УПК РФ указано то, что допускается в качестве доказательств. В. А. Новицкий и Л. Ю. Новицкая относят цифровые доказательства к «иным документам»[11]. Действительно, согласно части 2 статьи 84 УПК РФ «документы могут содержать сведения, зафиксированные как в письменном, так и в ином виде. К ним могут относиться материалы фото- и киносъёмки, аудио- и видеозаписи и иные носители информации, полученные, истребованные или представленные в порядке, установленном статьёй 86 настоящего Кодекса». Статья 86 УПК РФ устанавливает порядок собирания доказательств. Доказательства должны быть собраны путём производства следственных и иных процессуальных действий. Таким образом, как пишут многие российские и зарубежные исследователи, цифровое алиби как цифровое доказательство должно считаться релевантным только в том случае, если оно подтверждается доказательствами, собранными с использованием традиционных методов расследования.

В связи с тем, что мы имеем дело с техническими устройствами, действия следователя также будут направлены на установление конкретного факта, а также на обнаружение и проверку цифровых следов. Цифровые следы отражают любое изменение состояния автоматизированной информационной системы и касаются удаления, внесения изменений, включения,

[9] De Santis A., Castiglione A., Cattaneo G., De Maio G., Ianulardo M. Automated Construction of a False Digital Alibi. // Availability, Reliability and Security for Business, Enterprise and Health Information Systems. 2011. Pp. 359–373 DOI 10.1007/978-3-642-23300-5_28.

[10] Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. 2019. № 6 (129). С. 62.

[11] Новицкий В. А., Новицкая Л. Ю. Понятие и виды цифровых доказательств // Ленинградский юридический журнал. 2019. № 1 (55). С. 216.

открывания, создания информации на компьютере и других гаджетов.

Д. В. Бахтеев и Е. В. Смахтин выделяют классификацию цифровых следов по следующим основаниям. Во-первых, по форме носителя различают следы, расположенные на оптических носителях (CD, DVD), полупроводниковых носителях (флеш-накопители) и магнитные носители (жёсткие диски). Во-вторых, по способу доступа к следам – локальный (доступ осуществляется непосредственно через устройство, на котором находятся цифровые следы) или удалённый (доступ возможен через подключение к телекоммуникационным сетям). В-третьих, по характеру доступа следы могут быть доступными, зашифрованными (доступ заблокирован с помощью паролей), скрытыми (скрытые файлы). В-четвёртых, по характеру происхождения следы дифференцируются на оставленные человеком непосредственно (записи в социальных сетях) и опосредованно (данные телеметрии). В-пятых, по месту нахождения выделяют следы, физически находящиеся на компьютерных устройствах преступника, потерпевшего, сторонних лиц[12].

Для проверки цифрового алиби следователю необходимо установить информацию о полных действиях, которые совершал подозреваемый или обвиняемый на устройстве. Для этого следует подробно допросить лицо, чтобы узнать во сколько был включён и выключен компьютер, создавались ли новые файлы, с какими файлами, программами он работал, была ли скопирована информация с компьютера на другие электронные носители, распечатывались ли документы, задействовалась ли при работе глобальная сеть «Интернет», какие именно ресурсы были использованы[13]. Для проверки действий производится выемка и осмотр устройства-источника информации, назначается судебная информационно-компьютерная экспертиза, которая позволит получить информацию, зафиксированную на материальном носителе. Данная экспертиза направлена на установление свойств и состояния информации до её удаления или модификации, а также условий, при которых была создана (изменена, удалена) информация. С помощью данной экспертизы следователь может выявить следы работы программ и приложений, определить транзакции, совершённые посредством информационных сетей, а также отследить деятельность и намерения пользователя компьютера.

Перед экспертом можно поставить следующие вопросы:

1) Является ли представленный компьютер (аппаратное средство) носителем информации?

[12] Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. 2019. № 6 (129). С. 67.

[13] Рудакова С. В. Цифровое алиби и цифровые доказательства // Юридический вестник Кубанского государственного университета. 2019. № 1. С. 57.

2) Доступен ли для чтения представленный носитель информации?

3) Имеются ли на представленном носителе данные о том, что пользователь работал на компьютере в указанный момент времени и даты?

4) С какими файлами / программами работал пользователь?

5) Каким было место нахождения персонального компьютера в определённый момент времени? и др.

Результатом проведения экспертизы может быть не только подтверждение слов подозреваемого (обвиняемого), но и опровержение цифрового алиби.

Следует иметь ввиду, что существует возможность фальсификации цифрового алиби посредством перевода компьютерных часов, использования планировщика событий, когда компьютер программируют с целью выполнения конкретного действия в определённое время и др.

Многие зарубежные исследователи в своих работах подчёркивают возможность создания ложного цифрового алиби полностью автоматическим способом без какого-либо вмешательства человека. Кроме того, экспертиза не может установить, были ли такие следы получены в результате деятельности человека или с помощью автоматизированного инструмента, поскольку за рубежом существуют различные платформы создания ложного алиби (например, AutoIt), которые моделируют реальные действия пользователя, то есть имитируют просмотр, отправку электронной почты, общение в чате, редактирование документа.

При проверке цифрового алиби нужно помнить о том, что связь с конкретным лицом зависит непосредственно от типа устройства. Так, подозреваемый может заявить, что только он имел доступ к своему компьютеру, именно он со своей учётной записи в социальной сети отправлял сообщения. К сожалению, ответы на такие вопросы судебная информационно-компьютерная экспертиза дать не может.

Цифровые следы также обладают высокой скоростью трансформации, в связи с чем существует угроза потери хранящейся информации (например, вследствие неправильных действий следователя). В связи с этим, при осмотре и изъятии электронных устройств, необходимо привлекать специалистов. Кроме того, доказательственная информация цифрового алиби недоступна для непосредственного личного восприятия без специального извлечения с помощью технических средств. По мнению Д. В. Бахтеева и Е. В. Смахтина, сложность заключается в том, что обеспечить участие специалиста во всех случаях изъятия такой информации практически невозможно прежде всего в силу отсутствия достаточного количества специалистов в области IT-технологий[14].

[14] Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. 2019. № 6 (129). С. 64.

Следует отметить, что при проверке цифрового алиби необходимо подтвердить факт нахождения электронного устройства в территориально отдалённом месте, а также факт взаимодействия с таким устройством лица, который заявляет о своём алиби. В данном случае необходимо получить показания свидетелей и изъять следы рук человека с клавиатуры компьютера и компьютерной мыши, которые могут идентифицировать конкретного пользователя. Однако, установить точное время оставления следов рук лица, которое постоянного работает на данном устройстве, невозможно. Кроме того, можно обнаружить следы рук, оставленные другим человеком. Это должно насторожить следователя, поскольку подозреваемый (обвиняемый), как правило, утверждает, что никто больше не имел доступа к его персональному устройству.

Цифровое алиби вряд ли будет иметь широкие перспективы в России. Цифровая доказательственная информация является крайне неустойчивой, проверка и разоблачение цифрового алиби осуществляются с помощью производства других следственных действий (осмотра места происшествия, допроса свидетелей, подозреваемого (обвиняемого), выемки и осмотра электронных носителей информации, назначения экспертиз и др.) и оперативно-розыскных мероприятий[15] (получение компьютерной информации, опрос, сбор образцов для сравнительного исследования). Такой комплексный подход поможет проверить заявленное субъектом цифровое алиби и в дальнейшем изобличить, если оно не подтвердилось.

Список литературы

1. Алексиенко О. Н. Криминалистические методы разоблачения ложного алиби по делам о преступлениях против жизни и здоровья: автореферат дис. ... канд. юрид. наук. Ростов-на-Дону, 2009. 23 с.

2. Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. 2019. № 6 (129). С. 61–68.

3. Бычкова В. А. Элементы информатизации следственной деятельности // Электронный сборник трудов молодых специалистов Полоцкого государственного университета / Полоцкий государственный университет; ред. кол.: Д. Н. Лазовский (пред.). 2018. Вып. 22 (92): Юридические науки. С. 276–278.

4. Иванов Н. А. Применение специальных познаний при проверке «цифрового алиби» // Информационное право. 2006. № 4. С. 31–34.

5. Николаева М. И. Алиби: уголовно-процессуальный и криминалистический аспекты: автореф. дис. ... канд. юрид. наук. М., 2005. 26 с.

[15] Смушкин А. Б. К вопросу о «цифровом алиби» в криминалистике // Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2019. № 2 (14). С. 29.

6. Новицкий В. А., Новицкая Л. Ю. Понятие и виды цифровых доказательств // Ленинградский юридический журнал. 2019. №1 (55). С. 213–220.

7. Пономарев И. П. Цифровое алиби и его проверка // Вестник Воронежского государственного университета. Серия: право. 2011. № 3. С. 437–444.

8. Рудакова С. В. Цифровое алиби и цифровые доказательства // Юридический вестник Кубанского государственного университета. 2019. № 1. С. 56–59.

9. Смушкин А. Б. К вопросу о «цифровом алиби» в криминалистике // Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2019. № 2 (14). С. 28–33.

10. Тимербаев А. Т., Сердюк Л. В. Тактика проверки заявления об алиби на предварительном следствии: Учебное пособие. Хабаровск: Хабаровская высшая школа МВД СССР, 1987. 62 с.

11. De Santis A., Castiglione A., Cattaneo G., De Maio G., Ianulardo M. Automated Construction of a False Digital Alibi. // Availability, Reliability and Security for Business, Enterprise and Health Information Systems. 2011. Pp. 359–373 DOI 10.1007/978-3-642-23300-5_28.

12. Colombo E. The Garlasco case and the digital alibi evidence: a difficult relationship between law and informatics // Digital evidence and electronic signature law review. 2017. Vol. 14. Pp. 31–38 DOI 10.14296/deeslr.v14i0.2452.

Diana A. Turkina
Student of the Institute of State and International Law
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
turkina.di@mail.ru

Ekaterina V. Safronova
Student of the Institute of State and International Law
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
Katia.safronowa@yandex.ru

Scientific Supervisor: Nelly V. Racheva,
PhD in Law, Associate Professor,
Associate Professor of the Department of Criminology
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
ekaterinburgg@mail.ru

ON THE QUESTION OF A DIGITAL ALIBI IN CRIMINALISTICS

Abstract. The article discusses the concept of "digital alibi", the features of its verification in the investigation of crimes. The complexity of working with digital evidence is analyzed, as well as the possibilities of falsifying a digital alibi identified by foreign researchers. The prospects for the development of digital alibi in the Russian Federation are assessed.

Keywords: digital alibi, digital evidence, digital alibi verification, digital information, digital traces.

УДК 347

Трутнева Екатерина Алексеевна
Магистрант
Казанский (Приволжский) федеральный университет
(г. Казань, Российская Федерация)
trutneva.lawyer@mail.ru

Научный руководитель: Михайлов Андрей Валерьевич
кандидат юридических наук, доцент,
заведующий кафедрой предпринимательского и энергетического права
Казанский (Приволжский) федеральный университет
(г. Казань, Российская Федерация)
avm@pravmail.ru

CHATGPT И ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ: КАК ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ПОМОГАЕТ ЗАЩИЩАТЬ АВТОРСКИЕ ПРАВА И ПАТЕНТЫ

Аннотация. Данная научно-юридическая статья рассматривает проблему защиты интеллектуальной собственности в эпоху цифровых технологий и роль искусственного интеллекта в усилении мер по защите авторских прав и патентов. Особое внимание уделено роли ChatGPT в защите интеллектуальной собственности, возможностям его использования в патентном поиске и анализе авторских прав, а также преимуществам его применения, рискам и ограничениям использования ChatGPT в защите интеллектуальной собственности.

Ключевые слова: искусственный интеллект, интеллектуальная собственность, инновационный инструмент, ChatGPT, цифровизация.

Для цитирования:
Трутнева Е. А. ChatGPT и интеллектуальная собственность: как искусственный интеллект помогает защищать авторские права и патенты // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 439–443.

Современный мир, насыщенный цифровыми технологиями, стал свидетелем резкого увеличения количества создаваемых и распространяемых в сети материалов, защита которых является задачей института интеллектуальной собственности. При этом следует учитывать, что охраняемые объекты интеллектуальной собственности могут существовать в различных формах и проявляться в самых разнообразных сферах деятельности, от научных исследований до художественного творчества, и каждый вид интеллектуальной собственности требует своего специфического подхода к защите прав

на него[1]. Таким образом, проблема защиты авторских прав и патентов становится всё более актуальной, особенно с учётом масштабов цифровой эры. Традиционные методы защиты уже не всегда позволяют достичь желаемого эффекта в новых условиях, поэтому необходимы новые решения и подходы. В этом контексте искусственный интеллект может стать мощным инструментом в усилении мер по защите интеллектуальной собственности, он способен предложить новые методы анализа и классификации данных, а также повысить скорость и точность обработки информации.

В данном контексте искусственный интеллект играет важную роль в усилении мер по защите авторских прав и патентов. Благодаря своим возможностям в области обработки и анализа данных, а также распознавания образов и текстов, искусственный интеллект способен эффективно обнаруживать нарушения авторских прав и помогать в их предотвращении.

В настоящее время защита интеллектуальной собственности становится всё более важной задачей в свете быстрого развития цифровых технологий и возросшего количества интернет-трафика. Существует множество традиционных методов защиты интеллектуальной собственности, включая регистрацию патентов и авторских прав, заключение лицензионных договоров, контроль за нарушением прав, а также судебное преследование нарушителей.

Регистрация патентов, являясь одним из наиболее распространённых методов защиты, позволяет обладателю патента получить монопольное право на изобретение, процесс или продукт, связанный с новыми технологиями или изобретениями.

Заключение лицензионных договоров даёт возможность обладателю прав предоставить третьей стороне право на использование своих технологий или изобретений в обмен на определённую плату.

Контроль за нарушением прав включает в себя мониторинг и преследование нарушителей прав, в том числе посредством отправки уведомлений о нарушении, заключения соглашений и судебного разбирательства.

В цифровой среде традиционные методы защиты интеллектуальной собственности (авторских прав и патентов) сталкиваются с рядом недостатков. Во-первых, цифровые технологии обеспечивают возможность создания и распространения копий защищённых материалов в неограниченном количестве, что приводит к незаконному использованию интеллектуальной собственности без разрешения правообладателя. Во-вторых, технологии распространения информации, такие как Интернет, делают практически невозможным контроль за нарушениями авторских прав и патентов. В-третьих, традиционные, в частности юридические, методы оказываются

[1] Митягин С. И. Интеллектуальная собственность и защита прав на нее // Юрист. 2016. № 10. С. 38.

неэффективными в отношении нарушителей из других стран, где законы о защите интеллектуальной собственности не так строги.

Например, оригинальный авторский текст может быть скопирован и изменён, чтобы создать новый текст, который уже не является защищаемым продуктом, но все ещё основан на оригинальном материале. Также могут быть использованы методы обхода технических средств защиты, таких как шифрование, что делает некоторые традиционные способы защиты бесполезными.

В связи с ростом числа объектов интеллектуальной собственности, которые могут быть скопированы или использованы незаконно, возникает необходимость в новых методах и технологиях для их защиты. В. Н. Григорьева утверждает, что проблемы с защитой авторских прав в цифровую эпоху всё ещё существуют и требуют дальнейшей работы и совершенствования, особенно с учётом быстрого развития технологий и появления новых способов нарушения прав авторов[2].

В этом контексте искусственный интеллект и, в частности, модель ChatGPT могут сыграть важную роль в защите авторских прав и патентов.

ChatGPT – это мощная система, обученная на огромном объёме текстовых материалов и способная генерировать тексты, которые подчас неотличимы от произведений, написанных людьми. Эта модель может быть использована для различных задач в области защиты интеллектуальной собственности, таких как:

1) Поиск и анализ патентов: ChatGPT может использоваться для анализа патентов и определения степени их оригинальности и новизны. Это может помочь в ускорении процесса выдачи патентов и сокращении времени, необходимого для их оценки и анализа.

2) Анализ авторских прав: ChatGPT может быть использован для анализа текстов на нарушение авторских прав, например, для поиска и обнаружения плагиата. Это может помочь компаниям и авторам защитить свои интеллектуальные права и предотвратить нарушения.

3) Генерация текстов для защиты интеллектуальной собственности: ChatGPT может использоваться для создания текстов, связанных с интеллектуальной собственностью, таких как патентные заявки, лицензионные соглашения и другие документы. Это может сократить время и усилить защиту интеллектуальной собственности.

Крупные компании уже используют модель ChatGPT в области интеллектуальной собственности. Например, компания Mastercard задействует её для поиска патентов и анализа их новизны и оригинальности, что позволяет компании получать патенты быстрее и усиливать защиту своей интеллектуальной собственности.

Однако, существуют определённые риски и ограничения при использовании ChatGPT, которые

[2] Григорьев В. Н. Защита авторских прав в цифровую эпоху: реалии и перспективы // Авторское право и интеллектуальная собственность. 2017. № 1. С. 62.

необходимо учитывать. Недостатки алгоритмов машинного обучения могут привести к возможным ошибкам в результатах анализа, что может повлечь за собой неверные выводы и решения. Например, ChatGPT может неправильно определить авторство текста, если автор использует схожие фразы и выражения с другим человеком. Это может привести к ошибочному приписыванию авторства или неправильной оценке нарушения авторских прав.

Возможные нарушения конфиденциальности могут возникнуть при обработке патентной и авторской информации, так как ChatGPT имеет доступ к большому объёму данных. Это может привести к утечке конфиденциальной информации, если не соблюдаются соответствующие меры защиты данных.

Также необходимо учитывать, что использование искусственного интеллекта в правовой сфере также вызывает ряд серьёзных вопросов, связанных с соответствием такого использования принципам правовой ответственности и справедливости[3]. Например, автоматические алгоритмы не всегда могут полностью заменить экспертов и юристов, их результаты могут быть оспорены в суде. Кроме того, законы и правила, регулирующие защиту интеллектуальной собственности, могут отличаться в разных странах, что также может ограничивать использование ChatGPT в некоторых ситуациях.

В этой связи следует согласиться с А. А. Левиным, который обращает наше внимание на необходимость разработки и совершенствования юридических инструментов и методов в части применения интеллектуальных систем для более эффективной защиты интеллектуальной собственности[4].

В заключение можно сделать вывод о том, что использование ChatGPT и других алгоритмов искусственного интеллекта может значительно усилить меры по защите интеллектуальной собственности. ChatGPT позволяет проводить более точный и быстрый анализ авторских прав и патентов, что снижает риски нарушений.

Однако, необходимо учитывать возможные риски и ограничения, связанные с использованием алгоритмов машинного обучения в данной области, такие как ошибки в результатах анализа, нарушения конфиденциальности и ограничения в использовании ChatGPT в правовых процессах.

Тем не менее, перспективы использования искусственного интеллекта в защите интеллектуальной собственности являются обнадёживающими, в связи с чем необходимо проводить дополнительные исследования и разработки в данной области. Особое внимание следует уделить разработке более точных и надёжных алгоритмов

[3] Петров М. Ю. Искусственный интеллект в праве: перспективы и риски // Российский юридический журнал. 2020. № 6. С. 60.

[4] Левин А. А. Юридические аспекты защиты результатов интеллектуальной деятельности с использованием методов машинного обучения // Интеллектуальная собственность в России. 2021. № 1. С. 70.

машинного обучения, которые смогут эффективно защищать права интеллектуальной собственности в цифровой среде.

Список литературы

1. Григорьев В. Н. Защита авторских прав в цифровую эпоху: реалии и перспективы // Авторское право и интеллектуальная собственность. 2017. № 1. С. 54–62.
2. Левин А. А. Юридические аспекты защиты результатов интеллектуальной деятельности с использованием методов машинного обучения // Интеллектуальная собственность в России. 2021. № 1. С. 62–70.
3. Митягин С. И. Интеллектуальная собственность и защита прав на нее // Юрист. 2016. № 10. С. 38–47.
4. Петров М. Ю. Искусственный интеллект в праве: перспективы и риски // Российский юридический журнал. 2020. № 6. С. 54–60.

Ekaterina A. Trutneva
Master's student, 1st year
Kazan (Volga Region) Federal University
(Kazan, Russian Federation)
trutneva.lawyer@mail.ru

Scientific Supervisor: Andrey V. Mikhailov
PhD in Law, Associate Professor,
Head of the Department of Business and Energy Law
Kazan (Volga Region) Federal University
(Kazan, Russian Federation)
avm@pravmail.ru

CHATGPT AND INTELLECTUAL PROPERTY: HOW ARTIFICIAL INTELLIGENCE HELPS PROTECT COPYRIGHTS AND PATENTS

Abstract. This scientific and legal article examines the problem of intellectual property protection in the digital age and the role of artificial intelligence in strengthening measures to protect copyrights and patents. Special attention is paid to the role of ChatGPT in the protection of intellectual property, the possibilities of its use in patent search and copyright analysis, as well as the advantages of its use, the risks, and limitations of using ChatGPT in the protection of intellectual property.

Keywords: artificial intelligence, intellectual property, innovative tool, ChatGPT, digitalization.

УДК 340.6

Тхай Виктория Рудольфовна
Студент Института государственного и международного права
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
thai.vika2002@gmail.com

Чернигова София Андреевна
Студент Института государственного и международного права
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
sofia_chernigova@mail.ru

Научный руководитель: Рачева Нелли Витальевна,
кандидат юридических наук, доцент
доцент кафедры криминалистики
Уральского государственного юридического университета
имени В. Ф. Яковлева
ekaterinburgg@mail.ru

ВОПРОСЫ ПРИМЕНЕНИЯ ВИРТУАЛЬНОЙ АУТОПСИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье рассмотрен метод виртуальной аутопсии (виртопсии), используемый при проведении судебно-медицинских экспертиз трупов. Данный метод относительно недавно появился в судебной медицине и имеет свои особенности в применении, что заслуживает отдельного внимания научного сообщества. Проанализирован опыт российской и зарубежной практики использования компьютерной томографии и магнитно-резонансной томографии трупов. Сделаны выводы о роли виртуальной аутопсии в судебно-медицинской экспертизе и возможности применения данного метода.

Ключевые слова: виртуальная аутопсия, судебно-медицинская экспертиза, компьютерная томография, посмертная визуализация, труп.

Для цитирования:
Тхай В. Р., Чернигова С. А. Вопросы применения виртуальной аутопсии в Российской Федерации // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 444–451.

С развитием инновационных технологий в различных сферах деятельности человека появляются новые методы и способы решения

задач с помощью внедрения высококачественных технических устройств. Судебная медицина не является исключением. На данный момент применение современных технологий в работе судмедэкспертов является неотъемлемой частью обеспечения их профессиональной деятельности.

Одним из таких технических новшеств в сфере судебно-медицинской экспертизы является виртуальная аутопсия.

Под виртуальной аутопсией понимается применение компьютерной томографии (КТ) и магнитно-резонансной томографии (МРТ) в процессе проведения патологоанатомических и судебно-медицинских исследований. Данный метод отличается от традиционного вскрытия (аутопсии) тем, что при виртопсии происходит построение изображения тела человека компьютерным и магнитно-резонансным томографами без обычных разрезов тканей и органов тела. Измерения и сканирование трупа в рамках данного способа производят при помощи специальных программ, заложенных в ЭВМ компьютерного томографа, исключая человеческий фактор и использование ручных инструментов.

Технология, которая используется в настоящее время для проведения «виртуального вскрытия», включает в себя следующее:

Во-первых, производится сканирование поверхности трупа под управлением робота для трёхмерной документации тела в масштабе и в цвете. Это позволяет дополнить внешнее патологоанатомическое обследование, которое проводится при обычном вскрытии.

Во-вторых, многосрезовая спиральная компьютерная томография, позволяющая увеличить временное и пространственное разрешение по сравнению с традиционной и спиральной компьютерной томографией для 3D-визуализации тела.

В-третьих, проводится посмертная ангиография. Она используется для визуализации внутренней части или просвета, кровеносных сосудов и органов тела, с особым вниманием к артериям, венам и камерам сердца. Данная процедура позволяет визуализировать сердечно-сосудистую систему исследуемого лица с помощью перистальтического насоса и контрастного вещества.

В-четвёртых, проводится отбор проб без контаминации с помощью изображений и роботов для широкого диапазона дополнительных судебно-медицинских анализов таких как: гистология, бактериология, вирусология, токсикология и диатомология. Эта процедура заменяет обычный сбор и хранение образцов материала тела и позволяет значительно упростить хранение результатов исследования[1].

Само развитие данного метода и получение его признания со стороны научного сообщества имеет достаточно долгую историю. Начиная с открытия рентгеновских лучей

[1] Скобеева А. С., Родина Е. Ю. Виртопсия – инновация в мире криминалистики // Ученые записки Казанского юридического института МВД России. 2023. Том 8. № 1 (15). С. 92–98.

Вильгельмом Конрадом Рентгеном в 1895 г., учёные стали заниматься вопросами применения рентгеновского излучения в судебной медицине. Первая посмертная компьютерная томография была сделана в Европе в 1977 г. по поводу огнестрельного ранения в голову, но изображение получилось в плохом качестве, и учёные предпочли другие артефакты, не менее интересные для исследования в судебной медицине[2].

В 1994 г. в Израиле были исследованы трупы погибших в результате механической травмы с помощью виртуальной и обычной аутопсии[3]. Исследование показало, результаты посмертной визуализации трупа во многом совпадают с результатами обычного вскрытия. Данный метод пробовали применять и во многих других странах Европы, однако случаи применения виртопсии не производили большого резонанса в научном сообществе. Многие криминалисты и эксперты всё равно больше придерживались классической аутопсии, так как современный метод посмертной визуализации ещё достаточно не был изучен.

Проведенные в дальнейшим исследования дали толчок для развития виртуальной аутопсии в сфере судебно-медицинской экспертной деятельности.

Немаловажную роль в этом процессе сыграл судебный медик, профессор Ричард Дирнхофер, основавший проект «Виртопсия» ещё в конце прошлого века. Этим проектом Р. Дирнхофер хотел установить перспективы применения виртопсии, узнать, насколько подробно трёхмерные изображения показывают повреждения трупа, ведь полученные данные могли бы помочь лицам, не имеющим медицинского образования и плохо понимающим данные вскрытия со сложными медицинскими терминами от экспертов, лучше понять заключения[4].

Ещё один случай зарубежной практики применения виртопсии приводится в научной работе 2014 г. Roberts I.S и Traill Z.C., где были зафиксированы 120 случаев использования уже мультиспиральной компьютерной томографии (МСКТ), в результате чего были сделаны выводы относительно перспективы применения данного метода. Согласно анализу, более, чем в 50 % случаев установленные причины смерти людей и при виртопсии, и при обычным вскрытии совпадали, а в 38 % обычное вскрытие можно было и не проводить. Также из этих 120 случаев имели место две ситуации, когда с помощью посмертной визуализации были обнаружены черепные травмы, которые при классической аутопсии не были найдены, что ещё раз показало большой потенциал использования

[2] Wullenweber R., Schneider V., Grumme T. A computer-tomographical examination of cranial bullet wounds // Z. Rechtsmed. 1977. Vol. 80. № 3. Pp. 227–246.

[3] Donchin Y., Rivkind A.I., Bar-Ziv J. [et al]. Utility of postmortem computed tomography in trauma victims // J. Trauma. 1994. Vol. 37. №. 4. Pp. 552–555.

[4] Patriquin L., Kassarjian A., Barish M., et al. Postmortem whole-body magnetic resonance imaging as an adjunct to autopsy: preliminary clinical experience // J. Magn. Reson. Imaging. 2001. Vol. 13. № 2. Pp. 277–287.

виртопсии в судебно-медицинских исследованиях[5].

Начиная с 2018 года, в России стали проводиться исследования Бюро Судебно-медицинской экспертизы Московской области по применению посмертной визуализации. Виртопсию стали пробовать как дополнение к традиционному судебно-медицинскому исследованию, с последующим тщательным сравнением полученных результатов[6].

В России, как и во многих других странах, применение данного метода обусловлено по большей части религиозными причинами. Часто возникают такие ситуации, когда близкие умершего возражают против обычного вскрытия. В таком случае будет проще и уместнее провести аутопсию с помощью компьютерной (КТ) и магнитно-резонансной томографии (МРТ), что позволит установить точную причину смерти без каких-либо физических внешних вмешательств в тело человека.

В 2016 г. в городе Грозном прошло заседание круглого стола, главной темой которого стали перспективы создания научно-практического центра «Криминалистической томографии – «виртуальной» аутопсии». На заседании круглого стола обсуждались причины отказа от обычного вскрытия трупов, к которым прежде всего относились религиозные запреты, личные убеждения семьи умершего, волеизъявление самого умершего. Были оценены перспективы внедрения в практику инновационных методов посмертного исследования трупов без вскрытия с использованием средств рентгеновской томографии.

Использование виртуальной аутопсии в криминалистическом исследовании даёт возможность исключить необходимость эксгумации трупов. По полученным снимкам криминалисты и судмедэксперты смогут так же, как и в обычных условиях вскрытия, устанавливать причины смерти, не травмируя психологически родственников умершего и их религиозные чувства[7].

В качестве одного из примеров использования КТ и МРТ в российской практике судебной экспертизы можно привести уголовное дело, рассмотренное в Московской области в 2018 г. На почве ревности мужчина расстрелял свою бывшую жену с её сожителем в присутствии несовершеннолетних детей, после чего совершил самоубийство. На всех трёх трупах было проведено компьютерно-томографическое исследование в отделении лучевой диагностики ГБУЗ МО «Видновская ЦРБ». В ходе данного исследования было выяснено, где конкретно располагались черепные травмы, переломы, установлены также

[5] Dirnhofer R., SchickP.J., Ranner G. Virtopsy – Obduktionneu in Bildern. Wien, Austria: Manzsche Verlags und Universitaets buchhandlung, 2010.

[6] Клевно В. А., Чумакова Ю. В. Виртопсия – новый метод исследования в практике отечественной судебной медицины // Судебная медицина. 2019. №5 (2). С. 27–31.

[7] Roberts I. S., Traill Z. C. Minimally invasive autopsy employing post-mortem CT and targeted coronary angiography: evaluation of its application to a routine Coronial service // Histopathology. 2014. Vol. 64. № 2. Pp. 211–217.

положение пуль, локализация кровоизлияний в телах. Компьютерная томография позволила эксперту выбрать тактику исследования, ускорить поиск инородных предметов (пули, металлические и костные осколки), установить направление раневых каналов. По снимкам также можно было увидеть изначальное положение переломов костей от пуль[8].

Говоря о других преимуществах виртопсии, следует выделить тот факт, что она позволяет зафиксировать признаки прижизненных повреждений в случаях асфиксии, механической травмы, воздействия пламени, утопления и др. Необходимо учесть и то, что снижается шанс заражений персонала опасными инфекционными заболеваниями, которые присутствуют в трупе. Результаты виртопсии можно хранить без ограничений по времени в электронном виде, что облегчает в дальнейшем их использование в других экспертизах уже после захоронения или кремации трупа. Хранение в электронном виде данных виртопсии помогает сотрудникам правоохранительных органов оперативно собирать информацию и быстрее обмениваться ею в схожих ситуациях.

Однако, рассматривая преимущества виртопсии, нельзя не указать на имеющиеся недостатки данной технологии.

Во-первых, следует обратить внимание на то, что отсутствует конкретная и подробная нормативная регламентация данного метода. Также нет методических рекомендаций и стандартов его применения. Зачастую могут возникать проблемы трактовки обнаруженных КТ и МРТ изменений в теле человека до и после смерти.

Во-вторых, одним из главных недостатков является стоимость томографии, поскольку оборудование для проведения измерений и съёмок в настоящее время достаточно дорогостоящее, так как для создания такой техники требуются качественные ресурсы[9].

Обращаясь к вопросу о том, как относится научное сообщество к проведению виртопсии, можно обнаружить, что мнения различаются.

У. Н. Туманова, доктор медицинских наук, ведущий научный сотрудник ФГБУ «Национальный медицинский исследовательский центр акушерства, гинекологии и перинатологии имени академика В. И. Кулакова» Минздрава России сделала вывод о том, что КТ обладает высокой эффективностью для выявления аномалий костной системы. Посмертная МРТ является более эффективным методом для выявления и оценки патологии внутренних органов, мягких тканей и сосудистой системы мертворождённых и умерших новорождённых.

Глава израильской общественной организации, объединяющей добровольные спасательные группы Йехуда Меши-Захав отмечает, что виртуальная аутопсия даёт более точную картину причины смерти, и провести её можно

[8] Мордюк А. В, Кичуткина Е. В. Актуальные вопросы применения виртуальной аутопсии в России // Научно-практический электронный журнал Аллея Науки. 2019. №4 (31).

[9] Клевно В. А., Чумакова Ю. В., Павлик Д. П., Дуброва С. Э. Возможности виртуальной аутопсии при огнестрельной травме // Судебная медицина. 2019. № 5 (3). С. 33–38.

намного быстрее, чем традиционное вскрытие.

В свою очередь, президент Королевского колледжа патологоанатомов Великобритании Питер Фернесс выражает мнение, что необходимы более широкие сравнения виртопсии с обычным вскрытием, настаивая на том, что обстоятельства, где это может быть необходимым, не до конца выяснены, надёжность подхода пока мала, и стоимость может быть значительной[10].

Проанализировав положительные и отрицательные стороны технологии виртуального вскрытия, можно сделать вывод о том, что данный метод является достаточно эффективным. Его применение в ходе расследования преступлений против жизни и здоровья человека позволит сохранить целостными тела умерших, что имеет важное значение для людей различного вероисповедания. Кроме того, виртопсия позволяет в трёхмерном пространстве решать идентификационные и диагностические задачи экспертного исследования трупов. Особенно это важно при изучении технически сложных с точки зрения традиционного вскрытия участков тела (лицевой скелет, основание черепа и т. д.). При наличии огнестрельных ранений и следов взрывов на теле КТ-исследование становится особенно необходимым, так как способствует обнаружению инородных тел.

Для развития виртопсии необходимо комплексное проведение ряда мероприятий по правовой регламентации применения данного способа исследования трупов. Необходимо усовершенствовать материально-техническое обеспечение судебно-медицинских экспертных подразделений, а также привлечение специалистов данной области (врачей-рентгенологов, специалистов в области посмертной визуализации и т. д.), повысить квалификации уже имеющихся специалистов.

Вместе с тем, данный метод не сможет заметить традиционную аутопсию по определённому ряду причин, отмеченных экспертами в этой области. К ним относятся: низкая эффективность в диагностике травм полых органов, желудочно-кишечного тракта, мочевыделительной системы и разрыва диафрагмы; дороговизна аппаратов КТ и МРТ; отсутствие необходимой базы знаний и опыта у специалистов, осуществляющих вскрытие с помощью современных 3D-технологий.

Список литературы:

1. Скобеева А. С., Родина Е. Ю. Виртопсия – инновация в мире криминалистики // Ученые записки Казанского юридического института МВД России. 2023. Том 8. № 1 (15). С. 92–98.

[10] Арефьев М. Л. Судебно-медицинская экспертиза трупа после забора внутренних органов для трансплантации // Судебная медицина. 2016. № 2 (2). С. 94–95.

2. Арефьев М. Л. Судебно-медицинская экспертиза трупа после забора внутренних органов для трансплантации // Судебная медицина. 2016. № 2 (2). С. 94–95.

3. Клевно В. А., Чумакова Ю. В., Павлик Д. П., Дуброва С. Э. Возможности виртуальной аутопсии при огнестрельной травме // Судебная медицина. 2019. № 5 (3). С. 33–38.

4. Клевно В. А., Чумакова Ю. В. Виртопсия – новый метод исследования в практике отечественной судебной медицины // Судебная медицина. 2019. №5 (2). С. 27–31.

5. Мордюк А. В, Кичуткина Е. В. Актуальные вопросы применения виртуальной аутопсии в России // Научно-практический электронный журнал Аллея Науки. 2019. № 4 (31).

6. Dirnhofer R., SchickP. J., Ranner G. Virtopsy – Obduktionneu in Bildern. Wien, Austria: Manzsche Verlags und Universitaets buchhandlung, 2010.

7. Donchin Y., Rivkind A.I., Bar-Ziv J. [et al]. Utility of postmortem computed tomography in trauma victims // J. Trauma. 1994. Vol. 37. № 4. Pp. 552–555.

8. Patriquin L., Kassarjian A., Barish M. [et al]. Postmortem whole-body magnetic resonance imaging as an adjunct to autopsy: preliminary clinical experience // J. Magn. Reson. Imaging. 2001. Vol. 13. № 2. Pp. 277–287.

9. Roberts I. S., Traill Z. C. Minimally invasive autopsy employing post-mortem CT and targeted coronary angiography: evaluation of its application to a routine Coronial service // Histopathology. 2014. Vol. 64. № 2. Pp. 211–217.

10. Wullenweber R., Schneider V., Grumme T. A computer-tomographical examination of cranial bullet wounds // Z. Rechtsmed. 1977. Vol. 80. № 3. Pp. 227–246.

Victoria R. Thai
Student of the Institute of State and International Law
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
thai.vika2002@gmail.com

Sofia A. Chernigova
Student of the Institute of State and International Law
Ural State Law University named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
sofia_chernigova@gmail.com

Scientific Supervisor: Nelly V. Racheva
PhD in Law, Associate Professor,
Associate Professor of the Department of Criminology
Ural State Law University named after V. F. Yakovlev
ekaterinburgg@mail.ru

ISSUES OF VIRTUAL AUTOPSY APPLICATION IN THE RUSSIAN FEDERATION

Abstract. The article discusses the method of virtual autopsy (virtopsy) used in conducting forensic medical examinations of corpses. This method has appeared relatively recently in forensic medicine and has its own peculiarities in application, which deserves special attention of the scientific society. Having analyzed the experience of Russian and foreign practice of using computed tomography and magnetic resonance imaging of corpses. Conclusions are drawn about the role of virtual autopsy in forensic medical examination and the possibility of using this method along with the traditional method of autopsy of corpses.

Keywords: virtual autopsy, forensic medical examination, computer tomography, post-mortem imaging, corpse.

УДК 004.032.2

Усиков Дмитрий Витальевич
Студент факультета подготовки следователей
Московская Академия Следственного комитета Российской Федерации
(г. Москва, Российская Федерация)
u.dmitriy.d@mail.ru

Сатаев Михаил Юрьевич
Студент факультета подготовки следователей
Московская Академия Следственного комитета Российской Федерации
(г. Москва, Российская Федерация)
sataev814@gmail.com

Научный руководитель: Рудакова Светлана Владимировна,
кандидат психологических наук, доцент,
Московская академия Следственного комитета Российской Федерации
(г. Москва, Российская Федерация)
rudakova@mail.ru

НАУКА ОПРЕДЕЛЕНИЯ LLM-СГЕНЕРИРОВАННОГО ТЕКСТА: ПЕР. С АНГЛ.

Аннотация. Развитие больших языковых моделей (Large Language Models – LLM) привело к распространению текстов, сгенерированных с их помощью, крайне изощрённых и практически неотличимых от текстов, созданных человеком. Помимо прочего, это вызвало беспокойство по поводу возможных злоупотреблений такими возможностями, а также распространения ложной информации или подрыва системы образования. И хотя уже было предложено множество подходов к определению таких текстов, полноценное понимание всех достижений и вызовов в данной сфере до сих пор отсутствует. Целью данного исследования является обзор существующих техник определения LLM-сгенерированных текстов и побуждение развития регулирования языковых генерируемых моделей. Более того, мы акцентируем внимание на ключевых замечаниях для дальнейших исследований, включая развитие всесторонней оценки показателей и угроз, создаваемых доступными открыто LLM, для того чтобы сподвигнуть прогресс в области определения LLM-сгенерированных текстов.

Ключевые слова: большие языковые модели, метод чёрного ящика, метод белого ящика, ChatGPT, технологии создания естественного языка.

Данная статья является адаптированным переводом с английского языка оригинальной статьи, опубликованной в форме препринта: Ruixiang Tang, Yu-Neng Chuang, Xia Hu (Department of Computer Science, Rice University, Houston, USA) The

science of detecting LLM-generated texts. DOI: https://doi.org/10.48550/arXiv.2303.07205.

Для цитирования:
Усиков Д. В., Сатаев М. Ю. Наука определения LLM-сгенерированного текста: пер. с англ.// Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 453–475.

«1. Введение

Последние достижения в области технологий создания естественного языка (Natural Language Generation – NLG) значительно расширили многообразие, повысили качество LLM-сгенерированных текстов, и их потенциал. Примечателен созданный OpenAI ChatGPT, продемонстрировавший исключительные результаты в таких задачах, как ответ на вопросы, написание писем, эссе и компьютерных кодов. Однако эта новоявленная способность к созданию текстов, имеющих высокое сходство с человеческими, также вызывает и беспокойство по поводу возможности выявления и предупреждения злоупотребления LLM, в таких случаях как, например, фишинг, дезинформация и научная недобросовестность. Так, например, многие учебные заведения запретили использование ChatGPT из-за опасности списывания[1], а СМИ забили тревогу опасаясь распространения фейковых новостей, созданных с помощью LLM[2]. Всё это беспокойство злоупотреблением возможностями LLM препятствует полезному использованию NLG в сферах СМИ и образования.

Возможность точно определить LLM-сгенерированный текст критически важна для использования полного потенциала NLG при минимизации серьёзных последствий. Начиная от самой перспективы и до конечного использования определение LLM-сгенерированного текста может повысить доверие к системам NLG и вдохновить людей на их применение. Для разработчиков и исследователей технологий машинного обучения, такая система может оказать значительную помощь в отслеживании сгенерированных текстов и предотвращении их несанкционированного использования. Интерес к такой технологии, в силу её значимости, возрос в науке и индустрии, что побуждает дальнейшие исследования в области LLM-сгенерированных текстов для улучшения нашего понимания глубинных механизмов этого явления.

[1] Elsen-Rooney M. NYC education department blocks ChatGPT on school devices, networks // Communication of the ACM [Electronic resource]. 2023, 6 января. URL: https://cacm.acm.org/news/268457-nyc-education-dept-blocks-chatgpt-on-school-devices-networks/fulltext (дата обращения: 08.05.2023).

[2] Floridi L., Chiriatti M. GPT-3: Its nature, scope, limits, and consequences //Minds and Machines. 2020. Vol. 30. Pp. 681–694.

Пока дискуссия по поводу того, может ли LLM-сгенерированный текст быть достоверно определён и как именно это должно происходить, продолжает разворачиваться, мы представляем комплексный обзор существующих ныне методов определения таких текстов, которые могут быть разделены примерно на два вида: определение методом чёрного ящика и определение методом белого ящика. Методы чёрного ящика ограничены уровнем доступа API к LLM. Они основаны на сборе образцов текстов, созданных человеком и машиной с тем, чтобы в дальнейшем подготовить классификационную модель, которая будет использована для различения текстов, созданных человеком и LLM. Детекторы типа чёрного ящика работают хорошо, поскольку нынешние LLM часто демонстрируют лингвистические и статистические паттерны. Всё же, с развитием LLM, такие методы станут куда менее эффективны. Альтернативные им методы белого ящика, для такого случая располагают прямым доступом непосредственно к механизму LLM и могут контролировать его с целью отслеживания результатов. На практике тестирование по стратегии чёрного ящика обычно построено на основе использования внешних по отношению к исследуемой системе составляющих, тогда как тестирование по стратегии белого ящика осуществляется в основном благодаря самим разработчикам LLM.

В этой статье обсуждается актуальная, для анализа данных и обработки естественного языка, тема. Отдельно нами впервые описаны методы тестирования по стратегии чёрного ящика в условиях жизненного круга анализа данных, включая их сбор, отбор по признакам и создание классификационной модели. Далее мы погружаемся в наиболее свежие достижения в области методов определения по стратегии белого ящика, такие как апостериорные «водяные знаки» и «водяные знаки» времени вывода. В заключении нами представлены направления и ограничения современных исследований методов определения, а также предложены потенциальные направления исследования. Мы ставим своей целью раскрыть потенциальные возможности LLM, представляя теоретические концепции, алгоритмы и конкретные примеры определения LLM-сгенерированных текстов.

2. Распространённость и влияние

Насколько же хороши LLM-генерируемые тексты, и какое влияние они оказывают на людей и общество? Последние достижения ChatGPT от OpenAI приоткрывают для нас их потенциал. Преимущества привнесённые ChatGPT обнадёживают своей эффективностью в применении на производстве и в образовании. К примеру, возможность ChatGPT показать хорошие результаты на таких тестах как MBA-экзамен в Wharton Business School демонстрируют его способность соперничать со знаниями человека и потенциал в помощи

профессионалам[3]. В сфере здравоохранения ChatGPT может оптимизировать ведение документации составляя записи о состоянии пациента и ходе болезни, а также отчёты, помогая студентам и практикующим врачам создавать удобные медицинские записи на ясном языке. В экстренных службах ChatGPT может помочь в составлении отчётов в режиме реального времени, уменьшая время ожидания для тех, кто непосредственно вовлечён в действия.

Тем не менее, включение ChatGPT в систему образования вызвало беспокойство среди экспертов. Использование данной технологии подпитывает опасения относительно возможного списывания, поскольку учащиеся могут эксплуатировать его для несанкционированного получения информации и достижения таким образом необходимых результатов. Пока инструмент представляет доступ к быстрым ответам, это не способствует развитию навыков критического мышления и решения задач, что губительно для развития в долгосрочной перспективе. Некоторые образовательные организации отреагировали на это, запретив использование ChatGPT в научных статьях и работах учащихся[4]. Это демонстрирует необходимость вдумчивого определения основных направлений и условиях интеграции LLM в образовательную систему. Более того, такие организации как Международная конференция по машинному обучению (International Conference on Machine Learning – ICML), а также издания, например «Nature», объявили, что использование ChatGPT не может считаться за авторский вклад в сборниках конференций и журналах. Это подчёркивает острую необходимость различения LLM-сгенерированных текстов и тех, что созданы человеком. В качестве вклада в борьбу с академической недобросовестностью OpenAI и несколько других разработчиков недавно создали инструменты для помощи в сфере образования, позволяющие идентифицировать возможные случаи академического подлога[5]. До сих пор не разочаровавшие, эти инструменты призваны достичь высокого уровня академической честности в обучении и исследованиях. Признавая важность этого, наука и индустрия проявляют растущий интерес к развитию исследований обнаружения LLM-сгенерированных текстов.

3. Метод чёрного ящика

Что касается метода чёрного ящика, то его возможности

[3] Rosenblatt K. ChatGPT passes MBA exam given by a Wharton professor // // NBCNews [Electronic resource] 2023, January 24. URL: https://www.nbcnews.com/tech/tech-news/chatgpt-passes-mba-exam-wharton-professor-rcna67036 (дата обращения: 08.05.2023).

4 Atallah M. J. [et al]. Natural language watermarking: Design, analysis, and a proof-of-concept implementation // Information Hiding: 4th International Workshop, IH 2001 Pittsburgh, PA, USA, April 25–27, 2001. Proceedings 4. Springer Berlin Heidelberg, 2001. Pp. 185–200.

[5] Bhatt P., Rios A. Detecting Bot-Generated Text by Characterizing Linguistic Accommodation in Human-Bot Interactions // arXiv preprint arXiv:2106.01170. 2021.

ограничены уровнем доступа API к LLM, как это описано на рис. 1.

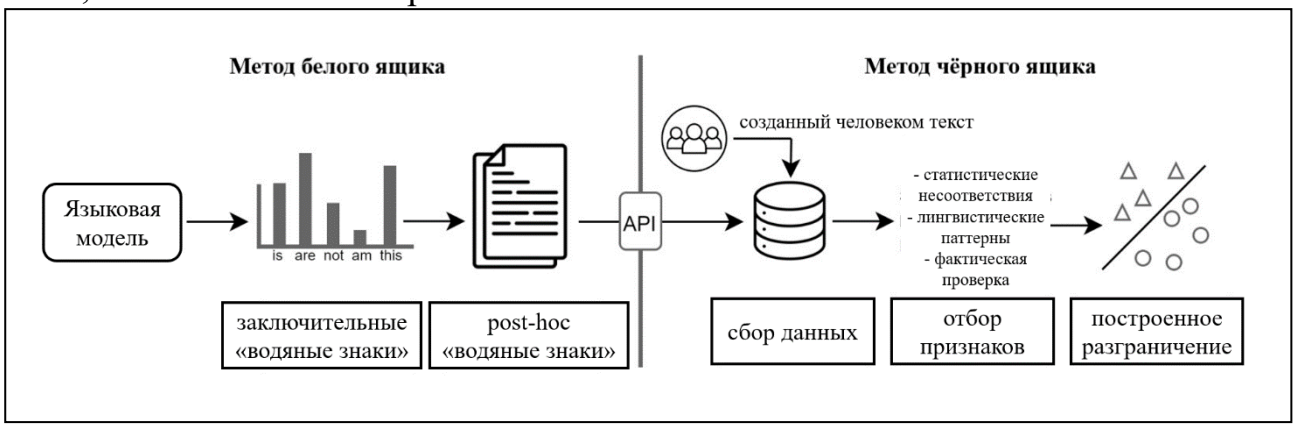

Рис. 1 Обзор методов выявления LLM-сгенерированных текстов.

Для обеспечения надлежащей точности определения тестирование по стратегии чёрного ящика подразумевает необходимость сбора образцов текстов, созданных и человеком, и машиной. После осуществления этого классификатор проектируется для разделения образцов между двумя категориями посредством выявления и разграничения релевантных признаков. Мы выделяем три необходимых элемента такого детектора: сбор данных, отбор признаков, осуществление модельной классификации.

3.1 Отбор данных

Эффективность детектора по типу чёрного ящика сильно зависит от качества и разнообразия собранных данных. В последнее время расширяющийся корпус исследований сосредоточился на накоплении ответов LLM и сравнении их с текстами, составленными человеком, которые охватывают широкий спектр различных сфер жизни. Настоящий раздел углубляется в различные стратегии получения указанных данных от человека и машины

3.1.1 LLM-сгенерированные данные

Конструкция LLM заключается в производстве оценки вероятности появления маркеров в последовательности, основанной на предшествующих словах. Последние достижения в области NLG привели к развитию LLM в различных направлениях, включая общение по типу вопрос-ответ, производство новостей и создание других текстов. Прежде, чем собирать корпус LLM-сгенерированных текстов, необходимо обозначить целевые области и модели генерации текстов. Обычно модели определения построены для распознавания текстов, созданных определённым LLM, на различную тематику. В целях расширения возможностей определения минимаксная стратегия предполагает отсечение худших случаев определения, что повлечёт за собой повышение способности к определению LLM сгенерированных текстов в ситуациях, когда их качество настолько высоко, что они

оказываются способны соперничать с созданными человеком[1].

Создание таких текстов высокого качества на определённые темы может быть достигнуто путём направленной настройки LLM на определённые данные, что существенно повышает качество генерируемых текстов. Так, например, Солэйман (Solaiman) и др. настроили GPT2 на обзорах товаров из Amazon[2], создавая таким образом другие обзоры, в том же стиле, характерном для Amazon. Более того, известно, что LLM способны к демонстрации таких артефактов как повторяемость, что может негативно повлиять на способность детектора к обобщению при исследовании текстов. Для их смягчения исследователи могут давать подсказки или направлять детектор в рамках узкой специализации ещё до непосредственного получения результатов. Так, Кларк (Clark) и др. случайным образом отобрали 50 статей из «Newspaper3k» для того, чтобы использовать их как подсказки при создании новостей, а также применили фильтры для ограничения применения при написании моделью текстов таких штампов как «однажды... «[3].

Стратегия отбора маркеров также значительно повлияла на стиль и качество генерируемых текстов. Пока детерминистски жадные алгоритмы подобно лучу собирают и генерируют самые вероятные последующие элементы текста, снижается креативность и языковое разнообразие на выходе[4]. С другой стороны, алгоритмы, основанные на случайности, отбирают, например, центральные образцы, в то же время исключая периферические, что делает такую систему более подходящей для свободной генерации текстов[5]. Отсюда следует вывод, что для исследователей чрезвычайно важно внимательно отбирать области, модели генерации, и стратегии отбора образцов LLM-сгенерированных текстов для того, чтобы повысить вероятность получения качественного, разнопланового, соответствующего конкретным сферам результата.

3.1.2 Данные, созданные человеком

Естественным методом сбора образцов аутентичных, созданных человеком текстов, является создание их собственноручно. К примеру, в исследовании, проведённом Дуганом (Dugan) и др.[6], авторы попытались измерить уровень качества NLG-систем, а также оценить восприятие сгенерированных текстов человеком. Чтобы провести такое исследование они наняли 200 работников Amazon

[1] Pagnoni A., Graciarena M., Tsvetkov Y. Threat Scenarios and Best Practices to Detect Neural Fake News //Proceedings of the 29th International Conference on Computational Linguistics. 2022. Pp. 1233–1249.

[2] Solaiman I. [et al]. Release strategies and the social impacts of language models // arXiv preprint arXiv:1908.09203. 2019.

[3] Clark E. [et al]. All that's' human'is not gold: Evaluating human evaluation of generated text // arXiv preprint arXiv:2107.00061. 2021.

[4] Tillmann C., Ney H. Word reordering and a dynamic programming beam search algorithm for statistical machine translation // Computational linguistics. 2003. Vol. 29. №. 1. Pp. 97–133.

[5] Holtzman A. [et al]. The curious case of neural text degeneration // arXiv preprint arXiv:1904.09751. 2019.

[6] Dugan L. [et al]. RoFT: A tool for evaluating human detection of machine-generated text // arXiv preprint arXiv:2010.03070. 2020.

Mechanical Turk и попросили их самостоятельно написать 10 аннотаций на веб-сайт компании естественным для них языком. Однако, сбор образцов вручную, может оказаться одновременно экономически- и трудозатратным, что особенно осложняет проведение исследований на больших массивах данных. Альтернативный подход предполагает извлечение образцов текстов прямиком из уже созданных человеком материалов, таких как веб-страницы или академические работы. Например, можно с лёгкостью собрать тысячи текстов из сферы компьютерных наук из Википедии, проверенных признанными экспертами[7]. Более того, количество публично доступных баз эталонов, таких как «ELI5»[8], которая охватывает 270 тысяч веток с форума на Reddit «Explain Like I'm Five» уже предлагает созданные человеком тексты в организованном виде. Использование этих легко доступных источников может заметно снизить издержки при сборе необходимых для исследования образцов. Впрочем, необходимо будет минимизировать потенциальные отклонения при сборе образцов и обеспечить разнообразие полученного корпуса текстов, включая созданные людьми из различных групп, в том числе тех, для кого данный язык не является родным.

3.1.3 Отбор образцов

Предшествующие исследования предложили достойные подходы к различению LLM-сгенерированных текстов и текстов, созданных человеком. Поверхностные наблюдения демонстрируют, что LLM-сгенерированные тексты куда менее эмоционально окрашены и более объективны, в сравнении с человеческими, которые часто используют грамматические и пунктуационные средства для передачи субъективных ощущений[9]. Так, например, люди часто снабжают свои тексты восклицательными и вопросительными знаками, многоточиями для того, чтобы выразить свои эмоции, в то время как LLM генерирует ответы, отличающиеся большей формальностью и структурированностью. Однако, необходимо признать, что LLM-сгенерированные тексты далеко не всегда являются точными и строгими, поскольку могут содержать в себе фальсификацию[10]. Исследования также показывают, что на уровне предложений тексты людей куда более последовательны, чем LLM-сгенерированные, которые отличаются тенденцией к повторению слов на

[7] Guo B. [et al]. How Close is ChatGPT to Human Experts? Comparison Corpus, Evaluation, and Detection // arXiv preprint arXiv:2301.07597. 2023.

[8] Fan A. [et al]. ELI5: Long form question answering // arXiv preprint arXiv:1907.09190. 2019.

[9] Guo B. [et al]. How Close is ChatGPT to Human Experts? Comparison Corpus, Evaluation, and Detection // arXiv preprint arXiv:2301.07597. 2023.

[10] Guo B. [et al]. How Close is ChatGPT to Human Experts? Comparison Corpus, Evaluation, and Detection // arXiv preprint arXiv:2301.07597. 2023; Shakeel D., Jain N. Fake news detection and fact verification using knowledge graphs and machine learning // 2021. DOI 10.13140/RG.2.2.18349.41448.

протяжении абзаца[11]. Эти наблюдения предполагают, что LLM может оставлять различные сигналы в генерируемом тексте, позволяя позднее наблюдателю выявить характерные признаки и с их помощью отделить текст LLM от текста человека.

3.2 Выявление характерных признаков

Как можно отличить LLM-сгенерированный текст от созданного человеком текста? В данном разделе обсуждается возможность выявления характерных признаков по разнообразным параметрам, включая статистические несоответствия, языковые паттерны и проверку фактов.

3.2.1 Статистическое расхождение

Выявление статистических различий между LLM-сгенерированными и написанными человеком текстами может быть осуществлено с помощью различных статистических показателей. К примеру, коэффициент Зипфиана (Zipfian) измеряет внутреннюю согласованность в тексте с помощью кривой, описывающей закон Зипфиана (Zipf's law)[12]. Визуализация с помощью GLTR[13] позволяет обнаружить артефакты генерации текста, через превалирующие элементы, как это показано на рис. 2, где слова, входящие в первую десятку по встречаемости подсвечены зелёным, в первую сотню – жёлтым, первую тысячу – красным, а остальные фиолетовым. Как видно, существует заметная разница между этими двумя текстами. Человеческий образец текста взят из «Chalkbeat New York»[14].

[11] Dugan L. [et al]. Real or Fake Text: Investigating Human Ability to Detect Boundaries Between Human-Written and Machine-Generated Text // arXiv preprint arXiv:2212.12672. 2022.; Pagnoni A., Graciarena M., Tsvetkov Y. Threat Scenarios and Best Practices to Detect Neural Fake News //Proceedings of the 29th International Conference on Computational Linguistics. 2022. – PP. 1233-1249.

[12] Piantadosi S. T. Zipf's word frequency law in natural language: A critical review and future directions // Psychonomic bulletin & review. 2014. Vol. 21. Pp. 1112–1130.

[13] Gehrmann S., Strobelt H., Rush A. M. Gltr: Statistical detection and visualization of generated text // arXiv preprint arXiv:1906.04043. 2019.

[14] Elsen-Rooney M. M. NYC education department blocks ChatGPT on school devices, networks // Communication of the ACM [Electronic resource]. 2023, 6 января. URL: https://cacm.acm.org/news/268457-nyc-education-dept-blocks-chatgpt-on-school-devices-networks/fulltext (дата обращения: 08.05.2023).

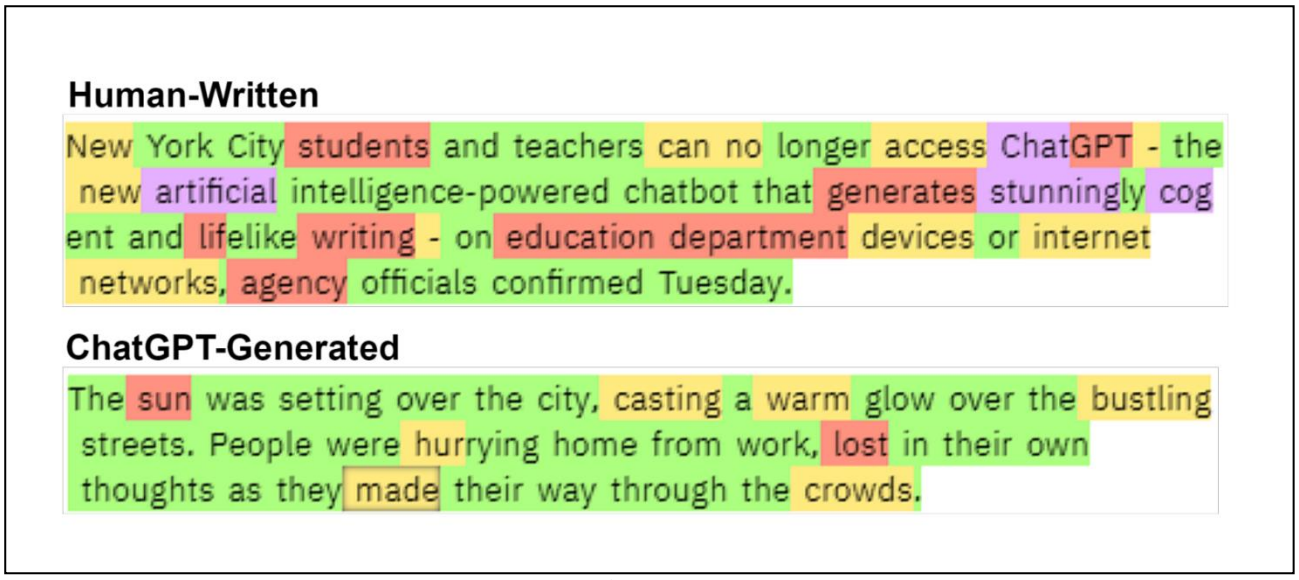

Рис. 2 Результат визуализации GLTR[1], выборка получена с помощью GPT-2.

В основе этого лежит предположение, что большинство систем будут осуществлять выборку из самых распространённых в языке элементов, благодаря чему такое ранжирование слов может быть использовано для выявления LLM-сгенерированных текстов. Перплексия также используется как метрика для определения LLM-сгенерированных текстов. Она измеряет уровень неопределённости или неожиданности появления очередного слова в последовательности, основываясь на предыдущих словах, высчитывая отрицательную среднюю логарифмической функции правдоподобия текста согласно языковой модели[1]. Исследователи определили, что языковые модели имеют тенденцию к концентрации на общих паттернах текстов, входящих в учебный датасет, что приводит к низким показателям перплексии. Напротив, люди обладают способностью к выражению самих себя в широком спектре стилей, менее предсказуемых для языковых моделей, что даёт более высокие показатели перплексии в созданных человеком текстах. Однако важно признать, что эти статистические методы различения ограничиваются необходимостью использовать тексты большого объёма, что неизбежно ослабляет различающую способность такого метода, как это описано на рис 3.

[1] Gehrmann S., Strobelt H., Rush A. M. Gltr: Statistical detection and visualization of generated text // arXiv preprint arXiv:1906.04043. 2019.

[1] Brown P. F. [et al]. An estimate of an upper bound for the entropy of English // Computational Linguistics. 1992. Vol. 18. №. 1. Pp. 31–40.

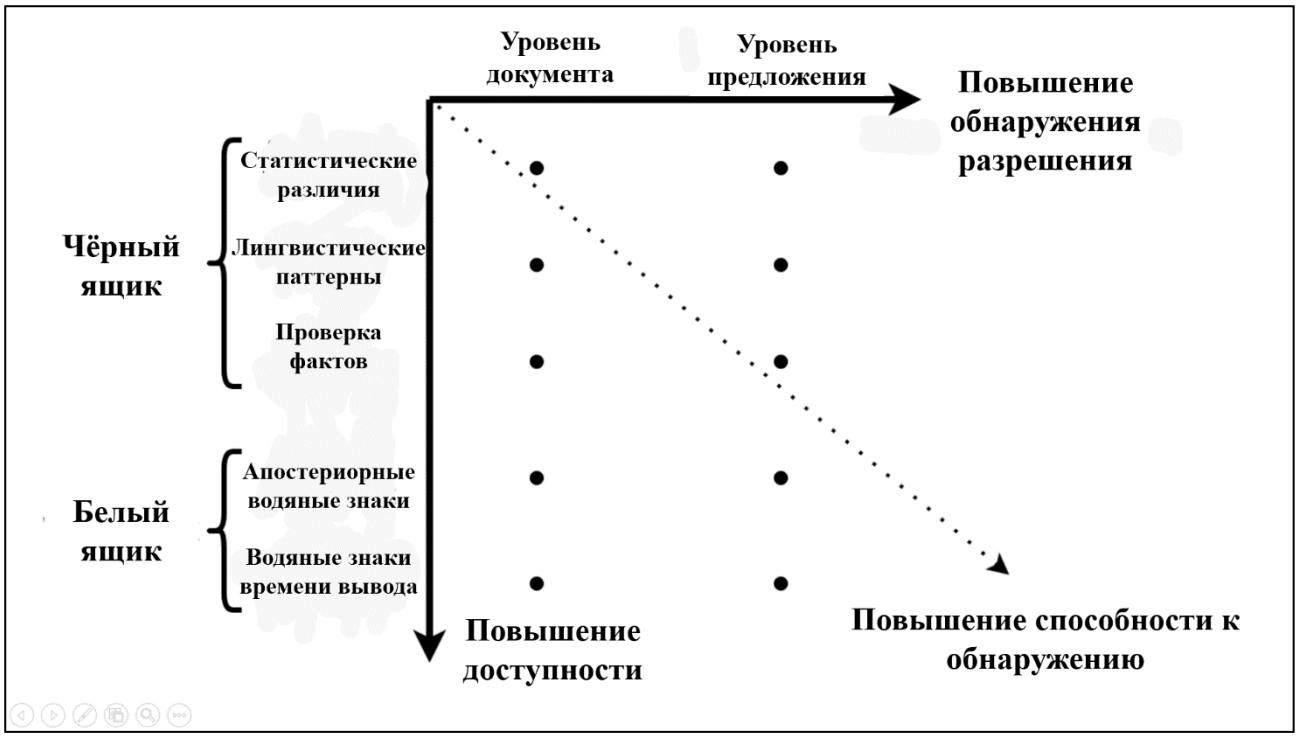

Рис. 3 Система методов обнаружения LLM-сгенерированных текстов

3.2.2 Лингвистические паттерны

Различные контекстуальные свойства могут быть использованы для анализа лингвистических паттернов человека и LLM-сгенерированных текстов. К ним относятся, например, лексические особенности, используемые части речи, синтаксис, и различные стилистические особенности. Использование лексических особенностей предполагает изучение паттернов употребляемых слов исследуемого текста, через анализ таких характеристик как, средняя длина слова, размер вокабуляра и плотность слов. Предыдущие исследования ChatGPT показали, что человеческие тексты показывают тенденцию к более разнообразному вокабуляру, но более короткой средней длине слов[1]. Анализ по частям речи акцентирует внимание на преобладании существительных в текстах ChatGPT, что подразумевает собой объективность и аргументацию, в то время как синтаксический анализ показывает, что ChatGPT использует куда большее количество зависимых предложений, союзов и вспомогательных глаголов[2]. Анализ эмоциональности, с другой стороны, обеспечивает измерение эмоциональной окрашенности и выразительности текста. В отличие от людей, LLM являются по умолчанию скорее нейтральными и имеют недостаток эмоциональной выразительности. Исследования показали, что ChatGPT демонстрирует значительно меньшее количество негативной эмоциональной окраски или вообще ненависти, по сравнению с

[1] Guo B. [et al]. How Close is ChatGPT to Human Experts? Comparison Corpus, Evaluation, and Detection // arXiv preprint arXiv:2301.07597. 2023.

[2] Guo B. [et al]. How Close is ChatGPT to Human Experts? Comparison Corpus, Evaluation, and Detection // arXiv preprint arXiv:2301.07597. 2023.

человеком. Стилистический анализ или стилометрия, включая измерение повторяемости отдельных элементов, недостатка смысла и читабельности, также известна как пристанище ценных сигналов для выявления LLM-сгенерированных текстов[3]. Помимо одиночных текстов, большое количество лингвистических паттернов может быть обнаружено в многовитковых *(Означает непрерывную цепочку последовательных сообщений двух взаимодействующих друг с другом сторон – прим. перевод.)* диалогах[4]. Эти паттерны являются отражением обучения определённым стратегиям на конкретных данных и служат ценным источником признаков, отличающих LLM-сгенерированные тексты. Однако важно отметить, что LLM может существенно варьировать свои лингвистические паттерны, в ответ на такой запрос. К примеру, добавление на вход такой функции, как «ответь с юмором» может изменить стиль и эмоциональную окрашенность ответа LLM, что отразиться на устойчивости лингвистических паттернов.

3.2.3 Проверка фактов.

Большие языковые модели часто опираются на цели максимизации правдоподобия во время обучения, что может привести к генерации бессмысленного или непоследовательного текста, к феномену, известному как галлюцинация. Это подчеркивает важность проверки фактов как важнейшего элемента для выявления[5]. Например, сообщалось, что ChatGPT от OpenAI генерирует ложные научные тезисы и публикует вводящие в заблуждение новостные сводки[6]. Исследования также показали, что популярные методы декодирования, такие как top-k и выборка ядра, приводят к более разнообразным и менее повторяющимся поколениям моделей. Однако они также создают тексты, которые менее поддаются проверке[7]. Эти результаты подчёркивают потенциал использования проверки фактов для обнаружения текстов, сгенерированных LLM.

Предыдущие исследования продвинулись в разработке инструментов и алгоритмов для проведения проверки фактов, которая включает в себя: извлечение

[3] Fröhling L., Zubiaga A. Feature-based detection of automated language models: tackling GPT-2, GPT-3 and Grover // PeerJ Computer Science. 2021. Vol. 7. Pp. 1–23. DOI 10.7717/peerj-cs.443.

[4] Bhatt P., Rios A. Detecting Bot-Generated Text by Characterizing Linguistic Accommodation in Human-Bot Interactions // arXiv preprint arXiv:2106.01170. 2021.

[5] Zhong W., Tang D., Xu Z., Wang R., Duan N., Zhou M., Wang J., and Yin J. Neural Deepfake Detection with Factual Structure of Text. // Association for Computational Linguistics/ Minnesota. 2020. Pp. 2461–2470.

[6] Guggenberger N. From Fake News to Fake Views: New Challenges Posed by ChatGPT-Like AI // LawFareBlog [Electronic resource]. 2023. January 20. URL: https://www.lawfareblog.com/fake-news-fake-views-new-challenges-posed-chatgpt-ai (дата обращения: 08.05.2023).

[7] Massarelli L., Petroni F., Piktus A., Ott M., Rocktäschel T., Plachouras V., Silvestri F., Riedel S. How Decoding Strategies Affect the Verifiability of Generated Text. // Association for Computational Linguistics Minnesota. 2020. Pp. 223–235.

доказательств для утверждений, оценку согласованности и релевантности, а также обнаружение несоответствий в текстах. Одна стратегия использует доказательства на уровне предложения, такие как сбор фактов из Википедии[8]. Ма и др. использовали репрезентативное обучение для встраивания доказательств на уровне предложений, основанных на моделировании согласованности и выводе на естественном языке, что приводит к более глубокому пониманию семантики текста[9]. Другой подход включает анализ доказательств на уровне документа с помощью графовых структур, которые отображают фактическую структуру документа в виде граф-объекта. Этот граф используется для изучения предложений-представлений с помощью графовой нейросети, с последующим составлением предложений-представлений в единый документ для проверки фактов. Этот метод показал, что созданные человеком тексты, как правило, повторяют термины, в то время как тексты, созданные LLM, часто имеют нерелевантное содержание[10]. В некоторых исследованиях также используются графы знаний, построенные на основе правдивых источников, таких как Википедия, для проверки фактов[11]. Эти методы оценивают согласованность путём запроса подграфов и выявляют информацию, не относящуюся к фактам, посредством перебора объектов и их связей. Учитывая, что тексты, созданные человеком, также могут содержать дезинформацию, жизненно важно дополнить результаты обнаружения другими функциями, чтобы точно отличать тексты, сгенерированные LLM.

3.3 Классификационная модель

К задаче обнаружения обычно подходят как к задаче бинарной классификации, направленной на захват текстовых признаков, которые различают тексты, созданные человеком, и тексты, сгенерированные LLM. В этом разделе представлен обзор основных категорий классификационных моделей.

3.3.1 Традиционные алгоритмы классификации.

Традиционные алгоритмы классификации используют различные функции, описанные в Разделе 3.2, для проведения различия между созданными человеком и сгенерированными LLM текстами. Некоторые из часто используемых алгоритмов – это машины опорных векторов, наивные байесовские

[8] Massarelli L., Petroni F., Piktus A., Ott M., Rocktäschel T., Plachouras V., Silvestri F., Riedel S. How Decoding Strategies Affect the Verifiability of Generated Text. // Association for Computational Linguistics Minnesota. 2020. Pp. 223–235.

[9] Ma J., Gao W., Joty S., Wong K. Sentence-level evidence embedding for claim verification with hierarchical attention networks. // Association for Computational Linguistics. Florence. 2019. Pp. 2561–2571.

[10] Zhong W., Tang D., Xu Z., Wang R., Duan N., Zhou M., Wang J., Yin J. Neural Deepfake Detection with Factual Structure of Text. // Association for Computational Linguistics Minnesota. 2020. Pp. 2461–2470.

[11] Shakeel D., Jain N. Fake news detection and fact verification using knowledge graphs and machine learning. 2021. DOI 10.13140/RG.2.2.18349.41448.

алгоритмы и деревья решений. К примеру, Фройлинг (Fröhling) и др. использовали модели линейной регрессии, SVM и случайных лесов, построенные на статистических и лингвистических особенностях, для успешной идентификации текстов, сгенерированных моделями GPT-2, GPT-3 и Grover[12]. Аналогичным образом, Солэйман (Solaiman) и др. достигли высокого уровеня идентификации текстов, сгенерированных GPT-2, благодаря сочетанию функций TF-IDF unigram и bigram с моделью логистической регрессии[13]. Кроме того, исследования также показали, что использование предварительно обученных языковых моделей для извлечения семантических текстовых признаков с последующим SVM для классификации может превзойти использование только метода статистических признаков[14]. Одним из преимуществ этих алгоритмов является их интерпретируемость, позволяющая исследователям анализировать важность входных функций и понимание того, почему модель классифицирует тексты как сгенерированные LLM или нет.

3.3.2 Подходы к глубокому обучению

В дополнение к использованию намеренно выделенных свойств для обнаружения в недавних исследованиях изучалось использование языковых моделей, таких как RoBERTa[15], в качестве основы. Такой подход предполагает тонкую настройку языковых моделей, основанных на комбинации текстов, созданных человеком и сгенерированных LLM, что позволяет улавливать текстовые различия имплицитно. В большинстве исследований используется парадигма контролируемого обучения для обучения языковой модели, как продемонстрировано Ипполито (Ippolito) и др.[16], которые доработали BERT. Их исследование показало, что проверяющие люди обладают значительно меньшей точностью, чем автоматические дискриминаторы, при идентификации сгенерированного LLM текста. При ситуации с ограниченным уровнем ресурсов Родригез (Rodriguez) и др.[17], показали,

[12] Fröhling L., Zubiaga A. Feature-based detection of automated language models: tackling GPT-2, GPT-3 and Grover // PeerJ Computer Science. 2021. Vol. 7. Pp. 1–23. DOI 10.7717/peerj-cs.443.

[13] Solaiman I., Brundage M., Clark J., Askel A., Herbert-Voss A., Wu J., Radford A., Krueger G., Kim J. W., Kreps S. Release strategies and the social impacts of language models. 2019. Pp. 1–46.

[14] Crothers E., Japkowicz N., Viktor H., and Branco P. Adversarial Robustness of Neural-Statistical Features in Detection of Generative Transformers. // Institute of Electrical and Electronics Engineers. Padua. 2022. Pp. 1–8.

[15] Liu Y., Ott M., Goyal N., Du J., Joshi M., Chen D., Levy O., Lewis M., Zettlemoyer L., Stoyanov V. Roberta: A robustly optimized bert pretraining approach 2019. Pp. 1–13.

[16] Ippolito D., Duckworth D., Callison-Burch C., Eck D. Automatic Detection of Generated Text is Easiest when Humans are Fooled. // Association for Computational Linguistics. Pp. 1808–1822.

[17] Rodriguez J., Hay T., Gros D., Shamsi Z., Srinivasan R. Cross-Domain Detection of GPT-2-Generated Technical Text. // Association for Computational Linguistics. Seattle. Pp. 1213–1233.

что нескольких сотен помеченных внутри-доменных аутентичных и синтетических текстов достаточно для надёжной работы, даже в условиях отсутствия полной информации от генератора текста LLM. Несмотря на высокую производительность в рамках парадигм контролируемого обучения, получение аннотаций к данным обнаружения может быть сложной задачей в реальных приложениях, что в некоторых случаях делает контролируемые парадигмы неприменимыми. Недавнее исследование[18] решает эту проблему путём обнаружения документов, сгенерированных LLM, с использованием повторяющихся n-грамм высшего порядка, которые могут быть обучены в рамках неконтролируемых парадигм обучения, не требуя наборов данных, сгенерированных LLM, в качестве обучающих значений. Помимо использования языковой модели в качестве основы, недавние исследования показали, что контекстуальную структуру можно рассматривать как граф, содержащий объекты, упомянутые в текстах, и семантически релевантные связи, который использует нейросеть Deep graph для захвата структурных особенностей документа для обнаружения информации, генерируемой LLM[19]. В то время, как глубокие подходы к обучению часто показывают значительные результаты обнаружения, их природа, как «чёрного ящика», серьёзно ограничивает интерпретируемость. Следовательно, исследователи обычно полагаются на инструменты интерпретации, чтобы понять логическое обоснование решений модели.

4. Метод белого ящика

В случае тестирования по методу белого ящика детектор получает полный доступ к модели целевого языка, облегчая интеграцию скрытых водяных знаков в свои выходные данные для отслеживания подозрительных или несанкционированных действий. В этом разделе мы сначала обрисуем три обязательных условия для водяных знаков в NLG. Далее мы представим краткий обзор двух основных классификаций стратегий нанесения водяных знаков белого ящика: апостериорных «водяных знаков» и «водяных знаков» времени вывода.

4.1 Требования к водяным знакам

Основываясь на предыдущих исследованиях в области традиционных цифровых водяных знаков, мы выдвинули три важнейших требования к ним в области NLG: 1) Эффективность: водяной знак должен быть эффективно встроен в сгенерированные тексты и поддаваться проверке при сохранении качества сгенерированных текстов. 2) Секретность: для достижения незаметности водяной знак должен быть интегрирован без внесения заметных изменений, которые могли бы быть легко обнаружены

[18] Gallé M., Rozen J., Kruszewski G., Elsahar H. Unsupervised and distributional detection of machine-generated text. 2021. P. 2.

[19] Wanjun Z., Duyu T., Zenan X., Ruize W., Nan D., Ming Z., Jiahai W., Jian Y. Neural Deepfake Detection with Factual Structure of Text. Minnesota. 2020. Pp. 2461–2470.

автоматическими классификаторами. В идеале он должен быть неотличим от текстов без водяных знаков. 3) Надёжность: водяной знак должен быть устойчивым, и его трудно удалить с помощью обычных модификаций, таких как замена синонимов. Чтобы устранить водяной знак, злоумышленникам потребуется внести значительные изменения, которые сделают тексты непригодными для использования. Эти три требования формируют основу для водяных знаков NLG и гарантируют отслеживание текстов, сгенерированных LLM.

4.2 Последующее нанесение водяных знаков

Учитывая специфику текста, сгенерированный LLM, специальные водяные знаки встроят в него скрытое сообщение или идентификатор. Проверка водяного знака выполняется путём восстановления скрытого сообщения из подозрительного текста. Существуют две основные категории методов апостериорного нанесения водяных знаков: подходы, основанные на правилах, и подходы, основанные на нейросетях.

4.2.1 Подходы, основанные на правилах.

Первоначально исследователи естественного языка адаптировали методы мультимедийного нанесения водяных знаков, которые были нелингвистическими по своей природе и в значительной степени основывались на изменениях символов. Например, метод водяного знака со сдвигом строки включает в себя перемещение строки текста вверх или вниз (или влево, или вправо) на основе двоичного сигнала (водяного знака)[20]. Однако эти подходы имели ограниченную применимость и не были устойчивы к переформатированию текста[21]. Более поздние исследования сместились в сторону использования синтаксической структуры для нанесения водяных знаков. Исследование, проведённое Аталла (Atallah) и др.[22], выявило перспективные возможности использования встроенных водяных знаков в проанализированные синтаксические древовидные структуры, сохраняющие смысл оригинальных текстов и делающие водяные знаки неразборчивыми для тех, кто не знаком с измененной древовидной структурой. Кроме того, синтаксические древовидные структуры трудно удалить с помощью редактирования и водяные знаки остаются в силе, когда текст переведён на другие языки. Дальнейшие усовершенствования были внесены в серию работ, где предлагались варианты метода, встраивающего водяные знаки на основе таблиц

[20] Brassil J. T., Low S., Maxemchuk N. F., O'Gorman L. Electronic marking and identification techniques to discourage document copying. // IEEE Journal on Selected Areas in Communications 13. 1995. № 8. Pp. 1495–1504.

[21] Kankanhalli M.S., Hau K.F. Watermarking of electronic text documents. // Electronic Commerce Research 2. 2002. Pp. 169–187.

[22] Atallah M. J., Raskin V., Crogan M., Hempelmann C., Kerschbaum F., Mohamed D., Naik S. Natural language watermarking: Design, analysis, and a proof-ofconcept implementation. // IH. Pittsburgh. 2001. Pp. 185–200.

синонимов вместо просто деревьев синтаксического анализа[23]. Наряду с синтаксической структурой исследователи также использовали семантическую структуру текста для встраивания водяных знаков, которая включает в себя использование признаков, заключающихся в глаголах, существительных, предлогах, правописании, сокращениях, правилах грамматики и т. д. Например, был предложен подход к замене синонимов, при котором водяные знаки внедряются путём замены определенных слов с их синонимами без изменения контекста[24]. Как правило, методы, основанные на правилах, используют фиксированные замены на основе нормативов, которые могут систематически изменять текстовую статистику, ставя под угрозу секретность водяного знака и позволяя злоумышленникам обнаружить и удалить водяной знак.

4.2.2 Подходы, основанные на нейросетях

В отличие от методов, основанных на правилах, требующих значительные инженерные усилия для проектирования, подходы, основанные на нейронных сетях, рассматривают процесс сбора информации как сквозной процесс обучения. Типично, они включают в себя три компонента: сеть кодировщика водяных знаков, сеть декодера водяных знаков и сеть дискриминатора[25]. Учитывая целевой текст и секретное сообщение (например, случайные двоичные биты), сеть кодирования водяных знаков генерирует изменённый текст, который включает в себя секретное сообщение. Затем сеть декодирования водяных знаков пытается извлечь секретное сообщение из изменённого текста. Одна из проблем заключается в том, что сеть кодировщиков водяных знаков может существенно изменить языковую статистику. Для решения этой проблемы фреймворк использует стратегию состязательного обучения и включает в себя сеть дискриминаторов[26]. Сеть распознавания принимает целевые тексты и тексты с водяными знаками в качестве входных данных и стремится различать их, в то время как сеть кодирования водяных знаков стремится сделать их неразличимыми. Тренировочный процесс продолжается до тех пор, пока три компонента не достигнут удовлетворительного уровня производительности. Для нанесения водяных знаков на текст, сгенерированный LLM, разработчики могут использовать сеть кодировщика водяных знаков для встраивания предварительно настроенного секретного сообщения в выходные данные LLM, а сеть декодера водяных

[23] Jalil Z., Mirza A. M. A review of digital watermarking techniques for text documents. // IEEE Computer Society. Washington DC. 2009. Pp. 230–234.

[24] Topkara U., Topkara M., Atallah M. J. The hiding virtues of ambiguity: quantifiably resilient watermarking of natural language text through synonym substitutions. // Association for Computing Machinery. Geneva. 2006. Pp. 164–174.

[25] Abdelnabi S., Fritz M. Adversarial watermarking transformer: Towards tracing text provenance with data hiding. // Institute of Electrical and Electronics Engineers. 2021. Pp. 121–140.

[26] Goodfellow I., Pouget-Abadie J., Mirza M., Xu B., Warde-Farley D., Ozair S., Courville A., Bengio Y. Generative adversarial networks. // Commun. ACM 63. 2020. №11. Pp. 139–144.

знаков – для проверки подозрительных текстов. Хотя подходы, основанные на нейросетях, устраняют необходимость в разработке правил вручную, присущая им недостаточная интерпретируемость вызывает опасения относительно правдивости и наличия математических гарантий эффективности, секретности и надёжности водяного знака.

4.3 Водяной знак времени вывода

Водяные знаки времени вывода предназначены для процесса декодирования LLM, в отличие от апостериорных водяных знаков, которые наносятся после генерации текста. Языковая модель выдаёт распределение вероятности для последующего слова в последовательности, основанное на предыдущих словах. Стратегия декодирования, которая является алгоритмом, выбирающим слова из этого распределения для создания последовательности, предлагает возможность встроить водяной знак, изменив процесс выбора слова.

Показательный пример этого метода можно найти в исследовании, проведённом Киршенбауер (Kirchenbauer) и др.[27] Во время генерации токена создаётся хэш-код на основе ранее сгенерированного токена, который затем используется для заполнения генератора случайных чисел. Это начальное значение случайным образом делит весь словарный запас на «зелёный список» и «красный список» равного размера. Следующий токен впоследствии генерируется из «зелёного списка». Таким образом, водяной знак встраивается в каждое сгенерированное слово, как показано на рисунке 4.

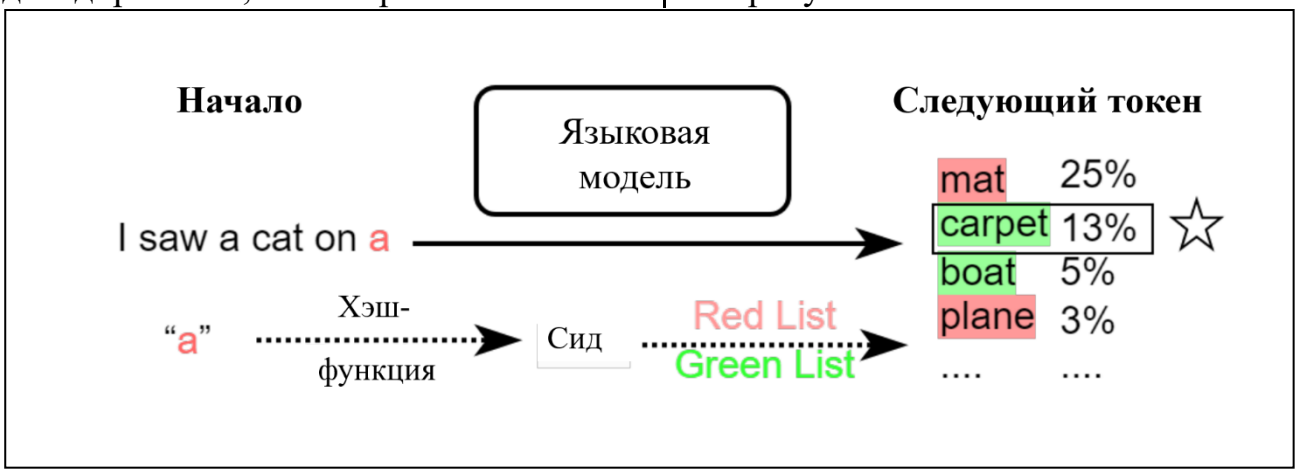

Рис. 4 Схема водяных знаков времени вывода. Случайный сид генерируется хэшированием предыдущего токена «a», разделением всех вариантов слов на «зелёный список» и «красный список». Следующий токен «carpet» выбирается из зелёного списка.

Чтобы обнаружить водяной знак, третья сторона, владеющая хэш-функцией и генератором случайных чисел, может воспроизвести красный список для каждого токена и подсчитать количество нарушений

[27] Kirchenbauer J., Geiping J., Wen Y., Katz J., Miers I., Goldstein T. A Watermark for Large Language Models. 2023.

правила красного списка, таким образом проверяя подлинность текста. Вероятность того, что природный источник производит токены N без нарушения правила красного списка, составляет всего ½ N, что исчезающе мало даже для текстовых фрагментов с несколькими десятками слов. Чтобы удалить водяной знак, злоумышленникам необходимо изменить по крайней мере половину токенов документа. Однако одна из проблем, связанных с этими водяными знаками во время вывода, заключается в том, что контролируемый процесс выборки может существенно повлиять на качество сгенерированного текста. Одним из решений является ослабление ограничений на использование водяных знаков, например, увеличение размера словаря зелёного списка, и стремление к балансу между водяными знаками и качеством текста[1].

5. Опасения авторов

5.1 Ограничения обнаружения «чёрного ящика».

Предвзятость в собранных наборах данных. Сбор данных играет жизненно важную роль в разработке детекторов «чёрного ящика», поскольку именно данные лежат в основе обучения и последующего функционирования таких систем. Однако важно отметить, что процесс сбора данных может приводить к искажениям, которые могут негативно повлиять на производительность и обобщение детектора[2]. Эти предубеждения могут принимать несколько форм. Например, многие существующие исследования, как правило, фокусируются только на одной или нескольких конкретных задачах, таких как ответы на вопросы или подготовка новостей, что может привести к несбалансированному распределению темы в данных и ограничивают способность детектора к обобщению. Кроме того, человеческие артефакты могут быть легко введены во время сбора данных, как показано в исследовании, проведенном Guo и др.[3], где отсутствие инструкций по стилю сбора ответов, сгенерированных LLM, привели к тому, что ChatGPT выдал результаты с нейтральным настроем. Эти ложные корреляции могут улавливаться и даже усиливаться детектором, что приводит к низкой производительности обобщения при развёртывании в реальных приложениях.

Калибровка достоверности. В развитии реального мира в системах обнаружения крайне важно не только иметь точные классификации, но и указывать на вероятность их ошибочности. Например, текст, с вероятностью 98 % сгенерированный LLM, следует считать с большей вероятностью сгенерированным машиной, чем текст с аналогичной вероятностью на уровне 90 %. Другими словами, предсказанные уровни вероятности должны отражать его

[1] Kirchenbauer J., Geiping J., Wen Y., Katz J., Miers I., Goldstein T. A Watermark for Large Language Models. 2023.

[2] Pagnoni A., Graciarena M., Tsvetkova Y. Threat Scenarios and Best Practices to Detect Neural Fake News. // International Committee on Computational Linguistics. Gyeongju. 2022. Pp. 1233–1249.

[3] Guo B., Zhang X., Wang Z., Jiang M., Nie J., Ding Y., Yue J., Wu Y. How Close is ChatGPT to Human Experts? Comparison Corpus, Evaluation, and Detection. 2023.

правильность. Точные показатели достоверности имеют первостепенное значение для оценки надёжности системы, поскольку они предлагают ценную информацию для пользователей, позволяя установить доверие к системе, особенно для нейросетей, чьи решения могут быть сложными для интерпретации. Хотя нейросети демонстрируют большую точность, чем традиционные модели классификации, обширные исследования в различных областях подчеркнули отсутствие у них надлежащей калибровки[4]. Исследований, посвящённых точности оценки достоверности в темах распознавания текста, генерируемых LLM, остаётся мало. Поэтому важно откалибровать показатели достоверности для классификаторов обнаружения «чёрного ящика», которые часто используют нейронные модели.

По нашему мнению, хотя в настоящее время обнаружение «чёрного ящика» работает благодаря выявляемым сигналам, оставляемым языковыми моделями в сгенерированном тексте, оно постепенно станет менее жизнеспособным по мере расширения возможностей языковой модели и в итоге станет неосуществимым. В свете быстрого улучшения текста, генерируемого LLM, будущее надёжных инструментов обнаружения лежит в подходах к обнаружению водяных знаков в «белых ящиках».

5.2 Отсутствие всеобъемлющих показателей оценки

Существующие исследования часто полагаются на такие показатели, как AUC или точность, для оценки эффективности обнаружения. Однако эти показатели учитывают только средний случай и недостаточны для анализа безопасности. Рассмотрим сравнение двух детекторов: Детектор A идеально идентифицирует 1 % текстов, сгенерированных LLM, но в остальных случаях достигает успеха со случайной вероятностью 50 %. Детектор B завершается успешно с 50,5 % по всем данным. В среднем два детектора имеют одинаковую точность обнаружения или AUC. Однако детектор A демонстрирует исключительную эффективность, в то время как детектор B практически неэффективен. Чтобы узнать, может ли детектор надежно идентифицировать текст, сгенерированный LLM, исследователям необходимо рассмотреть режим низкой частоты ложноположительных результатов (FPR) и сообщать о частоте истинных срабатываний детектора (TPR) при низкой частоте ложноположительных результатов. Эта цель разработки методов, основанных на режимах с низким уровнем ложноположительных результатов, широко используется в компьютерной безопасности[5]. Это особенно важно для групп населения,

[4] Guo C., Pleiss G., Sun Y., Weinberger K. Q. On calibration of modern neural networks. // In International conference on machine learning. PMLR. 2017. Pp. 1321–1330.

[5] Kantchelian A., Tschantz M. C., Afroz S., Miller B., Shankar V., Bachwani R., Joseph A. D., Tygar J. D. Better malware ground truth: Techniques for weighting anti-virus vendor labels. // Association for Computing Machinery. Denver. 2015. Pp. 45–56.

которые создают необычный текст, например, для людей, не являющихся носителями языка. Такие группы населения могут быть особенно подвержены риску ложноположительных результатов, что может привести к серьёзным последствиям, если описанные детекторы внедрить в систему образования.

5.3 Угрозы, исходящие от LLM с открытым исходным кодом.

Существующие методы обнаружения основаны на предположении, что LLM контролируется разработчиками и предлагается в качестве услуги конечным пользователям, это соотношение «один ко многим» способствует целям обнаружения. Однако проблемы возникают, когда разработчики открывают исходные коды своих моделей или когда хакеры крадут их. Например, последний LLM от Meta[6], LLaMA, изначально был доступен по запросу. Но всего через неделю после принятия запросов на доступ он просочился в Сеть через торрент 4chan, что вызвало опасения по поводу потенциального всплеска персонализированного спама и фишинга[7]. Как только конечный пользователь получает полный доступ к LLM, возможность изменять поведение LLM препятствует обнаружению «чёрного ящика» для идентификации обобщённых языковых сигналов. Встраивание водяных знаков в выходные данные LLM является одним из потенциальных решений, поскольку разработчики могут интегрировать скрытые водяные знаки в выходные данные LLM, прежде чем делать модели с открытым исходным кодом. Однако его всё ещё можно обойти, поскольку пользователи имеют полный доступ к модели и могут точно настроить её или изменить стратегии выборки, чтобы стереть существующие водяные знаки. Для решения этой проблемы разработчики могут увеличить уязвимость параметров модели для предотвращения модификации конечным пользователем, где незначительное изменение параметров модели может привести к значительному снижению производительности. Однако предыдущие исследования были проведены на миниатюрной модели крошечных задач классификации, что делает неясным, могут ли эти методы быть применены к большим языковым моделям. Учитывая значительные затраты и усилия, связанные с обучением LLM, в настоящее время маловероятно, что разработчики выпустят свои самые мощные продукты. Тем не менее, обнаружение текстов, сгенерированных LLM, из моделей с открытым исходным кодом остаётся важнейшей задачей, заслуживающей внимания в будущем.

6. Заключение

[6] Компания Meta Platforms Inc. признана экстремистской, запрещена в России и внесена Росфинмониторингом в перечень террористов и экстремистов.

[7] Vincent J. Meta’s powerful AI language model has leaked online – what happens now? // The Verge [Electronic resource]. 2023, March 8. URL: https://www.theverge.com/2023/3/8/23629362/meta-ai-language-model-llama-leak-online-misuse (дата обращения: 08.05.2023).

Обнаружение текстов, сгенерированных LLM, – это быстро растущая и развивающаяся область с множеством новых разработанных методов. Этот исследование обеспечивает точную классификацию и углублённое изучение существующих подходов, чтобы помочь исследовательскому сообществу понять сильные стороны и ограничения каждого метода[8]. Несмотря на стремительный прогресс в области обнаружения текста, генерируемого LLM, по-прежнему необходимо решать значительные задачи определения авторства. Дальнейший прогресс в этой области потребует разработки инновационных решений для преодоления этих проблем.

Список литературы

1. Abdelnabi S., Fritz M. Adversarial watermarking transformer: Towards tracing text provenance with data hiding // 2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021. Pp. 121-140.

2. Atallah M. J. [et al]. Natural language watermarking: Design, analysis, and a proof-of-concept implementation // Information Hiding: 4th International Workshop, IH 2001 Pittsburgh, PA, USA, April 25–27, 2001 Proceedings 4. Springer Berlin Heidelberg, 2001. Pp. 185–200.

3. Bhatt P., Rios A. Detecting Bot-Generated Text by Characterizing Linguistic Accommodation in Human-Bot Interactions // arXiv preprint arXiv:2106.01170. 2021.

4. Brassil J. T. [et al]. Electronic marking and identification techniques to discourage document copying // IEEE Journal on Selected Areas in Communications. 1995. Vol. 13. №. 8. Pp. 1495–1504.

5. Brown P. F. [et al]. An estimate of an upper bound for the entropy of English // Computational Linguistics. 1992. Vol. 18. №. 1. Pp. 31-40.

6. Clark E. [et al]. All that's' human'is not gold: Evaluating human evaluation of generated text // arXiv preprint arXiv:2107.00061. 2021.

7. Crothers E. [et al]. Adversarial Robustness of Neural-Statistical Features in Detection of Generative Transformers // 2022 International Joint Conference on Neural Networks (IJCNN). IEEE, 2022. С. 1–8.

8. Dugan L. [et al]. RoFT: A tool for evaluating human detection of machine-generated text // arXiv preprint arXiv:2010.03070. 2020.

9. Dugan L. [et al]. Real or Fake Text: Investigating Human Ability to Detect Boundaries Between Human-Written and Machine-Generated Text // arXiv preprint arXiv:2212.12672. 2022.

10. Elsen-Rooney M. NYC education department blocks ChatGPT on school devices, networks // Communication of the ACM [Electronic resource]. 2023, 6 января. URL: https://cacm.acm.org/news/268457-nyc-education-dept-blocks-chatgpt-on-school-devices-networks/fulltext (дата обращения: 08.05.2023).

[8] Wang L., Xu S., Xu R., Wang X., Zhu Q. NonTransferable Learning: A New Approach for Model Ownership Verification and Applicability Authorization. // Committee of ICLR. 2022. Рз. 1–24.

11. Fan A. [et al]. ELI5: Long form question answering // arXiv preprint arXiv:1907.09190. 2019.

12. Floridi L., Chiriatti M. GPT-3: Its nature, scope, limits, and consequences // Minds and Machines. 2020. T. 30. Pp. 681–694.

13. Fröhling L., Zubiaga A. Feature-based detection of automated language models: tackling GPT-2, GPT-3 and Grover // PeerJ Computer Science. 2021. Vol. 7. Pp. 1–23. DOI 10.7717/peerj-cs.443.

14. Gallé M. [et al]. Unsupervised and distributional detection of machine-generated text // arXiv preprint arXiv:2111.02878. 2021.

15. Gehrmann S., Strobelt H., Rush A. M. Gltr: Statistical detection and visualization of generated text // arXiv preprint arXiv:1906.04043. 2019.

16. Goodfellow I. et al. Generative adversarial networks // Communications of the ACM. 2020. Vol. 63. №. 11. Pp. 139–144.

17. Guggenberger N. From Fake News to Fake Views: New Challenges Posed by ChatGPT-Like AI // LawFareBlog [Electronic resource]. 2023. January 20. URL: https://www.lawfareblog.com/fake-news-fake-views-new-challenges-posed-chatgpt-ai (дата обращения: 08.05.2023).

18. Guo B. [et al]. How Close is ChatGPT to Human Experts? Comparison Corpus, Evaluation, and Detection // arXiv preprint arXiv:2301.07597. 2023.

19. Guo C. [et al]. On calibration of modern neural networks // International conference on machine learning. PMLR, 2017. С. 1321–1330.

20. Holtzman A. [et al]. The curious case of neural text degeneration // arXiv preprint arXiv:1904.09751. 2019.

21. Ippolito D. [et al]. Automatic detection of generated text is easiest when humans are fooled // arXiv preprint arXiv:1911.00650. 2019.

22. Jalil Z., Mirza A. M. A review of digital watermarking techniques for text documents // 2009 International Conference on Information and Multimedia Technology. IEEE, 2009. Pp. 230–234.

23. Kankanhalli M. S., Hau K. F. Watermarking of electronic text documents // Electronic Commerce Research. 2002. Vol. 2. Pp. 169–187.

24. Kirchenbauer J. [et al]. A watermark for large language models // arXiv preprint arXiv:2301.10226. 2023.

25. Liu Y. [et al]. Roberta: A robustly optimized bert pretraining approach // arXiv preprint arXiv:1907.11692. 2019.

26. Ma J. [et al]. Sentence-level evidence embedding for claim verification with hierarchical attention networks. Association for Computational Linguistics, 2019.

27. Massarelli L. [et al]. How decoding strategies affect the verifiability of generated text // arXiv preprint arXiv:1911.03587. 2019.

28. Pagnoni A., Graciarena M., Tsvetkov Y. Threat Scenarios and Best Practices to Detect Neural Fake News // Proceedings of the 29th International Conference on Computational Linguistics. 2022. Pp. 1233–1249.

29. Piantadosi S. T. Zipf's word frequency law in natural language: A critical review and future directions //Psychonomic bulletin & review. 2014. Vol. 21. Pp. 1112–1130.

30. Rodriguez J. [et al]. Cross-Domain Detection of GPT-2-Generated Technical Text // Proceedings of the 2022 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies. 2022. Pp. 1213–1233.

31. Shakeel D., Jain N. Fake news detection and fact verification using knowledge graphs and machine learning. 2021. DOI 10.13140/RG.2.2.18349.41448.

32. Solaiman I. [et al]. Release strategies and the social impacts of language models // arXiv preprint arXiv:1908.09203. 2019.

33. Tillmann C., Ney H. Word reordering and a dynamic programming beam search algorithm for statistical machine translation // Computational linguistics. 2003. Vol. 29. №. 1. Pp. 97–133.

34. Topkara U., Topkara M., Atallah M. J. The hiding virtues of ambiguity: quantifiably resilient watermarking of natural language text through synonym substitutions // Proceedings of the 8th workshop on Multimedia and security. 2006. Pp. 164–174.

35. Vincent J. Meta's powerful AI language model has leaked online – what happens now? // The Verge [Electronic resource]. 2023, March 8. URL: https://www.theverge.com/2023/3/8/23629362/meta-ai-language-model-llama-leak-online-misuse (дата обращения: 08.05.2023).

36. Wang L. [et al]. Non-transferable learning: A new approach for model ownership verification and applicability authorization // arXiv preprint arXiv:2106.06916. 2021.

37. Zhong W. [et al]. Neural deepfake detection with factual structure of text // arXiv preprint arXiv:2010.07475. 2020.

Dmitry V. Usikov
Student at the Faculty of Investigative Training
Moscow Academy of the Investigative Committee of the Russian Federation
(Moscow, Russian Federation)
u.dmitriy.d@mail.ru

Mikhail Yu. Satayev
Student at the Faculty of Investigator Training
Moscow Academy of the Investigative Committee of the Russian Federation
(Moscow, Russian Federation)
sataev814@gmail.com

Scientific Supervisor: Svetlana V. Rudakova
Doctor in Psychology, Associate Professor,
Moscow Academy of the Investigative Committee of the Russian Federation
(Moscow, Russian Federation)
rudakova@mail.ru

THE SCIENCE OF DETECTING LLM-GENERATED TEXTS

Abstract. The emergence of large language models (LLMs) has resulted in the production of LLM-generated texts that is highly sophisticated and almost indistinguishable from texts written by humans. However, this has also sparked concerns about the potential misuse of such texts, such as spreading misinformation and causing disruptions in the education system. Although many detection approaches have been proposed, a comprehensive understanding of the achievements and challenges is still lacking. This survey aims to provide an overview of existing LLM-generated text detection techniques and enhance the control and regulation of language generation models. Furthermore, we emphasize crucial considerations for future research, including the development of comprehensive evaluation metrics and the threat posed by open-source LLMs, to drive progress in the area of LLM-generated text detection.

Keywords: large language models, black-box detection, white-box detection, ChatGPT, natural language generation.

УДК 343

Цветкова Анна Денисовна
Студент Института юстиции
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Россия)
at@crimlib.info

Научный руководитель: Бахтеев Дмитрий Валерьевич,
доктор юридических наук, доцент
доцент кафедры криминалистики
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
ae@crimlib.info

ПРОБЛЕМЫ И ПУТИ АКТУАЛИЗАЦИИ СОДЕРЖАНИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ «CRIMLIB – СПРАВОЧНИК СЛЕДОВАТЕЛЯ»*

Аннотация. В статье рассматриваются проблемы, затрудняющие добавление актуального контента в мобильное приложение «CrimLib – Справочник следователя»: отсутствие достаточного количества временных и кадровых ресурсов; большой объём требующей обработки информации; необходимость соблюдения баланса между краткостью и полнотой рекомендаций; важность достижения равновесия между общедоступностью и защищённостью информации. Предлагаются пути их разрешения, а также описываются перспективные направления развития рассматриваемого приложения: адаптация изложенных в нём алгоритмов ко всем новеллам действующего законодательства; оптимизация и усовершенствование навигации по приложению, в том числе посредством гиперссылок; установление взаимодействия с практическими сотрудниками следственных органов и отечественными научными коллективами, занятыми близкими к рассматриваемому в статье проектами и др.

Ключевые слова: «CrimLib – Справочник следователя», электронный справочник судебных экспертиз, алгоритмизация следственной деятельности, интеграция науки и практики.

Для цитирования:
Цветкова А. Д. Проблемы и пути актуализации содержания мобильного приложения «CrimLib – Справочник следователя» // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 476–482.

* Исследование выполнено при финансовой поддержке УрГЮУ имени В.Ф. Яковлева в рамках реализации проекта ведущей научной школы № 0304/23.

Быстрые темпы повседневной жизни современного человека, большие объёмы информации, увеличивающиеся по экспоненте, оказывают влияние на все сферы деятельности. Не является исключением и деятельность по раскрытию и расследованию преступлений: постоянно появляются новые преступления, злоумышленники совершенствуют свои подходы к совершению противоправных деяний и сокрытию их следов; Верховный суд регулярно принимает Постановления Пленума, призванные разрешить спорные аспекты применения существующего уголовного законодательства, которое также обновляется согласно актуальным вызовам безопасности государства, общества и отдельных лиц. Криминалистическая наука также не стоит на месте, разрабатывая методические, технические и тактические рекомендации, призванные помочь субъектам расследования (следователям, дознавателям, оперативным сотрудникам, судебным экспертам) и повысить эффективность их работы. В связи с этим перед следователем (равно как и перед иными субъектами раскрытия и расследования преступлений) встаёт проблема «двигаться в ногу со временем» – то есть отслеживать, обрабатывать, запоминать и прикладывать к своей служебной деятельности все законодательные предписания, научные рекомендации, типичные практические кейсы. Следует отметить, что указанная задача не нова: на обязанность следователя владеть большим объёмом разнообразных по своей природе знаний указывал ещё основатель криминалистической науки Г. Гросс[1]. Считаем, что в условиях ограниченности доступных и освоенных возможностей человека (в первую очередь – его памяти) данная задача невыполнима. Однако помочь в её решении могут ресурсы, всегда находящейся вместе с человеком[2] и играющие роль «внешней памяти»[3], к числу которых относится мобильное приложение «Справочник следователя – CrimLib.info», разработанное на кафедре криминалистики УрГЮУ имени В. Ф. Яковлева с соответствующей целью.

Практика показывает значительную востребованность данного Приложения среди студентов, преподавателей и практических сотрудников следственных органов МВД России и СК России, что объясняется рядом достоинств, подробно описанных в научных статьях разработчиков[4]. Однако

[1] Гросс Г. Руководство для судебных следователей как система криминалистики. М. ЛексЭст, 2002. С. 6.

[2] Гармаев Ю. П., Чумаков А. В. Мобильные приложения и иные инновационные средства обучения в криминалистике // Современные технологии и подходы в юридической науке и образовании: Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. С. 272.

[3] Storm B., Stone S., Aaron B. Using the Internet to access information inflates future use of the Internet to access other information. // Memory. 2017. № 25. P.717. DOI 10.1080/09658211.2016.1210171.

[4] См. например: Беляков А. А., Бахтеев Д. В. Мобильный справочник следователя:

следует констатировать, что на сегодняшний день дальнейшая актуализация материалов приложения столкнулась с различного рода проблемами, ограничивающими развитие описанного проекта.

В первую очередь необходимо указать на кадровые преграды. Как было указано в начале работы, регулярно появляется большое количество новой информации, необходимой следователю для успешного выполнения своих должностных обязанностей, и, в той же мере, что один следователь не способен отследить и обработать все новшества, существующий на сегодняшний день коллектив, поддерживающий мобильный справочник, не имеет такой возможности. Это связано с рабочей и учебной нагрузкой, обязательствами по различным научным проектам, ограниченностью профессиональной области рамками криминалистики, тогда как Справочник аккумулирует в себе также знания из уголовного права, уголовного процесса, судебной экспертизы. Таким образом, для того чтобы обеспечить наполнение справочника актуальными материалами необходимо: расширить штат задействованных лиц и привлечь специалистов из других наук уголовно-правового цикла. Однако при этом невозможно нанять сотрудников на полный рабочий день, поскольку новые материалы не появляются со стабильной регулярностью. В связи с этим оптимальным представляется вариант привлечения заинтересованных сотрудников смежных кафедр, в том числе, из других вузов, с распределением обязанностей для исключения проблемы возможного дублирования функций. Весьма печальным видится невозможность привлечения студентов к деятельности по актуализации содержания Справочника, к чему, например, располагает появившаяся в 2023 году в УрГЮУ имени В. Ф. Яковлева дисциплина «Проектная деятельность», поскольку требуется такой объём знаний, который позволит выделить только по-настоящему существенное из всего объёма информации, что представляется невыполнимым без практического и (или) преподавательского опыта в соответствующих сферах. Хотя следует указать, что Ю. П. Гармаев и А. В. Чумаков предлагают задействовать студентов для разработки учебных криминалистических приложений[5].

состояние и перспективы // Современные технологии и подходы в юридической науке и образовании: Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. С. 279–285; Беляков А. А., Бахтеев Д. В. Мобильный справочник следователя: содержание и технические условия разработки // Технологии XXI века в юриспруденции: Материалы Всероссийской научно-практической конференции, Екатеринбург, 24–25 мая 2019 года / Под редакцией Д. В. Бахтеева. Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2019. С. 23–26.

[5] Гармаев Ю. П., Чумаков А. В. Мобильные приложения и иные инновационные средства обучения в криминалистике // Современные технологии и подходы в юридической науке и образовании: Сборник материалов

Считаем, что учебные и рабочие задачи не могут быть сопоставимы в полной мере, в связи с чем, допустимость привлечения студентов к созданию материалов в образовательных целях не гарантирует такой же успех при реализации практико-ориентированных проектов.

Следующая проблема заключается в соблюдении баланса между краткостью и полнотой. Так, для удобства восприятия большинство рекомендаций в Справочнике представлено в виде алгоритмов (оптимальных последовательностей действий), занимающих не более 3–4 экранов смартфона. Одновременно с этим, стилистика юридического научного языка предполагает сложные предложения и длинные мысли, которые, соответственно, требуется перерабатывать в оптимальные краткие рекомендации, для чего необходим отдельный навык, а также значительные временные затраты.

Рассматривая отдельные аспекты перечисленных выше проблем, нельзя не упомянуть, что не всегда различные научные разработки носят в действительности обоснованный характер, содержат в себе апробированные методики, в связи с чем отдельную сложность представляет необходимость проверки отдельных фактов перед их включением в справочник. Помимо этого, не всегда даже самые ценные научные разработки соответствуют практическим возможностям, оснащению следственных органов, таким образом их отражение в справочнике будет перегружать контент без действительной пользы для сотрудников, выступающих целевой аудиторией. В этой связи считаем, что для актуализации материалов в Справочнике необходимо иметь постоянную возможность получения обратной связи от действующих следователей, для чего (в идеальной модели) требуется наличие в числе членов научного коллектива человека, ответственного за связи с пользователями Приложения, поскольку имеющиеся в Справочнике контакты разработчиков почти не привлекают внимание тех, для кого они рассчитаны.

Наконец, среди наиболее явных проблем можно назвать также необходимость соблюдения баланса между доступностью информации и защиты критически важных (стратегических) сведений, обеспечивающих успешность в деятельности по раскрытию и расследованию преступлений, от злоумышленников, для которых доступ к ним позволит выработать эффективные методы противодействия. Возможным способом разрешения указанной проблемы является введение двух слоёв представления информации: когда к первому, содержащему общеизвестную информацию, доступ открыт всем желающим, а ко второму, содержащему условно конфиденциальную информацию в дополнение к той, что изложена на первом слое, – только субъектам

международного научно-практического форума, Калининград, 27–31 августа 2020 года. Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. С. 277.

расследования по индивидуальным логинам и паролям, предоставляемым каждому соответствующему подразделению.

Все описанные проблемы привели к тому, что мобильное приложение «CrimLib.info – Справочник следователя» на сегодняшний день нуждается в актуализации содержащихся в нём материалов и добавлении новых разделов.

В первую очередь, видится весьма перспективным автоматизировать работу по своевременному внесению новых Постановлений Пленума ВС РФ и обновлению разработанных ранее, для чего желательной видится непосредственная интеграция соответствующего подраздела Приложения с базами Справочных правовых систем.

Далее, необходимо расширить раздел, посвящённый программам расследования различных видов преступлений, первоочерёдно включив в него методики расследования тех криминальных деяний, которые являются наиболее распространёнными, но ещё не нашли своего отражения в Справочнике или недостаточно детально в нём рассмотрены. В первой тройке из числа таковых можно указать: угрозы убийством или причинением тяжкого вреда здоровью, количество которых в 2022 году составило 2,3 % от числа всех выявленных преступлений (45,1 тыс. из 1 966,8 тыс.), преступления коррупционной направленности (1,8 % или 35,3 тыс.) и грабежи (1,5 % или 29,2 тыс.)[6].

В разделе, посвящённом судебным экспертизам, необходимо обновить систему представления информации и общей навигации. Для этого перспективным представляется сотрудничество с научным коллективом Южно-Уральского государственного университета, возглавляемым Н. П. Папоян, который разрабатывает электронный справочник судебных экспертиз в формате веб-сайта.

Также требуется дополнить раздел «Программы допроса» сведениями, отражающими последние достижения в области судебной (юридической) психологии и оперативной психодиагностики, описав, в частности оптимальные модели установления психологического контакта и ведения допроса с представителями различных доминирующих радикалов[7]. Помимо этого, требуется включить для каждой уже содержащейся в Справочнике программы вариацию производства допроса посредством видео-конференц-связи, так как дистанционных характер накладывает определённые ограничения на эффективность различных «традиционных» следственных действий.

Говоря о новых разделах, которые требуется создать в справочнике, следует указать на запросы в части правил фотофиксации,

[6] Состояние преступности в России за январь – декабрь 2022 г.: статистический сборник / Главный информационный центр МВД России. Москва, 2023. С. 6.

[7] Пономаренко В. В. Практическая характерология: методика 7 радикалов. Москва: Издательство АСТ, 2021. 224 с.

положений цифровой криминалистики, тактических особенностей обыска в различных следственных ситуациях. Небесполезным видится выделение раздела с рассмотрением типичных решений из судебной практики по уголовным делам. Данный перечень не является исчерпывающим, но лишь воспроизводит наиболее интересующие практических работников темы.

Существенная работа требуется в части совершенствования навигации, настройки дополнительных гиперссылок как для переключения между связанными по смыслу статьями, так и для переключения в отдельных случаях на веб-ресурсы (нормативные источники, более подробно рассматривающие тот или иной вопрос статьи в Энциклопедии криминалистики CrimLib).

Работа по указанным направлениям совершенствования мобильного приложения «CrimLib.info – Справочник следователя» в совокупности с разрешением описанных в начале работы проблем позволит повысить эффективность деятельности по раскрытию и расследованию преступлений, обеспечить взаимодействие наук уголовно-правового цикла со следственной практикой; объединить научные усилия и проекты специалистов в сфере наук уголовно-правового цикла по всей России; усовершенствовать инструмент, способный облегчить работу субъектов расследования преступлений, высвободив больше сил для решения стоящих перед ними служебных задач, что представляется необходимым для действенной борьбы с преступностью.

Список литературы

1. Беляков А. А., Бахтеев Д. В. Мобильный справочник следователя: состояние и перспективы // Современные технологии и подходы в юридической науке и образовании: Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. С. 279–285.

2. Беляков А. А., Бахтеев Д. В. Мобильный справочник следователя: содержание и технические условия разработки // Технологии XXI века в юриспруденции: Материалы Всероссийской научно-практической конференции, Екатеринбург, 24–25 мая 2019 года / Под редакцией Д. В. Бахтеева. Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2019. С. 23–26.

3. Гармаев Ю. П., Чумаков А. В. Мобильные приложения и иные инновационные средства обучения в криминалистике // Современные технологии и подходы в юридической науке и образовании: Сборник материалов международного научно-практического форума, Калининград, 27–31 августа 2020 года. Калининград: Балтийский федеральный университет имени Иммануила Канта, 2021. С. 270–278.

4. Гросс Г. Руководство для судебных следователей как система криминалистики. М. ЛексЭст, 2002. 1088 с.

5. Пономаренко В. В. Практическая характерология: методика 7 радикалов. Москва: Издательство АСТ, 2021. 224 с.

6. Storm B., Stone S., Aaron B. Using the Internet to access information inflates future use of the Internet to access other information. // Memory. 2017. № 25. Pp.717–723. DOI 10.1080/09658211.2016.1210171.

Anna D. Tsvetkova
Student at the Institute of Justice
Ural State Law University
named after V. F. Yakovlev
(Ekaterinburg, Russia)
at@crimlib.info

Scientific Supervisor: Dmitry V. Bakhteev,
Doctor of Law, Associate Professor
Associate Professor of the Department of Constitutional Law
named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
ae@crimlib.info

PROBLEMS AND WAYS TO UPDATE THE CONTENT OF THE MOBILE APPLICATION «CRIMLIB – INVESTIGATOR'S GUIDE»

Abstract. This article discusses the problems that make it difficult to add relevant content to the mobile application «CrimLib – Investigator's guide»: the lack of sufficient time and human resources, the large volume of information to be processed, the need to balance between brevity and completeness of the recommendations, the importance of achieving a balance between public availability and security information. The ways of its solution are offered, and also the perspective directions of development of the considered application are described: adaptation of the algorithms stated in it to all innovations of the operating legislation; optimization and perfection of navigation on an application, including by means of hyperlinks; establishment of interaction with practical employees of investigations departments and the domestic scientific collectives occupied with projects similar to the considered in article, etc.

Keywords: «CrimLib – Investigator's guide», electronic forensic handbook, algorithmization of investigative activities, integration of science and practice.

УДК 343.14

Широкова Марина Сергеевна
Студент
Поволжский институт управления
имени П. А. Столыпина – филиал РАНХиГС
(г. Саратов, Российская Федерация)
maribroshi@mail.ru

Научный руководитель: Чурикова Анна Юрьевна
кандидат юридических наук, доцент,
доцент кафедры административного и уголовного права
Поволжский институт управления – филиал РАНХиГС
(г. Саратов, Российская Федерация)
a_tschurikova@bk.ru

ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Аннотация. В статье рассматривается понятие цифровых (электронных) доказательств в уголовном судопроизводстве. Необходимость их применения обусловлена развитием общества, внедрением новых технологий в нашу жизнь, с которыми порой не могут взаимодействовать сотрудники правоохранительных органов по причине отсутствия технической оснащённости и недостаточной квалификации кадров. Освещаются некоторые сложности при работе правоохранительных органов с цифровой информацией.

Ключевые слова: цифровые доказательства, уголовное судопроизводство, цифровые технологии, электронная информация, доказывание.

Для цитирования:
Широкова М. С. Цифровые доказательства в уголовном судопроизводстве // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 483–487.

Цифровизация, информационные технологи, информация в цифровом формате стали частью жизни современного общества, которую невозможно не учитывать при правовом регулировании, в том числе и в сфере уголовного судопроизводства. Одной из наиболее важных областей применения цифровых технологий в уголовном процессе являются, на наш взгляд, цифровые доказательства.

Само понятие цифровых доказательств нормативно не закреплено в российском уголовно-процессуальном законодательстве. Поэтому данное определение является достаточно дискуссионным. Например, В. А. Новицкий и Л. Ю. Новицкая предлагают провести

ревизию норм права, содержащих в себе упоминания об электронных доказательствах, устранить противоречия и нормативно закрепить определение цифровых доказательств[1]. В целом данная позиция представляется обоснованной, как и предлагаемое ими определение цифровых доказательств, под которыми они понимают «сведения о фактах в виде цифрового файла, сохранённого на цифровом носителе, локальной сети или Интернет»[2].

Зачастую цифровые доказательства именуют электронными. Это, на наш взгляд, связано с особенностями нормативного регулирования в сфере уголовного судопроизводства. Например, статья 164.1 Уголовно-процессуального кодекса Российской Федерации[3] закрепляет особенности изъятия электронных носителей информации, а ст. 474.1 УПК РФ – порядок использования электронных документов.

Дискуссионным является также вопрос, являются ли цифровые (электронные) доказательства самостоятельным видом доказательств.

Так, С. В. Зуев пишет, что информация в цифровой форме может быть вещественным доказательством или иным документом в зависимости от её «оформления, хранения, использования»[4].

Хотелось бы отметить так же мнение учёных, которые отрицают существование цифровых доказательств. Например, А. М. Баранов считает, что они являются лишь фантазией авторов, что единственным источником доказательств всегда является человек. По его мнению, электронные средства сохранения и передачи информации будут не вещественными доказательствами и не электронными доказательствами, а лишь хранителями информации[5].

Анализируя природу цифровых доказательств как информации, имеющей особенности носителя, хранения, копирования, воспроизведения и т. д., можно согласиться с мнением С. В. Зуева о том, что электронное доказательство имеет специфические свойства, отличающие его от иных видов доказательств[6].

---

[1] Новицкий В. А., Новицкая Л. Ю. Понятие и виды цифровых доказательств // Ленинградский юридический журнал. 2019. №. 1 (55). С. 217.

[2] Новицкий В. А., Новицкая Л. Ю. Понятие и виды цифровых доказательств // Ленинградский юридический журнал. 2019. №. 1 (55). С. 217

[3] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001№ 174-ФЗ (ред. от 28.04.2023) // Российская газета от 22 декабря 2001 г. № 249 // СПС «КонсультантПлюс» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения 06.05.2023)

[4] Зуев С. В. Электронные доказательства в уголовном судопроизводстве: понятие и значение // Правопорядок: история, теория, практика. 2020. №. 3 (26). С. 49.

[5] Баранов А. М. Электронные доказательства: иллюзия уголовного процесса XXI в. // Уголовная юстиция. 2019. № 13. С. 64–69.

[6] Зуев С. В. Электронные доказательства в уголовном судопроизводстве: понятие и значение // Правопорядок: история, теория, практика. 2020. №. 3 (26). С. 48

Проанализировав точки зрения учёных и действующее законодательство относительно цифровых (электронных) доказательств, можно прийти к выводу, что цифровые доказательства – это информация, полученная из цифровых устройств, таких как компьютеры, мобильные телефоны, планшеты и другие электронные устройства. Они могут быть использованы в качестве доказательств в уголовном судопроизводстве, чтобы подтвердить или опровергнуть обвинения.

Однако не только само понятие цифровых доказательств является дискуссионным, но и процедура доказывания, связанная с их получением и оценкой.

В настоящее время российскими судами общей юрисдикции в направлении цифровизации судопроизводства проводится целый ряд мероприятий: создаются электронные образы дел, формируется электронный архив, оптимизируется система электронного обращения в суд, предпринимаются попытки установления электронного взаимодействия судов с другими органами государственной власти и интеграция информационных систем этих органов и т. д.

Несмотря на всё это, при рассмотрении дел зачастую возникают сложности, которые, по мнению Д. Н. Маринкина связаны с тем, что информация, хранящаяся в цифровом виде, сложнее изымается и впоследствии используется для раскрытия преступлений[7]. Также, полученная информация может быть недостоверна, что может повлечь замедление рассмотрения дела.

Что касается процедуры изъятия электронной информации, Д. Н. Щедрин и С. М. Курбатова считают, что необходимо более детально регламентировать данную процедуру, определив способ фиксации исходя из местоположения цифровых данных[8]. В настоящее время действующим УПК регламентирована процедура изъятия электронных носителей. Но, в связи с низкой цифровой грамотностью правоприменителей[9], недостаточной степенью изученности данного способа собирания доказательств могут быть допущены ошибки, которые впоследствии поставят под сомнение достоверность полученной информации. Д. Н. Щедрин и С. М. Курбанова отмечают, что специалист, выполняющий скриншот экрана, впоследствии имеет возможность редактирования содержания снимка. В связи с этим полагаем, что при

[7] Маринкин Д. Н. Цифровые доказательства в уголовном судопроизводстве // Вестник Пермского института ФСИН России. 2019. № 1 (32). С. 33–36.

[8] Щедрин Д. Н., Курбатова С. М. Проблемы собирания и использования цифровых доказательств в уголовном судопроизводстве // Актуальные проблемы уголовного права, уголовного процесса и криминалистики: Сборник научных трудов по материалам 4-й Всероссийской научно-практической конференции молодых ученых, аспирантов, соискателей и магистрантов, Краснодар, 23 ноября 2018 года / Под редакцией В. Д. Зеленского. Краснодар: Кубанский государственный аграрный университет, 2019. С. 196–200.

[9] Чурикова, А. Ю. Проблемы цифровизации российского уголовного процесса // Вестник Саратовской государственной юридической академии. 2021. № 6 (143). С. 209–216. DOI 10.24412/2227-7315-2021-6-209-216.

проверке и оценке цифровых (электронных) доказательств необходимо особое внимание, в том числе со стороны органов прокуратуры. Так, можно согласиться с позицией А. Ю. Чуриковой о необходимости внедрения риск-ориентированного подхода в деятельности прокуроров[10], который бы позволил им в этой ситуации отнести данные доказательства к отдельной категории риска и уделять им больше внимания.

По нашему мнению, необходимо всё больше развивать технические средства получения, обработки электронных доказательств. Именно это позволит быть уверенными в их достоверности и использовать их в раскрытии и расследовании преступлений. Поскольку использование цифровой информации в качестве доказательств в уголовном судопроизводстве невозможно без применения технических средств, необходимо также повышать цифровую грамотность сотрудников правоохранительных органов.

Преступления, совершаемые с использованием цифровых технологий, встречаются всё чаще, а электронная информация всё в большей степени вытесняет другие носители информации. В связи с этим необходимо адаптировать действующее законодательство и внести соответствующие правки в нормативные акты, так как именно модернизация законодательства способствует узакониванию процессуальных действий, касающихся доказывания в уголовном судопроизводстве с помощью цифровых данных.

Список литературы

1. Баранов А. М. Электронные доказательства: иллюзия уголовного процесса XXI в. // Уголовная юстиция. 2019. № 13. С. 64–69.

2. Зуев С. В. Электронные доказательства в уголовном судопроизводстве: понятие и значение // Правопорядок: история, теория, практика. 2020. №. 3 (26). С. 46–51.

3. Маринкин Д. Н. Цифровые доказательства в уголовном судопроизводстве // Вестник Пермского института ФСИН России. 2019. № 1 (32). С. 33–36

4. Новицкий В. А., Новицкая Л. Ю. Понятие и виды цифровых доказательств / /Ленинградский юридический журнал. 2019. №. 1 (55). С. 213–220.

5. Чурикова А. Ю. Проблемы цифровизации российского уголовного процесса // Вестник Саратовской государственной юридической академии. 2021. № 6 (143). С. 209–216. DOI 10.24412/2227-7315-2021-6-209-216.

6. Чурикова А. Ю. Риск-ориентированный подход в уголовно-процессуальной деятельности прокурора // Законность. 2022. № 8 (1054). С. 48–50.

7. Щедрин Д. Н., Курбатова С. М. Проблемы собирания и использования цифровых доказательств в уголовном судопроизводстве // Актуальные проблемы

[10] Чурикова А. Ю. Риск-ориентированный подход в уголовно-процессуальной деятельности прокурора // Законность. 2022. № 8 (1054). С. 48.

уголовного права, уголовного процесса и криминалистики: Сборник научных трудов по материалам 4-й Всероссийской научно-практической конференции молодых ученых, аспирантов, соискателей и магистрантов, Краснодар, 23 ноября 2018 года / Под редакцией В. Д. Зеленского. Краснодар: Кубанский государственный аграрный университет, 2019. С. 196–200.

Marina S. Shirokova
Student
Volga Region Institute of Management
named after P. A. Stolypin – Branch of Russian Academy of National Economy and Public Administration
(Saratov, Russian Federation)
maribroshi@mail.ru

Scientific Supervisor: Anna V. Churikova
PhD in Law, Associate Professor,
Associate Professor at the Department of Administrative and Criminal Law
Volga Region Institute of Management – Branch of Russian Academy of National Economy and Public Administration
(Saratov, Russian Federation)
a_tschurikova@bk.ru

DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS

Abstract. The article deals with the concept of digital (electronic) evidence in criminal proceedings. The need for their use is due to the development of society, introduction of new technologies in our life, with which our law enforcement officers are sometimes unable to interact, due to lack of technical equipment and insufficient qualification of personnel. Some of the difficulties of law enforcement agencies in handling digital information are highlighted.

Keywords: digital evidence, criminal procedure, digital technology, electronic information, evidence.

УДК 347.2

Эмирбеков Фарид Язибекович
Студент,
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
emirbekov.farid00@mail.ru

Научный руководитель: Гончаров Максим Владимирович,
кандидат юридических наук,
доцент кафедры конституционного права
Уральский государственный юридический университет
имени В. Ф. Яковлева
(г. Екатеринбург, Российская Федерация)
m04@bk.ru

ГЕНЕТИЧЕСКАЯ ИНФОРМАЦИЯ: НЕДОСТАТКИ ПРАВОВОГО РЕГУЛИРОВАНИЯ И ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ

Аннотация. В данной статье автор проводит анализ действующего законодательства Российской Федерации, регулирующего генетические исследования, и выявляет основные проблемы, возникающие в результате использования генетической информации человека. На основе выявленных недостатков правового регулирования, автором предлагается совершенствовать законодательства в этой сфере и установить особый правовой режим использования полученной генетической информации человека.

Ключевые слова: генетическая информация, генетическая диагностика, генетические исследования, генетическая паспортизация, персональные данные.

Для цитирования:
Эмирбеков Ф. Я. Генетическая информация: недостатки правового регулирования и проблемы правоприменения // Технологии XXI века в юриспруденции: мат-лы Пятой междунар. науч.-практ. конф. (Екатеринбург, 19 мая 2023 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: АНО «КримЛиб», 2023. С. 256–265.

На сегодняшний день современные технологии в области исследований генома человека, а также активно применяемая ДНК-диагностика человека являются приоритетным направлением нашего государства, как, впрочем, и любого иного, поскольку позволяет существенно снизить расходы в сфере здравоохранения. О важности развития генетических технологий в нашей стране свидетельствуют недавно принятые нормативные акты. При этом, особое значение среди них имеет Указ Президента РФ от 28.11.2018 г. № 680 «О развитии генетических

технологий в Российской Федерации» и разработанная во исполнение данного Указа «Федеральная научно-техническая программа развития генетических технологий на 2019–2027 гг.»[1], определяющая основы дальнейшего совершенствования генетических исследований не только, традиционно, в сфере здравоохранения, но и во многих других отраслях.

Применение современных методов генодиагностики в настоящее время позволяет охватить все периоды жизненного цикла человека. При этом, на наш взгляд, особое значение имеют проблемы защиты генетической информации при проведении процедур генодиагностик.

Несмотря на довольно развитую правовую базу в России относительно генетических диагностик, небезосновательной видится точка зрения учёных о том, что «проведение таких диагностик, особенно пренатальных и преимплантационных в России не отличается последовательным нормативным регулированием»[2].

В частности, общие положения в отношении применения информационных технологий и методов генной инженерии, относящихся к высокотехнологичной медицинской помощи закреплены в Федеральном законе от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»[3].

Федеральный закон от 5.06.1996 г. № 86-ФЗ «О государственном регулировании в области генно-инженерной деятельности»[4], определяет термин «генодиагностика» как совокупность методов по выявлению изменений в структуре генома, а «генотерапия» как комплекс генно-инженерных (биотехнологических) и медицинских методов, направленных на внесение изменений в генетический аппарат соматических клеток человека в целях лечения заболеваний.

Федеральный закон от 23.06.2016 г. № 180-ФЗ «О биомедицинских клеточных продуктах»[5], регулирующий, в том числе, вопросы применения таких продуктов для профилактики,

[1] Указ Президента РФ от 28.11.2018 г. № 680 «О развитии генетических технологий в Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201811280061?rangeSize=1 (дата обращения: 13.05.2023).

[2] Комарова В. В., Алтынник Н. А., Бородина М. А., Суворова Е. И., Зенин С. С., Суворов Г. Н. Международно-правовое регулирование преимплантационной генетической диагностики (ПГД) и тенденции развития Российского законодательства в сфере вспомогательных репродуктивных технологий // Lex Russia. 2019. № 6 (151). С. 10.

[3] Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201111220007 (дата обращения: 13.05.2023).

[4] Федеральный закон РФ от 5.07.1996 г. № 86-ФЗ «О государственном регулировании в области генноинженерной деятельности» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102042295 (дата обращения: 13.05.2023).

[5] Федеральный закон РФ от 23.06.2016 г. № 180-ФЗ «О биомедицинских клеточных

диагностики и лечения заболеваний или состояний пациента, сохранения беременности и медицинской реабилитации пациента, также затрагивает в правовом регулировании и отношения, возникающие в связи с донорством биологического материала в целях производства биомедицинских клеточных продуктов.

Немаловажное значение имеют и принятые во исполнение положений Федеральных нормативных актов подзаконные акты, регламентирующие применение генетических технологий и проведение соответствующих исследований в различных отраслях.

В частности, можно отметить Приказ Министерства здравоохранения РФ от 31.07.2020 г. № 803н «О порядке использования вспомогательных репродуктивных технологий, противопоказаниях и ограничениях к их применению»[6], который содержит показания и противопоказания к применению вспомогательным репродуктивным технологиям (ВРТ) и определены сроки годности результатов обследований.

Отметим некоторые правовые проблемы, возникающие при проведении генодиагностики, которые напрямую связаны с защитой полученной в результате таких исследований генетической информации.

Во-первых, за пределами отечественного правового регулирования остаются вопросы, напрямую связанные с определением режима получения, использования и сохранности генетической информации о человеке. Также законодательно не определена процедура использования и последующей утилизации биологического материала как основы для проведения генодиагностики.

На наш взгляд, требуется законодательное закрепление понятия и содержания генетической информации, поскольку те её определения, которые содержаться в действующем законодательстве не отражают особых характеристик, а по большому счёту привязаны в своей терминологии к той или иной сфере деятельности, на которые распространяется тот или иной нормативный акт.

Так Федеральный закон от 03.12.2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» (п. 3 ст. 1) определяет её как персональные данные, включающие кодированную информацию об определённых фрагментах дезоксирибонуклеиновой кислоты физического лица или неопознанного

продуктах» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102402596 (дата обращения: 13.05.2023).

[6] Приказ Министерства здравоохранения РФ от 31.07.2020 г. № 803н «О порядке использования вспомогательных репродуктивных технологий, противопоказаниях и ограничениях к их применению» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202010190041 (дата обращения: 13.05.2023).

трупа, не характеризующих их физиологические особенности[7].

В то же время положениями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее по тексту – Закон № 152), такого рода информация имеет непосредственное отношение к категории биометрических данных (ст. 11) и требует оформление согласия индивидуума на её последующую обработку и распространение (ст. 7)[8].

Однако следует согласиться с мнением ряда учёных о том, что «ДНК-сведения о субъекте, по своим критериям, гораздо шире определения категории персональных данных». Соответственно, заслуживает поддержки мнение исследователей, согласно которому «генетическую информацию субъекта некорректно относить только к его персональным данным, поскольку обладателем данной информации является не только само лицо, предоставившее ДНК, но и его генетические родственники, как предки, так и потомки, и, следовательно, разрешение на ее распространение не должно определяться только волеизъявлением конкретного лица». Полагаем, что законодатель с учётом особых свойств генетической информации должен идти по пути закрепления её особого правового статуса (как информации о заранее неопределённом круге лиц), а не отождествлять её с персональной биометрической информацией.

Во-вторых, в связи с вышеуказанной первой проблемой, при соблюдении условия о конфиденциальности такой информации для третьих лиц, возникает вполне закономерная проблема соблюдения баланса интересов как носителя генетической информации, имеющей значение при проведении генетических диагностик, так и интересов его кровных родственников. Не исключено, что по результатам генетических диагностик, может быть установлена потенциальная угроза не только носителю такого рода информации, но и его ближайшим кровным родственникам. С целью обеспечения конфиденциальности информации клиента, полученной в результате генетического теста, требуется законодательное определение критериев, на основании которых возможны рекомендации врача по привлечению кровных родственников такого клиента к прохождению ими соответствующего генетического исследования.

В-третьих, немаловажную проблему составляет обеспечение сохранности полученной генетической информации. На наш взгляд, для решения данной проблемы важным представляется внесение поправок в

[7] Федеральный закон РФ от 3.12.2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102349622&backlink=1&&nd=102126015 (дата обращения: 13.05.2023).

[8] Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ ФЗ «О персональных данных» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108261 (дата обращения: 13.05.2023).

действующее законодательство с целью усиления мер обеспечения безопасности как носителей (биоматериала) генетической информации, так и самих сведений в них содержащихся. В частности, нуждается в дополнении ст. 37 Федерального закона от 23.06.2016 г. № 180-ФЗ «О биомедицинских клеточных продуктах», которая устанавливала бы требования к обеспечению безопасности генетической информации не только в процессе её хранения в биобанках, но и при транспортировке биологических материалов, которые тоже её содержат.

Конкретные меры такой деятельности должны быть оформлены подзаконными нормативными правовыми актами профильных ведомств. При этом целесообразно принять совместный приказ Министерств здравоохранения, внутренних дел Российской Федерации и Федеральной службы безопасности России для всесторонней проработки данного вопроса и введения в действие эффективных правовых норм, обеспечивающих права и законные интересы граждан, участвующих в правоотношениях, связанных с хранением и транспортировкой биологических материалов, содержащих в себе геномные сведения.

В-четвертых, помимо генетической информации человека, необходимо правовое признание и закрепление в качестве самостоятельных объектов правового регулирования данных, получаемых в результате генетических исследований, не относящиеся к персональным данным, например, результаты доклинических и клинических исследований лекарственных препаратов и клеточных продуктов, данные расшифровки генов и определение их особенностей в отношении определённого круга лиц или их популяции. Представляется, что данный вопрос должен в обязательном порядке находиться в сфере приоритетных направлений деятельности отечественного законодателя.

Анализ правового регулирования генетических диагностик в Российской Федерации и выявление ряда проблем, связанных с защитой генетической информацией, полученной в результате таких диагностик, позволяет согласиться с мнением учёных о том, что «отечественная нормативная база России, регулирующая сферу генетических исследований, в настоящее время находится только на начальном этапе ее развития»[9].

Учитывая интенсивное развитие технологий в сфере генетических диагностик, а соответственно возрастания возможностей различных манипуляций с геномом человека, видится необходимость совершенствования действующего законодательства, детально регулирующего применение

[9] Рузанова В. Д., Беляков В. И. Проблемы легализации и использования генетических технологий и данных циркадианной физиологии в сфере профессионального отбора // Юридический вестник Самарск. ун-та. 2020. Т. 6. № 2. С. 34. DOI https://doi.org/10.18287/2542-047X-2020-6-2-28-35.

молекулярно-генетических технологий
с соблюдением прав человека.

Список литературы

1. Владимиров В.Ю., Горбулинская И.Н., Кубитович С.Н. К вопросу о безопасности геномной информации // Биосфера. 2018. Т.10 № 1. С. 42–47.

2. Комарова В. В., Алтынник Н. А., Бородина М. А., Суворова Е. И., Зенин С. С., Суворов Г. Н. Международно-правовое регулирование преимплантационной генетической диагностики (ПГД) и тенденции развития Российского законодательства в сфере вспомогательных репродуктивных технологий // Lex Russia. 2019. № 6 (151). С. 10–16.

3. Малеина М. Н. Понятие и классификации геномной (генетической) информации // Lex Russica. 2020. Т. 73. № 7. С. 50–58.

4. Романовский Г.Б. Правовое регулирование генетических исследований в России и за рубежом // Lex Russica. 2016. № 7. С. 93–102.

5. Рузанова В. Д., Беляков В. И. Проблемы легализации и использования генетических технологий и данных циркадианной физиологии в сфере профессионального отбора // Юридический вестник Самарск. ун-та. 2020. Т. 6. № 2. С. 28–35. DOI https://doi.org/10.18287/2542-047X-2020-6-2-28-35.

6. Рыжова А.А. Правовая защита геномных данных граждан России // Наука. Общество. Государство. 2020. Т. 8. № 3. С. 54–63.

7. Хусаинова Р.И., Минниахметов И.Р., Ахтямова Е.В., Алсынбаева Э.М., Султанова Р.И. Правовые проблемы использования генетической информации, полученной при проведении пренатальной и преимплантационной генетической диагностики в Российской Федерации // Евразийский юридический журнал. 2020. № 10 (149). С. 163–166.

Farid Ya. Emirbekov
Student
Ural State Law University
named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
emirbekov.farid00@mail.ru

Scientific Supervisor: Maxim V. Goncharov,
PhD (Law),
Associate Professor of the Department of Constitutional Law
named after V. F. Yakovlev
(Yekaterinburg, Russian Federation)
m04@bk.ru

GENETIC INFORMATION: SHORTCOMINGS OF LEGAL REGULATION AND PROBLEMS OF LAW ENFORCEMENT

Abstract. In this article, the author analyzes the current legislation of the Russian Federation regulating genetic research and identifies the main problems arising from the use of human genetic information. Based on the identified shortcomings of legal regulation, the author proposes to improve legislation in this area and establish a special legal regime for the use of human genetic information obtained.

Keywords: genetic information, genetic diagnostics, genetic research, genetic certification, personal data.

Научное издание

ТЕХНОЛОГИИ XXI ВЕКА В ЮРИСПРУДЕНЦИИ

Материалы
Пятой международной научно-практической конференции

(г. Екатеринбург, 19 мая 2023 года)

Компьютерная вёрстка: Д. В. Бахтеев

Корректоры: С. А. Кошкина, А. Д. Цветкова

Рисунок на обложке: Андрей tramdrey Негруль

АНО «Центр содействия развитию криминалистики «КримЛиб»
Основной сайт: hub.crimlib.info
Энциклопедия: Crimlib.info
Канал: t.me/crimlib
ae@crimlib.info

Уральский государственный юридический университет
имени В. Ф. Яковлева
620137, г. Екатеринбург, ул. Комсомольская, 21
usla.ru

Союз криминалистов и криминологов
crimescience.ru

Подписано к использованию: 02.06.2023
Согласно п. 1. ч. 2 ст. 1, п. 1 ч. 4 ст. 11
Федерального закона от 29.12.2010 № 436-ФЗ
маркировке не подлежит

Электронное издание

Минимальные системные требования: ОС Windows XP/Vista/7/8/8.1/10/11,

RAM

512 MB и выше, необходимо на накопителе: 4,5 Мб, CD/DVD- привод,

программные средства для просмотра pdf-файлов

Объём издания: 4,5 Мб, 1 электрон.опт. диск (CD-ROM).