ФГБОУ ВО КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

www.kgau.ru

ВЫСОКОТЕХНОЛОГИЧНОЕ ПРАВО: СОВРЕМЕННЫЕ ВЫЗОВЫ

Материалы IV Международной межвузовской научно-практической конференции

Москва – Красноярск, 24–25 ноября 2022 г.

Часть первая

www.kgau.ru

Министерство науки и высшего образования Российской Федерации
ФГАО ВО Национальный исследовательский университет
«Московский институт электронной техники»
Министерство сельского хозяйства Российской Федерации
ФГБОУ ВО «Красноярский государственный аграрный университет»
АНО «Центр научных исследований и экспертизы»

ВЫСОКОТЕХНОЛОГИЧНОЕ ПРАВО: СОВРЕМЕННЫЕ ВЫЗОВЫ

Материалы IV Международной межвузовской научно-практической конференции

17-20 февраля 2023 года
Москва – Красноярск

Часть первая

Электронное издание

Красноярск 2023

ББК 32.973.2
В 93

В 93 Высокотехнологичное право: современные вызовы [Электронный ресурс]: материалы IV Международной межвузовской научно-практической конференции (17-20 февраля 2023 года, Москва – Красноярск) / Национальный исследовательский университет «Московский институт электронной техники»; Красноярский государственный аграрный университет. Часть 1. – Красноярск, 2023. – 336 с.

Представлены материалы IV Международной межвузовской научно-практической конференции «Высокотехнологичное право: современные вызовы», которая проходила 17-20 февраля 2023 года в Москве-Красноярске и соорганизаторами которой стали Федеральное государственное автономное образовательное учреждение высшего образования Национальный исследовательский университет «Московский институт электронной техники», Федеральное государственное бюджетное образовательное учреждение высшего образования «Красноярский государственный аграрный университет», кафедра криминалистики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет им. М. В. Ломоносова» и Автономная некоммерческая организация «Центр научных исследований и экспертизы».

Предназначено для ученых и специалистов образовательных и научно-исследовательских учреждений, представителей органов государственной и муниципальной власти, адвокатуры, иных организаций и учреждений, а также лиц, интересующихся вопросами правового регулирования и использования высоких технологий.

УДК 343.985.7

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ВЫЯВЛЕНИЯ И ПРОФИЛАКТИКИ КОРРУПЦИИ В ЭПОХУ ВЫСОКОТЕХНОЛОГИЧЕСКОГО ПРАВА

Авдеева Анастасия Юрьевна,
кандидат физико-математических наук
Красноярский государственный аграрный университет,
г. Красноярск, Россия
email: avdeeva.anastasia@gmail.com

Научный руководитель: Трофимова Светлана Алексеевна,
кандидат философских наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
email: trofimovas832@gmail.com

Аннотация*: проведено исследование, направленное на улучшение понимания возможностей использования систем искусственного интеллекта для выявления и противодействия коррупции при одновременном признании существующих правовых и технических рисков. Рассмотрен опыт использования нейронных сетей в борьбе с коррупцией в зарубежных странах. Обсуждаются механизмы правового регулирования внедрения технологии систем искусственного интеллекта.*

Ключевые слова*: коррупция, искусственный интеллект, нейронные сети, антикоррупционная деятельность.*

USING ARTIFICIAL INTELLIGENCE TO DETECT AND PREVENT CORRUPTION IN THE ERA OF HIGH-TECH LAW

Avdeeva Anastasia Yurievna,
candidate of Physical and Mathematical Sciences
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
email: avdeeva.anastasia@gmail.com

Supervisor: Trofimova Svetlana Alekseevna,
candidate of philosophical sciences, associate professor
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
email: trofimovas832@gmail.com

Abstract*: a study was conducted aimed at improving the understanding of the possibilities of using artificial intelligence systems to identify and combat corruption, while recognizing existing legal and technical risks. The experience of using neural*

networks in the fight against corruption by foreign countries is considered. The mechanisms of legal regulation of the introduction of artificial intelligence systems technology are discussed.

***Keywords**: corruption, artificial intelligence, neural networks, anti-corruption activities.*

Современные технологии, основанные на использовании систем искусственного интеллекта, находятся на передовой научно-технического прогресса и демонстрируют новые возможности для решения нетривиальных интеллектуальных задач. В том числе, к таким задачам относится проблема выявления и прогнозирования коррупционных преступлений [1].

Согласно данным отчетов МВД, выявляемые коррупционные преступления в Российской Федерации сохраняют угрожающие масштабы, так за 2021 год зафиксировано более 35 тысяч преступлений коррупционного характера, что соответствует приросту на 14%, по сравнению с 2020 годом [2].

Использование систем искусственного интеллекта, дает новую надежду на эффективную борьбу с коррупцией во всем мире. В докладе Генеральной Ассамблеи ООН, опубликованном в 2021 году, посвященном новым технологиям для устойчивого развития и борьбы с коррупцией, выделяют две области применения искусственного интеллекта непосредственно в борьбе с конкретными формами коррупции, такими как: взяточничество, незаконные финансовые потоки, отмывание денег, растрата, кумовство, и косвенное для повышения подотчетности и прозрачности [3].

В Российской Федерации понятие искусственный интеллект юридически закреплено в Национальной стратегией развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента РФ от 10 октября 2019г. [4], согласно которой «искусственный интеллект – 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. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений».

К настоящему буму искусственного интеллекта привели прорывы в области глубокого обучения, представляющего собой класс алгоритмов машинного обучения, использующего многоуровневые искусственные нейронные сети для имитации процесса принятия решений человеком. Именно нейронные сети с помощью алгоритмов, могут автономно выполнять широкий спектр задач при перекрестном анализе баз данных: производить первичную обработку предоставляемых сведений о доходах, расходах, имуществе, отслеживать цифровой след, выявлять социальные связи, выявлять конфликты интересов, анализировать тендерную документацию и результаты торгов, фиксировать нарушения при исполнении функций на должностях и др. Этот

анализ позволяет обнаружить в финансовом и налоговом секторах отмывание денег, уклонение от уплаты налогов и мошеннические схемы.

За последнее десятилетие накопился опыт использования нейронных сетей в антикоррупционной сфере. Например, управление по налоговым и таможенным сборам Великобритании применяют систему Connect, для сопоставления сведении в налоговой декларации с информацией из соцсетей, онлайн платформ торговли, операции Visa и MasterCard из банков более 60 стран, земельного кадастра, а также из анализа записей электронной почты [5]. В Испании нейронная сеть на самоорганизующихся картах вычисляет вероятность коррупции в испанских провинциях в зависимости от экономических условий региона, что позволяет властям принимать превентивные меры для снижения коррупционных рисков [6]. В одном из регионов Чехии нейросеть проанализировала общедоступные финансовые данные для выявления связи подрядчиков с политически значимыми лицами [3]. Некоторые аспекты применения высоких технологий противодействия коррупции в станах Азии освещаются в статье [7].

В Российской Федерации цифровизация государственных и частных баз данных также позволяет производить антикоррупционный мониторинг. Так, с апреля 2022 года, согласно указу Президента РФ, начала работу система в области противодействия коррупции «Посейдон» [8], подобная система несколько лет применяется в Росатоме [9]. Ожидается, что применение систем искусственного интеллекта способно повысить уровень доверия граждан к деятельности органов государственной власти.

Однако, как и любая другая мощная технология, технология нейронных сетей несет в себе ряд потенциальных правовых и технологических рисков, в том числе несущих коррупционный характер. Также, открытыми остаются вопросы, связанные с этикой, правами человека, конфиденциальностью и защитой данных.

Наиболее важной комплексной задачей является создание алгоритма работы нейронной сети, формирование перечня соответствующих индикаторов с участием многих экспертов и специалистов. При этом появляется риск использования алгоритмов, намеренно или непреднамеренно, для мошенничества и коррупционной деятельности. В связи с чем, актуальной является проблема аудита самих алгоритмов.

Сложность алгоритмов «черного ящика» делает невозможным точное определение того, как выполняется вычисление, приводящее к заданному результату. Это неизбежно приводит к отсутствию прозрачности и затрудняет объяснение и интерпретацию решений, принятых в результате глубокого обучения, что неизбежно может привести к отсутствию доверия к системе. Например, экспериментальная антикоррупционная система искусственного интеллекта «Zero Trust», работающая в некоторых провинциях Китая, которая может получать доступ к защищенным базам данных в органах власти, способна создавать многоуровневые карты социальных отношений и проводить анализ поведения государственных служащих, что позволяет обнаруживать подозрительные передачи собственности, рост баланса на банковском счете

госслужащего и его семьи, выявлять случаи, когда чиновники или их друзья или родственники участвуют в тендерах. После анализа система оценивает действие на предмет коррупции, если оценка получается выше среднего значения, то правительство получает предупреждение. С 2012 года «Zero Trust» уличило 8 721 государственных служащих в таких преступлениях как растрата, злоупотребление властью, нецелевое использование государственных средств и кумовство. Нейронная сеть может быстро указать на коррумпированного чиновника, при этом способность объяснить процесс, в результате которого система пришла к такому выводу, ограничена. Поэтому, местные органы власти стали отказываться от системы «Zero Trust», ссылаясь на то, что они «могут чувствовать себя не совсем комфортно с новой технологией» [10,11].

Доступ к данным принципиально важен для систем искусственного интеллекта. Тем не менее, конфиденциальность данных может не быть защищена теми, кто их использует. Особо актуальна проблема защиты биометрических данных. Поскольку утечка биометрических данных, сделает невозможным последующую идентификацию человека в цифровой среде.

Отметим, что последними поправки в ст. 13.11 КоАП РФ законодатель ужесточает наказание за утечку персональных данных. Также принят Федеральный закон от 29.12.2022 № 572-ФЗ, регламентирующий идентификацию, в том числе и аутентификации физических лиц с применением биометрических персональных данных [12]. Тем не менее, остается высокой вероятность того, что в будущем мир столкнётся с большим количеством новых виртуальных преступлений, порожденными использованием систем искусственного интеллекта в преступной деятельности [13].

Согласно Международному пакту о гражданских и политических правах принятому 16.12.1966 года Резолюцией 2200 на 1496-ом пленарном заседании Генеральной Ассамблеи ООН [14], государство обязано охранять неприкосновенность частной жизни, в том числе защищать человека от посягательств на нарушение данного права. Поэтому, принимая решение о внедрении систем искусственного интеллекта на государственном уровне должны быть проанализированы возможности профилактики правонарушений и их влияние на права человека.

На сегодняшний день правовым механизмом внедрения систем искусственного интеллекта являются экспериментально правовые режимы. Так, в городе федерального значения Москва с 01.06.2020 года на пять лет введен экспериментальный режим в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта [15].

Таким образом, использование систем искусственного интеллекта, может повысить скорость, эффективность, а также точность анализа больших объемов данных для выявления и прогнозирования коррупции. Однако, внедрение новых технологий добавляет новое измерение уязвимости, приводит к появлению новых рисков неправильного использования технологий, включая коррупционную деятельность на высокотехнологическом уровне. При этом эффективность и безопасность использования систем искусственного

интеллекта в решении проблемы с коррупцией, напрямую зависит от добросовестного и ответственного внедрения современных цифровых технологий.

Список литературы

1. Искусственный интеллект в профилактике правовых рисков и противодействии коррупции: докл. к XXIII Ясинской (Апрельской) междунар. науч. конф. по проблемам развития экономики и общества, Москва, 2022 г. / Е.А. Артеменко, А.М. Волкова, Р.О. Долотов [и др].; под науч. ред. Д.В. Крыловой; Нац. исслед. ун-т «Высшая школа экономики». М.: Изд. дом Высшей школы экономики, 2022. 48 с.
2. Министерство Внутренних Део Российской Федерации: офиц. сайт. // URL: https://мвд.рф (дата обращения: 21.01.2023).
3. New Technologies for Sustainable Development: perspectives on integrate y, trust and anti corruption. / One United Nations Plaza, New York, NY 10017, USA. // URL: https://www.undp.org/publications/new-technologies-sustainable-development-perspectives-integrity-trust-and-anti-corruption.
4. Российская Федерация. Указы. О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»). Указ Президента РФ №490. Утвержден 10 октября 2019 года. // URL: http://actual.pravo.gov.ru/text.html#pnum=0001201910110003.
5. Colin C Williams. Her majesty's revenue and customs (hmrc) connect data analytics tool United Kingdom/Colin C Williams, The University of Sheffield, Technical Report May 2021. // URL: https://www.academia.edu/49035707/HER_MAJESTYS_REVENUE_AND_CUSTOMS_HMRC_CONNECT_DATA_ANALYTICS_TOOL_United_Kingdom.
6. Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces / Félix J. López-Iturriaga, Iván Pastor Sanz / Social Indicators Research. – 2018. Vol. 140, № 3. P. 975–998.
7. Трофимова, С.А. Некоторые аспекты сбора доказательств в странах Азии // Актуальные вопросы российского судопроизводства: доказывание с использованием современных технологий: материалы Всероссийской (национальной) научно-практической конференции (21.10.2022 года, г. Красноярск). Красноярск: Красноярский ГАУ, 2022. 184 с.
8. Российская Федерация. Указы. О государственной информационной системе в области противодействия коррупции «Посейдон» и внесении изменений в некоторые акты Президента Российской Федерации. Указ Президента РФ №232. Утвержден 25 апреля 2022 года // URL: http://publication.pravo.gov.ru/Document/View/0001202204250032.
9. РОСАТОМ: офиц. Сайт // URL: https://www.rosatom.ru/about/protivodeystvie-korruptsii/.
10. Chen, S. Is China’s corruption-busting AI system “Zero Trust” being turned off for being too efficient? / South China Morning Post, Hong Kong, 4 February 2019 // URL:

https://www.scmp.com/news/china/science/article/2184857/chinas-corruption-busting-ai-system-zero-trust-being-turned-being?module=perpetual_scroll_0&pgtype=article&campaign=2184857.

11. J. Christian. China built an AI to detect corruption and officials shut it down/ The Byte/ 4 February 2019.

12. Российская Федерация. Законы. 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 №572-ФЗ: принят Государственной Думой 21 декабря 2022 года: одобрен Советом Федерации 23 декабря 2022 года // URL: https://www.consultant.ru/document/cons_doc_LAW_436110/.

13. Ерахтина, Е.А. Преступления, совершаемые с использованием искусственного интеллекта: проблемы квалификации и расследования / Е.А. Ерахтина, В.А. Тирранен // Вестник Сибирского юридического института МВД России. 2019.№ 2 (35). С. 36-41.

14. Международный пакт о гражданских и политических правах (Принят 16.12.1966 г. Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН) // URL: https://www.consultant.ru/document/cons_doc_LAW_5531/.

15. Российская Федерация. Законы. О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных». Федеральный закон №123-ФЗ: принят Государственной Думой 14 апреля 2020 года: одобрен Советом Федерации 17 апреля 2020 года // URL: https://www.consultant.ru/document/cons_doc_LAW_351127/.

УДК 342.9

К ВОПРОСУ О ГОСУДАРСТВЕННОЙ И МУНИЦИПАЛЬНОЙ КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ В КОНТЕКСТЕ ЦИФРОВИЗАЦИИ АДМИНИСТРАТИВНО-УПРАВЛЕНЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Айснер Лариса Юрьевна,
кандидат культурологии, доцент,
Наумов Олег Дмитриевич,
кандидат философских наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: stud.ui@kgau.ru

Аннотация: в статье предпринимается попытка концептуального анализа сущности и содержания процесса цифровизации государственной и муниципальной контрольно-надзорной деятельности в условиях трансформации административно-управленческих отношений в системе публичной власти.

Ключевые слова: *цифровизация, государственное и муниципальное управление, государственный и муниципальный контроль, государственный и муниципальный надзор, административно-управленческие отношения, стратегическое управление и развитие.*

ON THE QUESTION OF STATE AND MUNICIPAL CONTROL AND SUPERVISORY ACTIVITIES IN THE CONTEXT OF DIGITALIZATION OF ADMINISTRATIVE AND MANAGEMENT ACTIVITIES

Aisner Larisa Yurievna,
candidate of cultural studies, associate professor,
Naumov Oleg Dmitrievich,
candidate of philosophy, associate professor
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: stud.ui@kgau.ru

Abstract*: the article attempts to conceptually analyze the essence and content of the process of digitalization of state and municipal control and supervision activities in the context of the transformation of administrative and managerial relations in the system of public authority.*

Keywords: *digitalization, state and municipal management, state and municipal control, state and municipal supervision, administrative and managerial relations, strategic management and development.*

Цифровизация общественной жизни – характерная черта современности [3], находящая свое выражение не только в увеличении применения инструментов автоматизации и алгоритмизации в привычных рутинных практиках социального осуществления административно-управленческой деятельности. Не стало исключением и осуществление управления государством и муниципальными образованиями.

В действующей на сегодняшний день на территории Российской Федерации нормативно-правовой базе, регламентирующей порядок осуществления стратегического управления и развития территорий, нормативно закреплен принцип цифровизации экономики [1,4,5], влекущей за собой необходимость комплексной модернизации не только имеющейся материально-технической базы и факторов производства, но и трансформации контрольно-надзорной деятельности, осуществляемой со стороны государства и муниципальных образований [2].

Между тем, сфера государственной и муниципальной контрольно-надзорной деятельности не ограничивается исключительно контролем в сфере финансов. Кроме того, развитие современной отечественной юридической науки характеризуется тенденцией усиления междисциплинарного рассмотрения вопросов государственного и муниципального управления через призму нормативно-правового сопровождения, а также инструментов цифровизации [12].

Говоря о процессе цифировизации государственной и муниципальной контрольно-надзорной деятельности следует заметить, что данный вопрос в современной отечественной юридической науке освещен еще недостаточно [6,7,8,9]. В научной дискуссии по этому поводу можно выделить диаметрально противоположные точки зрения: если одни специалисты связывают цифровизацию исключительно с качественной трансформацией общественных отношений, то другие указывают на наличие элементов цифровизации не в объекте контроля, а его главном субъекте, классифицируя доступные ему на сегодняшний день инструменты.

В связи с этим, не лишним будет уточнение о дифференцированном подходе при рассмотрении процесса цифровизации государственной и муниципальной контрольно-надзорной деятельности [10], в рамках которой можно выделить:

1. качественную трансформацию процесса сбора, обработки и анализа оперируемых данных с применением информационно-коммуникативных технологий в рамках набирающего сегодня популярность анализа big data;

2. автоматизацию самой контрольно-надзорной деятельности, выходящей далеко за рамки сугубо экономической сферы.

Таким образом, фокусируя внимания на второй составляющей рассматриваемой проблемы, нужно отметить, что цифровизация государственного и муниципального контроля и надзора – это деятельность, направленная на широкое применение цифровых технологий в административно-управленческой деятельности государственных органов контроля и надзора с целью радикальной модернизации последней. Иными

словами, суть описываемой модернизации административно-управленческих отношений заключается в том, что субъект контрольно-надзорной деятельности – соответствующий государственный или муниципальный орган осуществляет свое взаимодействие с подконтрольным лицом в режиме реального времени, но в электронном формате. Таким образом, сокращается не только время осуществляемого в процессе деятельности документооборота, но и скорость реакции, а также упрощение сбора и анализа необходимой статистической информации [11].

В связи с этим следует признать, что цифровизация государственной и муниципальной контрольно-надзорной деятельности, вопреки декларируемым нормам действующего законодательства, а также нормативных актов стратегического решения, не подразумевает качественной трансформации административно-управленческих полномочий соответствующих субъектов публичной власти, а лишь предполагает модернизацию процедурной природы осуществляемой ими профессиональной деятельности.

Список литературы

1. Айснер, Л.Ю. Применение высоких технологий в сфере государственного управления в свете вызовов цифровой экономики / Л.Ю. Айснер, О.Д. Наумов // Высокотехнологичное право: генезис и перспективы. Материалы III Международной межвузовской научно-практической конференции. Красноярск: Красноярский ГАУ, 2022. С. 3-7.
2. Айснер, Л.Ю. К вопросу об оценке государственно-стратегического управления в контексте глобального посткризисного ландшафта: старые проблемы и новый формат решения / Л.Ю. Айснер, О.Д. Наумов // Тренды развития современного общества: управленческие, правовые, экономические и социальные аспекты. Сборник научных статей 10-й Всероссийской научно-практической конференции. Курск, 2020. С. 19-21.
3. Айснер, Л.Ю. Социальная роль цифровизации в трансформации условий жизни современного общества / Л.Ю. Айснер, О.Д. Наумов // Высокотехнологичное право: генезис и перспективы. Материалы II Международной межвузовской научно-практической конференции. Красноярск: Красноярский ГАУ, 2021. С. 15-21.
4. Айснер, Л.Ю. Использование цифровых технологий при планировании, мониторинге и оценке государственного управления: анализ зарубежной практики / Л.Ю. Айснер, О.Д. Наумов // Высокотехнологичное право: генезис и перспективы. Материалы II Международной межвузовской научно-практической конференции. Красноярск: Красноярский ГАУ, 2021. С. 12-15.
5. Айснер, Л.Ю. Применение высоких технологий в сфере государственного управления в свете вызовов цифровой экономики / Л.Ю. Айснер, О.Д. Наумов // Высокотехнологичное право: генезис и перспективы. Материалы III Международной межвузовской научно-практической конференции. Красноярск: Красноярский ГАУ, 2022. С. 3-7.

6. Гриценко, Е.В. Цифровизация контрольно-надзорной деятельности: опыт России и Франции / Е.В. Гриценко, П.А. Курындин // Правоприменение. 2020. Т. 4. № 3. С. 25-45.

7. Добролюбова, Е.И. Оценка цифровой зрелости государственного управления / Е.И. Добролюбова // Информационное общество. 2021. № 2. С. 37-52.

8. Добролюбова, Е.И. Перспективы цифровизации российского государственного управления: анализ ведомственных программ цифровой трансформации / Е.И. Добролюбова, И.С. Шемончук // Государство и граждане в электронной среде. 2021. № 5. С. 21-44.

9. Леонтьев, П.Б. Совершенствование системы регулирования контрольно-надзорных функций / П.Б. Леонтьев // ЭГО: Экономика. Государство. Общество. 2020. № 3 (42).

10. Любченко, Н.Н. Цифровизация контрольно-надзорной деятельности / Н.Н. Любченко // Цифра и право. Сборник научных статей. Отв. редактор Л.В. Зайцева. Тюмень, 2021. С. 98-104.

11. Магомедов, З.А. Реформирование контрольно-надзорной деятельности: результаты и перспективы / З.А. Магомедов, О.Е. Ступникова // Вестник экспертного совета. 2021. № 1 (24). С. 8-15.

12. Спиридонов, А.А. Особенности модели контрольно-надзорной деятельности в рамках развития механизмов государственного управления в России: конституционно-правовой взгляд / А.А. Спиридонов // Lex Russica (Русский закон). 2023. Т. 76. № 1 (194). С. 63-75.

13. Южаков, В.Н. К вопросу о цифровой трансформации государственного управления / О.Н. Слоботчиков, С.Д. Козлов, М.В. Шатохин, С.А. Попова, А.Н. Гончаренко // «Цифра и власть: цифровые технологии в государственном управлении». М.: НАНО ВО «ИМЦ», 2020) // Вопросы государственного и муниципального управления. 2020. № 4. С. 243-254.

УДК 342.9

К ВОПРОСУ О ПЕРСПЕКТИВАХ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В АДМИНИСТРАТИВНО-УПРАВЛЕНЧЕСКОЙ И КОНТРОЛЬНО-НАДЗОРНОЙ ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВА

Айснер Лариса Юрьевна,
кандидат культурологии, доцент,
Наумов Олег Дмитриевич,
кандидат философских наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: stud.ui@kgau.ru

Аннотация: *в статье анализируются актуальные вопросы применения искусственного интеллекта в сфере государственного и муниципального контроля, а также административно-управленческой деятельности органов государственной и муниципальной власти.*

Ключевые слова: *цифровизация, государственное и муниципальное управление, государственный и муниципальный контроль, государственный и муниципальный надзор, административно-управленческие отношения, стратегическое управление и развитие.*

TO THE QUESTION OF PROSPECTS OF APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE ADMINISTRATIVE AND MANAGEMENT AND CONTROL AND SUPERVISORY ACTIVITIES OF THE STATE

Aisner Larisa Yurievna,
candidate of cultural studies, associate professor,
Naumov Oleg Dmitrievich,
candidate of philosophy, associate professor
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: stud.ui@kgau.ru

Abstract*: The article analyzes topical issues of the use of artificial intelligence in the field of state and municipal control, as well as administrative and managerial activities of state and municipal authorities.*

Keywords: *digitalization, state and municipal management, state and municipal control, state and municipal supervision, administrative and managerial relations, strategic management and development.*

Применение высоких технологий в различных сферах общественной жизни – требование нормативно-правовых актов [12], регулирующих стратегическое развитие и технологическую модернизацию государства [1]. В связи с этим, существующая практика государственного и муниципального

администрирования не может обойтись без системной трансформации, направленной на внедрение управленческую практику прорывных технологий [2]. Ярчайшим примером, иллюстрирующим изменения в сфере взаимодействия государственной и муниципальной власти с населением, является функционирование портала «Госуслуги», демонстрирующего положительную динамику в количестве обращений граждан, а также предоставления им соответствующих государственных и муниципальных услуг [3].

Между тем, неотъемлемой составляющей деятельности органов исполнительной власти разного уровня является осуществление контрольно-надзорной деятельности. В настоящее время данная сфера административно-управленческой деятельности государственной и муниципальной власти не может похвастаться такими же успехами, хотя, безусловно, внимания заслуживают онлайн платформы отдельных профильных ведомств и служб: например, электронный сервис Федеральной службы по труду и занятости (Роструд) «Онлайн-инспекция.рф».

Вместе с тем, сфера государственного и муниципального управления в Российской Федерации идет по пути цифровизации [10]: созданы и развиваются такие информационные системы как «Федеральный реестр государственных и муниципальных услуг (функций)», автоматизированная система «Управление», а также ведомственные государственные информационные системы контрольно-надзорных органов, которые еще не объединены в единый онлайн супер-сервис [4,5,8].

Стоит отметить, что уже сейчас большинство экспертов в сфере высоких технологий указывают на необходимость трансформации государственной и муниципальной контрольно-надзорной деятельности в направлении цифрового государственного контроля [6]. С точки зрения правового обеспечения, рассматриваемая модернизация не только потребует соответствующих поправок в действующее законодательство в сфере контрольно-надзорной деятельности, но и переосмыслит ее назначение в рамках административно-управленческой деятельности государства [7,9,11,13]. Во-первых, речь идет о полном переходе текущего ведомственного делопроизводства в режим электронного бэк-офиса, во-вторых, изменению регламентов проведения контрольно-надзорных мероприятий, выдвигая в качестве обязательного условия рассматриваемой деятельности наличие сети Интернет, в-третьих, речь идет о сокращении времени на сбор и обработку необходимой информации, вызванном дистанционным характером мониторинга и оценки рисков в рамках осуществляемой соответствующими органами деятельности, в-четвертых, автоматический анализ собранных данных и их проверка на соответствие формальным требованиям, что существенно снизит субъективный фактор в осуществлении государственного и муниципального управления.

Кроме того, описываемые изменения в сфере государственного и муниципального контроля приведут к пониманию последнего в качестве цифрового инструмента предупреждения возможных рисков. Таким образом, исследователи отмечают, что цифровизирующийся контроль не только

повышает качественные показатели эффективности деятельности государственных и муниципальных контрольно-надзорных органов, но и способствует их более широкому распространению не только в сфере административной деятельности государственных и муниципальных органов, но и в рамках гражданского общества, а также граждан, будучи направленным обеспечение принципов законности, открытости и гласности.

Список литературы

1. Айснер, Л.Ю. Применение высоких технологий в сфере государственного управления в свете вызовов цифровой экономики / Л.Ю. Айснер, О.Д. Наумов // Высокотехнологичное право: генезис и перспективы. Материалы III Международной межвузовской научно-практической конференции. Красноярск: Красноярский ГАУ, 2022. С.3-7.
2. Айснер, Л.Ю. К вопросу об оценке государственно-стратегического управления в контексте глобального посткризисного ландшафта: старые проблемы и новый формат решения / Л.Ю. Айснер, О.Д. Наумов // Тренды развития современного общества: управленческие, правовые, экономические и социальные аспекты. Сборник научных статей 10-й Всероссийской научно-практической конференции. Курск, 2020. С. 9-21.
3. Айснер, Л.Ю. Социальная роль цифровизации в трансформации условий жизни современного общества / Л.Ю. Айснер, О.Д. Наумов // Высокотехнологичное право: генезис и перспективы. Материалы II Международной межвузовской научно-практической конференции. Красноярск: Красноярский ГАУ, 2021. С.15-21.
4. Айснер, Л.Ю. Использование цифровых технологий при планировании, мониторинге и оценке государственного управления: анализ зарубежной практики / Л.Ю. Айснер, О.Д. Наумов // Высокотехнологичное право: генезис и перспективы. Материалы II Международной межвузовской научно-практической конференции. Красноярск: Красноярский ГАУ, 2021. С.12-15.
5. Айснер, Л.Ю. Применение высоких технологий в сфере государственного управления в свете вызовов цифровой экономики / Л.Ю. Айснер, О.Д. Наумов // Высокотехнологичное право: генезис и перспективы. Материалы III Международной межвузовской научно-практической конференции. Красноярск: Красноярский ГАУ, 2022. С.3-7.
6. Гриценко, Е.В. Цифровизация контрольно-надзорной деятельности: опыт России и Франции / Е.В. Гриценко, П.А. Курындин // Правоприменение. 2020. Т. 4. № 3. С.25-45.
7. Добролюбова, Е.И. Оценка цифровой зрелости государственного управления / Е.И. Добролюбова // Информационное общество.2021. № 2. С. 37-52.
8. Добролюбова, Е.И. Перспективы цифровизации российского государственного управления: анализ ведомственных программ цифровой трансформации / Е.И. Добролюбова, И.С. Шемончук // Государство и граждане в электронной среде. 2021. № 5. С.21-44.

9. Леонтьев, П.Б. Совершенствование системы регулирования контрольно-надзорных функций / П.Б. Леонтьев // ЭГО: Экономика. Государство. Общество. 2020. № 3 (42).

10. Любченко, Н.Н. Цифровизация контрольно-надзорной деятельности / Н.Н. Любченко // Цифра и право. Сборник научных статей. Отв. редактор Л.В. Зайцева. Тюмень, 2021. С. 98-104.

11. Магомедов, З.А. Реформирование контрольно-надзорной деятельности: результаты и перспективы / З.А. Магомедов, О.Е. Ступникова // Вестник экспертного совета. 2021. № 1 (24). С.8-15.

12. Спиридонов, А.А. Особенности модели контрольно-надзорной деятельности в рамках развития механизмов государственного управления в России: конституционно-правовой взгляд / А.А. Спиридонов // Lex Russica (Русский закон). 2023. Т. 76. № 1 (194). С.63-75.

13. Южаков, В.Н. К вопросу о цифровой трансформации государственного управления / О.Н. Слоботчиков, С.Д. Козлов, М.В. Шатохин, С.А. Попова, А.Н. Гончаренко // «Цифра и власть: цифровые технологии в государственном управлении». - М.: НАНО ВО «ИМЦ», 2020) // Вопросы государственного и муниципального управления. 2020. № 4. С. 243-254.

УДК 343.48

О НЕКОТОРЫХ АКТУАЛЬНЫХ НАПРАВЛЕНИЯХ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ В ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКЕ

Аминев Фарит Гизарович,
доктор юридических наук, профессор,
профессор кафедры криминалистики Института права
Уфимский университет науки и технологий,
г. Уфа, Россия;
профессор кафедры судебно-экспертной деятельности
Краснодарский университет МВД России,
г. Краснодар, Россия
e-mail: faminev@ mail.ru

Аннотация: *в статье рассмотрены направления использования высоких технологий в судопроизводстве. В статье показано, что в практическую деятельность успешно внедряются компьютерные программные комплексы исследования мобильных устройств, компьютерные конструкторы осмотров мест происшествий в 3Д-формате и т.д. В один ряд с прорывными направлениями, используемыми в судопроизводстве, следует поставить внедрение молекулярно-генетических технологий. Рассмотрены направления использования высокотехнологичных методов геномного исследования, в том числе- следов биологического происхождения, в правоприменительной практике.*

Ключевые слова: *судебно-экспертная деятельность, молекулярно-генетические исследования, базы данных, ДНК кошек и собак, регистрация.*

ABOUT SOME CURRENT DIRECTIONS OF USING MODERN TECHNOLOGIES IN LAW ENFORCEMENT PRACTICE

Aminev Farit Gizarovich,
doctor of law, professor
professor of the Department of criminology of the Institute of Law
Ufa university of science and technology,
Ufa, Russia;
Professor of the Department of Forensic Expertise
FGKOU HE "Krasnodar university of the Ministry of internal affairs of Russia",
Krasnodar, Russia
e-mail:faminev@ mail.ru

Abstract: *the article considers the directions of using high technologies in legal proceedings. The article shows that computer software complexes for the study of mobile devices, computer constructors for inspections of accident sites in 3D format, etc. are successfully introduced into practical activity. The introduction of molecular genetic technologies should be put on a par with the breakthrough directions used in legal proceedings. The directions of using high-tech methods of genomic research, including traces of biological origin, in law enforcement practice are considered.*

Keywords: *forensic activity, molecular genetic research, databases, DNA of cats and dogs, registration.*

В последние годы в судебно-экспертной деятельности с большим успехом применяются специально разработанные и приспособленные приборы, оборудование и расходные материалы, новейшие методы исследования и научные разработки. Уже с конца XX столетия в рамках уголовного, гражданского, административного и арбитражного судопроизводства проводятся высокотехнологичные фоноскопические, молекулярно-генетические, компьютерно-технические и другие роды и виды судебных экспертиз.

С началом объявленной в 2016 году четвертой индустриальной революции, которую Е.Р. Россинская еще ранее представила как «методологическую и технологическую основу использования IT-технологий в экспертных исследованиях любых объектов судебной экспертизы» [1, с. 264] произошел еще больший скачок использования современных технологий в правоприменительной практике. В настоящее время в стадии внедрения в практическую деятельность находятся компьютерные программные комплексы исследования мобильных устройств с разрушенными носителями;

компьютерные конструкторы осмотров мест происшествий в 3Д-формате; компьютерные программные комплексы по использованию БПЛА в следственных действиях и оперативно-розыскных мероприятиях и т.д.

В один ряд с вышеназванными и другими прорывными направлениями, используемыми в судопроизводстве, следует поставить внедрение молекулярно-генетических технологий. В результате научных разработок удалось не только «прогнозировать будущее состояние здоровья и оценить риски возникновения патологических состояний» [2, с. 123], но и предложить осуществить всеобщую геномную регистрацию всего населения путем генетического штрих-кодирования на основе тетрааллельных снипов (SNP-локусов. SNP-локус (Single-NucleotidePolymorphismlocus) — это участок ДНК, последовательности аллелей которого различаются одним нуклеотидом), характеризующихся наивысшим уровнем цифровизации (объем полученной таким способом генетической информации для одного человека равен не более 1 килобайта) [3]. Причем эти базы данных геномной информации (нейтральной информации, без возможности узнать что-либо о человеке, кроме его джин-кода) в целях ДНК-идентификации, введенных с помощью отечественных компьютерных программ и оборудования, будут содержаться в серверах, необходимое количество которых будет в 200 раз меньше, чем количество серверов, используемых сейчас в России американской системой CODIS на базе STR-локусов.

Еще одному актуальному направлению использования высокотехнологичных молекулярно-генетических исследований в правоприменительной практике следует уделить внимание.

Хорошо известно, что кошки и собаки оставляют на одежде хозяев и прочих домочадцев свою шерсть, которые не всегда удается полностью убрать, и таким образом при физическом контакте преступника и жертвы часть таких шерстинок может переноситься с одежды одного на одежду другого человека. То есть, если преступник в своем жилище имеет кошку или собаку, то вполне вероятно, что их шерсть перейдет на одежду жертвы. И тогда, выделив из них ДНК и определив ее полиморфизм, можно будет установить конкретное животное и, соответственно лицо (хозяина животного), причастное к совершению преступления.

Возможна и обратная ситуация, когда одежда пострадавшего будет загрязнена шерстинками его домашних питомц(а)ев, и они перенесутся на одежду преступника, по которым, также, будет ясно, что между ними имел место физический контакт. Собачьи или кошачьи шерстинки могут также перенестись на одежду как жертв, так и преступников опосредованно, например через сиденья их личных автомобилей (где перевозили собак и кошек без специальных контейнеров), либо мебель в их домах, что уже применялось при расследовании за рубежом ряда преступлений и послужило одним из доказательств, в том числе принятых судом.

Кроме того, собаки могут быть еще и агрессорами, способными покусать свою жертву, нанеся ей тяжкие телесные повреждения, вплоть до смертельного исхода. Поскольку в этих случаях в ранах пострадавшего остается слюна

собаки, содержащая ДНК, то по ней с помощью тест-систем на ядерную и митохондриальную ДНК также может быть идентифицирована конкретная собака и установлен ее хозяин, если таковой имеется. В отсутствии всеобъемлющей базы данных по ДНК собак такие анализы пока должны проводиться для тех собак, чьи хозяева потенциально могли иметь отношение к расследуемым криминальным происшествиям. При этом ДНК-регистрацию собак (начиная с бойцовских пород) нужно будет начинать проводить, тем более что она, помимо криминалистических целей, имеет целью еще и борьбу с бродячими собаками, число которых в Российской Федерации сейчас оценивается в более чем 700 тысяч из общего поголовья в 22 миллиона собак. ДНК-регистрацию собак следует обязать осуществлять их заводчиков, которые смогут платить за эту услугу специализированным диагностическим фирмам, которые непременно возникнут. При этом у собак появится дополнительный генетический документ, по которому можно будет отслеживать родословные и подтверждать чистоту породы, что лучше делать с помощью однонуклеотидного полиморфизма (ОНП), мутирующего с гораздо меньшей скоростью, чем сейчас используемые для проводимого весьма редко генотипирования собак микросателлитные STR-локусы.

Несмотря на то, что уже есть отдельные примеры использования в некоторых странах (Австралия, Венгрия и др.) в расследовании правонарушений ДНК собак и кошек [4, 5], а также имеются рекомендации по их обнаружению, фиксации и изъятию [6, с. 158-164], такой подход до сих пор не носит массовый характер. Для этого требуются дальнейшие исследования особенностей полиморфных состояний геномов этих видов домашних животных и поиск новых более удобных маркеров и разработка наиболее оптимальных подходов их детекции (генотипирования) для однозначной ДНК-идентификации «владельцев» найденной на месте преступления шерсти (имеется в виду самих кошек и собак) и через нее установление настоящих преступников. При этом в Российской Федерации подобные подходы в криминалистике пока не применялись, и в этой связи значимость таких исследований представляется весьма высокой, поскольку, является, по сути, задачей государственной важности по внедрению передовых технологий в расследование преступлений.

В настоящее время коллективом ученых Института права Уфимского университета науки и технологий совместно с учеными-генетиками Института биохимии и генетики УФИЦ Российской академии наук разрабатываются методические и инструктивные указания по использованию в расследовании преступлений полиморфизма ДНК кошек и собак; а также – новый отечественный оригинальный метод изотермической амплификации целевых фрагментов ДНК для выявления полиморфизма ДНК кошек и собак. При этом новый метод легко может быть применим для работы как с ядерной, так и с митохондриальной ДНК. По своей чувствительности новый изотермический метод амплификации не только не уступает ПЦР, но даже ее превосходит, что очень важно при работе с ничтожными количествами доступного экспертам биологического материала, содержащего к тому же крайне мало ДНК, что

присуще собачьим и кошачьим шерстинкам без волосяных луковиц. Будет завершена разработка нового варианта ПЦР, рассчитанного на комплексный анализ однонуклеотидных замен из разных частей генома в составе единого ампликона (за счет так называемого ПЦР-конструктора), который будет запатентован.

На основе этих новых методов амплификации (изотермического и модифицированной ПЦР) будут создаваться панели полиморфных локусов для выявления полиморфизма ядерных и митохондриальных геномов собак и кошек, которые обеспечат однозначную ДНК-идентификацию исследуемых особей этих домашних животных, благодаря чему при обнаружении на месте преступления их шерстинок, выделения из них ДНК и установления ее полиморфизма, это будет реально помогать в розыске и изобличении преступников. Помимо митогеномных и микродиплотипных локусов, в состав подобранных панелей будут входить гендерные локусы AMELX, AMELY, SRY для определения пола животных, чья шерсть окажется в виде вещественных доказательств в руках экспертов, поскольку это также будет сужать круг «подозреваемых» кошек и собак, а через них и людей, причастных к конкретным криминальным событиям.

При этом для собак будет создана база ДНК-данных, которую можно будет использовать не только для расследования преступлений, но и для «борьбы» с бродячими собаками, а также для ведения родословных на новом генетическом (ДНК) уровне.

Таким образом, разрабатываемые геномные технологии приведут к созданию новых возможностей генотипирования кошек и собак, что, в свою очередь, приведет к опережающему импортозамещению и импортовытеснению путем разработки новых диагностических наборов для ДНК-идентификации кошек и собак на основе полиморфизма их митохондриальных и ядерных геномов.

Таким образом, дальнейший поиск и разработка новых направлений использования современных геномных технологий в правоприменительной практике позволят, в конечном итоге, вывести на более высокую ступень качество судопроизводства в целом.

Список литературы

1. Россинская, Е.Р. Учение о цифровизации судебно-экспертной деятельности в системе частных теорий судебной экспертологии / Е.Р.Россинская // Теория и практика судебной экспертизы в современных условиях: материалы VIII Международной научно-практической конференции. МГЮУ, 28-29 января 2021г.М.,2021. С. 261-267.

2. Хусаинова, Р.И. Современные молекулярно-генетические технологии в медицине: этнические и правовые вопросы / Р.И. Хусаинова и др. // Правовое государство: теория и практика. Уфа. 2020. № 2 (60). С.123-133.

3. Garafutdinov, R.R. A new digital approach to SNP encoding for DNA identification / R.R. Garafutdinov, et al. // Forensic Science International. 2020; 317:110520.

4. Clarke, M., Vandenberg, N. Dog attack: the application of canine DNA profiling in forensic casework // Forensic Sci. Med. Pathol. 2010. V. 6(3). P. 151-157.

5. Pádár, Z., Egyed, B., Kontadakis, K., Füredi, S., Woller, J., Zöldág, L., Fekete, S. Canine STR analyses in forensic practice. Observation of a possible mutation in a dog hair // Int. J. Legal Med. 2002.V. 116(5).P. 286-8.

6. Криминалистика: учебник для бакалавров / под ред. Л.В. Бертовского. М.: РГ-Пресс, 2018. 960 с.

УДК 122/129

ЧЕЛОВЕК В ЦИФРОВОМ МИРЕ: ПРАВОВЫЕ АСПЕКТЫ ИДЕЙ ГУМАНИЗМА

Белобрагина Анна Сергеевна,
аспирант 2 года обучения
Института высокотехнологичного права и социально-гуманитарных наук,
Национальный исследовательский университет «МИЭТ»,
г. Москва, Россия
e-mail: belobragina@gmail.com

Научный руководитель: Даниелян Наира Владимировна,
доктор философских наук,
профессор Института высокотехнологичного права и социально-гуманитарных наук,
Национальный исследовательский университет «МИЭТ»,
г. Москва, Россия
e-mail: vend22@yandex.ru

Аннотация: *повсеместная цифровизация и роботизация требуют от специалистов в области юриспруденции активной работы над закреплением новых цифровых прав человека. В условиях становления цифровой экономики заложить крепкий фундамент для современного законодательства и сохранить гуманистический вектор правовой деятельности поможет популяризация идей цифрового гуманизма. В статье рассматривается гуманистическая сущность правовых норм, сформулированы причины трансформации правового гуманизма и сформулированы предложения по укреплению гуманистического вектора законодательства РФ с философской точки зрения.*

Ключевые слова: *гуманизм, цифровой гуманизм, цифровое право, искусственный интеллект, цифровизация.*

MAN IN THE DIGITAL WORLD: LEGAL ASPECTS OF THE IDEAS OF HUMANISM

Belobragina Anna Sergeevna,
2-year postgraduate student of Institute of high-tech law,
social and human sciences,
National research university of electronic technology
Moscow, Russia
e-mail: belobragina@gmail.com

Scientific adviser
Danielyan Naira Vladimirovna,
doctor of philosophy,
professor of the Institute of high-tech law and social sciences and humanities,
National research university of electronic technology
Moscow, Russia
e-mail: vend22@yandex.ru

Abstract: *widespread digitalization and robotization require experts in the field of jurisprudence to work actively on securing new digital human rights. In the context of the digital economy formation, the popularization of digital humanism ideas will help to lay a solid foundation for modern legislation and maintain the humanistic vector of legal activity. The article discusses the humanistic essence of legal norms, formulates the reasons for the transformation of legal humanism, and gives suggestions for strengthening the humanistic vector of the legislation of the Russian Federation from a philosophical point of view.*

Keywords: *humanism, digital humanism, digital law, artificial intelligence, digitalization.*

Традиционные ценности гуманизма в контексте современного права находятся под угрозой, поскольку в правовом поле возникает множество противоречий, а гуманистические идеи уже не могут существовать в прежних формах. Актуальность темы также обусловлена нарастающими объёмами правонарушений, совершаемых в цифровом пространстве (утечка персональных данных, распространение технологий прослушивания и видеонаблюдения за гражданами, посягательство на неприкосновенность частной жизни и т.д.). Чтобы разобраться в причинно-следственных связях в рамках этого процесса, для начала рассмотрим и сравним гуманистическую сущность правовых норм с точки зрения права в традиционном смысле и с точки зрения цифрового права в широком его понимании.

Идеи гуманизма, центральная из которых провозглашает человека высшей ценностью, лежат в основе современных правовых норм и определяют закономерности правотворчества. «Понимание человека как субъекта общественных отношений является квинтэссенцией гуманизма и его ценностно-нормативного значения, укорененного в институциональной и неинституциональной системах регуляции» [7, стр.91]. С точки зрения права идеи гуманизма стоит понимать как основополагающий принцип правовых

отношений. Законодательно он отражен в базовых юридических документах. Так, согласно Статье 7 УК РФ в ходе уголовного процесса должна быть обеспечена безопасность человека, а меры уголовно-правового характера не могут быть направлены на причинение физических страданий или унижение человеческого достоинства [7]. Признании безусловной ценности человека также закреплено в Конституции РФ, согласно которой «достоинство личности охраняется государством. Ничто не может быть основанием для его умаления. Никто не должен подвергаться пыткам, насилию, другому жестокому или унижающему человеческое достоинство обращению или наказанию» [4]. Таким образом, гуманизм зафиксирован как важнейшая характеристика построения правовых отношений между людьми. Содержание этих отношений отражается в таком юридическом феномене как правовой гуманизм.

Трансформация современного права под влиянием высоких технологий запустила процесс становления цифрового права. Это отрасль права для определения условий и пределов цифровизации как средства внедрения технологий в целях улучшения и оптимизации человеческой жизнедеятельности, она в некоторой степени позволяет традиционным юридическим механизмам адаптироваться к цифровой реальности.

С онтологической точки зрения в условиях цифрового общества право можно рассматривать как «традиционный человеческий регулятор общественных отношений, дополненный цифровым измерением» [1]. Первичными элементами правового измерения становятся не только традиционные принципы и нормы права, но и алгоритмы и цифровые коды. Это дополнение и новая технологическая среда ставит перед юриспруденцией вопросы о категориальном аппарате (например, является ли робот субъектом права), и прямым образом отражается на гуманистической сущности права. С точки зрения гуманистического вектора в новом правовом пространстве права человека и робота не могут быть равны, и именно человек должен оставаться фундаментальной основой. В юридической практике, где ИИ будет являться полноценным правосубъектом, принцип антропоцентризма будет нарушен.

Таким образом, если предметом права в классическом понимании можно считать общественные отношения или источники права, то с точки зрения права цифрового его предметом, по мнению современных исследователей, можно определить искусственный интеллект и криптовалюту [2]. В первом случае в центре внимания находятся правовые отношения между людьми как индивидуальными субъектами права, во втором – правовые отношения в информационной и виртуальной среде, участником которой является не только человек, но и искусственный интеллект. Сохранить гуманистическую сущность правовых норм в новых реалиях могут принципы, закреплённые в философской концепции цифрового гуманизма, для которого технологии вторичны по отношению к человеку. Цифровой гуманизм – по мнению М. Дуэйи, — это четвёртый тип гуманизма, «результат беспрецедентного столкновения между нашим всеобъемлющим культурным наследием и техникой, которая сегодня является уникальной площадкой для социального общения» и способом осмысления новой реальности [6].

К факторам, трансформирующим идеи и принципы гуманизма в контексте правовых норм, можно отнести три основных аспекта. Во-первых, это популяризация идей трансгуманизма, согласно которому человек несовершенен и его физические и когнитивные способности могут быть изменены с помощью новых технологий, при этом информации, технологиям и данным отводится приоритетная роль. Во-вторых, это процессы цифровизации и роботизации практически всех сфер социальной практики, порождающие новые правовые инструменты, законы и приводящие к появлению новых субъектов права. В-третьих, это появление цифрового гуманизма, который можно считать закономерным развитием гуманистических идей и тем самым фундаментом, который удержит гуманистический вектор в цифровом мире.

В качестве иллюстрации рассмотрим ситуацию из юридической практики, которая свидетельствует о том, что права человека ставятся под сомнения в условиях цифровой экономики. При заключении договора со страховой компанией заказчик неверно интерпретировал договор и ввел в электронную анкету не ту форму страхования ответственности. Ещё лет 10 назад такую ошибку мог быть легко устранить всего лишь один телефонный звонок. Однако в условиях цифровизации заработал каскад программных действий, продолжавшийся несколько недель без остановки. Вкратце: «договор» вступил в силу без согласия страхователя, списание средств со счета не могло быть остановлено, переписка, которую вело программное обеспечение, продолжалась неделями, независимо от того, что страхователь не подписал этот договор. В итоге страхователь отозвал разрешение и заблокировал прямое дебетование, что привело сначала к уведомлениям, а затем к письмам, угрожающим юридическими мерами. Только когда, наконец, позвонил реальный человек, процесс получилось остановить.

При этом между клиентом и компанией не было конфликта интересов, всем участникам коммуникации было очевидно, что это была всего лишь ошибка. Не исключено, что именно цифровая некомпетентность сотрудника в компании спровоцировала проблему, но для нас интересно другое: имитация личных интересов в виде заключения договоров, переписки, уведомлений, и т. д., все из которых выполняются без участия человека, принимающего решения, и тем не менее создается впечатление, что человек, принимающий решения, инициировал и несет ответственность за эти действия в каждом случае. Однако, как впоследствии признала компания, такого человека не оказалось.

Цифровизация юридической и экономической практики, которая в конечном итоге может привести к исчезновению всех людей, принимающих решения, станет путем к бесчеловечной экономике и юриспруденции. В этом случае отдельные люди-агенты окажутся во власти анонимной сети программно-контролируемых действий, за которые человек не будет нести никакой ответственности. В этом контексте становится очевидно, что в эпоху цифровых технологий право на человеческое общение должно стать одним из основных прав человека. Именно этой идеи придерживаются сторонники цифрового гуманизма.

Укреплению правовых аспектов идей гуманизма в ответ на современные вызовы цифровой трансформации, дегуманизации и популяризации идей трансгуманизма могут способствовать следующие факторы:

- своевременная оценка угроз трансформации права гуманизма в право трансгуманизма и систематическая работа по снижению уровня этих угроз;
- обдуманное использование возможностей цифровых технологий с проведением соответствующей правовой экспертизы для оценки последствий внедрения новых технологий;
- правовая нейтрализация отрицательного воздействия цифровизации и ИИ на ключевые институты права;

Первостепенную важность в данном контексте приобретают права человека, которые позволят соблюсти баланс между цифровизацией и гуманизацией, это право на живое общение, право на уважение частной жизни, свобода слова, запрет дискриминации. Все эти и другие права человека должны найти отражение в регуляторной и институциональной политике государства. Только симбиоз человека и технологий, построенный на принципах цифрового гуманизма, позволит сохранить свободу воли человека, его сущность как личности и как высшую ценность в системе правовой защиты.

Список литературы

1. Василькова, Е. В. К вопросу об определении предмета цифрового права / Е.В. Василькова, З.А. Шелковникова // Молодой ученый. 2021. № 14 (356). С. 182-184. URL: https://moluch.ru/archive/356/79667/ (дата обращения: 08.02.2023).
2. Волков, В.Э. Цифровое право. Общая часть : учеб. пособие / В.Э. Волков ; М-во науки и высш. образования Рос. Федерации, Самар. нац. исслед. ун-т им. С. П. Королева (Самар. ун-т.Самара: Изд-во Самар. ун-та, 2022. 1 файл (910,48 Кб).
3. Гаврилова, Ю.А. Проблема смысла права в цифровом обществе / Ю.А. Гаврилова // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2020. Т. 24. № 3. С. 608–628.
4. Конституция Российской Федерации: принята всенародным голосование 12 декабря 1993 года. :(принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения 01.02.2023).
5. Латыпова, Э.Ю., Нечаева, Е.В. Спорные вопросы содержания принципа гуманизма в уголовном праве / Э.Ю. Латыпова, Е.В. Нечаева // Вестник Казанского юридического института МВД России. 2019. Т. 10. № 3. С. 355-360.
6. Милад, Дуэйи. В век новых технологий, цифровой гуманизм / Милад, Дуэйи // Журнал Организации объединённых наций по вопросам образования, науки и культуры «Курьер ЮНЕСКО». 2011.№ 4.С. 32-33. URL: http://ru.unesco.kz/the-unesco-courier-humanism-a-new-idea (дата обращения: 14.04.2022).

7. Мусаев, М.А. Гуманизм в структуре правовой системы / М.А. Мусаев// Философия права. Ростов-на-Дону: Изд-во Рост. юрид. ин-та МВД России. 2012. № 4. С. 91-94.

8. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2022) // URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 01.02.2023).

УДК 343.1

ВЫСОКОТЕХНОЛОГИЧНОЕ ПРАВО: СОВРЕМЕННЫЕ ВЫЗОВЫ

Бертовский Лев Владимирович,
доктор юрид. наук, профессор, директор института высокотехнологичного права, социальных и гуманитарных наук
Национальный исследовательский университет «МИЭТ»,
г. Москва, Россия
e-mail: bgl1980@yandex.ru

Аннотация: *в статье обосновывается логистичность, наукоемкость и технологичность современного права и делается вывод о появлении нового феномена высокотехнологичного права. Рассматриваются проблемы становления цифрового судопроизводства, сформулированы этапы обработки релевантной для судопроизводства информации.*

Ключевые слова*: право, регулятор общественных отношений, высокие технологии, унификация доказательств, цифровое судопроизводство, информационные технологии, высокотехнологичное право, обработка информации.*

HIGH-TECH LAW: MODERN CHALLENGES

Bertovsky Lev Vladimirovich,
doctor of law, professor,
Director of the Institute of high-tech law, social sciences and humanities,
National research university of electronic technology (MIET),
Moscow, Russia
e-mail: bgl1980@yandex.ru

Abstract: *the article substantiates the logistics, knowledge-intensive and technological nature of modern law and concludes about the emergence of a new phenomenon of high-tech law. The problems of the formation of digital legal proceedings are considered, the stages of processing relevant information for legal proceedings are formulated.*

Keywords: *law, regulator of public relations, high technologies, technological law, digital legal proceedings, information technologies, high-tech law, information processing.*

Президент РФ Путин В.В. 9 мая 2017 года подписал указ № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы», где определил в качестве одной из важнейших задач, стоящих перед государством обеспечение использования российских информационных и коммуникационных технологий в органах государственной власти Российской Федерации, компаниях с государственным участием, органах местного самоуправления.

Существует тесная связь между социально-экономическими преобразованиями в обществе и судьбой институтов государственной власти, в частности судебных органов. Без коренной модификации судопроизводства, без внедрения информационных технологий, стандартизации процессуальных документов, использование алгоритмов в процессе доказывания, включение всех или большинства судебных актов в единую аналитическую систему сложно представить себе дальнейшее гармоничное развитие общества.

Экспоненциальное развитие науки и техники, изменение социальных укладов и другие глобальные изменения, которые произошли за последнее время, потребовали значительной модернизации и права. Мы вступил в эпоху высокотехнологичного права под которым понимается такой логистичный, наукоемкий и технологичный регулятор общественных отношений, который, с одной стороны, использует высокие технологии в процессе правоприменения, а с другой - регламентирует возникающие с ними отношения [1].

Реалии правоприменения требуют ускорения судебных процессов. Поэтому обоснованно выглядит постепенный переход к цифровому судопроизводству - урегулированному нормами процессуального права деятельность суда, участвующих в деле лиц и других участников процесса, а также органов исполнения судебных решений по разрешению юридических дел, в которой ключевым фактором являются данные в цифровом виде, обработка и использование результатов анализа которых по сравнению с традиционными формами судопроизводства позволяют существенно повысить его эффективность.

С этой точки зрения, представляется наиболее важным четыре процесса:

1. Получение и трансформация релевантной для целей судопроизводства информации в машиночитаемую;

2. Дальнейшее ее накопление и обработка;

3. Обратная трансформация информации в человекочитаемый вид;

4. Использование полученных результатов.

В современном судопроизводстве наибольшее количество информации к правоприменительным органам поступает после соответствующей трансформации в виде документов, реже в натуральном виде (вещественные доказательства, похищенное или оспариваемое имущество, и т.д.). К документам можно отнесите различные заявления, справки, выписки, протоколы следственных действий и др. Для последующей обработки все они должны быть преобразованы в машиночитаемую форму. В отношении документов особо больших проблем не возникает: сегодня существуют и

успешно широко используются как технические средства сканирования, так и программные методы распознавания (оптическое распознавание символов (англ. optical character recognition, OCR) - механический или электронный перевод изображений рукописного, машинописного или печатного текста в текстовые данные, использующиеся для представления символов в компьютере, например, в текстовом редакторе). Хотя здесь также имеются свои проблемы. Накопленные эмпирические данные в виде различных справок, обзоров, дел в архивах судов, следственных отделов и необходимые для последующего машинного анализа и использования, а также создания нейросетей для выработки предложений решений по аналогичным делам содержаться на бумажных носителях. Они требуют соответствующей обработки, как это делается в современных библиотеках, для чего кадровое и техническое обеспечение в правоприменительных органах отсутствует, да и материальные затраты довольно существенные. Организации, которые занимаются подобными вопросами оценивают сканирование одного листа в 1 рубль и еще один рубль придется заплатить за его распознавание. С учетом объемов архивов сумма получается колоссальной! И это, не считая проблем с распознаванием рукописных текстов, для которых соответствующего программного обеспечения надлежащего качества пока нет, а те, которые есть дороги, и предъявляют высокие требования к аппаратному обеспечению.

Еще сложнее приходится, когда возникает задача «оцифровки» различных материальных объектов, в т.ч. и места происшествия. Конечно, в настоящее время имеются 3D-сканеры, которые осуществляют сканирование небольших объектов, а также сканеры, которые сканируют здания, сооружения, помещения, однако, первые хоть и обеспечивают точность от 0.018 мм, что позволяет сканировать в т.ч. и выявленные следы рук, для последующей идентификации, но работают медленно и, как указано выше, только с небольшими объектами, а вторые хоть и работают с большими объектами и достаточно быстро, обеспечить необходимую точность не могут. Кроме того, формат отсканированных изображений не всегда согласуется со средами виртуального моделирования: 3Ds Max, Maya, Rhinoceros и пр. Для решения задач судопроизводства нужно решить техническую задачу по созданию компактного, мобильного комплекса, обеспечивающего 3D-сканирование больших объектов, в т.ч. места происшествия, с разрешением позволяющем фиксировать различные следы, с целью последующего их воспроизводства для проведение экспертных исследований.

Таким образом, полученная в машиночитаемом виде информация готова к дальнейшей накоплению и обработке искусственным интеллектом. Для подготовки предложений по разрешению находящего в производстве дела может понадобиться дополнительная информация, которая может быть получена в результате производства следственных и судебных действий, а также при обращении ИИ к различным организациям, базам данных (о судимости, административной практики, расписания движения транспортных средств и др.). Причем в последнем случае возникает проблема с обеспечения доступа к этим базам, которая должна решаться путем принятия

соответствующих нормативных актов. Представляется, что процессы накопления и обработки информации должны осуществляться на основе проведенной унификации доказательств различных видах судопроизводства.

Считаю, что по результатам машинного анализа имеющейся информации ИИ должен готовить не решение по юридическому делу, а именно проект решения. Исследователи многих стран обсуждают проблему может ли ИИ выступать в качестве судьи.

Однако многочисленные дискуссии пока ни к чему не привели, но все настойчивее звучат мнения о том, что судья имеет право на усмотрение и определенную свободу действий при принятие решении по делу, исходя из конкретной ситуации и своего внутреннего убеждения.

Так, в Европейской этической хартии об использовании искусственного интеллекта в судебных системах и окружающих их реалиях Принята на 31-м пленарном заседании ЕКЭП (Страсбург, 3-4 декабря 2018 года) сформулировано пять принципов об использовании искусственного интеллекта в судебных системах и окружающих их реалиях:

1. Уважения основополагающих прав: обеспечить разработку и внедрение инструментов и услуг, основанных на искусственном интеллекте, соответствующих основным правам.

2. Недискриминации: определенным образом препятствовать развитию или усилению любой дискриминации между отдельными лицами или группами лиц.

3. Качества и безопасности: при обработке судебных решений и данных, необходимо использовать сертифицированные источники и нематериальные данные с применением моделей, разработанных на междисциплинарной основе, в безопасной технологической среде.

4. Прозрачности, беспристрастности и достоверности: сделать методы обработки данных доступными и понятными, разрешить проведение внешнего аудита.

5. Контроля пользователем: избежать предписывающего подхода и позволить пользователю выступать в роли информированного лица, ответственного за свой выбор [2].

Наиболее важным представляется принцип контроля пользователя, в соответствии с которым, судья человек должен иметь возможность опровергнуть предложение искусственного интеллекта и принять собственное решение по делу, а участники процесса должны иметь возможность прямого обращение к человеческому суду (состоящего из людей) и оспорить решение, принятое искусственным интеллектом.

Примечательно, что большинство споров среди специалистов ведется по поводу назначения наказания человеку, т.е. по сути принятия решения машиной, учету мотива совершенного поступка, наличии смягчающих обстоятельств, в т.ч. и основанных на эмоциональном состоянии виновного. Но не менее важно понимать, как, на основе какого алгоритма, принимается такое решение.

Поэтому человекочитаемый проект решения должен содержать ссылку на те факторы, которые позволили ИИ сделать те или иные выводы для окончательной оценки и принятия решения человеком.

Для качественного обеспечения функционирования цифрового судопроизводства непростой проблемой является низкий уровень технической подготовленности кадров. Необходимо дополнительное обучение всех категорий юристов современным информационным технологиям не только как продвинутых пользователей офисных программ, а как лиц, осведомленных в стандартах и новациях IT в целом, особенно осведомленных в юридических аспектах обеспечения функционирования IT. Решением данной проблемы может стать создание новых основных и дополнительных инновационных профессиональных образовательных программ на стыке двух специальностей юридического и технического направления, реализуемых на базе многопрофильных университетов.

Очевидно, что рассматриваемый подход к организации судопроизводства потребует внесения значительных корректив в реализуемую Концепцию судебной реформы, а также в целый ряд нормативно-правовых актов, как-то УПК РФ, ГПК РФ, АПК РФ, «О судебной системе Российской Федерации», «О прокуратуре Российской Федерации», и ряд других. Кроме того, необходима разработка соответствующих планов мероприятий («дорожная карта»), сформированных в рамках системы управления реализацией вышеуказанного указа Президента РФ от 09.05.2017г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».

Очевидно, что потребуется еще много интеллектуальных, материальных, финансовых, временных затрат, прежде чем инновационные предложения реализуются в практической деятельности судов, правоохранительных и иных государственных органов. Однако совершенно ясно, что судопроизводство должно отвечать современным реалиям и имплементация в деятельность его субъектов новейших информационных и коммуникационных технологий – жизненная необходимость.

Список литературы

1. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский // Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. № 4. С. 735-749.

2. Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях Принята на 31-м пленарном заседании ЕКЭП // Страсбург, 3-4 декабря 2018 года. URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4.

УДК 343.982.4

АКТУАЛЬНЫЕ ВОПРОСЫ ПОЧЕРКОВЕДЧЕСКОГО ИССЛЕДОВАНИЯ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ РУКОПИСЕЙ

Бобовкин Станислав Михайлович,
кандидат юридических наук, доцент кафедры исследования документов учебно-научного комплекса судебной экспертизы
email: s.m.bobovkin@mail.ru

Кудяков Тимур Тагирович,
старший преподаватель кафедры огневой подготовки учебно-научного комплекса специальной подготовки
email: awers87@yandex.ru

Ермолов Андрей Сергеевич,
преподаватель кафедры огневой подготовки учебно-научного комплекса специальной подготовки
Московский университет МВД России им. В.Я. Кикотя
(МосУ МВД России им. В.Я. Кикотя),
г. Москва, Россия
email: an76n@yandex.ru

Аннотация: *в статье рассматриваются отдельные вопросы практики криминалистического исследования изображений рукописей. Отмечаются ключевые особенности используемых в различных государственных судебно-экспертных учреждениях Российской Федерации методических подходов к производству судебно-почерковедческих экспертиз указанных современных объектов. Обозначаются перспективные направления развития обозначенной области использования специальных знаний.*

Ключевые слова: *судебно-почерковедческое исследование, изображения рукописей, экспертная практика, актуальные подходы, особенности методики, перспективы совершенствования, возможности комплексного подхода, разграничение компетенции экспертов.*

TOPICAL ISSUES OF HANDWRITING RESEARCH OF DIGITAL IMAGES OF MANUSCRIPTS

Stanislav Mikhailovich Bobovkin,
candidate of law, associate professor of the department of document research of the educational and scientific complex of forensic examination
email: s.m.bobovkin@mail.ru
Timur Tagirovich Kudyakov,
senior lecturer of the firearms training department of the special training educational and scientific complex
email: awers87@yandex.ru

Andrey Sergeevich Ermolov ,
Instructor at the Firearms Training Department of the Special Training Educational and Scientific Complex
Moscow university of the Ministry of internal affairs of Russia named after V.Ya. Kikotya (MosU of the Ministry of Internal Affairs of Russia named after V.Ya. Kikotya),
Moscow, Russia
email: an76n@yandex.ru

Abstract: *the article deals with certain issues in the practice of forensic investigation of images of manuscripts. The key features of the methodological approaches used in various state forensic institutions of the Russian Federation to the production of forensic and penmanship examinations of these modern objects are noted. Prospective directions of improvement in the indicated area of special knowledge usage are outlined.*

Keywords: *forensic and penmanship examination; images of manuscripts; expert practice; current approaches; peculiarities of methodology; prospects for improvement; possibilities of complex approach; delimitation of experts' competence.*

В период цифровизации судебно-почерковедческая экспертиза характеризуется появлением современных экспертных методик, увеличением количества исследований, возрастанием их сложности, а также появлением новых видов объектов. Среди последних наибольшее распространение получили цифровые и аналоговые изображения рукописей (текстов, кратких записей и подписей различного объема, состава, а также информативности). Основными причинами их широкого распространения являются развитие электронного документооборота, большие возможности фотофиксации, появление значительного количества копий (в том числе электронных), удобство архивирования рукописей в цифровом формате, отсутствие реальной возможности получения (истребования) документов и случаи повреждения (непреднамеренного и целенаправленного) либо утраты документов.

Сложности криминалистического исследования указанных специфических объектов в первую очередь обусловлены особенностями процессов их фиксации и воспроизведения, меньшей степенью информативности, ограниченной пригодностью, искажением информативных признаков почерка исполнителя. Помимо этого, специфика судебно-почерковедческой экспертизы изображений почерковых реализаций определена наличием дополнительных диагностических признаков, вызванных свойствами использовавшихся фиксирующих и копировально-множительных устройств (например, дефектами отдельных узлов), широкими возможностями применения технических средств и приемов при их выполнении (в особенности – монтажа документа в целом либо его реквизитов, в число которых входят изображения почерковых объектов) [1, с. 114]. Дополнением к этому выступают отдельные межведомственные разногласия в части определения сущности рассматриваемого объекта и особенностях методики,

препятствующие созданию единого методического подхода к процессу их экспертного исследования.

Об актуальности и практической значимости обозначенной тематики свидетельствуют итоги рецензирования заключений экспертов-почерковедов, демонстрирующие существенное количество отказов от решения вопроса по существу, значительный процент недостаточно обоснованных выводов и допущение грубых экспертных ошибок. В дополнение к этому о существенных проблемах почерковедческого исследования изображений рукописей в процессе интервьюирования отмечают государственные и негосударственные эксперты. С учетом указанных обстоятельств обозначенная проблема требует скорейшего решения со стороны экспертного сообщества.

Рассмотрим основные современные подходы к производству рассматриваемых экспертиз, реализуемые различными государственными судебно-экспертными учреждениями Российской Федерации.

Экспертно-криминалистическими подразделениями МВД России в 2020 году был пересмотрен длительный запрет на исследование изображений рукописей. В работе «Исследование изображений почерковых объектов в документах, выполненных при помощи копировально-множительной техники», подготовленной коллективом авторов ЭКЦ МВД России, проделана значительная работа по описанию возможностей почерковедческого исследования данных объектов и алгоритму их проведения [2]. Также рассмотрены отдельные теоретические положения обозначенного направления криминалистического исследования документов, затронуты вопросы формулирования выводов эксперта, изложен собственный взгляд на проблему пригодности изображений почерковых объектов.

Авторами обуславливается подход к почерковедческому исследованию изображений рукописей, основанный на формулировании выводов об их исполнителе в условной форме с учетом невозможности выявления признаков технической подделки реквизитов, изображенных в копиях документов [3, с. 52]. Его сущность заключается в использовании традиционной качественно-описательной методики с определенными дополнениями посредством включения новых этапов исследования и расширением решаемых задач в рамках существующих. В частности, в предварительную стадию предлагается включать этапы, направленные на установление способа выполнения изображения рукописи и оценку его качества, а также расширить количество задач на этапе определения наличия либо отсутствия признаков применения технических и программных средств, предварительной технической подготовки, дополнив этот перечень вопросами об установлении признаков монтажа документа либо его реквизитов методами технико-криминалистической экспертизы. В рамках стадии детального исследования, по мнению указанных специалистов, специфика заключается лишь в определенных сложностях в части изучения ряда информативных признаков почерка, что обусловлено отсутствием возможности непосредственного анализа штрихов рукописи [3, с. 55]. Между тем авторы констатируют, что стадия оценки результатов должна проводиться по аналогии с соответствующей

стадией методики идентификационной почерковедческой экспертизы оригиналов текстов, кратких записей и подписей. Тогда как формулирование выводов осуществляется применительно к исполнителю оригинала рукописи. При этом отмечается безальтернативность формулировки условного идентификационного вывода в отношении изображений почерковых реализаций по причине отсутствия возможности исключения факта применения технических средств и приемов при выполнении оригинала исследуемого объекта. В связи с чем, сформировавшаяся практика производства судебно-почерковедческих экспертиз в системе МВД России предполагает возможность исследования изображений почерковых объектов с формулировкой по их результатам различных по степени определенности выводов при условии, что оригинал исследуемой почерковой реализации выполнен без применения технических приемов и средств.

Вышеизложенные положения свидетельствуют о существенном пересмотре подходов к исследованию изображений рукописей и допустимости их исследования методами почерковедческой и технико-криминалистической экспертизы документов. Научно-практический интерес представляют теоретические и методические положения вышеуказанной работы. В качестве основного достоинства следует также отметить включение в методику дополнительных этапов по установлению способа выполнения объекта, оценку его качества, а также обязательное решение задач об установлении признаков монтажа документа либо его реквизитов на этапе определения наличия либо отсутствия технической подделки. Полагаем, что обязательное решение указанного вопроса приведет к более полному изучению анализируемого объекта, увеличению фактов установления простого монтажа реквизитов документов, а также снизит процент грубых экспертных ошибок.

В системе государственных судебно-экспертных учреждений Минюста России используются собственные методические рекомендации по криминалистическому исследованию почерковых объектов, изложенные в работе «Производство судебно-почерковедческих экспертиз подписей по электрофотографическим копиям» [4]. В ней содержатся правовые, теоретические, методические основы и отдельные организационно-тактические положения почерковедческого исследования рукописей, предложены некоторые направления совершенствования отмеченной области использования специальных знаний. В части особенностей методики исследования авторами обосновывается потребность в осуществлении предварительного технико-криминалистического исследования копий документов, обусловленная широкими возможностями монтажа реквизитов в исследуемых объектах. При этом указанный этап исследования по определению способа выполнения документа и установления признаков монтажа должен производиться специалистом в области судебно-технической экспертизы документов.

Практика решения идентификационных задач почерковедческой экспертизы в отмеченных учреждениях реализуется по пути исследования изображений рукописи с установлением исполнителя почеркового объекта, выступившего оригиналом для изготовления копии. В свою очередь, вопросы,

связанные с определением способа выполнения документа, наличием либо отсутствием оригинала, исследованием рукописи на предмет применения технических средств и приемов экспертом-почерковедом, не решаются, т.к. находятся за пределами его компетенции. Таким образом, в судебно-экспертных лабораториях и центрах судебной экспертизы при Минюсте России сложилась практика последовательного проведения судебно-технической и судебно-почерковедческой экспертизы. Отмеченный подход продиктован вопросами разграничения компетенции экспертов нескольких специальностей, особенностями их профессионального обучения и повышения квалификации.

Внимания заслуживает специфика формулирования выводов в заключениях по результатам производства почерковедческих экспертиз в системе государственных судебно-экспертных учреждений Минюста России. Примечательно, что выводы о конкретном исполнителе спорной рукописи дополняются данными о том, что вопрос о процессе получения изображения рукописи, а также возможностях монтажа документа и его реквизитов не решался ввиду его нахождения за пределами компетенции эксперта-почерковеда. По мнению авторов, данная формулировка позволяет минимизировать факты некорректной трактовки вывода следственными и судебными органами.

Научно-практическое значение имеют методические разработки авторского коллектива РФЦСЭ при Минюсте России в части экспертного исследования изображений почерковых объектов в цифровых копиях документов. Указанные рекомендации подготавливаются в рамках соответствующей научно-исследовательской работы, а на настоящем этапе получили свою реализацию в научных публикациях по указанной теме [5, с. 70-80; 6, с. 94-103]. В работах рассматриваются технологические аспекты цифрового фотографирования и сканирования, приводится криминалистическая характеристика цифрового фотоснимка (скана) как объекта почерковедческой экспертизы, уточняются некоторые базовые понятия данного направления рассматриваемой области использования специальных знаний. В дополнение к этому предлагаются качественные характеристики изображений почерковых объектов, полученных способом сканирования и фотографирования, обуславливающие их пригодность для проведения рассматриваемого экспертного исследований и возможность формулирования определенных выводов по существу поставленных вопросов. Особое внимание отводится факторам, влияющим на снижение качества цифрового копирования, и их признакам. В частности, авторами выделены три группы факторов: технические, обусловленные отдельными характеристиками устройств ввода, печати и копирования; технологические, связанные с внешними условиями получения изображения (фотографирования); особенности либо недостатки как оригинала документа, так и почерковой реализации (например, наложение штрихов оттиска печати на подпись). Помимо этого, приводятся алгоритмы действий эксперта-почерковеда при производстве судебно-почерковедческих экспертиз цифровых копий, представленных на исследование посредством компьютерных файлов, в рамках которых особый интерес вызывают

предложение о включении в структуру стадии предварительного исследования рассматриваемой методики дополнительного этапа по улучшению качества исследуемого почеркового объекта путем его обработки посредством графических редакторов [6, с. 94-103].

Вместе с тем анализ трудов сотрудников экспертных учреждений системы Минюста России свидетельствует о сохранении в основе актуальных методических рекомендации ключевого постулата о наличии оригинала документа и предоставлении на экспертизу его прямой копии. В результате эксперт решает только идентификационную задачу по установлению исполнителя оригинала рукописи, тогда как диагностические задачи, направленные на определение способа выполнения рукописи и установление факта технической поделки остаются за пределами его компетенции.

Таким образом, анализ сформировавшейся практики производства судебно-почерковедческих экспертиз изображений рукописей в разных государственных и негосударственных судебно-экспертных учреждениях России, а также изучение работ видных отечественных и иностранных ученых позволили наметить некоторые перспективные направления развития данной области использования специальных знаний:

1. Формирование базовых теоретических положений криминалистического исследования изображений почерковых объектов (понятие, предмет, круг решаемых экспертных задач, многообразие объектов, а также перечень субъектов).

2. Разработка современных критериев определения качества изображений рукописей для решения вопросов о пригодности объектов в целях дальнейшего идентификационного почерковедческого исследования.

3. Подготовка методических рекомендации по установлению признаков, свидетельствующих о монтаже всего документа либо его отдельных реквизитов.

4. Разработка общей валидированной и сертифицированной методики почерковедческого исследования рукописей, а также ряда частных методик исследования изображений почерковых реализаций с учетом особенностей технологических процессов конкретных видов фиксирующих и копировально-множительных устройств.

5. Определение возможностей реализации комплексного подхода при производстве судебно-почерковедческих экспертиз изображений рукописей со специалистами из других областей научных знаний: технико-криминалистической экспертизы документов (направленного на определение способа выполнения изображения рукописи), компьютерно-технической экспертизы (в целях решения задач по установлению признаков и фактов монтажа), фототехнической экспертизы (для решения вопросов в части определения наличия фотомонтажа). Помимо этого, практически значимым представляется рассмотрение специфики использования в экспертизе указанных объектов различных форм комплексного исследования: комплекса исследований в рамках судебно-почерковедческой экспертизы, комплекса экспертиз и комплексной экспертизы.

6. Создание современных практических рекомендаций по тактике назначения и организации производства криминалистического исследования изображений рукописей, а также рекомендации консультативного характера по тактике оценки и использованию полученных результатов в правоохранительной деятельности.

7. Внедрение в методику судебно-почерковедческого исследования изображений почерковых реализаций отдельных кибернетических методов и методик, расширяющих возможности установления монтажа документа и его отдельных реквизитов.

8. Созданию в рамках судебного почерковедения соответствующего раздела «Почерковедческое исследование изображений рукописей» и формирование одноименного спецкурса.

Поэтапное решение вышеуказанных задач позволит решить значительную часть проблем в области судебно-почерковедческой экспертизы изображений рукописей, а также внесет существенный вклад в процесс совершенствования научно-методических и организационно-тактических положений судебно-экспертной деятельности.

Список литературы

1. Бобовкин, С.М. Изображения рукописей – современные объекты почерковедческой экспертизы/ С.М. Бобовкин // Правосудие / Justice. Москва: РГУП, 2022. Т. 4. № 2. С.113-133.

2. Карпухин, А.В. Исследование изображений почерковых объектов в документах, выполненных при помощи копировально-множительной техники / А.В. Карпухин, А.А. Плинатус, А.А. Сафонов, Е.А. Болдырева. ЭКЦ МВД России, 2020. 38 с.

3. Плинатус, А.А. Актуальные вопросы исследования изображений почерковых объектов / А.А. Плинатус, Л.М. Круглов // Научный портал МВД России. 2021. № 3 (55). С.52–56.

4. Ефремова, М.В. Производство судебно-почерковедческой экспертизы по электрофотографическим копиям (информационное письмо) / М.В. Ефремова, В.Ф. Орлова, А.Д. Старосельская // Теория и практика судебной экспертизы. М.: ГУ РФЦСЭ при Минюсте России, 2006. № 1 (1).

5. Жижина, М.В. Судебно-почерковедческое исследование по цифровым фотографическим копиям документов / М.В. Жижина // Теория и практика судебной экспертизы. 2020. Т. 15. № 2. С.70–80.

6. Жижина, М.В. Судебно-почерковедческое исследование по цифровой скан фотокопиям документов (часть 2) / М.В. Жижина // Теория и практика судебной экспертизы. 2022. Т. 17. № 3. С.94–103.

УДК 343.1

ПРОТИВОДЕЙСТВИЕ НЕЗАКОННОМУ НАРКООБОРОТУ И НАРКОПОТРЕБЛЕНИЮ НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ И ИХ АНАЛОГОВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Власов Валерий Александрович,
канд. юрид. наук, доцент
Красноярский государственный аграрный университет,
Сибирский юридический институт МВД России,
г. Красноярск, Россия
Сибирская пожарно-спасательной академия ГПС МЧС России,
г. Железногорск, Россия
e-mail: vav.70@mail.ru

Аннотация: в *статье исследуются некоторые теоретические и практические аспекты противодействия незаконному обороту наркотических средств и психотропных веществ, и их аналогов, совершаемых с использованием электронных или информационно-телекоммуникационных сетей. Автором предложены отдельные эффективные средства противодействия незаконному обороту наркотических средств, психотропных веществ и их аналогов, а также сделаны обоснованные выводы о необходимости дальнейшей работы по данному направлению. В частности, предлагается закрепить в КоАП РФ ответственность не только за пропаганду, но и за незаконную рекламу наркотических средств и психотропных веществ, и их аналогов в сети Интернет.*

Ключевые слова: *наркооборот, наркопотребление, пронаркотическая информация, противодействие, незаконная реклама наркотических средств и психотропных веществ, наркотические средства, психотропные вещества, цифровизация, информационно-телекоммуникационные системы, электронные технические средства, сеть Интернет, доказательства, наркотизация общества, молодежная наркозависимость.*

COUNTERACTION TO ILLEGAL DRUG TRAFFIC AND DRUG USE OF NARCOTIC DRUGS AND PSYCHOTROPIC SUBSTANCES AND THEIR ANALOGUES COMMITTED WITH THE USE OF ELECTRONIC OR INFORMATION AND TELECOMMUNICATION NETWORKS: THEORY AND PRACTICE ISSUES

Vlasov Valery Alexandrovich,
candidate of legal sciences, associate professor
Krasnoyarsk state agrarian university,
Siberian law institute of the Ministry of internal affairs of Russia,

Krasnoyarsk, Russia
Siberian fire and rescue academy of the state fire service of the Ministry of emergency situations of Russia,
Zheleznogorsk, Russia
e-mail: vav.70@mail.ru

Abstract: *the article examines some theoretical and practical aspects of combating illicit trafficking in narcotic drugs and psychotropic substances, and their analogues, committed using electronic or information and telecommunication networks. The author proposes some effective means of countering the illicit trafficking in narcotic drugs, psychotropic substances and their analogues, and also draws reasonable conclusions about the need for further work in this area. In particular, it is proposed to consolidate in the Code of Administrative Offenses of the Russian Federation responsibility not only for propaganda, but also for illegal advertising of narcotic drugs and psychotropic substances, and their analogues on the Internet.*

Keywords: *drug trafficking, drug consumption, pro-drug information, counteraction, illegal advertising of narcotic drugs and psychotropic substances, narcotic drugs, psychotropic substances, digitalization, information and telecommunication systems, electronic technical means, the Internet, evidence, drug addiction of society, youth drug addiction.*

В сегодняшних экономических реалиях и сложной политической обстановке, имеющиеся проблемы наркомании угрожают национальным интересам России, отрицательно влияют на социально-экономическую политику внутри страны, подрывают авторитет Российского государства на международной арене, а также угрожают жизни и здоровью нации. В частности, в последнее время вызывает большую тревогу в обществе активное пропагандирование пронаркотической информации в Интернете, увеличение спроса наркотических средств посредством поисковых систем. Более того, появились новые опасные тенденции, направленные на подъем подростковой и молодежной наркозависимости. Считаем, что наркопреступность в сети Интернет – это отдельное одно из самых опасных направлений преступности, в содержании которой лежат две взаимозависимые и взаимообусловленные сферы: первая – это незаконный оборот наркотических средств и психотропных веществ, и их аналогов, вторая – непосредственно сеть Интернет.

В современный период времени политика Российского государства по противодействию незаконному наркообороту является приоритетной для нашей страны. В п. 47 Указа Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» прямо закреплено, что достижение целей обеспечения государственной и общественной безопасности осуществляется путем реализации государственной политики, направленной на решение следующих задач: снижение уровня криминализации общественных отношений, развитие единой государственной системы профилактики правонарушений; выявление и пресечение преступлений, связанных с

незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров [1].

В Указе Президента РФ от 23.11.2020 № 733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года» закреплено: «В результате реализации антинаркотической политики в 2010 - 2020 годах наркоситуация в России в целом стабилизировалась, однако согласно данным мониторинга, проводимого Государственным антинаркотическим комитетом, в большинстве регионов Российской Федерации она остается напряженной», поскольку ежегодно правоохранительными органами выявляется около 200 тысяч преступлений, связанных с незаконным оборотом наркотиков [2].

Следует обратить внимание на тот факт, что Президент Российской Федерации В.В. Путин дал поручение МВД России принять дополнительные меры, направленные на противодействие незаконному обороту наркотиков в государстве. Речь идет в первую очередь о профилактике потребления наркотиков, реабилитации и ресоциализации, поддержке негосударственных организаций, реализующих специальные программы помощи лицам, потребляющим подобные вещества [3].

Федеральный закон от 08.01.1998 № 3-ФЗ «О наркотических средствах и психотропных веществах» в главе VI. «Противодействие незаконному обороту наркотических средств, психотропных веществ и их прекурсоров» собственно и предусматривает целый ряд мероприятий в исследуемой области [4].

Ю.А. Гамидов, Е.Н. Холопова обращают внимание на то, что: «Наркооборот серьезную реальную угрозу национальной безопасности России, здоровью, жизни и достоинству людей, подрывает нравственные, социальные, политические, экономические устои общества и государства» [5].

Наркопреступность в сети Интернет - новое негативное явление, появившееся в конце XX века с развитием сети Интернет, преступники совершенствуют как формы, так и методы совершения преступлений в исследуемой области. Как показывает практика, использование правонарушителями электронных или информационно-телекоммуникационных сетей значительно увеличивает возможности для вовлечения гораздо большего числа лиц в преступную деятельность, пропаганды наркопотребления и увеличения количества других противоправных действий, связанных с изготовлением и сбытом наркотиков.

Безусловно, важнейшая роль при расследовании уголовных преступлений и административных правонарушений в рассматриваемой области отводится специалисту в обеспечении технически корректного обращения с электронным носителем с целью сохранения находящейся на нем компьютерной информацией. Именно он позволяет, в известных пределах, изучить содержимое носителя и технически правильно описать основные данные о его электронном наполнении в протоколе следственного действия Автор в своих публикациях уже обращал внимание на то, что желательно подкорректировать формулировку ч.2 ст. 164-1 УПК РФ и предусмотреть в ней, что не только изъятие, но также поиск и фиксация электронных носителей информации в

ходе проведения следственных действий проводились с обязательным участием специалиста. Такое решение вопроса позволит исключить двусмысленность и сориентирует правоохранительные органы на изыскание возможностей обеспечивать участие компьютерно-технических специалистов во всех следственных действиях, в ходе которых могут быть обнаружены электронные носители и информация на них [6]. Практика раскрытия преступлений в области незаконного оборота наркотиков свидетельствует, что на территории г. Красноярска рассматриваемый способ выполнения нехватки компьютерно-технических специалистов оказался в достаточной мере востребованным и в настоящее время демонстрирует устойчивую тенденцию к росту [7].

Специалисты верно отмечают, что российский законодатель не всегда учитывает современные достижения науки в области высоких технологий применительно к уголовному судопроизводству [8].

Предлагаем также закрепить в КоАП РФ ответственность не только за пропаганду, но и за незаконную рекламу наркотических средств и психотропных веществ, и их аналогов в сети Интернет. В частности, статью 6.13 «Пропаганда наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, новых потенциально опасных психоактивных веществ», а именно п. 1.1. «Пропаганда **и незаконная реклама** (дополнение – В.В.) наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства, психотропные вещества или их прекурсоры, их частей, содержащих наркотические средства, психотропные вещества или их прекурсоры, либо новых потенциально опасных психоактивных веществ с использованием информационно-телекоммуникационной сети «Интернет» - далее по тексту.

Обращает на себя внимание тот факт, что состояние преступности в сфере противоправного наркооборота, в том числе совершаемых с использованием сети Интернет, обусловлено достаточно высоким уровнем латентности. Поэтому специально уполномоченные подразделения по контролю за оборотом наркотиков МВД России должны качественно осуществлять постоянный профессиональный контроль как вновь создаваемых веб-сайтов в социальных сетях, так и отслеживать факты распространения массовых рассылок электронных писем или сообщений и т.п.

Подводя итог, следует сделать обоснованный вывод о том, что необходимо принимать системные меры по противодействию незаконному наркообороту наркотических средств, психотропных веществ или их прекурсоров, совершаемому с использованием электронных или информационно-телекоммуникационных сетей, чтобы получить реальный положительный результат.

Список литературы

1. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (часть II). Ст. 5351.

2. Указ Президента РФ от 23.11.2020 № 733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года» // СЗ РФ. 2020. № 48. Ст. 7710.

3. Перечень поручений по итогам встречи с представителями общественности Дальнего Востока (утвержден Президентом РФ 25.10.2019 г. № Пр-2196) // URL: http://www.kremlin.ru (дата обращения: 10.02.2023).

4. Федеральный закон от 08.01.1998 № 3-ФЗ (ред. от 29.12.2022 г.) «О наркотических средствах и психотропных веществах» // СЗ РФ. 1998. № 2. Ст. 219.

5. Гамидов, Ю.А. Актуальные проблемы привлечения органами, осуществляющими оперативно-розыскную деятельность, физических лиц к проведению проверочной закупки наркотических средств / Ю.А. Гамидов, Е.Н. Холопова // Наркоконтроль. 2012. № 3. С.18 - 21.

6. Червяков, М.Э. Участие специалиста в области компьютерной техники в следственных действиях по уголовным делам о незаконном обороте наркотических средств, психотропных веществ или их аналогов: отдельные актуальные аспекты (начало) / М.Э. Червяков, В.А. Власов // Право и государство: теория и практика. 2022. № 11 (215). С. 217-220.

7. Червяков, М.Э. Участие специалиста в области компьютерной техники в следственных действиях по уголовным делам о незаконном обороте наркотических средств, психотропных веществ или их аналогов: отдельные актуальные аспекты (продолжение) / М.Э. Червяков, В.А. Власов // Право и государство: теория и практика. 2022. № 12 (216). С. 283-285.

8. Курбатова, С.М. Высокие технологии как средство компенсаторного характера для реализации правового статуса участников уголовного судопроизводства, имеющих ограниченные возможности / С.М. Курбатова // Высокотехнологичное право: генезис и перспективы. Материалы III Международной межвузовской научно-практической конференции. Красноярск: Красноярский ГАУ, 2022.С. 115-119.

УДК 94(47).084.9

НЕКОТОРЫЕ ВОПРОСЫ БОРЬБЫ С ПРОЯВЛЕНЯМИ ЭКСТРЕМИЗМА В РОССИИ: ИСТОРИЧЕСКИЙ АСПЕКТ

Волков Александр Павлович,
доктор исторических наук, профессор, Заслуженный работник высшей школы РФ
Национальный исследовательский университет «Московский институт электронной техники»,
г. Москва, Россия
e-mail: ooovak09@mail.ru

Аннотация**:** *в статье рассмотрены проблемы борьбы с проявлениями экстремистских настроений в истории России на примере 60-80-х гг. двадцатого века. Отмечается важность учета конкретно-исторической обстановки, существовавшего в стране политического строя и руководящей роли КПСС. Подчеркивается, что это явление не является новым. История России полна подобных примеров. При анализе следует понимать исторические корни его происхождения. Автор констатирует, что существенными проблемами, о которых старались не говорить в обозначенный период открыто, было нарастание религиозного влияния и националистических настроений на сознание населения СССР и в первую очередь молодежь. Что считалось антисоветской в данные годы, а значит и антигосударственной деятельностью. Без истории проблемы экстремизма невозможно оценить его масштабность, и борьба с ним будет малоэффективной.*

Ключевые слова: *экстремизм, экстремистская деятельность, терроризм, национализм, религия, молодежь, история, идеологическая работа, патриотизм, веротерпимость.*

SOME ISSUES OF COMBATING EXTREMISM IN RUSSIA: HISTORICAL ASPECT

Volkov Alexander Pavlovich,
doctor of historical sciences, professor, Honored worker of the higher School of the Russian Federation
National research university of electronic technology (MIET),
Moscow, Russia
e-mail: ooovak09@mail.ru

Abstract: *the article deals with the problems of combating manifestations of extremist sentiments in the history of Russia on the example of the 60-80s of the twentieth century. The importance of taking into account the concrete historical situation, the political system that existed in the country and the leadership role of the CPSU is noted. It is emphasized that this phenomenon is not new. The history of*

Russia is full of similar examples. The analysis should understand the historical roots of its origin. The author states that the significant problems that they tried not to talk about openly during the designated period were the increase in religious influence and nationalist sentiments on the consciousness of the population of the USSR and, first of all, the youth. What was considered anti-Soviet in these years, and therefore anti-state activity. Without a history of the problem of extremism, it is impossible to assess its scale and the fight against it will be ineffective.

Keywords: *extremism, extremist activity, terrorism, nationalism, religion, youth, history, ideological work, patriotism, religious tolerance.*

Реалии сегодняшнего дня постоянно напоминают нам о таком явлении как экстремизм.

Согласно Федерального закона Российской Федерации от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» экстремистская деятельность (экстремизм):

- «насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности Российской Федерации (в том числе отчуждение части территории Российской Федерации), за исключением делимитации, демаркации, редемаркации Государственной границы Российской Федерации с сопредельными государствами;
- публичное оправдание терроризма и иная террористическая деятельность;
- возбуждение социальной, расовой, национальной или религиозной розни;
- пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;
- нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;
- воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;
- воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;
- совершение преступлений по мотивам, указанным в пункте «е» части первой статьи 63 Уголовного кодекса Российской Федерации;
- использование нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, за исключением случаев использования нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики

экстремистских организаций, при которых формируется негативное отношение к идеологии нацизма и экстремизма и отсутствуют признаки пропаганды или оправдания нацистской и экстремистской идеологии;

- публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;

- публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением;

- организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;

- финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг» [1].

То есть, экстремизм – приверженность к крайним взглядам и действиям [2]. По мнению большинства ученых - экстремизм порождают социально-экономические кризисы, деформации политических институтов, резкое падение жизненного уровня, ухудшение социальных перспектив значительной части населения, доминирование в обществе чувств, настроений хандры, социальной и личной нереализованности, неполноты бытия, страх перед будущим, подавление властями оппозиции, инакомыслия, блокирование легитимной самодеятельности индивида, национальный гнет, амбиции лидеров, политических партий, ориентации лидеров политического процесса на экстремальные средства политической деятельности [2].

Сегодня социальную базу экстремизма составляют прежде всего маргинальные слои, представители экстремистских националистических и религиозных движений.

Является ли это явление новым? Конечно нет. При анализе следует понимать исторические корни его происхождения.

Без этого невозможно оценить масштабность проблемы и борьба с ним будет малоэффективной. Примером может служить и недавнее советское прошлое 60-х-80-х гг. XX века, когда идеологическое воздействие было жестким и конкретным, когда государственная машина действовала основательно и казалось уверенно и правильно. Но, отсутствие гибкости и учета исторического опыта прошлого и особенностей ментальности различных слоев населения приводило к обратной реакции.

Существенной проблемой, о которой старались не говорить в открыто, было нарастание религиозного влияния на сознание населения СССР и в первую очередь молодежь. Что считалось антисоветской, а значит и антигосударственной деятельностью. Думается, что здесь руководство СССР проявляло недостаточно гибкости и такта. В итоге шел постепенный процесс

объединения религиозного экстремизма в ряде регионов СССР с националистическими настроениями.

Конечно, можно констатировать, что высшие эшелоны власти отчетливо понимали какую «мину» замедленного действия закладывали под официальную атеистическую» воинственно настроенную против религии идеологию неконтролируемые действия церкви.

В этой связи программа КПСС 1961 г. требовала систематически вести широкую научно-атеистическую пропаганду» терпеливо разъяснять несостоятельность религиозных верований возникших в прошлом, на почве придавленности людей стихийными силами природы и социальным гнетом из-за незнания истинных причин природных и общественных явлений. В специальном постановлений ЦК КПСС «Об усилении атеистического воспитания населения» от 13 июля 1971 г. отмечалось, что «не преодолено ошибочное мнение о стихийном отмирании религии в процессе коммунистического строительства», а в качестве ошибки партийных органов признавалась их неверная позиция» не учитывающая «стремление религиозных центров приспособиться к сегодняшней обстановке». Особую тревогу государственных структур вызывала деятельность различных запрещенных сект, создание подпольных кружков и «лагерей» отдыха, где шло обучение нелегальной религиозной работе. [3]

Большую активность здесь проявляла прежде всего католическая и униатская церковь в Западной Украине.

В итоге, несмотря на принимавшиеся меры при отсутствии специальных знаний, подготовленных кадров и понимания конкретно-исторической обстановки религиозность молодежи в рассматриваемые годы увеличивалась и именно этот фактор стал одним из определяющих в развале СССР.

Непроизвольную, но объективно запрограммированную помощь распространению религиозности населения и в том числе молодежи оказывало религиозным конфессиям само государство, которое широко использовало не только меры убеждения, но и принуждения, вызывая законный интерес ко всякому запретному.

Например, в том же постановлении от 13 июля 1971 г. прямо говорилось, что «любая религиям это чуждая марксистско-ленинскому мировоззрению идеология. На фоне научно-технического и социального прогресса в СССР, побед в коммунистическом строительстве религиозные пережитки особенно нетерпимы. Они все больше противоречат советскому образу жизни, мешают духовному росту советских людей» [3].

Из государственных решений, говорящих об отрицательном отношении к религии, можно привести Постановление ЦК КПСС, Совмина СССР от 10.06.1986 г. № 699 «О подготовке молодежи допризывного и призывного возрастов к действительной военной службе в Вооруженных Силах СССР» подписанного М.С. Горбачевым и Н.И. Рыжковым. В ответ на рост негативных тенденций в подготовке молодежи к защите Отечества требовалось «усилить борьбу с пацифистскими, религиозными и иными негативными настроениями, вызывающими уклонение отдельных призывников от службы в Вооруженных

Силах СССР. В предупреждении антипатриотических проявлений полнее использовать меры воспитательного, административно-правового характера, возможности общественности» [4].

Результатом такого бездумного подхода стало резкое усиление сопротивления надругательствам над религией: в конце 70-х гг., например, значительно усилилась религиозная обрядность. Если в 1974 г. зарегистрировано 78834 венчания в церкви, то в 1979 г. - 99270; число крещений в 1979 г. составило 87822 (17,87% от числа родившихся) плюс к этому было окрещено 33762 школьника (1977 г. -25980) и 27762 взрослых (1977 г. – 20043) [5, с.13].

В итоге утвердительный ответ на вопрос "Являетесь ли Вы верующим?" в 1990 г, уже дало следующее количество молодых людей призывного возраста: Закарпатская область Украину - 39,8%; Грузии - 62%,Узбекистан - 49,6%; Таджикистан - 69,8%; г. Москва и область - 26,9%; г. Ленинград и область — 18,3% [5, с.12].

Нарастание религиозного воздействия на население тесно переплеталось с усилением националистических проявлений, носивших с порой яркий экстремистский характер.

Чрезвычайным происшествием для властей стало покушение гражданина Михбаева 14 июля 1960 г. на саркофаг В.И.Ленина, в результате чего он был разбит, а тело основателя Советского Союза оказалось поврежденным множеством осколков [5, с.18]. *(После этого террористического акта саркофаг В.И. Ленина сделали более «антивандальным»- авт.).*

Изучение различных источников показывает» что центрами таких проявлений являлись Прибалтика, Закавказье, Северный Кавказ, Западная Украина. Активным участником этого процесса была молодежь, закалившаяся в борьбе с советской властью и уже окрепшая и возмужавшая ставшая во главе борьбы за развал СССР в 80-гг.

Наиболее сильные националистические настроения среди молодых людей отмечались в Прибалтике. Именно здесь в силу исторического прошлого региона национализм наиболее переплетался с экстремизмом, который тогда называли «антисоветизмом».

Несмотря на усилия местных органов власти, подпитываемые Западом националисты чувствовали себя здесь вполне уверенно, проводя регулярные антирусские и антисоветские акции.

Так в докладе «О серьезных недостатках в идеологической и контрпропагандистской работе в пограничных районах страны» работавшей в Прибалтийских республиках комиссии ЦК ВЛКСМ в январе 1963 г. отмечалось, что «за последнее время в ряде союзных республик активизируют свою деятельность националистические элементы» которые пытаются оказать влияние на молодежь. В Литве в 1981 г. группа учащихся и студентов в Вильнюсе изготовила свыше 900 антисоветских листовок, на своих собраниях они выступали с лозунгами «Свободной Литвы». Во время событий в районе Карибского моря в Капсукском районе Литвы, группа националистов устроила погром на кладбище советских солдат. Всего же в Прибалтийских республиках

в I960-1962 гг. пресечена деятельность более 40 антисоветских групп» в которых принимала участие молодежь [5, с.9].

Существовавшая в 1965 г. антисоветская молодежная организация в Таллине выпускала газету, где выражалось недовольство «русификацией Эстонии» советской властью. Путь «освобождения» - вооруженная борьба, считали ее члены.

В последующем обстановка здесь только обострялась. Эстонские студенты открыто говорили, что «слишком много понаехало в Эстонию «искателей счастья», «здесь много русских нехороших, это - отбросы русского народа» и т.д. Фиксировались и постоянные драки коллективного характера подростков эстонской и русской национальности, распространение антирусских материалов в молодежных газетах и изготовление аналогичных листовок. Все это фиксировалось соответствующими государственными структурами, но этого оказалось мало [5, с.9; 6].

Активно участвовало в националистических выступлениях в рассматриваемые годы молодое поколение Северо-Кавказского в Закавказского регионов СССР. Постоянно тлел конфликт между Арменией и Азербайджаном по поводу Нагорного Карабаха, вылившийся в кровавые столкновения и войну во второй половине 80-х гг.

В 1967 г. в Нагорном Карабахе прошли массовые беспорядки в связи с убийством армянского мальчика азербайджанцем. Через десять лет произошел террористический акт в Московском метрополитене, исполнителями которого были молодые люди армянской национальности из «Национальной объединенной партии». Свои действия они объяснили целью «отомстить русским за их угнетение армянского народа» [9, с.128].

Постоянная напряженность в национальных отношениях присутствовала в районе Северной Осетии и Чечено-Ингушетии, Западной Украине, где были очень сильны связи с украинской диаспорой за границей; в Молдове где постоянно тлели мысля о «притеснении» молдован, о насильственном присоединения к СССР. Попытки настроить население против «неверных» отмечались в республиках Средней Азии и Казахстане [7; 4, с.10].

На фоне справедливых требований репрессированных народов за их возвращение на историческою родину, особо выделились крымские татары, о чем открыто было заявлено только во второй половине 80-х гг.

В 60-х гг. на территории только Узбекистана проживало более 160 тыс. крымских татар. В центральные органы власти постоянно поступали обращения крымско-татарской молодежи с просьбой помочь вернуться в Крым. Только в I964-I965 гг. зарегистрировано около 60 тыс. подобных писем. Ранее в 1962 г. была организована нелегальная молодежная организация крымских татар во глазе с А. Умаровым. К сожалению, сегодня несмотря на все принятые и претворяемые в жизнь руководством России меры, Запад продолжает разыгрывать «крымско-татарскую» карту с помощью лидеров запрещенного в России меджлиса, призывающего в открытую к террористическим актам на территории Крыма [8; 4, с.10-11].

Опыт прошлого учит, что националистические проявления, направленные против русского населения, вызывали у него аналогичную реакцию. по данным социологических исследований, проведенных среди интеллигенции (до 30 лет) в Белгороде, Гороно-Алтайской автономной области, Петропавловске-Казахском в середине 80-х гг, положительно народы Средней Азии оценивали 44% опрошенных (отрицательно- 56%), народы Кавказа - 56% положительно и 44% отрицательно [9, с.133].

Такие настроения приводили к межнациональным конфликтам, таким как драка в г. Рыбинске 19.01.82 г. между учащимися-таджиками ТУ №3 и местной молодежью или драка местных молодых людей с «бойцами» стройотряда из Азербайджана в г. Вольске 30.05.87 г. Аналогичные случаи произошли в Комсомольске-на-Амуре 31.05.87 г., когда бал брошен лозунг «Бей казахов», и в 1986г. в Якутске, где выясняли отношения якутская и русская молодежь [9, с.133-134].

В целом, можно констатировать, что мощным средством противодействия распространению экстремизма сегодня является активная пропаганда духовно-нравственных ценностей истории и традиций народов России: их патриотизма, веротерпимости, присущего им обостренного чувства ответственности за судьбу будущих поколений, векового опыта преодоления жизненных трудностей совместными усилиями.

Требуется комплексный подход к осуществлению противодействия экстремизму и терроризму в любых их проявлениях, который включал бы в себя меры регулирующего, запретительного и профилактического характера. Как показывает анализ международного и национального опыта по противодействию экстремизму и терроризму, наиболее эффективными в этой области мерами являются совершенствование правовой базы, укрепление и совершенствование деятельности спецслужб, усиление борьбы с финансированием экстремизма и терроризма, а также активизация разъяснительной и пропагандистско-идеологической работы.

Наиболее эффективными путями борьбы с идеологией и практикой экстремизма и терроризма [10] являются:

- органы государственной власти РФ должны расширить взаимодействие государственных органов и религиозных объединений по всем направлениям сотрудничества, в первую очередь в активизации борьбы с проявлениями религиозно-политического экстремизма и терроризма, борьбе с преступностью, в духовно-нравственном оздоровлении общества;

- муниципальные органы власти должны уделять особое внимание воспитанию населения в духе национальной и религиозной терпимости, непринятия идеологии религиозно-политического экстремизма и терроризма;

- главный упор в стратегии противодействия экстремизму и терроризму следует делать на улучшении социально-экономической ситуации в стране, так как это способствует урегулированию социально-политических конфликтов и существенно сужает социальную базу экстремистов и террористов;

- одновременно следует принимать решительные меры по перекрытию каналов финансирования экстремистов и террористов из-за рубежа и из местных источников;

- в плане блокирования терроризма, как уголовного проявления, следует совершенствовать правовую базу, укреплять и совершенствовать деятельность специальных служб, а также активизировать идеологическую работу;

- продолжать предпринять энергичные меры, препятствующие распространению различных экстремистских течений вне Российской Федерации, питающих сепаратизм, терроризм, внутри нашей страны и т.д.

Противодействие экстремизму и терроризму становится одной из главных проблем сегодняшнего дня не только России, но и всего мирового сообщества, требует объединения усилий в принятии решительных, эффективных мер и согласованных действий, направленных на предупреждение и пресечение проявлений любых их форм.

Список литературы

1. URL: base.garant.ru›12127578/ (доступ 16.02.2023).

2. URL: ru.wikipedia.org›Экстремизм (доступ 16.02.2023).

3. Галдобина, С.В. Советская молодежь в 60-е гг. XX столетия: малоизвестные страницы истории / С.В.Галдобина // Вестник Екатерининского института. № 1. 2008. С. 37-41.

4. Постановление ЦК КПСС, Совмина СССР от 10.06.1986 г. № 699 «О подготовке молодежи допризывного и призывного возрастов к действительной военной службе в Вооруженных Силах СССР» // URL: consultant.ru›cons/cgi/online.cgi.

4. Волков, А.П. Молодежь и советское государство в 60-80- е гг. XX столетия: некоторые проблемы эффективности воспитания и взаимоотношений / А.П. Волков и др. // Вестник Екатерининского института. № 4. 2016. С.7-15. (Интересные архивные материалы по данной проблеме хранятся в Российском государственном архиве социально-политической истории, в фондах бывшего центра хранения документов молодежных организаций)// РГАСПИ, ф.1. с.3, д.61, л.2.

5. Волков, А.П. Хрущевская «оттепель»: некоторые страницы истории / А.П. Волков // Вестник Екатерининского института. 2016. № 2. С.15-21.

6. РГАСПИ, ф.1. оп.1, д.388, л.1-2.

7. РГАСПИ, ф.1. оп.1, д.808, л.128; д.862, л.152-153.

8. РГАСПИ, ф.1. оп.1, д.398, л.7-11.

9. Галдобина, С.В. Военно-патриотическое воспитание населения СССР в 1946-1991 гг.: Историографическое исследование: дис. … докт. ист.наук / С.В. Галдобина. Санкт-Петербург, 2008. 506 с.

10. Терроризм (от лат. terror - страх, ужас) — это идеология насилия и практика воздействия на принятие решения организациями международного сообщества, государственными органами, органами местного самоуправления, осуществляемые через устрашение населения и (или) через другие формы противоправных насильственных действий // URL: pravo. team›Преступления против государственной безопасности (доступ 16.02.2023).

УДК 343.98

РАЗВИТИЕ ЯЗЫКА КРИМИНАЛИСТИКИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Волчецкая Татьяна Станиславовна,
доктор юридических наук, профессор,
Балтийский федеральный университет имени И.Канта,
г. Калининград, Россия
e-mail: TVolchetskaya@kantiana.ru

Аннотация*: в статье раскрыто влияние процесса цифровизации на содержание основных разделов криминалистики: криминалистической методологии, техники, тактики и криминалистической методики. Доказана необходимость совершенствования языка криминалистикой науки, обоснования целесообразности введения новых терминов, связанных с цифровыми технологиями в криминалистике, и создания соответствующего тезауруса.*

Ключевые слова: *цифровая криминалистика, цифровые технологии в расследовании преступлений, язык криминалистики.*

DEVELOPMENT OF THE LANGUAGE OF CRIMINALISTICS IN CONDITIONS OF DIGITALIZATION

Volchetskaya Tatyana Stanislavovna,
doctor of law, professor,
Immanuel Kant Baltic federal university,
Kaliningrad, Russia
e-mail: TVolchetskaya@kantiana.ru

Abstract: *the article reveals the influence of the digitalization process on the content of the main sections of criminalistics: criminalistics methodology, technology, tactics and private criminalistics methods. The necessity of improving the language of criminalistics, substantiating the need to introduce new terms related to digital technologies in criminalistics and creating an appropriate thesaurus is shown.*

Keywords: *digital forensics, digital technologies in crime investigation, language of forensics.*

В последнее десятилетие с учетом ряда социально-экономических и политических событий мир существенно изменился, и к сегодняшнему дню цифровизация практически полностью охватила практически все сферы: социальную жизнь людей, экономику, политику, здравоохранение, и, конечно же, право.

На страницах юридической печати ведутся научные споры по философским аспектам внедрения и использования высоких технологий в правоприменительную деятельность, по историческим, социальным и

междисциплинарным вопросам информатизации права. В юридической науке активно дискутируются проблемы, связанные с цифровыми технологиями и искусственным интеллектом в различных отраслях материального и процессуального права, с вопросами использования современных технологий в административном, уголовном, гражданском и арбитражном судопроизводстве[1].

Пожалуй, в наибольшей мере эти вопросы коснулись наук уголовно-правового цикла, и в частности – криминалистики, фундаментальные основы цифровизации которой, заложены в трудах В.А. Мещерякова, А.Л. Осипенко, А.Б. Вехова, Е.Р. Россинской, Л.В. Бертовского и ряда других ученых.

Причем, это оказало свое влияние, как на процесс расследования преступлений, так и на саму преступную деятельность, которая также окунулась в виртуальный мир. Преступники нередко используют цифровую среду как средство или орудие, а иногда и место совершения преступления. Например, это касается сбыта наркотических средств дистанционным методом, разнообразных новых способов совершения мошеннических действий и целого ряда других преступлений. В других криминальных ситуациях преступники оказывает воздействие на информацию в информационно-телекоммуникационных системах, либо представленную на электронных носителях. Также в преступной деятельности нередко используются цифровые технологии для фальсификации доказательственной информации. И, наконец, деятельность преступников бывает также направлена и на функционирование информационных систем, например, на критическую информационную структуру государства.

Однако в большей степени учеными криминалистами изучаются проблемы использования цифровых технологий в процессе реализации уголовно-процессуальной деятельности, которые уже давно нашли свое практическое применение на различных стадиях уголовного судопроизводства для решения различных задач.

С позиций системного и ситуационного подходов мы проанализировали основные направления использования высоких технологий в различных разделах криминалистической науки. В значительной мере это коснулось криминалистической техники. В следственной практике уже давно используются цифровые фотоаппараты и видеокамеры для фиксации следовой картины преступлений, а также результатов следственных действий. На этой же основе были в свое время разработаны и многочисленные компьютерные системы поддержки принятия следственных решений. Большая часть специальных приборов, устройств, аппаратно-программных криминалистических комплексов работает на основе специализированного программного обеспечения и цифрового принципа представления информации в целях обнаружения, фиксации, изъятия и проверки криминалистически значимой информации. Это связано с тем, что цифровые технологии обладают весьма существенными характеристиками работы с информацией: длительным сроком ее хранения, высокой скоростью передачи, возможностью сжатия объема данных и сохранения их на небольших по физическому объему

накопителях, возможностью восстановления данных в случае изменения или удаления.

Появились интересные предложения, к примеру, по созданию цифрового двойника места происшествия. Различные цифровые технологии используются органами, осуществляющими оперативно-розыскную деятельность, достаточно апробирован сервис «Правосудие онлайн», искусственный интеллект и нейросети активно исследуется учеными с целью его внедрения в правоохранительную деятельность [2].

Одним из активно развивающихся способов реализации использования цифровых следов в расследовании преступлений является криминалистический профайлинг [3], на этом же основана и методика построения криминалистической модели личности неизвестного преступника [4].

Именно цифровые позволили по другому взглянуть и на криминалистическую тактику, выявив в ней большой потенциал для дальнейших научных исследований. В этом плане можно привести пример получения ценной доказательственной и тактически значимой информации путем анализа аккаунтов социальных сетей [5]. Так, информация из геотегов фотографий может оказать помощь в установлении местонахождения подозреваемого, а соотнесение времени и места изготовления фотографий позволит следователю определить маршруты перемещений преступника, в то время как статус лица в социальной сети может помочь установить его эмоциональное состояние в конкретный момент времени.

Еще одним перспективным направлением криминалистической тактики является научное исследование тактических и организационных особенностей проведения следственных и судебных действий с использованием видеоконференцсвязи, разработка тактических приемов их фиксации.

И, разумеется, частные криминалистические методики, синтезирующие в себе все достижения современной криминалистики, также постепенно оптимизируются по ряду направлений. На протяжении многих лет учеными были разработаны различные вопросы методики расследования преступлений в сфере компьютерной информации, а сегодня на повестку дня некоторые учеными ставят проблему разработки частной криминалистической методики расследования высокотехнологичных преступлений [6]. Несомненный интерес представляют различные мультимедийные межотраслевые средства предупреждения преступности, также изготовленные с применением современных информационных и интернет-технологий [7].

В связи с этим, пожалуй, наибольшая фундаментальная научная задача возникла перед криминалистической методологией как разделом криминалистической науки, в рамках которой необходимо выявить, а затем и решить многие проблемные вопросы нового учения в криминалистической науке , связанного с ее цифровизацией. В их числе следует выделить такие, как: вопрос о едином названии этого учения и его структуре, об особенностях криминалистического мышления, на основе которого разрабатываются соответствующие нейросети и.т.д.

Но в первую очередь здесь необходимо решить вопрос об однообразном понимании уже используемых и вновь появившихся терминов, связанных с цифровыми технологиями в юриспруденции, в частности, в криминалистической науке. Поскольку в монографиях, статьях, в иной научной продукции все термины, которые связаны с цифровизацией, далеко не всегда трактуются однозначно.

Криминалистика, как и любая другая наука, имеет свой устоявшийся терминологический аппарат. Основы научного исследования языка криминалистики, его понятие, система, тенденции развития были заложены Р.С. Белкиным [8]. Именно он обратил внимание на то, что язык науки - это всегда система динамичная, в силу влияния на нее целого ряда различных факторов, что мы, собственно, наблюдаем и сегодня. В связи с цифровизацией круг используемых в криминалистике понятий значительно расширяется параллельно с ростом и качественным расширением криминалистических знаний. Пришло время изменения целого ряда определений, равно как и замены одних определений другими, уточнения употребляемых понятий. В связи с этим и необходима унификация криминалистической терминологии с целью сокращения числа терминов, обозначающих один и тот же объект.

И в первую очередь, это касается самого криминалистического учения, связанного с цифровизацией. Проблема развития научных знаний об использовании цифровых технологий в криминалистике является весьма важной, поэтому многие авторы и делают попытки приведения всех накопленных криминалистической наукой знаний в одну единую систему. Если обратиться к истории, то мы увидим, что среди первых предложений о наименовании этого учения были такие как: «ЭВМ в криминалистике», предложенная в свое время Н.С. Полевым «Правовая информатика и кибернетика», [9], затем появились «Компьютерная криминалистика», «Электронная цифровая криминалистика» [10], «Основы теории электронных доказательств» [11], «Теория информационно-компьютерного обеспечения криминалистической деятельности». [12]. Некоторые авторы под влиянием западных ученых высказали предложения о создании «Форензики», а также «Судебной дигитологии» [13; 14; 15].

Аргументации создания вышеуказанных теорий были разные, что не могло не отразиться и на их структуре и содержании. Например, В.Б. Вехов в своей частной криминалистической теории «электронная криминалистика», объединил учение о компьютерной информации и исследование компьютерных устройств и информационно-телекоммуникационных сетей; включая сюда также и также криминалистическое использование компьютерной информации, средств ее обработки и защиты [16].

Е.Р. Россинская и А.И. Семикаленова, в свою очередь, выделили концептуальные основы теории вместе с тем включили в нее ряд относительно самостоятельных учений: о способах совершения компьютерных преступлений; о цифровых следах; о криминалистическом исследовании компьютерных средств и систем; об информационно-компьютерном

криминалистическом обеспечении тактики следственных и судебных действий и ряд других [12].

Однако настало время определиться с единым общепринятым наименованием этого актуального криминалистического учения, что необходимо как в научных, так и в образовательных целях. При его выработке следует учитывать то, что речь идет о цифровизации всей криминалистической науки и изучаемых ею объектов, поскольку применение цифровых технологий, как в криминальной, так и в криминалистической деятельности, влечет за собой развитие всей криминалистической науки, затрагивая практически все ее основные разделы: криминалистическую методологию, технику, тактику и методику. В силу этого, нам представляется оптимальным предложенное в монографии, под редакцией Е.Р. Россинской название «Теория информационно-компьютерного обеспечения криминалистической деятельности» [17]. Развитие этой теории, по сути, только начинается. И одним из направлений ее развития нам видится оптимизация и унификация языка криминалистики, для чего для начала необходимо создать тезаурус, в составе которого следует единообразно и однозначно определить такие понятия, как: цифровые, виртуальные и электронные следы; электронные доказательства и цифровые доказательства; электронная, компьютерная и цифровая информация; компьютерные преступления и преступления в сфере информационных технологий, нейросети, искусственный интеллект и роботехника в криминалистике и ряд других.

Список литературы

1. Волчецкая, Т.С. Современная криминалистическая наука: реалии и перспективы развития / Т.С. Волчецкая // Казанские уголовно-процессуальные и криминалистические чтения. Материалы Международной научно-практической конференции. В 2-х частях. Редколлегия: Ю.Н. Кулешов (отв. ред.) [и др.]. Казань, 2022. С.17-22.

2. Баширов, А.В. Компьютерное моделирование на основе нейросети как инструмент получения криминологически значимой информации по оценке состояния преступности (на материалах республики Казахстан) / А.В. Баширов, Т.С. Волчецкая, Б.М. Нургалиев, Т.А. Ханов // Вестник Томского государственного университета. Право. 2022. № 46. С. 5-25.

3. Волчецкая, Т.С. Криминалистический профайлинг в россии и за рубежом / Т.С. Волчецкая, А.А. Абрамовский // Известия Тульского государственного университета. Экономические и юридические науки. 2018. № 4-2. С. 3-9.

4. Малыхина, Н.И. Актуальные проблемы установления лица, совершившего преступление, в криминалистике / Н.И. Малыхина // Современные проблемы криминалистики и судебной экспертизы. Материалы VIII Всероссийской научно-практической конференции. Саратов, 2020. С. 62-64.

5. Болвачев, М.А. Социальная сеть как объект криминалистического исследования / М.А. Болвачев // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 4. С. 64-71.
6. Поляков В.В. Источники и принципы формирования частной методики расследования высокотехнологичных преступлений / В.В. Поляков // Lex Russica. 2022.Т.6.С. 85-96.
7. Гармаев, Ю.П. Мультимедийные межотраслевые средства предупреждения преступности: перспективы разработки и внедрения / Ю.П. Гармаев // Всероссийский криминологический журнал. 2014. № 3. С. 71-80.
8. Белкин, Р.С. Курс криминалистики: Криминалистические средства, приемы и рекомендации / Р.С. Белкин. В 3-х томах. Т. 1. М., 1977. 340 с.
9. Полевой, Н.С. Правовая информатика и кибернетика / Н.С. Полевой. М., 1993.
10. Смушкин, А.Б. К вопросу о наименовании теории «Электронная цифровая криминалистика» / А.Б. Смушкин // Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2019. № 1 (13).С. 15–21.
11. Основы теории электронных доказательств / Под ред. С.В. Зуева. М. Юрлитинформ, 2019.
12. Россинская, Е.Р. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности / Е.Р. Россинская, А.И. Семикаленова // Вестник Санкт-Петербургского университета. Право. 2020. Т. 11. № 3. С.745-759.
13. Федотов, Н.Н. Форензика - компьютерная криминалистика / Н.Н. Федотов. М., 2007.
14. John Sammons. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics (2nd Edition), Syngress, 2015.
15. Joakim Kävrestad J. Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications (2nd Edition), Springer, 2020.
16. Вехов, В.Б. Электронная криминалистика в XXI веке: тенденции развития / В.Б. Вехов // Криминалистика – наука без границ: традиции и новации: матер. ежегод. всерос. научн.-практич. конф. / сост. О.С. Лейнова. СПб.: Санкт-Петербургский университет МВД РФ, 2019. С. 51-54.
17. Теория информационно-компьютерного обеспечения криминалистической деятельности. Монография / под ред Е.Р. Россинской. М.: Проспект, 2022.

УДК 363.1

ПОНЯТИЕ ДОКАЗАТЕЛЬСТВА И ИСПОЛЬЗОВАНИЕ «ЦИФРОВОЙ» ИНФОРМАЦИИ В ДОКАЗЫВАНИИ ПО УГОЛОВНОМУ ДЕЛУ

Воскобитова Лидия Алексеевна,
доктор юрид. наук, профессор, заведующий кафедрой
уголовно-процессуального права
Московский государственный юридический университет
имени О.Е. Кутафина (МГЮА),
г. Москва, Россия
e-mail: lavosk@mail.ru

Аннотация: *в статье ставится вопрос об особенностях познавательной деятельности в уголовном судопроизводстве с использованием цифровых технологий; выявлены различия использования цифровой информации при расследовании традиционных преступлений и преступлений в сфере компьютерной информации, когда вся информация о преступной деятельности существует только в цифровой форме, что создает существенные трудности в доказывании.*

Ключевые слова: *уголовное судопроизводство, доказательства, познание, цифровая информация, цифровые технологии, цифровые доказательства.*

THE CONCEPT OF EVIDENCE AND THE USE OF "DIGITAL" INFORMATION IN EVIDENCE IN A CRIMINAL CASE

Voskobitova Lidiya Alekseevna,
doctor of law, professor, head of the department
criminal procedure law
Kutafin Moscow state law university (MSAL),
Moscow, Russia
e-mail: lavosk@mail.ru

Abstract: *the article raises the question of the peculiarities of cognitive activity in criminal proceedings using digital technologies; the differences in the use of digital information in the investigation of traditional crimes and crimes in the field of computer information are revealed, when all information about criminal activity exists only in digital form, which creates significant difficulties in proving.*

Keywords: *criminal proceedings, evidence, cognition, digital information, digital technologies, digital evidence/*

Современное представление о доказательстве в уголовном процессе формировалось постепенно от интуитивного понимания необходимости чем-то подтвердить заявления спорящих, чтобы суд мог понять, что же произошло и кто прав, а кто виноват в частно-исковом процессе, до современных

размышлений о трансформации доказывания при использовании цифровых технологий и современной дискуссии по вопросу, а не появился ли новый вид доказательств – «цифровые доказательства». Между тем, понимание доказательства в уголовном судопроизводстве обусловлено не столько теоретическими определениями, сколько самой природой процессуального познания, базирующегося на великом принципе презумпции невиновности: если не доказана вина, значит не может быть признан виновным. Чтобы «*доказать вину»,* как известно, требуется сложная и многоуровневая познавательная деятельность, которая в своем правовом регулировании сориентирована на *специфический предмет доказывания* и *особые процессуальные средства познания.*

К сожалению, процессуальное законодательство, определяя *предмет доказывания*, заложило в ст.73 УПК РФ скорее план описания познавательного результата. Между тем, явно недооцениваемая практикой ст. 8 УК РФ категорично предписывает, что *основанием уголовной ответственности является совершение деяния, содержащего все признаки состава преступления.* Следовательно, *предмет познания* в уголовном судопроизводстве должен включать: а) сначала установление самого факта совершения деяния; б) затем выяснение всех юридически значимых фактических обстоятельств этого деяния; в) только после этого определение признаков конкретного состава преступления и фактического проявления каждого из них в данном конкретном деле; в) установление, кто именно совершил это деяние, является ли он субъектом преступления и какова форма и степень его вины.

В реальности такой предмет доказывания никогда не дается познающему субъекту в готовом, наглядном, сохраненном виде. Познание в уголовном судопроизводстве всегда *ретроспективно*, поскольку на момент познавательной деятельности само событие уже в прошлом, а познающий субъект не мог его наблюдать непосредственно в силу ст.61 УПК РФ. Это познание всегда *фрагментарно,* поскольку на момент познания события уже нет и могут сохраниться лишь его отдельные фрагменты: повреждения, разрушения, следы, впечатления очевидцев и т.п. Кроме того, познающий субъект самостоятельно и субъективно отбирает для познания лишь те *фрагменты реальности*, которые он оценивает, как имеющие юридическое значение для данного дела. Процессуальное познание всегда *опосредовано,* поскольку осуществляется посредством выявления, анализа, оценки оставленных в физическом мире или в сознании отдельных лиц *следов/отражений* данного события.

Процессуальное познание, по сути своей, это *реконструкция образа реального события на основе фрагментов информации, полученных в результате процессуального доказывания.* Поэтому для процессуального познания необходимо накопление информации, которая, с позиций математического подхода становится «*мерой снятой неопределенности*»: «*…чем больше получают информации о системе, тем больше ее состояние становится определенным, предсказуемым*» [1]. Поэтому к познанию в

современном состязательном уголовном судопроизводстве предъявляется ряд процессуальных требований: а) *полного и объективного* выявления таких следов-отражений, как подтверждающих обвинение, так и опровергающих его или ставящих под сомнение отдельные познавательные выводы; б) *правильной оценки* юридического значения каждого из следов в перспективе не только процессуального познания события в целом, но и правильного решения правоприменительных задач производства по уголовному делу; в) точной и непредвзятой *процессуальной фиксации/оформления*, которые могут гарантировать отбор всей юридически значимой информации и правильность ее фиксации; сохранение в неизменном виде на протяжении всего производства по делу; обеспечение возможности ее оспаривания, опровержения заинтересованными субъектами процесса.

Именно эти объективные особенности и сложности процессуального познания и должны формировать представление о возможных средствах познания. Определяющим в современной процессуальной науке стало представление о *доказательствах как следах/отражениях*, оставленных событием в физическом мире или в сознании лиц, оказавшихся очевидцами или участниками данного события. Такое представление обусловлено способностью человека к «аналоговому мышлению», когда каждый след способен порождать в сознании познающего *образ* того или иного фрагмента реального события [2, С. 25-26]. Из совокупности образов воспринятых фрагментов реальности постепенно формируется *образ всего события* в целом. Например, если на шоссе мы видим длинный след торможения автомобиля, осколки стекла на дорожном полотне, сломанный бордюр и т.п., мы сразу «рисуем» в своем сознании возможные образы/варианты дорожного происшествия, которое могло здесь произойти. Поэтому в уголовном судопроизводстве *доказательство всегда имеет информационную природу*: *это фрагменты информации, относящейся к исследуемому событию, на основании которой субъект, ведущий процесс, может решать познавательные и правоприменительные задачи по конкретному уголовному делу.*

Для правильного установления *предмета познания* в его полном объеме, обеспечивающем установление *фактической основы дела,* необходимо получить совокупность таких фрагментов информации, чтобы в итоге можно было бы сформировать непротиворечивый и юридически полный образ события преступления. Этим обусловлены такие процессуальные требования как допустимость и относимость каждого из доказательств, их достаточность, их достоверность. Сохраняют свое значение и требования, которые в ст. 20 УПК РСФСР четко определялись как всесторонность, полнота и объективность установления фактических обстоятельств дела. УПК РФ необоснованно отказался от такого принципиального требования, однако эти требования фактически вытекают из смысла или прямо указаны в ряде статей, регулирующих отдельные вопросы производства по делу. Например, ст. 14 УПК РФ предписывает стороне обвинения выполнение бремени доказывания не только обвинения, но и опровержения доводов, которые приводятся в защиту обвиняемого, а если такие доводы не могут быть опровергнуты

обвинением, то неустранимые сомнения толкуются в пользу обвиняемого. Глава 9 УПК РФ, регулирующая отводы, по сути, призвана обеспечивать объективность и непредвзятость всех властных субъектов, ведущих процесс. Пункты 5-7 ч.1 ст. 73 УПК РФ включают в предмет доказывания и предписывают устанавливать обстоятельства, явно нацеленные на обеспечение всесторонности и объективности доказывания. В ч.2 ст. 154 УПК РФ законодатель прямо предписывает, что выделение уголовного дела допускается только при условии, что «*это не отразится на всесторонности и объективности предварительного расследования и разрешения дела*». Системный анализ положений УПК РФ подтверждает, что и в современном, состязательном уголовном процессе властные субъекты должны обеспечивать всесторонность, полноту и объективность познания в целях реализации назначения уголовного судопроизводства (ст. 6 УПК РФ). Только такой подход обеспечивает юридически важное и значимое соотношение *объективности* собирания необходимой доказательственной информации и *субъективности* оценок, по внутреннему убеждению, относимости, достоверности, достаточности этой информации лицом, ведущим производство по делу.

Появление в человеческой практике цифровых технологий и цифровой информации порождает новую проблему в области процессуального познания и доказывания, с которой сталкиваются юристы. Это проблема «машиночитаемости» права техническими цифровыми устройствами, с одной стороны, и «человекочитаемости» цифровой информации, получаемой субъектами доказывания, с другой стороны [3]. Следует признать, что цифровая техника существенно увеличивает и расширяет возможности следователя и суда в получении информации о совершенном деянии. Например, цифровые фото- и видеоприборы могут запечатлеть картину места происшествия более детально, а возможность увеличения масштабов изображения позволяет обнаружить и рассмотреть детали, которые могут быть незаметны и даже недоступны человеческому зрению. Как показала практика, наличие множества видеокамер в пространстве города позволяет выявлять и раскрывать до 70% правонарушений, совершаемых в Москве [4]. Более того, информация с видеокамер может быть доступна не только должностным, но и частным лицам, и адвокатам, оказывающим квалифицированную юридическую помощь невластным участникам процесса. Это позволяет человеку существенно расширить возможности защиты и оспаривания обвинения, если познавательные выводы следователя не соответствует реальной обстановке совершения деяния. Существенно расширяется возможность поиска и собирания различной информации о совершенном деянии в многочисленных базах данных, социальных сетях, блогах и т.п. Появляется возможность, используя цифровую технику, получать вербальную или визуальную информацию, имеющую значение по делу, на удаленных или закрытых объектах. Уже на данный момент развития цифровой техники и технологий можно утверждать, что возможности доказывания существенно расширяются и цифровая трансформация доказывания требует своевременного и системного регулирования процедур использования новых возможностей.

Но, на наш взгляд, цифровые возможности расследования традиционных преступлений, совершаемых в физическом мире и мире социального взаимодействия людей, все же не меняют самой природы и понимания *доказательства как сведений*, имеющих юридическое значение для данного дела. Появление новых возможностей использовать в доказывании цифровую технику и технологии требует внимания к своевременному уточнению и дополнению правового регулирования. Целесообразно уточнять процессуальный порядок и определять параметры допустимости использования в доказывании новых, дополнительных, более эффективных возможностей выявлять, фиксировать, собирать и использовать информацию о фактической стороне совершения преступления, получаемую из «цифровой среды». Для таких преступлений как оборот наркотических средств с помощью электронных сетей; мошенничество в сфере компьютерной информации; неправомерный оборот средств платежей и т.п. сама цифровая информация, получаемая с помощью электронных средств, так же как информация, получаемая от свидетелей и из других традиционных источников (ч.2 ст. 74 УПК РФ), происходит в результате отражения в цифровой среде и цифровой форме фрагментов преступной деятельности в окружающем мире (например, способа совершения, умышленного характера совершаемых действий и т.п.).

Вместе с тем представляется, что остается недостаточно изученным процессуальное познание преступлений, совершаемых в самой цифровой среде. Полагаем, что при совершении действий, признаваемых уголовным законом как «компьютерные преступления» (гл. 28 ст. 272, 273, 274.1 УК РФ), процессуальное познание и тем более доказывание столкнутся с принципиально иной ситуаций. А.И. Зазулин справедливо признает, что цифровая информация в природе не существует и является изобретением человеческого разума, тогда как человек может воспринимать только аналоговые сигналы. Современные цифровые устройства уже способны преобразовывать аналоговую информацию в цифровую для целей ее хранения и обработки, а также могут преобразовывать цифровую информацию в аналоговую для целей восприятия информации человеком. Цифровая информация может быть записана и храниться только на определенных материальных носителях, тогда как человек не может хранить в своей памяти информацию в цифровой форме [2, С. 28-30]. Добавим, что человек не может и оперировать информацией в цифровой форме: выявлять содержательно значимую информацию, изложенную в виде двоичного числового кода; предъявлять ее к ознакомлению в непреобразованном виде; представлять в судебном заседании в подтверждение обвинения.

Компьютерные преступления, например, неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) и пр. *происходят в самой цифровой среде*: человек, имея преступный умысел взаимодействует с цифровой техникой и/или технологией, создавая и запуская вредоносные программы, преследуя свою корыстную или иную преступную цель, используя для этого исключительно цифровой язык. Он выполняет

технические действия и манипуляции с техническими цифровыми устройствами, вводит цифровую информацию, получает цифровой результат своих действий. Сам процесс совершения преступления совершенно не очевиден, он не проявляет себя во вне цифровой среды и цифрового языка, его нет нигде, кроме цифровых носителей, без цифрового носителя он просто не существует. В этот момент деятельности цифровой язык может вообще не иметь перевода на язык человеческих слов и смыслов. Возможно только «на выходе», т.е. в момент завершения всего объема цифровой активности преступника, иное лицо, как правило, ставшее жертвой преступных цифровых действий, может обнаружить некий вредоносный результат. Но цифровой результат далеко не сразу, не явно и далеко не однозначно может быть соотнесен с чьим-то преступным намерением, действием, целью. Он может восприниматься как технический сбой, как неисправность собственной цифровой техники, как атака на цифровую сеть, не являющаяся преступной и т.п. Первые действия по исправлению возникшего сбоя могут существенно изменить всю цифровую информацию, уничтожая то, что можно было бы расценить как след преступления. Учитывая, что цифровая среда не знает границ и расстояний, имеет открытый, неограниченный круг пользователей, способна модифицироваться внешними вторжениями как целенаправленными, так и случайными, поиск доказательственной информации существенно затрудняется. Не случайно, во многих государствах создаются специальные службы цифрового технического обеспечения и оперативно-розыскной, и процессуальной деятельности по выявлению и пресечению компьютерных преступлений.

Легализация цифровой информации и превращение ее в доказательство преступления в сфере компьютерной информации требует выявления и учета ее специфики. Так, следует учитывать, что для выявления и раскрытия компьютерных преступлений не пригоден метод «аналогового мышления». Во-первых, цифровой язык (сочетание «0» и «1») не порождает образов, аналогичных жизненным ситуациям, создаваемым традиционной формой преступной деятельности, поэтому преступление остается не явным до тех пор, пока не будет обнаружен вредоносный результат, пока технически не будет установлено, что этот результат наступил от чьих-то целенаправленных и противоправных действий. Во-вторых, сам результат также выражен в цифровой форме и не несет традиционной информации о деянии, как привычный след - отпечаток совершенных действий. В-третьих, сама информация, существующая только в цифровой форме и находящаяся в цифровой среде; вне этой среды и этого языка не существует и, соответственно, не может быть выявлена.

Чтобы понять преступное значение цифровой информации ее необходимо так или иначе отыскать в цифровой среде и «обратить» ее в «человекочитаемую» форму. Совершенно справедливо Т.Я. Хабриева и Н.Н. Черногор определили машиночитаемость права как «*правоположения, изложенные в виде машинных алгоритмов, реализованных на языках программирования (программного кода), понимаемых машиной и последующей машиноисполняемой реализацией*» [5]. Всякий раз, когда юрист сталкивается с

цифровой информацией, необходимостью ее обнаружения, изъятия, копирования и пр. закон предписывает привлечение специалиста (см. ч. 2.1 ст. 82 УПК РФ) Напрашивается предложение использовать помощь специалиста и в делах о компьютерных преступлениях, перечисленных в гл. 28 УК РФ. Однако, для «компьютерных преступлений» традиционный подход к пониманию и правовому регулированию специалиста в уголовном судопроизводстве (ст. 58 УПК РФ) не подходит. Следователь, не владея цифровым языком и достаточными знаниями о возможностях цифровой техники и цифровых технологий, даже не сможет сформулировать специалисту поисковую задачу. Одновременно специалист, владеющий достаточными знаниями и навыками в цифровых технологиях и технических устройствах, не может знать, какая информация из этой среды, выраженная цифровым языком, может иметь юридическое значение, а какая не отвечает уголовно-правовому и процессуальному требованию относимости. Следует признать, что цифровая информация не способна отразить содержание признаков состава преступления с «аналоговой очевидностью». Скрытые в цифрах преступное намерение и преступная цель, преступный характер действий в цифровой среде не очевидны так, как это бывает с преступлениями, совершаемыми в физическом мире. Требуется некая новая процессуально-правовая деятельность человека по интерпретации цифровой информации в «человекочитаемую» и «правочитаемую». О последующей *машиноисполняемой реализации,* когда сам компьютер сможет сразу же сможет определять преступный характер цифровых действий и незамедлительно пресекать их уже в момент их совершения или отправления по сети, мечтать пока не приходится. Для решения задач уголовного судопроизводства пока именно человек должен и выявлять, и интерпретировать цифровую информацию с позиций ее юридического, уголовно-правового или доказательственного значения. Более того, эта информация должна стать *понятной и доступной* не только следователю, суду, узким специалистам. Она должна обладать свойством *проверяемости.* Каждый человек, сомневаясь в утверждениях обвинения, должен иметь возможность понять, на чем основан вывод о преступном характере деяния, совершенного от начала и до конца в цифровой среде; достаточно ли доказательств виновной причастности подсудимого к совершению данного преступления, несмотря на то что все его обстоятельства выражены только техническим или цифровым языком.

Можно ли решить такую задачу, привлекая специалиста по цифровым технологиям в качестве переводчика, который смог бы помочь следователю и всем иным субъектам судопроизводства в переводе информации, обнаруженной в цифровом языке, не только на обычный человеческий язык, но еще на язык права, поскольку цифровые знаки сами по себе несут принципиально иную цифровую информацию? Увы, здесь требуется не просто перевод с одного доступного языка на другой доступный язык, чем обычно занимается переводчик в уголовном судопроизводстве. Здесь необходима расшифровка и даже интерпретация цифровых знаков, а также цифровых действий в некое вербальное объяснение: что могут означать те или иные сочетания цифровых знаков в данном случае, какие команды «стоят» за набором цифр, в чем правовое значение этих действий, связаны ли они с

преступным результатом причинно-следственной связью и пр. К сожалению, ст. 59 УПК РФ, регулирующая понятие и статус переводчика, не пригодна для решения таких вопросов. Более того, следует еще раз подчеркнуть, что в таких делах вся информация существует и сохраняется только на цифровых носителях: серверах, флеш-картах, дисках и т.п. Ее нельзя изъять и представить для ознакомления, изучения, использования в устном судебном разбирательстве, когда в зале присутствуют не только участники судебного разбирательства, но и публика, журналисты, родственники фигурантов дела. Все они должны получить очевидное, наглядное предъявление *содержания* доказательств, иначе нарушается принцип гласности судебного разбирательства, устности судопроизводства. Представить сам носитель цифровой информации можно, но необходимо еще и убедить в том, что на этом носителе есть именно доказательственная информация, можно только предъявив ее содержание на языке, который понятен человеку. Не случайно В.Г. Афанасьев обращал внимание на то, что информация, будучи объективной по источнику происхождения, предполагает наличие «приемника, преобразователя и пользователя» [6, С. 238]. И это очень важно для уголовного судопроизводства, в котором все субъекты процессуальной деятельности и даже иные лица имеют право знать, на основании какой информации вынесен приговор по делу.

Очевидно, что природа выявления и доказывания совершения преступлений в собственно компьютерной среде, существенно иная. Предложения о необходимости просто дополнить перечень видов доказательств в ч.2 ст. 74 УПК РФ указанием в нем еще и «электронных доказательств», новых проблем не решит. Полагаю, что необходимы комплексные исследования, в которых должны принимать участие одновременно юристы, владеющие знаниями об уголовном судопроизводстве и его не только процессуальных, но и криминалистических, и оперативно-розыскных, и уголовно-правовых аспектах, а также представители разных специальностей в области цифровизации и цифровых технологий.

Список литературы

1. Борисенко, А.А. О сущности информации / А.А. Борисенко // Фундаментальные исследования. 2005. № 7. С.32-33.

2. Основы теории электронных доказательств: монография / под ред. С.В. Зуева. Юрлитинформ, 2019. 398 с.

3. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский // Вестник РУДН. Серия: Юридические науки. - 2021. Т. 25. № 4. С.735-749.

4. Программа «Безопасный город» // URL: https://www.mos.ru/drbez/documents/programma-bezopasnyi-gorod/?ysclid=lf5hpj3tzi62253483.

5. Хабриева, Т.Я. Будущее права. Наследие академика В.С. Степина и юридическая наука /Т.Я. Хабриева, Н.Н. Черногор.М.: ИНФРА-М, 2020. 176 с.

6.Афанасьев, В.Г. Системность и общество / В.Г.Афанасьев. М.,1980. 368 с.

УДК 004.8

ПРАВОСУБЪЕКТНОСТЬ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: CONTRADICTIO IN ADJECTO

Галахтин Михаил Геннадьевич,
канд. филос. наук., доцент
Национальный исследовательский университет
«Московский институт электронной техники»,
г. Москва, Россия
email: m.galakhtin@gmail.com

Аннотация: *исследуются вопросы правовых последствий использования систем искусственного интеллекта в различных сферах. Акцентируются проблемы конкретизации юридической ответственности в случае причинения вреда при использовании систем искусственного интеллекта. Особое внимание обращено на вопросы надлежащего субъекта при создании произведений с использованием систем искусственного интеллекта. Делается вывод о невозможности правовой охраны произведений, созданных с использованием систем искусственного интеллекта, как объектов авторского права.*

Ключевые слова: *искусственный интеллект, субъект права, юридическая ответственность за причинение вреда, объекты авторского права, автор произведения.*

LEGAL PERSONALITY OF ARTIFICIAL INTELLIGENCE SYSTEMS: CONTRADICTIO IN ADJECTOM

Galakhtin Mikhail Gennadievich,
candidate of philosophy, associated prof.
National research university of electronic technology (MIET),
Moscow, Russia
email: m.galakhtin@gmail.com

Abstract: *this paper investigates the legal consequences of artificial intelligence systems use in various areas are. It higlights the problems of legal liability concretization when prejudice is caused by the use of the artificial intelligence systems. A special attention is placed to the issues related to the authentic subject in the production of texts using the artificial intelligence systems. It makes a conclusion about the impossibility of legal protection of productions created by the artificial intelligence systems as copyright items.*

Keywords: *artificial intelligence, subject of law, legal responsibility for harm-doing, items of copyright, text author.*

Интенсивное развитие современных компьютерных систем, в особенности широкое распространение и внедрение в различные сферы экономики, социальных и государственных институтов технологий

искусственного интеллекта, зачастую позиционируемых как конкурентный фактор при принятии решений, представляет собой реальный вызов действующей правовой системе, столкнувшейся с новым феноменом, способным пошатнуть сами основы современной доктрины права. Целый ряд проблем, связанных с трансформацией правовой системы под влиянием развития технологий искусственного интеллекта, сформулированы в «Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» – далее Концепция (утверждена Распоряжением Правительства РФ от 19 августа 2020 г. № 2129-р).

В указанной Концепции выделены наиболее значимые проблемы применения систем искусственного интеллекта. К ним относятся, в частности, проблемы правового «делегирования» решений системам искусственного интеллекта и робототехники, ответственности за причинение вреда с использованием систем искусственного интеллекта и робототехники, а также правового режима результатов интеллектуальной деятельности, созданных с использованием систем искусственного интеллекта (п.4 раздела I Концепции).

Закрепленные в Концепции принципы функционирования систем искусственного интеллекта и робототехники включает в себя приоритет благополучия и безопасности человека, защиты его основополагающих прав и свобод (цель обеспечения благополучия и безопасности человека должна преобладать над иными целями разработки и применения систем искусственного интеллекта и робототехники), запрет на причинение вреда человеку по инициативе систем искусственного интеллекта и робототехники (по общему правилу следует ограничивать разработку, оборот и применение систем искусственного интеллекта и робототехники, способных по своей инициативе целенаправленно причинять вред человеку), подконтрольность человеку (в той мере, в которой это возможно с учетом требуемой степени автономности систем искусственного интеллекта и робототехники и иных обстоятельств).

Вместе с тем Концепция предполагает некоторую трансформацию института юридической ответственности «в случае причинения вреда системами искусственного интеллекта и робототехники, имеющими высокую степень автономности, при принятии ими решений, в том числе с точки зрения определения лиц, которые будут нести ответственность за их действия, доработки при необходимости механизмов безвиновной гражданско-правовой ответственности, а также возможности использования способов, позволяющих возместить причиненный действиями систем искусственного интеллекта и робототехники вред (например, страхование ответственности, создание компенсационных фондов и др.; п.2 раздела II Концепции). Во-первых, данные положения косвенно допускают возможность причинения вреда системами искусственного интеллекта, что, как показано выше, противоречит самим исходным принципам их применения. Во-вторых, «делегирование» полномочий системам искусственного интеллекта с высокой степенью автономности при принятии решений в значительной степени размывает механизм ответственности за причиненный использованием этих систем вред.

Провозглашаемый в Концепции принцип распределенной ответственности, который должен быть реализован на основе эффективных и справедливых механизмов функционирования институтов юридической ответственности, и направлен на доведение ответственности до конкретных лиц. Гражданское законодательство в ряде случаев допускает привлечение к ответственности лиц, непосредственно не причастных к причинению вреда. В частности, юридические лица и граждане несут ответственность за вред, причиненный их работниками при исполнении ими своих служебных обязанностей (ст. 1068 ГК РФ), законные представители малолетнего несут ответственность за вред, причиненный малолетним (ст.1073 ГК РФ), опекуны несут ответственность за вред, причиненный недееспособным (ст. 1076 ГК РФ). Во всех перечисленных случаях субъект, несущий деликтную ответственность заранее определен. Очевидно, что субъектом такой ответственности не может быть сама система. К ответственности может привлекаться только её пользователь или разработчик. При этом лицо, несущее ответственность за причиненный вред, может привлекаться к ответственности без наличия его вины. В этом смысле, безвинное привлечение к ответственности лица, использующего системы искусственного интеллекта, в случае причинения вреда является вполне оправданным. В данном случае должна применяться аналогия с использованием средства повышенной опасности, поскольку причинение вреда в результате применения систем искусственного интеллекта сопряжено с повышенными социальными и даже экзистенциальными рисками. Обязательным требованием при этом должна быть идентификация реального субъекта, создавшего или использующего такие системы.

Особый состав деликтной ответственности составляет причинение вреда в результате неправомерных действий органов дознания, следствия, прокуратуры или суда (ст. 1070 ГК РФ). В случае незаконного осуждения, привлечения к уголовной или административной ответственности, применения мер пресечения в виде заключения под стражу или подписки о невыезде вред возмещается за счет казны. Данная норма, по всей видимости, потребует дополнений и изменений в связи с широким использованием систем искусственного интеллекта при расследовании преступлений и отправления правосудия. Проблема деликтной ответственности при принятии юридически значимых решений в ситуации все возрастающей автономизации систем искусственного интеллекта и нередко замещения правовой оценки деяния экспертным заключением с использованием алгоритмов компьютерных программ будет одной из ключевых при трансформации института юридической ответственности при использовании систем искусственного интеллекта.

Как в недалеком будущем, возможно, будет трансформирована система отправления правосудия можно проследить на примере современной правовой системе Китая. Тотальная цифровизация правовой сферы в КНР направлена главным образом на максимальное упрощение рутинных технологических процессов и ускорение получения и обработки правовой информации. В частности, при принятии решения судье доступны необходимые прецеденты по

аналогичным делам за предыдущий период, а также ссылки на применимые к данному случаю статьи закона. При этом система подсказывает возможное решение по конкретному делу на основе обработки и анализа всего массива информации, относящегося к делу. Если судья принимает решение, отличное от рекомендованного, то требуется пояснение и внесение в систему обоснования принятого решение. Данные требования направлены на снижение возможных судебных ошибок и уровня коррупции. При этом решение по делу остается за судьей. Цифровой трансформации подвергаются сопроводительные процедуры и делопроизводство, например, составление протоколов судебных заседаний через системы распознавания голоса, онлайн загрузка доказательств и улик, мгновенное размещение запретов на совершение определенных действий, дистанционная реализация конфискованного имущества на аукционе. Все большее распространение в Китае получают механизмы внесудебного урегулирования споров на основе медиации с использованием онлайн коммуникационных технологий. Иными словами, системы искусственного интеллекта призваны не замещать субъектов правоприменительной деятельности следователей, судей и прокуроров, а, напротив, обеспечить прозрачность и эффективность их деятельности посредством освобождения от рутинных функций, занимающих время и силы. Косвенным результатом применения систем искусственного интеллекта в сфере расследования преступлений и отправления правосудия должно стать снижение количества прецедентов привлечения к ответственности государства за незаконные действия правоохранительных и судебных органов и их должностных лиц.

Одной из сложных проблем введения в правовое поле результатов применения систем искусственного интеллекта является легализация и возможность правовой охраны объектов, созданных с использованием этих систем. Широкое применение технологий искусственного интеллекта при создании аудио-визуальных и текстовых произведений в настоящее время получило широкое распространение и имеет тенденцию к дальнейшему распространению и захвату все новых областей человеческой творческой деятельности.

Особый общественный резонанс в последнее время вызвала технология ChatGPT, созданная американским стартапом OpenAI, контролируемым И. Маском. Система, опирающаяся на принципы глубокого обучения, способна, в частности, по запросу пользователя самостоятельно генерировать научные тексты, не отличимые по стилистике и содержанию от текстов, создаваемых человеком. Применение таких систем в сфере образования при выполнении в том числе выпускных квалификационных работ, как это имело место в РГГУ, ставит довольно нетривиальные проблемы перед руководством университетов и Минобрнауки. Дело в том, что при прохождении обучающимися процедур допуска к защите этих работ, они успешно преодолевали барьер проверки на плагиат и процент оригинальности составлял более 80%, что зачастую превышает аналогичный показатель в работах, выполненных традиционным способом. Если учесть, что во многих учебных заведениях прием и выпуск

обучающихся осуществляется на основе представленной квалификационной работы масштаб проблемы представляется весьма значительным.

В более широком плане проблему следует сформулировать как возможность или невозможность признать охраноспособность произведений, созданных с помощью систем искусственного интеллекта. Уже обыденностью стали примеры использования компьютерных систем для создания аудио произведений. Программы на основе искусственного интеллекта, такие как, например, Flow Machines (разработанная в исследовательской лаборатории Sony CSL) или AIVA (Artificial Intelligence Virtual Artist, виртуальный композитор) способны создавать произведения поп и даже классической музыки на основе обработки огромного массива информации по аналогичным произведениям. Может ли в данном случае этим произведениям предоставляться правовая охрана?

Прежде всего, сам факт использования искусственного интеллекта при создании произведений литературы, науки или искусства, в том числе синтезированных образов или голосов должен быть декларирован. Поставщик услуг по использованию программного продукта обязан указать посредством специальной метки, или иного обозначения, что произведение получено в результате обработки текстового, аудио или видео контента с помощью программных средств систем искусственного интеллекта. Данное требование содержится, в частности, принятом в КНР «Положении об администрировании глубокого синтеза информационных сервисов Интернета» (п. 19.), вступившим в силу 10 января 2023 г. В указанном документе все поставщики услуг «глубокого синтеза», т.е. предоставляющие возможность получения виртуальных объектов, относящихся к области создания текстовых, аудио, видео произведений, редактирования изображений человека и звука его голоса, иных биометрических данных на основе использования технологий искусственного интеллекта должны проходить обязательную регистрацию и публично заявлять о предоставлении таких услуг. При этом пользователи услуг должны в обязательном порядке быть идентифицированы при обращении к соответствующим сайтам. Данные процедуры призваны сделать процесс использования систем искусственного интеллекта максимально прозрачным.

Согласно нормам российского гражданского законодательства правовая охрана предоставляется только тем произведениями литературы, науки и искусства, которые созданы *творческим* трудом автора. Если под творчеством понимать процесс воплощения автором идеи или образа в произведение, то алгоритмы работы систем искусственного интеллекта осуществляют прямо противоположное действие: от созданных произведений они получают некий усредненный и оптимизированный конечный результат. Техническое содействие в любой форме не признается творческой деятельностью, результаты этой деятельности не получают правовой охраны (ст.1228 ГК РФ). Исходя из действующего законодательства произведения, созданные с помощью систем искусственного интеллекта, не могут получить правовой охраны, поскольку отсутствует ключевое условие такой охраны - надлежащий субъект, осуществляющий творческую деятельность. Правовую охрану в

данном случае может получить только сама программа, использующая алгоритмы искусственного интеллекта, созданная творческим трудом разработчиков. В этом смысле следует согласиться с В. Витко, что «в деятельности искусственного интеллекта по созданию результатов, похожих на объекты авторского права, отсутствует творчество, поэтому созданные им результаты не могут быть квалифицированы в качестве объектов авторского права и не подлежат охране правом интеллектуальной собственности». В этом смысле произведения, созданные искусственным интеллектом, можно приравнять к картинам, написанным слоном. Они представляют собой артобъекты, обладающие имущественным содержанием и, возможно, коммерческой ценностью, но не имеющие автора, интересы которого следует охранять и защищать. Распоряжение данными объектами находится в компетенции пользователя компьютерной программы, с помощью которой они были созданы, использующим её на законном основании.

Особый случай составляет создание с применением систем искусственного интеллекта текстовых произведений, использование которых может иметь юридическое значение, например, квалификационных или диссертационных работ. Поскольку авторство таких произведений отсутствует, лицо, выдающее их за собственные научные исследования, является ненадлежащим субъектом, недобросовестно присвоившим себе право авторства. Такие работы не должны признаваться и допускаться к защите и подлежат аннулированию. Вместе с тем распознавание произведений, созданных с использованием систем искусственного интеллекта, представляется нетривиальной технической задачей, справляться с которой, по всей видимости, придется другим системам, основанным на тех же принципах.

УДК 343.13

ИСТРЕБОВАНИЕ СУДОМ ДОКАЗАТЕЛЬСТВ В ЭЛЕКТРОННОМ ВИДЕ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ

Галицкая Елизавета Евгеньевна,
помощник судьи Красноярского краевого суда, аспирант
Красноярский государственный аграрный университет,
г. Красноярск, Россия
email: ques13@yandex.ru

Аннотация: *целью данной статьи является рассмотрение возможностей использования современных технологий при истребовании судом доказательств в уголовном судопроизводстве. Результатом исследования явился вывод о необходимости расширения работы сервисов ГАС «Правосудие», позволяющих осуществлять электронный обмен информацией между различными информационными системами (базами данных) государственных и муниципальных органов, а также вывод об использовании*

усиленной квалифицированной электронной подписи для оформления копий судебных актов.

Ключевые слова: *современные технологии, ГАС «Правосудие», доказательства, электронное судопроизводство, УКЭП.*

THE COURT'S RECLAMATION OF EVIDENCE IN ELECTRONIC FORM USING MODERN TECHNOLOGIES

Galitskaya Elizaveta Evgenievna,
assistant judge of the Krasnoyarsk regional court, graduate student
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
email: ques13@yandex.ru

Abstract: *the purpose of this article is to consider the possibilities of using modern technologies when a court demands evidence in criminal proceedings. The result of the study was the conclusion about the need to expand the work of the services of the GAS "Justice", which allow for electronic exchange of information between various information systems (databases) of state and municipal bodies, as well as the conclusion about the use of enhanced qualified electronic signature for registration of copies of judicial acts.*

Keywords: *modern technologies, GAS "Justice", evidence, electronic legal proceedings, UKEP.*

В ходе рассмотрения судом в порядке уголовного судопроизводства дел и материалов в порядке исполнения приговора нередко возникает необходимость в истребовании дополнительных доказательств, некоторые из которых содержатся в информационных электронных базах различных государственных органов, например, сведения о судимости, судебные акты судов различных инстанций.

Так, в случае установления обстоятельства привлечения подсудимого, в отношении которого в суд поступило уголовное дело, к уголовной ответственности и вынесения в отношении него обвинительного приговора, для правильного рассмотрения и разрешения уголовного дела суд обязан истребовать заверенную надлежащим образом копию приговора из суда, его постановившего. Содержание истребованного приговора влияет на назначение наказания в случае постановления по настоящему уголовному делу обвинительного приговора, например, на применение норм о совокупности преступлений или совокупности приговоров.

Такая же необходимость возникает и при принятии судом постановлений в порядке исполнения приговора, например, при разрешении вопроса об освобождении от наказания или о смягчении наказания вследствие издания уголовного закона, имеющего обратную силу, в соответствии со статьей 10 Уголовного кодекса Российской Федерации.

Как разъяснил Пленум Верховного Суда Российской Федерации, решая вопрос об освобождении осужденного от наказания или о смягчении ему наказания вследствие издания уголовного закона, имеющего обратную силу, суд основывает постановление только на обстоятельствах, установленных вступившим в законную силу приговором суда, назначившего наказание, и не вправе оценивать правильность применения этим судом уголовного закона (пункт 17 постановления от 20.12.2011 N 21 «О практике применения судами законодательства об исполнении приговора») [4].

При этом разрешение данного вопроса сопровождается, кроме прочего, истребованием сведений о судимости осужденного, обратившегося с таким ходатайством. Без указанных сведений зачастую невозможно установить обстоятельства погашения или снятия соответствующей судимости, поскольку истребованная из Министерства внутренних дел справка содержит развернутую информацию о принявшем судебный акт органе, сроках содержания под стражей, наименовании исправительного органа и сроках отбывания наказания.

Таким образом, процедура принятия судебного решения по разрешению вопросов в порядке исполнения приговора предполагает необходимость доказывания соответствующих вопросу обстоятельств, информацию о которых суд уполномочен истребовать путем направления судебных запросов.

На смену традиционному почтовому методу обмена информацией приходят цифровые технологии, призванные повысить оперативность информационного взаимодействия судов с другими органами государственной власти. В этих целях была создана Государственная автоматизированная система Российской Федерации «Правосудие», которая была построена на основе использования новых информационных технологий [2]. Развитие судебной системы с использованием достигнутого уровня современных информационных технологий осуществляется в соответствии с планом, предусмотренным Концепцией информатизации судов и системы Судебного департамента до 2030 года (утвержденным постановлением президиума Совета судей Российской Федерации от 02 декабря 2019 года № 785), а также мероприятиями национальной программы «Цифровая экономика Российской Федерации» [1]. В настоящее время введены в эксплуатацию сервисы ГАС «Правосудие», предназначенные для организации информационного взаимодействия между информационными системами участников в целях предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, позволяющие формировать электронный запрос в государственные органы посредством специального программного обеспечения, основными преимуществами которого являются скорость и удобство получения ответа.

В настоящее время стало возможным электронное взаимодействие с ФССП России, органами кадастрового учета (Росреестр), ФНС, Федеральным казначейством и другими, что в силу существенного сокращения времени на отправку и доставку информации отражается на сроках рассмотрения дел.

На наш взгляд, использование технического прогресса позволило бы государственным органам, в том числе и судебным, осуществлять обмен

юридически значимой информацией в наиболее короткие сроки при использовании в качестве подтверждения наделения соответствующими полномочиями на истребование получаемой информации электронной цифровой подписи.

Так, сведения о судимости выгружаются правоохранительными органами в единую информационную систему, доступ к которой имеют в каждом отдельно взятом структурном подразделении, и которые так же могут быть переданы по электронному запросу суда в течение короткого промежутка времени в электронном виде через сервисы ГАС «Правосудие».

Вопрос о том, насколько надлежаще заверенной будет получена такая информация, перестает быть насущным с появлением усиленной квалифицированной электронной подписи (УКЭП), которая является цифровым аналогом собственноручной подписи, а документы, подписанные от руки или с помощью УКЭП, имеют равнозначную ценность.

Постановлением Пленума ВАС РФ от 25.12.2013 N 100 утверждена Инструкция по делопроизводству в арбитражных судах Российской Федерации (первой, апелляционной и кассационной инстанций), которая дает определения современным понятиям [3].

Так, утверждением документа называется процедура утверждения документа лицами, уполномоченными на выполнение данной операции, путем проставления грифа утверждения. Гриф включает личную подпись или электронную подпись лица, если утверждение производится в электронном виде; ее расшифровку (Ф.И.О.); должность лица, утверждающего документ; дату утверждения документа, а электронный образ документа – это электронная копия документа, изготовленного на бумажном носителе.

Видится, что арбитражное судопроизводство оказалось в свете применения современных технологий куда более прогрессивным, чем судопроизводство в судах общей юрисдикции.

В пункте 9.5 вышеназванного постановления указано, что тексты всех судебных актов, за исключением текстов судебных актов, которые содержат сведения, составляющие государственную и иную охраняемую законом тайну, размещаются в информационном ресурсе "Картотека арбитражных дел", автоматизированной системе "Банк решений арбитражных судов" в сети Интернет в полном объеме через 24 часа с момента их подписания в САС.

Более того, судебные акты арбитражных судов высылаются участникам процесса за усиленной квалифицированной электронной подписью судьи (УКЭП), что делает возможным передачу электронного образа судебного акта, в том числе и через сервисы ГАС «Правосудие».

Возможность получения в столь короткий промежуток времени надлежащим образом заверенной копии приговора также представляет колоссальные резервы для экономии бумаги, конвертов, расходных материалов для печатающей техники и общих трудозатрат работников суда.

Таким образом, развитие информационных технологий в контексте высокотехнологичного права [5] и применение этих достижений в судопроизводстве [6], в частности на стадии исполнения приговора,

характеризующейся активной ролью суда, осуществляющего на стадии подготовки к судебному заседанию деятельность по истребованию необходимой для доказывания информации, позволяет в значительной мере упростить и оптимизировать выполнение задач судопроизводства.

Список литературы

1. Информационный бюллетень Амурского областного суда, судейского сообщества Приамурья и Управления Судебного департамента в Амурской области № 26 (2021) // URL: https://files.sudrf.ru/2425/user/IB26.pdf (дата обращения: 02.02.2023). Текст: электронный.
2. Портал технической поддержки Государственной автоматизированной системы Российской Федерации «Правосудие» // URL: https://techportal.sudrf.ru/ (дата обращения: 02.02.2023) - Текст: электронный.
3. Постановление Пленума ВАС РФ от 25.12.2013 № 100 (ред. от 11.07.2014) «Об утверждении Инструкции по делопроизводству в арбитражных судах Российской Федерации (первой, апелляционной и кассационной инстанций)» // URL: http://www.consultant/ru (дата обращения: 02.02.2023). Текст: электронный.
4. Постановление Пленума Верховного Суда РФ от 20 декабря 2011 года № 21 «О практике применения судами законодательства об исполнении приговора» // URL: http://www.consultant/ru (дата обращения: 02.02.2023). Текст: электронный.
5. Бертовский, Л. В. Высокотехнологичное право: понятие, генезис и перспективы / Л. В. Бертовский // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2021. Т. 25, № 4. С. 735-749.
6. Бертовский, Л. В. Перспективы применения технологии "блокчейн" в уголовном судопроизводстве / Л. В. Бертовский, Г. С. Девяткин // Деятельность правоохранительных органов в современных условиях: сборник материалов XXIV международной научно-практической конференции, Иркутск, 06–07 июня 2019 года / Восточно-Сибирский институт МВД России. Иркутск: Восточно-Сибирский институт Министерства внутренних дел Российской Федерации, 2019. С. 115-118.

УДК 363.1

ОБ АКТУАЛЬНЫХ ВОПРОСАХ ПРОВЕДЕНИЯ ЭКСПЕРТИЗЫ ЭЛЕКТРОННО-ЦИФРОВЫХ СЛЕДОВ ПРИ РАССЛЕДОВАНИИ ДОЛЖНОСТНЫХ НАСИЛЬСТВЕННЫХ ПРЕСТУПЛЕНИЙ

Галяутдинов Рушан Радикович,
кандидат юридических наук, ассистент кафедры криминалистики
Институт права Уфимского университета науки и технологий, г.Уфа
e-mail: rushan-94@mail.ru

Аннотация: *при подготовке эмпирического материала в ходе работы над диссертацией на соискание ученой степени кандидата юридических наук были выявлены особенности категоризации определения электронно-цифровых следов. Исходя из этого, возникли вопросы с назначением соответствующих экспертиз электронно-цифровых следов в связи с тем, что такая следовая картина в определенных случаях исчезает спустя некоторое время. В работе дается определение понятиям «должностные насильственные преступления», «электронно-цифровые следы», подробно разбирается назначение фоноскопической экспертизы, выделяются проблемные вопросы.*

Ключевые слова: *должностные насильственные преступления, электронно-цифровые следы, фоноскопическая экспертиза, эмпирический материал, цифровизац Galyautdinov Rushan Radikovich – Candidate of Law, Assistant of the Department of Criminology of the Institute of Law of the Ufa University of Science and Technology,*

ON TOPICAL ISSUES OF THE EXAMINATION OF ELECTRONIC AND DIGITAL TRACES IN THE INVESTIGATION OF OFFICIAL VIOLENT CRIMES

Galyautdinov Rushan Radikovich
candidate of law, assistant of the department of criminology
Institute of law of the Ufa university of science and technology,
e-mail: rushan-94@mail.ru

Abstract*: during the preparation of empirical material during the work on the dissertation for the degree of Candidate of Legal Sciences, the features of the categorization of the definition of electronic digital traces were revealed. Based on this, there were questions with the appointment of appropriate examinations of electronic and digital traces due to the fact that such a trace pattern in certain cases disappears after some time. The paper defines the concepts of "official violent crimes", "electronic digital traces", the purpose of phonoscopic examination is elementally analyzed, problematic issues are highlighted.*

Keywords*: official violent crimes, electronic digital traces, phonoscopic examination, empirical material, digitalization.*

Должностные насильственные преступления в рамках нашего исследования – специфичный термин, обозначающий противоправное применение насилия при использовании своих полномочий должностными лицами, как правило, правоохранительных органов. С позиций материального права мы включаем сюда определенные виды преступлений – превышение должностных полномочий с применением насилия, пытки, или повлекшие по неосторожности смерть потерпевшего или причинение тяжкого вреда его здоровью (ч. 3, 4, 5 ст. 286 УК РФ) и принуждение к даче показаний путем насилия, издевательств или пыток, или повлекшее по неосторожности смерть потерпевшего или причинение тяжкого вреда его здоровью (ч. 2, 3, 4 ст. 302 УК РФ) [1]. Рассматриваемые нами преступления в основном совершаются должностными лицами органов внутренних дел – наиболее многочисленными среди всех правоохранительных органов, а также сотрудниками ФСИН РФ и других правоохранительных органов. Должностные лица правоохранительных ведомств чаще всего вступают в непосредственный контакт с лицами, совершающими преступления и иные правонарушения, в связи с чем в большей степени подвержены «обратному» негативному влиянию с их стороны. Статистика должностных насильственных преступлений, совершаемых сотрудниками органов внутренних дел, с одной стороны, свидетельствует об уменьшении их количества, с другой – о латентности таких деяний и противодействии их расследованию в связи с лояльным отношением к ним самих сотрудников правоохранительных органов. К тому же следует сказать, что должностные насильственные преступления, совершенные должностными лицами уголовно-исполнительной системы, – это уже не отдельные, а системные деяния в отношении лиц, находящихся в местах лишения свободы. Такие преступления негативно влияют на сферу досудебного и судебного производства, порождают причинно-следственную цепочку, нарушающую механизм реализации закона и систему правосудия, негативно сказываются на нравственно-психологическом состоянии общества в целом.

Анализ следственной и судебной практики показывает, что абсолютное большинство должностных насильственных преступлений совершается путем активных действий преступника. Результаты такого взаимодействия неминуемо отражаются в виде следовой картины преступления. Следует отметить, что криминалистически значимая информация, которую содержат в себе следы, образовавшиеся в результате совершения преступного деяния, может быть, как доказательственной, так и ориентирующей при расследовании должностных насильственных преступлений. То есть, на наш взгляд, такого рода сведения могут быть доказательствами по делу либо могут способствовать получению доказательств и принятию как тактических, так и процессуальных решений. Например, информация о психологических либо социальных особенностях лица, совершившего преступление, может быть получена путем исследования идеальных и цифровых следов и использована в целях поиска преступника, в тех случаях, когда конкретное должностное лицо не известно.

Следовая картина должностных насильственных преступлений включает в себя спектр идеальных, материальных и цифровых следов. Следы остаются в

различных формах. Считаем важным определить различия между понятиями «цифровой след», «электронно-цифровой след», «виртуальный след», «информационный след». Проанализируем многообразие этих определений через призму некоторых научных источников. В.Б. Вехов в своей монографии «Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки» вводит такое понятие как «цифровой след» и определяет его как любую криминалистически значимую компьютерную информацию, т.е. сведения (сообщения, данные), находящиеся в цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов. При этом «цифровые следы» являются материальными невидимыми следами [2, с. 293]. Определяя сущность «виртуального следа», Г.М. Шаповалова вводит термин «информационный след» и определяет его через традиционное понятие следа в криминалистике как «любое изменение среды под влиянием преступления», при этом данное определение дополнено уточнениями [3, с. 109]. В более поздних работах автор уточнял, что «информационный след» можно определить, как изменение информационной среды в виде сигналов и кодов на электронных и иных физических носителях.

Почему же в нашей работе рассматриваемые следы получили название электронно-цифровых. Дело в том, что если рассматривать цифровые следы, то речь бы шла о всей совокупности компьютерной информации, хранящейся на физических носителях. Если говорить о информационных следах, то речь бы шла о информации в сети Интернет [4, с. 219]. Анализируя научные мнения, отметим, что с целью оптимизации расследования должностных насильственных преступлений включать электронно-цифровые следы в состав материальных следов не всегда целесообразно, так как они зависят от способа считывания, не всегда имеют неразрывной связи с устройством, с помощью которой осуществлялась запись информации и иногда неустойчивы. Электронно-цифровые следы в контексте нашего исследования также включают в себя видеозаписи, хранящиеся в облачных хранилищах, на онлайн-серверах, в виртуальной памяти телефона: айклауд, гугл драйв, информация, полученная из социальных сетей, сообщения с таймером, которые могут исчезать онлайн спустя некоторое время и в этих аспектах кроется важная особенность этой категории. Показателен следующий пример: А., будучи инспектором отдела безопасности исправительной колонии, превысил свои должностные полномочия, применил насилие с использованием специальных средств в отношении осужденного Б. При этом преступление было совершено в помещении для личного обыска и досмотра вещей, оборудованном видеокамерами. Для сокрытия следовой картины преступления по указанию А. в целях противодействия расследованию должностного насильственного преступления видеозапись была повреждена, однако в ходе расследования преступления удалось установить, что частичные ее элементы сохранились на облачном хранилище исправительной колонии, экспертам в ходе проведения компьютерно-технической экспертизы удалось установить причастность А. к

совершению преступления. Как итог, А. был привлечен к уголовной ответственности по п. «б» ч. 3 ст. 286 УК РФ [5].

В вышеописанном примере проведена компьютерно-техническая экспертиза электронно-цифрового следа. Остановимся на назначении и проведении фоноскопической экспертизы электронно-цифровых следов. Отметим, что в науке уделяется достаточное внимание проведению фоноскопической экспертизы звукозаписей, однако особенности экспертизы электронно-цифровых следов не отмечаются. Фоноскопическая экспертиза проводится с целью идентификации по голосу и звучащей речи, установления природы образования объектов-источников звука, технического исследования носителей информации, аппаратной и программной частей устройств записи и для решения иных задач, вытекающих из научно-методических возможностей экспертов и имеющейся в распоряжении экспертной организации материально-технической базы [6, с. 81]. Комплексный характер исследования объектов фоноскопической экспертизы формируется за счет трансформации и интеграции знаний из различных областей научного знания. Сложность проведения фоноскопической экспертизы электронно-цифровых следов заключается в их правильной интерпретации. Звукозаписи, хранящиеся на онлайн-серверах, могут быть уничтожены дистанционно, или повреждены частично, в связи с этим необходимо как можно скорее назначать и проводить фоноскопическую экспертизу. Служебная, справочная и иная информация в совокупности с другими, выявленными инструментальным и лингвистическим методами анализа, основными признаками, может рассматриваться в качестве добавочных, в том числе частных или групповых, признаков подлинности и достоверности цифровых онлайн-фонограмм. Лишь комплексное (аудитивно-лингвистическое, инструментально-акустическое и компьютерно-техническое) исследование в совокупности позволит установить все свойства, характеристики и условия производства записи (перезаписи, копирования, редактирования) цифровой онлайн-фонограммы в ходе проведения фоноскопической экспертизы для формирования объективного и обоснованного вывода на поставленный вопрос при расследовании должностных насильственных преступлений в категорической форме.

Подытожим теорию фоноскопической экспертизы интересным примером из изученной нами судебной практики. Должностное насильственное преступление было совершено в служебном автомобиле, при этом сотрудники правоохранительных органов заранее старались скрыть следы преступления. Судебный пристав-исполнитель А. нанес потерпевшему Б. многочисленные удары в служебном автомобиле за отказ от прохождения медицинского освидетельствования. При этом перед совершением преступления служебный видеорегистратор, установленный в автомобиле и направляющий видеозапись в онлайн-формате на специальный сервер, был направлен на потолок и в связи с этим на видеозаписи были слышны лишь голоса, без визуализации должностных лиц. Несомненно, важным источником информации явилась данная видеозапись. С помощью фоноскопической экспертизы электронно-цифрового следа экспертам удалось идентифицировать голоса и конкретно

установить, кому они принадлежат. Судебный пристав-исполнитель А. был привлечен к установленной законом ответственности по п. «а» ч. 3 ст. 286 УК РФ [7].

Как итог, сделаем вывод, что, исходя из материалов научных источников и правоприменительной практики, назрела необходимость осмысления и категоризации понятия «электронно-цифровой след» с включением в нее многообразия онлайн-источников возможного нахождения доказательственных источников при расследовании должностных насильственных преступлений. Ряд уголовных дел о должностных насильственных преступлениях к сожалению, обходится без проведения фоноскопической экспертизы электронно-цифровых следов, что тоже вполне объяснимо сложностью проведения такой экспертизы в связи с необходимостью определения электронно-цифровых следов. Электронно-цифровые следы по должностным насильственным преступлениям в виде носителей информации, содержащие аудио и/или видеозаписи, должны быть особенно внимательно исследованы при расследовании, поскольку они станут важным элементов в цепочке доказательств по должностным насильственным преступлениям.

Список литературы

1. Уголовный кодекс РФ от 13 июня 1996 г. №63-ФЗ (с посл. изм. и доп. от 21 ноября 2022 г. № 446-ФЗ) // Официальный интернет-портал правовой информации // URL: http://www.pravo.gov.ru/.

2. Вехов, В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография / В.Б. Вехов. Волгоград: ВА МВД России, 2008. 500 с.

3. Шаповалова, Г.М. Возможность использования информационных следов в криминалистике: дис. … канд. юрид. наук / Г.М. Шаповалова. Владивосток, 2005.199 с.

4. Баев, О.Я., Солодов, Д.А. Производство следственных действий: Криминалистический анализ УПК России, практика, рекомендации: практ. Пособие / О.Я. Баев, Д.А. Солодов. М.: ЭКСМО, 2009. 298 с.

5. Архив Калининского районного суда г. Уфы Республики Башкортостан // Д. №1-7/2019.

6. Каганов, А.Ш. Криминалистическая экспертиза звукозаписей / А.Ш. Каганов. М.: Юрлитинформ, 2015. 364 с.

7. Архив Октябрьского районного суда г. Уфы Республики Башкортостан // Д. №1-118/2015.

УДК 343.985.7

О НЕОБХОДИМОСТИ ИСПОЛЬЗОВАНИЯ ОПЕРАТИВНО-РОЗЫСКНОГО ИНСТИТУТА СОДЕЙСТВИЯ ГРАЖДАН В РАСКРЫТИИ КИБЕРПРЕСТУПЛЕНИЙ

Давыдов Сергей Иванович,
доктор юридических наук, доцент
Барнаульский юридический институт МВД России,
г. Барнаул, Россия
e-mail: davidov_ord @mail.ru

Аннотация*: в статье приводятся данные о состоянии киберпреступности. Раскрывается потенциал законодательно установленного института содействия граждан оперативным подразделениям в раскрытии киберпреступлений. На примере группового дистанционного мошенничества обосновывается необходимость привлечения граждан к сбору информации, имеющей доказательственное значение по уголовным делам.*

Ключевые слова*: содействие граждан, оперативно-розыскные органы, раскрытие киберпреступлений.*

ON THE NEED TO USE THE OPERATIONAL-SEARCH INSTITUTE TO ASSIST CITIZENS IN THE DISCOVERY OF CYBERCRIMES

Davidov Sergey Ivanovich,
doctor of law, associate professor
Barnaul law institute of the Ministry of internal affairs of Russia,
Barnaul, Russia
email: davidov_ord@mail.ru

Abstract*: the article provides data on the state of cybercrime. The potential of the legally established institution of assisting citizens to operational units in disclosing cybercrimes is revealed. On the example of group remote fraud, the necessity of involving citizens in the collection of information of evidentiary value in criminal cases is substantiated.*

Keywords: *assistance of citizens, operational-investigative bodies, disclosure of cybercrime.*

Статистические данные свидетельствуют о том, что в 2021 году зарегистрирован прирост многих видов киберпреступлений, т.е. преступлений, совершенных с использованием информационно-телекоммуникационных технологий (ИТТ). Так, количество фактов мошенничества (ст. 159, 159.3, 159.6 УК РФ) возросло по сравнению с 2020 годом на 249249 или на 5,1%. При этом раскрываемость их составила всего 7%. Количество преступлений, связанных с незаконным оборотом наркотических средств (ст. 228.1, 228.2, 228.4, 230, 234 УК РФ), увеличилось на 52033 случая (+9,65%). Неправомерный оборот

средств платежей (ст. 187 УК РФ) возрос на 1755 или на 118,3%. Тенденции высокого уровня киберпреступности сохраняются и в 2022-23 годах. Как известно способы совершения таких преступлений постоянно совершенствуются, со стороны преступников принимаются меры по маскировке, сокрытию своей преступной деятельности.

В этих условиях для раскрытия киберпреступлений оперативно-розыскным органам необходимо предпринимать более эффективные меры, направленные на поиск и получение информации о следах, образующихся при их совершении. Среди таких эффективных средств следует выделить институт содействия граждан оперативным подразделениям. Возможность привлечения граждан к сотрудничеству для решения задач раскрытия преступлений предусмотрена Федеральным законом «Об оперативно-розыскной деятельности». Содействие граждан в соответствии с законом возможно не только гласно, но и на конфиденциальной основе, с заключением контракта. Оперативно-розыскным органам предоставлено право устанавливать отношения сотрудничества с конфидентами на безвозмездной или возмездной основе. Финансовые средства, которые выделяются на оперативно-розыскную деятельность, могут расходоваться на выплату вознаграждений содействующим лицам. Законом предусмотрен целый комплекс мер по социальной и правовой защите лиц, содействующих по контракту.

Почему же в настоящее время является актуальным более пристальное рассмотрение вопросов использования содействия граждан в борьбе с киберпреступностью. Ответ на это мы находим, изучая результаты научных исследований, посвященных разработке частных оперативно-розыскных методик раскрытия киберпреступлений. Отмечается некоторый уклон в сторону разработки рекомендаций по проведению оперативно-розыскных мероприятий, направленных исключительно на поиск следов преступления в информационной среде. Рекомендации содержат в основном практические советы относительно того, какие сведения можно получать у интернет-провайдеров, в кредитно-финансовых организациях, у операторов сотовой связи и интернет-сервисов, в т.ч. социальных сетей.

Например, у операторов сотовой связи при раскрытии киберпреступлений оперативно-розыскным органам предлагается запрашивать следующие сведения: полные данные владельца абонентского номера; детализацию входящих и исходящих телефонных соединений; используемые IMEI; о базовых станциях, с использованием которых осуществлялась регистрация входящих и исходящих звонков абонента, с указанием следующих технических характеристик: количество секторов (антенных блоков в месте установки), азимут направленности использованных антенных блоков и угол охватываемой ими территории; о входящих и исходящих платежах по лицевому счету абонентского номера; об использовании мессенджеров и др.

Содержатся в рекомендациях перечень сведений, которые можно получить, в частности: по банковским картам и расчетным счетам, по электронным кошелькам, по сайтам объявлений, по социальным сетям, по

доменному имени сайта, по электронной почте; сведения, запрашиваемые у Интернет-провайдера, у провайдера SIP- телефонии.

Все это правильно и, безусловно, должно содержаться в методических рекомендациях для оперативных подразделений, работающих по раскрытию киберпреступлений.

Однако информация доказательственного характера об обстоятельствах совершенных IT-преступлениях содержится не только в информационной среде.

Прежде чем проиллюстрировать на конкретных примерах потребность использования содействия граждан в выявлении и раскрытии, к примеру, дистанционного мошенничества, важно сделать посылку методологического характера. Для оперативно-розыскной деятельности характерно то, что оперативно значимой является не только информация о событии преступления, но и информация о том, что с этим преступлением связано, что ему предшествовало, и что ему сопутствовало. А это не всегда информация о противоправных деяниях как таковых. Но именно такого рода информация зачастую способствует установлению лиц, совершивших деяния, подпадающие под признаки преступных.

Действия лиц, которые каким-либо образом, даже косвенно связаны с преступной деятельностью в теории оперативно-розыскной деятельности называют по-разному - криминальная активность, криминальное поведение. Оно выражается в разных формах – например, создание условий для преступлений, склонность к преступной деятельности, ее поддержка, обучение преступников, оказание им содействия и т.д.

К тому же особенностью деятельности оперативного сотрудника заключается в том, что ему важно выявить потенциального преступника уже на этапе возникновения замысла совершить преступление, его планирования и подготовки.

Приведем конкретные примеры, подтверждающие потребность в использовании института содействия граждан в раскрытии дистанционного мошенничества, совершаемого преступной группой.

Изучение уголовных дел по указанной категории преступлений позволяет представить, как действует типичная преступная группа, совершающая мошенничество дистанционно с использованием информационных технологий, из кого она состоит и как распределяются роли. И, соответственно, где и какую информацию о деятельности участников группы и их связей следует искать. Особенности ее функционирования определяют следующие характеристики преступной группы, имеющие, кстати, значение для квалификации преступлений (например, вменение преступного сообщества):

Из представленных далее характеризующих группу сведений становится понятно, что без помощи содействующих лиц собрать доказательства ее преступной деятельности практически невозможно.

Во-первых, это наличие руководителя, который осуществляет общее руководство и координацию деятельности членов группы, распределяет между

ними преступные роли и прибыль, полученную в результате совершения преступлений. Информация о такой деятельности образуется явно не в информационном пространстве.

Во-вторых, соблюдение правил конспирации и мер безопасности – запрет членам преступной группы на использование за пределами арендованных офисов и использование в личных целях «рабочих» средств связи и сим-карт. Кстати, в качестве доказательств по таким делам выступают договоры аренды на офисные помещения. Соответственно эти помещения кто - то подбирал, договоры заключал. Значит, имеются лица – носители информации о таких действиях.

В-третьих, использование в преступных целях сим-карт и банковских карт, а также Интернет-сайтов, зарегистрированных на имя третьих лиц; регулярная смена сим-карт и банковских карт; привлечение в качестве новых членов группы знакомых и родственников.

В-четвертых, жесткая внутренняя дисциплина – постоянный контроль со стороны руководителя преступной группы за соблюдением рядовыми ее членами режима рабочего дня и мер конспирации; установление системы учета всех поступивших доходов, заключающейся в регулярном предоставлении руководителю отчетов о проделанной работе, в том числе, в целях пресечения попыток рядовых участников присвоить похищенные деньги. Как правило, ведутся рукописные записи в тетрадях, отражающие доходы и расходы группы.

В-пятых, устойчивость внутренних связей между членами группы, которое выражается в наличии между многими из них родственных, семейных и дружеских связей, возникших еще в детстве и юности. Среди таких людей достаточно много носителей информации, хотя сами они и не принимали непосредственного участия в преступной деятельности.

В-шестых, существование членов группы на денежные средства, добытые преступным путем. Никто из преступников, как правило, не имеет законного источника дохода. В преступном сообществе формируется общая денежная касса, средства из которой тратятся на аренду офисных помещений, приобретение мебели и оргтехники, приобретение средств связи, банковских карт и сим-карт, оплату услуг сотовой связи и Интернет-провайдеров, оплату за создание Интернет-сайтов и их продвижение, на выдачу заработной платы.

Таким образом, нетрудно прийти к выводу, что уклон разработчиков методик раскрытия киберпреступлений в сторону поиска только цифровых следов надо как-то преодолевать и более активно думать надо тем, как использовать эффективный по своей сути оперативно-розыскной институт содействия граждан в поиске преступников, свидетелей, вещественных доказательств в процессе раскрытия и расследования IT-преступлений.

УДК 347

К ВОПРОСУ ОБ УДОСТОВЕРЕНИИ НОТАРИУСОМ СДЕЛОК В ЭЛЕКТРОННОЙ ФОРМЕ

Дадаян Елена Владимировна,
кандидат юридических наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: dadaelena@yandex.ru

Сторожева Анна Николаевна,
кандидат юридических наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: storanya@yandex.ru

Аннотация: *в настоящей статье авторами поднимается вопрос о возможностях использования цифровых технологий в деятельности нотариуса. Так, цифровые технологии позволяют решить вопрос об удостоверении сделок в электронной форме. Делается вывод, что любая цифровая технология (информационный сервис) окажется эффективной только тогда, когда будет продуман до мельчайших подробностей алгоритм ее внедрения, начиная с правового закрепления процедуры ее применения.*

Ключевые слова: *цифровые технологии, нотариус, удостоверение, сделка, электронная форм, информационные сервисы.*

ON THE ISSUE OF NOTARY CERTIFICATION OF TRANSACTIONS IN ELECTRONIC FORM

Dadayan Elena Vladimirovna
candidate of legal sciences
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: dadaelena@ yandex.ru

Storozheva Anna Nikolaevna
candidate of legal sciences
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: storanya@yandex.ru

Abstract: *in this article, the authors raise the question of the possibilities of using digital technologies in the activities of a notary. Thus, digital technologies make it possible to solve the issue of certifying transactions in electronic form. It is concluded that any digital technology (information service) will be effective only*

when the algorithm of its implementation is thought out to the smallest detail, starting with the legal consolidation of the procedure for its application.

Keywords: *digital technologies, notary, certificate, transaction, electronic forms, information services.*

Специалист в любой сфере профессиональной деятельности должен не только иметь представления о применяемых информационных технологиях, но и уметь получать, анализировать значимую информацию из различных источников для решения актуальных и повседневных задач профессиональной деятельности [1].

Активное развитие цифровых технологий, оказывающих влияние на все сферы жизни общества не обошло вниманием нотариальную сферу деятельности.

Безусловно, использование современных цифровых технологий и информационных сервисов способствует оперативному и юридически защищенному действию по заключению сделок между субъектами гражданского оборота. Так, после ознакомления участников с проектом составленного документа (проект сделки), каждая из сторон подписывает экземпляр сделки в электронной форме с использованием простой электронной подписи, а также экземпляр на бумажном носителе, который остается в делах нотариуса, удостоверившего договор [2]. Завершающим этапом является подписание нотариусами экземпляров сделки, усиленными квалифицированными электронными подписями с последующим внесением информации о совершенном нотариальном действии в реестр единой информационной системы нотариата, а также оплата тарифа и услуг правового и технического характера каждым из заявителей. За совершение указанного нотариального действия нотариусы будут нести солидарную ответственность. Следует отметить, что при отчуждении недвижимого имущества один из нотариусов должен находиться в том субъекте Российской Федерации, где расположен объект недвижимости. Нотариальное действие, совершаемое в электронной форме, имеет ряд преимуществ [3].

Конечно, наряду с положительными моментами удостоверение сделок в электронной форме имеет ряд трудностей. Сложности, прежде всего заключаются в том, что требуется не только соответствующий алгоритм и техническое оснащение (бесперебойная работа компьютеров, специальное программное обеспечение с высоким уровнем защиты от несанкционированного доступа третьих лиц), но и наличие у участников сделки квалифицированной электронной подписи. На сегодняшний день отсутствуют какие-либо серьезные сложности в получении такой подписи, требуются лишь финансовые возможности. Поэтому, для большинства граждан получение квалифицированной электронной подписи не актуально, а значит, такая возможность удостоверения сделок в электронном виде для них отсутствует.

Отсюда можно сделать вывод, что в большей части актуально удостоверение сделок в электронной форме лишь для индивидуальных предпринимателей и юридических лиц.

Следует обратить внимание, что многие удостоверяющие центры готовы за 15-20 минут организовать деятельность по созданию электронной подписи под ключ. Поэтому в данной сфере не исключаются недобросовестные действия. Так, электронная подпись может быть выдана не тому лицу, на кого она оформлена, это к вопросу о безопасности и должном внимании каждого гражданина не только к своим документам, но и к месту хранения сертификата ключа.

Поэтому, все указанное выше, безусловно, на практике замедляет процессы активного внедрения новых цифровых технологий. Представляется, что любая цифровая технология (информационный сервис) окажется эффективной только тогда, когда будет продуман до мельчайших подробностей алгоритм ее внедрения, начиная с правового закрепления процедуры ее применения.

Список литературы

1. Дадаян, Е.В., Сторожева, А.Н. К вопросу о роли информационных технологий в решении задач профессиональной деятельности / Е.В. Дадаян, А.Н. Сторожева // Применение в юриспруденции современных технологий: актуальные вопросы теории и практики. Красноярск, 2021. С.2.

2. Степаненко, О.Г., Самцов, А.В. К вопросу об обязательном нотариальном удостоверении сделок с недвижимостью / О.Г. Степаненко, А.В. Самцов // Глаголъ правосудия.2019. № 2 (20). С.10-13.

3. Тресцова, Е.В. Права на недвижимое имущество и их обеспечение в механизме осуществления нотариальной деятельности / Е.В. Тресцова // Бюллетень нотариальной практики. 2017. № 1. С. 46- 48.

УДК 343.97

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПНОСТИ И ИНФОРМАЦИОННЫЕ УГРОЗЫ ЛИЧНОСТИ

Далгалы Татьяна Александровна,
кандидат юридических наук, доцент
Южно-Уральский государственный университет
(Национальный исследовательский университет),
г. Челябинск, Россия
email: tanya.rodionova@gmail.com

Аннотация*: в статье рассмотрен ряд аспектов, связанных с ключевыми понятиями «информационные угрозы», «информационная безопасность», «кибербезопасность», «противодействие преступности». Определяется необходимость разработки комплекса мер, направленных на укрепление информационной безопасности в условиях возможных вызовов и угроз, что позволит наиболее эффективно противодействовать преступности.*

Ключевые слова*: информационные угрозы, кибербезопасность, информационная безопасность, противодействие преступности, информационные угрозы личности.*

COUNTERACTION CRIME AND INFORMATION THREATS TO THE PERSON

Dalgaly Tatyana Aleksandrovna,
candidate of legal sciences, associate professor
South ural state university (National research university),
Chelyabinsk, Russia
email: tanya.rodionova@gmail.com

Abstract: *the article considers a number of aspects related to the key concepts of "information threats", "information security", "cyber security", "crime counteraction". The necessity of developing a set of measures aimed at strengthening information security in the face of possible challenges and threats, which will most effectively counteract crime, is determined.*

Keywords: *information threats, cybersecurity, information security, crime prevention, information threats to the individual.*

Информационные угрозы личности в настоящее время представляют собой наиболее актуальную проблемы обеспечения информационной безопасности и противодействия преступности как в России, так и во всем мире. Существенное возрастание масштаба и интенсивности информационного воздействия на личность определяет основные тенденции уголовной политики государств в противодействии преступности и обеспечения информационной

безопасности страны. Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.

В настоящее время под информационными угрозами принято понимать, например, атаки программного обеспечения, хищение информации, нарушение требований конфиденциальности данных и т.д. По сути, цель противодействия преступности от информационных угроз личности состоит в том, чтобы защитить личную информацию от несанкционированных действий. Необходимость противодействия преступности от информационных угроз личности обусловлена, например, потребностью личности в защите персональных данных, обеспечением безопасной работы устройств и программ, обеспечением финансовой и интеллектуальной безопасности личности.

Как показали научные исследования [1], следует отличать информационную безопасность от кибербезопасности. Нередко эти два термина используются взаимозаменяемо, однако они все же отличаются как масштабом, так и целью. Информационная безопасность категория более широкая и включает в себя кибербезопасность. Последняя касается в первую очередь угроз, связанных с только технологиями. Доктрина информационной безопасности Российской Федерации [2], утвержденная Указом Президента РФ № 646 от 5 декабря 2016 года, определяет информационную безопасность как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

В Российской Федерации в 2011 году была создана Межведомственная Комиссия Совета Безопасности Российской Федерации по информационной безопасности. Основными направлениями ее деятельности являются подготовка предложений и рекомендаций Совету Безопасности по выработке и реализации основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации; анализ информации о состоянии информационной безопасности Российской Федерации; прогнозирование, выявление и оценка угроз информационной безопасности Российской Федерации и их источников, подготовка предложений и рекомендаций Совету Безопасности по предотвращению выявленных и недопущению прогнозируемых угроз в области обеспечения информационной безопасности Российской Федерации и другие. В феврале 2023 года на заседании Комиссии было отмечено, что необходимо разработать комплекс мер, который будет направлен на укрепление информационной безопасности в условиях возможных вызовов и угроз, что позволит наиболее эффективно противодействовать преступности.

Вместе с тем необходимо отметить, что в условиях стремительного развития технологий и киберпространства правоохранительных органа

становится все сложнее адекватно и эффективно противодействовать данным угрозам личности. Об этом, в частности, свидетельствует рост зарегистрированных преступлений в сфере информационных технологий.

Таким образом, необходимо отметить возрастающую роль и значимость противодействия преступности в сфере информационных угроз личности и обеспечения информационной безопасности как одного из приоритетов обеспечения национальной безопасности Российской Федерации.

Список литературы

1. Матяш, С.А. Информационная безопасность личности как социальная проблема современности / С.А. Матяш // Вестник Университета (Государственный университет управления). 2013. №8. С.38-45.

2. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646: Доктрина информационной безопасности Российской Федерации // СПС «КонсультантПлюс».

УДК 165.24

ЭКЗИСТЕНЦИАЛЬНОСТЬ ЧЕЛОВЕКА В СОВРЕМЕННОМ ВЫСОКОТЕХНОЛОГИЧНОМ МИРЕ

Даниелян Наира Владимировна,
доктор философских наук, доцент
Национальный исследовательский университет
«Московский институт электронной техники»,
г. Москва, Россия
e-mail: vend22@yandex.ru

Аннотация: *в статье проводится сравнительный анализ восприятия человеком своего существования в классической философии и в современном высокотехнологичном мире. Автор полагает, что одной из ключевых проблем является осмысление взаимоотношений человека и машины с позиции правильности распределения функций между ними. Проникновение технологий во все сферы человеческой жизни рассматривается на примерах виртуальной и дополненной реальности, а также искусственного интеллекта. В статье сформулирован вывод, что наиболее актуальным вопросом ближайшего времени становится не только техническая деятельность сама по себе, которая направлена на создание материальных благ и искусственной среды обитания, но и осмысление человеком своего существования в этом мире и места в нем.*

Ключевые слова: *человек, проблема существования, мышление, высокие технологии, виртуальная среда, искусственный интеллект.*

HUMAN EXISTENTIALITY IN MODERN WORLD OF HIGH TECHNOLOGIES

Danielyan Naira Vladimirovna,
doctor of philosophy, associate professor
National research university of electronic technology,
Moscow, Russia
e-mail: vend22@yandex.ru

Abstract: *the comparative analysis of human perception of his being in classic philosophy and the modern world of highly developed technologies is carried out in the article. According to the author, one of the key challenges is to cognize the relationships between a human being and a machine and separate their functions correctly. The technological penetration in all spheres of our life is examined of the examples of virtual reality (VR), augmented reality (AR), and artificial intelligence (AI). The author concludes that the most topical issue of the near future is not only technical activity per se being directed at the production of material welfare and the artificial environment for the humanity, but man's cognition of his existence in the world and his position in it.*

Keywords: *person, existence, thinking, high technology, virtual environment, artificial intelligence.*

Две основы восприятия человеком своего существования были заложены в работе И. Канта «Критика практического разума»: «Две вещи наполняют душу всегда новым и все более сильным удивлением и благоговением, чем чаще и продолжительнее мы размышляем о них, – это звездное небо надо мной и моральный закон во мне. И то и другое мне нет надобности искать и только предполагать, как нечто окутанное мраком или лежащее за пределами моего кругозора; я вижу их перед собой и непосредственно связываю их с сознанием своего существования» [1, с. 499].

Сегодня в свете все большего проникновения высоких технологий во все сферы жизни общества особую актуальность приобретают вопросы, связанные с осмыслением их применения. Под их влиянием бытие человека трансформируется, все больше переходя в сферу «искусственного», подвергая важность и необходимость понимания его существования сомнению. Рассмотрим данный вопрос более подробно.

Как мы воспринимаем мир сегодня? Все более как виртуальную среду, предоставляемую нам через сотовый телефон, ноутбук, планшет, монитор компьютера. Нам все меньше дела до «звездного неба над головой» и «морального закона во мне». Коммуникация в чатах, просмотр блогов и прочий информационный контент становятся средой обитания человека в цифровую эпоху. Навыки мышления человеком утрачиваются, их вытесняет «жвачка-мысль», которую Ж.-П. Сартр определял как «Я СУЩЕСТВУЮ» [2, с. 118], а мы сегодня можем определить как «Я ПОТРЕБЛЯЮ», будь то услуги, информация, материальные блага. Таким образом, общество потребления налицо, что имеет достаточно негативную тенденцию в свете замещения не

только физического, но и интеллектуального труда человека искусственными системами, которые несут с собой по мере их невероятно быстрого совершенствования и развития все большие риски для его благополучия.

Здесь появляется целый круг вопросов, связанных с проблематикой распределения функций между человеком и машиной вследствие их все более тесного взаимодействия. Н. Винер, основатель кибернетики, полагал: «Отдайте человеку – человеческое, а вычислительной машине – машинное. В этом и должна, по-видимому, заключаться разумная линия поведения при организации совместных действий людей и машин» [3, с. 212].

Сегодня трудно сказать, насколько человечество в будущем будет следовать данной «разумной линии поведения», так как сегодня компьютерные технологии все больше проникают во все сферы нашей деятельности. В качестве примера рассмотрим дополненную реальность (AR).

Многие люди сегодня пользуются технологиями AR в разных музеях и выставочных комплексах по всему миру. При наведении телефона на код объекта, пользователь может мгновенно получить информацию как теоретического, так и практического характера о нем, включая последние разработки. Если установить соответствующее приложение, такое как Google-переводчик, то можно получить мгновенный перевод надписи на любой из загруженных в него языков. На лекциях и практических занятиях в разных университетах мира используют очки виртуальной реальности (VR), которые помогаю не только проиллюстрировать, но и «оживить» изучаемый материал [4, с. 29].

Эти примеры демонстрируют, что в современном мире, в частности, благодаря появлению виртуальной среды посредством соответствующих технологий, исчезает необходимость в посреднике между человеком и компьютерный устройством. Они взаимодействуют таким образом, что действие человека перестает быть внешним. Оно превращается в неотъемлемую часть системы. Можно заключить, что человек становится частью системы и включается в поле ее возможных состояний. Как результат, существование человека более не является внешним по отношению к системе, это ее неотъемлемая часть.

Далее снова вернемся к «довысокотехнологичному» миру и рассмотрим, как проблема существования человека представлена во французском экзистенциализме в лице его яркого представителя Ж.-П. Сартра на примере произведения «Тошнота». Единственное, в чем человек может найти смысл своего бытия по Сартру, – это свобода осмысления и осознания своего существования. «Моя мысль – это я: вот почему я не могу перестать мыслить. Я существую, потому что мыслю, и я не могу помешать себе мыслить» [2; с. 119]. В такой постановке вопроса «экзистенция» предстает в земном, конечном виде. Нет человека – нет мысли, таким образом, решение проблемы кроется в «экзистенциально-онтологической постановке вопроса как единственно адекватного подхода к ее проблематике» [5, с. 117]. Однако так ли это сегодня, когда речь начинает идти о все более широком применении технологий искусственного интеллекта (ИИ)?

Давайте вдумаемся в сам термин – искусственный интеллект (ИИ). Так как речь идет о создании некоего аналога человеческого интеллекта, то ему должны быть присущи сознание и мышление, то есть ученым, инженерам, разработчикам необходимо добиться когнитивной имитации процессов, которые происходят в человеческом мозге.

В литературе можно найти описание двух версий ИИ: «Сторонники слабой версии теории ИИ считают, что соответствующим образом запрограммированный компьютер может только моделировать мыслительные акты человека, в то время как сторонники сильной версии допускают, что запрограммированные компьютерные устройства действительно мыслят и в силу этого могут находиться в соответствующих когнитивных состояниях» [6, с. 669]. Последнее утверждение является крайне спорным, так как означает наделение компьютеризированного устройства способностью мыслить. С. Ллойд и Дж. Энджи описывают пример непосредственного обмена информацией между человеком и компьютером со встроенным нейроинтерфейсом [7]. Появление подобных устройств означает большой шаг вперед в области создания сильного ИИ. Таким образом, мышлением и существованием будет наделено не только естественное, но и искусственное. Уже не только для нас станет возможна постановка вопроса о таком критерии существования, как мышления, что коренным образом меняет всю онтологически-гносеологическую плоскость экзистенции человека.

Выводом мог бы стать ответ на вопрос, возвышают ли технологии человека. Нельзя отрицать, что они помогают человеку, делая его труд более качественным и профессиональным. Так, в области права, как отмечает Л.В. Бертовский в статье «Высокотехнологичное право: понятие, генезис и перспективы», «использование юристами высокотехнологичных информационно-коммуникационных систем… позволяет повышать результативность принятия законов, которых на сегодняшний день на территории Российской Федерации действует около 2400, и обеспечивать эффективность их применения» [8, с. 740]. Также ярким примером положительного влияния высоких технологий на деятельность человека и повышение ее качества является машинное обучение роботов, при создании которых используются искусственные нейронные сети. Они одновременно способны не только перерабатывать огромное количество вхолной информации, но и сохранять результат по технологии безличного знания, т.к. все выводные результаты распределяются сетью и используются при дальнейшем функционировании системы. С.А. Диане справедливо отмечает, что «переход на новый качественный уровень позволяет сместить акцент исследований от решения частных прикладных задач к построению универсальных информационно-управляющих систем» [9, с. 319].

С другой стороны, они несут угрозу индивидуальности человека и самому его существованию. Так, по мнению В.Г. Горохова, «научно-технический прогресс открывает не только новые возможности для принятия решений, но и принуждает к определенным решениям со своими собственными рисками» [10, с. 17]. Как было показано в данной статье, наиболее важной в современном

мире становится техническая деятельность, посредством которой создаются материальные блага и появляется искусственная среда обитания. Однако она также влияет на осмысление человеком своего существования в этом мире и места в нем. Целью технологий может быть, как положительное, так и отрицательное воздействие на человека и общество. Поэтому наиболее актуальным на сегодняшний день становится вопрос, в каком направлении данная деятельность человека направит социальный прогресс: созидательном или деструктивном.

Список литературы

1. Кант, И. Критика чистого разума / И. Кант // Сочинения в шести томах. М.: «Мысль», 1965.Т. 4, ч. 1. С.311-501.
2. Сартр, Ж.-П. Тошнота; Стена; Слова; Ставок больше нет: сборник: перевод с французского / Ж.-П. Сартр. М.: Издательство АСТ, 2020. 608 с.
3. Винер, Н. Кибернетика и общество. Творец и робот / Н. Винер. М.: Тайдекс Ко, 2003. 248 с.
4. Зильберман, Н.Н. Возможности приложений дополненной реальности в образовании / Н.Н. Зильберман, В.А. Сербина // Открытое и дистанционное образование. 2014. № 4 (56). С.28-33.
5. Хайдеггер, М. Бытие и время: Пер. с нем. В.В. Бибихина / М. Хайдеггер. М.: Академический проект, 2015. 460 с.
6. Меркулов, И.П. Мышление с точки зрения компьютерной эпистемологии / И.П. Меркулов // Субъект, познание, деятельность: К 70-летию В.А. Лекторского. М.: «Канон+» РООИ «Реабилитация», 2002. С. 664-683.
7. Ллойд, С. Сингулярный компьютер / С. Ллойд, Дж. Энджи // В мире науки. Физика. 2005. № 2. С. 33-42.
8. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский // Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. № 4. С. 735-749.
9. Диане, С.А. Обучение и социальная интеграция автономных роботов на основе применения современных когнитивных технологий / С.А. Диане // Философия и социология техники в XXI веке. К 70-летию В. Г. Горохова / под общ. редакцией И.Ю. Алексеевой, А.А. Костиковой, А.Ф. Яковлевой. М.: Аквилон, 2018. С. 316-321.
10. Горохов, В.Г. Новая жизнь «искусственного интеллекта» в проблеме искусственного усовершенствования человека / В.Г. Горохов // Естественный и искусственный интеллект: методологические и социальные проблемы / под ред. Д.И. Дубровского и В.А. Лекторского. М.: «Канон +» РООИ «Реабилитация», 2011. С. 17-47.

УДК 343.1

О ПРОБЛЕМЕ ПЕРЕВОДА ИЗ МАШИНОЧИТАЕМОЙ ФОРМЫ ИНФОРМАЦИИ В ЧЕЛОВЕКОЧИТАЕМУЮ И ПРИНЯТИЕ НА ОСНОВАНИИ НЕЕ СУДЕБНОГО РЕШЕНИЯ

Девяткин Генрих Сергеевич
кандидат юрид. наук, заместитель директора института высокотехнологичного права, социальных и гуманитарных наук
Национальный исследовательский университет «МИЭТ»
г. Москва, Россия
e-mail: devyatkings@gmail.com

Аннотация: *рассматриваются некоторые правовые и технические вопросы использования высоких технологий при принятии судом решений, анализируется проблема обоснования «мотивированности» текста, сгенерированного искусственным интеллектом. Сформулированы рекомендации по возможности использования высокотехнологичных инструментов в судопроизводстве.*

Ключевые слова*: высокотехнологичное право, машиночитаемое право, обработка информации, судебный акт, анализ текста, искусственный интеллект, нейросети.*

ABOUT THE PROBLEM OF TRANSFERRING INFORMATION FROM A MACHINE-READABLE FORM TO A HUMAN-READABLE ONE AND MAKING A COURT DECISION BASED ON IT

Devyatkin Genrikh Sergeevich
candidate of law sciences, deputy director of the institute of high-tech law, social sciences and humanities,
National research university of electronic technology (MIET)
Moscow, Russia
e-mail: devyatkings@gmail.com

Abstract*: Some legal and technical issues of the use of high technologies in court decision-making are considered, the problem of substantiating the "motivation" of the text generated by artificial intelligence is analyzed. Recommendations on the possibility of using high-tech tools in legal proceedings are formulated.*

Keywords*: high-tech law, machine-readable law, information processing, judicial act, text analysis, artificial intelligence, neural networks.*

За последние несколько лет высокие технологий активно внедряются в повседневную жизнь судей, адвокатов, прокуроров, органов следствия, а также иных участников судопроизводства. Высокотехнологичное право полноценно функционирует и развивается, наступила новая «юридическая революция» [1].

Но что следует считать высокими технологиями: видеоконференцсвязь и возможность использовать усиленную квалифицированную электронную подпись? Безусловно некоторые элементы цифровизации уже внесены в российское судопроизводство, но присутствует ли в нем искусственный интеллект и нейросети. Так, в 2023 году в Колумбии судья использовал нейросеть для получения информации, на основе которой вынес судебное решение. Рассматривалось дело о покрытии расходов на медицину и транспорт для ребенка с расстройством аутистического спектра. Предстояло выяснить, должны ли все расходы покрываться страховкой, так как родители ребенка не могли позволить себе это. Судья спросил у нейросети, следует ли освободить семью ребенка от платы за лечение. Нейросеть ответила, что согласно законам Колумбии, несовершеннолетние с аутистическим расстройством освобождаются от платы за терапию [2].

Возможно ли применение искусственного интеллекта, нейросетей судьями в России? Технически любой участник судопроизводства способен установить компьютерную программу, например, для оценки вероятности исхода судебного дела на основе анализа больших данных. Данные приложения следует установить на смартфон, указать вводную информацию (сведения об участниках, суть спора, иные данные), после чего программа предложит возможный результат. В этом случае разработчик приложения загрузил из открытых источников (картотеки арбитражных дел, ГАС «Правосудие» и т.д.) информацию, установил необходимые алгоритмы ее обработки и принятия решения. Данные программы актуальны при рассмотрении судебных дел, где есть спор о праве. Адвокаты вправе использовать такие приложения уже сейчас. Например, необходимо понять, какое решение вынесет конкретный судья по делу об административном правонарушении. Загрузив в программу информацию о судье, а также рассматриваемом споре, адвокат за несколько секунд увидит на экране смартфона, что выбранный судья в 90 % случаях по данному делу назначает наказание, связанное с административным арестом на срок 10 суток. Приложение проанализирует все похожие дела, которые рассмотрел именно данный судья. Полученная информация не ограничивается статистическими результатами. При необходимости адвокат способен получить более детализированные варианты исхода дела его доверителя.

Является ли автоматизированная обработка судебных актов неприемлемой для правоприменителя в России? Прямого запрета для судьи использовать такие программы не предусмотрено. В той или иной мере суд при анализе обстоятельств дела может воспользоваться различными инструментами. Хотя бы калькулятором для оценки размера неустойки с учетом ключевой ставки Центрального Банка РФ. Либо проанализировать алгоритм работы компьютерной программы, вокруг которой происходит спор истца правообладателя и недобросовестного ответчика. Правоприменители перестали быть исключительно юристами по причине активного распространения высокотехнологичного права. Но какие последствия будут для судебного акта, который был принят судом с учетом «подсказок» от нейросети? Наличие в судебном решении строки о том, что судья использовал программу,

скорее всего, позволит проигравшей стороне отменить судебный акт в вышестоящей инстанции.

Согласно гражданскому процессуальному кодексу (далее – ГПК РФ) суд оценивает доказательства по своему внутреннему убеждению, основанному на всестороннем, полном, объективном и непосредственном исследование имеющихся в деле доказательств. В соответствии со ст. 17 Уголовно-процессуального кодекса судья, присяжные заседатели, а также прокурор, следователь, дознаватель оценивают доказательства по своему внутреннему убеждению. Статья 195 ГПК РФ предусматривает наличие обязательных признаков законности и обоснованности решения суда. Постановление Пленума Верховного Суда РФ от 19.12.2003 № 23 «О судебном решении» также не содержит запретов или ограничений на использование вспомогательных инструментов судьи для принятия им законного и обоснованного решения, с учетом своего внутреннего убеждения.

В совокупности отсутствие запрета равно и дозволения на вспомогательные программы ориентирующего характера создают правовую неопределенность именно для судей. Использование нейросетей остальными участниками судопроизводства является дополнительной возможностью получить больше информации по делу и построить на основе этого свою позицию.

О перспективах развития высокотехнологичных инструментов можно уверенно говорить с учетом концепции машиночитаемого права, которое согласно «Концепции развития технологий машиночитаемого права» [3] к 2030 году должно быть внедрено в судопроизводство. Машиночитаемое право включает в себя нормы права, которые изложены на формальном языке - на языках программирования и разметки текста, применимых для ЭВМ. Кроме того, в машиночитаемое право входят инструменты применения таких норм: информационные системы и программное обеспечение. Благодаря этим технологиям, нормативно-правовые акты переводятся в компьютерный код.

Машиночитаемое право будет востребовано в законотворчестве, судопроизводстве, при заключении сделок, стандартизации и сертификации. Так, искусственный интеллект сможет сопоставлять тексты разных правовых актов и автоматически выдавать юристам применяемые нормы. Машиночитаемое право незаменимо в судебных делах без спора о праве. Например, при вынесении судебных приказов. Пилотный проект внедрения автоматизированных систем для подготовки судебных приказов стартовал в 2021 году в Белгородской области.

Несомненными преимуществами машиночитаемого права являются: повышение объективности, сокращение сроков, доступность правовых документов. К возможным минусам относится: сырая инфраструктура, удаление цифровых профилей (проблема «цифровой смерти пользователей».

В любом случае при использовании нейросети любым участником судопроизводства необходимо понимать принципы работы программы, алгоритмы принятия того или иного результата. Первоочередная задача не столько урегулировать в законодательстве возможность внедрения

высокотехнологичных инструментов, сколько обеспечить прозрачность его работы, а также соблюсти права человека [4]. Возвращаясь к судебному кейсу в Колумбии, принятому с учетом позиции нейросети, необходимо понять, были ли у судьи познания в сфере высоких технологий, компетентно ли он оценил алгоритм «действий» нейросети. Представляется, что внедрение в российское судопроизводство искусственного интеллекта допустимо, но только при условии наличия у всех участников минимально необходимого уровня познаний в программировании, математике, алгоритмов работы компьютерных программ, используемых в качестве «ассистентов». Иначе как судья, адвокат, прокурор оценит правильность работы применяемой нейросети? Привлечение специалиста способно решить данную задачу, но о каком высокотехнологичном праве можно говорить без наличия юристов с компетенциями в технике?

Развивая мысль о возможности применения нейросетей, следует предусмотреть возможность наличия одновременно двух версий судебных решений: принятого на основе машиночитаемого права и принятого судьей-человеком (при условии единого результата исхода дела). Это позволит оценить алгоритмы, которые применяла программа, например, при определении размера наказания. Кроме того, решение, принятое при помощи искусственного интеллекта, может быть направлено на так называемое «двойное слепое рецензирование». Рецензентами в данном случае могут выступить автор компьютерной программы либо любой специалист в соответствующей сфере. Необходимо не запрещать высокие технологии, а готовить инфраструктуру под их внедрение, включая техническую подготовку правоприменителей.

Список литературы

1. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский // Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. № 4. С.735-749.

2. Российская газета. Вып. от 03.02.2023. URL: https://rg.ru/2023/02/03/v-ssha-sudia-vynes-prigovor-s-pomoshchiu-chat-bota-chatgpt.html?ysclid=lffmordtxa271405730.

3. Концепция развития технологий машиночитаемого права: утв. Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 15.09.2021. № 31// СПС «КонсультантПлюс».

4. Бертовский, Л. В. Защита прав и законных интересов участников судопроизводства как элемент уголовной политики государства / Л. В. Бертовский // Военно-правовые и гуманитарные науки Сибири. 2020. № 4(6). С. 81-84.

УДК 343.1

ОСОБЕННОСТИ ПРИМЕНЕНИЯ В УГОЛОВНОМ ПРОЦЕССЕ СИСТЕМ ВИДЕО-КОНФЕРЕНЦ-СВЯЗИ СУДАМИ ОБЩЕЙ ЮРИСДИКЦИИ

Донченко Елена Сергеевна,
Красноярский государственный аграрный университет,
г. Красноярск, Россия
email: e.s.donchenko@mail.ru

Научный руководитель: Бертовский Лев Владимирович,
доктор юридических наук, профессор
ФГАОУ ВО «Национальный исследовательский университет «Московский институт электронной техники»
г. Москва, Россия
email: bgl1980@yandex.ru

Аннотация*: проанализированы особенности применения судами общей юрисдикции в уголовном процессе систем видео-конференц-связи, с учетом изменений, внесенных в декабре 2022 года, также рассмотрен опыт США по применению систем видео-конференц-связи, дана оценка влияния видео разбирательств на справедливость и доступ к правосудию в суде.*

Ключевые слова*: видео-конференц-связь, суд, подсудимый, уголовное судопроизводство, предварительное расследование, правосудие, уголовный процесс.*

THE HISTORY OF THE FORMATION OF THE STATUS OF A SUSPECT IN CRIMINAL PROCEEDINGS

Donchenko Elena Sergeevna,
Krasnoyarsk state agrarian university
Krasnoyarsk, Russia
email: e.s.donchenko@mail.ru

scientific adviser: ***Bertovsky Lev Vladimirovich,***
doctor of law, professor
National research university «Moscow institute of electronic technology», Moscow, Russia
email: bgl1980@yandex.ru

Abstract*: the features of the use of video conferencing systems in criminal proceedings by courts of general jurisdiction are analyzed, taking into account the changes made in December 2022, the US experience in the use of video conferencing systems is also considered, the impact of video proceedings on justice and access to justice in court is assessed.*

***Keywords**: video conference call, court, the defendant, criminal proceedings, preliminary investigation, justice, criminal process.*

Принцип непосредственности и устности судебного разбирательства, несомненно вытекает из таких конституционных принципов, как осуществление правосудия только судом, принцип состязательности, обеспечения права на защиту обвиняемому (подсудимому) и других принципов уголовного судопроизводства. Принцип непосредственности и устности судебного разбирательства, является необходимым условием реализации вышеуказанных принципов в уголовном судопроизводстве. Непосредственность и устность судебного разбирательства – важнейшие гарантии достижения задач правосудия. Непосредственное восприятие судом показаний подсудимых, потерпевших, свидетелей предполагает их допрос сторонами и судом в устной форме. В исключительных случаях, когда слушается дело в отсутствие не явившихся свидетелей их показания оглашаются, что является соблюдением принципа устности, но отступление от непосредственности. Если устность – форма общения между судом и участвующими в деле лицами, то непосредственность – необходимый способ восприятия судом доказательств по делу – судоговорение. Данный принцип регламентирован и законодательно закреплен в статье 240 Уголовно-процессуального кодекса Российской Федерации (далее по тексту – УПК РФ) [1].

В декабре 2022 года внесены изменения, которые коснулись общих условий судебного разбирательства, в части принципа непосредственности и устности. Согласно данного принципа в судебном разбирательстве все доказательства по уголовному делу подлежат непосредственному исследованию, за исключением случаев, рассмотрения дела судами в особом порядке. Суд заслушивает показания подсудимого, потерпевшего, свидетелей, заключение эксперта, осматривает вещественные доказательства, оглашает протоколы и иные документы, производит другие судебные действия по исследованию доказательств. В 2011 году была введена 4 часть, дополняющая статью возможностью допроса судом свидетеля и потерпевшего путем использования систем видео-конференц-связи. В настоящее время данная часть изменена, ввиду дополнения уголовно-процессуального кодекса статьей 241.1 «Участие в судебном заседании путем использования систем видео-конференц-связи». Теперь помимо непосредственного участия подсудимого в судебном заседании, предусмотрено, что при наличии технической возможности суд вправе по ходатайству подсудимого принять решение о его участии в судебном заседании путем использования систем видео-конференц-связи. Суд по ходатайству стороны или по собственной инициативе принимает решение об участии в судебном заседании подсудимого путем использования систем видео-конференц-связи также в случае, если имеются обстоятельства, исключающие возможность его участия в судебном заседании непосредственно. Однако данной нормой не раскрыт перечень обстоятельств, исключающих возможность участия, можно ли их отнести к тому перечню, который содержится в

постановления Пленума Верховного Суда РФ от 19.12.2013 г. № 41 [2], или данный перечень не ограничен и остается оценочным на усмотрение суда.

Также предусмотрена возможность участия в судебном заседании подсудимого, содержащегося под стражей, путем использования систем видео-конференц-связи при рассмотрении уголовных дел о тяжких и особо тяжких преступлениях, в целях обеспечения безопасности участников уголовного судопроизводства при наличии технической возможности по ходатайству любой из сторон суд праве принять такое решение. Решение об участии иных лиц, вызванных в судебное заседание, путем использования систем видео-конференц-связи может быть принято судом по ходатайству стороны или по собственной инициативе. В случае участия в судебном заседании подсудимого путем использования систем видео-конференц-связи участие защитника является обязательным. Защитнику обеспечивается возможность беспрепятственного конфиденциального общения с подсудимым, содержащимся под стражей и участвующим в судебном заседании путем использования систем видео-конференц-связи. Установлено, что не допускается участие в судебном заседании подсудимого путем использования систем видео-конференц-связи при рассмотрении уголовного дела с участием присяжных заседателей.

Данной нормой помимо прочего регламентирован порядок установления личность и получении подписки о разъяснении председательствующим судьей прав лицу участвующему путем использования систем видео-конференц-связи.

Однако до настоящего момента остается нерешенным вопрос, каким образом будет обеспечена гарантия конфиденциальности общения подсудимого и защитника.

Данные изменения хоть и носят положительный характер, однако в силу сложившейся практики являются весь запоздавшей мерой реагирования. Рассмотрев на примере материалов уголовного дела, совершенного в сфере информационно-телекоммуникационных технологий, в ходе предварительного расследования было установлено, что Х. находясь по месту своего жительства расположенного в Приволжском Федеральном округе используя информационно-коммуникационную сеть «Интернет» совершил преступление по хищению денежных средств с банковского счета, то есть несанкционированные переводы денежных средств, со счета потерпевшего который находится на территории Сибирского Федерального округа.

Согласно такого рода преступной схеме все фигуранты преступления находятся в разных городах, порой даже в разных регионах Российской Федерации и как правило производство предварительного расследования производится по месту обращения потерпевшего лица, что часто совпадает с местом его жительства, после раскрытия такой категории преступления совершенных посредством информационно-телекоммуникационных технологий, производится задержание лица и доставления его на территорию оперативного обслуживания органа проводившего расследования, ему избирается мера пресечения в виде заключения под стражу, поскольку отсутствует реальная возможность, выполнения ряда следственных действий с

использованием систем видео-конференц-связи, но в большей степени избрание самой строгой меры пресечения продиктовано обеспечением явки такого лица в суд, для рассмотрения дела по существу. В вышеприведенном уголовном деле лицо не заключалось под стражу, была избрана мера пресечения в виде подписке о невыезде и надлежащем поведении, дело было направлено надзирающему прокурору с обвинительным заключением, при этом лицо совершившее преступление осталось по месту своего жительства, уголовное дело было направлено по подсудности в районный суд по месту жительства и месту открытия счета потерпевшей стороны, а денежных средств на перелеты в суд Х. не оказалось, ввиду чего последний столкнулся с ситуацией, когда ему заменили меру пресечения на заключение под стражу, только по причине, что согласно уголовно-процессуального законодательства до декабря 2022 года, подсудимый должен участвовать непосредственно. А также согласно ранее действующего постановления пленума Верховного суда категория таких преступления должна быть рассмотрено в районном суде по месту открытия счета потерпевшей стороны или его места жительства. Перед заключением под стражу, лицом совершим преступление Х. было написано на имя председательствующего судьи ходатайство о передачи уголовного дела в суд по месту его жительства, так как он не имеет материальной возможности прилететь в суд который находится в другом регионе, либо рассмотрения путем применения систем видео-конференц-связи, кроме того, большинство свидетелей находятся по месту его жительства. Судом было отказано, так как это нарушение прав потерпевшей стороны, кроме того, нарушение принципа непосредственности. Однако в материалах уголовного дела имелись сведения о том, что потерпевший не возражает против передачи дела в другой суд, а также действующее на тот момент законодательство содержало норму предусматривающую допрос судом потерпевшего с использованием систем видео-конференц-связи.

На основании вышеизложенного остается открытым вопрос может ли лицо совершившее преступление в сфере информационно-телекоммуникационных технологий рассчитывать на рассмотрение уголовного дела с применением систем видео-конференц-связи, можно ли отнести территориальную отдаленность и отсутствие денежных средств на перелеты к случаям исключающим возможность его участия в судебном заседании непосредственно, а также необходимо только ходатайство обвиняемого для применения судом систем видео-конференц-связи, и будет ли учитываться мнение участвующих лиц, будет ли препятствием если потерпевший будет возражать против такого порядка рассмотрения дела судом, ведь принцип непосредственного участия подсудимого на судебном заседания также остался закрепленным.

Однако не только вопрос о необходимости законодательного закрепления случаев исключающих возможность участия в судебном заседании непосредственно, а также случаев принятия решения судом рассмотрения дела по ходатайству подсудимого с использованием систем видео-конференц-связи, являются основными проблемами в правоприменительной практике, учитывая

в совокупности все положительные результаты введения таких технологий и их обусловленной необходимости, нельзя не отметить и негативные стороны влияние видео-конференц-связи на справедливость и доступ к правосудию в суде. Так, изучая исследования в области психологии, и рассматривая опыт Соединенных Штатов Америки, можно оценить негативные последствия повсеместного применения систем видео-конференц-связи.

Профессор психологии Sara Landstrom, которая изучала видеосвидетельства детей, отмечает: «Можно утверждать, что живые показания, благодаря непосредственного общения, воспринимаются присяжными как более яркие, чем, например, видеосвидетельства, и, в свою очередь, воспринимаются более благосклонно, считаются более достоверными и более запоминающимися» [3]. Аналогичным образом, опираясь на исследования в области коммуникации и социальной психологии, профессор права Anne Bowen Poulin утверждала: «Исследования показывают, что люди оценивают тех, с кем они работают лицом к лицу, более позитивно, чем тех, с кем они работают по видеосвязи. Когда лица, принимающие решения, взаимодействуют с ответчиком через технологический барьер, они, вероятно, будут менее чувствительны к воздействию негативных решений на ответчика». [4] Также в ряде исследований отмечалось смещение перспективы камеры в контексте видео-записанных признаний, обнаружив, что наблюдатели с большей вероятностью поверят, что признание было добровольным, когда камера была сфокусирована только на обвиняемом во время видеозаписи допроса. Кроме того, отмечалось, что из-за нехватки места может потребоваться использование изображения более крупным планом что явно будет преувеличивать черты лица, искажать восприятие размера и возраста человека и скрывать язык тела. Как установил Альберт Мейерабиан, передача информации происходит за счет вербальных средств (только слов) на 7 %, за счет звуковых средств (включая тон голоса, интонацию звука) на 38%, и за счет невербальных средств на 55% [5].

Хотя технология видео-конференц-связи была ценным инструментом во время пандемии Covid-19, существующие научные исследования указывают на причины проявлять осторожность в отношении расширения или долгосрочного внедрения дистанционного судебного разбирательства. Необходимы дополнительные исследования как о потенциальном влиянии дистанционных технологий на результаты в самых разных делах, так и о преимуществах и недостатках в отношении доступа к правосудию. В то же время, по мере разработки судами политики дистанционного судопроизводства, им следует консультироваться с широким кругом заинтересованных сторон, включая государственных защитников и прокуроров, поставщиков юридических услуг, адвокатов жертв и инвалидов, общественных лидеров и ученых-юристов [6].

Нельзя также не отметить, то обстоятельства, что для применения такого рода технологий и активного внедрения их в существующие реалии необходимы соответствующие кадры имеющие специальные познания в данной области, по применению такого рода технологий. Как уже было, верно, указано, что выпускники ВУЗов, в частности, получающих юридическое образование,

выпускаясь, должны обладать бинарными компетенциями: в сфере юриспруденции и высоких технологий [7].

Исходя из анализа действующего законодательства, с учетом внесенных изменений, опыта Соединенных Штатов Америки, можно сделать вывод, что использование систем видео-конференц-связи является исключительной мерой, для которой необходимо законодательное закрепление, возможно не исчерпывающего перечня, но в целом более ориентированного на конкретные случаи, что видится необходимым разъяснить в постановления Пленума Верховного Суда РФ, поскольку такие изменения затрагивают конституционные права граждан на доступ к правосудию. Как отмечает Л.А. Воскобитова, произвольная и безграничная цифровизация уголовно-процессуальной деятельности без учета ее природы, объективно присущих ей особенностей представляется недопустимой, внедрение цифровых технологий должно происходить продуманно и не в ущерб традиционным ценностям и принципам уголовного судопроизводства [8], а также правам человека [9].

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ (ред. от 29.12.2022), (с изм. и доп., вступ. в силу с 11.01.2023 г.) // СПС «КонсультантПлюс».

2. Постановление Пленума Верховного Суда РФ от 19.12.2013 г. № 41 (ред. от 11.06.2020 г.) «О практике применения судами законодательства о мерах пресечения в виде заключения под стражу, домашнего ареста, залога и запрета определенных действий» // СПС «КонсультантПлюс».

3. Landstrom. “Children’s Live and Videotaped Testimonies,” 335. See also Richard E. Nisbett and Lee Ross, L. Human Inference: Strategies and Shortcomings of Social Judgment. (Englewood Cliffs, NJ: Prentice-Hall, 1980).

4. Anne Bowen Poulin, “Criminal Justice and Videoconferencing Technology: The Remote Defendant,” Tulane Law Review 78 (2004): 1118.

5. Пиз, А. «Язык телодвижений» / А. Пиз. С. 5. URL: http://psychologi.net.ru/1/piz_yazik_telodvigenia.pdf (дата обращения: 09.02.2023).

6. Влияние видео разбирательств на справедливость и доступ к правосудию в суде // URL: https://www.brennancenter.org/our-work/research-reports/impact-video-proceedings-fairness-and-access-justice-court (дата обращения: 09.02.2023).

7. Бертовский, Л.В. Проблемы развития высокотехнологичного права / Л.В. Бертовский // Высокотехнологичное право: генезис и перспективы: Материалы III Международной межвузовской научно-практической конференции, Москва-Красноярск, 24–25 февраля 2022 года. Красноярск: Красноярский государственный аграрный университет, 2022. С. 26-29. EDN DAUFGX.

8. Воскобитова, Л.А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости / Л.А. Воскобитова // Lex russica. 2019. № 5 (150). С.91—104.

9. Бертовский, Л. В. Защита прав и законных интересов участников судопроизводства как элемент уголовной политики государства / Л. В. Бертовский // Военно-правовые и гуманитарные науки Сибири. 2020. № 4(6). С. 81-84.

УДК 343.982, 347.948

ОПЫТ РОССИИ И ОТДЕЛЬНЫХ ЗАРУБЕЖНЫХ СТРАН ПО ИСПОЛЬЗОВАНИЮ СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ПРЕДНАЗНАЧЕННОГО ДЛЯ ОБНАРУЖЕНИЯ И ЭКСПЕРТНОГО ИССЛЕДОВАНИЯ МАТЕРИАЛОВ, СОДЕРЖАЩИХ ИНФОРМАЦИЮ О СЕКСУАЛЬНОЙ ЭКСПЛУАТАЦИИ НЕСОВЕРШЕННОЛЕТНИХ

Дорофеев Кирилл Игоревич,
Договорно-правовой департамент Министерства внутренних дел Российской Федерации,
г. Москва, Россия
email: moskowlirik@mail.ru

Аннотация: *автором исследованы возможности современных технологических средств, позволяющих эффективно обнаруживать в информационно-телекоммуникационных сетях, в том числе сети «Интернет», материалы, содержащие информацию о сексуальной эксплуатации несовершеннолетних. Также в статье приведен потенциал существующих аппаратно-программных комплексов, позволяющих решать экспертные задачи при исследовании электронных носителей информации, содержащей указанную запрещенную информацию.*

Ключевые слова: *специальное программное обеспечение, технологии искусственного интеллекта, противодействие распространению материалов с порнографическими изображениями несовершеннолетних.*

EXPERIENCE OF RUSSIA AND INDIVIDUAL FOREIGN COUNTRIES ON THE USE OF SPECIAL SOFTWARE INTENDED FOR DETECTION AND EXPERT STUDY OF MATERIALS CONTAINING INFORMATION ON THE SEXUAL EXPLOITATION OF MINORS

Dorofeev Kirill Igorevich,
MIA Treaty and law department
Moscow, Russia
email: moskowlirik@mail.ru

Abstract: *the author explored the possibilities of modern technological means that allow to effectively detect in information and telecommunication networks,*

including the Internet, materials containing information about the sexual exploitation of minors.

The article also presents the potential of existing hardware and software systems that allow solving expert problems in the study of electronic media containing the specified prohibited information.

***Keywords**: special software, artificial intelligence combating online sexual abuse of children, child sexual abuse materials (CSAM).*

В последнее время мировым экспертным сообществом отмечается увеличение сексуальной эксплуатации несовершеннолетних, совершаемой лицами посредством информационно-телекоммуникационных сетях, в том числе сети «Интернет» (далее – ИТКС, сеть Интернет соответственно).

Изложенное обусловлено развитием цифровой инфраструктуры, удешевлением стоимости услуг по размещению сайтов в сети Интернет (хостинга), созданием и развитием мобильных сетей нового поколения, распространением средств вычислительной техники среди населения.

При этом эффективное противодействие сексуальной эксплуатации несовершеннолетних осложнено активным использованием преступниками современных технологий, позволяющих им скрытно осуществлять противоправную деятельность в ИТКС. К таким технологиям относятся [1]:

сервисы обмена мгновенными сообщениями (мессенджерами), имеющих сквозное шифрование (WhatsApp, Telegram, SnapChat);

технологии по встраиванию программными средствами контейнера с информацией в графический или текстовый файл (стеганография) с целью скрытного обмена сообщениями или материалами с порнографическими изображениями несовершеннолетних [2, с. 185-186];

облачные хранилища информации (Google Drive, Dropbox, iCloud), предоставляющие в режиме реального времени вычислительные мощности для размещения на них зашифрованных объектов, содержащих материалы с порнографическими изображениями несовершеннолетних;

зашифрованные каналы связи в сети Интернет (proxy, VPN), анонимные сети (DeepWeb, DarkWeb), специализированные веб-инструменты, предназначенные для скрытного доступа в ИТКС (TOR, I2P);

расчеты с использованием криптовалют с целью избежать проверки по идентификации личности, проводимой кредитными организациями или платежными системами;

воздействие на ребенка с использованием высококачественных трудно различимых аудиовизуальных подделок (deepfakes) в целях побуждения последнего изготовить порнографические материалы с его изображением и передачи их злоумышленнику.

Анализируемая преступная деятельность характерна и для России, которая может быть подразделена на две группы:

– преступления, связанные с оборотом порнографической информации (часть 3 статьи 242, статьи 242.1, 242.2 Уголовного кодекса Российской Федерации, далее – УК);

– преступления, связанные с насильственными и ненасильственными действиями сексуального характера в отношении несовершеннолетних, а также с сексуальной эксплуатацией несовершеннолетних (статьи 127.1, 131-135, 240, 241 УК).

При этом материалы с порнографическими изображениями несовершеннолетних активно используются в указанных группах преступлений в качестве предмета преступления, средства платежа или обмена, объекта накопления (коллекционирования), орудия совершения иного преступления (шантаж, развратные действия).

Согласно данным ГИАЦ МВД России за последние три года отмечается рост регистрации преступлений, предусмотренных статьей 242.1 УК [3]. Так, в 2020 году было зарегистрировано 551 преступление, в 2021 году – 628, в 2022 году – 898.

В целях противодействия указанным преступлениям в Российской Федерации создана трехуровневая система мониторинга и удаления материалов с порнографическими изображениями несовершеннолетних, а также последующего расследования случаев, содержащих признаки преступлений анализируемого вида.

Так, в соответствии со статьей 15 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор) возложена обязанность по блокированию материалов с порнографическими изображениями несовершеннолетних в ИТКС, а также по ведению реестра доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащих информацию, распространение которой в Российской Федерации запрещено [4].

В целях незамедлительного удаления запрещенной информации, размещаемой в ИТКС, законодательством Российской Федерации [5] на социальные сети, имеющие ежесуточно аудиторию в размере более 500 000 пользователей, возложена обязанность по самостоятельному мониторингу своих серверов с целью выявления и блокирования запрещенной информации, включая материалы с порнографическими изображениями несовершеннолетних. Такие организации в отдельных случаях могут обращаться в Роскомнадзор для решения вопроса об отнесении спорных объектов к категории запрещенной информации. Для учета таких Интернет-платформ создан реестр социальных сетей, ведение которого поручено Роскомнадзору.

В рамках организации указанной деятельности разработаны соответствующие правила взаимодействия между представителями социальных сетей, Роскомнадзором и государственными органами, уполномоченными принимать решение об отнесении спорных объектов к категории запрещенной информации [6].

Выявление и документирование преступлений против половой неприкосновенности и половой свободы личности, в том числе совершаемых злоумышленниками в отношении несовершеннолетних посредством ИТКС, отнесено к компетенции ГУУР МВД России и УБК МВД России [7]. В дополнении к этому между Роскомнадзором и МВД России осуществляется обмен информацией по преступлениям анализируемого вида.

Для противодействия обороту запрещенной информации в ИТКС используется различное программное обеспечение: поисковые веб-сканеры; реестры, содержащие сведения об адресах веб-сайтов и Интернет-страниц, на которых обнаружена запрещенная информация; фильтры по отграничению запрещенной информации от сведений, находящихся в свободном доступе; программное обеспечение, предназначенное для блокирования доступа к сайтам в ИТКС, не предназначенным для ознакомления с их содержанием несовершеннолетними и ряд других.

К методам обнаружения информации с порнографическими изображениями несовершеннолетних, в том числе основанные на технологиях ИИ, относятся:

– использование контрольных сумм (хэширование);

– семантический анализ текста (поиск по ключевым словам);

– алгоритмы распознания и классификации аудиовизуального материала;

– сетевой аналитики;

– специальное программное обеспечение, аппаратно-программные средства и комплексы, отдельные веб-инструменты.

В настоящее время к наиболее эффективным технологическим инструментам для противодействия запрещенной информации в ИТКС относится специальное программное обеспечение, основанное на использовании технологий искусственного интеллекта (далее – СПО, технологии ИИ соответственно). В частности, программные средства, использующие в своей основе нейронные сети, которые позволяют решать узкоспециализированные задачи (например, распознавать образы, текст или речь, осуществлять кластеризацию или анализ данных, оказывать помощь в принятии управленческих решений). Их функциональность повышается при объединении нескольких нейронных сетей (так называемые сверточные нейронные сети) в рамках одного технологического инструмента [8].

Рассмотрим указанные технологические инструменты.

Хэш-значение представлено в виде шестнадцатеричного кода, которое позволяет установить уникальное числовое значение для файла. Вероятность того, что два файла имеют одинаковое значение хеша, рассчитанного с помощью алгоритмов MD5 или SHA-1, крайне мала. Однако данная технология также имеет свои ограничения. Например, хэш-значение файла изменяется, как только файл модифицируется.

В целях нивелирования указанного ограничения, а также для поиска схожих или преобразованных аудиовизуальных материалов создана и успешно используется технология PhotoDNA (компания Microsoft, США), принцип

которой построен на исследовании аудиовизуальных материалов с присвоением определенным его участкам контрольной суммы (хэш-функции), что повышает ее функциональность [9].

Представленная технология используется при сравнении информационных объектов с фото-, аудио- и видеоматериалами, хранящимися в международной базе данных Интерпола ICSE (INTERPOL's International Child Sexual Exploitation database, далее – ICSE).

ICSE представляет собой пополняемое авторизованными пользователями информационную систему, позволяющую по заложенным в нее алгоритмам проводить в мировом масштабе идентификацию личности злоумышленников и их жертв, подвергшихся сексуальной эксплуатации, доступ к которой имеют также отечественные правоохранительные органы.

Вместе с тем возможности PhotoDNA ограничены поиском уже известных и проиндексированных аудиовизуальных материалов.

Для установления ранее неизвестных правоохранительным органам аудиовизуальных материалов используются СПО, основанные на технологиях ИИ. Примером здесь выступает технологический инструмент под названием Griffeye (Швеция), который, используя технологии сверточных нейронных сетей и модель компьютерного обучения, осуществляет сканирование аудиовизуального объекта для распознавания, маркировки и кластеризации изображений и видео с целью обнаружения ранее неизвестных и не проиндексированных материалов с порнографическими изображениями несовершеннолетних.

В частности, указанным СПО при анализе аудиовизуального материала осуществляется определение телесной наготы (цвет кожи, форма обнаженных органов) и возраста изображенных лиц, движения тела людей и звукового ряда с целью отнесения исследуемого информационного объекта к категории порнографических. Кроме того, с помощью данного СПО возможно осуществить доступ к служебной информации файла (EXIF), установить его хэш-значение, собрать биометрическую информацию (изображение лиц и частей тела, образцы голоса) для последующего ее использования при проведении сравнительного анализа аудиовизуальных изображений [10].

Технологический инструмент под названием childsafe.ai (США) использует технологию поиска по ключевым словам (обработки естественного языка) в целях поиска информации о фактах торговли людьми с целью их сексуальной эксплуатации на «закрытых» популярных веб-сайтах коммерческого секса, расположенных в DeepWeb и DarkWeb. Tellfinder (США) осуществляет индексацию и хранение на своих серверах сотни тысяч онлайн-объявлений о сексуальных услугах, позволяя визуально строить связи (графы) на основании телефонных номеров и адресов электронной почты с привязкой к временным и геопространственным метаданным. Такое СПО как Crisp (США), выступает и в качестве программного обеспечения (фильтра), устанавливаемого на мобильное устройство ребенка, и как программное средство, используемое Интернет-платформами социальных сетей и онлайн-игр в целях выявления и

блокирования в режиме реального времени нежелательного общения (сексуализированная переписка, обмен порнографическими материалами) злоумышленников с несовершеннолетними [10].

Опыт использования такого технологического инструмента, как Sweetie 2.0 (Нидерланды), позволяет устанавливать лиц, склонных к совершению сексуальных преступлений, в рамках проводимых поисковых мероприятий в сети Интернет [11].

Существуют и готовые технологические решения, которые объединяют некоторые из перечисленных технологий. Примером здесь может выступить технологический инструмент – NuDetective (Бразилия).

В деятельности Роскомнадзора используется СПО «Окулус» [12], позволяющее автоматизировать процесс поиска запрещенной информации (обрабатывает более 200 000 фото- и видеоизображений в сутки).

Вместе с тем создание универсального СПО в настоящее время представляется затруднительной задачей. Изложенное связано с различиями в законодательной регламентации указанных преступных деяний, что также обусловливает расхождения в терминологии и описательных признаках, используемых правоохранительными органами с целью отнесения исследуемых объектов к категории порнографических (шкалы COPINE, SAP, Sexual Definitive Offences Guideline, CETS, I-KiZ).

Технологии ИИ для автоматизированного поиска и классификации запрещенной информации требуют использования вычислительных мощностей современных центральных процессоров и графических карт, которыми не всегда располагают государственные органы.

В целях повышения результативности технологических инструментов, использующих технологии ИИ, производящие автоматизиронную оценку аудиовизуальных объектов, таким СПО необходимо постоянно обучаться на наборах данных (датасетах), доступ к которым затруднен по этическим и юридическим основаниям.

Представляется, что для решения указанных задач следует объединить усилия академического сообщества (научные методы исследования), промышленности и бизнеса (готовые технологические платформы, наличие необходимого оборудования) и государственных органов (объекты криминалистического учета) для создания таких СПО.

Различные СПО также активно применяются при проведении судебных компьютерных экспертиз (далее – СКЭ), используемых для обнаружения материалов с порнографическими изображениями несовершеннолетних, а также иных цифровых следов, свидетельствующих о противоправной деятельности лиц.

Одним из таких универсальных средств исследования цифровых объектов выступает такие технологические инструменты, как «Мобильный криминалист Эксперт» (компания Oxygen Software, Россия), а также Belkasoft Evidence Center (компания Belkasoft, Россия), возможности которых подробно описаны в специализированной литературе [13, 14].

Применительно к преступлениям анализируемого вида данные аппаратно-программные комплексы позволяют:

осуществлять поиск запрещенной информации по ключевым словам, и контрольным суммам (хэш-значениям);

использовать фильтр определения наготы (установление обнаженных участков кожи на представленных изображениях);

индексировать все аудиовизуальные материалы с последующим извлечением кадров-превью у фото- и видеоизображений;

определять количества видеопотоков в обычном видеофайле в случае намеренного сокрытия лицом запрещенной информации;

работать с вложенными и зашифрованными файлами (например, в Belkasoft Evidence Center внедрены технологии российской компании Passware, предоставляющей услуги по подбору пароля к зашифрованной информации).

В завершении статьи необходимо отметить, что в Российской Федерации создана организационно-правовая и технологическая база, позволяющая эффективно противодействовать преступлениям анализируемого вида. При этом в рамках деятельности по импортозамещению работу по дальнейшему изучению и внедрению в деятельность правоохранительным органов современных технологических средств, основанных на технологиях ИИ, необходимо продолжить.

Список литературы:

1. IWF Annual Report 2018: Once Upon a Year. April 2019 / Internet Watch Foundation website // URL: https://goo-gl.me/A82h3 (дата обращения: 16.02.2023).

2. Радаев, С.В. Комбинированный стеганографический алгоритм встраивания конфиденциальной информации в цифровые изображения формата JPEG / С.В. Радаев, Д.В. Орлов, О.О. Басов // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2017. № 23 (272). С. 185, 186.

3. Единый отчет о состоянии преступности по России / Форма 1-ЕГС. ГИАЦ МВД России// СТРАС «Юрист».

4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 29 декабря 2022 г. № 604-ФЗ) // СЗ РФ. 2006. № 31. Ч. 1. Ст. 3448.

5. Федеральный закон от 30 декабря 2020 г. № 530-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2021. № 1. Ч. 1. Ст.69.

6. Постановление Правительства Российской Федерации от 15 июля 2021 г. № 1192 «Об утверждении Правил рассмотрения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций информации, указанной в пункте 1 части 5 статьи 10.6 Федерального закона «Об информации, информационных технологиях и о защите информации», а также Правил взаимодействия с уполномоченными государственными

органами» // Текст данного нормативного правового акта опубликован на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru).

7. Приказ МВД России от 11 июля 2011 г. № 823 «Об утверждении Положения о Главном управлении уголовного розыска Министерства внутренних дел Российской Федерации»; приказ МВД России от 29 декабря 2022 г. № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-телекоммуникационных технологий Министерства внутренних дел Российской Федерации» // СТРАС «Юрист».

8. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // СЗ РФ.2019. № 41. Ст. 5700.

9. PhotoDNA. Microsoft. Help stop the spread of child exploitation // URL: https://goo-gl.me/nTPG3 (дата обращения: 16.02.2023).

10. Artificial intelligence Combating Online Sexual Abuse of Children / Respect international // URL: https://respect.international.com (дата обращения: 16.02.2023).

11. Schermer, B.W., Georgieva, I., van derHof, S. & Koops, B. J. (2019). Legal Aspects of Sweetie 2.0. In S. van der Hof, I. Georgieva, B. Schermer, & B. J. Koops (Eds.), Sweetie 2.0. Information Technology and Law Series, vol. 31 (pp. 1-94). Springer. DOI:10.1007/978-94-6265-288-0_1(дата обращения: 16.02.2023).

12. Роскомнадзор запустил систему поиска запрещенного контента «Окулус» / Коммерсант // URL: https://goo-gl.me/TdSRT (дата обращения: 16.02.2023).

13. Мобильный криминалист // Oxygen Software. URL: https://goo-gl.me/a4QkD (дата обращения: 16.02.2023).

14. Belkasoft Evidence Center X / Belkasoft. - URL: https://goo-gl.me/iO8ze (дата обращения: 16.02.2023).

УДК 343.1

ВЛИЯНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА ПРОВЕДЕНИЕ ДОПРОСА НЕСОВЕРШЕННОЛЕТНИХ: ПРОБЛЕМНЫЕ ВОПРОСЫ

Дударев Виталий Анатольевич,
старший преподаватель
Брянский государственный университет
имени академика И.Г. Петровского,
г. Брянск, Россия
e-mail: dudarev-vitalii@mail.ru

Аннотация: *в статье рассматриваются проблемные вопросы влияния цифровых технологий на проведение такого следственного действия как допрос. Особое внимание уделено такой категории участников расследования как несовершеннолетние. Представлены как плюсы, так и минусы допроса с применением режима видео-конференц-связи (дистанционного допроса).*

***Ключевые слова*:** *цифровизация, цифровые технологии, допрос, несовершеннолетние, видео-конференц-связь (ВКС), дистанционный допрос.*

THE IMPACT OF DIGITAL TECHNOLOGIES ON THE INTERROGATION OF MINORS: PROBLEMATIC ISSUES

Dudarev Vitaly Anatolyevich,
senior lecturer
Bryansk state university
named after Academician I.G. Petrovsky,
Bryansk, Russia
e-mail: dudarev-vitalii@mail.ru

Abstract: *the article deals with the problematic issues of the influence of digital technologies on the conduct of such an investigative action as an interrogation. Particular attention is paid to such a category of participants in the investigation as minors. Both the pros and cons of interrogation using the video-conferencing mode (remote interrogation) are presented.*

Keywords: *digitalization, digital technologies, interrogation, minors, video conferencing (VC), remote interrogation.*

В последние годы цифровизация и цифровые технологии набирают все большую популярность и актуальность. Цифровые технологии начинаются в простых домашних условиях и заканчиваются разными предприятиями и организациями государственного уровня, что оказывает влияние на всю жизнедеятельность современного человека.

Современные глобальные изменения, экспоненциальное развитие науки и техники, изменение социальных укладов ускорили преобразования и в праве. Новые тенденции активно внедряются и применяются в уголовном

судопроизводстве. Цифровые технологии не только внедряются в уголовный процесс, но и активно его развивают и даже преобразуют.

Как отмечает Л.В. Бертовский «мы вступили в эпоху высокотехнологичного права, под которым понимается такой логистичный, наукоемкий и технологичный регулятор общественных отношений, который, с одной стороны, использует высокие технологии в процессе правоприменения, а с другой – регламентирует возникающие с ними отношения» [3].

Реалии правоприменения требуют ускорения судебных процессов. Поэтому обоснованно выглядит постепенный переход к цифровому судопроизводству – урегулированной нормами процессуального права деятельности суда, участвующих в деле лиц и других участников процесса, а также органов исполнения судебных решений по разрешению юридических дел, в которой ключевым фактором являются данные в цифровом виде, обработка и использование результатов анализа которых по сравнению с традиционными формами судопроизводства позволяют существенно повысить его эффективность [4, с. 10].

Так, в уголовных делах уже активно применяют цифровые носители (как в качестве хранения вещественных доказательств, так и как средство их получения). Благодаря цифровизации активно стала применяться видеоконференцсвязь (далее – ВКС) при осуществлении судебных процессов [19, с. 157], а с принятием новых изменений в УПК РФ и некоторых следственных действий, в частности: допроса, очной ставки, предъявления для опознания (Федеральный закон «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» от 30.12.2021 г. № 501-ФЗ // Собрание законодательства Российской Федерации от 3 января 2022 г. № 1 (часть I) ст. 70).

Касательно уголовного процесса здесь также еще не все стадии доведены до цифрового автоматизма и, как правило, применяются лишь в случаях крайней необходимости. К сожалению, такой необходимостью выступила мировая пандемия коронавирусной инфекции 2019 года (COVID-19) когда практически два последующих года (2020 – 2021) мир и Россия, в том числе вынуждены были работать по большей части удаленно. Это коснулось практически всех отраслей нашего общества. Ведь за пандемией последовали различные ограничения (ношение защитных масок, перчаток, введение QR-кодов). Проведение дистанционных совещаний, семинаров, рассмотрение уголовных дел, дистанционное образование, все это было вынужденной мерой из-за пандемии. Но с дугой стороны, пандемия дала большой скачок для развития цифровых технологий, чтобы сделать возможной удаленную работу общества в пандемийный период.

Однако после отмены ковидных ограничений, следственные органы опять вернулись к стандартному процессуальному порядку расследования уголовных дел и в настоящее время применение таких технологий следователями или дознавателями используется минимально.

Скажем о том, что некоторых странах мира имеется положительный опыт как по внедрению, так и уже по применению цифровых технологий (Киргизия,

Казахстан, Германия, Нидерланды, Саудовская Аравия, Южная Корея) [2,6,8,15,18,20].

По этому поводу справедливо отмечает Ю.Б. Абрамович, что Российская Федерация нуждается в создании общей базы уголовного судопроизводства, которая включала бы в себя такие важные элементы как: фиксация уголовного процесса, при помощи технических средств; сохранение и отражение результатов в электронном виде; применение электронного документооборота; использование дистанционных форм проведения процессуальных действий на всех стадиях судебного разбирательства; предоставление потерпевшему возможности отслеживать на какой стадии разбирательства находится его дело; возможность электронной подписи процессуальных документов участниками процесса и упрощенной системы ее получения; применение электронного помощника судьи, который бы оценивать фактические данные [1, с. 444]. С данными инновационными положениями трудно не согласиться, однако на это нужно определенное время и большие финансовые вложения.

Отметим, что современные цифровые технологии еще не достигли такого уровня развития, чтобы полностью отказаться, например, от бумажных носителей информации. Однако отказ от бумажного документооборота является больше плюсом, чем минусом.

Юридическая литература пестрит публикациями, в которых предлагается переход к цифровым документам (цифровым уголовным делам и базам данных) и отказ от бумажных носителей [9,10,11,13,14]. Конечно, есть свои плюсы в электронном документообороте это и хранение информации, и быстрый доступ к ней, быстрый обмен информацией между различными силовыми службами, ведомствами и судом. Ведь судебной практике известны случаи, когда материалы уголовных дел составляли рекордное количество томов: уголовное дело в отношении Дмитрия Захарченко – 55 томов; уголовное дело Ангарского маньяка – 195 томов, уголовное дело в отношении бывшего сенатора Арашукова – 350 томов и просто немыслимое уголовное дело в отношении преступной группы из 19 человек под руководством Дарьи Щербаковой из Волгограда занимавшейся наркобизнесом – доказательная база по уголовному делу, составила порядка 1000 томов, в общей сложности это более 250 тыс. страниц с описанием допросов, результатов экспертиз и прочими этапами следствия и суда [7, с. 156]. Представим себе на минуту, сколько нужно места для размещения всех этих томов, да еще и времени на его ознакомление.

И если в рамках судебного производства ВКС применяется уже более 20 лет, то так называемый дистанционный допрос в рамках предварительного расследования — это совсем новая норма, которая еще не нашла своего повсеместного применения.

Первые слушания в удаленном режиме посредством ВКС состоялись в ВС РФ по трем уголовным делам 19 апреля 2000 года. Непрерывный сеанс связи был установлен с СИЗО-77/3 Главного управления исполнения наказаний г. Москвы и продолжался около 3-х часов. С того времени в России проведен большой объем работы по оснащению судов федерального уровня системами ВКС для проведения судебных заседаний в режиме видеоконференции. В

настоящее время ВС РФ может работать с любым из федеральных судов. С 2018 года к системе ВКС стали также подключаться судебые участки мировых судей [21].

Как уже было отмечено выше, изменения в уголовно-процессуальный закон 2021 года позволили проводить дистанционный допрос. Однако как отмечается в литературе, проведение допроса по уголовному делу традиционно вызывает ряд не только юридических, но и организационно-технических аспектов. С развитием высоких технологий неизбежно меняются механизмы совершения преступлений, что влечет за собой пересмотр сложившейся практики производства следственных действий. Следователи достаточно осторожно относятся к различным нововведениям при проведении допросов участников по уголовному делу, однако уже сейчас требуются локальные изменения, в первую очередь, связанные с техническими аспектами проведения таких допросов (в первую очередь связанных с таким видом преступности, как – киберпреступность) [5, с. 18].

Одной из проблем проведения дистанционного допроса является тактика его проведения, как правильно технические и тактически провести такой допрос? К сожалению, здесь больше вопросов, чем ответов. Опрос следователей, дознавателей МВД и следственного комитета по Брянской области показал, что никто их них в течение 2022 года не проводил такие дистанционные допросы. Все допросы они проводили как «говориться по старинке», с вызовом того или иного участника расследования к себе в кабинет.

В рамках расследования уголовных дел несовершеннолетних перед следователем оказываются подростки с разным процессуальным статусом. Если речь идет о потерпевшем подростке, в литературе [19, с. 159; 17, с. 27] отмечается о возможности дистанционного допроса в тех случаях, когда подросток в силу каких-то физических недостатков (из-за нападения) лежит в больнице или значительной удаленности (он проживает в одном субъекте, а производство находится в другом) не может физически присутствовать при проведении следственных действий. Конечно, в таком допросе появляется большая необходимость и его дистанционное проведение полностью себя оправдывает.

Еще одним плюсом такого допроса является его применение к лицам которые, при наличии у них затруднений физического характера (отсутствие конечностей, тяжелая болезнь, заболевания опорно-двигательного аппарата и т. п.) и (или) когнитивных, не ставящих под сомнение их дееспособность (жертвы сексуального насилия, несовершеннолетние, запуганные и пр.) не способны в официальной обстановке кабинета следователя или зала судебного заседания надлежащим образом реализовать свои процессуальные права и исполнить обязанности [12, с. 125].

Тем не менее, современная редакция УПК РФ не содержит каких-либо ограничений по статусу лица, которого можно допрашивать в ходе предварительного расследования дистанционно. Представляется, что таким образом, можно допрашивать лишь потерпевших, свидетелей, экспертов и специалистов.

Однако отметим, что в УПК РФ нет статьи или какой-то отсылки к тому, что допрос несовершеннолетних можно проводить с использованием системы – ВКС. В отличие от нас в уголовно-процессуальном законодательстве республики Казахстан такая норма есть. Так УПК Республики Казахстан (2014 г.) существует норма, регламентирующая особенности допроса с использованием научно-технических средств в режиме видеосвязи (дистанционный допрос), где на основании п. 3 ч. 1 ст. 213 регламентировано проведение дистанционного допроса малолетнего или несовершеннолетнего потерпевшего. Дистанционный допрос производится в случаях: 1) невозможности непосредственного прибытия лица в орган, ведущий уголовный процесс, по месту расследования (рассмотрения) уголовного дела по состоянию здоровья или другим уважительным причинам; 2) необходимости обеспечения безопасности лица; 3) проведения допроса малолетнего или несовершеннолетнего свидетеля, потерпевшего; 4) необходимости обеспечения соблюдения сроков досудебного расследования, судебного рассмотрения дела; 5) наличия причин, дающих основания полагать, что допрос будет затруднен или связан с излишними затратами. Решение о производстве дистанционного допроса принимается лицом, осуществляющим расследование дела, по собственной инициативе или ходатайству стороны или других участников уголовного процесса либо по указанию прокурора с направлением поручения в порядке, предусмотренном ст. 188 УПК Республики Казахстан.

Также отметим, что похожая норма есть и в УПК Республики Беларусь (1999 г.). Ст. 224.1 УПК Республики Беларусь говорит о том, что допрос потерпевшего, свидетеля, очная ставка или предъявление для опознания лиц и (или) объектов с участием потерпевшего или свидетеля могут быть проведены дистанционно с использованием систем видеоконференцсвязи (веб-конференции) в случаях: если потерпевший, свидетель являются несовершеннолетними. Что на наш взгляд является положительной тенденцией для проведения дистанционных допросов таких категорий подростков как свидетели и потерпевшие.

Еще одной проблемой при проведении дистанционного допроса, является процесс предъявления доказательств. Безусловно, проведение дистанционного допроса существенно ограничивает возможности следователя по установлению фактических обстоятельств, которые важны для расследования уголовного дела. Мы считаем, что данное положение (дистанционное предъявление доказательств) должно быть более детально проработано, иначе следователю придется от них отказаться.

Мы полностью согласны с Н.В. Машинской [16, с. 157], в том, что результаты научно-технического прогресса, безусловно, должны быть использованы в сфере уголовного судопроизводства, однако их использование не должно ставить под сомнение доброкачественность собранных по уголовному делу доказательств, содержать угрозу нарушения прав участников процесса, подрывать авторитет правосудия.

Учитывая вышеизложенное отметим, что сегодня развитие цифрровизации и цифровых технологий идет большими темпами. Эти

технологии уже активно применяются и в рамках уголовного процесса. Благодаря ним оптимизируется вся работа правоохранительных органов, что в свою очередь позволяет улучшать реализацию и защиту прав и законных интересов различных участников уголовного процесса как взрослых, так и несовершеннолетних лиц. Однако в силу определенных тенденций и недоработки технической стороны вопроса проведения дистанционного допроса, как взрослых, так и несовершеннолетних о полном переходе к этой норме говорить пока не приходится.

Список литературы

1. Абрамович, Ю.Б. Обеспечение прав несовершеннолетнего потерпевшего в условиях цифровизации общественных отношений в сфере уголовного судопроизводства / Ю.Б. Абрамович // Вопросы Российской юстиции.2021. Выпуск № 20. С. 442 – 454.
2. Антонович, Е.К. Электронное правосудие по уголовным делам в Нидерландах: современное состояние и перспективы / Е.К. Антонович // Вестник Университета имени О.Е. Кутафина (МГЮА).2020. № 10 (74). С. 136–149.
3. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский // Вестник РУДН. Серия: Юридические науки. 2021.Т. 25. № 4. С. 735–749.
4. Бертовский, Л.В. Теории оценки доказательств: назад в будущее / Л.В. Бертовский // Актуальные вопросы российского судопроизводства: доказывание с использованием современных технологий: материалы Всероссийской (национальной) научно-практической конференции (21 октября 2022 года, г. Красноярск). Красноярск: Красноярский ГАУ, 2022. С.8–12.
5. Девяткин, Г.С. Особенности организации допроса потерпевшего с использованием высоких технологий по уголовным делам, связанным с совершением киберпреступлений / Г.С. Девяткин // Вестник военного права. 2021. № 1. С. 17–23.
6. Дударев, В.А. Опыт цифровизиции уголовного судопроизводства в зарубежных странах и Российской Федерации / В.А. Дударев // Журнал Международное уголовное право и международная юстиция. № 2. 2022. С.15–17.
7. Дударев, В.А. Цифровизация уголовного судопроизводства России: плюсы и минусы / В.А. Дударев // Научное обозрение. Серия 1. Экономика и право. 2021. № 2. С. 151–161.
8. Зуев, С.В. Цифровая среда уголовного судопроизводства: проблемы и перспективы / С.В. Зуев // Сибирский юридический вестник. 2018. № 4. С.118–122.
9. Ищенко, П.П. Современные подходы к цифровизации досудебного производства по уголовным делам / П.П. Ищенко // Lex russica (Русский закон). 2019. № 12 (157). С. 68–79.

10. Качалова, О.В. Электронное уголовное дело – инструмент модернизации уголовного судопроизводства / О.В. Качалова и др. // Российское правосудие.2015. № 2 (106). С.95–101.

11. Колпакова, Л.А. Готовность общества к внедрению цифровых технологий в уголовное судопроизводство / Л.А. Колпакова // Ius Publicum Privatum. 2020. № 5 (10). С.65–68.

12. Курбатова, С.М. Использование ВКС в уголовном судопроизводстве как гарантия реализации прав его участников из числа лиц с ограниченными возможностями / С.М. Курбатова // 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.124–126.

13. Малышева, О.А. Особенности доказывания, в условиях цифровизации уголовного судопроизводства / О.А. Малышева // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 10 (74). С. 82–88.

14. Марковичева, Е.В. Цифровая трансформация российского уголовного судопроизводства / Е.В. Марковичева // Правосудие. 2020. Т. 2. № 3. С. 86–99.

15. Масленникова, Л.Н. Опыт цифровизации уголовного судопроизводства Федеративной Республики Германия и возможности его использования при цифровизации уголовного судопроизводства России / Л.Н. Масленникова, Т.Е. Сушина // Актуальные проблемы российского права. 2020. Т. 15. № 6. (115). С. 214–224.

16. Машинская, Н.В. Проблемы законодательного регулирования допроса, очной ставки и опознания с использованием систем видеоконференцсвязи / Н.В. Машинская // 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. 154–158.

17. Плетникова, М.С., Семенов, Е.А. К вопросу использования видеоконференцсвязи при производстве допроса / М.С. Плетникова и др. // Вестник Уральского юридического института МВД России. 2021. № 1. С. 25–28.

18. Сыдыкова, З.Д. Вопросы информатизации уголовного судопроизводства Киргизской Республики в условиях внедрения цифровых технологий / З.Д. Сыдыкова // Бюллетень науки и практики. 2020. Т. 6. № 9. С. 316–323.

19. Федотова, М.М. Особенности проведения допроса и обеспечение прав несовершеннолетнего в условиях цифровизации общественных отношений в сфере уголовного судопроизводства / М.М. Федотова // Актуальные вопросы российского судопроизводства: доказывание с использованием современных технологий. Материалы Всероссийской (национальной) научно-практической конференции. Красноярск, 2022. С. 156–160.

20. Якушкин, А.А. Цифровизация начального этапа досудебного производства в Российском уголовном процессе: использование опыта Республики Казахстан / А.А. Якушкин // Тамбовские правовые чтения имени Ф.Н. Плевако. Материалы III Международной научно-практической конференции. В 2-х томах / ответственный редактор В.Ю. Стромов.2019. С. 463–465.

21. ВС РФ отмечает 20-летие использования видео-конференц-связи // URL: https://www.garant.ru/news/1361912/ (дата обращения: 27.01.2023).

УДК 347.167.2:316.347:323.1

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЭТНИЧЕСКИХ ПРОЦЕССОВ

Емелин Сергей Михайлович,
доктор юридических наук, профессор
Институт этнологических исследований им. Р.Г. Кузеева –обособленное структурное подразделение
Федерального государственного бюджетного научного учреждения
Уфимского федерального исследовательского центра
Российской академии наук (ИЭИ УФИЦ РАН),
г. Уфа, Россия
email: emelin_sm@mail.ru

Семенов Сергей Николаевич,
кандидат философских наук
Институт этнологических исследований им. Р.Г. Кузеева –обособленное структурное подразделение
Федерального государственного бюджетного научного учреждения
Уфимского федерального исследовательского центра
Российской академии наук,
г. Уфа, Россия
email: semenov777@mail.ru

Аннотация: *этнические процессы в «информационном обществе» в значительной степени виртуализируются. Это требует нового правового регулирования, что вызывает необходимость использования новых технологий для своей реализации. Поэтому такие проблемы, как повышения эффективности и легитимности формирования и функционирования экстерриториальных национально-культурных автономий, и появление новых форм объективации национально-этнического самосознания в виртуальной сфере, явно требуют развития высокотехнологичного права.*

Ключевые слова: *этничность, высотехнологичное право, виртуальность, национально-культурная автономия, национально-этническое самосознание, объективация.*

MODERN TECHNOLOGIES OF LEGAL SUPPORT OF ETHIC PROCESSES

Emelin Sergey Mikhailovich,
doctor of law, professor
R.G. Kuzeev Institute for Ethnological Studies - Subdivision of the Ufa federal research centre of the Russian academy of sciences (IES UFRC RAS),
Ufa, Russia
email: emelin_sm@mail.ru

Semenov Sergey Nikolaevich,
candidate of philosophical sciences
R.G. Kuzeev Institute for Ethnological Studies - Subdivision of the Ufa federal research centre of the Russian academy of sciences (IES UFRC RAS)
Ufa, Russia
email: semenov777@mail.ru

Abstract: *ethnic processes in the "information society" are largely virtualized. This requires new legal regulation, which requires new technologies for its implementation. Therefore, such problems as increasing the effectiveness and legitimacy of the formation and functioning of extraterritorial national-cultural autonomies and new forms of objectification of national-ethnic identity in the virtual sphere clearly require the development of high-tech law.*

Keywords: *ethnicity, high-tech law, virtuality, national-cultural autonomy, national-ethnic identity, objectification.*

Этничность — одна из важнейших характеристик человека и общества, проявляющаяся в самых разных сферах их существования. Соответственно, этнические процессы в общественной жизни требуют значительного объёма правового регулирования, с учётом их влияния на ситуацию в социуме и значения для личности. В современном «информационном обществе» многие аспекты подобного регулирования начинают применять «высокие технологии», что относят к формам «высокотехнологичного права». Согласно Л.В. Бертовскому: «<…> высокотехнологичное право — это такой логистический, наукоёмкий и технологический регулятор общественных отношений, который, с одной стороны, использует высокие технологии в процессе правоприменения, а с другой – регламентирует возникающие с ними отношения» [1, с. 742].

Полагаем, важным аспектом внедрения высокотехнологичного права является открытие новых возможностей организации общественной жизни и её понимания. В этнических отношениях можно выделить целый ряд подобных моментов.

Прежде всего, это новые формы существования и проявлений этнической (национальной) психологии — её определенная объективация не только в некоторых особых действиях, культурных и политических, но и в более

широких проявлениях активности людей в информационном поле, которые могут в определенных аспектах даже количественно оценивать через Big Date.

Информационные технологии создают возможность в чём-то опровергнуть подход Б. Андерсона к нациям как «воображенным сообществам» [2, с. 30-31], основанный на том соображении, что между представителями национальной общности нет непосредственных (как в «реальном» сообществе) связей, знакомства. Но именно интернет, социальные сети могут в принципе создать «виртуальное» объединение представителей определенной этнической общности и даже формировать реально фиксированную общую её позицию по определенным вопросам.

Здесь возникают интересные возможности именно с учётом возможностей высокотехнологичного права. Дело в том, что в системе национально-государственных отношений в Российской Федерации законодательно утверждена такая форма национально-этнического самоопределения как экстерриториальная национально-культурная автономия. Если с национально-территориальными образованиями проблемы формирования их системы управления достаточно понятны, то с подобными политическими феноменами возникают проблемы.

Как определить позиции членов данных автономий по определенным вопросам, как избрать определенный круг руководителей, как организовать обсуждение насущных проблем и просто общение (в том числе и на родном языке)? В настоящее время здесь в основном опираются на деятельность национально-культурных обществ и отдельных активистов, что недостаточно полно отражает реальные позиции, пожелания и потребности представителей подобной автономной группы граждан. Здесь именно современные технологии могут обеспечить хотя бы дистанционный, но вполне действенный контакт, а также совместное общение, выражение мнений, обсуждения и, даже избрание определенных представителей. Но легитимность подобному, хотя и «виртуальному», но и не воображаемому, а реальному этнонациональному сообществу на основе национально-культурной автономии должно придать именно высокотехнологичное правовое обеспечение: именно обеспечение, а не просто «оформление».

Дело в том, что здесь необходимо не только сформулировать правовые основания работы подобной структуры, но и обеспечить необходимые для этой работы технологии, разработав и правовые основы для работы этих технологий. Это пример современных проблем. «Виртуализация этнического развития несомненно будет возрастать и её специфику необходимо понять и использовать» [3, с. 11].

В этнологических исследованиях в условиях «информационного общества» надо учитывать, что национально-этническое самосознание не только отображается и выражается через современные информационные технологии, но и получает новые формы существования с новыми свойствами.

Здесь требуется подробнее рассмотреть само понятие «национально-этническое самосознание», а главное – стоящую за этим понятием реальность, которая в определенных аспектах должна быть и предметом правового

регулирования, причём именно высокотехнологичного. Это не некая механическая совокупность индивидуальных чувств и мыслей всех представителей определенного этноса, которая не складывается в некоторую целостную и выполняющую некоторые функции систему, а некоторый хаотичный и беспрерывно меняющийся психологический феномен, остающийся во многом на единичном уровне. Хотя и здесь возможно изучение мнений и, с помощью Big Data даже составление «эмотиана», т.е. карты-схемы эмоциональных состояний жителей мегаполиса [4, с. 237].

Но это лишь «моментальные снимки» беспрерывно меняющихся ситуаций, но дающие понимание существенных аспектов. Все это низший уровень общественной психической жизни — общественная психология, стихийное её проявление.

Специализированный (его называют «идеологией» или «теоретическим», но это не полностью раскрывает его содержание) уровень общественного сознания, на котором существует в более оформленном и системном виде национально-этническое самосознание — это сфера идей, теорий, художественных образов, духовных ценностей и т.д., специально и целенаправленно создающиеся, фиксирующихся и распространяющихся, т.е. всецело социально-культурная сфера. Реальная форма полноценного существования национально-этнического самосознания — это некоторая духовно-информационная целостность, складывающаяся из совокупности выраженных на уровне специализированного сознания (т.е. идеологическом, художественном, публицистическом) идей, оценок и ценностных ориентаций, эстетических позиций и художественных образов, мнений по поводу истории, состояния, положения в обществе, перспектив развития определенного народа, выработанная представителями его духовной «элиты» и принимаемая большинством данного народа. А в основе этой системы находится исторически формирующаяся «национальная духовность» – «органичная совокупность глубинных принципов и артефактов, формирующих специфическое отношение к миру, стиль и способ самовыражения науки в любой сфере» [5, с. 125].

Формирующаяся на базе подобной национальной духовности как совокупности неких «силовых линий» некоторая духовно-информационная реальность уже не зависит в своих основных параметрах от деятельности и психики отдельных людей. В истории она чаще существовала потенциально, как возможность и тенденция, проявляясь в различных формах — от мифов, ритуалов и обрядов, бытового этикета, стиля оформления жизнедеятельности — до образцов «высокой» культуры, вплоть до современных информационных ресурсов. Но если раньше широкие слои населения лишь давали основы для этой информационной реальности, больше воспринимали её как свои высшие духовные основы, очень редко в периоды исторических потрясений активно участвовали в её формировании — то современные информационно-коммуникативные технологии расширяют возможности большинства членов общества участвовать в процессе формирования коллективных форм сознания. При этом современные информационные технологии делают национально-

этническое самосознание значительно более «объективированным», хотя больше в «виртуальном» виде.

А развивающаяся виртуальная жизнь общества, в том числе и в этнической сфере требует и новых правовых норм по недопущению экстремизма и обеспечению как прав и потребностей национально-этнических общностей, так и поддержания, и укрепления межнационального согласия. А это, в свою очередь, требует и соответствующих технологий, обеспечивающих реализацию этих прав.

Таким образом, высокие технологии XXI века как создают новые формы проявления этничности, так и требуют соответствующих форм высокотехнологичного права для их регулирования на благо общества и граждан.

Список литературы

1. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский // Вестник РУДН. Серия «Юридические науки». 2021. Т. 25. № 4. С.735-749.

2. Андерсон, Б. Воображаемые сообщества / Б. Андерсон. М.: «Канон-пресс-Ц», «Кучково поле», 2001. 288 с.

3. Емелин, С.М. Научное наследие Р.Г. Кузеева и современные проблемы этнологии / С.М. Емелин // Этнос. Общество. Цивилизация. Шестые Кузеевские чтения. Уфа: ООО «Первая типография», 2022. С.7-13.

4. Артамонова, Я.Н. Проблемы анализа эмоциональных состояний на основе Big Data в связи с геолокацией / Я.Н. Артамонова, А.А. Артёмов, А.А. Прозоров // Актуальные вопросы нейрофилософии.2015. Ежегодник / Ред.: А.Ю. Алексеев, Д.И. Дубровский, В.Т. Кузнецов. М.: ИИнтелл, 2016. С.232-240.

5. Семенов, С.Н. Ориентиры национальной политики: постметанации или национальная духовность / С.Н. Семенов, А.Н. Семенова // Исторический бюллетень. 2022. Т. 5. № 6. С.124-126.

УДК 343

ВОПРОСЫ НАЗНАЧЕНИЯ СУДЕБНЫХ ФОНОСКОПИЧЕСКИХ ЭКСПЕРТИЗ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Ерахтина Елена Александровна,
кандидат юридических наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
email: 345nn@mail.ru

Аннотация*: в работе рассмотрены особенности назначения судебной фоноскопической экспертизы, основные задачи судебной фоноскопической экспертизы, требования к объектам судебной фоноскопической экспертизы, а также - алгоритм процессуальных действий лица, ведущего расследование.*

Ключевые слова: судебная *фоноскопическая экспертиза, фонограмма, звуковая информация, аналоговая запись, цифровая запись, акустическая среда, голос человека.*

PARTICIPATION OF THE PUBLIC PROSECUTOR IN JUDICIAL INVESTIGATION

Erakhtina Elena Alexandrovna,
candidate of legal sciences, associate professor
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
email: 345nn@mail.ru

Abstract: *the paper considers the features of the appointment of a forensic phonoscopic examination, the main tasks of a forensic phonoscopic examination, the requirements for the objects of a forensic phonoscopic examination, as well as the algorithm of the procedural actions of the person conducting the investigation.*

Keywords: *forensic phonoscopic examination, phonogram, sound information, analog recording, digital recording, acoustic environment, human voice.*

Устная речь человека оставляет изменения в материальной среде, следы которых могут быть зафиксированы в звуковой форме (звуковые следы). Указанные данные зачастую имеют важное значение для дела, так как позволяют установить лиц, причастных к событию преступления. Впрочем, определение причастных к делу лиц, степень их участия и вины с помощью специального исследования фонограмм посредством лингвистических, инженерно-технических, физико-математических, информационных специальных комплексов стало возможно только с 1962 года.

Основные задачи судебной фоноскопической экспертизы представлены на схеме № 1.

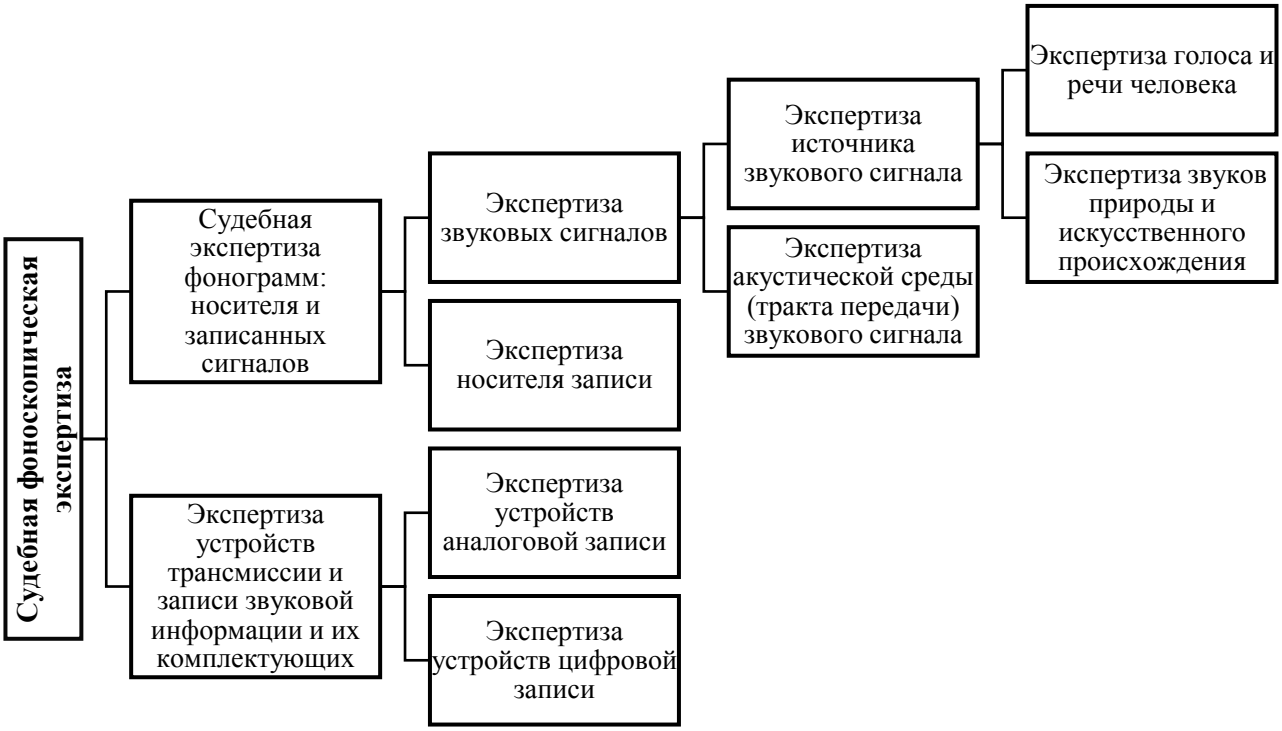
Схема № 1 «Основные задачи судебной фоноскопической экспертизы»

Учитывая основные задачи судебной фоноскопической экспертизы, рассмотрим её особенности назначения, а также производства.

Объектами судебной фоноскопической экспертизы являются фонограммы, содержащие голос и речь неизвестного лица (спорная фонограмма), а также фонограммы, содержащая голос и речь известного лица (фонограмма образцов). Звуковая и речевая информация может быть зафиксирована как в аналоговом, так и в цифровом виде на различных материальных носителях (Схема № 2).

Производство судебной фоноскопической экспертизы, которая выступает в роли доказательства, строго регламентировано законом, ровно, как и остальных видов судебных экспертиз, поэтому исследуемые фонограммы проходят оценку со звучащей речью на относимость и достоверность.

Схема № 2 Классификация видов судебной фоноскопической экспертизы



Производство судебной фоноскопической экспертизы по уголовным делам может быть назначено на выполнение двум государственным судебным экспертам, которые имеют специальные знания в различных областях науки, а также имеют необходимую аттестацию для её производства.

Назначение судебной фоноскопической экспертизы представляет собой систему следующих процессуальных действий:

Процессуальные действия лица, ведущего расследование	Решение о назначении судебной экспертизы;
	Определение рода, определение вопросов, необходимых для решения, которые будут поставлены на решение судебным экспертам;
	Подготовка необходимых материалов, необходимых для экспертизы, а также их грамотное оформление;
	Выбор судебно-экспертного учреждения для производства экспертизы;
	Вынесение постановления (определения) о назначении судебной экспертизы;
	Ознакомление участников с процесса, указанных в нормативных правовых актах, с постановлением (определением) о назначении судебной фоноскопической экспертизы;
	Направление материалов для производства судебной фоноскопической экспертизы в экспертное учреждение

Лицо, ведущее расследование определяется каким учреждением будет проводиться экспертиза территориально. В том случае, если производство экспертизы невозможно по своему территориальной привязке к

государственному судебному учреждению в связи с отсутствием эксперта определенной конкретной специальности, отсутствием необходимых условий для её производства, либо же необходимая материально-техническая база попусту отсутствует у данного судебного учреждения, то есть для этого есть решение – необходимо обратиться к соседним судебным учреждениям, производящим подобные экспертизы.

Не стоит забывать о том, что производство судебной фоноскопической экспертизы может быть назначено и негосударственным экспертам в негосударственных судебных учреждениях, где специалисты в свою очередь обладают специальными знаниями, которые позволяют им проводить данные исследования.

В постановлении о назначении фоноскопической экспертизы должны быть отображены установленные обстоятельства, материалы и какие условия были при установлении обстоятельств, какие были условия и материалы при производстве звукозаписи. Также обязательно должны быть указаны словесные границы и местонахождение подлежащей исследованию фонограммы, где должны быть указаны начальные слова и конечные во время разговора и многое другое, на полученном носителе информации, который поступил на исследование судебному эксперту: например, имеется ли на фонограмме, зафиксированной на … (указывается носитель) в звуковом файле … (указывается наименование звукового файла) и начинающейся словами: « … », заканчивающейся словами: « … », голос и речь … (указывается Ф.И.О.), образцы голоса и речи которого представлены на … (указывается носитель) в звуковом файле … (указывается наименование звукового файла)?

Важно отметить, что особое внимание в данном виде экспертиз должно удалятся подготовке материалов, которые будут использованы в процессе производства судебной фоноскопической экспертизы.

Образцы для сравнительного исследования для производства экспертизы регламентируются ст. 10 Федерального Закона «О государственной судебно-экспертной деятельности в Российской Федерации» [1]. Такого вида образцы для исследования являются прямыми объектами исследования, которое предоставляются на судебную фоноскопическую экспертизу.

Сравнительные образцы и их получение для сравнительного исследования регламентируются уже статьёй 202 УПК РФ [2]. Для сравнительного исследования в процессе фоноскопической экспертизы используются образцы голоса и речи подозреваемого; обвиняемого; свидетеля и потерпевшего.

Главной особенностью для производства сравнительного исследования заключается в сложности получения необходимой полной и целостной, максимально приближенной к действительности фонограммы речи и голоса человека с той фонограммой, из-за которой была назначения судебная фоноскопическая экспертиза.

К другой группе образцов в фоноскопической экспертизе относятся образцы голоса, которые отражают родовые признаки, к таким можно отнести

образцы жаргона, диалекта, образцы речи человека в различных ситуациях (алкогольное опьянение, наркотическое и т.п.).

Общие требования, предъявляемые к объектам исследования – фонограмма представляется с указанием содержания точных начальных и конечных реплик разговора в соответствии с прилагаемым к постановлению протоколом осмотра и прослушивания, в котором посредством прослушивания и фиксации содержания фонограммы лицом, назначившим экспертизу, отражается криминалистическая значимость данного объекта.

Как известно, огромное значение для идентификационных исследований имеет: качество записи фонограммы представленных образцов; представительность речевого материала; сопоставимость образцов речи по акустическим, лингвистическим характеристикам, эмоционально-физическому состоянию и форме речевого представления сравниваемых лиц.

При выявлении значительных различий сравнительных образцов речи и речи участников разговоров срок производства идентификационных исследований увеличится.

Поэтому прежде всего основанная задача сотрудника, изымающего образцы речи, – обеспечить оптимальные условия записи и исключить возможности искажения или утраты речи диктора, а также получения образцов в виде чтения. Для этого при фиксации образцов голоса и речи необходимо применять современные качественные звукозаписывающие устройства (цифровые средства звукозаписи), аудиоформаты без сжатия (PCM, DPCM, ADPCM). По возможности производить запись с использованием выносного микрофона. Проверить, что микрофон направлен в сторону лица, чьи голос и речь изымаются в качестве образцов, и находится перед ним на расстоянии 30–40 см.

Для исключения акустических шумов следует закрыть двери, окна и форточки; отключить телевизор, радиоприемник, телефоны, кондиционер; прекратить все посторонние разговоры; исключить возможность диктору производить шумы (например, стук по мебели или полу) и искажать речевые признаки (запретить курить, жевать, держать посторонний предмет (конфету, спичку и др.) во рту, прикрывать нос или рот); не рекомендуется перебивать диктора и пользоваться клавиатурой ПЭВМ. Образцы голоса и речи для сравнительного исследования должны быть представлены в виде развернутых ответов или свободной беседы длительностью не менее 15 мин и сопоставимы по эмоционально-психологическому состоянию с идентифицируемым лицом. В случае если реплики неизвестного лица на исследуемой фонограмме имеют малую длительность, на образцах известного лица обязательно должны присутствовать те же слова (фразы), что и на исследуемой фонограмме.

Объекты, поступившие на экспертизу, хранятся в условиях, исключающих их хищение, утрату, порчу или видоизменение, в опечатываемых сейфах, металлических шкафах.

После того, как эксперт завершит назначенное ему экспертное исследование, он обязан составить заключение эксперта (ст. 206 УПК РФ), либо же дать мотивированное объяснение о невозможности дать заключение по

назначенному делу. Следователь в свою очередь предоставляет результат следующим процессуальным лицам по делу.

Следователь разъясняет права всем участникам процесса, которые в свою очередь могут ходатайствовать о назначении повторной экспертизы, если они не согласны с результатами первоначального исследования, а также в соответствии с ч.1 ст. 205 УПК РФ произвести допрос эксперта, но стоит отметить, что допрос эксперта, пока тот в свою очередь не предоставить результаты исследования, не допускаются. Дополнительная экспертиза может быть назначена в случае недостаточности заключения эксперта, в случае если возникают новые вопросы, необходимые для полного исследования, а также если допрос эксперта не позволит ответить на эти дополнительные вопросы.

Повторная экспертиза может быть назначена на производство другому эксперту в том случае, если в первоначальном заключении эксперта возникают сомнения в правдивости и обоснованности первоначального экспертного исследования. На повторную экспертизу помимо вопросов, которые решались в первоначальном заключении, могут быть поставлены и вопросы, которые связаны с оценкой правильности использования методических рекомендация для производства фоноскопической экспертизы, которая использовалась при даче первоначального заключения эксперта.

В заключение необходимо добавить, судебная фоноскопическая экспертиза по уголовным делам зависит от всех процессуальных действий. Наличие и достаточность сравнительных образцов для производства экспертизы, а также возможность изучения звукозаписывающей аппаратуры со всех сторон, предоставляет огромное поле для изучения и исследования объектов фоноскопической экспертизы.

Список литературы

1. Федеральный закон от 31.05.2001 г. № 73-ФЗ (ред. от 01.07.2021 г.) «О государственной судебно-экспертной деятельности в Российской Федерации»// СПС «КонсультантПлюс».

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ (ред. от 25.03.2022 г., с изм. От 19.04.2022 г.)//СПС «КонсультантПлюс».

УДК 343

ИСПОЛЬЗУЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ПРОИЗВОДСТВА ФОНОСКОПИЧЕСКОЙ ЭКСПЕРТИЗЫ

Ерахтина Елена Александровна,
кандидат юридических наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
email: 345nn@mail.ru

Аннотация*: в работе рассмотрено программное обеспечение, используемое при производстве исследования речи и голоса человека для идентификации говорящего лица по фонограммам.*

Ключевые слова: *наукоёмкие методы, звуковой канал, фоноскопическая экспертиза, розыск преступников, доказывание преступной связи, Phonexi-Pro, СПО ИС «Диамант».*

USED SOFTWARE FOR THE PRODUCTION OF PHONOSCOPIC EXAMINATION

Erakhtina Elena Alexandrovna,
candidate of legal sciences, associate professor
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
email: 345nn@mail.ru

Abstract: *the paper considers the software used in the production of the study of human speech and voice to identify the speaking person by phonograms.*

Keywords: *science-intensive methods, sound channel, phonoscopic examination, search for criminals, proof of criminal connection, Phonexi-Pro, open source software IS "Diamant".*

Криминогенная обстановка сегодня характеризуется тщательно замаскированными и технически хорошо оснащенными преступлениями, что создаёт огромные трудности в их расследовании. Борьба с проявлениями высокотехнологичной преступности невозможна традиционными способами. В настоящее время сфера уголовного судопроизводства испытывает настойчивую потребность в интеграции наукоёмких методов и средств, расширяющих возможности доказывания и розыска преступников.

Эффективность расследования высоко латентных преступлений связана с использованием информации, передаваемой по звуковому каналу. Уход преступности в виртуальный сектор привело в свою очередь к увеличению потребности в сборе криминалистически значимой информации (о совершенных, скрываемых или только планируемых преступлениях), передаваемой по каналам связи, а также последующей процессуальной проверке собираемых таким способом доказательств посредством судебной фоноскопической экспертизы.

Исследованием речевой и звуковой информации при доказывании преступной связи лица с событием преступления занимается фоноскопическая судебная экспертиза.

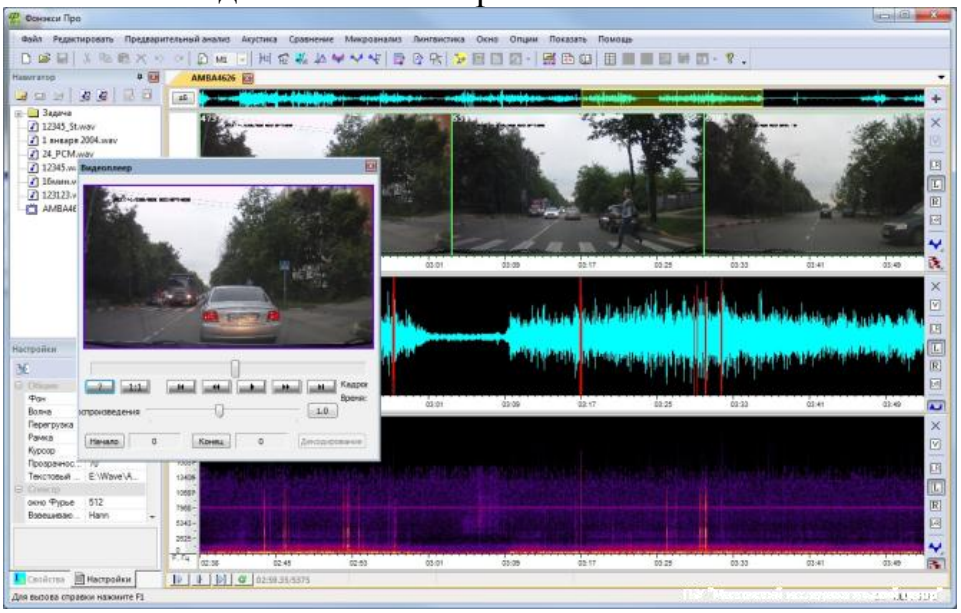
Задачами криминалистической идентификации человека по голосу и речи экспертизы является не только установление дословного содержания фонограммы и атрибуции речевых высказываний конкретному лицу, но и установление фактов непрерывности фонограмм, наличия (отсутствия) признаков их монтажа. Выполнению столь важных криминалистических задач при производстве фоноскопической экспертизы по уголовным делам помогают передовые технологии распознавания речи и голоса человека.

При производстве фоноскопических исследований сегодня применяются автоматизированные идентификационные системы, которые более точно и качественно оказывают помощь в процессе исследования. Перечень программных комплексов многообразен и пополняется постоянно. Рассмотрим некоторые из автоматизированных комплексов.Программным продуктом для идентификации говорящего лица по фонограммам на русском языке, рекомендованным для применения в экспертно-криминалистических подразделениях МВД РФ является – Фонэкси /Phonexi-Pro [1].

Функциональная основная возможность «Фонэкси» заключается в обеспечении в проведении идентификации говорящего лица по фонограммам при комплексном использовании индивидуализирующих как с лингвистических, так и с акустических признаков, где вероятность ошибки идентификации личности будет примерно равна 0.01% [2].

Программное обеспечение «Фонэкси» используется для извлечения звуковых и видео сигналов, сдвига видеоряда относительно видео, вычисления моментального и интегрального спектров фонограмм и их фрагментов, проведения идентификации говорящего по коротким фонограммам устной речи не высокого качества.

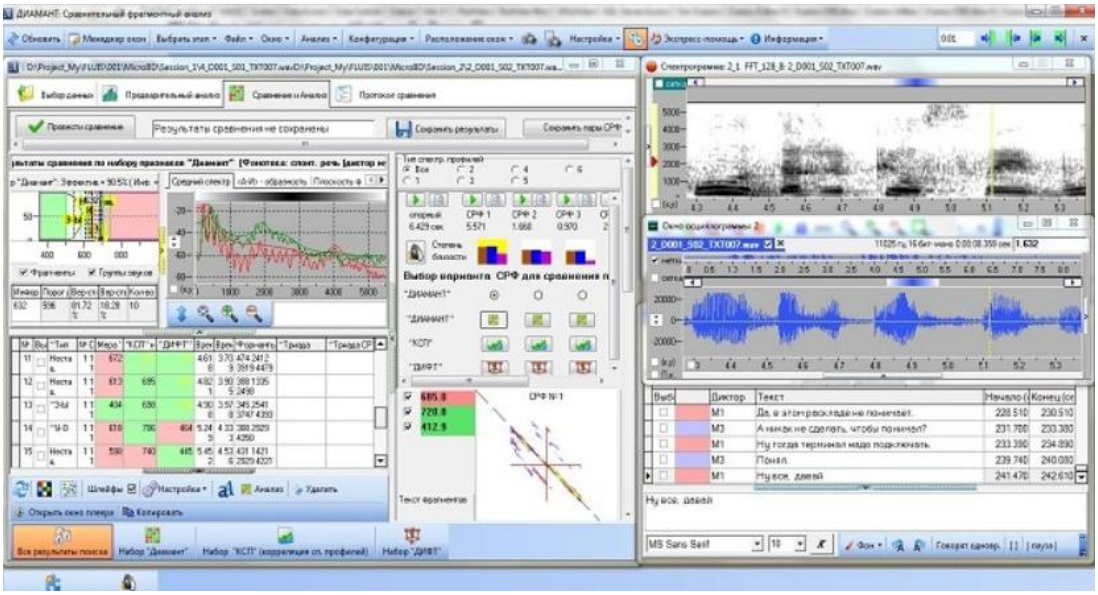
Фото № 1. Фонекси программное обеспечение для фоноскопических исследований и экспертиз



Другим специальным программным обеспечением для идентификации говорящего лица по фонограммам устной речи на русском языке, также рекомендованным для применения в экспертно-криминалистических подразделениях МВД РФ является – специальное программное обеспечение интерактивная система идентификации лиц по фонограммам устной речи «ДИАМАНТ» (далее по тексту: СПО ИС «Диамант»), которая базируется на основных принципах методики идентификации лиц по фонограммам речи «Диалект».

При вводе речевых сигналов в СПО ИС «Диамант» осуществляется преобразование их из аналоговой формы в цифровую и запись соответствующей информации в виде файла данных в память ПЭВМ. Далее речевые сигналы подвергаются сегментации и редактированию для устранения речи оппонента, длительных пауз, импульсных помех и искаженных участков речи.

Фото № 2. СПО ИС «Диамант»



Часто фонограммы речи, поступающие на экспертизу, имеют низкое качество, содержат помехи, имеют искажения и ограниченный частотный диапазон. СПО ИС «Диамант» предусмотрены средства, позволяющие проводить идентификационные исследования записей посредством адаптивного выбора режимов анализа и обработки, которые соответствуют данному типу фонограмм.

Проводя сравнение спорной фонограммы и фонограммы устной речи подозреваемого лица по лингвистическим признакам в СПО ИС «Диамант», эксперт выявляет совпадающие, дополняющие, противоречащие признаки. Сопоставление заключается в поочередном сравнении соответствующих признаков в исследуемых фонограммах, которые могут быть указаны словесно или с помощью фонетической транскрипции. Одновременно проводится и

слуховое сравнение фрагментов речи неизвестного и подозреваемого лица, содержащих выделенные признаки.

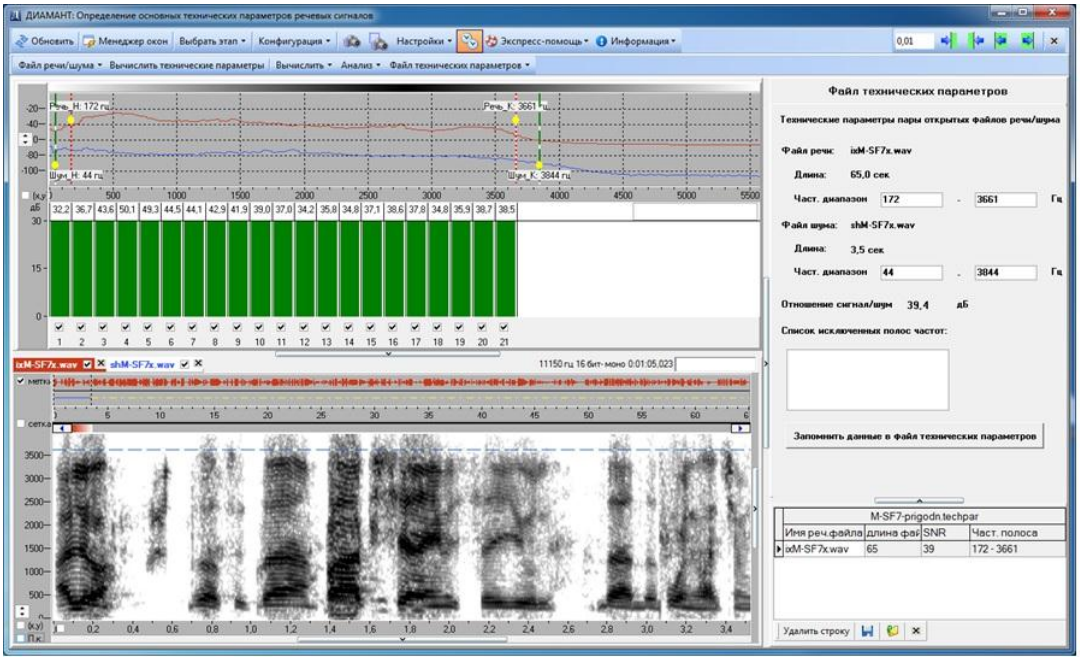
Парное слуховое сравнение позволяет уловить наиболее тонкие нюансы проявлений лингвистических признаков, которые при раздельном исследовании и описании могут остаться незамеченными.

Сопоставление признаков, зафиксированных в протоколе лингвистического анализа, проводится систематично, поэтапно, по всем группам признаков. Как правило, сравнение начинается с признаков самого крупного элемента речевой структуры - речевого потока и заканчивается сопоставлением особенностей произнесения отдельных звуков.

Для установления тождества лиц по фонограммам их речи необходимо выявление индивидуального комплекса совпадающих лингвистических признаков, определенных на всех элементах, составляющих структуру речи

СПО ИС «Диамант» состоит из программных модулей, каждый из которых предназначен для выполнения определённого уровня исследований и имеет своё окно пользовательского интерфейса.

Фото № 4. СПО ИС «Диамант»



Как известно, звуковая информация является сложным объектом экспертного исследования, требующим специальных познаний в области судебной фоноскопической экспертизы, возможностей их комплексного применения в совокупности с другими областями и направлениями судебно-экспертной деятельности. СПО ИС «Диамант» объективно обеспечивает решение следующего блока задач, стоящих перед судебной фоноскопической экспертизой (Схема № 1).

Схема № 1. Экспертные задачи (СПО ИС «Диамант»)

Экспертные задачи	Подготовка фонограмм для проведения идентификационных исследований;
	Установление дословного содержания фонограммы и/или содержания акустической обстановки;
	Дифференциация и сегментация атрибутированных по принадлежности реплик, автоматизированное создание дикторских файлов, файлов с сегментированной речью неизвестного и подозреваемого лиц, файлов шума;
	Определение основных технических параметров речевых сигналов и основных лингвистических характеристик;
	Проведение автоматического поиска сопоставимых (однотипных по спектрально-временным характеристикам) речевых фрагментов, необходимых эксперту для проведения лингвистического анализа и акустического микроанализа;
	Проведение лингвистического анализа по системе признаков, автоматизированное составление протоколов результатов проведенных раздельного и сравнительного лингвистического анализа;
	Проведение акустического интегрального анализа, автоматизированное составление протокола результатов сравнительного акустического интегрального анализа;
	Проведение раздельного и сравнительного акустического микроанализа (анализа микроструктуры звуков), составление автоматизированное протокола результатов сравнительного микроанализа;
	Автоматизированное сравнение сопоставимых речевых фрагментов для оценки степени близости голосов при решении задачи идентификации диктора, автоматизированное составление протокола результатов сравнительного анализа сопоставимых речевых фрагментов.

В заключении хотелось бы отметить, что использование автоматизированных программных комплексов расширило возможности использования аудиозаписей, полученных в результате оперативно-розыскных мероприятий, в доказывании и розыске преступников.

Дальнейшая автоматизация производства судебной фоноскопической экспертизы, разработка и усовершенствование новых программных комплексов расширяют возможности решения экспертом идентификационных задач в рамках уголовного судопроизводства в исследовании аудиозаписей.

Список литературы

1. Положение «Об Экспертно-криминалистическом центре МВД Российской Федерации». Приложение к Приказу МВД РФ от 22 декабря 1998 г. № 835//СПС «КонсультантПлюс».

2. Возможности судебной видеофонографической экспертизы: сборник научных трудов. М.: изд. ВНИИСЭ МЮ СССР, 1989.135 с.

3. Женило, В.В. Компьютерные технологии в криминалистических фоноскопических исследованиях и экспертизах / В.В. Женило, В.А. Минаев. М.: Изд. Академии МВД России, 1994.137 с.

УДК 343.982.43

РАЗРАБОТКА АРМ ЭКСПЕРТА-ПОЧЕРКОВЕДА КАК СИНЕРГИЯ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Жижина Марина Владимировна,
доктор юридических наук, доцент,
профессор кафедры криминалистики
Московский государственный университет имени М.В. Ломоносова
главный научный сотрудник ФБУ РФЦСЭ при Минюсте России,
г. Москва, Россия
e-mail: mzhizhina@yandex.ru

Аннотация: *настоящая статья оформляет часть исследования, проводимого в рамках запланированной научно-исследовательской работы ЛСПЭ ФБУ РФЦСЭ при МЮ РФ в целях разработки методических рекомендаций по проведению судебно-почерковедческой экспертизы изображений почерковых объектов в цифровых копиях документов. В ней рассматриваются алгоритмы действий эксперта-почерковеда при работе с изображениями цифровых почерковых объектов, представленных на исследование в виде компьютерного файла, а также предлагаются рекомендации по разработке нового АРМ в целях решения соответствующих задач.*

Ключевые слова: *судебно-почерковедческая экспертиза, цифровая фотокопия документа, электронный файл, графический редактор, автоматизированное рабочее место.*

DEVELOPMENT OF ARM EXPERT-HANDMARK AS A SYNERGY OF METHODOLOGICAL SUPPORT AND INFORMATION TECHNOLOGIES

Zhizhina Marina Vladimirovna,
doctor of law, docent, professor of the Department of criminalistics, Faculty of law,
Moscow state university named after M.V. Lomonosov;
Chief Researcher, FBU RFTSSE under the Ministry of Justice of Russia
Moscow, Russia
e-mail: mzhizhina@yandex.ru

Abstract: *this article draws up a part of the study carried out as part of the planned research work of the LSPE FBU RFTSSE under the Ministry of Justice of the*

Russian Federation in order to develop guidelines for conducting a forensic handwriting examination of images of handwriting objects in digital copies of documents. It discusses the algorithms of actions of a handwriting expert when working with images of digital handwriting objects submitted for research in the form of a computer file, and also offers recommendations for the development of a new workstation in order to solve the corresponding problems.

Keywords: *forensic handwriting examination, digital photocopy of a document, electronic file, graphic editor, automated workplace.*

Цифровая фотокопия документа является новым объектом – носителем почерковых реализаций в современной практике судебного почерковедения. В методическом плане разработанность ее экспертного исследования находится на заключительной фазе [1, 2]. Соответственно, новые для эксперта-почерковеда объекты исследования требуют пересмотра существующих алгоритмов и разработки новых форматов работы, на что справедливо обращают внимание отдельные авторы [3, 4]. В связи с этим особое внимание следует уделить рассмотрению ситуации, когда на экспертное исследование представляется цифровая копия документа в виде компьютерного файла на электронном носителе (флэш-карте, CD-диске) или в качестве вложения в сообщение электронной почты.

С представленным в таком виде объектом эксперт-почерковед работает с помощью программных средств (графических и текстовых редакторов), которые, с одной стороны, представляют возможность более оперативного исследования с получением качественного изображения, с другой – редактирования и преобразования исходного графического объекта. Так, например, графические редакторы (Adobe Photoshop, CorelDraw и др.) позволяют значительно улучшить исходное качество изображения цифрового снимка: подавить фон и выявить слабовидимые штрихи, повысить контрастность, резкость изображения, удалить «шум», под которым понимаются любые элементы, мешающие восприятию информативной составляющей – почерковой реализации. Улучшение качества исследуемого почеркового объекта возможно и при использовании опций «яркость» и «контрастность» при работе с графическими элементами (фото, рисунками) в текстовом редакторе Microsoft Word, которым пользуются все без исключения эксперты, оформляя свои заключения.

Конечно, данные возможности хотелось бы использовать для устранения недостатков изображения почерковых объектов. Однако, возникает закономерный вопрос о границах применения опций графических редакторов в рамках судебно-почерковедческой экспертизы (далее – СПЭ) с точки зрения соблюдения методических рекомендаций и предписаний Закона.

Одним из общих приоритетных принципов производства любой судебной экспертизы является обеспечение сохранности объекта исследования в

неизмененном виде. Если для решения задач, поставленных на разрешения эксперта, требуется повреждение (уничтожение) объекта или существенное изменение его свойств, то в соответствии со ст. 16 ФЗ Федерального закона от 31.05.2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» эксперт обязан получить разрешение на соответствующие действия от органа или лица, назначивших экспертизу.

В рассматриваемом нами аспекте – применения возможностей и опций аппаратных средств в отношении цифрового изображения почерковой реализации – будет ли это являться внесением существенных изменений в его свойства? Допустимо ли применение различных опций графических/текстовых редакторов в рамках производства СПЭ?

На наш взгляд – да, возможно и допустимо, если применение соответствующих опций программных средств направлено на получение большего количества информации об исследуемом почерковом объекте. Более того, подобное использование аппаратных опций должно стать методной составляющей экспертного исследования. Потому при разработке методики проведения судебно-почерковедческой экспертизы рукописных объектов в цифровых копиях данный технологический процесс следует выделить в качестве отдельного подэтапа предварительного этапа исследования. При этом последний необходимо правильно отразить в заключении. Таким образом, мы сталкиваемся с необходимостью пересмотра содержательной составляющей заключения эксперта-почерковеда при проведении исследования цифрового изображения рукописи, представленного в виде компьютерного файла, путем включения в него фиксации процесса обработки.

Нам представляется, что подробное протоколирование с указанием каждой команды и промежуточных результатов в виде снимков почеркового изображения является избыточным исходя из задач, решаемых СПЭ. Поэтому считаем целесообразным фиксацию исходного изображения, представленного на исследование, и окончательного – с приведением перечня использованных опций.

Например, при обработке изображений почерковых объектов достаточно указать следующее: «*обработка исходного изображения подписи от имени Иванова А.А. производилась в текстовом редакторе Microsoft Word 11 Pro путем коррекции недостаточной или избыточной яркости и контрастности*».

При этом обязательным является представление исходного и обработанного изображения в таблице снимков или по тексту заключения (см. ниже: Рис. 1, 2).

Рис. 1. Исходное изображение исследуемой подписи от имени Иванова И.И., расположенное в копии договора купли-продажи, представленной в виде файла формата*.pdf

Рис. 2. Изображение исследуемой подписи от имени Иванова И.И. после коррекции яркости и контрастности

Если какой-либо цифровой обработки изображений почерковых объектов экспертом не проводилось, он пользовался только опцией оптимального увеличения при просмотре изображения рукописи на экране монитора, отдельно отмечать это в заключении нет необходимости.

Вместе с тем, применение возможностей цифровой обработки изображений почерковых реализаций – объектов СПЭ с неизбежностью ставит вопросы об унификации деятельностной составляющей эксперта-почерковеда, в т.ч. в части конкретизации аппаратных средств. Данный аспект в настоящее время представляется достаточно проблемным, с одной стороны, по причине ухода с российского рынка ряда IT-компаний, разрабатывающих программное обеспечение для работы с графикой (например, компании Adobe), с другой – необходимостью владения определенными навыками для работы с графическими редакторами, что предопределяет дополнительное обучение и подготовку действующих экспертов-почерковедов – сотрудников экспертных учреждений.

Как нам представляется, наиболее оптимальным решением данной коллизии в современных условиях является разработка и создание специального российского софта – компьютерной программы цифровой обработки изображений почерковых объектов, непосредственно приспособленной для задач почерковедческой экспертизы (с возможностью устранения «шума», коррекции недостаточной или избыточной яркости и контрастности, цветокоррекции, повышения резкости). Реализация данного предложения целиком и полностью согласуется с основными направлениями развития современной России.

Учитывая личностные характеристики субъекта-пользователя такого софта – эксперта-почерковеда, не являющегося специалистом в сфере IT-технологий, существуют определенные требования к его интерфейсу, которые заключаются в максимальной логичности и интуитивной понятности применения. Так, например, особого внимания требует набор элементов управления, их расположение на экране и дизайн. На наш взгляд, целесообразно их приблизить к привычным, используемым в редакторе Microsoft Word. Соблюдение данных критериев позволит обеспечить быстрое обучение пользователей и субъективное удовлетворение от результата, что внедрит данное ПО в современное АРМ эксперта-почерковеда и повысит эффективность его работы.

Список литературы

1. Жижина, М.В. Судебно-почерковедческое исследование по цифровым фотографическим копиям документов / М.В. Жижина // Теория и практика судебной экспертизы.2020. № 15 (2). С.70-80.

2. Жижина, М.В. Судебно-почерковедческое исследование по цифровым копиям документов (часть 2) / М.В. Жижина // Теория и практика судебной экспертизы.2022. №17(3). С. 94-103.

3. Черепенько, Г.В. Алгоритм предварительного исследования копий рукописных реквизитов в рамках производства почерковедческой экспертизы / Г.В. Черепенько // Вестник МГЮА. 2020. № 6. С.141-148.

4. Heidi, H. Harralson Developments in Handwriting and Signature Identification in the Digital Age / H. Heidi. Routledge. 2014. 148 p.

УДК 343

О НЕКОТОРЫХ ПРОБЛЕМАХ НОРМАТИВНОГО ОБЕСПЕЧЕНИЯ ЦИФРОВОГО СУДОПРОИЗВОДСТВА НА УРОВНЕ СУБЪЕКТОВ ФЕДЕРАЛЬНОГО ПРАВОТВОРЧЕСТВА

Исаков Игорь Николаевич,
кандидат юридических наук, доцент
Национальный исследовательский университет «МИЭТ»,
г. Москва, Россия
e-mail: isakov2009@yandex.ru

Аннотация: *в статье предпринимается попытка охарактеризовать системную деятельность субъектов федерального правотворчества по нормативному обеспечению цифрового судопроизводства. Раскрывается смысл цифровизации, а также факторы, способствующие проникновению цифровых технологий в судопроизводство. Акцентируется внимание, что судопроизводство стремительно становится цифровым, а электронные доказательства приобретают всё большую актуальность.*

Ключевые слова*: цифровизация, федеральное правотворчество, судопроизводство, нормативное обеспечение, цифровые технологии.*

ABOUT SOME PROBLEMS OF REGULATORY SUPPORT OF DIGITAL LEGAL PROCEEDINGS AT THE LEVEL OF SUBJECTS OF FEDERAL LAW-MAKING

Isakov Igor Nikolaevich,
candidate of legal sciences, associate professor
National research university of electronic technology (MIET) ,
Moscow, Russia
e-mail: isakov2009@yandex.ru

Abstract: *the article attempts to characterize the systemic activity of the subjects of federal law-making on the regulatory support of digital legal proceedings. The meaning of digitalization is revealed, as well as the factors contributing to the penetration of digital technologies into legal proceedings. It is emphasized that legal proceedings are rapidly becoming digital, and electronic evidence is becoming increasingly relevant.*

Keywords: *digitalization, federal law-making, legal proceedings, regulatory support, digital technologies.*

Высокотехнологичный информационный ресурс как ключевой признак российского информационного общества, бесспорно, выступает сегодня важнейшим источником *цифровизации* судопроизводства.

Характеризуя с этих позиций нормативное обеспечение цифрового судопроизводства на уровне субъектов федерального правотворчества, можно

отметить, что первоначально Стратегия развития российского информационного общества была утверждена Указом Президента РФ 7 февраля 2008 года №Пр-212. Мероприятия по осуществлению названной Стратегии концентрировались в Федеральной программе «Информационное общество». В Указе Президента РФ от 9 мая 2017 года №203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» определена широкомасштабная задача – обеспечить системное использование информационных и коммуникативных технологий в органах государственной власти, компаниях с государственным участием и органах местного самоуправления. Названная задача была конкретизирована в Указе Президента РФ от 21 июля 2021 года № 474 «О национальных целях развития Российской Федерации на период до 2030 года».

Исходя из этого, в рамках государственной программы «Информационное общество», в настоящее время реализуется Федеральный проект «Цифровое государственное управление», инициированный Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации. Указанный документ предусматривает мероприятия цифровой трансформации в системе государственных органов власти, увеличение доли массовых социально значимых услуг, осуществляемых в электронном виде, до 95% [1].

Итак, вступление в эпоху цифровых технологий потребовало нормативного обеспечения всех органов государственной власти. Однако в числе первых такую потребность ощутили органы правосудия.

Если в этом контексте обратиться к началу нулевых годов, то в названный период остро стояла задача совершенствования уголовно-процессуального законодательства. Неслучайно с момента принятия УПК (2001 г.) в него вносилось большое количество изменений. Как отмечали авторы, многие изменения носили ситуативный, хаотический либо запоздалый характер, что не могло не отразиться на судопроизводстве. Подмечалось также, что уголовное судопроизводство на досудебных стадиях во многом имело «обвинительный характер» [2, с. 91; 3, с. 10]. Н.А. Попова, Е.А. Подковыров и др. авторы говорили, что в ряде случаев, вносимые в УПК РФ изменения искажали цели уголовно-правового регулирования, становились, по их мнению, следствием резкого увеличения влияния судебной практики на отношения, возникающие в области уголовно-процессуальной деятельности [4, с. 257].

Дальнейшие изменения в уголовно-процессуальном регулировании стали органично связываться с развитием цифровых технологий. В решение столь важной задачи включились законодательные органы. Так, Федеральный закон от 30 декабря 2021 года № 501-ФЗ дополнил УПК РФ (ст. 189.1) положениями, касающимися особенностей проведения допроса, очной ставки, опознания путём использования систем видео-конференц-связи. В этой связи можно отметить, что проведение следственных действий с применением ВКС значительно уменьшает финансовые и временные затраты участников уголовного судопроизводства, поскольку последним не приходится преодолевать значительные расстояния для участия в следственных действиях.

Также следует отметить, что сегодня в суд могут быть предоставлены все известные виды доказательств с использованием цифровых технологий, включая материалы оперативно-розыскной деятельности.

По мере нормативного закрепления цифровизации в праве быстро изменялся и облик судопроизводства. Скорость изменений нарастала практически ежедневно. Как отмечает Л.В. Бертовский, «приспособившись» к новым технологиям, право, а вместе с ним и судопроизводство становились всё более «высокотехнологичными», «цифровыми» [5, с. 735].

Стремительному проникновению цифровых технологий в судопроизводство способствовали: 1) высокий динамизм и в то же время противоречивость российской правовой жизни (например, неполнота построения «логических цепочек» в уголовно-процессуальной деятельности); 2) появление новых уровней и видов правового регулирования, новых первичных норм; 3) закрепление в Гражданском кодексе РФ понятия «цифровые права» (ст. 141.1); 4) использование в некоторых статьях УПК РФ словосочетаний «электронные носители информации»; 5) введение в государственных и негосударственных органах, предприятиях, учреждениях и организациях электронного документооборота; 6) использование в юридической практике машиночитаемых документов и др. Совокупность названных факторов во всей своей полноте отразилась на судопроизводстве. При этом, несмотря на отсутствие нормативного закрепления статуса «цифровое судопроизводство», «электронные доказательства» и др., а также чрезмерную абстрактность и расплывчатость формулирования в литературе понятия «цифровое судопроизводство», данный феномен реально существует, активно развивается и набирает обороты. Судопроизводство и досудебная практика становятся всё больше цифровыми, а электронные доказательства приобретают всё большую актуальность [6, 7].

В этом контексте смысл цифровизации в судопроизводстве можно определить как – системное проникновение в него новейших высоких технологий, т.е. перенос в компьютер знаний о судебном праве, о его функциях в сферах судебной защиты прав физических и юридических лиц, восстановлении нарушенных прав, принципах и условиях осуществления судопроизводства, его стадиях, судейском правотворчестве и автоматизированной обработке материалов по конкретному делу.

Исходя из этого, системная деятельность по нормативному обеспечению цифрового судопроизводства, как нам представляется, предполагает: 1) глубокий системный анализ современного цифрового судопроизводства; 2)потребность в цифровизации судопроизводства в рамках государственной программы «Информационное общество»; 3) обоснование направлений дальнейшего развития цифровизации судопроизводства в системе российского права.

Нормативное обеспечение цифровизации всех видов судопроизводства, в зависимости от его целей, можно разделить на внешнее и внутреннее.

Внешнее обеспечение цифрового судопроизводства на федеральном уровне осуществляют следующие субъекты.

1. *Государственная Дума*. В профильных комитетах вырабатываются научно обоснованные рекомендации: а) законодательного регулирования с применением цифровых технологий; б) повышения эффективности применения цифровых технологий в судебных инстанциях; в) законодательного регулирования использования технологий робототехники в судебной практике и др. [8].

Организационно-правовое обеспечение цифровизации в судопроизводстве осуществляет и Аппарат Государственной Думы. Последний самостоятельно не вырабатывает новой правовой информации нормативного характера, но обеспечивает функционирование базовых механизмов, в том числе цифровизации судопроизводства. Аппарат выполняет координирующую функцию. В частности, координирует участие в информационных процессах субъектов права законодательной инициативы, комитетов Госдумы, депутатов, привлечение экспертов, специалистов в сфере правосудия и др.

2. *Президент РФ*. Является наиболее активным субъектом права законодательной инициативы, в том числе по вопросам цифровизации судопроизводства. В ежегодных посланиях Федеральному Собранию Президент определят судебно-правовую политику. Предметом его особого внимания является вопрос развития высоких технологий в российском информационном обществе. Активно участвует Президент и в законодательном процессе, имеет полномочия подписания либо неподписания принятых законов, возврата их в законодательный орган с замечаниями относительно поступивших к нему законов. Принимает указы, конкретизирующие федеральные законы, в том числе по вопросам цифровизации судопроизводства.

3. *Федеральные органы исполнительной власти*. На своём уровне принимают нормативные правовые акты, касающиеся исполнения государственной политики в сфере цифровизации судебной деятельности. Во-первых, конкретизируют федеральные законы и указы Президента РФ, а во-вторых – организуют материально-техническое и программное обеспечение судопроизводства, создают благоприятные условия для работы судов и др.

4. *Высшие судебные инстанции*, обладающие правом законодательной инициативы.

5. *Граждане Российской Федерации* выступают субъектом правотворчества посредством референдумов, обсуждения проектов процессуальных законов, иных нормативных правовых актов.

Внутренним ресурсом цифровизации судопроизводства являются:

- электронные справочные и аналитические правовые и информационные системы;

- базы федеральных и региональных законов, указов Президента РФ, постановлений Правительства РФ и высших судебных инстанций;

- аналитические и статистические справки учёта общественного мнения на принятые судебные решения и оценки результатов судебной деятельности;

- материалы о состоянии правопорядка в обществе, регионах, городах, городских и сельских поселениях;

- архивные фонды документов видеосъёмок и др.;

- сводки обращений, запросов всех видов, результаты их рассмотрений и принятые меры;

- экспертные и аналитические материалы судопроизводства;

- автоматизированная система документооборота;

- данные сравнительного анализа внутринационального судопроизводства и зарубежной практики [9, с. 363].

Краткий обзор нормативного обеспечения цифровизации судопроизводства на уровне субъектов федерального правотворчества, его состояния и перспектив развития в рамках программы «Информационное общество» показывает высокую роль такого феномена в судебной деятельности. В то же время решение многих вопросов цифровизации судопроизводства находится ещё в начале пути. Предстоит немало сделать в этом направлении.

Представляется необходимым на законодательном уровне закрепить положение о необходимости в первоочередном порядке осуществить обеспечение цифровизации судебной деятельности и дать поручение федеральным органам исполнительной власти и их высшему органу – Правительству РФ принять Федеральную программу широкой цифровизации органов правосудия и осуществить контроль за её исполнением.

Обобщая сказанное, можно сделать следующие выводы.

Во-первых, постоянный рост объёма задач, выполняемых российскими судами, их чрезмерная загруженность, затрудняющая судебную деятельность, требует широкомасштабной цифровизации судопроизводства. Положительным примерами могут служить использование судами: 1) федеральной автоматизированной системы ГАС «Правосудие», включающей комплекс новейшего специализированного программного обеспечения; 2)автоматизированных сетей на федеральном и региональном пространстве; 3)локальных вычислительных сетей; 4) машиночитаемых текстов; 5)унифицированных нормативных правовых актов и др. В данном случае высокие технологии оказывают значительную помощь в решении задач судопроизводства и способствуют всестороннему, полному и объективному разрешению судами уголовных, административных и иных дел.

Например, процессуально закреплённые электронные носители информации, предоставляемые в суд в виде электронных доказательств, приобретают статус официальных судебных доказательств и на полном основании используются в ходе принятия судебных решений. Более того, как показывает практика, в сложных комбинированных судебных ситуациях (острые конфликты, соперничество, процессуальные и тактические ошибки и др.) электронные носители информации могут вызывать больше доверия. В подавляющем большинстве случаев в ходе судебного следствия выяснялось, что электронные носители информации обеспечивают бóльшую достоверность представленных доказательств, чем показания потерпевших, свидетелей и иных участников процесса. При рассмотрении больших по объёму уголовных дел электронные носители информации повышают эффективность судебного

следствия. В отдельных случаях суд по собственной инициативе исследует электронные носители информации, полученные в ходе проведения оперативно-розыскной деятельности, которые, как известно, служат вспомогательным средством установления конкретных обстоятельств уголовного дела. Однако нередко именно электронные доказательства, полученные в ходе ОРМ, выступали объективным источником информации в судопроизводстве.

Во-вторых, законодательное закрепление системного использования цифрового судопроизводства, его дальнейшее нормативное обеспечение при рассмотрении уголовных и иных дел можно характеризовать как *тенденцию*, проявляющуюся в виде комплексной систематизации, с одной стороны, высокотехнологичного информационного ресурса, а с другой – систематизации создаваемой нормативной базы на уровне субъектов федерального правотворчества. Такой подход может способствовать не только упорядочению судебной деятельности, но и повышению её эффективности.

Список литературы

1. «Цифровое государственное управление» // URL: https://digital.gov.ru/ru/activity/ directions/882/ (дата обращения: 03.02.2023 г.).

2. Малюгин, С.В. Законодательная политика в отношении УПК РФ / С.В. Малюгин // Российский юридический журнал. 2013. № 6. С.87-94.

3. Божьев, В.П. Изменения УПК РФ – не всегда средство его совершенствования / В.П. Божьев // Законность. - 2005. - №8. - С. 2-6.

4. Попова, Н.А. Проблемы и перспективы формирования уголовно-процессуального права России на современном этапе /Н.А. Попова и др./ Проблемы формирования нового российского права и новой российской государственности. Тамбов: Изд-во ТГУ, 2015. 471 с.

5. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский // Вестник РУДН, серия юрид. Науки, 2021. Т. 25. № 4. С.735-749.

6. Основы теории электронных доказательств: монография / А.Н. Балашов [и др.] / под ред. С.В. Зуева. Москва. Юрлитинформ, 2019. 400 с.

7. Балашова, А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: автореф. дис. … канд. юрид. наук / А.А. Балашов. АУ МВД РФ. Москва, 2020. 30 с.

8. Аналитический вестник. – М.: издание Государственной Думы. - 2020. 192 с. URL: http://duma.gov.ru/media/files/vALRZNAAios ZvSEl2LtcE6KMBgqQVMzr.pdf/ (дата обращения: 05.02.2023).

9. Солдаткина, О.Л. Информационные ресурсы правотворческой политики / О.Л. Солдаткина // Правотворческая политика современной России / под ред. А.В. Малько. М.: Проспект, 2016. 456 с.

УДК 367.1

О ПРОБЛЕМЕ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КАЧЕСТВЕ СУДЬИ

Казиханова Светлана Сергеевна,
кандидат юридических наук, доцент, доцент института высокотехнологичного права и социально гуманитарных наук
Национальный исследовательский университет «МИЭТ» ,
г. Москва, Россия
доцент кафедры гражданского и административного судопроизводства
Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),
г. Москва, Россия
e-mail: sskazihanova@msal.ru

Аннотация: *в статье анализируются аргументы сторонников и противников замены судьи искусственным интеллектом при осуществлении судопроизводства. Выражается согласие с теми учеными и практическими работниками, которые не допускают такую возможность в силу специфики судебной деятельности (оценка доказательств по внутреннему убеждению судьи) и норм российского права (оценочные нормы и судейское усмотрение при их применении). Иное существенно снизило бы уровень процессуальных гарантий правосудия, и по существу его разрушило. Вместе с тем с учетом того, что не вся судебная деятельность является правосудием, и есть такие производства, где фигура судьи достаточно формальна, при этом привлечение искусственного интеллекта, наоборот, поспособствовало бы созданию хоть каких-либо гарантий правильности конечного решения, такая замена допускается. В частности, о замене судьи искусственным интеллектом можно задуматься в приказном производстве в цивилистических процессах.*

Ключевые слова*: правосудие, искусственный интеллект, цифровые технологии, замена судьи, приказное производство.*

ON THE PROBLEM OF USING ARTIFICIAL INTELLIGENCE AS A JUDGE

Kazikhanova Svetlana Sergeevna,
candidate of legal sciences, associate professor, associate professor of the Institute of high-tech law and social sciences
National research university of electronic technology (MIET),
Moscow, Russia,
associate professor of the Department of civil and administrative procedure
Kutafin Moscow State Law University (MSAL),
Moscow, Russia
e-mail: sskazihanova@msal.ru

Abstract: *the article analyzes the arguments of supporters and opponents of replacing a judge with artificial intelligence in the implementation of legal proceedings. An agreement is expressed with those scientists and practitioners who do not allow such a possibility due to the specifics of judicial activity (evaluation of evidence based on the inner conviction of the judge) and the norms of Russian law (evaluative norms and judicial discretion in their application). Otherwise, it would significantly reduce the level of procedural guarantees of justice and essentially destroy it. At the same time, taking into account the fact that not all judicial activity is justice, and there are such proceedings where the figure of a judge is quite formal, while the involvement of artificial intelligence, on the contrary, would contribute to the creation of at least some guarantees of the correctness of the final decision, such a replacement is allowed. In particular, one can think about replacing a judge with artificial intelligence in writ proceedings in civil law processes.*

Keywords: *justice, artificial intelligence, digital technologies, replacement of a judge, writ proceedings.*

Чрезмерная загруженность судов, которая в конечном итоге может привести к снижению качества правосудия и подрыву доверия к суду как органу, его осуществляющему, требует срочных мер, направленных на оптимизацию судебной деятельности. В решении этой проблемы на первый план выходит активное применение цифровых технологий. Как отмечает в первой главе монографии, посвященной цифровым технологиям в цивилистическом судопроизводстве, Е.Г. Стрельцова, применение цифровых технологий в сфере защиты права связано с двумя основными направлениями: 1) сервисное направление использования цифровых технологий, не ставящее своей целью заменить суд или изменить характер участия заинтересованных лиц при разрешении спора; 2) замещающие технологии, сконцентрированные на передаче функций человека компьютеру [1]. Рассмотрим подробнее второе направление применения цифровых технологий в части замены судьи искусственным интеллектом.

В настоящее время возможности искусственного интеллекта активно используются в мировой практике (Китай, США и др. страны) в основном для досудебного разрешения споров в рамках альтернативных процедур. В современных судебных системах не встречается полная замена судьи искусственным интеллектом. Однако дискуссии в отношения вопроса передачи определенных функций судьи роботу для осуществления прогнозируемого правосудия активно ведутся.

Следует отметить, что в большинстве публикаций и выступлений, посвященных применению технологий искусственного интеллекта в правосудии, как ученые, так и практикующие юристы отрицательно оценивают возможности замены судьи. Однако справедливости ради заметим, что у этой позиции есть и сторонники, которые полагают, что роботизация процесса отправления правосудия является неизбежной.

Так, Н.А. Колоколов указывает на то, что «человеческая деятельность – алгоритм, причем на 99% рутина, бесконечное повторение прошлого опыта.

Что мешает боту повторить то, чему его обучили?» Кроме того, автор видит существенным преимуществом искусственного интеллекта над человеком отсутствие произвола, поскольку «машине человеческие слабости неведомы!». Подобный аргумент, свидетельствующий о существующей в обществе низкой степени доверия к суду, автору настоящего исследования приходилось слышать и от обычных граждан, не имеющих отношения к юридическому сообществу.

В качестве аргументов недопустимости такой замены обычно приводится то, что судьи осуществляют оценку доказательств по своему внутреннему убеждению и принимают во внимание при вынесении решения множество факторов. К примеру, речь идет о значительном числе оценочных норм, таких как разумность, справедливость, целесообразность, добросовестность, и деятельность судьи при применении этих норм не может быть алгоритмизирована [3]. Опасения ученых связаны с тем, что идея судьи-робота, который выносит решение или приговор по делу, уничтожает институт судейского усмотрения. Так, в своей работе Коваленко К.Е., Печатнова Ю.В., Стаценко Д.А., Коваленко Н.Е. справедливо обращают внимание на то, что «помимо нормативных формул, которые можно перенести на кодированную информацию, есть немаловажное судебной усмотрение, включающее дух закона, мораль, совесть, машиной не распознающиеся. Исключить институт судейского усмотрения – значит лишить судопроизводство смысла» [4].

Следует отметить, что последний подход можно считать общеевропейским, поскольку в Европейской этической хартии об использовании искусственного интеллекта в судебных системах и окружающих их реалиях 2018 г. прямо говорится о том, что «тип искусственного интеллекта, который был бы оснащен не только интеллектом, но и сознательностью, остается чисто вымышленным» (пункт 63).

Этот подход поддерживается и судьями. Так, в своем докладе 2020 года «Перспективы использования искусственного интеллекта в судебной системе Российской Федерации» председатель Совета судей РФ Виктор Момотов подчеркнул, что «смысл законодательства, то есть его дух, может быть выявлен только человеком с высоким уровнем правовой культуры, а никак не компьютером».

Некоторые авторы, в частности, Браво-Хуртадо П., пишут о нежелательности замены судьи искусственным интеллектом также в силу этической стороны вопроса – человека может судить лишь равный ему гражданин, наделенный такими же правами государством [5].

При этом многие авторы допускают и даже считают полезным использование искусственного интеллекта не в качестве замены, а в качестве помощника судьи, который позволит сократить сроки рассмотрения дела и будет способствовать вынесению законного, обоснованного и справедливого решения. В частности, в своей докторской диссертации, посвященной правосубъектности искусственного интеллекта в сфере права интеллектуальной собственности, судья Арбитражного суда Московской области П.М. Морхат пришел к выводу о том, что полная замена судей-людей «электронными судьями» маловероятна, однако применение ИИ в судопроизводстве

обоснованно и возможно для выполнения целого ряда обеспечительных функций при задействовании ИИ как «компаньона» судьи [6].

Так, в одном из телеграмм-каналов, а также на сайте Российской газеты (информация датирована 05.02.2023) приводился следующий пример, когда судья в Колумбии вынес решение совместно с чат-ботом ChatGPT. В ходе разбирательства судья должен был постановить, покрывает ли медицинская страховка ребенка с аутизмом все расходы на его лечение. При оглашении вердикта господин Падилья решил посоветоваться с искусственным интеллектом и спросил коллегу «без души»: «Освобожден ли несовершеннолетний аутист от уплаты сборов за его лечение?» Робот ответил положительно, сославшись на местное законодательство.

Участие искусственного интеллекта в судебном процессе спровоцировало волну споров как в юридическом сообществе, так и среди простых людей, обеспокоенных тем, что реальных вершителей закона пытаются заменить машинами. Господин Падилья, в свою очередь, объяснил, что не пытается лишить коллег судейского молотка, а лишь оптимизирует работу системы правосудия. Для этого он «нанял» ChatGPT, чтобы тот выступал в роли секретаря и помогал структурировать информацию. К тому же при вынесении приговора он опирался не только на мнение робота, но и на прецедент из предыдущих постановлений. Но сам чат-бот не разделил точку зрения «начальника». Он заявил The Guardian, что ChatGPT не место в судопроизводстве, ведь искусственный интеллект «не заменяет знаний, опыта и суждений судьи-человека». Попутно робот посоветовал журналистам осторожнее цитировать его изречения, ведь зачастую он демонстрирует предвзятость и правдоподобно лжет [7]. В блогах юристов и научных статьях все чаще встречаются рассуждения о возможности вынесения судебных приказов в автоматизированном режиме и даже конкретные предложения по организации этой работы [8]. Коваленко К.Е., Печатнова Ю.В., Стаценко Д.А., Коваленко Н.Е. также предлагают автоматизировать вынесение определения об оставлении искового заявления без движения, об отложении судебного заседания, а также решений в порядке упрощенного производства [9]. Однако надо понимать, что к такой замене судьи искусственным интеллектом необходимо подходить крайне обдуманно, взвесив все преимущества и недостатки.

Безусловным аргументом в пользу допущения возможности замены судьи в приказном производстве выступает то, что приказное производство не является правосудием, в нем не действуют присущие правосудию и пронизывающие его гарантии, призванные обеспечить вынесение правильного судебного акта и не допустить произвола со стороны как суда, так и тяжущихся. Роль судьи при вынесении судебного приказа сводится к проверке приложенных к заявлению взыскателя письменных доказательств, которые, как правило, заранее известны по каждому установленному законом требованию. К тому же сами судьи не скрывают, что на практике выносят судебные приказы их помощники. При этом в приказном производстве практически отсутствует возможность проверки достоверности представленных взыскателем документов, что привело в гражданском процессе к тому, что судебный приказ выдавался по фальсифицированным договорам, распискам и т.д., и у граждан

со счетов списывали денежные средства по несуществующим обязательствам. И эти случаи приобрели массовый характер [10]. Подобные примеры встречаются и в арбитражном процессе [11].

В связи с этим убедительной видится высказанная Д.А. Тумановым мысль о возможности передачи дел о выдаче судебного приказа искусственному интеллекту. В частности, это позволило бы использовать его возможности выявления подложности представленных документов. Верно указал автор и на то, что с помощью искусственного интеллекта также должна быть обеспечена возможность автоматического сличения подписи должника на документе, представленном заявителем, с образцами этой подписи, которые могут находиться в различных базах, а также возможность автоматического запроса к нотариусу для получения данных о том, что сделка в действительности имела место.

Вместе с тем невозможно согласиться с авторами по вопросу возможности замены судьи в упрощенном производстве, поскольку последнее снабжено в отличие от приказного производства определенными гарантиями, для сохранения которых требуется судья-человек.

В завершении хотелось бы привести весьма меткое и крайне справедливое изречение Д.А. Туманова, которое заставляет задуматься со всей серьезностью над вопросом о замене судьи в процессе: «Искренне надеемся, что увлечение техническими новшествами в конечном итоге не приведет к нивелированию правосудия в той форме, о которой много раз писали фантасты, когда описывали будущее, в котором правосудие осуществляет не человек, а машина. Нечто подобное в ироничной форме было описано А.И. Куприным в рассказе «Механическое правосудие», где машина для наказания «беспристрастная, непоколебимая, спокойная, справедливая...» «и никакая сила не может ни остановить действия машины, ни ослабить ударов, ни увеличить или уменьшить скорость вращения вала до тех пор, пока не совершится полное правосудие…» в конечном итоге сломалась и покарала своего изобретателя» [13].

Список литературы

1. Цифровые технологии в гражданском и административном судопроизводстве: практика, аналитика, перспективы / отв. ред. Е.Г. Стрельцова. М.: Инфотропик Медиа, 2022.

2. Колоколов, Н.А. Еще раз об искусственном интеллекте в правосудии / Н.А. Колоколов // Уголовное судопроизводство. 2020. № 4. С. 3-6.

3. Трезубов, Е.С. Тенденции цифровизации цивилистического процесса/ Е.С. Трезубов // Вестник гражданского процесса. 2022. № 5. С. 204-227.

4. Коваленко, К.Е., Печатнова, Ю.В., Стаценко, Д.А., Коваленко, Н.Е. Судья-робот как преодоление противоречий судебного усмотрения (юридические аспекты) / К.Е. Коваленко, Ю.В. Печатнова, Д.А. Стаценко, Н.Е. Коваленко // Юридический вестник ДГУ. 2020.№ 4. С.169-173.

5. Браво-Хуртадо, П. Автоматизация отправления правосудия: обращение к трем ошибочным суждениям об искусственном интеллекте / П. Браво-Хуртадо // Вестник гражданского процесса. 2018. № 1. С. 181-199.

6. Мохат, П.М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: Автореф. дис. …д-ра юрид. Наук / П.М. Мохат. М., 2018. С. 33-34.

7. Сайт Российской газеты // URL: https://rg.ru/2023/02/06/chat-bot-na-strazhe-zakona.html.

8. Барсегян, А.Л. Автоматизированное приказное производство. Вторжение в правосудие или хорошая оптимизация? / А.Л. Барсегян // URL: https://zakon.ru/blog/2018/2/14/avtomatizirovannoe_prikaznoe_proizvodstvo_vtorzhenie_v_pravosudie_ili_horoshaya_optimizaciya.

9. Коваленко, К.Е. Судья-робот как преодоление противоречий судебного усмотрения (юридические аспекты) / К.Е. Коваленко, Ю.В. Печатнова, Д.А. Стаценко, Н.Е. Коваленко // Юридический вестник ДГУ. 2020.№ 4. С.171.

10. Просвирин, А. Суд использован в мошеннической «схеме». Кто ответит за ущерб? / А. Просвирин // URL: https://zakon.ru/blog/2019/7/25/sud_ispolzovan_v_moshennicheskoj_sheme_kto_otvetit_za_uscherb «Без меня меня судили»: волгоградец получил судебный приказ из Калуги о несуществующем кредите.

11. В Интернете появились практические советы, как противодействовать мошенникам в приказном производстве в арбитражном процессе. Судебный приказ арбитражного суда: как противодействовать мошенникам // https://konchin.ru/sudebnyj-prikaz-arbitrazhnogo-suda-kak-protivodejstvovat-moshennikam/.

12. Туманов, Д.А. Некоторые размышления о правосудии и оптимизации судопроизводства / Д.А. Туманов // Законы России: опыт, анализ, практика. 2020. № 8. С.14.

13. Туманов, Д.А. О некоторых тенденциях развития гражданского процессуального права / Д.А. Туманов, С.А. Алехина // Законы России: опыт, анализ, практика. 2015. № 3. С.12-28.

14. Туманов, Д. А. Некоторые размышления о правосудии и оптимизации судопроизводства /А.Д.Туманов// Законы России: опыт, анализ, практика. 2020. № 8. С.14.

15. Цифровые технологии в гражданском и административном судопроизводстве: практика, аналитика, перспективы / отв. ред. Е.Г. Стрельцова. М.: Инфотропик Медиа, 2022 (автор главы И.И. Черных).

16.https://www.volgograd.kp.ru/daily/27150.3/4245055/https://www.volgograd.kp.ru/daily/27150.3/4245055/.

17. Без меня меня судили // https://mos- jkh.livejournal.com/9333609.html.

18. Колоколов, Н.А. Компьютер вместо судьи - арифметика вместо души / Н.А. Колоколов// Уголовное судопроизводство. 2019. № 3. С. 3-7.

19.Незнамов, А.В. К вопросу о применении технологий искусственного интеллекта в правосудии: терминологический аспект / А.В. Незнамов // Арбитражный и гражданский процесс. 2019. № 10. С. 16-17.

20. Козырева, А.А. Применение технологий искусственного интеллекта в правосудии /А.А.Козырева, Т.В. Пирожкова // Администратор суда. 2021. № 2. С. 12-16.

21. Сычева, О.А. Здравый смысл в судебном доказывании /О.А.Сычева // Российский судья. 2019. № 8. С. 15-20.

22. Котлярова, В.В. К вопросу о цифровизации процесса отправления правосудия / В.В. Котлярова // Арбитражный и гражданский процесс. 2019. №12. С. 48.

УДК 34.

ИНТЕЛЛЕКТУАЛЬНОЕ И КОГНИТИВНОЕ ПРАВО В АСПЕКТЕ ПРОБЛЕМ ВЫСОКОТЕХНОЛОГИЧНОГО ПРАВА

Колмаков Владимир Юрьевич [1]
канд. филос. наук, доцент
Курбатова Светлана Михайловна [1, 2]
канд. юрид. наук, доцент

1 Красноярский государственный медицинский университет им. проф. В.Ф. Войно-Ясенецкого,
2 Красноярский государственный аграрный университет
г. Красноярск, Россия
e-mail: sveta_kurbatova@mail.ru

Аннотация*: в статье рассмотрен ряд аспектов, касающихся понятия и сущности интеллектуального и когнитивного права, а также их взаимодействия и соотношения друг с другом, в том числе - в контексте и под воздействием высокотехнологичного права.*

Ключевые слова*: когнитивное право, интеллектуальное право, высокотехнологичное право*

INTELLECTUAL AND COGNITIVE LAW IN THE ASPECT OF HIGH-TECH LAW PROBLEMS

Kolmakov Vladimir Yuryevich [2]
candidate of philos. sciences, associate professor
Kurbatova Svetlana Mikhailovna [1, 2]
candidate of legal sciences, associate professor
[1] Krasnoyarsk Medical University named after Prof. V. F. Voino-Yasenetsky
[2]Krasnoyarsk state agrarian University
Krasnoyarsk, Russia
sveta_kurbatova@mail.ru

Abstract*: The article considers a number of aspects related to the concept and essence of intellectual and cognitive law, as well as their interaction and correlation with each other. Including in the context and under the influence of high-tech law.*

Keywords*: cognitive law, intellectual property law, high-tech law*

Инновационные проблемы в современном праве, как в системе общей теории права, так и в отдельных конкретных направлениях, возникают в силу достаточно быстрого и даже, можно сказать, интенсивного развития современных технологий, и особенно технологий, связанных с развитием искусственного интеллекта. Это ставит новые и инновационные задачи перед правовой системой и отдельными областями права. Необходимость этого возникает из-за потенциала этих технологий для преобразования различных аспектов общества, а также того, чтобы правовая база оставалась адекватной по отношению к изменениям, происходящим в современном обществе, его высокотехнологичной сфере с тем, чтобы устранять негативные последствия.

Понятие «искусственный интеллект» и «правовое регулирование области применения искусственного интеллекта» тесно связаны, поскольку определение того, что представляет собой искусственный интеллект, может иметь существенные последствия для того, как он регулируется правовой системой.

Чтобы сопоставить эти два понятия важно иметь четкое и общепринятое определение искусственного интеллекта. Это определение может служить основой для определения того, что следует считать искусственным интеллектом в контексте правового регулирования. Существуют различные определения искусственного интеллекта, но в целом он относится к разработке систем и алгоритмов, которые могут выполнять задачи, которые обычно требуют человеческого интеллекта, такие как восприятие, рассуждение, обучение и решение проблем.

После того, как определение искусственного интеллекта будет установлено, его можно использовать для руководства по правовому регулированию области применения искусственного интеллекта. Этот регламент может охватывать широкий круг правовых вопросов, включая защиту данных, конфиденциальность, интеллектуальную собственность, ответственность и этические соображения. Конкретный объем правового регулирования будет зависеть от сферы применения искусственного интеллекта, а также целей и задач регулирования.

Таким образом, соотношение понятий «искусственный интеллект» и «правовое регулирование сферы применения искусственного интеллекта» требует четкого определения, в котором понятие искусственного интеллекта должно быть в качестве отправной точки. В дальнейшем это можно будет использовать для разработки нормативной правовой базы, направленной на решение проблем, связанных с использованием искусственного интеллекта.

При этом вопрос о применении искусственного интеллекта в процессах принятия решений поднимает вопросы об ответственности в тех случаях, когда эти решения имеют негативные последствия для отдельных лиц или общества. Защита личных данных и конфиденциальности в контексте систем и алгоритмов на основе ИИ также вызывает серьезную озабоченность. Кроме того, развитие ИИ и других новых технологий подняло вопросы о защите прав интеллектуальной собственности, особенно в отношении создания оригинальных произведений или открытий с помощью автоматизированных процессов. Эти инновационные проблемы требуют активного и междисциплинарного подхода с участием не только юристов, но и

специалистов в области технологий, философии, этики и других областей знаний, чтобы правовая база могла эффективно решать проблемы, возникающие в связи с развитием современных технологий.

Интеллектуальное право и когнитивное право - это две разные области права, которые имеют дело с разными областями интереса.

Интеллектуальное право касается защиты прав интеллектуальной собственности, таких как патенты, товарные знаки, авторские права и коммерческая тайна. Оно направлено на то, чтобы сбалансировать интересы создателей и новаторов с общественными интересами и продвижением инноваций.

Когнитивное право имеет дело с регулированием когнитивных технологий, таких как искусственный интеллект, машинное обучение и интерфейсы мозг-компьютер. В нем рассматриваются этические, юридические и социальные последствия, возникающие в результате разработки и использования этих технологий, такие как конфиденциальность, подотчетность и ответственность.

Корреляция между этими двумя областями права заключается в том, что достижения в области когнитивных технологий могут влиять на создание и защиту интеллектуальной собственности, а права интеллектуальной собственности также могут играть роль в формировании и внедрении этих технологий. В результате пересечение этих сфер может потребовать нюансированного подхода к правовому регулированию. При этом можно утверждать, что интеллектуальное и когнитивное право относятся к высокотехнологичному праву, о котором пишет профессор Л.В. Бертовский [1]. Они охватывают широкий спектр правовых вопросов, возникающих в результате разработки и использования передовых технологий, таких как искусственный интеллект и машинное обучение. Эта область права касается правовых последствий создания, использования и защиты интеллектуальной собственности, такой как патенты, товарные знаки, авторские права и коммерческая тайна, в контексте новых и появляющихся технологий. Когнитивное право, в частности, имеет дело с юридическими последствиями взаимодействия между технологиями и человеческим познанием, включая вопросы, связанные с неприкосновенностью частной жизни, защитой данных, интеллектуальной собственностью и ответственностью. Например, когнитивное право может касаться правовых последствий использования алгоритмов машинного обучения для обработки и анализа больших объемов персональных данных или для принятия автоматизированных решений, влияющих на отдельных лиц. Когнитивное право в широком смысле этого термина предполагает рассмотрение всех социальных отношений, в которых тем или иным образом когнитивность может проявляться.

Проблемы высокотехнологичного права в контексте интеллектуального и когнитивного права могут быть сложными и сложными и часто требуют междисциплинарного подхода, сочетающего юридические, технические и этические знания. Быстро развивающийся характер технологий в этой области делает ее динамичной и постоянно развивающейся областью права, требующей гибкого и адаптивного подхода к решению новых и возникающих правовых вопросов.

Итак, в контексте предмета настоящего исследования можно выделить три направления правового регулирования, три сферы права – интеллектуальное право, когнитивное право и высокотехнологическое право. В дополнение к интеллектуальному праву и когнитивному праву высокотехнологичное право является еще одной отраслью права, которая занимается правовыми вопросами, возникающими в связи с использованием технологий в различных областях. Оно охватывает широкий спектр институтов, таких как электронная коммерция, конфиденциальность данных, кибербезопасность и регулирование Интернета и пр. Закон о высоких технологиях может пересекаться как с интеллектуальным, так и с когнитивным правом, поскольку может включать защиту прав интеллектуальной собственности на продукты и услуги, связанные с технологиями, а также регулирование использования передовых технологий.

И ещё один важный аспект. По сути дела, мы уже видим как правовая концепция информационных технологий расходится с концепцией правового регулирования системы тех правовых отношении, где прямо или косвенно субъектом правовых отношений может выступать искусственный интеллект. Например, кто будет нести ответственность, если автомобиль, управляемый ИИ, собьёт человека, нанесёт физический, материальный и моральный вред? В случае причинения вреда человеку автомобилем с искусственным интеллектом ответственность может лежать на производителе транспортного средства или на технологии, лежащей в основе системы искусственного интеллекта. Однако точное распределение ответственности будет зависеть от конкретных обстоятельств и законов той юрисдикции, где произошел инцидент. В каких случаях водитель транспортного средства, владелец транспортного средства или оба могут быть привлечены к ответственности. Возможно, что в таких случаях к ответственности могут быть привлечены несколько сторон, и распределение ответственности будет зависеть от различных факторов, таких как причина аварии, конструкция транспортного средства и договорные соглашения между соответствующими сторонами. Поскольку транспортные средства с искусственным интеллектом становятся все более распространенными, вероятно, будет продолжено юридическое и этическое рассмотрение ответственности, связанной с такими инцидентами.

Все это может привести к недопониманию, неправильному толкованию и неправильному применению закона, к юридическим спорам и проблемам при их разрешении, а также к негативным последствиям для отдельных лиц, бизнеса и общества в целом. Важно, чтобы правовая система не отставала от быстрых изменений, вызванных достижениями в области технологий, и обеспечивала ясность и понятность закона в целях обеспечения справедливости и справедливости.

При этом можно отметить, что в широком смысле когнитивное право является общей смысловой платформой. И, возможно, на фоне изменения представлений о правовых аспектах права ИИ, необходимо говорить о когнитивном человеческом праве в каких-то принципиально новых аспектах, о когнитивных правах человека в новых, фундаментальных форматах. Развитие и использование ИИ приводит к новым правовым проблемам и трудностям, которые требуют более глубокого понимания взаимосвязи между технологиями

и законом. Поэтому важно выстроить надлежащим образом концепцию когнитивных прав человека в свете этих событий, чтобы обеспечить защиту прав и интересов людей в эпоху ИИ.

Список литературы

1. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский // Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. № 4. С.735—749.

2. Штыров, В. Защита авторских прав / В. Штыров, Л. Бертовский // Законность. 2007. № 2(868). С. 28-30.

УДК 343.98

«СОВРЕМЕННЫЙ» ЯЗЫК КРИМИНАЛИСТИКИ

Комаров Игорь Михайлович,
доктор юридических наук, профессор, заведующий кафедрой криминалистики
Московский государственныйй университет имени М.В. Ломоносова,
г. Москва, Россия
e-mail: mgu.ikomarov@mail.ru

Аннотация. *В настоящей публикации автор приводит основные положения, связанные с языком криминалистики как одним из важных компонентов, характеризующих ее в качестве юридической науки. Обосновывается важность формирования языка и его основные позиции, сохранение которых необходимо для того, чтобы криминалистика в ее понятиях как учеными, так и практиками воспринималась, понималась и применялась однозначно. В статье, с точки зрения автора, приводятся негативные тенденции, которые могут угрожать объективному процессу формирования языка криминалистики и меры, необходимые для того, чтобы сохранить этот язык для научных и прикладных исследований.*

Ключевые слова*: язык криминалистики, криминалистические понятия.*

THE «MODERN» LANGUAGE OF CRIMINOLOGY

Komarov Igor Mikhailovich
doctor of law, professor, head of the department of criminology
Lomonosov Moscow state university
Moscow, Russia
e-mail: mgu.ikomarov@mail.ru

Современные достижения криминалистики обуславливаются коллективными усилиями исследователей как для развития науки, так и для правоприменительной деятельности. Взаимоотношения участников системы «исследователь – правоприменитель», в первую очередь, связаны их

взаимопониманием на основе использования необходимого общего запаса понятий, одинаково отражаемых и используемых и в науке, и на практике. Научно-практический язык, в отличии от естественного, бытового языка отличается точностью и однозначностью употребляемых понятий.

Подмечено, что по мере развития науки совершенствуется ее язык, его структура и содержание приобретают строго определенный характер, понятия и суждения становятся все более общими и аргументированными, улучшается системная связанность научных высказываний. Понятийный аппарат совершенствуется, а это, в свою очередь, позволяет более точно отражать действительность.

Как любая другая отрасль научного знания криминалистика имеет свой язык. Его основным предназначением является функция придания большей точности и однозначности употребимым специальным терминам. Это средство и способ реализации криминалистического научного мышления, обусловленного объектом и предметом исследования.

Язык криминалистики имеет тесные связи с естественным, бытовым языком, посредством которого осуществляется не только толкование, но и всеобщее осмысление учеными и практиками научных и практических положений, выраженных в понятийном аппарате науки. «Увлечение» естественным языком в процессе научно-практического общения по криминалистической тематике неизбежно влечет за собой неопределенность толкований отдельных криминалистических понятий, что, зачастую, искажает понимание обоснованных научных положений. Однозначное же толкование введенных криминалистикой понятий к установленным в процессе научного исследования явлениям, предметам и процессам имеет важное значение для всей познавательной деятельности в науке и практике, в первую очередь для эмпирической проверки этих понятий, посредствам правоприменительной деятельности.

Отношения естественного и формализованного научного языка в развитии правовой науки на протяжении трех последних десятилетий является предметом спора, который определился двумя позициями: идеей использования естественного (общеупотребительного) языка [1, с. 90] и взглядов о возможности сочетания общеупотребительных и специальных юридических терминов (естественного и формализованного языков) [2, с. 263 – 264; 153 – 154].

В этой связи в отношении языка криминалистики можно с уверенностью сказать, что в его основе лежал не только естественный язык, но и часто употребимые устоявшиеся формализованные понятия естественных и технических наук. Поэтому очевидно – язык криминалистики представлял и представляет собой разумное сочетание естественного и формализованного языка.

Общие процессы формирования языка науки соответствуют и формированию языка криминалистики, который представляет собой «систему общих и частных понятий, выражаемых определениями и обозначениями (знаками, терминами)» [3 с. 183].

Под понятием, логика понимает целостную совокупность суждений о каком-либо объекте. Определение понятия раскрывает его содержание, посредством указания на существенные признаки объектов, объединенных данным понятием. Однако, как отмечали специалисты в области системных исследований «каждое научное понятие существует в языке науки не изолировано, само по себе, а лишь в системе связанных с ним понятий, относящихся к одному и тому же предмету изучения, и лишь в этой системе оно приобретает свой смысл и значение» [4, с. 31]. Данный тезис, как никогда, актуален для современной криминалистики, чья система понятия – важнейшая часть ее языка, который не так давно вступил в стадию активной формализации.

Логическая категория, именуемая понятием, является «элементарной частицей» познания, поэтому познание как отражение субъектом объективной реальности в конечном итоге есть процесс формирования понятий. Венгерский логик Б. Фогараши так определяет этот инструмент познания «понятие есть высший продукт человеческого мозга, высший продукт материи, основная форма мышления, выражающаяся в звуковом языке; оно путем обобщения выделяет общие элементы объективного внешнего мира, предметов и существующих между ними связей, резюмирует их и таким образом отражает в мыслях определенные части и связи объективной действительности» [5, с. 150].

В соответствии со своим гносеологическим статусом понятия ядро познавательной деятельности. Реальным познавательным средством являются чувства субъекта познания, связанные с его мыслью, то есть с понятием. Формирование понятия многокомпонентный процесс, связанный с мыслительной и практической деятельностью субъекта познания. Однако для того, чтобы понятие активно участвовало в познавательной деятельности оно должно быть правильно и точно определено. На определения, как на существенные основания опираются все субъекты расследования преступлений, так как они определяют и дисциплинируют обоснованное криминалистическое мышление. Достоинство определенных криминалистических понятий заключается в том, что «они являются наиболее адекватными природе познавательного процесса средствами оптимальной концентрации знания в форме единой мысли, ибо в них подытоживается главное» [6, с. 76].

Все, что изложено выше, полагаем, криминалистам должно быть хорошо известно.

Однако ознакомление с рядом криминалистических исследований последних лет свидетельствует о том, что в них просматривается тенденция, связанная с определениями понятий, которая не всегда соответствуют требованиям теории, на которые мы уже обратили внимание.

Отметим, например, что в ряде монографических и диссертационных исследований их авторы предпринимают попытки дать определения понятий, которые уже устоялись в криминалистике и необходимость в их пересмотре в общем отсутствует, так как она не вызвана изменением условий существования уже определенных явлений, предметов и процессов.

Так, например, в последнее время, по понятным причинам особую актуальность приобрели криминалистические исследования, связанные с экстремизмом и экстремистской деятельностью.

В этих работах авторы предпринимали попытки обоснования определения «экстремистская деятельность». Однако это понятие было определено еще в ФЗ №114 от 25 июля 2002 года и нет никакой необходимости определять его снова в исследованиях, посвященных разработке методик расследования этих преступлений, тем более выносить, как это делалось не раз, данное определение на защиту в качестве новизны исследования.

Не редки случаи, когда авторы в своих работах определяют понятия, которые давно определены в криминалистике и нет необходимости давать их новые определения, по причине того, что эти определения ничего нового в науку не привносят.

По понятным всем причинам мы не ссылаемся на конкретные исследования, но в качестве обезличенного примера приведу ситуацию, когда на защиту выносится определения понятия «планирование расследования по уголовному делу». Определение этого понятия известно криминалистам с 1957 года, когда профессоры А.Н. Васильев, Г.Н. Мудьюгин и Н.А. Якубович дали его в своей фундаментальной работе «Планирование расследования преступлений» и это определение не вызвало возражение.

И этот случай не единичный.

Порой мы, исследуя ту или иную проблему, забываем устоявшийся методологический принцип, в кратком виде гласящий: «Не следует множить сущее без необходимости» или «Многообразие не следует предполагать без необходимости».

Проблема дачи определений криминалистических понятий связана, как было отмечено, не только с антинаучным и ненужным «приумножением сущностей». Она более сложная по причине того, что многие молодые криминалисты, которые грешат этим занятием, не в полной мере владеют методологией формулирования определений, как совершенствуемых, так и вновь создаваемых.

Причину такой ситуации мы, в значительной мере, видим в их слабой теоретической подготовке к этому важному виду научной деятельности. В частности, анализ ряда работ свидетельствует о том, что их авторы не знают о необходимости формирования в первую очередь концепции искомого понятия, которую следует класть в основу его разработки, не понимают какое определение предполагается в итоге сформулировать – номинальное, аналитическое или синтетическое, а также какие существенные признаки для этого следует отыскать и аргументировать. Вся эта работа скорее всего ведется по наитию, а не на основе устоявшейся научной методологии. По этой причине определенное понятие может быть ущербным, а запущенное в криминалистический оборот оно принесет больше вреда чем пользы.

Нет понимания и того факта, что научное определение того или иного понятия всегда связано с его сущностью, а прикладной аспект выражается в

определении, данном на уровне явления, что всегда актуально для правоприменительной практики.

Криминалистам старшего поколения хорошо известны работы выдающихся отечественных ученых Дмитрия Павловича Горского, Владимира Ивановича Кондаурова и других, в которых детально описан процесс формирования определений научных понятий, что и в настоящее время является актуальной базой для этого вида деятельности в криминалистике.

По причине нарушения требований языка криминалистики страдает и современная методология научных исследований.

Так, например, в работах часто допускается не вполне корректное использование понятия «типовая» в отношении характеристики тех или иных практикоориентированных понятий (следственных ситуаций, следственные версии и пр.). Известно, что аутентичное толкование понятия «типовая» означает – соответствующая определенному типу, образцу, модели, то есть стандартная, однажды данная, то есть типовым можно называть научноопределенное понятие. Обобщение результатов судебно-следственной практики и выделение на этой основе наиболее часто повторяющихся в определенном пространственно-временном континууме свойств того или иного явления, предмета или процесса является «типичным», то есть воплощающими в себе характерные особенности какого-либо типа указанных явлений, предметов или процессов.

В этой связи уместно упомянуть, что достаточно часто понятие «следственная ситуация» представляется как типичная, между тем «следственная ситуация», как понятие является категорией науки криминалистики и выступает как модель, главным образом информационного характера, типичных ситуаций расследования. Как и любая модель, следственная ситуация в таком ее понимании ограничивает себя лишь наиболее значимыми, наиболее типичными свойствами и признаками тех ситуаций расследования конкретных преступлений, моделью которых она выступает. К ним и должны создаваться криминалистические средства разрешения реальных ситуаций расследования.

Язык криминалистики отличается от языка уголовного процесса, выраженного в понятиях, определенных наукой уголовного процесса и действующим уголовно-процессуальным законодательством. Поэтому правильно определять особенности организационных и проверочных мероприятий не на стадии возбуждения уголовного дела, как это часто встречается в криминалистических исследованиях, а в ходе доследственной проверки, которая является частью криминалистического понятия – первоначальный этап расследования.

Не всегда в работах авторы видят различие в понятиях – «система» и «структура», ставя между ними знак равенства. Однако понятие «структура» отражает характер связи между элементами системы, а не сами элементы, что важно, например, для описания содержания такой категории как криминалистическая характеристика преступлений.

В диссертационных исследованиях последних лет обращает на себя внимание тот факт, что соискатели, нарушая установленный понятиями языка криминалистики порядок, не видят разницы между частной, групповой и видовой методиками расследования преступлений, назначением криминалистической классификации преступлений, научными и практическими методами познания и т.п.

Последнее время в научно-квалификационных работах стали встречаться факты того, что криминалистический объект исследования, вопреки устоявшемуся в криминалистике языку, определяется через «общественные отношения». Между тем, криминалистика не изучала и не изучает никакие «общественные отношения», это прерогатива отраслевых юридических наук, которые изучают общественные отношения в форме правоотношений, а наша наука в качестве объекта исследует преступную деятельность и законную деятельность.

Можно и далее приводить примеры того, как по причинам различного характера, коверкается и искажается язык криминалистики. Однако мы не видим в этом необходимости по причине того, что, важно вовремя заметить эту негативную тенденцию и обратив на нее внимание научной общественности принять должные меры к «лечению» образовавшейся проблемы.

Список литературы

1. Прянишников, Е.А. Терминология уголовно-процессуального законодательства / Е.А. Прянишников // Правоведение. 1968. № 6. С. 88-96.

2. Белкин, Р.С. Курс криминалистики. Т. 1.; Пиголкин А.С. Подготовка проектов нормативных актов. М., 1968.

3. Белкин, Р.С. Курс криминалистики: Учеб. пособие для вузов. 3-е изд., дополненное / Р.С. Белкин. М.: ЮНИТИ-ДАНА, Закон и право, 2001.

4. Блауберг, В.В. Системный подход: предпосылки, трудности, проблемы / В.В. Блауберг, В.Н. Садовский, Э.Н. Юдин. М., 1969.

5. Фогараши Б. Логика / Б. Фогарши. М., 1959. 496 с.

6. Кондауров, В.И. Процесс формирования научного знания (онтологический, гносеологический и логический аспекты): Монография / В.И. Кондауров. М.: ИНФРА-М, 2014. 128 с.

УДК 343.985

ОСОБЕННОСТИ ОСМОТРА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Костюкевич Денис Викторович,
Учреждение образования «Академия Министерства внутренних дел Республики Беларусь»,
г. Минск, Республика Беларусь
e-mail: valevachi@tut.by

Аннотация: *в статье рассматриваются основания и процессуальный порядок нового для белорусского законодательства следственного действия — осмотр компьютерной информации. Определяются свойства компьютерной информации как объекта криминалистического исследования, а также тактические особенности осмотра и фиксации компьютерной информации, раскрываются отдельные особенности данного следственного действия.*

Ключевые слова: *осмотр, компьютерная информация, компьютерная техника, следователь, протокол.*

ON THE USE OF A COGNITIVE APPROACH TO THE FORMATION AND IMPLEMENTATION OF THE LEGAL STATUS OF PARTICIPANTS IN CRIMINAL PROCEEDINGS

Kostyukevich Denis Viktorovich,
Educational Institution "Academy of the Ministry of Internal Affairs of the Republic of Belarus",
Minsk, Republic Of Belarus
e-mail: valevachi@tut.by

Abstract: *the article discusses the grounds and procedural order of a new investigative action for the Belarusian legislation — examination of computer information. The properties of computer information as an object of forensic research are determined, as well as the tactical features of the examination and fixation of computer information, and certain features of this investigative action are revealed.*

Keywords: *inspection, computer information, computer equipment, investigator, protocol.*

При совершении различных видов преступлений все чаще используется различная компьютерная техника, включая персональные компьютеры, ноутбуки, планшеты, смартфоны; задействуются иные коммуникационные устройства, многочисленные платежные инструменты, а также возможности интернета. Указанное выступает как основной источник электронных (цифровых) следов и, соответственно, может выступать доказательством преступной деятельности. Поэтому в 2021 году Уголовно-процессуальный кодекс Республики Беларусь (далее - УПК) был дополнен ст. 204-1 «Осмотр

компьютерной информации». Таким образом, осмотр компьютерной информации наряду с иными видами осмотров как места происшествия, трупа, местности, помещения, жилища и иного законного владения, предметов, документов, выделен в самостоятельное следственное действие. Обусловлено это специфичностью компьютерной информации как таковой – виртуальностью, то есть возможностью одновременно представляться в материальном виде (физическое наличие устройств, машинных носителей и др.) и нематериальным характером (сосредоточение различного массива данных в облачных сервисах) и определенным способом доступа. Законодатель закрепляя данную норму подчеркнул первостепенную важность именно самой компьютерной информации, а не компьютерной техники, которая по сути выступает посредником между пользователем и самой информацией и в определенных случаях может и не содержать на себе каких-либо следов.

Осмотр компьютерной информации, которая хранится на машинных носителях (сервере), расположенных на территории иностранных (в основном западных) государств, следователь может провести, находясь на своем рабочем месте или в ином месте. Тем самым отсутствует необходимость направления соответствующих международных поручений (просьб) на которые в условиях необъявленной полномасштабной гибридной войны [1] со стороны западных государств не всегда будет дан положительный ответ.

Основание для проведение осмотра компьютерной информации является традиционным как и для остальных видов осмотра, а именно наличие достаточных данных полагать, что в ходе этого следственного действия могут быть обнаружены следы преступления и иные материальные объекты, выяснены другие обстоятельства, имеющие значение для уголовного дела.

Порядок осмотра компьютерной информации зависит от ее вида и применения ее обладателем средств защиты. В случае если компьютерная информация защищена ее обладателем (например, требуется введение логина и пароля либо иных данных (например, биометрических данных (лицо, отпечаток пальца)) и требуется аутентификация пользователя или она содержит сведения, распространение и (или) предоставление которых ограничено (например, о частной жизни лица, его персональные данные, включая сведения, составляющие личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, касающиеся состояния его здоровья, составляющие охраняемую законом тайну, служебную информацию ограниченного распространения и т. д.), для осмотра такой информации законодателем предусмотрен ряд альтернативных требований:

- согласие обладателя компьютерной информации и его присутствие при осмотре (даже если он добровольно сообщил логин и пароль и не возражает против осмотра без его участия, его присутствие обязательно), что должно быть отражено в протоколе;

- постановление следователя, органа дознания, санкционированное прокурором или его заместителем, в котором обязательно отражаются обстоятельства совершенного преступления и основания для проведения

осмотра компьютерной информации, содержащейся в компьютерной системе, сети или на машинном носителе информации.

В случаях, не терпящих отлагательства, такой осмотр может быть проведен по постановлению следователя, органа дознания без санкции прокурора с последующим направлением ему в течение 24 часов сообщения о проведенном следственном действии, то есть так же, как и при осмотре жилища или иного законного владения.

В ходе осмотра компьютерной информации следователем, органом дознания могут производиться действия, предусмотренные функционалом информационных систем, информационных ресурсов, а также использоваться научно-технические средства, оборудование, аппаратура, приборы, компьютерные программы (например, Belkasoft Evidence Center «Мобильный криминалист», и т. д.). Их использование должно быть отражено в протоколе осмотра компьютерной техники.

Одним из наиболее эффективных средств фиксации проведения осмотра компьютерной информации и полученных результатов является использование снимков графического интерфейса приложений (скриншот) либо осуществление видеозаписи экрана, с отображением этапов ввода логина и пароля, переходов по ссылкам и просмотра непосредственно обнаруженной информации.

Целесообразно выделить следующие особенности составления протокола осмотра компьютерной информации:

- в случае одновременного осмотра устройства и компьютерной информации (например, мобильного телефона, ноутбука) составляется протокол осмотра предметов и компьютерной информации с указанием ст. 203, 204 и 204-1 УПК, поскольку объектом осмотра, помимо компьютерной информации, является и компьютерное устройство;

- в случае осмотра компьютерной информации в ходе осмотра места происшествия (жилища или иного законного владения), проводимого по постановлению следователя без санкции прокурора, в протоколе осмотра указываются ст. 204 и 204-1 УПК;

- если в ходе осмотра жилища или иного законного владения, не являющегося местом происшествия, проводимого с согласия собственника или проживающих в нем совершеннолетних лиц, возникает необходимость осмотреть компьютерную информацию, а обладатель информации против этого, то осмотр жилища приостанавливается для вынесения постановления о проведении осмотра жилища и компьютерной информации по основанию, предусмотренному ст. 203 УПК, после чего осмотр возобновляется. Данная следственная ситуация относится к случаям, не терпящим отлагательства осмотра компьютерной информации, поскольку промедление может повлечь изменение или уничтожение информации. О проведенном осмотре жилища и компьютерной информации в течение 24 часов сообщается прокурору.

- осмотр компьютерной информации проводится без санкции прокурора, если она изъята при производстве санкционированных прокурором следственных действий. Данное правило распространяется на все

процессуальные действия, проводимые с санкции прокурора (осмотр жилища, выемка, обыск, проверка показаний на месте, требование о представлении информации и т. д.).

В то же время компьютерная информация может выступать объектом исследования судебной компьютерно-технической экспертизы и судебной экспертизы радиоэлектронных устройств. Экспертами при проведении указанных исследований осуществляется доступ к компьютерной информации, последующий поиск криминалистически значимых сведений, их исследование и сохранение. Постановления о назначении указанных экспертиз не требуют санкции прокурора, однако исследуемая компьютерная информация может относиться к той, распространение и (или) предоставление которой ограничено, о чем станет известно лишь в процессе производства процессуального действия. Данные обстоятельства необходимо учитывать после получения заключения эксперта с приложениями (например, оптическими дисками с компьютерной информацией), и в случае направления на экспертизу компьютерных устройств, изъятых в ходе процессуальных действий, не санкционированных прокурором, осмотр извлеченной в результате исследований компьютерной информации следует проводить в таком же порядке как и осмотр любой другой компьютерной информации и на нее распространяются все вышеперечисленные требования.

Таким образом, осмотр компьютерной информации представляет собой самостоятельное следственное действие целью которого является поиск, обнаружение, фиксация и изъятие компьютерной информация локального и удаленного доступа содержащей на себе признаки какого-либо преступления, либо представляющая интерес в ходе расследования уголовного дела.

Список литературы

1. Лукашенко: против Беларуси развязана полномасштабная гибридная война // URL: https://www.belta.by/president/view/lukashenko-protiv-belarusi-razvjazana-polnomasshtabnaja-gibridnaja-vojna-513103-2022/ (дата доступа 24.06.2016).

УДК 343.98

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ЦИФРОВЫХ ДВОЙНИКОВ МЕСТА ПРОИСШЕСТВИЯ В РОССИЙСКОМ СУДОПРОИЗВОДСТВЕ

[1]Костюченко Олег Георгиевич
старший следователь-криминалист,
[2]Бойко Антон Николаевич
кандидат технических наук, доцент
[2]Бертовский Лев Владимирович
доктор юридических наук, профессор
[2]Тимошенков Сергей Петрович
доктор технических наук, профессор

[1]Следственный комитет Российской Федерации,
[2]Национальный исследовательский университет «МИЭТ»
г. Москва, Россия
[1]email: kostucenkooleg746@gmail.com
[2]email: anton.bojko@mail.ru

Аннотация: *рассмотрены особенности создания и применения цифровых двойников места происшествия в качестве перспективного инструмента криминалистической техники. Проведен анализ развития данного направления с применением понятия «технологического пакета». Показано, что внедрение цифровых двойников в судопроизводство позволит перейти на новый уровень расследования и рассмотрения уголовных дел. Для развития данного направления необходимо, в том числе, развитие гуманитарных технологий, подготовки кадров, нормативно-законодательной базы.*

Ключевые слова: *криминалистическая техника, цифровой двойник места происшествия, цифровая копия, 3D-визуализация, технологический пакет, цифровое судопроизводство.*

PROSPECTS FOR THE APPLICATION OF DIGITAL TWINS OF INCIDENT SITES IN RUSSIAN LEGAL PROCEEDINGS

[1]Kostyuchenko Oleg Georgievich
senior forensic investigator
[2]Boiko Anton Nikolaevich
candidate of technical sciences, Associate Professor
[2]Bertovsky Lev Vladimirovich
doctor of law, professor
[2]Timoshenkov Sergey Petrovich
doctor of technical sciences, professor
[1]Investigative committee of the Russian Federation
[2]National research university of electronic technology

Moscow, Russia
[1]*email: kostucenkooleg746@gmail.com*
[2]*email: anton.bojko@mail.ru*

Abstract: *the features of the creation and use of digital twins of the scene as a promising tool for forensic technology are considered. An analysis of the development of this direction was carried out using the concept of "technological cluster". It is shown that the introduction of digital twins in legal proceedings will allow moving to a new level of investigation and consideration of criminal cases. For the development of this area, it is necessary, among other things, to develop humanitarian technologies, personnel training, and the regulatory and legislative framework.*

Keywords: *forensic technology, digital twin of the scene, digital copy, 3D visualization, technology cluster, digital litigation.*

Понятие «цифрового двойника» используется, в первую очередь, в промышленности, как компьютерное представление физического объекта, включающее его трёхмерную геометрию, характеристики и параметры функционирования, данные об окружающей среде и связях с другими объектами [1, 75]. В то время как использование программных аналогов позволяет увеличить эффективность процессов разработки и эксплуатации промышленных изделий, применение цифровых двойников в криминалистике способствует повышению эффективности работы правоохранительных органов[2].

Актуальными задачами судебной криминалистики, которые могут быть решены с помощью цифровых двойников, являются:

– создание трёхмерной цифровой копии места происшествия с высокой детализацией отдельных элементов (следы рук, ног, биологические следы), и высокой точностью (вплоть до папиллярных узоров) с целью последующего воспроизводства (создания моделей, слепков и т.д.), идентификации и проведении экспертных исследований;

– наглядная демонстрация места и картины происшествия при помощи созданной виртуальной модели, например, демонстрация в ходе судебного процесса участникам суда;

– возвращение на место происшествия в виртуальной реальности для повторного или дополнительного осмотра, получения новых данных, проведения различных судебных экспертиз (трасологической, дактилоскопической, медико-криминалистической, комплексной ситуационной и др.);

– возможность удалённой работы с цифровой моделью, что позволяет привлекать к расследованию любых специалистов и любых лиц, в том числе, находящихся на значительном расстоянии от места происшествия.

Использование современных технологий предполагает, что в будущем наиболее вероятной методикой использования цифрового двойника в криминалистике станет отображение полной материальной и виртуальной

картины места происшествия в цифровом формате, без составления каких-либо протоколов и письменных описаний. При производстве осмотра места происшествия, будет создаваться его 3D-модель, с внесением всех возможных размеров, географических координат и данных интересующих объектов, а также цифровой и эфирной информации. Также в этой модели будут отображаться различные следы преступления, в том числе папиллярные узоры пальцев рук, биологические вещества, следы крови, замытой крови, механические следы и следы борьбы, тепловые следы, состав окружающего воздуха и т.д. По итогу «сканирования места происшествия», программа указывает на интересующие предметы и объекты (образцы грунта, крови, орудие преступления, биологические следы и вещества, образцы воздуха и т.д.), которые необходимо изъять, для последующего проведения экспертных исследований. Помимо указанного, в цифровой двойник будут загружаться любые интересующие следствие данные, информационные сообщения, аудио и видео файлы с пояснениями, видеозаписи с камер видеонаблюдения, выводы экспертиз по изъятым объектам и предметам и т.д. Программа цифрового двойника места происшествия, позволит установить, чьи следы были обнаружены на месте происшествия и кому они принадлежат, например кровь или следы пальцев рук, какое-либо биологическое вещество. А программный анализ установит, например, подходит ли нож, обнаруженный на месте происшествия, к повреждениям, выявленным у потерпевшего, и является ли данный нож орудием преступления, какой механизм образования следов крови или следов борьбы на месте происшествии и т.д. Все результаты исследований, программой оформляются в виде выводов, которые будут передаваться вместе с цифровым двойником места происшествия в виде виртуальной модели, например, в суд или прокурору для принятия решения по данному делу.

Для создания цифровых трёхмерных копий в настоящее время используются различные методы, наиболее перспективными среди них являются активные методы 3D-сканирования с применением лазерного излучения [3]. Подобные устройства обеспечивают наилучшее разрешение, в меньшей степени зависимы от условий окружающей среды, процесс сканирование в большей степени автоматизирован и свободен от человеческих ошибок [4]. В то же время, не исчерпаны возможности и такого «традиционного» метода, как цифровая фотография. В методе фотограмметрии на основе нескольких фотоснимков с разных ракурсов может быть построена трёхмерная модель [5], а использование искусственного интеллекта и алгоритмов машинного обучения позволяет воссоздавать 3D-объекты по одной единственной фотографии [6].

За рубежом визуализация события преступления с использованием компьютерной 3D-модели выделилась в отдельную криминалистическую технологию, известную как «криминалистическая анимация» (forensic animation) [7,8]. Создаётся специализированное программное обеспечение, позволяющее создавать 2D и 3D-модели места происшествия, демонстрировать последовательность протекания событий, делает события наглядными для участников судебного разбирательства. Подобное программное обеспечение

создано также и в России, пример – программа «3D Свидетель», предназначенная для реконструкции мест преступлений, пожаров и дорожно-транспортных происшествий [9]. Для подготовки специалистов и студентов юридических специальностей разработано программное обеспечение «Виртуальный осмотр места происшествия» [10].

В российской следственной и судебной практике накапливается опыт применения 3D-моделирования мест и событий преступления. Например, с применением программ MicroSmith Poser и Agisoft PhotoScan была создана 3D-модель места происшествия, проведена визуализация криминального события и отдельных его этапов [2]. Полученные данные способствовали раскрытию преступления и формированию доказательной базы обвинения. В другом случае 3D-модель происшествия, выполненная в программе Blender 2.8 на основании протоколов и фототаблиц из материалов уголовного дела, использовалась в качестве визуального сопровождения речи прокурора в прениях сторон [11].

Исследования в области визуализации места и события преступления можно охарактеризовать как отдельное научно-техническое направление, для оценки состояния и управлением развития которого удобно использовать понятие «технологического пакета» [12]. Технологический пакет формально определяется как «генетически и функционально связанная совокупность технологий, обладающая системными свойствами» и включает в себя как технические, так и гуманитарные технологии. Если рассматривать «цифровой двойник места происшествия» как технологический пакет, то в качестве очевидных технических средств для его функционирования можно выделить следующие:

- персональные компьютеры и смартфоны;
- специализированное программное обеспечение;
- фототехника и лазерные 3D-сканеры;
- средства хранения и передачи данных;
- искусственный интеллект и методы обработки больших данных.

Гуманитарные технологии, определяющие развитие данного пакета:

- образовательные программы (программирование, использование средств 3D-сканирования и т.п.);
- законодательная и нормативная база создания и применения цифровых двойников в судебной практике.

При анализе нельзя обойти стороной вопросы фальсификации или непреднамеренного искажения цифровых объектов. Насколько особенности программы, квалификация и личность пользователя программы могут повлиять на интерпретацию и воссоздание событий преступления? Каким образом визуальные особенности 3D-моделей влияют на их психологическое восприятие, может ли это быть использовано для манипулирования мнением судей и присяжных? Также необходимо будет разрешить неизбежные противоречия между эффективностью программно-аппаратных комплексов и

их стоимостью, между сложностью комплексов и быстротой их освоения, сложностью и надёжностью применения, и т.д.

Развитие технологических пакетов может быть описано *S*-образной кривой Альтшуллера по какому-либо из ключевых параметров. При анализе пакета «цифровой двойник в судопроизводстве» в качестве такого параметра может выступать количество судебных заседаний с использованием криминалистической анимации. Очевидно, судя по данному параметру, что в России технологический пакет «цифровое судопроизводство» находится в начальной фазе – фазе накопления ресурсов, знаний и технологий. Уровень развития технологического пакета также можно оценить по количеству научных публикаций в исследуемой области, что для направления криминалистической анимации было сделано в работе [4]. Количество публикаций российских авторов в данной сфере на порядок меньше, чем авторов из США, значительно меньше, чем авторов из Австралии, Канады, Китая, Великобритании, Германии, Индии, Италии, Нидерландов, Швейцарии, Польши и Малайзии. Примерно на одном уровне по количеству публикаций Россия находится с Бельгией, Грецией и Румынией.

Таким образом, проведенный анализ создания и использования цифровых двойников в судопроизводстве показывает, что внедрение подобных разработок позволит качественно перейти на новый уровень расследования и рассмотрения уголовных дел. Актуальным является внедрение новых технических решений, накопление практического опыта, а также развитие так называемых гуманитарных технологий – образования и подготовки соответствующих специалистов, нормативно-законодательной базы.

Список литературы

1. Трачук, А.В. Трансформация промышленности в условиях четвертой промышленной революции: монография / А.В. Трачук, Н.В. Линдер, И.В. Тарасов / под ред. проф. А.В. Трачука. СПб.: Реальная экономика, 2018. 147 с.

2. Леонова, Е.Н. Визуализация реконструкции криминального события методом 3D-моделирования / Е.Н. Леонова, Ю.П. Шакирьянова, С.В. Леонов, А.С. Мосоян, Ю.И. Пиголкин // Судебно-медицинская экспертиза.2018. № 61 (1). С.52-54.

3. Еремченко, В.И. Принципы работы 3d-сканера и его использование для фиксации места происшествия / В.И. Еремченко // Общество и право.№1 (75). 2021.С. 61-65.

4. Maneli, M.A., Isafiade, O.E. 3D Forensic Crime Scene Reconstruction Involving Immersive Technology: A Systematic Literature Review, IEEE Access, vol. 10, 2022. P. 88821-88857.

5. Кугуракова, В.В. Цифровое представление в виртуальной реальности места происшествия как инструмент уголовного судопроизводства / В.В. Кугуртакова, И.О. Антонов, Б.В. Гончаренко, А.А. Чайбар // Программные системы: теория и приложения. 2022. С.193–223.

6. Khan M. S. U., Pagani A., Liwicki M., Stricker D., Afzal M. Z., Three-Dimensional Reconstruction from a Single RGB Image Using Deep Learning: A Review. J. Imaging, 8, 225, 2022.

7. Холопов, А.В. Компьютерные программы 3D-визуализации события преступления / А.В. Холопов // Криминалисть. 2021. № 3(36). С. 70-76.

8. Sainato, V. A., Giner, J. A. "Forensic Technologies in the Courtroom: A Multi-Disciplinary Analysis." Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice, edited by Information Resources Management Association, IGI Global, 2020. pp. 291-307.

9. Программное обеспечение «3D Свидетель», ООО «Криммедтех» // URL: https://kmtkazan.ru/node/256?ysclid=ldb7bd9en2540073976 (дата обращения 25.01.2023).

10. Программное обеспечение «Виртуальный осмотр места происшествия», АО «СофтЛайн Трейд» // URL: https://store.softline.ru/fsa3d/virtualnyiy-osmotr-mesta-proisshestviya/?ysclid=ldbc1c7j82907363053 (дата обращения: 25.01.2023).

11. Крысин, В.В. Цифровые технологии как средство обеспечения наглядности речи государственного обвинителя в прениях сторон с участием коллегии присяжных заседателей / В.В. Крысин // Следственная практика. Вып. 210. 2020. С.98-101.

12. Желтов, А.О. Понятие технологического пакета / А.О. Желтов // Инновации.2007. № 12. С.48-52.

УДК 343.98

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ЕДИНОЙ ГОСУДАРСТВЕННОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ В ВЫЯВЛЕНИИ, РАСКРЫТИИ И РАССЛЕДОВАНИИ НЕЗАКОННОГО ОБОРОТА ДРЕВЕСИНЫ

Кулик Валерия Андреевна,
адъюнкт 3-го факультета (подготовки научных и научно-педагогических кадров)
Академия управления МВД России,
г. Москва, Россия
email: leonteva1019@bk.ru

Аннотация: *в статье на основе анализа функционирования единой государственной автоматизированной информационной системы учета древесины и сделок с ней, рассмотрены возможности ее использования в целях получения информации, имеющей значения для расследования уголовных дел о незаконном обороте древесины. На основе изучения судебной практики выявлены закономерности следообразования при совершении отдельных видов преступлений в сфере незаконного оборота древесины, находящие отражение в ЛесЕГАИС. Предложены рекомендации по использованию данных системы в*

процессе выявления и расследования преступлений рассматриваемой категории.

Ключевые слова: *ЛесЕГАИС, контрабанда, незаконная рубка, оборот древесины, договор купли-продажи, таможенная декларация, места хранения древесины, транспортировка древесины.*

POSSIBILITIES OF USING A SINGLE STATE AUTOMATED INFORMATION SYSTEM FOR WOOD ACCOUNTING AND TRANSACTIONS THEREWITH IN DETECTING, DISCLOSING AND INVESTIGATING ILLEGAL TIMBER TRAFFICKING

Kulik Valeriia Andreevna,
Adjunct of the 3rd faculty (training of scientific and scientific-pedagogical personnel)
Management Academy of the Ministry of the interior of Russia,
Moscow, Russian Federation
email: leonteva1019@bk.ru

Abstract: *the article, based on an analysis of the functioning of the unified state automated information system for wood accounting and transactions with it, considers the possibilities of its use in order to obtain information that is important for investigating criminal cases of illegal timber trafficking. Based on the study of judicial practice, patterns of tracking in the commission of certain types of crimes in the field of illegal timber trafficking were revealed, which are reflected in LesEGAIS. Recommendations have been proposed for the use of system data in the process of identifying and investigating crimes of the category under consideration.*

Keywords: *ForestEGAIS, smuggling, illegal logging, timber turnover, sale and purchase agreement, customs declaration, wood storage places, wood transportation.*

На территории Российской Федерации с 1 января 2016 года введена в эксплуатацию Единая государственная автоматизированная информационная система учета древесины и сделок с ней (далее – ЛесЕГАИС), целью которой стало создание электронного документооборота, однако работа системы не позволяла отслеживать перемещение древесины.

Президент Российской Федерации 29 сентября 2020 года провел совещания о развитии и декриминализации лесного комплекса, в ходе которого указал на проблему сокращения доли России в мировой торговле древесиной, что связано с «серыми схемами» её использования. По итогам совещания утвержден перечень поручений, направленных на создание единой системы, позволяющей отслеживать сделки от начала заготовки древесины до момента ее продажи, как на территории нашей страны, так и за ее пределами. В связи с вышеуказанным, 1 января 2021 года введен в эксплуатацию обновленный

ЛесЕГАИС, запрещающий транспортировку древесины без создания электронного сопроводительного документа, а также ввел обязательную регистрацию мест временного хранения древесины и объекты лесоперерабатывающей инфраструктуры [1].

В настоящее время, ЛесЕГАИС выступает основной системой электронного контроля за сделками, осуществляемыми с древесиной. На основе анализ функционирования ЛесЕГАИС, рассмотрим возможности его использования при установлении обстоятельств, подлежащих доказыванию по уголовному делу.

Согласно ч. 6 ст. 50.6 Лесного кодекса Российской Федерации (далее – ЛК РФ) [2] юридические лица и индивидуальные предприниматели, занимающиеся деятельностью в сфере лесопромышленного комплекса, обязаны зарегистрироваться в ЛесЕГАИС, с целью прослеживаемости их деятельности и контроля объема лесных ресурсов, находящейся на балансе.

Изучение ЛесЕГАИС позволяет получить сведения о предполагаемом преступнике; содержит информацию о наименовании организации и сведения о ее руководителе, о государственной регистрации юридического лица, идентификационный номер налогоплательщика, фактический адрес организации. В отношении индивидуального предпринимателя система хранит сведения о государственной регистрации, паспортные данные физического лица, идентификационный номер налогоплательщика.

При получении информации о том, что некая организация или индивидуальный предприниматель осуществил незаконную рубку или иной вид сделки с древесиной, должностное лицо, осуществляющее проверку сообщения о преступлении, первоначально может обратиться в систему ЛесЕГАИС, с целью установления зарегистрирован ли подозреваемый в системе, и если зарегистрирован, то запросить данные о нем.

Указанная информация в системе также позволяет установить объем древесины, находящейся на балансе у юридического лица или индивидуального предпринимателя. Законным способом древесину на праве собственности возможно получить только при наличии следующих условий: лицо занимается непосредственно рубкой древесины; лицо не занимается рубкой, а приобретает ее у лесозаготовителей.

В первом случае, при непосредственном осуществлении лесозаготовки, организация или индивидуальный предприниматель имеет право осуществлять рубку только на основании заключенного с лесничеством договора аренды или договора купли-продажи (ст. ст. 29-29.1 ЛК РФ), сведения о которых вносятся в ЛесЕГАИС. Данные в систему вносят на основе создания декларации, в которой помимо сведений о лице, содержатся также сведения об арендованной лесосеке, с указанием лесничества, квартала, выдела, номера деляны, а также разрешенный объем к вырубке, срок рубки.

Во втором случае, при приобретении древесины продавец также обязан создать сделку в системе, по правилам составления декларации, покупатель

обязан ее подписать электронной подписью, в связи с чем в ЛесЕГАИС загрузятся такие сведения, как данные продавца, данные покупателя, место отгрузки древесины, место хранение древесины у нового приобретателя, объем преданной древесины, породный состав, время продажи, сведение о транспортом средстве, перевозящем древесину [3].

В целях получения сведений о сделках проведенных с древесиной конкретной организацией, можно получить и ряд дополнительной информации, связанной, как с приобретателем, так и качественными и количественными характеристиками древесины. При этом, необходимо понимать, что в случае продажи древесины, физическим лица, сведения о них в ЛесЕГАИС не хранятся, поскольку они не являются участниками оборота, то есть не имеют право отчуждать ее, в связи с чем не обязаны отчитываться о приобретаемых лесных ресурсах [4].

С учетом вышеизложенного, индивидуальный предприниматель или юридическое лицо, деятельность которых связана с лесопромышленным комплексом, обязаны отражать в ЛесЕГАИС данные о места хранения древесины или объектах лесоперерабатывающей инфраструктуры. В данном случае в системе хранятся такие данные, как идентификационный номер места хранения, данные собственника древесины, качественные и количественные характеристики, определение объема древесины до и поле переработки. Лица, осуществляющие сделки с древесиной не имеют право осуществлять продажу лесных ресурсов со складов, не зарегистрированных в системе [5].

Поскольку ЛесЕГАИС, прежде всего, создан в целях контроля за осуществляемыми сделками, то в системе можно получить сведения об объеме древесины, который был незаконным образом продан. Также сведения возможно получить путем сравнения данных находящегося на балансе объема древесины и осуществлённых сделкой с ней. При возникновении подобных ситуаций система выдаст ошибку, и данный факт станет основанием для проверки юридического лица или индивидуального предпринимателя. Например, в случаях выявления расхождения между фактическим объемом заготовленной древесины и объемом разрешенным к вырубке, который указывается в декларации, проверка в данном случае сотрудниками лесного хозяйства должна быть проведена в срок не позднее пяти рабочих дней [6].

Бородина О.Б., Гальченко С.А., Рассказова А.А., Чуксин И.В., рассматривают ЛесЕГАИС как переходную систему к федеральной государственной информационной системе, в связи с чем выделяют ее несовершенство, и констатируют, что существующая система не способна контролировать весь оборот древесины [7]. Однако, несмотря на существующие проблемы, проанализируем возможности применения ЛесЕГАИС, с учетом решаемых ей задач, на сегодняшний день.

ЛесЕГАИС, с учетом вносимых в него изменений, действует всего несколько лет, в рамках исследования проанализировано 300 обвинительных приговоров, по которым в настоящее время выявлены попытки обхода системы в 8 % дел [8]. По итогам изучения судебной практики, установлено, что такие попытки предпринимались преимущественно при совершении контрабанды

древесины (60 % дел); незаконной рубки и перевозки древесины (27 % дел) и незаконной рубки (13 % дел). На примере указанных категорий уголовных дел рассмотрим возможности использования ЛесЕГАИС в целях решения задач по установлению и сбору доказательственной информации.

Так, контрабанда древесины, связана с манипуляциями при вводе данных в ЛесЕГАИС, который осуществлялся двумя способами:

– попытка заключения договора купли-продажи с организацией, где лесные ресурсы фактические не переходили в собственность покупателя;

– инсценировка (создание видимости заключения договора купли-продажи).

В первом случае лицо приискивало организацию, которая бы согласилась заключить с ним мнимую сделку, однако в 90 % случаев покупатель достигал фиктивности сделки, где продавец не был осведомлён о преступных планах лица. Например, 28 июля 2022 года Кировский районный суд Красноярского края вынес обвинительный приговор № 1-34/22 в отношении индивидуального предпринимателя, который достиг договоренности с организацией о приобретении у нее древесины, но подсудимый не собирался реально покупать лесные ресурсы, в связи с чем после заключения электронного договора купли-продажи, лицо внесло сведения о нем в таможенную декларацию. Однако, по причине того, что сделка в действительности не состоялась, продавец не подал в ЛесЕГАИС отчет о данной сделке, и договор купли-продажи был аннулирован. Данный факт выявлен сотрудниками таможенных органов, в ходе проверки происхождения древесины по ЛесЕГАИС [9].

Отсюда следует, что для достижения корыстной цели подсудимому необходима договорённость с продавцом, однако поскольку лица не готовы совершать преступления ради корыстных целей покупателя, поэтому недобросовестные экспортеры прибегают к указанию в таможенных декларациях сведений договора купли-продажи, не соответствующего действительным характеристикам древесины. Например, Черновский районный суд Забайкальского края 7 февраля 2022 года вынес обвинительный приговор № 1-25/22 в отношении руководителя юридического лица, который зарегистрировал индивидуального предпринимателя, с целью осуществления с ним сделок в ЛесЕГАИС. Так, имея доступ в системе и к организации, и к индивидуальному предпринимателю, подсудимый оформил мнимую электронную сделку о продаже лесных ресурсов. Данный договор был внесен в таможенную декларацию, однако сведения о первоначальном собственнике древесины не соответствовали действительности. В ходе проверки таможенных деклараций, установлено три факта контрабанды организацией ООО «ЛД», где руководитель от имени индивидуального предпринимателя осуществил инсценировку продажи древесины, однако проверкой выявлено, что в период заключения договора купли-продажи предприниматель подал в систему отчет о том, что на его балансе нет древесины [10].

При одновременном осуществлении незаконной рубки и перевозки древесины (ст. ст. 260 и 191.1 УК РФ), как правило, подсудимые действовали

на основании заключенного договора на рубку древесины, однако превышая объемы за счет осуществления незаконной заготовки в местах, не предусмотренных договором. Например, 21 февраля 2022 года Нелидовский межрайонный суд Тверской области вынес обвинительный приговор № 1-2/22 в отношении Ш., который осуществлял лесозаготовительную деятельность, на что у него был заключённый договор купли-продажи. Однако у Ш. возник преступный умысел на рубку насаждений хвойных пород, которые в договоре не указаны. По вышеуказанному договору он несколько раз перевозил незаконно срубленные лесные ресурсы, о чем не оповестил иных учредителей организации, данный факт был выявлен самой компанией, в процессе проведения инвентаризаций, и проверки лесосеки, где было установлена незаконная рубка на 1967 куб м. Также лесным хозяйством установлено, что по ЛесЕГАИС разрешение на рубку не выдавалось, однако в пограничной лесосеке ведется рубка по договору купли-продажи с организацией ООО «Л.» [11].

Значительно реже использовались данные ЛесЕГАИС в случаях незаконной рубки (всего в 13 % дел). В таких случаях данные ЛесЕГАИС необходимы в качестве подтверждения сделки между лесным хозяйством и задержанным, а точнее отсутствие такой сделки. Например, Верещагинский районный суд Пермского края 6 июля 2021 года вынес общительный приговор № 1-147/21 в отношении С., который совершил рубку лесных ресурсов без правоустанавливающих документов. С., имея на руках 107 договоров купли-продажи на заготовку древесины для собственных нужд, полученных от граждан села, в целях осуществления для них рубки. Однако имея умысел на заготовку сырорастущих деревьев, осуществил незаконную рубку хвойного леса. В ходе осмотров лесосек и сравнения данных с ЛесЕГАИС установлено, что договоры купли-продажи на заготовку для собственных нужд в установленных лесосеках не заключались [12].

При изучении организации работы ЛесЕГАИС и судебной практики по фактам выявления незаконного оборота древесины установлены закономерности:

– ЛесЕГАИС эффективен при использовании его сотрудниками таможенных органов, поскольку осуществить вывоз древесины за пределы Российской Федерации без сопроводительных таможенных документов невозможно. Так, с 13 июля 2023 года в целях контроля за перевозимой древесиной, сотрудники таможенных органов обязаны сопоставлять предоставленные сведения перевозчиком с данными в системе ЛесЕГАИС. Однако данное сопоставление происходит путем запроса данных в Лесном хозяйстве, поскольку переходный период системы, в рамках которой таможенный орган получит доступ ЛесЕГАИС продлен до 2025 года. Данная мера представляется эффективной, но в настоящее время она действует в рамках проверок, при возникновении сомнений у сотрудников о законности происхождения древесины [13].

– цифровизация лесной отрасли не может существовать отдельно от фактических проверок индивидуальных предпринимателей и юридических

лиц. По этим причинам, предлагаем увеличить количество рейдовых мероприятий в отношении индивидуальных предпринимателей и юридических лиц, осуществляющих оборот лесных насаждений на внутреннем рынке Российской Федерации, как наиболее уязвимого вида деятельности.

Таким образом, ЛесЕГАИС позволяет должностным лицам, осуществляющим предварительное расследование получить такие следующие данные: наименование юридического лица или индивидуального предпринимателя; места рубок древесины и ее хранения, переработки; первоначального и конечного собственника древесина в рамках заключённого договора купли-продажи. Также, данная система позволяет проследить механизм сокрытия преступных действий, в случаях выявления «подставных» организаций, созданных для нелегального оборота или же при выявлении не подтверждения электронных сделок; с использованием, в целях перевозки, договора купли-продажи, несоответствующего фактически транспортируемому объему.

Вместе с тем, наибольшую эффективность и результативность возможно достичь только в случае обеспечения доступа сотрудников к ЛесЕГАИС в режиме реального времени для оперативного сопоставления фактических данных.

Список литературы

1. Перечень поручений по итогам совещания по вопросам развития и декриминализации лесного комплекса от 29 сентября 2020 года // URL: http://www.kremlin.ru/catalog/keywords/63/events/64379 (дата обращения: 20.01.2023).

2. Лесной кодекс Российской Федерации от 04 декабря 2006 г. (ред. на 29 декабря 2022 года). № 200-ФЗ. // СПС «КонсультантПлюс».

3.Постановление Правительства Российской Федерации от 3 декабря 2014 года № 1301 «Об утверждении Правил представления информации в единую государственную автоматизированную информационную систему учета древесины и сделок с ней» // СПС «КонсультантПлюс».

4. Постановление Правительства Российской Федерации от 30 ноября 2021 года № 2128. «О порядке определения характеристик древесины и учета древесины» // СПС «КонсультантПлюс».

5. Постановление Правительства РФ от 24 ноября 2021 года № 2017 «Об утверждении требований к размещению и характеристикам складов древесины» // СПС «КонсультантПлюс».

6. Приказ Министерства природных ресурсов и экологии Российской Федерации от 17.01.2022 № 23 «Об утверждении видов лесосечных работ, порядка и последовательности их выполнения, формы технологической карты лесосечных работ, формы акта заключительного осмотра лесосеки и порядка заключительного осмотра лесосеки» // СПС «КонсультантПлюс».

7. Бородина, О.Б., Гальченко, С.А., Рассказова, А.А., Чуксин, И.В. Необходимость внедрения цифровых технологий в лесное хозяйство России как главного механизма устойчивого лесоуправления / О.Б. Бородина, С.А.

Гальченко, А.А. Рассказова, И.В. Чуксин // Московский экономический журнал. 2021. № 2.

8. В рамках проведенного исследования изучено 300 обвинительных приговоров по делам о преступлениях, предусмотренных ст.ст. 260, 191.1, 226.1 УК РФ, вынесенных судами Российской Федерации в 2021-2022 гг. // URL: https://sudrf.ru/index.php?id=300 (дата обращения: 26.01.2023).

9. Обвинительный приговор Кировского районного суда Республики Башкортостан 28 июля 2022 года № 1-34/2021, в отн. индивидуального предпринимателя, по ч. 1 ст. 226.1 УК РФ // URL: https://bsr.sudrf.ru. (дата обращения: 25.01.2023).

10. Обвинительный приговор Черновского районного суда Забайкальского края 7 февраля 2022 года № 1-25/2022, в отн. индивидуального предпринимателя, по ч. 1 ст. 226.1 УК РФ // URL: https://bsr.sudrf.ru. (дата обращения: 25.01.2023).

11. Обвинительный приговор Нелидовского межрайонного суда Тверской области 21 февраля 2022 года № 1-2/2022, в отн. Ш., по ч. 3 ст. 260 УК РФ, ч. 1 ст. 191.1 УК РФ // URL: https://bsr.sudrf.ru. (дата обращения: 25.01.2023).

12. Обвинительный приговор Верещагинского районного суда Пермского края 6 июля 2021 года № 1-2/2022, в отн. С., по ч. 3 ст. 260 УК РФ // URL: https://bsr.sudrf.ru. (дата обращения: 25.01.2023).

13. Федеральный закон от 03 августа 2018 года № 289-ФЗ (ред. от 19 декабря 2022) «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс».

УДК 004.056.5

ОСОБЕННОСТИ ОБЕЗЛИЧИВАНИЯ ДАННЫХ: МЕЖДУНАРОДНЫЙ И РОССИЙСКИЙ ПОДХОД

Ламонов Климент Андреевич,
Военный Инновационный Технополис «ЭРА»,
г. Анапа, Россия
e-mail: 1_0_91@bk.ru

Тимошенко Александр Геннадьевич,
кандидат технических наук, доцент кафедры телекоммуникационных систем
Национальный исследовательский университет «МИЭТ»,
г. Москва, Россия

Аннотация: *в статье рассмотрены особенности подхода к защите персональных данных при помощи обезличивания. Проводится анализ и сравниваются российский и международный подход, а также дается сравнение особенностей применения алгоритмов обезличивания данных, используемых в Российской Федерации и в странах ЕС.*

Ключевые слова: *обезличивание, персональные данные, сравнение методов обезличивания, зарубежные методы обезличивания персональных данных.*

PECULIARITIES OF DATA DISCHARGE: INTERNATIONAL AND RUSSIAN APPROACH

Lamonov Kliment Andreevich,
Military innovative technopolis "ERA" ,
Anapa, Russia
email: 1_0_91@bk.ru

Timoshenko Alexander *Gennadievich,*
candidate of technical sciences, associate professor of the Department of telecommunication systems
National research university of electronic technology (MIET),
Moscow, Russia

Annotation: *the article discusses the features of the approach to the protection of personal data using depersonalization. The analysis and comparison of the Russian and international approaches are carried out, as well as a comparison of the features of the application of data depersonalization algorithms used in the Russian Federation and in the EU countries.*

Keywords: *depersonalization, personal data, comparison of depersonalization methods, foreign methods of depersonalization of personal data.*

Множество стран применяют различные способы правового регулирования информации, находящейся в информационных системах персональных данных (ИСПДн). Из-за жестких требований некоторых государств к защите персональных данных (ПДн), одним из перспективных направлений в области информационной безопасности является обезличивание – метод защиты ПДн. Перспективность обуславливается экономией средств для его реализации и применения. Этот метод становится все более популярным, однако до сих пор не было проведено обзора и сравнения различных подходов к обезличиванию в России и зарубежных странах.

Целью и задачей обезличивания является снижение эффективности действий злоумышленника, по использованию общедоступных или полученных несанкционированным путем ПДн, во вред субъекту ПДн. Существует множество методов обезличивания ПДн. Так, согласно анализу законодательства РФ и научных работ, все методы можно разделить на 4 основных группы: введение идентификаторов, изменение состава или семантики, декомпозиция и перемешивание [1].

Далее проведен детальный обзор особенностей как Российского подхода к защите персональных данных методом обезличивания, так и зарубежных стран. Выполнено сравнение этих подходов, сделаны выводы.

Особенности обезличивания в РФ.

Правовое регулирование.

В РФ защита ПДн регулируется как Конституцией РФ (ст. 23, ст. 24), так и Трудовым Кодексом РФ (гл. 14). Но глубже всего вопрос регулирования был раскрыт Федеральным Законом № 152-ФЗ от 27 июля 2006 года «О персональных данных». В нем были конкретизированы такие понятия как персональные данные, оператор ПДн, обработка ПДн, а также обезличивание ПДн. В законе говорится, что обезличивание – это действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных [2].

Нормативная база для изучения обезличивания в РФ, следующая:

- Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
- «Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Роскомнадзором 13.12.2013)

Важно также отметить постановление правительства от 06.09.2014 №119, в котором отменяется обязанность государственных и муниципальных органов (операторов ПДн) осуществлять обезличивание ПДн в ИСПДн.

Методы обезличивания.

В Российской Федерации с начала 2009 г. было предложено несколько разных методов обезличивания, но только к 2013 г. Роскомнадзором [3] были

утверждены 4 основных – введение идентификаторов, изменение состава или семантики, декомпозиция и перемешивание.

Роскомнадзором также были установлены характеристики, которыми могут обладать эти методы. Далее приведена таблица (таблица 1) соответствия метода обезличивания к конкретной характеристике.

Таблица 1. Отношение методов обезличивания данных и их характеристик

	Введение идентификаторов	Изменение состава или семантики	Декомпозиция	Перемешивание
Обратимость	Метод позволяет провести процедуру деобезличивания	Метод не позволяет провести процедуру деобезличивания в полном объеме и применяется при статистической обработке данных	Метод позволяет провести процедуру деобезличивания	Метод позволяет провести процедуру деобезличивания
Вариативность	Метод позволяет перейти от одной таблицы соответствия к другой без проведения процедуры деобезличивания	Метод не позволяет изменять параметры метода без проведения предварительного деобезличивания	Метод позволяет провести процедуру обезличивания	Метод позволяет изменять параметры обезличивания без проведения процедуры деобезличивания
Изменяемость	Метод не позволяет вносить изменения в массив обезличенных данных без предварительного обезличивания	Метод позволяет вносить изменения в массив обезличенных данных без предварительного обезличивания	Метод позволяет вносить изменения в массив обезличенных данных без предварительного обезличивания	Метод позволяет вносить изменения в массив обезличенных данных без предварительного обезличивания
Возможность	Метод не исключает	Метод исключает возможность	Метод не исключает	Метод исключает

косвенного обезличивания	возможность деобезличивания с использованием ПДн, имеющихся у других операторов	деобезличивания с использованием ПДн, имеющихся у других операторов	возможность деобезличивания с использованием ПДн, имеющихся у других операторов	возможность деобезличивания с использованием ПДн, имеющихся у других операторов
Совместимость	Метод позволяет интегрировать записи, соответствующие отдельным атрибутам	Метод не обеспечивает интеграции с данными, обезличенными другими методами	Метод обеспечивает интеграцию с данными, обезличенными другими методами	Метод позволяет проводить интеграцию с данными, обезличенными другими методами
Параметрический объем	Объем таблицы (таблиц) соответствия числом записей о субъектах ПДн, подлежащих обезличиванию	Параметры метода определяются набором правил изменения состава или семантики ПДн	Определяется числом подмножеств и числом субъектов ПДн, массив которых обезличивается, а также правилами разделения ПДн на части и объемом связывания записей, находящихся в различных хранилищах	Зависит от заданных методов и правил перемешивания и требуемой стойкости к атакам на идентификацию
Возможность оценки качества данных	Метод позволяет провести анализ качества обезличенных данных	Метод не позволяет проводить анализ, использующий конкретные значения ПДн	Метод позволяет провести анализ качества обезличенных данных	Метод позволяет провести анализ качества обезличенных данных

Также были описаны свойства обезличенных ПДн, которыми могут обладать данные после их обезличивания одним из методов. В таблице 2 указано, обладают (+) данные определенным свойством, либо нет (-).

Таблица 2. Отношение свойства обезличенных ПДн
и методов обезличивания ПДн

Критерии	Введение идентификаторов	Изменение состава или семантики	Декомпозиция	Перемешивание
Полнота	+	-	+	+
Структурированность	+	+	+	+
Релевантность	-	+	+	+
Семантическая целостность	+	-	+	+
Применимость	+	+	+	+
Анонимность	-	+	-	+

Как можно видеть из таблицы 2, всеми свойствами обладает только один метод – перемешивание. Тогда возникает вопрос, для чего даны остальные. В методических рекомендациях от Роскомнадзора [4] указано, что наличие всех требуемых свойств для метода необязательно. Каждый метод может подходить под определённые, частные случаи, так:

- Метод введения идентификаторов – целесообразно применять при небольшом количестве атрибутов ПДн и небольшом объеме массива ПДн.
- Метод изменения состава и семантики – целесообразно применять в случае, когда задача обработки данных не требует деобезличивания.
- Метод декомпозиции – целесообразно применять при большом количестве атрибутов ПДн, но при редком внесении изменений в данные или аттрибуты.
- Метод перемешивания – имеет высокую эффективность при сложной обработке ПДн, частом изменении данных.

Особенности обезличивания в зарубежных странах.

Правовое регулирование.

Каждая страна имеет свои особенности правового регулирования защиты ПДн. Согласно исследованию [5] существует два типа систем правового регулирования: децентрализованная и централизованная.

- Децентрализованная система. Отсутствие единого подхода к защите ПДн. Акты рекомендательного характера играют значительную роль. Отсутствует единый надзорный орган. Примеры таких стран: США, Канада, Австралия.
- Централизованная система. Действие международных норм, гармонизирующих законодательства государств. Наличие законов, содержащих

общеобязательные нормы в отношении защиты ПДн. Регулирование обработки ПДн посредством учреждения единого надзорного ведомства. Примеры таких стран: Страны ЕС, Израиль, Мексика, Гонконг, Швейцария, Сингапур.

Также выделяются страны, в которых наличие одного или нескольких признаков, позволяют отнести ее систему правого регулирования защиты ПДн к централизованной или децентрализованной системе. Такая система называется смешанной. Примеры таких стран: Япония, Тайвань, Бразилия, Китай, Саудовская Аравия.

Для сравнения с РФ возьмем страны ЕС. Главные документы, определяющие правила защиты ПДн в Европейском Союзе – это Конвенция № 108 Совета Европы о защите частных лиц при автоматизированной обработке данных личного характера 1981 г., Директива 95/46/ ЕС «Общие положения о защите данных» и так далее. Сейчас актуальным считается Регламент от 25 мая 2018 г. 2016/679 Европейского парламента и Совета “О защите персональных данных и о свободном перемещении таких данных” (General Data Protection Regulation, GDPR).

Что касается информационной безопасности, в Европейском Союзе существует Агентство Европейского Союза по кибербезопасности (European Union Agency for Cybersecurity, ENISA). Оно тесно сотрудничает со странами-членами ЕС, чтобы предоставлять советы и решения по вопросам кибербезопасности, а также разрабатывает схемы сертификации кибербезопасности.

Методы обезличивания.

В ЕС разделяют понятия анонимизации и псевдонимизации, где последнее ближе всего соответствуют понятию обезличивания ПДн в РФ. У Агентства Европейского Союза по кибербезопасности (далее – ENSIA) существуют следующие два документа:

- Методы и лучшие практики псевдонимизаций (Pseudonymisation techniques and best practices) от 03.12.2019. В этом отчете исследуются основные понятия псевдонимизации, а также технические решения, которые могут поддержать реализацию на практике.
- Псевдонимизация данных: передовые методы и сценарии использования (Data Pseudonymisation: Advanced Techniques and Use Cases) от 28.01.2021. В этом отчете рассматриваются передовые решения для более сложных сценариев.

В [6] ENISA разрабатывает сценарии псевдонимизации, модель противника, а также методы псевдонимизации (с приведенными примерами). В отчете описаны основные методы псевдонимизации:

- Замена по счетчику (Counter). Идентификаторы заменяются числом, выбранным монотонным счетчиком. Очень важно, чтобы значения, выдаваемые счетчиком, никогда не повторялись, чтобы избежать неоднозначности.;
- Генерация случайного числа (Random Number Generator, RNG). Этот подход аналогичен замене по счетчику но идентификатору присваивается случайное число;

- Хеш-функция (Hash-function). Криптографическая хеш-функция принимает входные строки произвольной длины и отображает их в выходные данные фиксированной длины;
- Код аутентификации сообщения (Message Auth. Codes, MAC). Этот метод похож на хеш-функцию, за исключением того, что для генерации псевдонима вводится секретный ключ;
- Шифрование (Encrypting). Симметричное шифрование, например, Блочные шифры.

В отчете описаны особенности применения каждого из методов, представлено на таблице 3.

Таблица 3. Особенности методов псевдонимизации

Метод псевдонимизации	Особенности метода
Замена по счетчику.	Преимущества метода заключаются в его простоте, что делает его хорошим кандидатом для небольших и несложных наборов ПДн. Что касается защиты данных, счетчик обеспечивает псевдонимы без связи с начальными идентификаторами
Генерация случайного числа (RNG).	RNG обеспечивает надежную защиту данных поскольку, в отличие от замены по счетчику, для создания каждого псевдонима используется случайное число, поэтому трудно извлечь информацию о начальном идентификаторе, если таблица сопоставления не скомпрометирована.
Хеш-функция.	Хеш-функция может значительно способствовать целостности данных, однако она считается слабой в качестве метода псевдонимизации, поскольку подвержена атакам методом грубой силы и словарным атакам.
Код аутентификации сообщения (MAC)	MAC обычно рассматривается как надежный метод псевдонимизации с точки зрения защиты данных, поскольку восстановление псевдонима невозможно, пока ключ не был скомпрометирован.
Шифрование.	Шифрование также может быть надежным методом псевдонимизации с некоторыми свойствами, аналогичными MAC

Также, каждая методика имеет свой метод обратимости. Представлено на таблице 4.

Таблица 4. Соответствие метода псевдонимизации соответствующему методу обратимости

Метод псевдонимизации	Метод обратимости
Замена по счетчику.	Таблица сопоставления
Генерация случайного числа.	Таблица сопоставления
Хеш-функция.	Таблица сопоставления
Код аутентификации сообщения	Таблица сопоставления
Шифрование.	Дешифрование

Изучая [7] заметно, что в нем ENISA рассматривает более продвинутые методы псевдонимизации, приводит примеры их использования в здравоохранении и кибербезопасности. В отчете, описываются такие методы как:

- Асимметричное шифрование.
- Кольцевые подписи и групповые псевдонимы.
- Режим цепочки.
- Псевдонимы на основе нескольких идентификаторов или атрибутов.
- Псевдонимы с подтверждением права собственности.
- Безопасные многосторонние вычисления.
- Схемы обмена секретами.

Важно также отметить, что каждый из описанных выше методов имеет криптографические свойства.

Сравнение подходов.

В первую очередь заметно, что ENISA по сравнению с Роскомнадзором работает быстрее, а, следовательно, и активнее. В то время как Роскомнадзором в 2013 г. были предложены 4 метода обезличивания в странах ЕС ENISA в 2021 году дополнила собственный список методов псевдонимизации еще 7-ю более продвинутыми.

Роскомнадзор в приказе «Об утверждении требований и методов по обезличиванию персональных данных» рассматривает методы, которые не имеют криптографических свойств, в отличии методов, описываемых в отчете ENISA «Data Pseudonymisation: Advanced Techniques and Use Cases». Это обусловлено тем, что описанные методы не требуют сертификации, как криптографические. В РФ процесс сертификации довольно сложный и продолжительный.

Сравнивая особенности подходов к обезличиванию в РФ и странах ЕС ясно, что не существует одного универсального (лучшего) метода обезличивания для любых задач. Согласно методическим рекомендациям Роскомнадзора каждый из выдвинутых им методов необходимо подбирать под определенную задачу, тоже сказано и в отчетах ENISA.

Выводы.

Сравнение подходов к обезличиванию ПДн в разных странах является сложно выполнимой задачей. Во-первых, в каждой стране своя система

регулирования защиты ПДн (смешанная, централизованная и децентрализованная). Во-вторых, даже если системы приблизительно похожи, как например Российская Федерация и страны ЕС, подходы к обезличиванию ПДн могут отличаться. Однако, проведя анализ удалось сравнить некоторые особенности подходов к обезличиванию ПДн в РФ и странах ЕС.

Список литературы

1. Мищенко, Е.Ю., Соколов, А.Н. Алгоритмы реализации методов обезличивания персональных данных в распределенных информационных системах / Е.Ю. Мищенко, А.Н. Соколов // Доклады Томского государственного университета систем управления и радиоэлектроники. 2019.Т. 22. №. 1.URL: https://cyberleninka.ru/article/n/algoritmy-realizatsii-metodov-obezlichivaniya-personalnyh-dannyh-v-raspredelennyh-informatsionnyh-sistemah/viewer (дата доступа 25.03.2021).
2. Российская Федерация. Законы. О персональных данных: Федеральный закон № 152-ФЗ (принят Государственной Думой 8 июля 2006 года: одобрен Советом Федерации 14 июля 2006 года) // СПС «КонсультантПлюс».
3. Российская Федерация. Роскомнадзор. Об утверждении требований и методов по обезличиванию персональных данных : Роскомнадзор от 5 сентября 2013 г. № 996 (утв. Роскомнадзором 13 декабря 2013).Москва, 2013.URL: https://legalacts.ru/doc/prikaz-roskomnadzora-ot-05092013-n-996-ob/ (дата доступа 25.03.2021).
4. Российская Федерация. Роскомнадзор. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Роскомнадзором 13 декабря 2013).Москва, 2013.URL: https://rkn.gov.ru/docs/Xerox_Phaser_3200MFP_20131216122746.pdf (дата доступа 02.04.2021).
5. Параскевов, А.В. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом / А.В. Параскевов, А.В. Левченко, А.Ю. Кухоль // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2015. №. 110.URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-pravovogo-regulirovaniya-zaschity-personalnyh-dannyh-v-rossii-i-za-rubezhom/viewer (дата доступа 07.04.21).
6. Pseudonymisation techniques and best practices // Europian union agency for cybersecurity.2019. – URL: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices (дата доступа 25.03.2021).
7. Data Pseudonymisation: Advanced Techniques and Use Cases // EUROPIAN UNION AGENCY FOR CYBERSECURITY.2021.URL: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases (дата доступа 25.03.2021).

УДК 342.7

ВОЗДЕЙСТВИЕ ВЫСОКИХ ТЕХНОЛОГИЙ НА ГОСУДАРСТВО И ПРАВО: ИНСТРУМЕНТ ИЛИ ЦЕННОСТЬ (ТЕОРЕТИКО-ПРАВОВОЙ ПОДХОД)?

Левина Мария Ильинична,
кандидат юридических наук, доцент
Московский институт электронной техники (МИЭТ),
г. Москва, Россия
e-mail: mlevina@list.ru

Аннотация: *в статье ставится вопрос о последствиях применения инструментального подхода к сущности явлений государства и права в связи с воздействием на них высоких технологий.*

Ключевые слова: *цифровое государство и право, инструментальный подход, ценностный подход, сущность государства и права.*

THE IMPACT OF HIGH TECHNOLOGIES ON THE STATE AND LAW: INCTRUMENT OR VALUE (THEORETICLA LEGAL APPROACH)?

Levina Maria Ilyinichna,
candidate of legal sciences, associate professor
National research university of electronic technology (MIET),
Moscow, Russia
e-mail: mlevina@list.ru

Abstract: *the paper covers issues of consequences of applying an instrumental approach to the essence of the phenomena of the state and law in connection with the impact of high technologies on them.*

Keywords: *digital state and law, instrumental approach, value-based approach, the essence of state and law.*

Споры о сущности государства и права ведутся на протяжении веков со времен сотворения мира. Хочется внести свою лепту в дискуссию, которая вышла на новый виток в связи с развитием высоких технологией и их воздействием на государство и право. Ни государство, ни право сами по себе, по своей сущности, не являются (высоко)технологичными. Однако и государство, и право всегда впитывали в себя новейшие технологии своего времени и обогащали правоприменительную практику под их влиянием.

Цифровизация, высокие технологии (смарт-контракты, блокчейн, информационные технологии в судебной, нотариальной, правоохранительной, законодательной и любой другой деятельности) деятельности) – это инструмент, очень удобный, но инструмент. Этот инструмент оказывает воздействие на государство и право, но изучение того, каким образом может применяться этот инструмент, восторг от его возможностей и очарование им не

должны заслонять сущности этих важнейших явлений человеческого общежития. Государство и право трансформировались в течение многих столетий под воздействием «высоких» технологий своего времени, присваивая их и впитывая в себя.

Сами по себе технологии не меняют сущность предметов и явлений. В современных работах, посвященных цифровизации, воздействию высоких технологий на государство и право, происходит либо подмена понятий (чаще всего) либо вообще эти понятия никак не раскрываются. Между тем, понять, что происходит с государством и правом в цифровую эпоху и каковы векторы дальнейшего движения, можно только отталкиваясь от сущности этих явлений.

В данной статье ставится вопрос о том, как инструментальный подход к государству и праву влияет на внедрение и применение высоких технологий.

Определимся с понятиями. Сущность какого-либо явления или предмета - устойчивая категория, хотя и не означает неизменности самого явления. Государство и право трансформировались на протяжении многих веков, но их сущность - совокупность устойчивых внутренних, глубинных свойств и отношений, составляющих их основу и проявляющих их природу, - не меняется.

Существует множество теорий, объясняющих сущность государства. Позиция каждого автора зависит от типа понимания государства и права. Большинство представлений о государстве и праве относятся к позитивистскому или непозитивистскому пониманию государства и права. В свою очередь, каждый из этих типов включает в себя множество разнообразных теорий и представлений о сущности государства и права. В данной статье, раскрывается собственно юридическое понятие государства. Под государством понимается публично-властная (властно-политическая) организация народа (общества), т.е. организация, обладающая суверенитетом, аппаратом управления и принуждения и устанавливающая правовой порядок на определенной территории [1].

Понятие права раскрывается с позиций теории различения права и закона, автором которой является академик В.С.Нерсесянц. Право понимается как социо-нормативный регулятор общественных отношений; нормативная форма выражения свободы посредством принципа формального равенства людей в общественных отношениях. Это означает, что качественной основой права является сочетание формального равенства, меры свободы и эквивалента в отношениях свободных индивидов. Из этого следует, что право и закон – понятия не тождественные [2].

Во многих современных работах авторы, по сути, отождествляют право и закон. Так, Т.Я.Хабриева и Н.Н.Черногор считают, что «право становится не только средством, инструментом, обеспечивающим цифровизацию экономики, управления и других сегментов социального бытия, но и объектом воздействия “цифровизации”, в результате которого оно претерпевает изменения своей формы, содержания, системы, структуры, механизма действия и демонстрирует тенденцию к усилению наметившихся трансформаций» [3]. В многочисленных статьях эта мысль повторяется на все лады и усиленно тиражируется [4].

Государство же в цифровую эпоху, понимаемое как цифровое (электронное) государство, довольно единодушно понимается исключительно как цифровое (электронное) правительство. При этом многие авторы отмечают, что понятие цифрового правительства уже понятия цифрового государства [5].

Государство, отождествляемое с цифровым правительством, таким образом, понимается как администратор, услугодатель, попечитель (автоматическая раздача пособий, пенсий, социальных выплат), регистратор, сборщик налогов, охранитель, контролер. Государство коммуницирует с гражданами напрямую, без посредников, в киберпространстве (или в МФЦ, но также посредством цифровых технологий). Значительно сокращается время для получения всевозможных выписок, справок, документов, актов, упрощаются и облегчаются сделки с недвижимостью, регистрации права собственности, оформление личных документов, медицинские и образовательные услуги. Казалось бы, затрагивается сбылась вековая мечта человечества – государство-слуга, обслуживающее своих граждан.

Что здесь не так? Во-первых, здесь затрагивается лишь одно из свойств государство – управление. Более того, осуществляется лишь одна из многих функций государства – социальная. Именно осуществлением этой функции достигается социальное назначение государства. Во-вторых, опять (как и в случае с правом) имеем дело с инструментальным подходом.

Если государство – это инструмент, слуга, администратор и т.д., это означает что государство отделено от общества, а граждане не составляют самой основы, сущности государства. Таким образом, государство не является публично-властной организацией народа. Вообще не представляет собой организацию народа, а лишь аппарат управления и принуждения.

Такой инструментальный подход не только низводит право с его пьедестала верховенства, но и существенно снижает его ценность как регулятора общественных отношений, устанавливающего единый объем свободы для всех индивидов до простого инструмента, используемого наряду с другими. Такой подход также обедняет и искажает сущность государства, что мешает определить вектор развития «действительно» цифрового государства и права, их признаки, содержание, характеристики и формы.

Государство и право регулируют различные виды отношений. Государство – вертикальные, политические, отношения власти-подчинения. Право – горизонтальные отношения независимых, автономных, свободных индивидов. Регулирование и тех, и других отношений – вопрос установления границ личной свободы каждого отдельного индивида и общества в целом. Все сводится к установлению границ осуществления прав, очерчивающих свободу каждого индивида.

Сетования многих авторов на то, что право (на самом деле, законодательство, законодательное регулирование) отстает от развития и применения высоких технологий, означает, что жизнь в киберпространстве осуществляется по нормам офлайна, а не по тем нормам, которые должны и могут работать в киберпространстве. Это связано с тем, что киберпространство «искажает» привычные пропорции и границы, они иные, чем в офлайне.

Цифровизация и высокие технологии – средства достижения правовых целей и результатов. Более того, нельзя применять их бесконтрольно и произвольно. Их применение должно осуществляться в соответствии с правовыми нормами и строго на правовых основаниях. Необходимо отметить, что внедрение и применение многих высоких технологий сегодня осуществляется без широкого общественного обсуждения и каких-либо правовых оснований.

Регламентация, регулирование внедрения, применения высоких технологий должно осуществляться только посредством правовых норм. Никакие соображения практической и иной целесообразности не могут стоять выше правовых норм. Так называемое отставание законодательства от уверенной поступи высоких технологий означает, что еще не определен правовой механизм, посредством которых высокие технологии внедряются, используются, а главное – устанавливаются пределы их применения. Не государство диктует, а правовые нормы определяют объем и степень вмешательство государства в деятельность, осуществляемую в киберпространстве. Сам же правовой механизм должен быть необходимым и достаточным – без серьезных лакун, но и без излишнего, мелочного регулирования.

Главная же задача государства – не цифрового, обычного государства – навести в нем порядок и установить пределы деятельности всех «жителей» киберпространства.

До недавнего времени на просторах киберпространства царила вольница, «феодальная раздробленность». Государство в нем занимало крайне скромное место и значительно уступало корпорациям и соцсетям. Каждая корпорация и соцсеть имеет свое вполне лояльное населения (и делая все, чтобы оно было лояльным) в определенных границах своей экосистемы.

Банки, крупные платформы-агрегаторы, интернет-маркетплейсы (такие, как Озон, Вайлдбериз и др.) трансформировались в экосистемы – «государство в государстве». Наперегонки с государством они бросились собирать всевозможные данные о своих клиентах и пользователях – бесконтрольно, бессистемно, без каких-либо правовых оснований, без стандартов и критериев, буквально вымогая формально согласие, которое невозможно не дать. Регулярные скандалы по поводу утечек только подчеркивают «пиратский» способ сбора данных – собирают побольше, авось пригодится. Сегодня в киберпространстве идет борьба за «души» людей, точнее, за их персональные (включая биометрические) данные между государством и корпорациями, коммерческим сектором. Объем и методы вмешательства государства в сферу применения высоких технологий, деятельность бигтехов и соцсетей должны устанавливаться правом и законодательством.

Научная литература, публицистика, не говоря уже о художественной сфере, полны радужных или апокалиптических предсказаний о будущем в цифровом мире. На самом деле выбор того или иного вектора развития – выбор возможностей, варьирующихся по шкале от «большого брата» до «цифрового рая», зависит именно от того, какой подход мы изберем: инструментальный или ценностный.

Инструментальный подход лишает ценностного значения государства и права, а также государства и права как ценности человеческого общежития. Понимание (и отношение) к государству и праву как к инструменту развития экономики, повышения благосостояния и проч., если не отрицает, то существенно снижает их значение и сущность. Инструментальный подход к пониманию современного, т.е. цифрового государства и права обедняет содержание как явлений, так и понятий, описывающих эти явления. Напротив, цифровизация, и высокие технологии должны быть инструментами формирования правового государства, достижение состояния правовой свободы как отдельного индивида, так и общества в целом, обеспечения принципа формального равенства и истинного правосудия. Если же высокие технологии не служат инструментом для реализации глубинных, сущностных свойств государства и права, то не имеет ровно никакого значения, насколько они эффективны и хороши сами по себе.

Список литературы

1. Мамут, Л.С. Социальное государство с точки зрения права / Л.С. Мамут // Государство и право. 2001. № 7. С.5-14.

2. Нерсесянц, В.С. Общая теория государства и права: учебник для вузов / В.С. Нерсесянц. М.: Норма – Инфра- М., 1999. С.70-71.

3. Хабриева, Т.Я. Право в условиях цифровой реальности/ Т.Я. Хабриева, Н.Н. Черногор // Журнал российского права. 2018.№ 1. С. 85–102.

4. Хабриева, Т.Я. Право перед вызовами цифровой реальности / Т.Я.Хабриева // Журнал российского права. 2018. № 9 (261). URL: https://cyberleninka.ru/article/n/pravo-pered-vyzovami-tsifrovoy-realnosti (дата обращения: 08.02.2023).

5. Головенчик, Г. Построение современного цифрового государства / Г. Головенчик // Наука и инновации.2019. №11 (201). URL: https://cyberleninka.ru/article/n/postroenie-sovremennogo-tsifrovogo-gosudarstva (дата обращения: 11.02.2023).

6. Михеева, Т.Н. К вопросу о правовых основах цифровизации в Российской Федерации / Т.Н.Михеева // Вестник Университета имени О. Е. Кутафина. 2019. № 9 (61). URL: https://cyberleninka.ru/article/n/k-voprosu-o-pravovyh-osnovah-tsifrovizatsii-v-rossiyskoy-federatsii (дата обращения: 08.02.2023).

7. Солдаткина, О.Л. Цифровое право: методология исследования / О.Л.Солдаткина // Правовая политика и правовая жизнь. 2019. № 3. URL: https://cyberleninka.ru/article/n/tsifrovoe-pravo-metodologiya-issledovaniya (дата обращения: 11.02.2023).

8. Багалей, Е. И. Право в условиях цифровой реальности / Е. И. Багалей. Текст: непосредственный /Е.И.Багалей// Молодой ученый. 2023. № 2 (449). С. 242-245. URL: https://moluch.ru/archive/449/98770/ (дата обращения: 11.02.2023).

9. Усачева, Е. Б. Право в условиях цифровой реальности / Е. Б. Усачева, А. С. Кирса. Текст: непосредственный // Молодой ученый. 2020. № 51 (341). С. 298-300. URL: https://moluch.ru/archive/341/76874/ (дата обращения: 11.02.2023).

УДК 167.6

ПРАВО ПОД ВОЗДЕЙСТВИЕМ ЦИФРОВИЗАЦИИ И ВИРТУАЛИЗАЦИИ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ – ЧТО МЕНЯЕТСЯ?

Ломакина Наталья Борисовна,
аспирант,
Научный руководитель: Даниелян Наира Владимировна
профессор
Национальный исследовательский университет
«Московский институт электронной техники»,
г. Москва, Россия
e-mail: krisyankin@yandex.ru

Аннотация: *в статье рассмотрены факторы, ведущие к изменению института права под воздействием цифровизации и виртуализации. Описаны трансформации в области государственного управления в сетевом обществе – расширение субъектного состава публичной политики, децентрализация власти, рост уровня участия граждан в политике. Приведены новые типы отношений, связанных с развитием информационно-коммуникативных технологий, которые должны найти отражение в правовом поле, например, связанные с юридически значимой идентификацией личности или реализацией прав человека в виртуальном пространстве, применением криптовалюты или происходящие между виртуальными или цифровыми «личностями». Сделан вывод о необходимости использования философского опыта в разработке новых управленческих моделей и правовых нормативов, так как в философии накоплен большой пласт наработок в области разработки управленческих моделей, применимых в сетевом обществе, методологии, искусственного интеллекта и других.*

Ключевые слова: *цифровизация, виртуализация, право, философия, технологии.*

LAW UNDER THE INFLUENCE OF DIGITALIZATION AND VIRTUALIZATION IN PUBLIC ADMINISTRATION – WHAT IS CHANGING?

Lomakina Natalia Borisovna,
postgraduate student of the institute of hl shs,
Scientific supervisor: Danielyan Naira Vladimirovna
professor
National research university of electronic technology (MIET),
Moscow, Russia
e-mail: krisyankin@yandex.ru

Abstract: *the article considers the factors leading to a change in the institution of law under the influence of digitalization and virtualization. Transformations in the field of public administration in a networked society are described – the expansion of*

the subject composition of public policy, the decentralization of power, the increase in the level of citizen participation in politics. New types of relations related to the development of information and communication technologies are presented, which should be reflected in the legal field, for example, related to legally significant identification of a person or the realization of human rights in the virtual space, the use of cryptocurrencies or occurring between virtual or digital "personalities". The conclusion is made about the need to use philosophical experience in the development of new management models and legal standards, since philosophy has accumulated a large layer of developments in the development of management models applicable in a network society, methodology, artificial intelligence and others.

Keywords: *digitalization, virtualization, law, philosophy, technology.*

В XXI веке мир крайне нестабилен. Под воздействием стремительно развивающихся технологий происходит быстрая смена типов общества. Как сетевом обществе, так и в обществе знаний многие институты трансформируются, изменяются под воздействием среды, подстраиваясь под новые нужды и потребности человека, и право – не исключение. Попробуем выяснить, какие факторы окажут влияние на его трансформацию.

В любом типе общества начинается поиск адекватных управленческих моделей, и поэтому в сетевом обществе (и в обществе знаний впоследствии) происходит принципиальная сетевая модернизация государственного управления, связанная с децентрализацией власти. Сетевое государство представляет собой «новую геометрию власти», в которой доминирует горизонтальный, а не вертикальный тип связей [1, с. 501].

Коммуникация виртуализируется, и государственное управление, подчиняясь этому, меняется, так как происходит усиление влияния гражданских структур на процесс принятия решений, модификация государственного управления в совместное с составляющими общество индивидами, возрастает уровень участия граждан в производстве и исполнении политических решений. Публичное управление становится многослойным и многосторонним, субъектный состав публичной политики расширяется, у государства и структур гражданского общества возникает принципиальная необходимость сотрудничества в части принятия политических решений. И это, безусловно, должно найти отражение в правовом поле.

И хотя, по мнению С.В. Липеня, юриспруденция рассматривает роль сетей с неким скепсисом и считает иерархические вертикальные властные отношения необходимыми условиями любой государственности, тем не менее, осознавая, что социо-гуманитарное знание активно пользуется сетевой терминологией, осознает, что и юридическая наука не может ее игнорировать [2]. Только в том случае, если сетевая логика будет «вписана» в существующие «властеотношения», она приведет к модификации определенных государственных институтов и процессов.

С.В. Липень отмечает, что во многих странах, в том числе и в России, наблюдается готовность общества и государства в целом к переходу к сетевой

модели, однако одновременно с этим еще сильны сформированные в докомпьютерную эпоху тенденции к сохранению иерархии и вертикалей власти, в связи с чем современное государственное управление представляет собой некий переходный тип.

Следует отметить, что юристы способны использовать преимущества сетевой методологии, которую можно органично включить в методологический инструментарий юридической науки. Однако направление, механизм и закономерности трансформации социальных институтов, в том числе и права, под влиянием цифровизации, пока не вполне понятны. Зарубежные научные деятели склонны рассматривать цифровизацию в правовом контексте как естественный феномен. Поэтому в своих работах они обращаются к темам, связанным с практическими аспектами цифровизации законодательства и правоприменительной практики – например, удобству пользования электронными нормативными источниками, возможности хранения большого объема информации, развитию рынка правовых услуг и т.п. Российские же ученые уделяют большое внимание созданию искусственного интеллекта, поиску оптимальных решений и разработке моделей правового регулирования общественных отношений, сопряженных с применением цифровых технологий в области финансов, публичного управления. Наблюдается постоянный рост объема законодательства, которое регулирует связанные с использованием цифровых технологий отношения.

Т.Я. Хабриева выделяет четыре характерные черты российского законодательства [3]:

1) применение традиционных инструментов – нормативных правовых актов, преимущественно законов, в то время как практика выявляет необходимость увеличения количества применяемых регуляторов;

2) возрастание важности актов стратегического планирования;

3) отсутствие официальной и научной концепций развития законодательства в сфере сетевых и цифровых технологий;

4) игнорирование накопившейся международно-правовой практики в этой области.

Поиск оптимальной модели нормативного правового регулирования общественных отношений, возникших в связи с цифровизацией, уже начат, и сейчас предполагается сосредоточиться на разработке актов стратегического планирования и использовании гибких регуляторов – подзаконных актов, правовых экспериментов.

Цифровизация наряду с глобализаций и межгосударственной интеграцией воздействует на динамику права, оказывая влияние в первую очередь на область правового регулирования, в которую «втягиваются» новые виды общественных отношений, прежде не существовавшие или не требующие регуляции. Это отношения между виртуальными или цифровыми «личностями», или связанные с юридически значимой идентификацией личности в виртуальном пространстве, или возникающие в связи с реализацией прав человека в виртуальном пространстве, или создаваемые посредством применения криптовалюты, и многие другие. Таким образом, сфере правового регулирования начинает быть присуща «мультисодержательность», ее структура и связи масштабно изменяются.

Под влиянием технологического фактора право «натыкается» на факт необходимости перемен, поскольку его основные теоретические признаки теряют прежний смысл в цифровую эпоху. По мнению Э.В. Талапиной, благодаря ходу мирового развития право сейчас ясно видит насущную потребность в том, чтобы не просто признать информационно-коммуникационные технологии и сопряженные с ними правоотношения, но адаптировать к ним всю систему и структуру права [4]. И если в частном праве Интернет преображает традиционные институты зачастую формально, то в публичном праве нейтральность и экстерриториальность Интернета могут нанести серьезный урон государственному суверенитету, а социальные сети – патерналистски-вертикальной организации государства.

Проанализировав работы специалистов в области права и их мнение относительно влияния на институт права цифровизации и виртуализации, можно сделать вывод, что проблема стоит достаточно остро, а инструменты для ее решения находятся лишь в стадии разработки. Философия может помочь в этом процессе, предложив наработки в области разработки управленческих моделей, применимых в сетевом обществе, методологии, искусственного интеллекта. Здесь могут быть полезны работы М. Кастельса, Э. Тоффлера и других философов.

Также следует отметить, что не последнее значение в высокотехнологичном праве будет иметь политическая философия, так как с появлением категории «киберпространство» возникла угроза классической теории государственного суверенитета. К тому же, как уже отмечалось ранее, государственное управление претерпевает изменения под воздействием сетевой парадигмы, и необходимо вырабатывать новые категории и новые теории в этом направлении. Также необходима выработка новых норм в отношении новых объектов права (криптовалюты, вещей, созданных посредством цифровых технологий), обеспечения прав человека в цифровом мире, защиты прав на информацию. Рассмотрение всех подобных категорий в философском ключе дает более полное и верное представление о них для создания максимально четких нормативов.

Список литературы

1. Кастельс, М. Информационная эпоха: экономика, общество и культура / М. Кастельс / пер. с англ. под науч. ред. О.И. Шкаратана. М.: ГУ ВШЭ, 2000. 608 с.

2. Липень, С.В. Сетевое общество, «новая геометрия власти» и модернизация государства в современных юридических исследованиях / С.В. Липень // Государственное управление. Электронный вестник. 2020. № 82. С. 290-305.

3. Хабриева, Т.Я. Право перед вызовами цифровой реальности / Т.Я. Хабриева // Журнал российского права. 2019. № 9. С.5-16.

4. Талапина, Э.В. Право и цифровизация: новые вызовы и перспективы / Э.В. Талапина // Журнал российского права. 2018. № 2. С.5-17.

УДК 34.096

О ЦЕЛЕСООБРАЗНОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ИХ РЕЗУЛЬТАТОВ

Межуева Юлия Сергеевна,
студент
Московский государственный технический университет им. Н.Э. Баумана,
г.Москва, Россия
email: mezhuevayus@student.bmstu.ru
Яковлев Алексей Николаевич,
кандидат юридических наук, доцент,
Московский государственный технический университет им. Н.Э. Баумана,
Национальный исследовательский университет
«Московский институт электронной техники»
г.Москва, Россия
email: mgtu-temp@yandex.ru

Аннотация: *в статье рассмотрены отдельные аспекты правового регулирования технологий искусственного интеллекта и их результатов, история формирования этих технологий, некоторые относимые нормы технического регулирования и отдельные вопросы правоприменительной практики. Проанализированы правовые и технические аспекты развития технологий искусственного интеллекта, высказано мнение о необходимости соответствия правового регулирования содержательной части таких технологий.*

Ключевые слова: *технологии искусственного интеллекта, искусственный интеллект, правовая охрана, уголовный процесс, этика искусственного интеллекта, современные технологии в юриспруденции, высокотехнологичное право.*

ABOUT EXPEDIENCY OF LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES AND THEIR RESULTS

Mezhuyeva Julia Sergeevna,
student
Bauman Moscow state technical university (BMSTU)
email: mezhuevayus@student.bmstu.ru
Yakovlev Alexey Nikolaevich,
candidate of law, associate professor
Bauman Moscow State Technical University (BMSTU)
Moscow Institute of Electronic Technology (MIET)
Moscow, Russia
email: mgtu-temp@yandex.ru

Abstract: *the article discusses some aspects of the legal regulation of artificial intelligence technologies and their results, the history of the formation of these*

technologies, some relevant technical regulations and individual issues of law enforcement practice. The legal and technical aspects of the development of artificial intelligence technologies are analyzed, the opinion is expressed on the need for compliance of legal regulation with the content of such technologies.

Keywords: *artificial intelligence technologies, artificial intelligence, legal protection, criminal procedure, ethics of artificial intelligence, modern technologies in jurisprudence, high-tech law.*

Искусственный интеллект как математическая теория и ее реализация в виде практических технологий берет свое начало в прошлом столетии. Родоначальником этой теории стал Алан Тьюринг. В статье «Computing Machinery and Intelligence» он описал придуманный им тест с названием «Игра в имитацию», содержащий вопросы, которые задает участникам игры главное действующее лицо - интервьюер. Он знает про двух участников опроса: один из которых человек, другой машина, но не видит их, поскольку все участники, включая самого интервьюера, находятся в изолированном от других пространстве. По окончании теста опрашивающий должен угадать, кто из респондентов был машиной [1].

Такой тест был придуман за десятилетие до изобретения компьютера, поэтому Алан Тьюринг не успел реализовать его на практике. Однако сегодня такое тестирование не только проводится, но даже популярно, а за успешное прохождение теста организаторы предлагают участникам денежные вознаграждения. Такая практика направлена на поощрение разработчиков, которые занимаются усовершенствованием технологий искусственного интеллекта.

Помимо Тьюринга, существенный первоначальный вклад в развитие технологий искусственного интеллекта внесли Уоррен Маккалок и Уолтер Питтс, которые в статье «A logical calculus of the ideas in nervous activity» сравнили мозг и машину, указав на то, что по сути процессы в нейронах головного мозга реализуют простейшую логику и математику, а в мышлении можно выделить логические операторы И, ИЛИ и НЕ [2]. Схожие научные идеи содержатся и в работе Норберта Винера «Cybernetics: or control and communication in the animal and the machine» [3].

Чтобы быть точным в описании технологий искусственного интеллекта, рассмотрим отдельные базовые понятия этой области знаний.

В научной и научно-популярной литературе искусственный интеллект чаще всего описывают как компьютеризированное устройство, обладающее некоторыми когнитивными функциями человеческого мозга и в процессе «размышления» получающее результаты, сопоставимые с результатами интеллектуальной деятельности человека [4].

Считаем, что такое определение мало соответствует как теоретическим основам технологий искусственного интеллекта, так и действительности. Технологии искусственного интеллекта для внешнего наблюдателя лишь имитируют когнитивность, не обладая ей. Такие технологии алгоритмически

предопределены, и особенностью их является лишь алгоритмический учет недостаточности исходных данных или их определенная вариативность.

В отличие от человека, который может принимать решения в условиях не только частичной, но и полной неопределенности исходных данных, устройство, реализующее технологии искусственного интеллекта, действует «правильно» лишь в условиях допустимой разработчиком неопределенности исходных данных, и не может «правильно» работать в условиях полной неопределенности данных. Именно поэтому компьютер, реализующий технологии искусственного интеллекта, дает «правильные» ответы лишь в случае предварительного обучения системы искусственного интеллекта на специальной выборке вопросов и соответствующих им ответов, либо если определены правила формирования ответа на «неизвестный» системе вопрос. При этом лишь человеку доступны такие когнитивные возможности как аналогия, дедукция, индукция, которые дают нам возможность быть по-настоящему интеллектуальными.

Более точное, на наш взгляд, определение искусственного интеллекта дал А.С. Потапов: искусственный интеллект – это большое направление научных и прикладных исследований, целями которой являются автоматизация деятельности человека (преимущественно, интеллектуальной) и реализация компьютерных моделей, которые способны имитировать процессы решения интеллектуальных задач человеком (а также поиск алгоритма таких процессов в человеческом мозге) [5]. Ключевым в этом определении является положение об имитации процессов решения интеллектуальных задач человеком, что полностью соответствует действительности и не вводит в заблуждение тех, кто видит только внешние эффекты технологий искусственного интеллекта.

Дефиниция термина «искусственный интеллект» в настоящее время дана и в высокоуровневых правовых актах. Так, в Указе Президента Российской Федерации от 10 октября 2019 года «О развитии искусственного интеллекта в Российской Федерации» искусственный интеллект определяется как совокупность решений технологического характера, под которыми подразумевается информационно-коммуникационная инфраструктура, методы машинного обучения, программное обеспечение, процессы и сервисы обработки данных и поиска решений, подражающих когнитивным функциям человека, а также получающих результаты, которые могут быть приблизительно равны продуктам мыслительной и интеллектуальной деятельности человека [6]. Обращаем внимание на то, что в определении констатируется факт синонимичности понятий «искусственного интеллекта» и «технологий искусственного интеллекта», которые определены через решения технологического характера.

Таким образом, искусственный интеллект – это технологии, использующие специальные математические методы работы с данными (например, основанные на теории семантических сетей, использовании методов машинного обучения), и реализованные в специализированном программном обеспечении.

В определении искусственного интеллекта, кроме математической составляющей, есть технологическая составляющая. Она определена в различных ГОСТ одинаково, несмотря на различные области применения стандартов.

Так в ГОСТ Р 59276-2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения» искусственный интеллект определен как способность технической системы имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных практически значимых задач обработки данных результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека [7].

В ГОСТ Р 59921.1-2022 «Системы искусственного интеллекта в клинической медицине. Часть 1. Клиническая оценка» это определение воспроизведено с уточнением, что искусственный интеллект – это комплекс технологических решений, который использует информационно-телекоммуникационную инфраструктуру и включает в себя программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных, анализу и синтезу решений [8].

Аналогичное определение искусственному интеллекту дает ГОСТ Р 59895-2021 «Технологии искусственного интеллекта в образовании. Общие положения и терминология» [9] и иные национальные стандарты.

Если представители технических профессий рассматривают развитие технологий искусственного интеллекта исключительно с технологической точки зрения, то особую позицию занимают представители юридических наук, которые периодически дискутируют по различным проблемам, связанным с применением технологий искусственного интеллекта. Как результат, такие дискуссии и обсуждение проблем вынесены на уровень Президента и Правительства, результатом чего стало появление документов проектного характера соответствующего уровня.

Так, в упомянутом выше Указе Президента Российской Федерации от 10 октября 2019 года [6] и распоряжении Правительства Российской Федерации от 19 августа 2020 года № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» [10] ставится достаточно дискуссионная задача правового регулирования технологий искусственного интеллекта. Дискуссионность ее в том, что собственно технические аспекты технологий искусственного интеллекта ничем не отличаются от технических аспектов иных технологий и нормативно урегулированы федеральными законами, постановлениями Правительства Российской Федерации, ведомственными организационно-распорядительными документами и документами технического регулирования. Вследствие этого неочевидно, какие аспекты технологий искусственного интеллекта нуждаются в дополнительном нормативном закреплении и правовом урегулировании.

Относительно результатов применения технологий искусственного интеллекта в рассмотренных выше ГОСТ так же дана очевидная подсказка «сопоставимые, как минимум, с результатами интеллектуальной деятельности человека». Вследствие этого результаты применения технологий искусственного интеллекта в общем порядке уже урегулированы как результаты интеллектуальной деятельности человека. Какие при этом частности требуют дополнительного правового регулирования, содержание дискуссии умалчивает.

Вместе с тем, обращают на себя внимание отдельные аспекты упомянутого распоряжения Правительства Российской Федерации от 19 августа 2020 года № 2129-р. В нем говорится о том, что формирование правовой базы стимулирует развитие технологий искусственного интеллекта, их использование и внедрение в жизнь общества; что исполнение распоряжения будет способствовать экономическому развитию общества, повышению качества жизни граждан, а также повышению позиций российской экономики в области искусственного интеллекта [8].

Отметим несколько особенностей этого правового акта.

Согласно части 2 статьи 5 Федерального конституционного закона от 06.11.2020 № 4-ФКЗ «О Правительстве Российской Федерации» распоряжения Правительства Российской Федерации не имеют нормативного характера и являются актами Правительства Российской Федерации по оперативным и другим текущим вопросам. Согласно части 5 статьи 12 указанного закона такие акты носят координирующий характер для федеральных министерств и иных федеральных органов исполнительной власти, указанных в части 2 указанной статьи [11]. Таким образом, распоряжение Правительства Российской Федерации от 19 августа 2020 года № 2129-р лишь подлежит учету при планировании работы федеральными министерствами и иными федеральными органами исполнительной власти.

Кроме того, дискуссионны положения распоряжения о влиянии формирования правовой базы на развитие технологий искусственного интеллекта, их использование и внедрение в жизнь общества, на экономическое развитие общества, повышение качества жизни граждан.

Все современные технологии сначала внедрялись их разработчиками в жизнь общества, и лишь после, при выявлении негативных аспектов технологий, разрабатывались правовые компенсационные меры. Не являются исключением и технологии искусственного интеллекта. Обратим внимание на то, что даже Правительством Российской Федерации в отношении технологий искусственного интеллекта выбрана не регулятивная, а координирующая, «рекомендательная» форма правового акта. На текущем этапе развития и внедрения технологий искусственного интеллекта было бы преждевременным использовать иные, регулятивные подходы.

Также отметим тезис распоряжения Правительства Российской Федерации от 19 августа 2020 года № 2129-р о том, что технологии искусственного интеллекта могут нанести угрозу правовой системе государства, государственного управления и гражданам. Подобное

предположение также не соотносится с имеющимся уровнем развития и внедрения технологий искусственного интеллекта и, скорее, отражает реакцию разработчиков документа на новые, малоизвестные им технологии, и особенности отдельных профессиональных публикаций на эту тему.

Любопытно, что подобное настороженное отношение к новым технологиям и ожидание от них неприятностей не ново. Еще в 1865 году в Англии в ответ на появление самодвижущихся повозок был принят закон, согласно которому в городской черте устройства могли двигаться не быстрее 3 км/ч, за городом - 6 км/ч. Экипаж машины должен был состоять из трёх человек, из которых один был обязан идти в 50 метрах впереди неё с красным флагом. Лишь спустя 31 год эти ограничения были существенно смягчены [12].

Подобно смягчению первой реакции законодателя Англии на самодвижущиеся повозки, следует смягчить и негативные ожидания от технологий искусственного интеллекта. В настоящее время область их применения – образование, медицина, транспорт – и степень развития технологий не позволяют считать общество в опасности. Пока технологии искусственного интеллекта направлены на оптимизацию и улучшение качества жизни, достаточно мониторить возникающие проблемы и решать их адекватными ситуации инструментами.

Исходя из распоряжения Правительства Российской Федерации от 19 августа 2020 года № 2129-р, также можно сделать вывод о том, что разработчики документа предполагают возможность автономности действий искусственного интеллекта, что не вполне отвечает сути рассматриваемых технологий.

В соответствии с ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения», автоматизированный процесс - процесс, осуществляемый при совместном участии человека и средств автоматизации; автоматический процесс - процесс, выполняемый техническими средствами по ранее заданному алгоритму без участия человека [13].

В случае технологий искусственного интеллекта на этапе обучения системы процесс автоматизированный, осуществляется с участием человека; на этапе функционирования обученной системы процесс автоматический, выполняемый по ранее заданному алгоритму уже без участия человека.

Только в случае неумышленного или умышленного обучения системы, построенной на технологиях искусственного интеллекта, потенциально опасным действиям, решениям, использование такой системы может наносить ущерб. Однако, и при этом собственно система искусственного интеллекта угрозы человеку или обществу не несет, так как ее обучает и программирует человек. Человек несет ответственность за последствия создания, обучения, использования системы точно так же, как он несет ответственность за эксплуатацию транспортного средства, являющегося источником повышенной опасности. И важно, что в рассматриваемой аналогии правила дорожного движения регулируют действия человека, но не автомобиля.

Применительно к системам искусственного интеллекта, какие-либо правила должны или могут регулировать деятельность человека, связанную с эксплуатацией таких систем или технологий. Возникнет ли потребность в более общем регулировании использования систем или технологий искусственного интеллекта, правовым актом какой силы следует урегулировать те или иные аспекты их использования, в настоящее время предполагать преждевременно.

Отдельным аспектом научных дискуссий о технологиях искусственного интеллекта является обсуждение вопросов «этики искусственного интеллекта». Как нам представляется, и в этом аспекте проявляется настороженность участников дискуссии.

Предлагаем сформулировать вопрос так, чтобы он соответствовал определению и сути технологий искусственного интеллекта: «Возможно ли соотносить вопросы этики и морали с некоторым алгоритмом или его программной реализацией?» В этом случае ответ будет очевиден. Сам по себе никакой алгоритм не является носителем идей добра или зла. Вопросы этики и морали могут возникать лишь при выборе области применения алгоритма, программной реализации, технологий искусственного интеллекта. Неконтролируемое человеком использование таких технологий при принятии решений на поле боя, в ходе хирургической операции, при управлении транспортным средством вызывает вопросы и опасения. Вместе с тем, в настоящее время крайне мало областей применения технологий искусственного интеллекта, в которых ему «доверяют» окончательное и неконтролируемое принятие решений. В максимальном числе ситуаций применение таких технологий иное - корректируемое, контролируемое, прогнозируемое либо носит справочный обеспечивающий характер.

Все сказанное выше в полной мере относится и к аспектам внедрения технологий искусственного интеллекта в судопроизводство. Миф неизвестного источника происхождения о том, что при определенном развитии технологий машина будет выносить решение по вопросам вины человека и влиять на ограничение его свободы, не выдерживает никакой критики. Зададимся вопросом: существуют ли однотипные выборки данных (датасеты) по некоторым уголовным, гражданским или арбитражным делам и неоспариваемые сторонами однотипные же судебные решения по ним? Представляется, что ответ содержится в статье 17 УПК РФ (применительно к уголовному процессу): «Судья оценивает доказательства по своему внутреннему убеждению, основанному на совокупности имеющихся в уголовном деле доказательств, руководствуясь при этом законом и совестью» [14]. Все перечисленное - чисто когнитивный процесс, задействующий восприятие, внимание, память, размышление, по-своему неповторимый и в определенной степени невоспроизводимый во внешне схожих ситуациях, поскольку обстоятельства совершения преступления и личность подсудимого также различаются в разных уголовных делах.

Таким образом, и в случае внедрения технологий искусственного интеллекта в судопроизводство такие технологии будут носить исключительно вспомогательный характер, не требующий какого-либо правового

регулирования, так как судебное решение в соответствии с требованиями процессуального кодекса будет по-прежнему формировать и оглашать суд.

Перечисленные аргументы авторов обусловливают их вывод о том, что текущий уровень развития технологий искусственного интеллекта не дает поводов и оснований для разработки мер правового регулирования таких технологий и их результатов. Усилия федеральных министерств и иных федеральных органов исполнительной власти должны быть направлены на максимально широкое внедрение технологий искусственного интеллекта, а научное сообщество должно максимально полно и понятно информировать всех потребителей будущих «интеллектуальных» услуг и товаров об их особенностях и безопасности.

Список литературы

1. Computing Machinery and Intelligence. Author(s): A. M. Turing. Source: Mind, New Series, Vol. 59, No. 236 (Oct., 1950), pp. 433-460 // URL: https://phil415.pbworks.com/f/TuringComputing.pdf/ (дата обращения: 01.11.2022).

2. McCulloch, W.S., Pitts, W. A logical calculus of the ideas immanent in nervous activity. Bulletin of Mathematical Biophysics 5, 115–133 (1943). // URL: https://doi.org/10.1007/BF02478259/ (дата обращения: 01.11.2022)

3. Norbert Wiener. Cybernetics: Or Control and Communication in the Animal and the Machine. 2nd revised ed.. — Paris: Hermann & Cie, Camb. Mass. (MIT Press), 1961. ISBN 978-0-262-73009-9. Первое издание — 1948 // URL: https://ia801701.us.archive.org/26/items/cybernetics-or-communication-and-control-in-the-animal-and-the-machine-norbert-wiene-ocr/Cybernetics%20or%20Communication%20and%20Control%20in%20the%20Animal%20and%20the%20Machine%20-%20Norbert%20Wiene_OCR.pdf/ (дата обращения: 01.11.2022).

4. Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // Собрание законодательства РФ, 27 апреля 2020 г., № 17, Ст. 2701 // URL: http://www.consultant.ru/document/cons_doc_LAW_351127/ (дата обращения: 01.11.2022).

5. Потапов, А.С. Технологии искусственного интеллекта / А.С. Потапов. М., 2010. 218 с.

6. Указ Президента Российской Федерации от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // URL: http://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 01.11.2022).

7. ГОСТ Р 59276-2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения» (утв. и введен в действие приказом

Федерального агентства по техническому регулированию и метрологии от 23 декабря 2020 г. № 1371-ст)//СПС «КонсультантПлюс».

8. ГОСТ Р 59921.1-2022 «Системы искусственного интеллекта в клинической медицине. Часть 1. Клиническая оценка» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 28 июня 2022 г. № 545-ст))//СПС»КонсультантПлюс».

9. ГОСТ Р 59895-2021 «Технологии искусственного интеллекта в образовании. Общие положения и терминология» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 26 ноября 2021 г. № 1617-ст))//СПС «КонсультантПлюс».

10. Распоряжение Правительства Российской Федерации от 19.08.2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // URL: http://www.consultant.ru/document/cons_doc_LAW_360681/ (дата обращения: 25.10.2022).

11. Федеральный конституционный закон от 06.11.2020 № 4-ФКЗ «О Правительстве Российской Федерации» // URL: http://www.consultant.ru/document/cons_doc_LAW_366950/ (дата обращения: 08.11.2022).

12. Locomotive Acts // URL: https://en.wikipedia.org/wiki/Locomotive_Acts/ (дата обращения: 08.11.2022).

13. ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» (утв. и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 ноября 2021 г. No 1520-ст))//СПС «КонсультантПлюс».

14. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ (ред. от 07.10.2022 г.) // URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 08.11.2022).

УДК 367

КИБЕРПРЕСТУПНОСЬ. К ВОПРОСУ О ПОНЯТИИ

Мерзляков Сергей Энгельсович,
Заслуженный юрист РФ, кандидат юридических наук, доцент
Национальный исследовательский университет
«Московский институт электронной техники» (МИЭТ),
г. Москва, Россия
e-mail: semel54@mail.ru

Аннотация: *в статье рассматриваются теоретические аспекты формирования концептуального определения феномена киберпреступности. Определяются классификационные основания формирования модели данного системного образования и характеризуются его структурные элементы. Определяются содержательные характеристики таких терминов как «киберпреступление», «преступления в сфере компьютерной информации».*

Ключевые слова: *киберпреступность, киберпреступление, киберпространство, преступность в сфере высоких технологий.*

CYBERCRIME. ON THE QUESTION OF THE CONCEPT

Merzlyakov Sergey Engelsovich,
Honored lawyer of the Russian Federation,
candidate of law, associate professor
National Research University of Electronic Technology (MIET) ,
Moscow, Russia
e-mail: semel54@mail.ru

Abstract: *the article deals with the theoretical aspects of the formation of a conceptual definition of the phenomenon of cybercrime. The classification grounds for the formation of a model of this systemic formation are determined and its structural elements are characterized. The content characteristics of such terms as "cybercrime", "crimes in the field of computer information" are determined.*

Keywords*: cybercrime, cybercrime, cyberspace, high-tech crime.*

Современный мир быстро меняется, трансформируясь под влиянием стремительно развивающихся информационных технологий. Данный процесс не может не затрагивать национальные интересы и национальную безопасность, т.к. с развитием информационных технологий растет и преступность в данной сфере. По данным П.В. Шмарион около 50% зарегистрированных киберпреступлений относятся к категориям тяжких и особо тяжких. По данным того же автора структуру данной преступности образуют деяния, предполагающие использование возможностей Интернета (53%), средств мобильной связи (39,4%), пластиковых карт (11,7%) и компьютеров (6,2%). Основными преступлениями в данной сфере являются

мошенничество (46.4%), кражи (33,5%), незаконный оборот наркотиков (8,4%)[1].

К сожалению, Интернет пока не приобрел официальный правовой статус, что не может не сказываться на характере киберпреступности, приобретающей глобальный характер. Кроме того, в современном международном законодательстве отсутствует единый подход к определению понятий *киберпреступность* и *киберпреступление*. Это приводит к тому, что преступники сами выбирают национальные правовые системы, наиболее соответствующие реализации их преступных намерений.

Термин «киберпреступность» характерен для государств, входящих в англо-саксонскую правовую семью, однако его применение возможно и в других странах, т.к. данный термин характеризует совокупность преступных посягательств, реализуемых в сфере информационно-телекоммуникационных технологий.

Остановимся на различных подходах к понятию «киберпреступление. Так, в США киберпреступления – это противоправные деяния, связанные с электронными устройствами, подключенными к сети. Данные деяния по положению, закрепленному Департаментом Юстиции, разделены на 3 группы:

1. Противозаконные деяния преступного характера, целью которых является само электронное устройство.

2. Противозаконные деяния преступного свойства, в которых электронное устройство выступает в качестве орудия преступления.

3. Противозаконные деяния преступного свойства, в которых устройство выступает в качестве источника хранения [2].

В России отсутствует нормативно закрепленное понятие «киберпреступление». Действующее уголовное законодательство использует термин «преступления в сфере компьютерной информации», который можно найти в названии соответствующей главы Уголовного кодекса страны. Данный закон фиксирует в гл.28 перечень деяний, признаваемых законодателем преступлениями. Это:

1. Неправомерный доступ к компьютерной информации (модификация, копирование или уничтожить информацию с помощью компьютера) (ст. 272 УК).

2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК).

3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК).

4. Неправомерное воздействие на критическую информационную инфраструктуру (ст. 274.1 УК) [3].

Попробуем разобраться с соотношением понятий «киберпреступления», «компьютерные преступления», «преступления в сфере компьютерной информации». Как представляется, ответ можно найти в материалах Конвенции о киберпреступности, открытой для подписания в Будапеште в ноябре 2001 года. Материалы данной конвенции определяют киберпреступления как деяния,

направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, а также злоупотребления такими системами, сетями и данными [4].

Особенностью данной группы преступлений является то, что они совершаются в «киберпространстве», которое, как утверждает испанский исследователь Г.М. Рамон, характеризуется отсутствием границ, суверенитета или территориальной юрисдикции, и как к моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленных в математическом, символьном или любом другом виде и что находятся в процессе движения по локальным и глобальным компьютерным сетям, или сведениях, которые хранятся у памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи [5].

В целом можно согласиться с мнением российского исследователя В.А. Голубева, который определяет киберпреступность как совокупность противоправных деяний, направленных на нарушение общественных отношений и персональной и коллективной безопасности во время осуществления лицами обмена данных с помощью электронных средств [6].

Кроме того, ряд исследователей данной проблемы, ставит знак равенства между киберпреступностью и преступностью в сфере высоких технологий. Так Л.А. Доровских говорит о том, что киберпреступление является актом социальной девиации, имеющего целью нанесение экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет [7].

В Российской Федерации применительно к комплексу изучаемых отношений употребляются термины «преступления в сфере высоких технологий», «преступность в сфере информационно-телекоммуникационных технологий». Как представляется, не вполне корректным является разделение компьютерной информации и информационных технологий. В соответствии с законом компьютерная информация представляет собой форму представления, а содержанием информационных технологий являются «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов» [8]. Соответственно, отделение информационных технологий от компьютерной информации представляется нецелесообразным. Юридические документы страны достаточно часто отождествляют преступления, совершаемые в сфере высоких технологий, с преступлениями, совершаемыми с использованием информационно-телекоммуникационных сетей [9]. В силу изложенного представляется целесообразным использование единого термина, обозначающего совокупность преступлений данной группы – это и может быть понятие «киберпреступность», тем более что оно является родовым понятием, нашедшем свое отражение в международных документах [10]. Этого же мнения придерживается и И.М. Рассолов, говоря о киберпреступности как о

совокупности уголовно-наказуемых деяний, совершаемых с использованием компьютерных сетей в виртуальном пространстве [11].

Можно отметить характерные особенности киберпреступности, выделяющие ее из системы преступности общеуголовной:

1. Наличие формируемой субъектами этой преступности субкультуры. Ее носители отличаются достаточно высоким уровнем интеллекта и имеют специфический набор знаний, выделяющих их из общей массы преступников-профессионалов.
2. Преступления данной группы можно совершать, даже не выходя из дома. Достаточно иметь компьютер и доступ в интернет.
3. Киберпреступники всегда анонимны и неперсонифицированы.
4. Киберпреступления совершаются на расстоянии. Потерпевшего от преступника могут отделять тысячи километров.
5. Очень высокий уровень латентности киберпреступности во много определяемый ранее обозначенными признаками и часто незначительным ущербом.
6. Транснациональный характер киберпреступности и совершение киберпреступлений достаточно часто в составе организованных групп. (по данным И.А. Кучеркова до 62% киберпреступлений совершаются именно в составе организованных преступных формирований [12].

Основными видами киберпреступлений на сегодняшний день являются:

1. Общественно-опасные деяния, посягающие на конституционные права и свободы человека и гражданина (неприкосновенность частной жизни, нарушение авторских и смежных прав и т.д.)
2. Общественно-опасные деяния, посягающие на жизнь и здоровье. Исследователи данной проблемы приводят пример убийства, осуществленного с помощью Интернета, когда потерпевшему через Сеть изменили режим работы кардиостимулятора и отключили аппарат искусственной вентиляции легких [13]. Кроме того, широкое распространение в сети получили сайты, пропагандирующие суицидальное поведение, употребление наркотиков и т.п.
3. Преступления, объектами которых становятся честь и достоинство личности (распространение клеветнической информации и т.п.).
4. Общественно опасные деяния, объектами которых становится собственность. Именно данные преступления во всех своих проявлениях и являются самыми распространёнными видами киберпреступлений.
5. Преступления, посягающие на финансово-банковскую сферу. Исследователи данной группы отношений отмечают изменение объектов кибератак (от клиентов непосредственно на финансовые организации) [14].
6. Общественно опасные посягательства на компьютерную информацию (создание, использование и распространение вредоносных программ и т.п.).
7. Общественно опасные деяния, посягающие на общественную нравственность (порнобизнес во всех его проявлениях).
8. Незаконный оборот наркотических средств и психотропных препаратов.
9. Общественно опасные деяния, посягающие на государственную безопасность (государственная измена, шпионаж, разглашение государственной тайны и т.д.).

10. Преступления террористической и экстремистской направленности.

Можно отметить, что киберпреступность одна из наиболее опасных угроз национальной безопасности. Важнейшей задачей государства и гражданского общества страны является задача выявления и нейтрализации ее детерминант, объединение усилий всех заинтересованных сторон. Это предполагает соответствующее нормативное урегулирование вопросов данного взаимодействия, связанного с обменом необходимой информацией, составлением соответствующих программ, сбором информации обо всех блоковых элементах криминологического и криминалистического планирования (детерминанты киберпреступности, данные о жертвах киберпреступлений и их личностных характеристиках и т.п.).

Список литературы

1. Шмарион, П.В. Киберпреступность - вызов 21 века / П.В. Шмарион // Вестник экономической безопасности. 2021. № 1. С. 147.
2. Evans, L.E. Internet Overview / L.E. Evans, Jr. New York: 63 TEX. B.J. 2000. P. 23.
3. Уголовный кодекс Российской Федерации от 13.06.1996г. № 63-ФЗ (ред. от 02.08.2019)//СПС»КонсультантПлюс».
4. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) // URL: https://base.garant.ru/4089723/.
5. Ramón, J.M. Territorio, tiempo y estrutura del ciberespacio / J.M. Ramon. 2014. P.25-26. Ibidem.
6. Голубев, В.А. «Кибертерроризм» - миф или реальность? // Центр исследования компьютернных преступлений. URL: http://www.crime-research.org .Computer Crime Research Centre.
7. Доровских, Л.А. Преступления в сфере высоких технологий. Киберпреступность / Л.А. Доровских // Sciencetime. 2016. № 4 (28).
8. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Рос. Газ. 2006. 29 июля. № 165.
9. утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола: приказ МВД России № 786, Минюста РФ № 310, ФСБ РФ № 470, ФСО РФ № 454, ФСКН РФ № 333, ФТС РФ № 971 от 06.10.2006 г. (ред. от 22.09.2009 г.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2006. № 47.
10. Всестороннее исследование проблемы киберпреступности // Организация Объединенных Наций. Нью-Йорк, 2013 год. - URL: https://www.unodc.org/documents/organizedcrime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 10.02.2023).
11. Рассолов, И.М. Право и интернет: теоретические проблемы: дис. … д-ра юрид. наук / И.М. Рассолов. М., 2008. 357 с.
12. Кучерков, И.А. О понятии «киберпреступление» в законодательстве и научной доктрине / И.А. Кучерков // Юридическая наука. 2019. № 10. С.80.

13. Алескеров, В.И. Особенности отдельных следственных действий при расследовании преступлений в сфере компьютерной информации / В.И. Алескеров, И.А. Максименко // Вестник ВИПК МВД. 2010. № 3. С.9.
14. Захаров, Д.Н. Особенности расследования кибепреступлений / Д.Н. Захаров, В.В. Щерба // Вопросы кибербезопасности. 2017. № S2 (20). С. 72.

УДК 34.1

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЛЕ ОБЕСПЕЧЕНИЯ ПРАВОПОРЯДКА В СОВРЕМЕННОЙ ГЕРМАНИИ

Мерзляков Сергей Энгельсович,
Заслуженный юрист РФ, кандидат юридических наук, доцент
Чопсиев Руслан Адильевич,
студент,
Национальный исследовательский университет
«Московский институт электронной техники» (МИЭТ),
г. Москва, Россия
e-mail: semel54@mail.ru
e-mail: chopsiev2@bk.ru

Аннотация: *в статье рассматриваются вопросы теоретического и практического плана, связанные с возникающими в правоохранительной деятельности проблемами использования искусственного интеллекта. Отмечается возможность его использования в континентальной системе уголовного правосудия. В статье приводятся также концептуальные подходы к определению феномена искусственного интеллекта для современной Европы.*

Ключевые слова: *искусственный интеллект, кибератака, дипфейк, системы обучения и предсказания судебных решений.*

THE ROLE OF ARTIFICIAL INTELLIGENCE IN LAW ENFORCEMENT IN MODERN GERMANY

Merzlyakov Sergey Engelsovich,
Honored lawyer of the Russian Federation,
candidate of law, associate professor
Chopsiev Ruslan Adilevich,
student
National research university of electronic technology (MIET) ,
Moscow, Russia
e-mail: semel54@mail.ru
e-mail: chopsiev2@bk.ru

Abstract: *the article deals with theoretical and practical issues related to the problems of using artificial intelligence arising in law enforcement. The possibility of*

its use in the continental criminal justice system is noted. The article also provides conceptual approaches to the definition of the phenomenon of artificial intelligence for modern Europe.

Keywords: *artificial intelligence, cyberattack, deepfake, training systems and predicting court decisions.*

*Развитие общества в современном мире нера*зрывно связано со стремительным развитием информационных технологий, применяемых в том числе правоохранительными органами в качестве вспомогательных элементов обеспечения правопорядка.

Знаковым явлением в данном процессе стало внедрение в правоохранительную деятельность искусственного интеллекта (ИИ).

Следует отметить, что преступный мир также активно его использует, что предполагает необходимость своевременного реагирования на появляющиеся в мире вызовы и угрозы, качественно изменяющиеся в процессе обретения преступниками профессиональных навыков в данной сфере.

Правоохранительные системы в мире стали активно использовать ИИ в борьбе с противоправными посягательствами после 2010 года.

Проблемы его определения и применения на международном уровне, в частности, активно рассматривались в рамках деятельности соответствующих комитетов организации по безопасности и сотрудничеству в Европе [1].

Изучение различных аспектов применения ИИ в деятельности правоохранительных структур предполагает учитывать, что:

1) ИИ является важнейшим элементом обеспечения общественной безопасности;

2) ИИ позволяет оптимизировать распределение сил и средств эту безопасность, обеспечивающих;

3) использование ИИ должно осуществляться специализированными подразделениями правоохранительных структур, обладающих не только соответствующими знаниями в данной сфере, но и необходимым набором нравственных качеств, исключающих противоправное использование ИИ [2].

Рассмотрение основных направлений деятельности правоохранительных органов современной Германии по борьбе с преступностью в стране предполагает необходимость изучения и практики применения ИИ в этом виде деятельности.

Решение данной задачи требует определения того, чем же является ИИ. Современные немецкие исследователи данного феномена отмечают отсутствие единообразного понимания его сущностных характеристик.

В попытке преодолеть терминологическую неопределенность в данном вопросе Комиссия ЕС разработала проект Закона об искусственном интеллекте, основанный на комплексном изучении данного феномена.

В основу формирующегося понимания сущности ИИ Комиссия положила подходы к ИИ, которые связаны с: а) его машинным обучением, включая контролируемые и неконтролируемые виды; б) логикой и знаниями, учитывающими базы знаний, логические и дедуктивные механизмы,

символические рассуждения и экспертные оценки; в) подходами, связанными со статистической оценкой, минимизирующей апостериорное математическое ожидание функции потерь [3].

В отличии от большинства материалов на тему применения ИИ в целях помощи правосудию, мы предлагаем первоначально посмотреть на применение ИИ самими преступниками. Ведь понимая, как может действовать злоумышленник, мы сможем эффективно ему противостоять.

Рассмотрение методик применения ИИ в правоохранительной деятельности предполагает необходимость учета того обстоятельства, что преступники уже достаточно давно используют его в своих целях. Немецкие криминалисты обращают наше внимание на наиболее опасные варианты использования злоумышленниками возможностей ИИ в целях личного обогащения или дестабилизации политической ситуации. В частности, речь идет о дипфейках.

Дипфейки (Deepfake) - методика синтеза изображения, основанная на возможностях ИИ. Методика синтеза изображения используется для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики. Сейчас этот метод активно развивается киберпреступниками. Существуют как базовые программы, так и очень технически и интеллектуально продвинутые. Уже зафиксированы случаи, когда изображение человека и его голос формируемые с помощью ИИ получались настолько достоверными, что у других людей даже не вызывало сомнение, что с ними разговаривает настоящий человек [4]. С помощью дипфейков вы можете заставить изображенных людей совершать действия или делать заявления, которых никогда не было.

Эти же специалисты говорят и о кибератаках. Следует отметить, что они не обязательно должны идти рука об руку с использованием технологий, называемых ИИ. Тем не менее, и здесь прослеживается четкая тенденция, что уже известные криминальные методы досмотра в цифровом пространстве которые могут быть изменены, усилены или расширены с помощью высокотехнологичного информационного инструментария.

До сих пор успешные кибератаки обычно характеризовались высокой привязкой к конкретному целевому объекту [5]. Ярким примером таких случаев являются атаки с использованием так называемых «программ-вымогателей» [6]. Ранее злоумышленники активно использовали так называемые «баннеры» и «программы шифровщики», которые зашифровывают конкретные типы файлов на персональном компьютере. Здесь ИИ сам генерирует код, поэтому просто невозможно уничтожить внедренный «вирус» с помощью антивирусных программ. Пользователь рискует потерять всю свою информацию, так как ИИ шифруя файлы, по сути, маркирует их как «вирусные».

Исследователи отмечают также случаи разжигание ненависти с помощью «социальных ботов»

Это автономные компьютерные программы, которые способны имитировать текстовое человеческое общение [7]. В то время как так называемые «доброжелательные боты» в основном используются службами

поддержки клиентов или в рекламных целях, «вредоносные боты» могут распространять ложную информацию или фальсифицировать мнения якобы большинства с целью повлиять на формирование общественного мнения. Наверное, самый известный пример — чат-бот «Tay» от Microsoft, который вышел в сеть 23 марта 2016 года в Twitter. Через некоторое время он начал публиковать расистские, сексистские и антисемитские сообщения, поэтому Microsoft была вынуждена прекратить эксперимент через 16 часов и вывести вышедшего из-под контроля социального бота в автономный режим [8].

Кратко остановимся на применении ИИ в судопроизводстве. Вполне возможно, что в уголовном судопроизводстве системы ИИ могут использоваться в первую очередь для технической поддержки проводимых процессов. В Соединенных Штатах уже можно использовать системы обучения предсказанию судебных решений. Около 70,2 % решений Верховного суда можно было правильно предсказать с помощью «случайного» метода [9]. Подобные системы, как представляется, наиболее подходят для адвокатской практики, т.к. имеется возможность разработать наилучшую стратегию защиты во время судебного процесса.

Однако в настоящее время такие системы в Германии не применяются, что связано в первую очередь с системным отличием континентального права от англо-американского. В Германии не публикуется даже 1% вынесенных решений включая в основном судебную практику верховных судов [10]. Публикация решений судов, использующих прецедентное право, которая имела бы решающее значение для обучения систем прогнозирования, до сих пор представляла собой абсолютное исключение. Изменится ли это в ближайшее время - неизвестно.

Что касается помощи судьям в принятии решений, системы ИИ также предлагают возможности для решения таких задач. Речь идет не столько об идее робота-судьи - утопической или антиутопической, в зависимости от вашей точки зрения, сколько о подходах к системам поддержки, которые могут облегчить повседневную работу судов [11].

По мнению немецких юристов, существует значительный потенциал применения ИИ в сфере вынесения судебных решений, где на протяжении десятилетий известны большие региональные различия в принимаемых постановлениях о наказаниях за сопоставимые правонарушения. Таким образом, можно избавиться от лишней работы, где не нужен профессионализм судьи. Это позволит ему сосредоточиться на рассмотрении характеристик дела, дающих возможность вынести истинно правосудное решение [12].

Список литературы

1. Яковец, Е.Н. Оперативно-разыскные меры полиции по обеспечению информационной безопасности Российской Федерации / Е.Н. Яковец // Труды Академии управления МВД России. 2017. № 3. С.127–131.

2. Ларина, Е.С. Роботы-убийцы против человечества. Кибер-апокалипсис сегодня / Е.С. Ларина, В.С. Овчинский. М.: Кн. Мир, 2018.416 с.

3. Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts от 21.04.2021 г. № 52021PC0206 // European Commission. 2021. с изм. и допол. в ред. от COM (2021) 206 final 21. April 2021.

4. Anna, L. Das Phänomen Deepfakes. Künstliche Intelligenz als Element politischer Einflussnahme und Perspektive einer Echtheitsprüfung / L. Anna, T Milan, A. Hartmut, F. Jan, K. Christian, D. Jana // Künstliche Intelligenz, Demokratie und Privatheit. Nomos, 2022. P. 265-287.

5. David, K. The Real Story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran's nuclearfuel enrichment program / K. David // IEEE Spectrum. 2013. P. 1-6.

6. Dieter Kochheim. Rechtshandbuch Artificial Intelligence und Machine Learning. München: Verlag C. H. Beck oHG, 2018. 964 p.

7. Volkmann, V. Hate Speech durch Social Bots / V. Volkmann // Multimedia und Recht. 2018. T. 2. P. 58-63.

8. Carlos Freitas, Fabrı´cio Benevenuto, Adriano Veloso, Saptarshi Ghosh. An empirical study of socialbot infiltration strategies in the Twitter social network / Carlos Freitas // Social Network Analysis and Mining. 2016. P. 1-3.

9. Daniel Martin Katz, Michael J Bommarito II, Josh Blackman. A General Approach for Predicting the Behavior of the Supreme Court of the United States // SSRN. 2017. 19.01.

10. Dr. Hanjo Hamann. Der blinde Fleck der deutschen Rechtswissenschaft – Zur digitalen Verfügbarkeit instanzgerichtlicher Rechtsprechung // JZ. 2021. P. 656-665.

11. Greco, L. Richterliche Macht ohne richterliche Verantwortung: Warum es den Roboter- Richter nicht geben darf / L. Greco // Rechtswissenschaft. 2020. № 11. P. 21– 62.

12.Frank Neubacher, Nicole Bögelein Krise. Kriminalität – Kriminologie. Mönchengladbach: Forum Verlag Godesberg GmbH, 2016. 645 p.

УДК 367.1

ДОПРОС В КАЧЕСТВЕ ПОТЕРПЕВШЕГО РЕБЕНКА В ВОЗРАСТЕ ДО СЕМИ ЛЕТ В КОНТЕКСТЕ ПРИНЦИПА ГУМАНИЗМА РОССИЙСКОГО ПРАВА

Николюк Вячеслав Владимирович
доктор юрид. наук, профессор,
Заслуженный деятель науки Российской Федерации,
главный научный сотрудник НИЦ-5
Всероссийский научно-исследовательский институт МВД России
г. Москва, Россия
e-mail: nvv56@mail.ru

Аннотация: *в статье с позиций принципа гуманизма анализируется закрепленный в УПК РФ порядок допроса в качестве потерпевших детей в возрасте до семи лет. Автор обращает внимание на психолого-физические особенности лиц данной возрастной группы с позиций способности их правильно воспринимать обстоятельства, имеющие значение для дела, и давать о них показания. Учитывая когнитивные характеристики дошкольников, затрудняющих их возможности давать объективные и полные показания, и руководствуясь соображениями гуманности автор выступает с предложением отказаться от их допроса в качестве потерпевших и свидетелей.*

Ключевые слова: *ребенок, малолетний, потерпевший, психолого-физиологические особенности, показания, допрос потерпевшего.*

INTERROGATION AS A VICTIM OF A CHILD UNDER THE AGE OF SEVEN IN THE CONTEXT OF THE PRINCIPLE OF HUMANISM OF RUSSIAN LAW

Nikolyuk Vyacheslav Vladimirovich
doctor of law sciences, professor,
Honored scientist of the Russian Federation,
Chief researcher of SIC-5
All-Russian Research Institute of the Ministry of Internal Affairs of Russia,
Moscow, Russia
e-mail: nvv56@mail.ru

Abstract*: from the standpoint of the principle of humanism, the article analyzes the procedure of interrogation as victims of children under the age of seven, enshrined in the Code of Criminal Procedure of the Russian Federation. The author draws attention to the psychological and physical characteristics of persons of this age group from the standpoint of their ability to correctly perceive the circumstances relevant to the case and give evidence about them. Taking into account the cognitive characteristics of preschoolers, which make it difficult for them to give objective and*

complete testimony, and guided by considerations of humanity, the author makes a proposal to refuse to interrogate them as victims and witnesses.

***Keywords**: child, juvenile, victim, psychological* and physiological features, testimony, interrogation of the victim.

Криминологическую ситуацию, характеризующую количество и виды совершаемых в отношении несовершеннолетних преступлений, следует признать неблагоприятной.

Согласно официальным данным статистической отчетности в 2022 г. зарегистрировано 115, 3 тыс. преступлений в отношении несовершеннолетних. В 2022 г. совершено 11,6 тыс. преступлений против половой неприкосновенности несовершеннолетних и их половой свободы, причинивших потерпевшим физические и психические травмы, часто имеющие пролонгирующее действие. 58 тыс. потерпевших – лица женского пола. В отношении 55,8 тыс. несовершеннолетних преступления совершили члены семьи, из них 54,6 тыс. преступлений совершены родителями.

В контексте освещаемой в докладе проблематики полагаем целесообразным заострить внимание на допросе в качестве потерпевшего детей, не достигших возраста семи лет. В ч. 1 ст. 191 УПК РФ эта возрастная группа обозначена отдельно. Проведение следственных действий с потерпевшими в возрасте до семи лет имеет ряд особенностей, встречает серьезные затруднения организационного, психологического плана, вследствие чего снижается или вовсе утрачивается их результативность. Подчеркнем, что речь идет не о единичных случаях, а о нескольких десятках тысяч следственных действий, главной фигурой которых являются дети в возрасте до семи лет.

Реализованная в отечественном уголовно-процессуальном законодательстве концепция пригодности в доказывании показаний малолетних потерпевших исходит из следующих положений:

1) дети в возрасте до семи лет в силу присущего им интеллекта способны при их допросе дать объективные показания о происшедшем;

2) пробелы в их показаниях объясняются главным образом чувством страха, стыда и смущения, испытываемых жертвой насилия, которые могут быть устранены следователем, психологом в ходе допроса. С учетом этих факторов строится криминалистическая тактика допроса в качестве потерпевшего ребенка в возрасте до семи лет.

Предусмотренные в УПК РФ (ст. 191) гарантии обеспечения прав и законных интересов несовершеннолетних потерпевших трудно реализуемы при производстве допроса лиц указанного возраста, практически не влияют на качество получаемых от них показаний. В действительности эффективность допроса детей в возрасте до семи лет находится в прямой зависимости от профессиональной подготовленности следователя.

Принимая решение допросить малолетнего потерпевшего, следователь исходит из того, что последний способен правильно воспринимать обстоятельства, имеющие значение для дела, и давать о них показания. При

возникновении сомнений в этом начинают действовать положения п. 4 ст. 196 УПК РФ об обязательном назначении экспертизы (в данном случае судебно-психологической экспертизы). Сомнения же в способности правильно воспринимать обстоятельства случившегося и давать о них показания объективно возникают у следователей, по их собственному признанию, в каждом случае, когда предстоит допрашивать ребенка в возрасте до семи лет.

Психологические особенности детей-дошкольников убеждают в том, что допросу детей в возрасте до семи лет в качестве потерпевших должно предшествовать назначение и производство экспертизы в соответствии с п. 4 ст. 196 УПК РФ. Только после получения заключения эксперта-психолога о способности малолетнего потерпевшего воспринимать и воспроизводить значимые для дела сведения следователь может принять решение его допросить. В следственной практике такой алгоритм действий следователя не приветствуется, он скорее исключение, чем правило.

Как можно судить по литературным источникам, практика применения ст. 191, п. 4 ст. 196 УПК РФ формируется в основном под влиянием двух факторов: 1) боязнь нанести ребенку психическую травму; 2) недооценка психологических возможностей детей, их способности воспроизводить воспринятые события.

Таким образом, целесообразность корректировки существующего порядка допроса в качестве потерпевших детей в возрасте до семи лет весьма актуальна. Рассмотрим два варианта оптимизации обозначенной ситуации.

1. Сохранение возможности допроса в качестве потерпевшего ребенка в возрасте до семи лет.

Первый вариант предполагает признание обязательным условием допроса таких лиц предварительное проведение судебно-психологической экспертизы для установления способности ими воспринимать обстоятельства, имеющие значение для уголовного дела, и давать о них показания (п. 4 ст. 196 УПК РФ). Такой подход позволит «отобрать» для участия в следственном действии только тех детей дошкольного возраста, которые способны давать показания. При этом следователь обязан принять меры и к обеспечению охраны здоровья потерпевшего (выбор времени, места проведения допроса, подбор участников следственного действия).

Предлагаемый порядок допроса указанных лиц увеличит процессуальную нагрузку следователей и экспертных учреждений, однако сократит число «допросов ради допросов» в качестве потерпевших детей дошкольного возраста, а значит и уменьшит риск причинения вреда их здоровью.

Реализация данного предложения потребует дополнения ч. 1 ст. 191 УПК РФ соответствующим положением.

2. Допрос в качестве свидетеля и потерпевшего детей в возрасте до семи лет не проводится. Когнитивные особенности лиц этой возрастной группы серьезно ограничивают их способность воспринимать обстоятельства наступившего события и давать о них показания, в связи с чем практическая

целесообразность допроса таких лиц, с точки зрения полезности их показаний для уголовно-процессуального доказывания, минимальна.

В целях получения доказательственной информации, носителем которой является ребенок – жертва преступления, представляется возможным допрашивать его родителей, близких родственников, педагогов, психолога и других лиц, которым могут быть известны сведения, имеющие значение для дела.

С такой постановкой вопроса согласились 68 % опрошенных следователей и 100 % следователей, которым при расследовании уголовных дел приходилось непосредственно допрашивать малолетних.

Безусловно, «жесткий» вариант решения проблемы допроса в качестве потерпевших детей в возрасте до семи лет ожидаемо вызовет определенные возражения. Можно даже спрогнозировать основное из них: *закрепление указанной нормы не позволит следователю произвести допрос несовершеннолетнего, не достигшего возраста семи лет, даже в том случае, когда его показания будут фактически единственным источником информации для производства дальнейших следственных действий и оперативно-розыскных мероприятий*.

Однако выводы следователя, прокурора и, конечно же, суда основываются не на главном, центральном, ключевом, решающем доказательстве, а на совокупности доказательств. Одно доказательство может быть ценным, важным, но недостаточным для разрешения дела по существу.

Отказ от допроса в качестве потерпевших детей в возрасте до семи лет послужит ярким примером гуманизации уголовного судопроизводства. В мире, включая естественно и Россию как значительную часть мирового пространства, стремительно происходят разительные перемены в большинстве сфер жизнедеятельности людей. Человеческая цивилизация достигла невиданного буквально несколько десятилетий назад уровня развития технологий, необратимо формирующих совершенно новые реальности, служащие фундаментом для права. Становление нового реального мира неизбежно приводит к смене или корректировке ценностей и идеалов, определяющих социокультурный феномен права и играющих роль своеобразных маяков, на которые ориентируется право в своем движении.

Как следствие указанных метаморфоз появляются проблемы разработки новых концептов человека в праве («правового человека») и прав человека, актуализируется в целом философско-правовая проблематика, предлагающая к усвоению новые процессы, обозначаемые динамикой права: сочетание в праве всечеловеческого, общечеловеческого и локального (национального); расширения сферы взаимодействия технического, этического и правового регулирования; дегуманизация права, его инфантилизация, цифровизация, конвергенция с машинным кодом[1]. Неправильный «крен» права в условиях последних тенденций технологического развития способен привести к дегуманизации общественной жизни и самого человека. «Для права данный процесс, - бьет тревогу В.В. Лапаева, - имеет фатальные последствия, поскольку право в своей основе есть право человека»[2] Практически об этом десять лет назад писал председатель Конституционного Суда РФ В.Д. Зорькин: «право человека – это высшая ценность именно государств, главное

содержание деятельности которого (законодательной, исполнительной и судебной) состоит в обеспечении и охране прав человека»[3].

В этой связи особое значение при расстановке приоритетов в праве приобретает принцип гуманизма, в центре внимания которого находятся достоинство, интересы, потребности человека, а сам человек считается высшей ценностью.

Тезис о приоритете прав человека, получив закрепление в ст. 2 Конституции РФ, приобретает общеправовой характер. Он находит отражение и на отраслевом уровне с закреплением его в качестве самостоятельного принципа в кодифицированных законах с выделением “под него” отдельной статьи и включением его в систему принципов той или иной отрасли законодательства. Примером тому служит ст. 7 УК РФ.

Таким образом, гуманизм как правовой принцип прошел этап легитимации и в той или иной степени участвует в механизме правового регулирования. Нормативно-правовая основа производства по уголовных делам с участием несовершеннолетних в большей степени чем другие уголовно-процессуальные институты и производства восприняла гуманистические идеи. Буквально чуть ли не каждая норма УПК РФ, участвующая в правовом регулировании производства по указанной категории дел, коррелирует с принципом гуманизма (ч. 2.1 ст. 45, ст. 105, ст. 191, гл. 50 УПК РФ). Запрет допрашивать в качестве потерпевших детей в возрасте до семи лет, будучи безусловным отражением принципа гуманизма, ориентированного на максимально полную защиту прав и законных интересов малолетних и несовершеннолетних как участников уголовного процесса, органически впишется в рамки современной российской уголовно-процессуальной политики.

Отметим, что еще в 1989 г. авторитетными отечественными учеными-процессуалистами обсуждались перспективы дальнейшей гуманизации тогда «советского» уголовного процесса». «Гуманные соображения требуют, например, - писал И.Ф. Демидов, - ввести в закон норму, освобождающую свидетеля от обязанности давать показания, учитывая его близкие родственные отношения с обвиняемым, либо потому, что ответы на поставленные ему вопросы могут скомпрометировать его самого»[4]. Данные предложения уже сравнительно давно реализованы в законе. Получение показаний от потерпевшего дошкольника не самоцель. Обычно акцент при этом делается на доказательственной ценности показаний в ущерб физическому и психическому здоровью ребенка. Представляется, что выбор должен быть сделан в пользу охраны человеческих ценностей.

Список литературы

1. Хабриева, Т.Я. Будущее права. Наследие академика В.С. Степина и юридическая наука / Т.Я. Хабриева, Н.Н. Черногор. М., 2020. С. 23-25.

2. Лапаева, В.В. Российская философия права в новых реалиях: главные вызовы / В.В.Лаптева// Российская юстиция. 2022. № 10. С. 5.

3. Зорькин, В.Д. Право в условиях глобальных перемен: монография / В.Д.Зорькин. М., 2013. 398с.

4. Курс советского уголовного процесса. Общая часть / Под редакцией А.Д. Бойкова и И.И. Карпеца. М., 1989. 146с.

УДК 343.1

О ПРОБЛЕМАХ КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Новогонская Маргарита Сергеевна,
аспирант
Московский государственный университет имени М.В. Ломоносова,
г. Москва, Россия

Фёдоров Алексей Роальдович,
кандидат технических наук, доцент
Национальный исследовательский университет
«Московский институт электронной техники» (МИЭТ),
г. Москва, Россия
e-mail: novogonskaya.m@mail.ru

Аннотация: *в статье рассмотрены проблемы компьютерного моделирования в уголовном судопроизводстве. Автор также рассматривает перспективы и возможности влияния компьютерного моделирования на уголовное судопроизводство на примере использования компьютерного моделирования в экспертной деятельности и цифрового двойника при расследовании серийных убийств.*

Ключевые слова: *Моделирование, экспертная деятельность, цифровой двойник, искусственный интеллект, нейронная сеть, машинное обучение, криминалистика, серийные убийства.*

HIGH-TECH MODELING AS A METHOD OF IDENTIFYING SERIAL KILLERS

Novogonskaya Margarita Sergeevna,
postgraduate student
Lomonosov Moscow State University,
Moscow, Russia

Fedorov Alexey Roaldovich ,
candidate of technical sciences, associate professor
National Research University of Electronic Technology (MIET),
Moscow, Russia
e-mail: novogonskaya.m@mail.ru

Abstract: *the article deals with the problems of computer modeling in criminal proceedings. The author analyzes the prospects and possibilities of computer modeling influence on criminal proceedings on an example of computer modeling usage in expert activity and digital twin during serial murders investigation.*

Keywords: *simulation, expert work, digital twin, artificial intelligence, neural network, machine learning, criminalistics, serial murders.*

Научная криминалистика имеет сложную синтетическую природу, закономерность развития которой определяется нормами следственно-судебной и экспертной практики, требованиями уголовного и уголовно-процессуального законодательства, развитием естественных, технических, информационных и иных наук. В последние годы весьма широкое распространение в уголовном судопроизводстве получили методы моделирования, используемые для решения самых разнообразных задач, и определены правовые основания и условия реализации этих методов в уголовном судопроизводстве.

В общенаучном смысле под моделью понимается такая мысленно представляемая или материально реализованная система, которая, отображая или воспроизводя объект исследования, способна заменить его так, что ее изучение даст нам новую информацию об этом объекте. Развитие компьютерных технологий способствовало появлению нового вида моделирования – компьютерного. Оно активно используется в технических и естественных науках, при этому все больше говорят о его возможностях и перспективах для криминалистики. Создание общедоступных компьютерных кластеров с высокой производительностью и публичных хранилищ данных практически бесконечного объема позволяет сегодня создавать весьма сложные криминалистические модели на основе технологий искусственного интеллекта, ориентированные на использование в деятельности по раскрытию и расследованию преступлений. Тематика искусственного интеллекта, являясь особо актуальной в настоящее время, в области криминалистики отмечена значимыми трудами А.А. Бессонова «Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений», докторской диссертацией М.П. Морхата «Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы». Возможности применения технологий искусственного интеллекта в криминалистике освещались в работах С.Б. Вехова, И.Р. Бегишева, С.В. Зуева, В.А. Мещерякова, А.В. Незнамова, А.Н. Охлупиной, Н.С. Полевого, В.Ю. Толстолуцкого и многих других Российских и зарубежных учёных.

Моделирование объединяет в себе несколько различных процессов: создание, модели путем отбора информации соответствующего направления, проведение модельных экспериментов, формирование суждений об изучаемом реальном объекте, получение нового знания. Одна из главных характеристик моделирования – его опосредованности. Модель в процессе познания объединяет объект познания, существующий в реальности, и субъект, его познающий. Модель – инструмент исследования, а не сама реальность. Функция модели: репрезентативность, её задача – представление, замещение какого-либо объекта в ходе его исследования и познания.

Применение моделирования в криминалистике целесообразно в строго определенных случаях, когда у следователя возникает необходимость в получении информации опосредованным путем. А именно:

– когда объект познания существовал в прошлом и его уже нет на момент исследования (например, преступное событие, криминальные ситуации);

– когда объект познания еще только будет существовать (возможная следственная ситуация в ходе предстоящего допроса, моделируемая в процессе подготовки к нему);

– когда объект существует реально на момент исследования, однако он либо чрезмерно сложен, либо вовсе недоступен для познания;

– когда познаваемый процесс протекает или слишком быстро или же, наоборот, слишком медленно (отдельные виды следственных экспериментов).

Под используемой в криминалистике моделью мы понимаем искусственно созданную материальную или идеальную систему, воспроизводящую и заменяющую исследуемое криминальное событие или отдельные ситуации и обстоятельства его совершения, а также ситуации и обстоятельства его расследования так, что ее изучение позволит получить об оригинале информацию, необходимую для раскрытия, расследования и предупреждения преступления.

Сущность математического моделирования в криминалистике состоит в формализации криминалистической проблемы, ее решение посредством математического аппарата и криминалистическая интерпретация полученных результатов. Разработка и внедрение различных математических моделей в следственную практику – важнейшая задача криминалистической науки.

В качестве особого вида моделирования можно рассматривать реконструкции вещественные и ситуационные. В следственной практике под реконструкцией воссоздание объектов или ситуаций по останкам, снимкам, описаниям или по другим сохранившимся данным. К подобного рода моделям можно отнести реконструкцию лица по черепу, изображение преступника, составленное при помощи фоторобота.

Проблемы внедрения компьютерного моделирования в уголовное судопроизводство в РФ видятся следующие:

1. Недостаточное техническое оснащение правоохранительных органов;

2. Недостаточное финансирование разработок программного обеспечения криминалистических моделей на основе ИИ;

3. Отсутствие законодательной базы и единого подхода к созданию криминалистических баз данных.

Общая цель внедрения компьютерного моделирования в уголовное судопроизводство видится как ускорение и упрощение работы следователя, дознавателя, эксперта.

Рассмотрим перспективы и возможности влияния компьютерного моделирования на уголовное судопроизводство на некоторых примерах.

Использование «цифрового двойника» при расследовании серийных убийств. Цифровой двойник (Digital Twins) — это синхронизированная виртуальная модель любых объектов, систем, людей, процессов и сред, имитирующая внутренние процессы, технические характеристики и поведение реального объекта в условиях воздействия помех и окружающей среды. Цифровой двойник отслеживает прошлое и предсказывает будущее и является обучаемой системой, состоящей из комплекса математических моделей разного уровня сложности, уточняемых по результатам натурных экспериментов, и представляет собой меняющийся цифровой профиль, содержащий

исторические и наиболее актуальные данные о физическом объекте или процессе. Цифровые двойники совместно с машинным обучением позволяют создавать достоверную модель и прогнозировать поведение изучаемого объекта в будущем, основываясь на анализе больших и слабоструктурированных массивов данных.

Цифрового двойника в криминалистике можно использовать в нескольких направлениях.

Модели первого типа определяют, кто с наибольшей вероятностью совершит преступление или, наоборот, станет жертвой. Они оценивают профили людей с учетом возраста, криминальной истории, данных о трудоустройстве, знакомств (например, через страницы в социальных сетях) и другой информации. Какие именно сведения для этого используются, зависит как от разработчиков, так и от сложившейся судебной практики. Перспективой применения данной модели является увеличение раскрываемости серийных убийств, снижение нагрузки на правоохранительные органы.

В моделях второго типа главное - время и место, то есть где и когда может быть совершено преступление. Алгоритмы делят территорию города на маленькие зоны площадью несколько десятков метров - это может быть конкретный квартал или перекресток - и высчитывают вероятности событий на основании поступающих данных.

Пример модели второго типа программа PredPol, строит прогнозы, опираясь на статистику сообщений об убийствах, кражах, ограблениях, угонах транспорта. Но также могут учитываться даже погода, часы работы окрестных баров и школ, данные об арестах или условно-досрочном освобождении. Если программа считает, что риск совершения преступления высок, на место отправляют наряд полиции. Предсказание преступлений методами машинного обучения используется полицией на всей территории США в течение почти десяти лет, однако в процессе её эксплуатации выявлен ряд существенных недостатков и Калифорнийский Санта-Круз стал первым американским городом, который запретил полицейскую деятельность по предсказанию преступлений. По мнению экспертов по цифровым правам, аналогичные шаги можно ожидать по всей стране.

Компьютерное моделирования в экспертной деятельности широко используется как в физическом моделировании – фотосьемка, гипсовые слепки, так и в мысленном моделировании – реконструкция любого вида. Моделирование используется во всех видах экспертиз – почерковедческой, трасологической, фототехнической, портретной, взрывотехнической, технической экспертизе документов [1]. Увеличивающееся количество ДТП увеличило объем экспертных исследований.

Рассмотрим возможности использования компьютерного моделирования на_примере расследования ДТП. 3D моделирование примеряется в США, Великобритании, Германии при автотехнических экспертных исследованиях и позволяет использовать информацию о техническом состоянии ТС, состоянии дорог, психофизиологических характеристик участников ДТП [2]. Одной из самых популярных программ является Компьютерная программа «PC Crash» – одна из самых функциональных на сегодняшний день компьютерных программ для анализа и моделирования механизма ДТП. Она позволяет анализировать,

моделировать и исследовать обстоятельства ДТП, установить реальные скорости ТС в каждый момент движения (включая и момент контакта), а также, произвести разбор сложной дорожной ситуации, восстановить картину деформации ТС, оценить вероятность нанесения телесных повреждений людям, оказавшимся вовлеченными в данную ситуацию (водителям ТС, их пассажирам, а также пешеходам).

Также следует отметить программу Carat-3, с помощью которой также можно выполнять расчёты и реконструкцию ДТП. В структуре программы существует интегрированная чертёжная программа. Все чертежи, составленные с её помощью, могут быть сохранены и при необходимости использованы для внесения корректировок. Существует возможность сканирования рисунков и эскизов, с последующей их загрузкой как в графические файлы или для дальнейшей обработки. Вычисления могут производиться как в динамическом (силы, действующие на автомобиль), так и в кинематическом (только движение) плане. Столкновения любых ТС и объектов могут моделироваться неограниченное количество раз. Результаты могут быть представлены как в двухмерном, так и в трёхмерном изображении, а в случае необходимости могут быть прозрачны, что позволяет подробно рассмотреть все детали сформированной модели. При всех отмеченных достоинствах вышеуказанных программ в практической деятельности экспертных подразделений они применяются редко по следующим причинам: высокая стоимость официальной версии программного продукта; перегруженный интерфейс программы, что затрудняет её применение лицами, не имеющие базового автотехнического образования; требуется специальное обучение пользователя программ.

Применение компьютерного моделирования обосновано при проведении пожарно-технической экспертизы – возможно виртуально реконструировать предметы, относительно которых произошло происшествие, можно воссоздать картину места пожара (определить зону термических повреждений, зону задымления, площадь зоны максимальных термических повреждений).

Преимущества использования 3D моделирования – наглядность. Ввиду того, что одной из целей современного государства является обеспечение национальной безопасности, судебно-экспертная деятельность должна внедрять, использовать и разрабатывать новейшие наукоемкие технологии для оказания содействия органам, ведущим уголовный, гражданский и административный процессы. Высокотехнологичное развитие экспертных организаций помогает предоставлять наиболее полное и подробное заключение эксперта, а впоследствии сократить и предотвратить ряд преступлений.

Список литературы

1. Новикова, Т.Б. Метод 3D-моделирования в современной судебно-экспертной / Т.Б. Новикова // Международный журнал гуманитарных и естественных наук. 2020. С.32-35.

2. Беляев, М.В. К вопросу о современных способах моделирования дорожно-транспортных происшествий / М.В. Беляев, М.А. Четвергов // Вестник Московского университета МВД России. 2018. № 4. С. 11-15.

3. Шаров, В.И. Формализация в криминалистике: Вопросы теории и методологии криминалистического исследования: дисс. докт. юрид. наук / В.И. Шаров. Нижний Новгород, 2003. 411 с.

УДК 343.1

АСПЕКТЫ УЧАСТИЯ СПЕЦИАЛИСТА ПРИ ПОЛУЧЕНИИ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Орешков Иван Андреевич,
аспирант
Балтийский федеральный университет имени И. Канта,
г. Калининград, Россия
e-mail: vsmile777@mail.ru
Научный руководитель: Волчецкая Татьяна Станиславовна,
доктор юридических наук, профессор
Заслуженный работник высшей школы РФ,
Балтийский федеральный университет имени И. Канта,
г. Калининград, Россия
e-mail: larty777@gmail.com

Аннотация: *в статье рассмотрены отдельные проблемы, связанные с целесообразностью привлечения специалиста к участию в следственных действиях, в ходе которых производится изъятие электронных носителей или осуществляется копирование с них информации. Проанализированы дискуссионные проблемы по проблемам участия специалиста на предварительном следствии, предложены пути их решения в целях обеспечения прав участников уголовного судопроизводства.*

Ключевые слова: *электронные носители информации, изъятие электронных носителей информации; копирование информации с электронных носителей информации; участие специалиста.*

ASPECTS OF THE SPECIALIST'S PARTICIPATION IN OBTAINING ELECTRONIC EVIDENCE IN THE INVESTIGATION OF CRIMES

Oreshkov Ivan Andreevich,
postgraduate student
the I. Kant BFU
Kaliningrad, Russia
e-mail: vsmile777@mail.ru
Scientific supervisor: ***Volchetskaya Tatiana Stanislavovna,***
doctor of law, professor
Honored worker of the higher school of the Russian Federation,

the I. Kant BFU
Kaliningrad, Russia
e-mail: larty777@gmail.com

Abstract: *the article considers some problems related to the expediency of attracting a specialist to participate in investigative actions during which electronic media is seized or information is copied from them. The discussion problems on the problems of the participation of a specialist in the preliminary investigation are analyzed, the ways of their solution are proposed. In order to ensure the rights of participants in criminal proceedings.*

Keywords: *electronic media, withdrawal of electronic media; copying of information from electronic media; participation of a specialist.*

В последнее время, практически во всех сферах человеческой деятельности стремительно развиваются цифровые технологии, которые стали также активно использоваться преступниками для совершения преступлений, при этом не только преступлений в сфере компьютерной информации, но и иных преступлений, посягающих на иные объекты, в том числе личность, собственность, безопасность общества и государства [1, с. 17-22].

Рассматривая проблему развития способов получения электронных доказательств при расследовании уголовных дел, немало важным вопросом остается модернизирование и развитие уголовно-процессуального законодательства, способного отвечать реалиям современного состояния развития информационно-телекоммуникационных технологий. В частности, уголовно-процессуальное законодательство должно обеспечивать баланс между соблюдением прав участников уголовного процесса, публичными интересами и соответствовать реалиям настоящего времени, тем самым не создавая излишних препятствий для осуществления своих прав участников уголовного процесса.

Анализируя вопросы получения электронных доказательств с электронных носителей информации, нельзя упустить из внимания сложившуюся в настоящее время на наш взгляд актуальную проблему, связанную с привлечением специалиста к проведению следственных действий, связанных с изъятием электронных носителей информации. Как известно, в 2018 году в УПК РФ введена ст. 164.1 УПК РФ «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий», устанавливающая порядок производства следственных действий, связанных с изъятием электронных носителей или копирование с них информации [2].

Анализируя генезис и необходимость появления в УПК РФ указанной нормы права, можно сделать вывод о том, что одной из целей ее введения послужило создание дополнительных гарантий защиты предпринимателей от необоснованного уголовного преследования, в частности, недопущения мер, способных привести к приостановлению законной деятельности юридических

лиц или индивидуальных предпринимателей при изъятии электронных носителей информации.

Так, в соответствии с ч. 2 ст. 164.1 УПК РФ «электронные носители информации изымаются в ходе производства следственных действий с участием специалиста. По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в следственном действии, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование последней. Копирование информации осуществляется на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации».

Спорным вопросом в данном контексте является категоричное требование законодателя относительно обязательного привлечения специалиста к участию в следственных действиях, в ходе которых осуществляется изъятие электронных носителей информации.

Законодательное определение электронного носителя информации в настоящее время отсутствует. Опираясь на определение электронного носителя информации, закрепленного в п. 3.1.9 ГОСТ 2.051-2013. «Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения», следует, что «электронным носителем информации является такой материальный носитель, который используется для записи, хранения и воспроизведения электронной информации, обработка которой происходит с помощью средств электронно-вычислительной техники».

Указанное определение является довольно широким. При буквальном толковании указанного определения, можно сделать вывод о том, что оно охватывает собой практически любой материальный носитель информации, на который возможно записать информацию, хранить ее на указанном материальном носителе и воспроизводить ее. Таким образом, понятием электронный носитель информации охватывается любой материальный носитель, на котором записана электронная информация, размер которой может быть различным, начиная от размера оптического диска и usb-носителя и заканчивая серверами крупных организаций. Анализируя вышеуказанное определение электронного носителя информации, можно сделать вывод, что под электронным носителем информации понимается довольно большой круг материальных носителей, в том числе используемых в настоящее время повсеместно и ежедневно обычными пользователями. С указанными «простыми» носителями информации каждый пользователь сталкивается ежедневно, записывая файлы на usb-носители, сохраняя их в памяти мобильных телефонов, ноутбуков, персональных компьютеров и так далее.

В настоящее время, в связи с внедрением информационных технологий во все сферы деятельности, уровень пользования компьютерной техникой и комплекс общих знаний относительно процесса изъятия электронных носителей информации и копирования с них информации, имеющийся у подавляющего большинства пользователей, в группу которых входят и

сотрудники правоохранительных органов - следователи, дознаватели, оперативные сотрудники, на наш взгляд, соответствует достаточной квалификации для производства изъятия стандартных электронных носителей информации или копирования с них доказательственно-значимой информации. В данную группу могут входить оптические диски, usb-носители, персональные компьютеры, мобильные телефоны. Каждый пользователь, чья работа ежедневно связана с персональным компьютером, в силу опыта работы с ним, владеет вышеуказанными базовыми познаниями.

Современные информационные технологии в настоящее время просты и понятны в обращении, в связи с чем, в большинстве случаев проведение следственных действий, связанных с получением доказательственной информации с электронных носителей возможно осуществить и непосредственно их инициатором самостоятельно не прибегая к помощи специалистов, обладающих специальными знаниями.

Однако, закрепленный в уголовно-процессуальном законе порядок изъятия электронных носителей информации закрепляет обязательность участие специалиста в производстве указанных следственных действий, что на практике довольно часто усложняет процесс расследования без оправданной на то необходимости.

В то же время ученые–криминалисты довольно неоднозначно видят решение проблемы получения электронной доказательственной информации. Так, например, Е.Р. Россинская считает, что «участие специалиста должно быть обязательным в случаях, когда требуется произвести изъятие компьютерной информации непосредственно с электронного носителя информации (персонального компьютера, планшета, мобильного телефон и т.д.), либо в случаях, когда требуется изъятие информации, находящейся на удаленных серверах, а не на самом электронном носителе информации» [3, с. 35-36].

Вместе с тем, по мнению С.В. Зуева, «современные информационные технологии являются вполне простыми в обращении. Их использование в большинстве своем не требуют каких-либо специальных умений и знаний по их применению» [4, с. 35-36].

Аналогичное мнение высказывает в своих трудах С.Б. Россинский, говоря о том, что обладая «базовыми специальными знаниями и умениями обращения с цифровой техникой, следователь при обращении с ней вполне может обойтись без помощи специалиста» [5, с. 118].

Отталкиваясь от позиции С.Б. Россинского, считаем, что привлечение к участию в следственных действиях, связанных с изъятием или копированием информации с электронных носителей специалиста, должно определяться следователем по собственной инициативе в порядке, предусмотренном ст. 168 УПК РФ. Законодательное закрепление обязательности привлечения специалиста к участию во всех следственных действиях, в ходе которых производится изъятие электронных носителей или копирование с них информации, безусловно, является излишним и не соответствующим фактической необходимости его привлечения. Кроме того, на наш взгляд, законодательное закрепление участия специалиста к участию в определенных

следственных действиях, в ходе которых, к примеру, производится изъятие информации с удаленных серверов или изъятие информации с электронных носителей информации, специальных знаний об изъятии информации с которых у следователя недостаточно, также является излишним. В случае изъятия или копирования информации с электронных носителей информации, специальных знаний об изъятии информации с которых у следователя недостаточно, он в любом случае прибегнет к помощи специалиста и привлечет его к участию в следственных действиях.

Вместе с тем, исключение требования об обязательности привлечения специалиста, послужит шагом к преодолению излишней забюрократизированности требований уголовно-процессуального законодательства, в частности, при наличии которых специалисты, в качестве которых в основном привлекаются сотрудники – эксперты подразделений ЭКЦ МВД России при их небольшой как штатной так и фактической численности, привлекаются к участию в следственных действиях, где фактически знаний по пользованию ПК, имеющихся у следователя, дознавателя или оперативного сотрудника, вполне достаточно, и применения каких-либо специальных знаний в этой области не требуется. В таких случаях, привлечение вышеуказанных сотрудников на участие в следственных действиях, где фактически применение специальных знаний не требуется в ущерб их основным обязанностям по производству компьютерно-технических экспертиз, не отвечает требованиям о разумном сроке уголовного судопроизводства, предусмотренном ст. 6.1 УПК РФ, поскольку «обстоятельства, связанные с организацией работы органов дознания, следствия, прокуратуры и суда не могут приниматься во внимание в качестве оснований для превышения разумных сроков осуществления уголовного судопроизводства».

Кроме того, в случае несогласия участвующих в следственном деле лиц с уровнем компетенции следователя, дознавателя или оперативного сотрудника, осуществляющих изъятие или копирование информации с электронных носителей информации, уголовно-процессуальным законом, в ст. 57 УПК РФ, в качестве гарантий прав стороны защиты, закреплено положение, согласно которому «стороне защиты не может быть отказано в удовлетворении ходатайства о привлечении к участию в производстве по уголовному делу специалиста для разъяснения вопросов, входящих в его профессиональную компетенцию».

Таким образом, мы полагаем, что целесообразно в законе исключить факт обязательности привлечения к следственным действиям, связанным с изъятием электронных носителей информации либо копированием с них электронной доказательственной информации участия специалиста, а установить возможность его привлечения по инициативе следователя или лица, осуществляющего дознание.

Список литературы

1. Волчецкая, Т.С. Современная криминалистическая наука: реалии и перспективы развития / Т.С. Волчецкая // Казанские уголовно-процессуальные

и криминалистические чтения. Материалы Международной научно-практической конференции. Редколлегия: Ю.Н. Кулешов (отв. ред.) [и др.]. Казань, 2022. С.17-22.

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ (ред. от 29.12.2022) (с изм. и доп., вступ. в силу с 11.01.2023 г.) // URL: https://www.consultant.ru/document/cons_doc_LAW_34481/?ysclid=ldyuj0j2k4478711924/ (дата обращения 10.02.2023).

3. Россинская, Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности. Монография / Е.Р. Россинская. М., 2022. С.111.

4. Зуев, С.В. Развитие информационных технологий в уголовном судопроизводстве: монография / С.В. Зуев. М.: Юрлитинформ, 2018. 248 с.

5. Россинский, С.Б. Следственные действия: монография / С.Б. Россинский. М.: Норма, 2018. № 6. С.118.

УДК 343.1

ПРИМЕНЕНИЕ ПРОКУРОРОМ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ПРИ УЧАСТИИ В СУДЕБНОМ СЛЕДСТВИИ

Пелисова Ирина Павловна,
аспирант
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: irina_pelisova@mail.ru

Научный руководитель: Бертовский Лев Владимирович,
доктор юридических наук, профессор кафедры уголовного процесса, криминалистики и основ судебной экспертизы
Московский государственный университет имени М.В. Ломоносова
г. Москва, Россия
e-mail: bgl1980@yandex.ru

Аннотация: *в статье рассмотрен вопрос применения прокурором современных технологий при рассмотрении уголовного дела, в том числе с участием присяжных заседателей. В век высоких технологий судебное следствие не должно отставать от времени. Отмечено, что внедрение в уголовное судопроизводство таких современных технологий, как виртуальной реальности, позволит решить ряд проблем, связанных с процессом доказывания.*

Ключевые слова: *современные технологии, цифровизация, виртуальная реальность, уголовное судопроизводство, судебное следствие, государственный обвинитель, присяжные заседатели.*

APPLICATION OF MODERN TECHNOLOGIES WITH THE PARTICIPATION OF THE PROSECUTOR IN THE JUDICIAL INVESTIGATION

Pelisova Irina Pavlovna,
postgraduate student
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: irina_pelisova@mail.ru

Scientific adviser: ***Bertovsky Lev Vladimirovich***
doctor of law, professor
Lomonosov Moscow state university,
Moscow, Russia
e-mail: bgl1980@yandex.ru

Abstract: *the article deals with the issue of using modern technologies in the consideration of a criminal case, including with the participation of jurors. In the age of high technology, the judicial investigation should not lag behind the times. It is noted that the introduction of such modern technologies in criminal proceedings as virtual reality will solve a number of problems associated with the process of proof.*

Keywords: *modern technologies, digitalization, virtual reality, criminal proceedings, judicial investigation, public prosecutor, jurors.*

Современном мире внедрение технологий обмена информацией развивается быстрыми темпами, что значительно опережает развитие законодательства. Поэтому возникает вопрос о внедрении этих технологий с целью усиления его превентивных функций.

Современные шаги по активному внедрению инновационных технологий в сферу судопроизводства Российской Федерации носят целенаправленный характер, следующий из государственных целевых установок на повышение качества осуществления правосудия, эффективности рассмотрения судебных дел, обеспечение доступности и открытости правосудия. Об этом свидетельствует последовательно проводимая государством стратегия развития и совершенствования судебной системы России, отраженная в федеральных целевых программах [1], которые ориентированы на разрешение проблем, связанных с недостаточно высоким качеством правосудия, выражающимся в несоблюдении сроков судопроизводства, недостаточном уровне информированности населения о судебной деятельности, неудовлетворительной работе судов и др. В качестве одного из важных средств разрешения названных проблем на государственном уровне предлагается скорейшее внедрение в организацию функционирования судебной системы современных цифровых технологий. Как можно видеть, по отношению к цели – повышению качества правосудия – цифровые технологии выступают одним из прогрессивных средств ее достижения.

Экспоненциальное развитие науки и техники, изменение социальных укладов и другие глобальные изменения, которые произошли за последнее время, потребовали значительной модернизации и права. Мы вступили в эпоху высокотехнологичного права под которым понимается такой логистичный, наукоемкий и технологичный регулятор общественных отношений, который, с одной стороны, использует высокие технологии в процессе правоприменения, а с другой — регламентирует возникающие с ними отношения [2].

Соглашаясь с Бородиновой Т.Г., полагаем, что цифровые технологии, используемые в уголовном судопроизводстве в качестве процессуальных средств, должны отвечать следующим основным критериям: 1) быть направленными на обеспечение назначения уголовного судопроизводства и конкретных прав и правовых интересов участников уголовного судопроизводства; 2) содержать завершенные правовые регуляторы, обладающие высокой степенью детализации в уголовно-процессуальном праве; 3) иметь техническую способность реализоваться в определенной уголовно-процессуальным законом форме; 4) носить альтернативный характер, не исключающий возможности использования в необходимых случаях традиционных процессуальных средств [3].

Особое значение для применения (внедрения) цифровых технологий имеет рассмотрение уголовных дел с участием коллегии присяжных заседателей. Так, с 1 июня 2018 г. вступил в силу инициированный Президентом России закон о поправках в Уголовный кодекс Российской Федерации (далее - УК РФ). Он включил три основных нововведения — возможность рассмотрения уголовных дел с участием присяжных заседателей в районных и гарнизонных военных судах, в том числе в отношении женщин, а также мужчин старше 65 лет (ранее они не имели права на суд присяжных, поскольку к ним не может быть применен самый суровый вид наказания — пожизненное лишение свободы), а также увеличено число статей в УК РФ, дела по которым могут рассматривать присяжные заседатели.

Закрепленный в ст. 17 Уголовно-процессуального кодекса Российской Федерации (далее - УПК РФ) принцип свободы оценки доказательств включает положение о том, что судья, присяжные заседатели в ходе судебного разбирательства уголовного дела должны оценивать предлагаемую совокупность доказательств по их внутреннему убеждению, основывающемуся не только на законе, но и на совести [4]. Под совестью в науке уголовного процесса предлагается понимать индивидуальную «способность судьи к самоконтролю в рамках уголовно-процессуального закона и к справедливости в праве» [5]. И совесть, и внутреннее убеждение, и справедливость – сугубо субъективные категории, верно применить которые к «нешаблонным» обстоятельствам конкретного уголовного дела способен только человек.

Результат рассмотрения и разрешения судом уголовного дела во многом зависит от тактики представления доказательств прокурором — государственным обвинителем, а также от результатов их исследования в судебном следствии. Особое значение это имеет для уголовных дел с участием коллегии присяжных заседателей.

В.Н. Исаенко обоснованно констатирует: «Если в результате изложения государственным обвинителем предъявленного подсудимому обвинения у присяжных заседателей может сформироваться изначально вероятностное суждение о преступлении и виновном в его совершении лице, то в процессе судебного следствия в результате реализации избранной им тактики представления и исследования доказательств государственный обвинитель должен обеспечить трансформацию вероятного знания в убеждение об обоснованности позиции обвинения» [6, 20].

Согласно ч.ч. 1 и 2 ст. 274 УПК РФ очередность исследования доказательств определяется стороной, представляющей доказательства суду [7]. При этом первой представляет доказательства сторона обвинения, а после их исследования переходят к доказательствам, представленным стороной защиты. Предоставление законодателем каждой стороне права самостоятельно определять очередность (последовательность) представления доказательств непосредственно указывает на возможность выбора каждой из них тактики представления доказательств по своему усмотрению. По нашему мнению, это является важной гарантией реального обеспечения закрепленного в ст. 123 Конституции РФ принципа состязательности и равноправия сторон при осуществлении судопроизводства. Согласно ч. 3 ст. 15 УПК РФ суд не является органом уголовного преследования, не выступает на стороне обвинения или защиты, а создает необходимые условия для исполнения сторонами их процессуальных обязанностей и осуществления предоставленных им прав. Это положение, по нашему мнению, дополнительно гарантирует сторонам возможность самостоятельно определять тактику своих действий в суде, которую не вправе корректировать другая сторона, а также не вправе корректировать суд.

Суд присяжных, являясь в своей основе непрофессиональным судом в части определения виновности (невиновности) подсудимого, выступает профессиональным судом в части назначения наказания. Каждому из присяжных необходимо использовать исключительно свое суждение, чтобы решить, виновен подсудимый или нет. Они заслушивают доказательства, представленные как обвинением, так и защитой. Присяжные должны принимать решения исключительно по фактам [8].

На сегодняшний день одна из основных проблем в том, что на присяжных заседателей может легко произвести впечатление адвокат (сторона защиты) для того, чтобы повлиять на исход решения по уголовному делу. Как мы понимаем, главная цель у адвоката - освободить своего доверителя от уголовной ответственности и наказания. Дело в том, что присяжные заседатели не обладают юридическими познаниями и, как правило, руководствуются эмоциями, что на пользу стороне защиты.

От того, как государственным обвинителем будут представлены присяжным заседателям доказательства виновности лица в совершении конкретного преступления, их доступность для понимания обычному гражданину, не обладающему юридическими познаниями, будет зависть результат рассмотрения уголовного дела.

На наш взгляд, для решения вышеуказанной проблемы, в том числе в целях минимизации введения в заблуждение адвокатами присяжных заседателей относительно существа рассматриваемого дела, в уголовное судопроизводство необходимо внедрить возможность проведения судебного следствия с помощью виртуальной реальности. С помощью виртуальной иллюстрации места, времени и способа совершения преступления, государственный обвинитель без юридической терминологии сможет доступно и понятно продемонстрировать присяжным заседателям, не обладающим правовыми познаниями, существо предъявленного обвинения. Так, государственный обвинитель наглядно сможет показать присяжным, как, например, обвиняемый наносил удары убитому, либо где в момент преступления находились дети, которые остались в результате совершенного преступления сиротами, либо где располагались орудия преступления.

Очевидно, что на указанные цели потребуются много как финансовых, так и временных затрат, однако в век цифровых технологий уголовное судопроизводство не должно отставать от времени, должно отвечать современным реалиям, учитывая при этом существующие проблемы в сфере правового регулирования технологий и самого высокотехнологичного права, на что обращает внимание профессор Л.В. Бертовский [9, 10], – это является на сегодняшний день жизненной необходимостью.

Список литературы

1. Постановление Правительства Российской Федерации от 20 ноября 2001 г. № 805 «О федеральной целевой программе «Развитие судебной системы России» на 2002–2006 годы»; Постановление Правительства Российской Федерации от 21 сентября 2006 г. № 583 «Развитие судебной системы России на 2007– 2012 годы»; Постановление Правительства Российской Федерации от 27 декабря 2012 г. № 1406 (ред. от 14 сентября 2021 г.) «О федеральной целевой программе «Развитие судебной системы России на 2013–2024 годы» // СПС «КонсультантПлюс» (дата обращения: 09.01.2023).

2. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский // Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. № 4. С.735—749.

3. Бородинова, Т.Г. Цифровые технологии в уголовном судопроизводстве России: пределы и проблемы внедрения / Т.Г. Бородинова. - Краснодар, 2022.- С. 82.

4. Федеральный закон от 18.12.2001 № 174-ФЗ «Уголовно-процессуальный кодекс Российской Федерации» // Собрание законодательства Российской Федерации. 2001. № 52 (ч. I). Ст. 4921.

5. Якушева, Т.В. Совесть судьи при оценке доказательств для постановления приговора как конституционная гарантия государственной защиты прав подсудимого / Т.В. Якушева, М.А. Стародубцева // Концепт. 2019. № 1. С.144–149.

6. Исаенко, В.Н. Тактико-психологические аспекты представления прокурором доказательств в суде с участием присяжных заседателей / В.Н.

Исаенко // Криминалистъ. 2018. № 2(23). С. 20.

7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ // СПС «КонсультантПлюс» (дата обращения: 09.01.2023).

8. Trial by Jury: Pros and Cons // URL: https://worldessays.com/blog/trial-by-jury-pros-and-cons.html. (дата обращения: 09.01.2023).

9. Бертовский, Л. В. Проблемы развития высокотехнологичного права / Л. В. Бертовский // Применение в юриспруденции современных технологий: актуальные вопросы теории и практики: мат-лы междунар. научно-практич. конф, Красноярск, 21 мая 2021 года. Красноярск: Красноярский государственный аграрный университет, 2021. С. 6-11.

10. Бертовский, Л. В. Проблемы развития высокотехнологичного права / Л. В. Бертовский // Высокотехнологичное право: генезис и перспективы : Материалы III Международной межвузовской научно-практической конференции, Москва-Красноярск, 24–25 февраля 2022 г. Красноярск: Красноярский государственный аграрный университет, 2022. С. 26-29.

УДК 343.9

КРИМИНАЛИСТИЧЕСКИЕ ПРОБЛЕМЫ ДОКАЗЫВАНИЯ ФАЛЬСИФИКАЦИИ СВЕДЕНИЙ В КОНТЕКСТЕ «ИННОВАЦИОННЫХ» ЦИФРОВЫХ ТЕХНОЛОГИЙ

Полстовалов Олег Владимирович,
доктор юридических наук, доцент
АНО «Экспертно-координационный центр комиссий Государственного Совета Российской Федерации»,
г. Москва, Россия
e-mail: polstovalov74@mail.ru

Аннотация: *в статье рассматриваются проблемы применения отдельных цифровых технологий не только как сферы трансформации подлежащих исследованию в процессе доказывания обстоятельств события преступления и виновности в его совершении конкретных лиц, но и как средства оптимизации высокотехнологичной преступной деятельности, фальсификации имеющих отношение к делу сведений. Автор останавливается на рассмотрении вопросов отдельных негативных сценариев появления новых и совершенствования имеющихся способов преступных посягательств, сокрытия их следов, внешнеполитических провокаций и развития средств обеспечения недобросовестной конкуренции и прочих подобных вызовов на основе новейших цифровых технологий фальсификации и выработки средств противодействия этому на уровне криминалистического обеспечения.*

Ключевые слова: *цифровые технологии, криминалистическое обеспечение, фальсификация сведений, технологии преобразования звука.*

CRIMINALISTIC PROBLEMS OF EVIDENCE IN THE CONTEXT OF «INNOVATIVE» DIGITAL FALSIFICATION TECHNOLOGIES

Polstovalov Oleg Vladimirovich,
doctor of law, associate professor
ANO «Expert Coordinating Center of Commissions of the State council of the Russian Federation», Moscow, Russia
e-mail: polstovalov74@mail.ru

Abstract: *the article deals with the problems of using individual digital technologies not only as areas of transformation to be investigated in the process of proving the circumstances of a crime event and the guilt of specific persons in its commission, but also as a means of optimizing high-tech criminal activity, falsifying relevant information. The author dwells on the issues of certain negative scenarios for the emergence of new and improvement of existing methods of criminal attacks, hiding their traces, foreign policy provocations and the development of means to ensure unfair competition and other similar challenges based on the latest digital falsification technologies and the development of means to counter this at the level of forensic support.*

Keywords: *digital technologies, forensic support, falsification of information, sound conversion technologies.*

Оптимизация процессов собирания, проверки и оценки доказательств в современных условиях цифровизации практически всех сторон жизни общества не всегда идет в ногу со все более широко открывающимися высокотехнологичными возможностями, ряд из которых уже давно и успешно используются в зарубежных странах. Аэрофотосъемка, снимки из космоса, видеозапись с летательных аппаратов, использование специального оборудования сканирующего типа на них, удаленные методы работы с информацией посредством интернет-ресурсов и сведение больших данных к весьма достоверному анализу процессов, событий и фактов на основе искусственного интеллекта уже не кажутся фантастикой в приложении к процессам доказывания в разных сферах правоприменения. Между тем, актуальность уголовно преследования лиц, совершающих преступления из-за рубежа против интересов нашего государства и граждан, в последние годы становится все более очевидной. Нарастает и внутренняя угроза новых форм преступлений на высокотехнологичной основе.

Н.П. Яблоков писал о том, что главной и основной задачей криминалистики с момента ее возникновения является «своими научно разработанными средствами, приемами и методами, с привлечением средств и методов естественных, технических и иных гуманитарных наук, сделать наиболее оптимальной деятельность органов дознания, предварительного следствия и суда в деле раскрытия преступления и установления истины в процессе осуществления доказывания». Обязательным условием принятия

правомерного решения по делу Н.П. Яблоков называл установление истины [1, с. 17]. Ни редактора цитируемого учебника И.А. Александрова, ни одного из самых выдающихся отечественных криминалистов Н.П. Яблокова к великому сожалению уже нет в живых, но проблема совершенствования доказывания в контексте вступления России в постиндустриальное информационное пространство развития на основе высоких технологий в области отображения данных о преступлении и его совершившем лице становится все более значимой.

Цифровые технологии позволяют работать с большим объемом информации на удалении, порой в скрытой для многих форме и с получением весьма репрезентативной картины происходящего или уже случившегося события. В частности, аэрокосмические снимки давно уже стали средством собирания сведений в рамках разведывательной деятельности в ходе вооруженных конфликтов, используемые программные комплексы на беспилотных летательных аппаратах применяются при землеустроительных работах, в рамках развития проекта цифровой археологии, а также при выявлении последствий крупных экологических правонарушений, связанных с загрязнением природных объектов в результате хозяйственной деятельности.

Много споров и инсинуаций вызвала ситуация со сбитым в небе над Украиной пассажирским самолетом Boeing-777 компании Malaysia Airlines, летевшим рейсом MH17 из Амстердама (Нидерланды) в Куала-Лумпур (Малайзия). Достоверно известно по-прежнему только то, что самолет потерпел крушение 17 июля 2014 года на востоке Украины, в результате чего погибли все 298 находившихся на борту человек, граждан десяти стран, большая часть которых (193 человека) были подданными Нидерландов, 43 –Малайзии, 27 – гражданами Австралии. Совместная следственная группа (Joint Investigation Team, JIT), расследовавшая и обеспечивающая техническое и юридическое сопровождение процесса, в своих отчетах опиралась в том числе на доказательства с цифровых носителей, ряд из которых как по происхождению, так и по форме носили сомнительный характер (снимки из отрытых интернет-источников, анимированная фальсификация ролика с перемещением ракетной установки). Одновременно громкие заявления о наличии представленных американской стороной снимков из космоса о неопровержимости версии о запуске ракеты с контролируемой ополченцами Донбасса территории так и не стали достоянием общественности. Представляемые же российской стороной доказательства были проигнорированы. На предмет достоверности и отсутствия признаков фальсификации цифровых материалов, используемых в качестве доказательств по делу, ни судья, ни следственная группа не посчитали нужным сделать хоть сколько-нибудь вразумительные и обоснованные заявления. Вместе с тем, в современных условиях цифровизации не менее остро стоит вопрос расширения возможностей фальсификации доказательств, в том числе из конъюнктурных геополитических соображений. Анимированный ролик из одной картинки о географии перемещения ЗРК «Бук» был без труда разоблачен российскими специалистами с высокой степенью очевидности, но и это было практически проигнорировано. А вот якобы имевшие место

«неопровержимые свидетельства» из перехваченных переговоров «террористов» прозвучали в общественном пространстве разве что в качестве триггера. В этой связи попытки накачать общественное мнение «высокодостоверными» средствами объективного контроля и цифровыми свидетельствами порой не получали должного подтверждения, но шли опережающими темпами и давали высокорезонансный конъюнктурный эффект.

Не меньшего внимания заслуживает такая категория цифровых фальсификаций, как deepfake, а также технологии преобразования текста в звук, которые все чаще становится средством совершения преступлений. Подчёркивая необходимость криминализации распространения дипфейков, как это было сделано в ряде стран, и констатируя отсутствие большого резонанса от такого рода расширения криминальных возможностей, специалисты отмечают: «Оценивая негативные проявления процесса цифровизации общества, следует выделить технологию, манипулируемую искусственным интеллектом, которая осуществляет синтез лица и голоса – Deepfake (дипфейк). Фактически указанная методика позволяет генерировать и распространять недостоверную информацию» [2, с. 184]. К примеру, так называемый «фотошоп» для голоса работает с цифровым потоком записи человеческой речи и на основе технологии искусственного интеллекта «обучается этому голосу» с последующим воспроизведением текстового материала цифровым аналогом голоса-оригинала. Программа Adobe VoCo в качестве инструмента для работы с голосом справляется с задачей на основе записи в нескольких минут исходного голоса. Устная речь с помощью микрофона в открытом приложении VoCo сканируется и после непродолжительного «обучения» может быть воспроизведена с полной и точной имитацией требуемого голоса. Хорошо, если эти технологии используются для безобидных розыгрышей. Однако возможности фальсификации доказательств и использования этих современных технологий для совершения преступлений нельзя отрицать. Тем более, что по миру наметилась такая тенденция. В купе с полученными незаконным путем персональными данными граждан мошеннический бизнес по обзвону доверчивых лиц, как правило зрелого и преклонного возраста, на основе генерации голосов близких родственников не за горами. Л.В.Бертовский справедливо пишет: «Для плавного и безопасного перехода общества и государства на «цифровые рельсы» потребуется безопасное хранение персональных данных. Ежегодно фиксируется рост количества преступлений, связанных с использованием в незаконных целях информации о гражданах» [3, с. 744].

Цифровые голосовые подделки уже активно используются в конкурентной борьбе в корпоративной практике для дискредитации отдельных сотрудников, якобы не придерживающихся норм этики и позволяющих себе разглашение служебной тайны, оскорбительные высказывания в адрес начальства. Порой такие фальсифицированные материалы позволяют создать гандикап для конкурентов, высокотехнологично устраняющих наиболее

грамотных и профессиональных менеджеров их дискредитацией в глазах руководства компании.

Изготовление цифрового аналога в режиме реального времени или с последующей обработкой файла, высокотехнологичная «склейка» или «монтаж» оригинальной записи и прочие способы фальсификации в принципе распознаются и для этого есть необходимые средства. А.К.Лебедева отмечает, что измененный голос на фонограмме «можно исследовать путем анализа служебной информации аудиофайлов, в рамках которого проводится изучение бинарной структуры аудиофайла, его метаданных и иных служебных свойств. Подобный анализ проводится с помощью таких программ, как «DUMP», «Exiftool», «WinHEX» или 16-ричных редакторов, типа «Tiny Hexer» [4, с. 326].

Современные условия гипердинамичного развития IT-отрасли и программных продуктов с нею напрямую связанных во многом диктует складывающийся рынок, уровень научно-технологического развития отдельных регионов и России в целом. Однако все благоприобретения от такого прогресса одновременно предопределяют риски появления новых и совершенствования имеющихся приемов и способов преступных посягательств, сокрытия их следов, внешнеполитических провокаций и развития средств обеспечения недобросовестной конкуренции и прочих подобных вызовов. В этой связи чрезвычайно актуальным представляется расширение формата криминалистического сопровождения профилактической деятельности, работы на предупреждение неблагоприятных сценариев использования того или иного программного обеспечения и сервисов в деструктивных целях. Одновременно несмотря на то, что имеются отдельные достаточно серьезные исследования в области работы с цифровыми носителя звуко- и видео- информации на предмет поиска следов вносимых изменений (изготовления аналогов) с помощью соответствующего программного обеспечения не существует апробированной и утвержденной конкретной экспертной методики, что трудно признать оправданным. Здесь мы не только отстаем, а скорее безнадежно утратили ориентиры на все чаще складывающуюся практику работы на уровне компьютерно-технической экспертизы с цифровой феноменологией и одновременно с акцентом на звуковую, лингвистическую составляющие устной речи человека со всеми соответствующими идентификационными полями.

Список литературы

1. Криминалистика: учебник для вузов / И.В. Александров [и др.] ; под редакцией И.В. Александрова. 2-е изд., испр. и доп. Москва: Издательство Юрайт, 2023.376 с.

2. Грешнова, Т.А. Обеспечение общественного интереса в условиях цифровизации: проблемы уголовного законодательства в России (на примере технологии дипфейк (deepfake)) / Т.А. Грешнова, В.Н. Ситник // Вестник Саратовской государственной юридической академии.2022.№ 5 (148).С.183–189.

3. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский // Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. № 4. С.735–749.

4. Лебедева, А.К. Особенности судебно-экспертного исследования голоса, изменённого при помощи компьютерно-технических средств / А.К. Лебедева // Известия Тульского государственного университета. Экономические и юридические науки. 2016.№ 2-3. С.323 – 328.

УДК 336.7

ЭЛЕКТРОННЫЕ СРЕДСТВА ПЛАТЕЖА В РОССИИ И ВЕЛИКОБРИТАНИИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕРМИНОЛОГИИ

Полякова Светлана Александровна,
начальник отдела нормативно-правового обеспечения
Национальный исследовательский университет «МИЭТ»,
г. Москва, Россия
e-mail: sa_pol@mail.ru

Аннотация: в *данной статье рассматриваются вопросы подходов к определению понятия «электронное средство платежа» и его характерные признаки в законодательстве Российской Федерации и законодательстве Великобритании. Изучаются основные нормативные акты, регламентирующие понятие и функции электронных средств платежа в указанных странах.*

Ключевые слова: *электронное средство платежа, терминология, платежные системы, Российская, Великобритания.*

ELECTRONIC MEANS OF PAYMENT IN RUSSIA AND THE UK: A COMPARATIVE ANALYSIS OF TERMINOLOGY

Polyakova Svetlana Alexandrovna,
head of the regulatory support department
National research university of electronic technology,
Moscow, Russia
e-mail: sa_pol@mail.ru

Abstract: *this article discusses the issues of approaches to the definition of the concept of "electronic means of payment" and its characteristic features in the legislation of the Russian Federation and the legislation of the United Kingdom. The main normative acts regulating the concept and functions of electronic means of payment in these countries are studied.*

Keywords: *electronic means of payment, terminology, payment systems, Russian, UK.*

Актуальность рассматриваемой автором темы подтверждается статистическими данными, представленными Центральным банком банка Российской Федерации. Так, за 9 месяцев 2022 года в России использовалось 219,9 млн единиц электронных средств платежа (ЭСП – далее). Количество операций через ЭСП за те же 9 месяцев 2022 года составило 2441,7 млн единиц (в денежном эквиваленте составило 2 119,16 млрд рублей), в 2021 года за тот же период было осуществлено 2348,8 млн операций на сумму 1882,76 млрд руб. В процентном соотношении объем операций за год вырос на 4% (больше на 92,9 млн единиц операций), а в денежном эквиваленте – на 13% (больше на 236,4 млрд руб.) [1]. Указанные данные Центрального банка Российской Федерации свидетельствуют о росте объемов осуществления операций посредством ЭСП, что обуславливает актуальность и нарастающую роль ЭСП в рамках национальной платежной системы.

Применение в России расчетов с применением контрольно-кассовой техники (ККТ), осуществляется в соответствии с требованиями Федерального закона от 22 мая 2003 г. № 54-ФЗ [2]. Расчеты осуществляются в форме приема и выдачи денежных средств в наличной и безналичной форме в качестве оплаты работ, товаров и услуг. Поэтому применение ЭСП (помимо платежной банковской карты) обязательно предусматривает использование ККТ при расчетах. Данный нормативный акт также прямо указывает обстоятельства, при которых продавец обязан использовать онлайн-ККТ (онлайн-кассу).

В российском законодательстве «электронное средство платежа» определяется в Федеральном законе от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» [3] как «средство, обеспечивающее клиенту возможность осуществлять операции по переводу денег безналичными способами с использованием информационных технологий и техники» [3].

Особенное распространение применение ЭСП обрело с возрастающей популярностью Интернет-торговли, где могут применяться абсолютно все доступные формы оплаты. В этом аспекте к ЭСП относятся платёжные карты банков и всевозможные платежные приложения, а также мобильные банковские онлайн-приложения, интернет-банки и т.д.

Осуществление оплаты посредством ЭСП считается безналичной формой оплаты покупки, которая производится с помощью современных возможностей информационных технологий.

Характерными чертами расчетов посредством ЭСП являются:

- совершение покупки в дистанционном формате взаимодействия (личный контакт продавца с покупателем отсутствует);
- для осуществления транзакции применяются современные технологии (технические устройства) и возможности сети «Интернет».

Так, наиболее популярным видом ЭСП является оплата банковской картой, осуществляемая следующими способами: оплата через POS-терминал напрямую продавцу; оплата на интернет-сайте; оплата товара (услуги) через агента (курьера, интернет-площадки).

Второй вид ЭСП в России – электронные денежные средства (Яндекс.Деньги, QIWI Кошелек, WebMoney и другие). В данном случае продавец также применяет ККТ нового образца.

Третий вид ЭСП – оплата через агента продавца (например, наложенным платежом через Почту России). В данном случае агент применяет ККТ, действуя от имени или за счет принципала.

Рассмотрев основные аспекты правового подхода к определению термина «электронное средство платежа», следует обратиться к законодательной позиции Великобритании в вопросе терминологии электронных средств платежа.

В качестве предисловия следует отметить, что в 1992 году Великобритания отказалась от обязательств по введению евро в национальную платежную систему. По Протоколу №15, Великобритания продолжает денежную политику в соответствии с национальными нормами, поэтому национальное регулирование денежных потоков породило образование собственной стерлинговой зоны.

Регулирование обращения электронных денежных средств (ЭДС – далее) осуществляется на основании таких нормативных актов, как Директива (ЕС) 2015/2366 [4], Директива 2009/110/ЕС [5], а также ряда других международных актов Европейского Союза.

П. 2 ст. 2 Директивы 2009/110/ЕС содержит определение электронных денег, под которыми понимают «хранящуюся на электронном, в том числе магнитном, носителе денежную стоимость, представляющую собой требование к эмитенту, эмитируемую при получении средств для проведения платежных трансакций, определенных в пункте 5 Статьи 4 Директивы 2007/64/ЕС, и принимаемую физическим или юридическим лицом, отличным от эмитента электронных денег» [5].

В содержалось определение понятия «платежный инструмент» (понимавшаяся, как «совокупность процедур между пользователем и оператором платежных услуг для инициирования платежного поручения»).

Национальное законодательство Великобритании имплементирует вышеуказанные нормы, и, соответственно, подход к определению ЭСП и электронных денег идентичен подходу к терминологии в нормах документов ЕС в этом вопросе. Кроме того, в Великобритании не существует единой нормативной базы, регулирующей оборот ЭДС, однако, существует регулирующий орган – Служба финансового надзора.

Директива 2009/110/ЕС в пункте 13 преамбулы указывает, что «виртуальные деньги являются денежными суррогатами и их нельзя использовать в качестве средства сбережения» [5].

Можно обобщить, что Европейская комиссия устанавливает, что ЭДС – 1) денежный суррогат, 2) денежная стоимость, 3) обязательство эмитента. В России цифровые валюты также считаются денежными суррогатами.

В Великобритании зарегистрированы и распространены следующие платежные системы, не требующие открытия банковского счета: NETELLER, Skrill, ecoPayz, Entropaay (Ixaris) и другие.

Таким образом, проведенный анализ терминологии в нормах двух государств показал, что российские нормы содержат четкое определение сущности термина ЭСП в своем национальном законодательстве, а нормы Великобритании имплементируют нормы документов Европейского Союза, ссылаясь на определение «электронных денег». Проведенный анализ позволяет говорить о большей степени проработанности данной отрасли национального правового регулирования в России, нежели в Соединенном Королевстве. Действующие в России нормы законодательства стали эффективной базой для развития цифровизации финансовой сферы и регулирования электронных платежей в целях недопущения противоправных деяний с денежными средствами.

Список литературы

1. Центральный Банк Российской Федерации. Официальный сайт // URL: https://www.cbr.ru.

2. Федеральный закон «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации» от 22.05.2003 № 54-ФЗ (ред. от 29.12.2022) // URL: http://www.consultant.ru/document/cons_doc_LAW_42359/.

3. Федеральный закон «О национальной платежной системе» от 27.06.2011 г. № 161-ФЗ (ред. от 28.12.2022 г.) // URL: http://www.consultant.ru/document/cons_doc_LAW_115625/.

4.Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment servic- es in the internal market, amending Directives 2002/65/ EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC // Of- ficial Journal of the European Union. L 337. 23.12.2015. P. 35–127.

5. Директива Совета Европейских Сообществ 2009/110/ЕС от 16 сентября 2009 г. об учреждении и деятельности организаций, эмитирующих электронные деньги, о пруденциальном надзоре за их деятельностью, а также об изменении Директив 2005/60/ЕС и 2006/48/ЕС и об отмене Директивы 2000/46/ЕС // URL: https://base.garant.ru/71312234/.

УДК 343.1

СОЦИАЛЬНЫЕ, ИНТЕЛЛЕКТУАЛЬНЫЕ И МАШИННЫЕ ТЕХНОЛОГИИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Пржиленский Владимир Игоревич,
доктор философских наук, профессор
Московский государственный юридический университет имени О.Е. Кутафина (МГЮА),
г. Москва, Россия
e-mail: viprzhilenskij@msal.ru

Аннотация*: в статье рассмотрен ряд аспектов технологизации уголовного судопроизводства в процессе его цифровизации. Отдельно рассматривается аспект взаимодействия человека и компьютера в пространстве правоприменительных практик. Встреча в данном пространстве социальных, интеллектуальных и машинных технологий создает ряд возможностей, но и порождает ряд трудностей, исследованию которых и посвящена представленная статья.*

Ключевые слова*: компьютер, социальные технологии. интеллектуальные технологии, уголовное судопроизводство.*

SOCIAL, INTELLIGENT AND MACHINE TECHNOLOGIES IN CRIMINAL JUDGEMENT

Przhilenskiy Vladimir Igorevich,
doctor of philosophy, professor
Kutafin Moscow state law university (MSAL),
Moscow, Russia
e-mail: viprzhilenskij@msal.ru

Abstract: *the article considers a number of aspects of the technologization of criminal proceedings in the process of its digitalization. The aspect of human-computer interaction in the space of law enforcement practices is considered separately. The meeting in this space of social, intellectual and machine technologies creates a number of opportunities, but also gives rise to a number of difficulties, the study of which is the subject of this article.*

Keywords: *computer, social technologies. intellectual technologies, criminal proceedings.*

Стремительно развивающиеся IT-технологии изменяют все сферы социальной жизни, активно вторгаясь в пространство межчеловеческих отношений, преобразуя все без исключения виды индивидуальной и коллективной деятельности [3]. В особом положении оказались юристы, чья профессия с самого начала была направлена на достижение строгого

соблюдения писанных правил, на основе точного их истолкования. Ничто не обеспечивает такой строгости и точности как применение новейших средств электронно-вычислительной техники, но ее внедрение в работу органов предварительного следствия и суда способно оказать неконтролируемое воздействие на алгоритмы судопроизводства, складывавшиеся веками. Эти алгоритмы предполагали, что их применение находится под непосредственным и повседневным контролем человека, способного вовремя вмешаться в их исполнение, заново все переделать или в ручном режиме устранить ошибки и недочеты. Вот почему вызывает беспокойство возможность нарушения баланса формы и содержания судебной деятельности, несоблюдения тщательно проработанного и теоретически обоснованного соответствия процедуры и смысла в правоприменительных практиках.

Технологии всегда были неотъемлемой частью человеческой жизни. Они усложнялись, развивались и совершенствовались по мере того, как усложнялась, развивалась и совершенствовалась сама деятельность человека как разумного существа. Для обслуживания и совершенствования технологий применялось все, чем располагал и на что мог влиять человек. Для этого в свое время были созданы теории, алгоритмы. Но только сегодня технологии осознаются в качестве таковых, их применение и создание носит системный и рефлексивный характер. К технологиям можно отнести все те знания, умения и навыки, которые используются для производства чего-либо. Отличие производства, основанного на технологии от обычного изготовления чего-либо в том, что первое носит серийный характер и его результаты схожи друг с другом. В этом случае знания, умения и навыки, составляющие технологию, могут быть аналитически отделены от процесса производства, устно описаны или даже записаны в виде инструкции, что позволяет тиражировать сам процесс производства.

Как отмечают современные исследователи, социальные технологии описывают интегральную совокупность видов человеческой деятельности, которые могут быть осмыслены через концептуальные пары «организованное – стихийное», «профессиональное – любительское» и «трудовое – досуговое». Активное применение результатов развития социальных наук в процессе управления обществом привело к появлению безличных алгоритмов операций и в области межиндивидуального или межгруппового взаимодействия. Как отмечает И.Т. Касавин, понятия социального проектирования, социального конструирования, управления, обучения, экспертизы, программирования сознания, социальной инициативы характеризуют наиболее известные формы социальных технологий. При помощи понятий свободы, коммуникации, ситуации, информации, субъективности можно определить предпосылки социальных технологий, а понятия «социальный институт», «организация», «бюрократия», «технократия», «общество знания» и некоторые другие относятся к возможным заказчикам и сферам реализации социальных технологий» [2, С. 360].

Политика и экономика, наука и религия, семья и образование, культура и досуг оказались буквально пронизаны применением тех или иных видов

технологий. Не осталась свободна от них также и сфера права: с появлением новых и развитием уже известных технологий модернизации подвергаются сферы правотворчества и правоприменения. Сегодня все больше оснований для того, чтобы взглянуть под этим углом зрения на судопроизводство, описав отправление правосудия как одновременное применение целого ряда социальных, когнитивных и гуманитарных технологий. Особую ценность данный подход приобретает в эпоху отчасти стихийной, отчасти управляемой цифровизации сферы права и правоприменения. Внедрение в деятельность суда интеллектуальных технологий (IT) будет ровно в той степени обоснованным, эффективным и прогнозируемым, в какой сами эти технологии смогут быть представлены как один из видов технологизации правоприменительной деятельности и в какой они смогу сопоставляться, сравниваться и даже противопоставляться другим технологиям: социальных, когнитивным или гуманитарным.

В самом общем виде *технология* — это совокупность знаний и умений, специально разработанных или подобранных для решения однотипных задач. При этом технология позволяет зафиксировать ту часть действия, знания о которой и умение воспроизводить которую необходимы для воспроизводства всего действия. Применение технологии позволяет так репродуцировать ранее осуществленное действие, чтобы в точности или с незначительными отклонениями повторить ранее достигнутый результат. Как отмечает В.М. Розин, «о технологии стали говорить после того, как выяснилось, что цивилизационные завоевания, достижение новых эффектов труда связаны не только с новой техникой, но и с новыми формами кооперации, организации производства и деятельности, с возможностями концентрации ресурсов, с культурой труда, с накопленным научно-техническим и культурным потенциалом, с целеустремленностью усилий общества и государства и т.д.» [4, С. 503]. Российский философ расширяет понятие технологии, предлагая видеть в последней «сложную реальность», позволяющую сохранять цивилизационные завоевания посредством сочетания новаций и развития. Такое расширение не представляется продуктивным, ибо соединяет технологии с их применением и деятельностью как таковой.

Для того, чтобы что бы добиться повторения как самого действия, так и его результата, необходимо что-то знать, что-то помнить, что-то уметь. При этом то, что невозможно сохранять с помощью обычной человеческой памяти, нуждается в иных средствах для своего сохранения: либо при помощи описания, либо в виде схем и рисунков. Для того, чтобы повторить это действие смог кто-то другой, необходимо его обучить, предоставив те самые описания, схемы или рисунки. Все это давно уже стало рутинным элементом производственной деятельности, вошло в повседневность образовательных и управленческих практик. Образовательные и управленческие технологии не обязательно выстроены вокруг сферы «материального производства», но образом и образцом технологии как таковой все же остается взаимодействие человека с природой, будь то производство вещей или лечение больного.

Между тем, за последнее столетие бурное развитие получили технологии взаимодействия человека с обществом, человека с человеком, человека со знанием и даже человека с самим собой. Поэтому первыми в поле зрения теоретика попали технологии изготовления вещей, то есть материального производства. Но затем философское осмысление семейства технологий было расширено: к области изготовления вещей добавились сферы производства знаний, совершенствования институтов, формирования ценностей, выявления смыслов и даже обработки информации. Предметом широкого обсуждения теоретиков стали когнитивные, социальные, гуманитарные и, наконец, интеллектуальные технологии. То есть, эти виды деятельности стали рассматриваться в качестве технологизированных, то есть подвергнутых схематизации, формализации, алгоритмизации. Этому способствовала не только чрезвычайная их распространенность и массовость, но и то воздействие которое они оказали на жизнь человека и общества.

Социальная технология – способ организации межиндивидуального, внутригруппового и межгруппового взаимодействия. В.М. Быченков определяет социальные технологии как «практически ориентированное социальное знание, имеющее целью создание и изменение организационных структур, и управление социальным поведением людей; совокупность методов и приемов решения задач (достижения целей), выработанных в процессе социального планирования и социального проектирования» [1, С. 503].

Возвращаясь к принципам уголовного судопроизводства, необходимо отметить и следующее. Данные принципы не предполагают консервацию, трансформацию или репродукцию каких-либо особенностей социальной структуры, институтов или процессов, но всецело обращены к системе личности и ее охране от агрессивных воздействий внешней (социальной) среды. Между тем цифровизация не может оказать одностороннего и изолированного воздействия на личность или на общество. Ее действие затрагивает всю систему отношений между ними. Алгоритмы, призванные исключить влияние человеческой субъективности, на самом деле не достигают подобной цели, но приводят к ее «отложенному действию». Как и человек, компьютер может быть предвзятым. Искусственный интеллект накапливает не только информацию, но и знания, оценки, допущения и убеждения, которые также полны предвзятости, как и знания, оценки, допущения и убеждения реальных индивидов. Более того, само накопление данных, независимо от того, является ли оно индуктивным или имеет более сложную модель, включающую в себя распознавание образов, способно рождать новые «предвзятости», которые являются результатом спонтанных и неконтролируемых комбинаций из имеющихся оценок и убеждений, «усвоенных» компьютером прежде.

Список литературы

1. Быченков, В.М. Технологии социальные / В.М. Быченков // Новая философская энциклопедия. М.: Мысль, 2010. 503с.

2. Касавин, И.Т. Социальная эпистемология / И.Т. Касавин // Фундаментальные и прикладные проблемы. М.: Альфа-М, 2013.460 с.

3. Пржиленский, В.И. Социальные технологии и принципы уголовного судопроизводства в условиях его цифровизации/ В.И. Пржиленский // Lex russica.2020.Т. 73.№ 4. С. 84-92.

4. Розин, В.М. Технология / В.М. Розин // Новая философская энциклопедия. М.: Мысль, 2010. 503с.

УДК367.1

ПРОБЛЕМНЫЕ АСПЕКТЫ УЧАСТИЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ НА ПРЕДВАРИТЕЛЬНОМ СЛЕДСТВИИ: ПУТИ ИХ РЕШЕНИЯ ПРИ ИСПОЛЬЗОВАНИИ ВОЗМОЖНОСТЕЙ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Ракитина Валерия Игоревна,
заместитель руководителя
Уваровского межрайонного следственного отдела
следственного управления Следственного комитета
Российской Федерации по Тамбовской области
Московская академия Следственного комитета Российской Федерации,
г. Москва, Россия
e-mail: lera.rakitina@yandex.ru

Научный руководитель: Шаталов Александр Семёнович
доктор юридический наук,
профессор кафедры уголовного процесса Московской академии Следственного комитета Российской Федерации

Аннотация: *в данной работе автором уделяется внимание цифровизации уголовного процесса как неотъемлемой части научно-технического прогресса. Отмечается высокая степень необходимости внедрения информационно-телекоммуникационных технологий на досудебных стадиях уголовного судопроизводства. Автором рассмотрены точки зрения на процесс интеграции информационно-телекоммуникационных технологий в практическую деятельность уполномоченных должностных лиц правоохранительных органов. В статье автором отражены предпринимаемые законодателем двух стран ближнего зарубежья меры к усовершенствованию уголовно-процессуального закона в части использования информационно-телекоммуникационных технологий при производстве следственных и иных процессуальных действий. Автором отражена необходимость применения таких технологий при производстве следственных и иных процессуальных действий, где участниками уголовного судопроизводства выступают наиболее социально незащищённая категория населения - лица с ограниченными возможностями здоровья.*

Ключевые слова: *уголовное судопроизводство, цифровизация, информационно-телекоммуникационные технологии, лица с ограниченными возможностями здоровья, следственные действия, инвалиды.*

PROBLEMATIC ASPECTS OF THE PARTICIPATION OF PERSONS WITH DISABILITIES IN THE PRELIMINARY INVESTIGATION: WAYS TO SOLVE THEM WHEN USING THE CAPABILITIES OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Rakitina Valeria Igorevna,
deputy head
Uvarovsky interdistrict Investigative Department
of the Investigative department of the investigative committee
of the Russian Federation in the Tambov region
Moscow Academy of the investigative committee of the Russian Federation, Moscow, Russia
e-mail: lera.rakitina@yandex.ru

Scientific supervisor: Shatalov Alexander Semyonovich
doctor of law,
professor of the Department of criminal procedure of the Moscow Academy of the investigative committee of the Russian Federation

Abstract: *in this article, the author pays attention to the digitalization of the criminal process as an integral part of scientific and technological progress. There is a high degree of need for the introduction of information and telecommunication technologies at the pre-trial stage of criminal proceedings. The author considers the points of view on the process of integration of information and telecommunication technologies into the practical activities of authorized law enforcement officials. In the article, the author reflects the measures taken by the legislator of the two neighboring countries to improve the criminal procedure law in terms of the use of information and telecommunication technologies in the production of investigative and other procedural actions. The author reflects the need for the use of such technologies in the production of investigative and other procedural actions, where the most socially unprotected category of the population - persons with disabilities - act as participants in criminal proceedings.*

Keywords: *criminal proceedings, digitalization, information and telecommunication technologies, persons with disabilities, investigative actions, people with disabilities.*

В настоящее время актуальными вопросами как для представителей научной среды в области уголовного процесса, так и для правоприменителей выступают особенности участия лиц с ограниченными возможностями на предварительном следствии. Как показывает изучение норм действующего

уголовно-процессуального законодательства, процессуальным правам и обязанностям лиц с ограниченными возможностями здоровья законодателем уделено совсем мало внимания: не предусмотрены особенности производства следственных действий с участием инвалидом с учётом их различного процессуального статуса: будь то потерпевший, свидетель или подозреваемый (обвиняемый). Прежде, чем перейти к рассмотрению конкретных проблем, связанных с обеспечением участия в следственных действиях лиц с ограниченными возможностями, полагаем необходимым обратиться к позициям учёных на предмет цифровизации уголовного судопроизводства в целом.

Следует отметить, что возникновение цифровых технологий обусловило мощный толчок для развития других сфер жизнедеятельности, что коснулось и уголовного судопроизводства. Популяризацию получили две параллельные тенденции: совершенствование судебной системы ввиду использования судебными органами в своей деятельности средств «электронного правосудия», а также развитие так называемого «электронного уголовного дела» [1, с. 7] - достижения цифровизации активно используются как на досудебных стадиях, так и в ходе судебного разбирательства.

Отдельные учёные-процессуалисты акцентируют внимание на возможностях в сфере информационно-телекоммуникационных технологий для оптимизации уголовно-процессуальной деятельности. Так, О.В. Качалова и Ю.А. Цветков полагают, что цифровизация уголовного судопроизводства должна совершенствоваться в двух параллельных друг другу направлениях: «Во-первых, в направлении внедрения новых информационных технологий, способствующих повышению открытости, доступности и оперативности правосудия, а во-вторых, в направлении усовершенствования самого процесса посредством снижения его избыточного формализма» [2, с. 95]. Мы согласимся с их мнением, поскольку досудебные и судебные стадии уголовного процесса связаны между собой, одна стадия последовательно сменяет другую, в связи с чем при внедрении цифровых технологий законодателем должно быть обеспечено внесение соответствующих изменений в нормативно-правовые акты, регулирующие обе стадии.

Развивая идею «электронного уголовного дела», ученые-процессуалисты Е. В. Никитин и С. В. Зуев указывают на необходимость изменения «самой модели доказывания и на внедрение как в судебную практику, так и в практическую работу следователей элементов «гибридного» искусственного интеллекта, позволяющего выполнить некую алгоритмизацию процесса принятия судебных и процессуальных решений» [3, с. 589].

В. С. Власова полагает, что преобразование системы уголовного судопроизводства не может заключаться только во внесении предложений «по переходу на электронный документооборот, созданию электронного аналога «уголовного дела», о дублировании процессуальных действий и решений в электронном виде» [4, с. 11]. Она видит «революционный» потенциал информационно-телекоммуникационных технологий для сущностного изменения всей системы уголовного судопроизводства, в том числе на

досудебных его стадиях. Мы соглашаемся с её позицией и в обоснование своего мнения отметим, что возможности информационно-телекоммуникационных технологий не ограничиваются лишь обменом и составлением процессуальных документов в электронном виде. Благодаря внедрению цифровых технологий возможно производство следственных действий с применением электронных и информационно-телекоммуникационных сетей, а также использование систем видео-конференц-связи.

Актуальность данной проблемы присуща не только отечественной юридической науке. Зарубежные учёные в области уголовного права и процесса активно обсуждают возможности и риски цифровизации уголовного судопроизводства [5, с. 94]. Одним из сторонников цифровой революции уголовного процесса выступает Ричард Сасскинд - профессор Оксфордского университета, который получил докторскую степень за изучение особенностей использования искусственного интеллекта в уголовном праве. Он предлагает в дальнейшем отойти от традиционного отправления правосудия в части малозначительных уголовных дел благодаря реализации концепции так называемых онлайн-судов. Предложенная им идея, заключается в трансформации синхронного и публичного судебного процесса в асинхронный, который не предполагает взаимодействия многих людей. Первый этап трансформации предполагает принятие решений человеком, а на последующих процессах они принимаются с использованием возможностей искусственного интеллекта. [6, с. 126]. Мы оцениваем предложенную Р. Сасскиндом концепцию по внедрению цифровых технологий положительно, поскольку полагаем, что она может быть использована и на досудебных стадиях уголовного судопроизводства. В частности, такое следственное действие как очная ставка может быть проведено с использованием видео-конференц-связи, что особенно актуально для лиц с ограниченными возможностями здоровья.

Ученые также выражают скептическое отношение относительно возможности качественного сущностного изменения отечественного уголовного судопроизводства в связи с внедрением в него цифровых технологий. Л. В. Головко полагает, что допустимо говорить лишь о том, что «уголовный процесс и его участники, включая, разумеется, государственные органы, являются одними из потребителей коммерциализации достижений научно-технической революции», но такие преобразования не способны «заменить классический уголовный процесс каким-то «новым уголовным процессом» [7, с. 16]. Кроме того, он считает, что в целях скорейшего внедрения в отечественный уголовный процесс электронного уголовного дела необходимо изучить и принять во внимание зарубежный опыт использования современных цифровых технологий, что позволит трезво оценивать риски, сопутствующие трансформации уголовного судопроизводства.

По нашему мнению, к лицам с ограниченными возможностями здоровья относятся, в том числе, лица, имеющие физические недостатки. В связи с этим, к основным проблемным аспектам в плане участия лиц, имеющих физические недостатки, на предварительном следствии уголовного судопроизводства, можно отнести:

- физическая затруднённость при принятии участия в различных следственных действиях (допрос, проверка показаний на месте, очная ставка, следственный эксперимент);

- сложности в понимании существа следственного действия ввиду наличия какого-либо физического недостатка, затрудняющего дачу показаний и их демонстрацию при производстве конкретного следственного действия;

- невозможность ознакомления с содержанием процессуального документа ввиду наличия физического недостатка;

- невозможность подписания процессуального документа по окончании производства следственного действия.

В связи с этим, нам хотелось бы отметить особенности использования информационно-телекоммуникационных технологий при производстве следственных действий с участием лиц с ограниченными возможностями здоровья на примере стран ближнего зарубежья в целях разрешения одной из вышеуказанных проблем, каковой является физическая затруднённость при принятии участия в следственных действиях. Так, нами было изучено уголовно-процессуальное законодательство Республики Беларусь (*далее – УПК РБ*), которое содержит нормы, регламентирующие особенности производства следственных действий с участием инвалидов. В статье 194 УПК РБ предусмотрена возможность удостоверения факта подписи протокола лицом, которое в силу физических недостатков или состояния здоровья не может подписать протокол. В данном случае факт невозможности проставления таким лицом подписи в протоколе с согласия следователя удостоверяется иным лицом. Также УПК РБ содержит еще одну норму, представляющую для нас интерес. Она предполагает возможность производства допроса потерпевшего, свидетеля, проведения очной ставки, предъявления для опознания лиц и (или) объектов с их участием дистанционно с использованием систем видеоконференцсвязи (веб-конференции) в случае невозможности прибытия участника процесса для производства следственного действия по состоянию здоровья [8]. По нашему мнению, данную норму можно рассматривать как дополнительную процессуальную гарантию для лиц, имеющих ограниченные возможности здоровья, в части упрощения процедуры проведения с их участием следственных действий.

Уголовно-процессуальный кодекс Республики Казахстан (*далее – УПК РК*) также содержит ряд положений, касающихся производства предварительного следствия при участии лиц с ограниченными возможностями здоровья, с применением информационно-телекоммуникационных технологий. Он, в частности, содержит нормы о производстве допроса потерпевшего или свидетеля, с использованием научно-технических средств в режиме видеосвязи (дистанционный допрос) [9]. В ходе такого допроса участники процессуального действия (потерпевший, свидетель) в режиме трансляции воспринимают показания допрашиваемого лица. Такой допрос может производиться в случае, если допрашиваемое лицо по состоянию здоровья не может лично явиться к следователю, что также можно рассматривать в качестве определенной

процессуальной гарантии для лиц, имеющих ограниченные возможности здоровья и участвующих при производстве предварительного следствия.

Признавая такой опыт в качестве положительного, мы предлагаем внести изменения в статью 189.1 УПК РФ [10], которые возлагали бы на следователя, дознавателя право на применение при проведении таких следственных действий как допрос, очная ставка и опознание, где потерпевшим, свидетелем, подозреваемым или обвиняемым выступает лицо, имеющее физические недостатки, видео-конференц-связи. Для этого предлагаем изложить новую её часть в следующей редакции: «*9. Положения данной статьи распространяются на случаи проведения допроса, очной ставки, предъявления для опознания лиц и (или) объектов с участием лица (лиц), с ограниченными возможностями здоровья»*.

Данное изменение представляется особенно важным и актуальным для лиц с ограниченными возможностями, которые имеют физические недостатки, препятствующие (полностью либо частично) их участию в производстве процессуальных действий. Внедрение данного подхода к организации предварительного расследования будет способствовать не только реализации их права на обжалование принятого должностным лицом решения о применении или не применении информационно-телекоммуникационных технологий, но и приведёт к повышению уровня качества предварительного расследования.

Изучив уголовно-процессуальные законодательства ряда стран ближнего зарубежья, а также с учётом мнения учёных-процессуалистов, мы пришли к выводу о необходимости внедрения в уголовно-процессуальный закон нашей страны правовых норм, которые регламентируют особенности производства следственных действий с участием лиц с ограниченными возможностями здоровья. Цифровизация уголовного судопроизводства непременно должна прочно укорениться в деятельности современных практических работников правоохранительных органов. При этом, законодателем должен быть обеспечен грамотный подход к регламентации данных норм, поскольку их реализация будет способствовать наибольшей защите прав такой группы участников уголовного процесса, как инвалиды.

Список литературы

1. Зуев, С.В. Электронное уголовное дело: за и против / С.В. Зуев // Правопорядок: история, теория, практика. 2018. № 4. С.7.

2. Качалова, О.В. Электронное уголовное дело - инструмент модернизации уголовного судопроизводства / О.В. Качалова, Ю.А. Цветков // Российское правосудие. 2015. № 2. С. 95-101.

3. Зуев, С.В. Информационные технологии в решении уголовно-процессуальных проблем / С.В. Зуев, Е.В. Никитин // Всероссийский криминологический журнал. 2017. Т. 11.№ 3. С. 587-595.

4. Власова, В.С. К вопросу о приспосабливании уголовно-процессуального механизма к цифровой реальности / В.С. Власова // Библиотека криминалиста: науч. журн. 2018. № 1. С. 9-18.

5. Богданович, Н.А. Правовые аспекты формирования электронного уголовного дела: достоинства и недостатки (на примере зарубежного опыта) / Н.А. Богданович // Информационные технологии и право: Правовая информатизация - 2018: Сб. материалов VI Междунар. науч.-практ. конф. / под общ. ред. Е.И. Коваленко. Минск: Национальный центр правовой информации Республики Беларусь, 2018. С. 91-95.

6. Susskind, R. Online courts and the future of justice / R. Sussking // Oxford University Press. 2019. 368 p.

7. Головко, Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция / Л.В. Головко // Вестник экономической безопасности. 2019. № 1. С.15-25.

8. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 15.02.2022 г.) // URL: adilet.zan.kz/rus/docs/K1400000231.

9. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 15.02.2022 г.) // URL: https://adilet.zan.kz/rus/docs/K1400000231.

10. Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 года № 174ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 ноября 2001 года: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 декабря 2001 года // Рос. газ. 2001. 22 декабря.

УДК 367.1

АКТУАЛЬНЫЕ ВОПРОСЫ УНИФИКАЦИИ ДОКАЗАТЕЛЬСТВ В РОССИЙСКОМ СУДОПРОИЗВОДСТВЕ

Русаков Алексей Геннадьевич
старший преподаватель
Красноярский государственный аграрный университет,
г. Красноярск, Россия
email: rusalger@mail.ru
Научный руководитель: Бертовский Лев Владимирович
доктор юрид. наук, профессор,
Национальный исследовательский университет «МИЭТ»
г. Москва, Россия
e-mail: bgl1980@yandex.ru

Аннотация*: В статье исследуются некоторые актуальные вопросы унификации межотраслевого процессуального института доказательств в российском судопроизводстве как основополагающего элемента общей тенденции унификации российского процессуального законодательства.*

Автор обосновывает тезис о возможности и необходимости разработки теории унификации доказательств (и доказывания), обозначает актуальные вопросы, требующие немедленного разрешения, намечает границы

проводимого исследования, формулирует некоторые основные выводы и предложения по заявленной тематике.

***Ключевые слова**: унификация судопроизводства, унификация доказывания, унификация доказательств, цифровизация доказательств, российское административное, арбитражное, гражданское и уголовное судопроизводство.*

CURRENT ISSUES OF UNIFICATION OF EVIDENCE IN RUSSIAN LEGAL PROCEEDINGS

Rusakov Alexey Gennadievich
senior lecturer
Krasnoyarsk State Agrarian University,
Krasnoyarsk, Russia
email: rusalger@mail.ru

scientific adviser: ***Bertovsky Lev Vladimirovich***
doctor of law sciences, professor,
National research university of electronic technology,
Moscow, Russia
e-mail: bgl1980@yandex.ru

***Annotation:** The article examines some topical issues of unification of the intersectoral procedural institution of evidence in Russian legal proceedings as a fundamental element of the general trend of unification of Russian procedural legislation.*

The author substantiates the thesis about the possibility and necessity of developing a theory of evidence (and proof) unification, identifies topical issues that require immediate resolution, outlines the boundaries of the ongoing research, formulates some main conclusions and proposals on the stated topic.

***Keywords:** unification of legal proceedings, unification of evidence, unification of evidence, digitalization of evidence, Russian administrative, arbitration, civil and criminal proceedings.*

15 февраля 2023 г. на ежегодном совещаний судей Президент Российской Федерации В.В. Путин заявил о необходимости обеспечить защиту прав и законных интересов граждан страны при отправлении правосудия.

Основными институтами судопроизводства, без сомнения, являются институты доказательств и доказывания. Поэтому, по нашему мнению, общая тенденция унификации отечественного материального права и процессуального права требует, в первую очередь, унификации отдельных межотраслевых комплексных институтов доказывания и доказательств.

Вопросы унификации российского права в целом, его материальных и процессуальных отраслей, некоторых смежных институтов процессуального права стали предметом широкого обсуждения на страницах научных работ,

выступают в качестве предмета научных исследований и дискуссий [1,2,3,5.6, 9,10-11,12,13]. В юридической науке, в основном, исследуются актуальные вопросы унификации судопроизводства в целом (как процессуальной формы) или процедуры доказывания как упрощенной формы судопроизводства [4,8], также исследуются актуальные вопросы унификации уголовно-процессуальных форм, унификации упрощенных процедур в гражданском судопроизводстве, обосновывается вывод о создании на базе арбитражного, гражданского и административного законодательства Единого или Модельного кодекса [2,8,12].

Однако, указанные авторы недостаточно уделяют внимания вопросам унификации межотраслевого института доказательств в российском судопроизводстве, в юридической науке отсутствует единообразие в понимании и толковании основных положений правовой унификации: по-разному определяют объект правовой унификации – изменение содержания права [13], изменение нормы права [8], изменение правовой терминологии [12] и др., существуют различные подходы к целям и задачам унификации: создание качественно новой [10], совершенствование существующей процессуальной формы [11]; к формам, методам и средствам унификации, под которыми исследователи понимают соответственно правотворческую деятельности и внутреннюю кодификацию [12], использование юридической техники [11]. средства достижения единообразия процесса [9].

В настоящий момент дискуссионными остаются проблемы терминологического и организационно-правового плана. Предлагаемая нами концепция унификации доказательств базируется на следующих общетеоретических положениях.

1. Объективно существуют единые (тождественные) начала в различных институтах процессуальных отраслей российского права, таких как: принципы и механизмы их реализации (в том числе с использованием видеоконференцсвязи), процессуальные сроки, извещения и вызовы участников процесса, судебные расходы, судебное представительство, правовой статус участников судопроизводства, средства доказывания, требования к судебным актам, порядок и основания их пересмотра и многие другие. Примеры унификации норм указанных институтов арбитражного, гражданского и административного судопроизводства общеизвестны.

2.Доказывание представляет собой комплекс объединенных единой логикой последовательных действий субъектов доказывания (алгоритм, технология), а именно: формирование (собирание) доказательств с процессуальной фиксацией; исследование доказательств с фиксацией процедуры и результатов исследования; оценка доказательств управомоченным правоприменителем с фиксацией результатов исследования; перепроверка (например, судом апелляционной инстанции). Данный алгоритм соответствует подразделению процесса на стадии и вилы судопроизводства.

3. Элементы доказывания, и в первую очередь, доказательства и средства доказывания, состоят в специфической связи между собой. Например: свидетель-субъект процесса доказывания и носитель (источник) информации;

показания свидетеля - это доказательство как информация, которая относится к делу (признак относимости) и допустимый законом источник доказательственной информации (признак допустимости): средство доказывания-допрос свидетеля в порядке, установленном процессуальным законом (признаки допустимости и достоверности доказательств).

4. Триединства признаков (относимости, допустимости и достоверности) доказательств явно недостаточно в эпоху цифровизации экономики и использования в гражданском обороте электронных документов, а в судопроизводстве – электронно-цифровых доказательств. Актуальным является вопрос об использовании четвертого признака («электронно-цифровая визуализация»), который должен отражать «читаемость документа» электронными машинами, т.е. возможность использования участниками судопроизводства современных технологий, чтобы формировать доказательства (отбирать искомую информацию) фиксировать доказательства, хранить, обрабатывать, передавать, воспроизводить и использовать доказательства в процессе доказывания обстоятельств юридических дел.

5. При доказывании обстоятельств юридических дел необходимо использовать термины «электронно-цифровые доказательства», «электронно-цифровая визуализация доказательств», которые, полагаем, верно отражают их правовую сущность и использовании в судопроизводстве.

6. Указанное триединство признаков доказательств: относимость (информации), допустимость (источника), достоверность (соблюдение процедуры формирования, исследования, оценки, перепроверки доказательств) выступает не только признаками (свойствами, чертами доказательств), а в первую очередь является критериями их оценки правоприменителями. Полагаем, что в современных условиях, с учетом цифровизации судопроизводства данные критерии оценки доказательств приобретают качественно новое содержание.

7. Необходима реализация единого унифицированного подхода к использованию при доказывании обстоятельств юридических дел материалов служебных расследований, ведомственных и прокурорских проверок, материалов, полученных на доследственных и досудебных стадиях судопроизводства (результатов ОРД), документов гражданского оборота, претензионных и примирительных процедур (применяя, в том числе возможности электронно-цифрового отображения и «машинной читаемости»). К настоящему моменту правовое регулирование использования большинства указанных материалов (за исключением ОРД) отсутствует.

8. Возможно обеспечить достаточный уровень унификациидоказательств по всем категориям юридических дел вообще и в рамках каждого вида судопроизводства-административного, арбитражного, гражданского и уголовного, а также- в рамках третейского разбирательств при обращении в его участников в компетентный суд для оказания им правовой помощи по обеспечению иска, при оспаривании решения третейского суда или просьбы о выдаче исполнительного листа на принудительное исполнение решения третейского суда.

На основании изложенного сформулируем следующие основные воды и предложения.

1.Полагаем необходимым выработать четкую юридическую терминологию теории правовой унификации доказательств, выработать принципы и методы унификации (общие, отраслевые и специальные) доказательств, в качестве таковых принципов унификации института доказательств предлагаем следующие: законность, универсальность, системность.

2.Унификация доказательств, считаем, потребует разработки и обоснования термина «унифицированное доказательство» и формирования собственной классификации унифицированных доказательств, в том числе электронно-цифровых; создание собственной классификации унифицированных средств доказывания. В качестве критериев классификацию электронных (цифровых) доказательств предлагаем следующие по содержанию информации, по субъекту, от которого исходит информация, по субъекту-адресату, по характеру носителя, по способу обнаружения, и формирования (изъятия), по способу фиксации, по способу хранения, по способу передачи и т.п.

3. Требуется разработать и апробировать систему унификации средств доказывания**.**

4. Предлагаем следующую редакцию понятия доказательств: доказательства — это сведения о фактах, имеющих значение для правильного разрешения юридического дела, полученные из допустимых процессуальным законом источников, сформированные, исследованные и подвергнутые оценке (в том числе- с применением технических средств электронно-цифровой визуализации») при соблюдении правил, предписанных процессуальным законодательством.

5.Также считает необходимым разработать стандарты допустимости и достоверности доказательств вообще и электронно- цифровых доказательств- в частности, унифицировать требования в форме и содержанию заключения эксперта, письменным материалам и иным документам, содержащим доказательственную информацию.

6. Поэтому назрела необходимость разработать и принять Федеральный закон «О доказательствах и доказывании в Российской Федерации», чтобы без внесения существенных изменений в действующие процессуальные кодексы обеспечить процедуру унификации института судебных доказательств (параллельно с разрешением ряда других проблем доказывания), чтобы обеспечить эффективность российского судопроизводства.

Список литературы

1. Бертовский, Л.В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Л.В. Бертовский [Электронный ресурс] / Научная электронная библиотека «КиберЛенинка». URL:

https://cyberleninka.ru/article/n/tehnologiya-blokcheyna-v-ugolovnom-protsesse-kak-element-tsifrovogo-sudoproizvodstva (Дата обращения: 14.02.2023).

2. Бертовский, Л.В. Высокотехнологичное право: понятие. Генезис, перспективы / Л.В. Бертовский [Электронный ресурс] // Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/vysokotehnologichnoe-pravo-ponyatie-genezis-i-perspektiv (Дата обращения: 14.02.2023).

3. Баранов, А.М. Электронные доказательства: иллюзия уголовного процесса XXI века / А.М. Баранов [Электронный ресурс] Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/elektronnye-dokazatelstva-illyuziya-ugolovnogo-protsessa-xxi-v (Дата обращения: 14.02.2023).

4. Воскобитова, Л.А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости / Л.А. Воскобитова [Электронный ресурс] / Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/ugolovnoe-sudoproizvodstvo-i-tsifrovye-tehnologii-problemy-sovmestimosti (Дата обращения: 14.02.2023).

5. Гаврилин, Ю.В., Модернизация информационного общества уголовно-процессуальной формы в условиях информационного общества / Ю.В. Гаврилин, А.В. Побежкин [Электронный ресурс] Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/modernizatsiya-ugolovno-protsessualnoy-formy-v-usloviyah-informatsionnogo-obschestva (Дата обращения: 14.02.2023).

6. Громошина, Н.А. Дифференциация и унификация в гражданском судопроизводстве: автореферат дисс. на соискание степени доктора юрид. наук / Н.А. Громошина. Москва, 2010. 50 с.

7. Гусева, И.И. Унифицированный дифференцированный подход к структуре уголовного процесса Российской Федерации: автореферат дисс. на соискание степени канд. юрид. наук / И.И. Гусева. Владимир, 2004. 32 с.

8. Зазулин, А.И. Цифровые доказательства в суде / А.И. Зазулин [Электронный ресурс] Научная электронная библиотека «КиберЛенинка». URL: https://clck.ru/ehw6d (Дата обращения: 14.02.2023).

9. Зуев, С.В. Слабые стороны информационного подхода в свете цифровизации уголовного судопроизводства / С.В. Зуев, А.С. Титова [Электронный ресурс] / Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/slabye-storony-informatsionnogo-podhoda-v-svete-tsifrovizatsii-ugolovnogo-sudoproizvodstva (Дата обращения: 14.02.2023).

10. Медведева, Е.В. Тенденции дифференциации и унификации в упрощенных производствах цивилистического процесса / Е.В. Медведева [Электронный ресурс] / Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/tendentsii-differentsiatsii-i-unifikatsii-v-uproschyonnyh-proizvodstvah-tsivilisticheskogo-protsessa (Дата обращения: 14.02.2023).

11. Мищенко, Е.В. Проблемы дифференциации и унификации уголовно-процессуальных форм производств по отдельным категориям

уголовных дел автореферат дисс. на соискание степени канд. юрид. наук / Е.В. Мищенко. Оренбург, 2014. 68 с.

12. Мищенко, Е.В. Проблемы унификации норм процессуальной формы в уголовном судопроизводстве / Е.В. Мищенко [Электронный ресурс] Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/problemy-unifikatsii-norm-protsessualnoy-formy-v-ugolovnom-sudoproizvodstve (Дата обращения: 24.02.2022).

13. Потапенко, Е.Г. Унификация права: понятие, формы. Методы (в контексте исследования унификации цивилистического процессуального права) / Е.Г. Потапенко [Электронный ресурс] Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/unifikatsiya-prava-ponyatie-formy-metody-v-kontekste-issledovaniya-unifikatsii-tsivilisticheskogo-protsessualnogo-prava (Дата обращения: 14.02.2023).

14. Смирнова, Л.Е. Унификация в уголовном праве: автореферат дисс. на соискание степени канд. юрид. наук / Л.Е. Смирнова. Казань, 2006. 27 с.

15. Стрюков, Е.А. Общие подходы к пониманию унификации нормативных правовых актов / Е.А. Стрюков [Электронный ресурс] Научная электронная библиотека «КиберЛенинка». URL: https://cyberleninka.ru/article/n/obschie-podhody-k-ponimaniyu-unifikatsii-normativnyh-pravovyh-aktov (Дата обращения: 14.02.2023).

УДК 343

КИБЕРБУЛИНГ-ПРЕСТУПЛЕНИЕ XXI ВЕКА

Сарсенова Ксения Сергеевна
обучающийся
Луценко Павел Александрович
кандидат юридических наук, доцент
Воронежский государственный аграрный университет имени императора Петра I, Россия, г. Воронеж,
e-mail: lawyer.vrn@mail.ru

***Аннотация**: Данная статья посвящена актуальной проблеме развития общества. Рассматриваются сложности организации противодействия преступлений в области киберпространства. Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, темпы роста преступности во всемирной сети, являются самыми быстрыми на планете.*

***Ключевые слова:** кибербуллинг, всемирная сеть, буллинг, интернет-травля, агрессор, манипуляция.*

CYBERBULLYING IS A CRIME OF THE XXI CENTURY

Sarsenova Ksenia Sergeevna
Student
Lutsenko Pavel Alexandrovich
candidate of legal sciences, associate professor
Voronezh State Agrarian University named after Emperor Peter I,
Russia, Voronezh,
e-mail: lawyer.vrn@mail.ru

Annotation: This article is devoted to the actual problem of the development of society. The complexities of the organization of countering crimes in the field of cyberspace are considered. The number of crimes committed in cyberspace is growing in proportion to the number of users of computer networks, the growth rate of crime in the world Wide web is the fastest on the planet.

Keywords: cyberbullying, worldwide network, bullying, Internet harassment, aggressor, manipulation.

Современное повседневное общение благодаря новейшим информационным технологиям становится более популярным и доступным. Сложности, возникающие с травлей в реальности, перешли в виртуальный мир. Перед людьми открываются новые, безграничные возможности в результате использования Всемирной сети, которая является огромным информационным банком и источником получения и распространения разного вида информации. Интернет расширяет социальные интересы и компенсирует нехватку общения. Люди получают неограниченную свободу создания и обмена информацией.

В настоящее время развитие навыков общения в виртуальном мире порождает возникновение новых форм преступных посягательств. Цифровой мир, в котором доступна анонимность, представляет собой допустимость антисоциального поведения, удобную площадку для проявления агрессивных форм девиации. Это влечет за собой возникновение виртуального конфликта.

Такие конфликты подвергают опасности пользователей, создают риски появления неприязненных отношений между подростками. Из-за подобных разногласий молодежь рискует стать жертвой кибербуллинга.

Анонимность сводит к минимуму уровень личной ответственности, и как следствие электронные письма крайне затруднительно контролировать. Жертва кибербуллинга становится объектом насмешек, оскорблений, преследования и травли. Человек испытывает беспокойство, стресс, страх, возникают суицидальные мысли. Электронные сообщения жертва получает внезапно, что ведет к сильнейшей эмоциональной встряске, и сильному психологическому прессингу со стороны агрессора.

Буллинг, в некоторой степени, новый термин, означающий, по утверждению американского ученого Д. И. Лейна, физическое или психологическое насилие со стороны одного человека в отношении другого [3].

Кибербуллинг – это хулиганские действия через различные средства коммуникации. Исследованность данного явления находится на начальном этапе развития. В российской правовой доктрине такой феномен как кибербуллинг стали исследовать сравнительно недавно. Для более полного представления данного термина обратимся к отечественным специалистам в данной области.

Е. А. Макарова, Е. Л. Макарова и Е. А. Махрина представляют кибербуллинг как более изощренную форму травли, включающую в себя моральное и психологическое насилие, доминирование и принуждение, социальную изоляцию, запугивание и вымогательство, осуществляемое с помощью электронных средств коммуникации [4].

Исследователи данного феномена обращают наше внимание на то, что интернет-травля несет в себе моральное и психологическое насилие над жертвой. Также выявляют вероятные исходы такого давления. В своих научных трудах специалисты подчеркивают, что насилие проявляется в виде запугивания, шантажа, издевательств. Исходя из данного определения, можно прийти к выводу, что кибербуллинг причиняет колоссальный вред психике людей и приводит к трагическому результату. Жертва испытывает тревожность, впадает в депрессию, ухудшается самооценка, происходит нарушение пищевого поведения, появляются суицидальные мысли.

Виртуальный мир позволяет людям использовать всевозможные формы и способы общения, примерять на себя различные роли и экспериментировать с собственной идентичностью. Интернет являет собой пространство поиска новых впечатлений и эмоций.

В настоящее время, в основном, среди молодежи развивается активное пользование интернет-коммуникациями. Лисовский В.Т. – один из первых ученых, который сформулировал понятие «молодежь»: «Молодежь» — это поколение людей, проходящих стадию социализации, усваивающих, а в более зрелом возрасте уже усвоивших образовательные, профессиональные, культурные и другие социальные функции; в зависимости от конкретных исторических условий, возрастные критерии молодежи могут колебаться от 16 до 30 лет» [2].

В интернет-травле фигурируют следующие лица:

1. Жертва

В следствие непрекращающейся онлайн-агрессии молодые люди замыкаются в себе, испытывают чувство безысходности, бессилия, появляются разного рода зависимости и развивается потеря веры в себя.

2. Агрессор или преследователь

Это люди, которые инициируют или поддерживают травлю. Зачастую, люди становятся агрессорами потому как сами подвергались издевательствам и унижению. Кибербуллеры испытывают враждебность, неприязнь к определенным группам людей. Они хотят получить положительные эмоции, путем проявления жестокости и доведения жертвы до состояния тревоги и стресса.

3. Наблюдатель

Это незримый двигатель в цикле буллинга. Около 90% молодых людей становятся свидетелями интернет-травли. Человек может находиться вне конфликта или активно участвовать в выяснении отношений.

Баранов А.А. и Рожина С.В. сформулировали следующие причины кибербуллинга:

1) Стремление к превосходству;
2) Комплекс неполноценности;
3) Зависть;
4) Месть;
5) Развлечения [1].

На сегодняшний день в научном мире проведено множество зарубежных исследований, которые дают возможность оценить важность и серьезность такого явления как кибертравля. В частности, Р. Ковальски, С. Лимбер, П. Агатсон уделили внимание описанию различных форм онлайн-агрессии. О. Юбарра исследовал соотношение кибербуллинга и стрессогенного состояния. Ульвеус излагал воздействия сильного на слабого.

На данный момент широко распространено манипулирование и киберзапугивание в таких социальных сетях как «ВКонтакте», «Телеграмм» и т.п. Манипуляция – это скрытое управление, при котором инициатор достигает своих эгоистических целей, нанося ущерб адресату своего воздействия [5]. Социальные сети способствуют распространению ложной информации и различных манипуляций. Очень сложно покончить с публикацией искаженных или порочных сведений.

По данным недавних исследований и экспериментов, жертвами онлайн-агрессии оказались более 40 % молодых людей. Исходя из этого, кибербуллингу подвергается каждый третий человек.

Феномен интернет-травли развит во многих странах мира: в Великобритании, США, Германии, Италии и других, где органы государственной власти должны уделять проблеме кибербуллинга больше внимания. Потому как, в современном мире интернет является неким целеуказателем, способствующим становлению, развитию сознания людей.

Агрессия сегодня является неотъемлемой частью интернет пространства. Это связано с тем, что люди все больше времени проводят в виртуальном мире, социальных сетях. У нынешней молодежи сложился совершенно другой образ жизни, являющий собой онлайн-оффлайн реальность. Значительное расширение контактов благодаря виртуальному пространству, существование связей с людьми, с которыми не было опыта общения в реальности, может привести к серьезным рискам, к проявлению агрессии.

Психологические травмы влияют на жизнедеятельность человека. Кибербуллинг влечет за собой злость, снижение учебной активность, низкий уровень концентрации, самобичевание. На ощущения жертв онлайн-агрессии влияет неосведомленность количества агрессоров и наблюдателей.

Таким образом, исходя из вышесказанного, искоренить кибербуллинг, как и многие другие проявления жестокости и агрессии во Всемирной сети, не представляется возможным. Следует максимально обезопасить себя и близких людей от риска стать жертвой кибер-травли, необходимо совершенствовать свои знания в области информационной безопасности, а также развивать осознанное отношение к своему поведению в виртуальном пространстве.

Список литературы

1. Баранов, А.А. Психологический анализ причин подросткового кибербуллинга / А.А. Баранов, С.В. Рожина // Вестник удмуртского университета. 2015. № 3. С. 5-8.
2. Лисовский. В.Т. Духовный мир и ценностные ориентации молодежи России / В.Т. Лисовский. СПб.: СПбГУП, 2000. 508 с.
3. Лэйн, Д. И. Школьная травля (буллинг) // Детская и подростковая психотерапия / под ред. Д. Лэйна, Э. Миллера. СПб.: Питер, 2001. С. 240.
4. Макарова, Е. А. Психологические особенности кибербуллинга как формы интернет-преступления / Е.А.Макарова и др. // Российский психологический журнал. 2016. № 3. С. 293–311.
5. Шейнов, В. П., Манипулирование и защита от манипуляций / В.П.Шейнов. Санкт-Петербург, 2014. 162 с.

УДК 343.3

ИСПОЛЬЗОВАНИЕ КОСМИЧЕСКОГО МОНИТОРИНГА ЗА СОСТОЯНИЕМ ЛЕСОВ ДЛЯ ВЫЯВЛЕНИЯ НЕЗАКОННОЙ РУБКИ ЛЕСНЫХ НАСАЖДЕНИЙ

Середа Ольга Викторовна,
ассистент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: o.v.sereda@mail.ru

Аннотация: *в статье рассматриваются действующие механизмы использования космического мониторинга за состоянием лесных массивов при выявлении незаконных рубок лесных насаждений. Приводятся примеры успешного выявления и расследования таких преступлений (на основе вынесенных приговоров по ст. 260 УК РФ). Дается оценка использования экспериментального проекта «Цифровая земля» и возможностей нейросети для оперативной обработки полученных в результате космического мониторинга данных.*

Ключевые слова: *космический мониторинг, незаконная рубка лесных насаждений, проект «Цифровая земля», обработка данных нейросетью.*

THE USE OF SPACE MONITORING OF THE STATE OF FORESTS TO DETECT ILLEGAL LOGGING OF FOREST PLANTATIONS

Sereda Olga Viktorovna,
assistant
Krasnoyarsk state agrarian university, Krasnoyarsk, Krasnoyarsk, Russia
e-mail: o.v.sereda@mail.ru

Abstract: *the article discusses the current mechanisms of using space monitoring of the state of forests in the detection of illegal logging of forest plantations. Examples of successful detection and investigation of such crimes on the basis of sentences under Article 260 of the Criminal Code of the Russian Federation are given. The evaluation of the use of the experimental project "Digital Earth" and the capabilities of the neural network for the operational processing of the data obtained as a result of space monitoring is given.*

Keywords: *space monitoring, illegal logging of forest plantations, the Digital Earth project, data processing by a neural network.*

Президент России Владимир Путин, в своем видеообращении к участникам заседания по управлению лесным хозяйством в рамках климатического саммита в 2021 году, четко поставил задачу о необходимости принятия самых серьезных и энергичных мер для сохранения лесов, в том числе путем борьбы с незаконными рубками [1].

Ситуация с незаконными рубками год от года не становится лучше, только в Красноярском крае ежегодно на протяжении многих лет выявляется более 700 преступлений по ст. 260 УК РФ Незаконная рубка лесных насаждений [2]. В целом же по России картина еще более удручающая, согласно данным портала Судебной статистики РФ, за 2021 год по всем составам ст. 260 УК РФ «Незаконная рубка лесных насаждений» осуждены более 2,7 тысяч лиц, причем более половины по ч.3 ст. 260 УК – деяние, совершенное в особо крупном размере [3].

Выявление незаконной рубки лесных насаждений в настоящее время проводится несколькими способами:

- проверка обстановки (обзорная проверка) в лесах участковых лесничих на вверенных им участках лесного фонда лесничества;
- рейды сотрудников правоохранительных органов в процессе оперативно-тактических мероприятий «Лес», «Лесовоз», «Колея» по местам возможных незаконных вырубок лесных насаждений;
- сообщение очевидцами наличия следов или процесса незаконной рубки лесных насаждений и передачи данной информации в правоохранительные органы;
- мониторинг лесного покрова на различных летальных аппаратах (вертолеты, беспилотные управляемые аппараты);

- космический мониторинг лесного покрова определенных участков планеты [4,5,6].

Последний из перечисленных способов представляет для нашего исследования особый интерес. Космический мониторинг земли в общепринятом смысле – это осмотр поверхности планеты с помощью космических средств наблюдения. Он отличается оперативностью выявления не только самих изменений, но и их динамики [7].

В настоящее время, для целей выявления незаконной рубки лесных насаждений Рослесхозом России введен эксперимент «Цифровая земля» по мониторингу лесов Архангельской и Иркутской областей, который проводится непрерывно с июня 2022 года. Данный проект ценен тем, что выявлением лесоизменений он не оканчивается. После выявленных изменений лесного покрова эти данные анализируются и соотносятся с существующими лесными декларациями на предмет легальности проводимых вырубок леса. При этом используемая нейросеть позволяет анализировать полученные данные в кратчайшие сроки. Если выявленные изменения не соотнесены с легальными рубками леса, информацию о признаках нарушений направляются в региональные ведомства [8].

Рассматривая судебную практику по незаконным рубкам лесных насаждений, мы видим, что не малое количество уголовных дел было возбуждено и расследовано с помощью данных космического мониторинга.

Так, например, Приговором Мурашинского районного суда Кировской области от 7 февраля 2022 г. был осужден гр. Н. лесничий Опаринского филиала Маромицкого участкового лесничества за преступление, предусмотренное ч.3 ст.260 УК РФ данные о котором были выявлены в 2020 году дистанционным мониторингом использования лесов. Указанная информация была признана доказательством по делу и помогла не только выявить площадь незаконной рубки в 2,8 га, но и предотвратить незаконную деятельность на данном участке [9].

Согласно Приговору Богучанского районного суда Красноярского края от 21 июля 2020 г. благодаря космическому мониторингу была выявлена организованная группа из трех человек, которые совершили преступление, предусмотренное ч.3 ст.260 УК РФ [10].

Приговором Вытегорского районного суда Вологодской области от 22 января 2020 г. по делу № 1-18/2020 за незаконную рубку лесных насаждений в крупном размере осужден гр.К. И в этом случае данные о месте вырубки были выявлены посредством космического мониторинга и переданы для дальнейшего выяснения обстоятельств в Вытегорский территориальный отдел государственного лесничества [11].

В заключение данного небольшого исследования хотелось бы сделать следующие выводы:

Выявление мест исчезновения лесного покрова посредством космического мониторинга, несомненно, является отличным средством выявления незаконных рубок лесных насаждений.

Учитывая оперативность выявления такой информации и оперативность ее передачи в контролирующие органы, существует отличная возможность не только фиксации совершенных преступлений, но и задержании лиц на месте совершения преступления, в случае совершения большой по площади и длительной по времени вырубки в отдаленных территориях.

Считаем необходимым продолжение взаимодействие подразделений Роскосмоса и Рослесфонда по дальнейшему использованию проекта «Цифровая земля», с распространением его действия на области России наиболее криминализированные в этой сфере.

Список литературы

1. Россия принимает энергичные меры по защите лесов, заявил Путин // РИА Новости. URL: https://ria.ru/20211102/les-1757377860.html (дата обращения: 15.02.2023).
2. Середа, О.В. О состоянии преступности в сфере незаконной рубки лесных насаждений (на примере Красноярского края) / О.В. Середа // Альманах лектория. Майские правовые чтения на Енисее: сборник научных трудов. Красноярск: Красноярский государственный аграрный университет, 2022. С.114-117.
3. Судебная статистика РФ. Уголовное судопроизводство // URL: https://stat.апи-пресс.рф/stats/ug/t/14/s/17 (дата обращения: 15.02.2023 г.).
4. Иванов, П.И. Об опыте проведения оперативно-профилактических мероприятий «Лесовоз 2014» (по материалам УТ МВД России по ДФО) / П.И. Иванов, П.Г. Кузнецов // Вестник Казанского юридического института МВД России. 2015. № 2 (20). С.110-115.
5. Амарсайхан, М. Особенности проверки сообщений о незаконной рубке лесных насаждений (по материалам России и Монголии) / М. Амарсайхан // Право и государство: теория и практика. 2020. № 12 (192).
6. Незаконные вырубки леса будут выявляться автоматически. Российская газета // URL: https://rg.ru/ (дата обращения: 15.02.2023).
7. Цветков, В.Я. Анализ применения космического мониторинга / В.Я. Цветков // ПНиО. 2015. № 3 (15). С.48-55.
8. Рослесхоз совместно с Роскосмосом обнаруживают незаконные рубки с помощью нейросети. Официальный портал Федерального агентства лесного хозяйства // URL: https://rosleshoz.gov.ru/news/2022-10-31/n10330 (дата обращения: 15.02.2023).
9. Приговор Мурашинского районного суда Кировской области от 7 февраля 2022 г. по делу № 1-2/3/2022 // URL: https://sudact.ru/ (дата обращения: 15.02.2023).
10. Приговор Богучанского районного суда Красноярского края от 21 июля 2020 г. по делу № 1-91/2020 // URL: https://sudact.ru/ (дата обращения: 15.02.2023).
11. Приговор Вытегорского районного суда Вологодской области от 22 января 2020 г. по делу № 1-18/2020 // URL: https://sudact.ru/ (дата обращения: 15.02.2023).

УДК 343.1

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ДИСТАНЦИОННОГО УЧАСТИЯ В СУДЕБНОМ РАЗБИРАТЕЛЬСТВЕ ПРИ РАССМОТРЕНИИ УГОЛОВНЫХ ДЕЛ СУДАМИ С НАРОДНЫМ ПРЕДСТАВИТЕЛЬСТВОМ В РОССИИ И КИТАЕ

Скрипов Сергей Владимирович,
судья
суд Ямало-Ненецкого автономного округа,
г. Салехард, Россия
e-mail: sergei_lex@mail.ru

Аннотация: *в статье рассматривается вопрос о возможности участия подсудимого в суде присяжных дистанционно. Анализируя законодательство и исходя из примеров некоторых уголовных дел, рассмотренных судом присяжных в России и судом с участием народных заседателей в Китае, автор приходит к выводу, что возможность представлять доказательства присяжным и участвовать в их исследовании дистанционно может способствовать сохранению баланса индивидуальных прав и общественных интересов в случаях, когда соображения безопасности вынуждают отказывать подсудимому в праве на суд присяжных или делают невозможным его пребывание в зале суда.*

Ключевые слова*. Суд присяжных, народные заседатели, право на суд присяжных, участие в суде, IT в уголовном судопроизводстве.*

LEGAL REGULATION OF THE USE OF MODERN TECHNOLOGIES OF REMOTE PARTICIPATION IN CRIMINAL PROCEEDINGS BY COURTS WITH PEOPLE'S REPRESENTATION IN RUSSIA AND CHINA

Skripov Sergey Vladimirovich,
judge
court of the Yamalo-Nenets Autonomous District,
Salekhard, Russia
e-mail: sergei_lex@mail.ru

Annotation: *the article discusses the issue of the possibility of participation of the defendant in the jury trial remotely. Analyzing the legislation and proceeding from the examples of some criminal cases considered by a jury in Russia and a court with the participation of people's assessors in China, the author comes to the conclusion that the ability to present evidence to jurors and participate in their research remotely could contribute to maintaining a balance of individual rights and public interests in cases where security considerations force to deny defendat the right to a jury trial or make impossible his stay in the courtroom.*

Keywords: *Trial by jury, people's assessors, the right to trial by jury, participation in court, IT in criminal proceedings.*

Высокая востребованность и положительная оценка применения в деятельности судов современных технологических средств, прежде всего видеоконференцсвязи и электронного документооборота, в период коронавирусной пандемии [1] логично привели к изменениям в действующем российском законодательстве. В целях оптимизации судебной стадии уголовного судопроизводства за счет использования современных цифровых платформ и технологий, повышения доступности правосудия и уровня защиты прав граждан [2], 29 декабря 2022 года в России был принят Федеральный закон №610-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» [3].

Центральным нововведением названного федерального закона, наряду с предоставлением возможности рассмотрения вопроса о заключении под стражу по видеоконференцсвязи (ч. 4 ст. 108 УПК РФ) и более детальной регламентацией порядка использования электронных документов в уголовном судопроизводстве (ст. 474 УПК РФ), стала ст. 241 УПК РФ — «Участие в судебном заседании путем использования систем видео-конференц-связи». Приветствуя в целом внесенные новеллы, отвечающие необходимости формирования и законодательного закрепления системы цифрового судопроизводства в условиях высокой динамики изменений в общественной жизни [4, с. 745], хотелось бы остановиться на некоторых вопросах использования цифровых технологий в суде присяжных.

Часть 4 ст. 241.1 УПК РФ не допускает участие в судебном заседании подсудимого путем использования систем видеоконференцсвязи при рассмотрении уголовного дела судом с участием присяжных заседателей. Из части 1 ст. 293 УПК РФ исключена возможность предоставления подсудимому последнего слова с использованием систем видеоконференцсвязи. Ранее мы отмечали, что отсутствие в законе указания на предоставление последнего слова подсудимому по ВКС только в исключительных случаях, может привести к необоснованному ограничению права подсудимого на непосредственное выступление перед присяжными и поэтому не соответствует правовой природе этого суда [5, с. 252]. Однако полное отсутствие у подсудимой возможности участвовать в судебном производстве в порядке главы 42 УПК РФ по видеоконференцсвязи вряд ли можно объяснить одной лишь правовой природой данного вида судебного разбирательства.

Авторы законопроекта в своей пояснительной записке никак не обосновывают и не объясняют недопустимость участия подсудимого в судебном заседании путем использования видеоконференцсвязи при рассмотрении уголовного дела судом с участием присяжных заседателей.

При этом, одной из целей использования ВКС закон называет обеспечение безопасности участников уголовного судопроизводства при рассмотрении уголовных дел о тяжких и особо тяжких преступлениях (ч. 2 ст. 241.1 УПК РФ), подсудных и суду присяжных. Ответа на вопрос, почему

безопасность профессиональных участников уголовного судопроизводства и свидетелей оказывается важнее безопасности судей от народа, авторы закона не дают. Хотя именно важностью обеспечения безопасности в свое время Конституционный Суд России мотивировал исключение из подсудности присяжных уголовных дел о терроризме [6, п. 4.1.]. В этом ключе, предусмотренная законом в исключительных случаях возможность участия подсудимого в судебном заседании путем использования видеоконференцсвязи при рассмотрении уголовного дела судом с участием присяжных заседателей обеспечивала бы гармоничное достижение как цели безопасности участников процесса, так и цели повышения гарантий прав граждан на судебную защиту, на реализацию которой направлены внесенные изменения, по замыслу их авторов [2]. Такое правовое регулирование в большей степени соответствовало бы конституционному требованию обеспечения баланса интересов участников уголовного судопроизводства, подтверждением чему является судебная практика.

В 2022 году судом Ямало-Ненецкого автономного округа с участием присяжных заседателей было рассмотрено уголовное дело в отношении трех лиц, обвиняемых в совершении тяжких преступлений, в том числе квалифицированного убийства, в исправительном учреждении, исполняющем наказания в виде пожизненного лишения свободы. Двое из подсудимых, шестеро потерпевших и более двадцати свидетелей по делу являлись лицами, осужденными к пожизненному лишению свободы. Начало процесса осложнялось тем, что один из подсудимых до поступления уголовного дела в суд был переведен для участия в следственных действиях в другой регион России в связи с написанием им явок с повинной по ранее совершенным и не раскрытым до настоящего времени убийствам. Пришлось буквально ждать следствие, не отдававшего подсудимого суду. Именно использование видеоконференцсвязи позволило оперативно провести предварительное судебное слушание с участием данного лица, в целях перехода к процедуре отбора кандидатов в присяжные заседатели и составления их предварительного списка, с проведением соответствующих сопутствующих проверок (ст. 326 УПК РФ), пока подсудимый готовился к отправке в место расположения суда. Когда другой подсудимый в ходе своего выступления в прениях сторон попытался разбить защитное стекло бокса безопасности в зале судебного заседания, суд вынужден был еще раз прибегнуть к помощи ВКС, чтобы подсудимый мог выступить перед судом с последним словом. Тогда такая возможность была предусмотрена частью 2 ст. 337 и частью 1 ст. 293 УПК РФ. Действия суда не вызвали сомнений в законности обвинительных вердикта и приговора, оставленного без изменений судом апелляционной инстанции [7]. Следуя букве изменений, внесенных Федеральным законом от 29 декабря 2022 года №610-ФЗ, сегодня суду пришлось бы возвратить подсудимого в зал судебного заседания, для выступления с последним словом перед присяжными, на которых его поступок произвел сильное эмоциональное впечатление — женщины испугались и закрывались руками, некоторые мужчины встали со своих мест.

Кроме этого, закон не исключает возможности допроса свидетелей и потерпевших в суде присяжных с использованием ВКС, хотя визуальный контакт (каким бы хорошим ни было качество видеоконференции, реального присутствия в зале суда она пока заменить не может) так же важен для оценки показаний названных лиц, как и для оценки показаний подсудимых.

Действительно необходимым видится присутствие подсудимого в зале суда только на стадии отбора присяжных, в первую очередь для того, чтобы он мог составить свое мнение о кандидатах. Но даже в данном случае, с учетом личности подсудимого и фактических обстоятельств дела, его права в зале суда могут реализовываться защитником, при участии самого подсудимого по видеоконференцсвязи, если единственной альтернативой является лишение подсудимого права на суд присяжных вовсе.

Говоря о расширении применения цифровых технологий в уголовном судопроизводстве, полезно изучить опыт и наработки соседних стран, активно развивающихся на данном поприще. Одной из таких стран является Китайская Народная Республика (далее — Китай, КНР), ставшая второй экономикой мира, третья по размеру территории и первая по численности населения.

Как такового суда присяжных в Китае нет. Однако действует суд с участием народных заседателей. Согласно закону КНР от 27 апреля 2018 года «О народных заседателях», при рассмотрении уголовных дел народные заседатели могут участвовать в сокращенном составе суда (один судья и два народных заседателя) или в расширенном составе суда — три судьи и народные заседатели в количестве от 4 до 7 человек). В расширенном составе суд первой инстанции рассматривает уголовные дела о преступлениях, за совершение которых предусмотрено наказание в виде лишения свободы на срок от 10 лет, бессрочного (пожизненного) лишения свободы, смертной казни, если данные дела обладают существенным общественным влиянием [8], что дает основания для проведения определенных сравнений с судом присяжных в Российской Федерации.

Непосредственно Уголовно-процессуальным законом КНР не регламентируется рассмотрение уголовных дел с использованием цифровых технологий [9]. Правила судебного разбирательства в народных судах в Интернете (далее — Правила) предусматривают возможность дистанционного (онлайн) рассмотрения дел в процедуре ускоренного судебного разбирательства, о замене наказания и об условно-досрочном освобождении, а также дел, которые не могут быть рассмотрены в автономном режиме из-за эпидемии или по другим причинам [10].

Видимо отсутствие четких нормативно-правовых регламентации и ограничения применения дистанционного судебного разбирательства на практике, особенно в условиях распространения коронавирусной инфекции COVID-19, привело к более широкому использованию современных технологий в судебной деятельности. Как отмечают китайские обозреватели, хотя разработчики Правил считают, что дела в рамках простых процедур больше подходят для судебных разбирательств в сети, на самом деле среди всех дел, рассматриваемых в режиме онлайн, дела в рамках сложных процедур составляют более высокий процент. В первой половине 2020 года среди уголовных дел первой инстанции, рассмотренных онлайн в судах Шанхая,

8,34% были рассмотрены в ускоренном порядке; 57,25% были заслушаны в порядке упрощенного судопроизводства; и 34,41% были рассмотрены в соответствии с обычными процедурами. Таким образом, дело может быть рассмотрено онлайн независимо от его сложности [11].

Примерами из судебной практики подтверждается широкое применение в Китае высоких технологий при рассмотрении уголовных дел о тяжких преступлениях в обычных процедурах. В январе 2019 года Шанхайский второй народный суд среднего звена в коллегиальном составе из семи человек (то есть, с участием народных заседателей) в открытом судебном разбирательстве рассмотрел уголовное дело об ограблении. Весь состав суда, прокурор, защитник, обвиняемый были оснащены электронными экранами, где отображался ход судебного разбирательства. На экранах суда и сторон так же отображались область захвата речи, преобразуемой в стенограмму судебного заседания; область интеллектуального захвата — автоматический захват и отображение соответствующей доказательственной информации и материалов на основе вопросов, заданных сторонами и судом; область судебных доказательств — централизованное отображение доказательств, предоставленных суду. Система так же включала функцию проверки доказательств, выстраивания логической цепи доказательств и заключений; обзор дефектов и противоречий в доказательствах [12].

Таким образом, в народных судах Китая не только широко используется система электронного (дистанционного) представления доказательств, но и применяются средства Искусственного Интеллекта (ИИ) для помощи в их обработке и оценке. Правила в принципе не оговаривают обязательного непосредственного присутствия подсудимого в зале суда, а китайская правоприменительная теория отмечает высокую эффективность процессов онлайн, в частности в таких аспектах как: 1) сокращение транзитного времени для доставления подсудимых в суд, поскольку обвиняемые будут участвовать в судебном разбирательстве из центра содержания под стражей, что так же 2) снизит риски побега обвиняемых и повысит безопасность судебного разбирательства, приведёт 3) к повышению коэффициента использования залов судебных заседаний, так как процессы будут начинаться раньше, а время между последовательными судебными процессами в одном зале судебных заседаний будет существенно сокращено [11]. Поэтому, если сегодня дистанционное участие подсудимых в судах с участием народных заседателей в Китае еще может быть не стало обычным явлением, то, видимо, в скором времени станет таковым.

Признавая существующую разницу между классической моделью суда присяжных — с неизбежными и необходимыми российскими особенностями исторически воспринятой в 1864 году Российской Империей и к которой склонен современный отечественный суд присяжных, — и моделью народного представительства в судах Китайской Народной Республики, в эру стремительного развития цифровых технологий, информационного общества, представляется полезным учесть опыт применения современных технических средств в судах Китая. Являясь несомненным достижением в сфере гарантий обеспечения независимости, беспристрастности и справедливости судебной деятельности, суд присяжных заседателей не должен отвергать достижения

научно-технического прогресса и становиться анахронизмом. Очевидно, что личное присутствие подсудимого в зале суда важно, как для присяжных, так и для самого подсудимого. Но когда требования обеспечения безопасности участников судебного разбирательства или иные, столь же важные причины, вынуждают законодателя отказываться от гарантий права на суд присяжных, либо когда подсудимый в судебном заседании пытается оказать воздействие на присяжных заседателей, злоупотребляя своим присутствием, предоставление обвиняемому возможности представлять присяжным доказательства и участвовать в их исследовании дистанционно, находясь в местах предварительного заключения, могло бы способствовать сохранению баланса прав личности и публичных интересов.

Список литературы

1. Совещание судей судов общей юрисдикции и арбитражных судов // URL: http://www.kremlin.ru/ events/president/news/67743 (дата обращения 07.02.2023).

2. Проект Федерального закона № 232773-8 «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации». Пояснительная записка // URL: http://www.consultant.ru (дата обращения 07.02.2023).

3. Собрание законодательства Российской Федерации. 02.01.2023. №1 (часть I). Ст. 57.

4. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский // Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. № 4. С.735-749.

5. Скрипов, С.В. Высокие технологии в уголовном судопроизводстве: реалии, перспективы, пределы применения / С.В. Скрипов // Высокотехнологичное право: генезис и перспективы: материалы III Международной межвузовской научно-практической конференции (24-25 февраля 2022 года, Москва – Красноярск). Национальный исследовательский университет «Московский институт электронной техники»; Красноярский государственный аграрный университет. Красноярск, 2022. 346 с.

6. Постановление Конституционного Суда Российской Федерации от 19.04.2010 г. № 8-П «По делу о проверке конституционности пунктов 2 и 3 части второй статьи 30 и части второй статьи 325 Уголовно-процессуального кодекса Российской Федерации в связи с жалобами граждан Р.Р. Зайнагутдинова, Р.В. Кудаева, Ф.Р. Файзулина, А.Д. Хасанова, А.И. Шаваева и запросом Свердловского областного суда» // URL: http://www.consultant.ru (дата обращения 07.02.2023).

7. Уголовное дело № 2-1/2022 // Архив суда Ямало-Ненецкого автономного округа.

8. Бажанов, П. Закон КНР «О народных заседателях»: краткий обзор / П.Бажанов // URL: https://cnlegal.ru/civil_criminal_administrative_procedure/china_peoples_assessors_law_2018/#more-3724 (дата обращения 07.02.2023).

9. Уголовно-процессуальный закон Китая (вступил в силу 26 октября 2018 года) // URL: https://ru.chinajustticejbserver.com/law/x/criminal-procedure-law-of-china-20181026 (дата обращения 07.02.2023).

10. Правила судебного разбирательства в народных судах в Интернете (2021 г.) // URL: https://ru.chinajusticeobserver.com/law/x/online-litigation-rules-for-people-s-courts-20210616 (дата обращения 07.02.2023).
11. Годун, Ду. Как ведется судебное разбирательство по уголовным делам в Интернете в Китае: пример Шанхая // URL: https://ru.chinajusticeobserver.com/a/how-online-criminal-litigation-works-in-china-the-case-of-shanghai (дата обращения 07.02.2023).
12. 严剑漪 ，梁宗。上海刑事案件智能辅助办案系统首次用于庭审 [Янь Цзяньи, Лян Цзун. Впервые в ходе судебного процесса была использована интеллектуальная вспомогательная система обработки уголовных дел в Шанхае] // URL: https://www.chinacourt.org/article/detail/2019/01/id/3713361.shtml (дата обращения 07.02.2023).

УДК 343.9

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КРИМИНАЛИСТИКЕ

Степаненко Диана Аркадьевна,
доктор юридических наук, профессор
Байкальский государственный университет,
г. Иркутск, Россия
e-mail: diana-stepanenko@mail.ru

Аннотация: *статья посвящена развитию искусственного интеллекта в криминалистической деятельности. В статье описываются основные особенности и виды систем искусственного интеллекта в криминалистике. Рассматриваются возможности использования таких систем в правоохранительной деятельности, а также методы их совершенствования.*

Ключевые слова: *искусственный интеллект, криминалистика, нейронные сети, человек, компьютер, информационные технологии, правоохранительная деятельность.*

ARTIFICIAL INTELLIGENCE IN CRIMINOLOGY

Stepanenko Diana Arkadyevna,
doctor of law, professor
Baikal state university,
Irkutsk, Russia
e-mail: diana-stepanenko@mail.ru

Annotation: *the article is devoted to the development of artificial intelligence in forensic activities. The article describes the main features and types of artificial intelligence systems in criminology. The possibilities of using such systems in law enforcement are considered, as well as methods of their improvement.*

Keywords: *artificial intelligence, criminalistics, neural networks, human, computer, information technology, law enforcement.*

XXI век – век современных технологий, инноваций и развития. В наше время компьютерные технологии, в том числе и искусственные нейронные сети, активно используют в разнообразных сферах человеческой деятельности, криминалистика не стала исключением [1].

Под искусственным интеллектом понимают свойство интеллектуальных систем выполнять такие функции, которые традиционно считаются прерогативой человека. Системы искусственного интеллекта имеют ряд отличительных особенностей:

- структурированность;
- связанность;
- взаимодополняемость;
- внутренняя интерпретируемость – вместе с информацией в базе данных представлены информационные структуры, позволяющие не только хранить знания, но и использовать их.

Так, специализированные машинные алгоритмы изучают материалы дел, классифицируют их и подготавливают к расследованию. Хотя нейронные сети не могут самостоятельно раскрывать уголовные дела, они выполняют всю рутинную работу. Специалисты отмечают, что искусственный интеллект может подготовить дело за несколько дней, тогда как обычный сотрудник может делать это неделями [2].

В практике расследования активно используются автоматизированные системы, позволяющие получать разнообразную информацию о возможных направлениях и методах раскрытия и расследования преступных деяний. Например, система «Блок», система «Маньяк», система «Спрут», система «Сейф», географическая информационная система «Зеркало» и другие. Специалисты отмечаю: «Они (автоматизированные информационные системы) способствуют повышению эффективности управления путем автоматизации деятельности и функционирования правоохранительных органов, позволяют значительно снизить временные затраты на принятие решений в рамках конкретной ситуации, обеспечивают улучшение качества принятого решения. Это становится возможным благодаря тому, что интеллектуальные системы являются результатом накопления всех имеющихся знаний и навыков в той или иной области». Стоит отметить, что рекомендации, выдаваемые машиной, носят консультативный характер, принятие решения всегда остается за человеком.

Искусственный интеллект уже активно используется во многих направлениях криминалистики: от анализа отпечатков пальцев до детального исследования тела [4].

Начнем с первого, анализ отпечатков пальцев с наше время не является чем-то удивительным, базы данных отпечатков – норма, но в XIX веке это был революционный шаг. С развитием технологий у каждого человека появился собственный «генетический паспорт», который помогает понять причастие

человека к совершенному преступлению. Искусственный интеллект сравнивает биоматериалы (ранее загруженные в базу и найденные на месте преступления) и делает заключение о причастности лица к совершенному деянию.

Следующим направлением, в котором активно используются искусственные нейронные сети, является проверка на полиграфе. Сегодня результаты использования полиграфа в первую очередь зависят от опыта допрашивающего специалиста, точности и правильности задаваемых вопросов. Сама технология уже достаточно устарела, в связи с этим появились способы обмануть полиграф, чтобы не допустить этого, необходимо принципиально ее изменить. Так, специалисты предлагают: «К психофизиологическим исследованиям посредством одновременной регистрации параметров дыхания, сердечно-сосудистой активности, сопротивления кожи и других физиологических параметров могут добавиться анализ реакции мозга с помощью возможностей ЭЭГ и МРТ».

Судмедэксперт, который работает с телом, должен обнаружить и зафиксировать все детали, обнаруженные на нём и внутри него. В результате анализа информации он пытается реконструировать «прошлое» – момент преступления. Однако не всегда тело умершего позволяют исследовать. В практике рабаты судмедэксперта максимально этично этот вопрос решает криминалистическая томография, или виртуальная аутопсия. Для исследования тела специалисты используют разнообразные компьютерные и информационные технологии, искусственные нейронные сети выявляют скрытые, неочевидные связи и закономерности [3].

Исходя из всего вышесказанного, можно сделать вывод, что искусственный интеллект, развиваясь с каждым годом, становится не только атрибутом эффективных уголовных процессов, но и передовых криминалистических методов расследования и раскрытия преступлений. Специфика искусственной нейронной сети определяется простотой работы, взаимосвязанностью и взаимозаменяемостью ее элементов. Каждый блок информации, загружаемый в сеть, сопоставляется с другими. На основании этого вырабатывается решение проблемы и пути ее решения. Функционирующая искусственная сеть способна решать весьма сложные задачи, на которые человек потратит гораздо больше времени. Однако надо помнить, что искусственный интеллект — лишь инструмент в руках правоохранительных органов, а не полная замена человека.

Список литературы

1. Ищенко, Е.П. Высокие технологии и криминальные вызовы / Е.П. Ищенко, Н.В. Кручинина // Всероссийский криминологический журнал. 2022. Т. 16. № 2.

2. Степаненко, Д.А. Использование систем искусственного интеллекта в правоохранительной деятельности / Д.А. Степаненко, Д.В. Бахтеев, Ю.А. Евстратова. 2020. Т. 14. № 2.

3. Суходолов, А.П. Big data как современный криминологический метод изучения и измерения организованной преступности / А.П. Суходолов, С.В. Иванцов, Т.В. Молчанова, Б.А. Спасенников // Всероссийский криминологический журнал. 2022. Т. 13. № 5.

4. Суходолов, А.П. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции / А.П. Суходолов, С.В. Иванцов, Т.В. Молчанова, Б.А. Спасенников. 2018.- Т. 12. № 6.

УДК 371

К ВОПРОСУ О ЗАКЛЮЧЕНИИ СМАРТ-КОНТРАКТОВ

Сторожева Анна Николаевна,
кандидат юридических наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: storanya@yandex.ru
Дадаян Елена Владимировна,
кандидат юридических наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: dadaelena@yandex.ru

Аннотация: *в статье рассматривается вопрос не типичного порядка заключения договора, а именно «смарт-контракта». В свете развития информационных технологий в гражданском законодательстве к объектам отнесены цифровые права. Авторы делают попытку анализа обязательств, возникших через блокчейн. Рассуждают, что в мире криптовалюты использование смарт-контрактов не регламентируются нормами гражданского законодательства.*

Ключевые слова: *смарт-контракт, блокчейн, криптовалюта, сделка, приложение, цифровые права, компьютерный протокол, цифровое соглашение.*

ON THE QUESTION OF CONCLUDING SMART CONTRACTS

Storozheva Anna Nikolaevna,
candidate of legal sciences, associate professor
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: storanya@yandex.ru
Dadayan Elena Vladimirovna,
candidate of legal sciences, associate professor
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: dadaelena@ yandex.ru

Abstract: *the article deals with the issue of not a typical procedure for concluding a contract, namely a "smart contract". In the light of the development of information technology in civil law, digital rights are classified as objects. The*

authors make an attempt to analyze the obligations that have arisen through the blockchain. It is argued that in the world of cryptocurrency, the use of smart contracts is not regulated by the norms of civil law.

Keywords: *smart contract, blockchain, cryptocurrency, transaction, application, digital rights, computer protocol, digital agreement.*

В связи со стремительным развитием цифровизации законодатель ввел новое определение объекта гражданских правоотношений как «Цифровые права», под которыми понимаются «названные в таком качестве в законе обязательственные и иные права, содержание и условия, осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Осуществление, распоряжение, в том числе передача, залог, обременение цифрового права другими способами или ограничение распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу» (ст. 141.1) [1].

Так, осуществление цифровых прав сегодня приобретает особую актуальность.

Общий порядок заключения гражданско-правовых договоров закреплен в Гражданском кодексе Российской Федерации.

Однако, стремительный интерес в мире к криптовалюте позволяет участниками гражданских правоотношений использовать собственный способ реализации смарт-контрактов.

Нормы гражданского законодательства не регулируют сегодня цифровые соглашения.

Смарт – контракты создаются как приложение, работающее на блокчейне.

Так, появляются новый вид взаимодействия контрагентов через блокчейн без необходимости определенного доверия друг к другу.

Смарт-контракт – «цифровое соглашение», в котором устанавливается набор правил, иначе говоря, компьютерный код, который копирует и обрабатывает все ноды сети.

Под «нодами» понимаются сетевые узлы как точка, в которой сообщения могут быть созданы, получены или переданы. Выделяют отдельные типы узлов Биткойна. Так, к ним относятся: полные узлы (Full Nodes), суперузлы (Super Nodes), майнер узлы (Miner Nodes) и SPV клиент.

Очевидно, что при несоблюдении условий (конкретных правил) контрагентом смарт –контракта это может привести к его аннулированию.

При соблюдении всех правил контрагент может быть избавлен от необходимости в посредниках, значительно снижая расходы на операции.

Заметим, что технология смарт-контрактов была впервые еще описана в 1990-х годах. Так, Ник Сабо определил смарт – контракт как «компьютерный протокол, который самостоятельно проводит сделки и контролирует их исполнение с помощью математических алгоритмов».

Таким образом, смарт-контракт работает как детерминированная программа, которая выполняет определенные действия, когда соблюдены

заданные условия. Очевидно, что смарт-контракт не определен, сегодня законодателем в юридическом смысле.

Заключить смарт-контракт возможно в различных сетях, к примеру, Ethereum, BNB, Cardano и др. где они отвечают за выполнение операций между пользователями (адресами). Смарт-контракты управляются программным кодом, а личные аккаунты – пользователями (контрагентами).

Структурно смарт-контракты состоят из кода (определенных условий выполнения) и двух публичных ключей. Один, из которых, предоставлен создателем контракта, другой представляет сам контракт, являясь цифровым идентификатором.

Выполнение смарт-контракта осуществляется по средством блокчейн-транзакции, которая активируется при инициации личным аккаунтом. Последовательность действий смарт-контракта возможна всегда с личного аккаунта пользователя.

Авторы обращают внимание, что самым распространёнными являются денежные рынки, которые построенные на блокчейне и представляют собой важнейшую финансовую инфраструктуру, которая при помощи смарт-контрактов соединяет кредиторов, желающих получить дополнительную прибыть от своих активов, с заемщиками, нуждающимся в свободном капитале. Это позволяет всем своим участникам получить дополнительную пользу от крипто активов, и участвовать одновременно на стороне и поставщика, и потребителя.

Вопросы использования в профессиональной деятельности различных информационных сервисов уже поднимались авторами настоящей статьи. Так, информационные сервисы значительно оптимизируют работу не только лиц, ответственных за размещение информации на таких информационных ресурсах, но и лиц, для которых важна общедоступная открытая информация для решения актуальных и повседневных задач профессиональной деятельности [2, с. 31].

Отельного внимания заслуживает и форма смарт-контракта, которая имеет значение, она зависит от автоматизации, а именно она показывает, может ли цифровое соглашение функционировать самостоятельно или необходимо получить дополнительный бумажный вариант контракта.

В практике выделяют определенные виды смарт-контрактов по форме: автоматизированные (без бумажного носителя); частично автоматизированные (необходима копия смарт-контракта на бумажном носителе); автоматизированные преимущественно в хранилище.

Следовательно, подводя итоги исследования, авторы отмечаю, что новый вектор цифровых возможностей позволяет сегодня участниками заключать смарт – контракты и без специального гражданского регулирования. Думаем, что введение в гражданское законодательство понятия «цифровых прав» это лишь первый шаг законодателя для дальнейшего регулирования, в том числе сделок с цифровыми правами.

Список литературы

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 г. № 51-ФЗ (ред. от 16.04.2022 г.) // СПС «КонсультантПлюс: Законодательство».

2. Дадаян, Е.В. К вопросу о роли информационных сервисов в решении задач профессиональной деятельности / Е.В. Дадаян, А.Н. Сторожева // Применение в юриспруденции современных технологий: актуальные вопросы теории и практики. Материалы международной научно-практической конференции. Красноярск, 2021. С.31-35.

УДК 371

ЦИФРОВЫЕ АКТИВЫ И ИХ ЗАЩИТА

Сторожева Анна Николаевна,
кандидат юридических наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail:storanya@yandex.ru

Дадаян Елена Владимировна,
кандидат юридических наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: dadaelena@yandex.ru

Аннотация: *в статье поднимаются вопросы нового обращения и выпуска цифровых финансовых активов (ЦФА) на финансовых рынках. Цифровые активы также представляют новый вид трансформации цифровых прав, включая одновременно и право требовать передачи исключительных прав на такие результаты. Авторы анализируют порядок и возможные способы защиты цифровых активов.*

Ключевые слова: *цифровые финансовые активы, финансовый рынок, оператор обмена, цифровые права, сделки, оператор информационной системы, номинальный счет, смарт-контракт.*

DIGITAL ASSETS AND THEIR PROTECTION

Storozheva Anna Nikolaevna,
candidate of legal sciences, associate professor
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: storanya@yandex.ru

Dadayan Elena Vladimirovna,
candidate of legal sciences, associate professor
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: dadaelena@ yandex.ru

Abstract: *the article raises issues of new circulation and issuance of digital financial assets (DFA) in financial markets. Digital assets also represent a new kind of transformation of digital rights, including at the same time the right to demand the transfer of exclusive rights to such results. The authors analyze the procedure and possible ways to protect digital assets.*

Keywords: *digital financial assets, financial market, exchange operator, digital rights, transactions, information system operator, nominal account, smart contract*

Финансовый рынок сегодня имеет новые цифровые возможности. С введением в 2020 году Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [1].

Теперь выпуск и обращение цифровых финансовых активов возможно через информационную систему.

Стремительное развитие цифровизации подвергло законодателя ввести новое определение объекта гражданских правоотношений как «Цифровые права», под которыми понимаются «названные в таком качестве в законе обязательственные и иные права, содержание и условия, осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Осуществление, распоряжение, в том числе передача, залог, обременение цифрового права другими способами или ограничение распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу» (ст. 141.1) [2].

Так, осуществление цифровых прав также возможно через информационную систему.

Отметим, что функционированием информационных систем осуществляет оператор информационной системы, деятельность которого заключается в выпуске и учете ЦФА.

Вся работа построена на совершение сделок с ЦФА, проведение расчётов по сделкам с ЦФА, включающих денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, право требовать передачи эмиссионных ценных бумаг, а также с периодическими выплатами по таким цифровым финансовым активам, погашением таких цифровых финансовых активов используя номинальный счет. Оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, вправе открыть в российской кредитной организации номинальный счет, бенефициарами по которому являются лицо, выпускающее цифровые финансовые активы, обладатель цифровых финансовых активов, лицо,

имеющее намерение приобрести цифровые финансовые активы, номинальный держатель цифровых финансовых активов (ст. 5.1. ФЗ № 259).

Банком России утверждены Правила информационной системы, согласно которых определены права и обязанности оператора, пользователей, порядок привлечения операторов обмена ЦФА, номинальных держателей и валидаторов транзакций.

Так сегодня в России действует национальная блокчейн-сеть «Мастерчейн», которая предназначена для передачи цифровых ценностей и информации о них между участниками. Она использует кодовую базу блокчейн-сети Ethereum, но при этом доработана с учетом требований к российской криптографии, процессу идентификации пользователей и безопасному процессу масштабирования. Логотип «Мастерчйен» в 2023 году выглядит так:

MASTER CHAIN [3]

Основной функционал платформы Мастречейн заключается в механизмах аллокации внутренних расчётных единиц (токенов), регистрация объектов токенизации; учетных записей (счетов), обеспечивающих адресацию транзакций, идентификацию, верификацию и авторизацию ее участников, и возможность депонирования токенов; проведения контролируемой передачи или обмена прав собственности на финансовые инструменты и активы (объекты токенезации) с выполнением соответствующего учета; поддержки оплаты услуг участников, поддерживающих работу сети, а также механизмы взимания комиссий с инициаторов транзакций; идентификация счетов участников на основе открытых ключей участников; исполнение смарт-контракта [3].

Вопрос защиты – это один из основных для банков процессов внедрения новых технологий. Блокчейн это самая защищенная, надежная и прозрачная технология. Она использует электронную подпись и средства криптографической защиты информации, которые требуют прохождения процедур сертификации безопасности. Так, Мастерчейн - это система с несколькими уровнями защиты, начиная с обеспечения защиты всех сетевых соединений и включая защиту самих данных. Все конфиденциальные данные хранятся в отдельном хранилище пользователя, доступ к которому предоставляется через средства ЭП, а для обеспечения безопасности используется ГОСТ-криптография. Также в Мастерчейне проработана система контроля доступа в сеть, которой нет у публичных блокчейн-платформ.

Однако, говоря о безопасности нельзя не упомянуть о смарт-контрактах, которые могут быть уязвимы для банковской сферы.

Оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, обязан в соответствии с гражданским законодательством возместить убытки пользователям этой информационной системы, возникшие вследствие: утраты информации, хранящейся в

информационной системе, об объеме цифровых финансовых активов, принадлежащих их обладателям, и (или) о самих обладателях цифровых финансовых активов; сбоя в работе информационных технологий и технических средств информационной системы; предоставления пользователям информационной системы недостоверной, неполной и (или) вводящей в заблуждение информации об информационной системе, о правилах работы информационной системы и об операторе информационной системы; нарушения оператором информационной системы правил работы информационной системы, в том числе нарушения требований бесперебойности и непрерывности функционирования информационной системы; несоответствия информационной системы требованиям законодательства.

Следовательно, говоря сегодня о финансовых цифровых активах, участники гражданских правоотношений должны четко осознавать, что отношения выходят на новый уровень цифровых отношений, субъекты которых, к сожалению не все готовы к таким взаимоотношениям.

Очевидно, что участниками информационной системы станут не все участники гражданских правоотношений, а лишь те которые являются активными пользователями информационных систем.

Список литературы

1. Федеральный закон от 31.07.2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс: Законодательство».

2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 г. № 51-ФЗ (ред. от 16.04.2022 г.) // СПС «КонсультантПлюс: Законодательство».

3. URL: https://www.tadviser.ru/index.php (дата обращения 07.03.2023).

УДК 343.98.068

РЕАЛИИ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПРАКТИКЕ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ

Халиков Аслям Наилевич,
доктор юридических наук, профессор
Институт права Уфимского университета науки и технологий,
г. Уфа, Россия
e-mail: han010@yandex.ru

Аннотация: *в статье проводится обзор применения цифровых технологий в работе следователей, что не претерпело существенных изменений с середины 90-х годов XX века. Предлагается с помощью цифровых технологий создать оптимальные условия следственной деятельности для получения любой информации, в основном из государственных структур, с целью их приобщения к уголовному делу. Это относится к отношениям со справочными системами правоохранительных органов, медицинскими учреждениями, судами и иными государственными органами. Данные изменения требуют правовых и технических преобразований, а следовательно создания отдельной системы истребования и получения информации следователями путем применения цифровых технологий.*

Ключевые слова: *банки данных; запросы; информация; поручения; следователь; следственные органы; цифровые технологии.*

THE REALITIES OF THE USE OF DIGITAL TECHNOLOGIES IN THE PRACTICE OF THE ACTIVITIES OF THE PRELIMINARY INVESTIGATION BODIES

Khalikov Aslyam Nailevich,
doctor of law, professor
Institute of law of Ufa University of Science and Technology,
Ufa, Russia
e-mail: han010@yandex.ru

Abstract: *the article reviews the use of digital technologies in the work of investigators, which has not undergone significant changes since the mid-90s of the twentieth century. It is proposed to use digital technologies to create optimal conditions for investigative activities to obtain any information mainly from government agencies in order to involve them in a criminal case. This applies to relations with the reference systems of law enforcement agencies, medical institutions, courts and other government agencies. These changes require legal and technical transformations, and therefore the creation of a separate system for requesting and obtaining information by investigators through the use of digital technologies.*

Keywords: *data banks; requests; information; instructions; investigator; investigative bodies; digital technologies.*

Активно развивающиеся цифровые технологии в виде компьютеров, мобильных телефонов со всевозможными опциями, печатными устройствами (принтеры, ксероксы) находят свое применение и в следственной деятельности. В этом отношении следует вспомнить, что различные цифровые устройства впервые в России в массовом порядке в следственных органах стали применяться примерно с 1995 года. В это время практически всех следователей снабдили компьютерами, принтерами, чуть позже руководителям следственных органов дали мобильные телефоны. В следственных подразделениях появились ксероксы, начиная с простых устройств и завершая более мощными. В содержание компьютерных баз были заложены мобильные программы для следователей с образцами процессуальных актов, словесного портрета и определенных методических указаний по алгоритмам расследования конкретных видов преступлений. И, в общем то, принципиальных каких-либо новых технических устройств с применением цифровых технологий у следователей до настоящего времени не стало больше. Единственно, следует добавить, что каждый следователь или дознаватель в настоящее время имеет купленный за свой счет мобильный телефон с опциями, количество которых зависит от их материальной обеспеченности. И следователи имеют в своем распоряжении аппаратуру аудио, видео и фото фиксации.

Кроме этого в обеспеченность цифровыми технологиями следователей входят электронные устройства в виде «Мобильного криминалиста» с программным обеспечением для извлечения данных с электронных устройств, которые в основном эффективно применяются для извлечения информации с памяти мобильных телефонов и иной цифровой аппаратуры. Служба криминалистов имеет квадрокоптеры, используемые для поисковых мероприятий и осмотров определенных участков местности и различные транспортные средства, оборудованные для успешной работы следственных служб. Последние перечисленные устройства имеются в центральных аппаратах следственных управлений и, конечно, рядовым следователям нет необходимости в их регулярном пользовании. Также, в плане цифрового оснащения деятельности органов расследования, можно сказать еще о различных информационных банках данных, имеющихся в основном в органах внутренних дел, содержание которых регулируется ст. 17 Федерального закона «О полиции». В названных банках данных активно задействованы цифровые технологии с целью системного учета криминальной и иной информации, ее анализа и извлечения. Напрямую следователь информацию из названных банков данных использовать не может, а получает информацию только в ответ на поручение в адрес информационных центров органов МВД.

Нельзя не сказать о возможности производства ряда следственных действий (допрос, очная ставка, опознание) с помощью систем видео-конферепнц-связи, но, что применяется на практике редко и при этом по

тактике перечисленных следственных действий могут возникнуть существенные проблемы.

Тем самым, предметы цифровых технологий в деятельности следственных подразделений и подразделений органов дознания, которые имели место с середины 90-х годов XX века, используются в основном и до настоящего времени. Речь идет только о более качественном оснащении программных устройств компьютеров, печатающих механизмов, мобильных телефонных устройств, аудио, видео и фото принадлежностей. Поэтому говорить на сегодня относительно деятельности следователей о некой цифровой криминалистике, искусственном интеллекте, цифровых программах расследования преступлений вряд ли есть основания.

Как ни парадоксально, но при наличии перечисленных цифровых устройств, качество которых улучшается регулярно, время, затрачиваемое следователями на расследование уголовных дел, постоянно увеличивается. Следователи перестали удивляться, что их рабочий день почти ежедневно продолжается до 22 - 23 часов вечера, у них нет выходных, пол отпуска они проводят, завершая расследуемые дела, ездят они по служебным делам на своих автомобилях, а электронные устройства часто применяют за свой счет (бумага, картриджи, батарейки и т.д.). Автор работал следователем 15 лет с начала 90-х годов прошлого века, но режим работы всегда был нормальный: вечера я проводил с семьей, выходные у меня всегда были, если не считать чрезвычайных происшествий в виде убийств.

Однако целью наших суждений является не критика состояния следственной службы в настоящее время, что требует отдельного разговора и улучшения, если не радикального пересмотра организации деятельности следователей СК РФ, МВД РФ И ФСБ. В данном случае хотелось бы внести предложения, что конкретно и, самое главное, реально возможно изменить в деятельности следователей с целью облегчить расследование уголовных дел с помощью применения цифровых технологий. Революции в данном случае трудно совершить, однако практика применения цифровых технологий в сфере хотя бы государственного сектора правовых отношений в России позволяет оптимизировать деятельность следственных органов.

В первую очередь отметим, что содержание уголовного дела - это информация. К данной информации предъявляется процессуальное правило с тем, чтобы данная информация была доказательственной, то есть которую следователь, прокурор, судья могли использовать для вынесения обоснованного и законного решения. В то же время много информации по уголовному делу не требует применения особой криминалистической тактики, когда необходимо активное участие в ее поиске, получении, исследовании и оценке самим следователем. В этом случае следователь вполне может получить подобную информацию исключительно с помощью применения цифровых технологий, а не «бегать за ней, высунув язык» по городу или области (республике, краю).

Только с помощью электронных устройств с использованием, допустим, цифровой подписи, возможно запрашивать и получать по России следующие

документы: приговоры из судов, справки с психодиспансеров и наркодиспансеров, справочные сведения из банков, налоговых учреждений, медицинских организаций. С применением цифровых технологий возможно отправлять поручения в оперативно-розыскные органы, уведомления в ИВС и в изоляторы временного содержания, требования в конвойные службы. Только следователи знают, сколько отнимает времени направление и получение перечисленных справок, сведений и поручений. Хотя все это можно выполнять в электронной форме, находясь в кабинете следователя и без посещения названных организаций. Все перечисленные и иные документы в большей части не влияют на доказывание существенных обстоятельств преступления и поэтому без ущерба для целей правосудия они могут быть получены исключительно цифровым способом.

Далее, значительное количество времени теряется следователями при посещении следственных изоляторов. Конечно, идеальным способом решения данной проблемы будет увеличение числа следственных комнат, что устранит абсурдные очереди в изоляторы. Однако ФСИН - это особый орган, который в ряде случаев упорно не видит давно возникшей проблемы, считая по Канту, что ФСИН это «вещь в себе», то есть вне внешнего восприятия и внешних вопросов со стороны следственных органов. Но тогда необходимо, как и в случае судебного рассмотрения дел (апелляция, кассация) обеспечить условия для «цифрового общения» следователя со следственно-заключенным в присутствии адвоката, который будет находиться, как и следователь, в кабинете следователя (или по выбору в следственном изоляторе), а подследственный в изоляторе. В этом случае подтверждением показаний подозреваемого или обвиняемого будет подпись адвоката и видеозапись следственного действия.

Возможно предложить и ряд других процессуальных или следственных действий, которые возможно произвести с помощью электронных устройств без ущерба для доказывания обстоятельств преступления, а значит прав и интересов субъектов уголовного процесса. Это, например, получение некоторых результатов оперативно-розыскной деятельности, направление поручений в другие следственные органы, получение иных справочных сведений.

В то же время мы категорически против применения цифровых технологий для получения доказательств в опосредованной форме, когда необходимо личное участие следователя. В этом случае мы весьма скептически относимся к производству очной ставки, а, тем более, к опознанию, путем применения систем видео-конференц-связи, что предусмотрено ст. 189-1 УПК РФ. Особенно не ясно, каким образом проводить опознание вне непосредственного участия его участников в данном следственном действии, когда, во-первых, любая ошибка может привести к некачественным результатам, а, во-вторых, сами результаты опознания могут оказать значительное негативное влияние на совокупность доказательств по установлению виновного (или невиновного) лица по уголовному делу.

Соответственно, задачей специалистов в сфере цифровых технологий применительно к деятельности правоохранительных органов, и, в частности,

следственных служб, является создание автоматизированной цифровой системы по истребованию и получению следователями всей совокупности требуемой информации по уголовному делу. То есть получения данных сведений следователями «не выходя из кабинета». Допустим, на сегодня созданы подобные системы в медицине (так называемая, про-медицина), когда любой лечащий врач может найти интересующие его сведения по пациенту в любом медицинском учреждении региона или России. Такая же система должна быть создана в правоохранительной деятельности, когда с помощью пароля и иных охранных обозначений и только с применением компьютерной техники возможно получить и приобщить к уголовному делу сведения о психо- и наркоучете, о судимости, о привлечении к административной ответственности, о наличии банковских вкладов, о состоянии налогового учета, об обращении в медицинские учреждения и т.д. Также цифровые технологии необходимы для выполнения следственных поручений в органы оперативно-розыскной деятельности, в следственные изоляторы, в конвойные службы. Также и с судом возможен обмен информацией по запросам и получению приговоров и иных судебных решений с целью их использования в материалах уголовного дела, когда судебные решения, заверенные электронным способом, могут быть приобщены к уголовному делу, то есть без «мокрой печати». В целом же речь идет о создании единой цифровой системы любых запросов следователей и их обязательного выполнения в таком же цифровом режиме в муниципальных, региональных и государственных организациях, учреждениях и предприятиях. Затем такую систему можно расширить и до коммерческих организаций.

Все названные и иные возможные предложения по активному использованию информации при расследовании уголовных дел требуют создания комплекса системного цифрового обеспечения работы следователя без ущерба, с одной стороны, правам и интересам граждан и, с другой стороны, исключая раскрытия личной и следственной тайны в процессе обмена названными сведениями. Разумеется, такие предложения требуют их реализации в соответствующих правовых актах как УПК РФ, федеральные законы «О полиции», «О Следственном комитете РФ», «О ФСБ» и т.д. Иными словами проблема состоит в системном нормативном и техническом изменении режима работы следственных органов при расследовании уголовных дел при получении обязательной информации по уголовному делу.

УДК 343.9

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАССЛЕДОВАНИИ ОТДЕЛЬНЫХ ВИДОВ ПРЕСТУПЛЕНИЙ

Харебин Денис Дмитриевич,
старший преподаватель
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: expertus.2014@yandex.ru

Аннотация: *в статье рассматриваются вопросы касающиеся использования правоохранительными органами информационных и компьютерных технологий в процессе раскрытия и расследования преступлений.*

Ключевые слова: *криминалистика, цифровая криминалистика, цифровые технологии, информационные технологии, преступления с применением цифровых технологий, метод аналогии, компьютерные программы, предварительное расследование, оперативно-розыскная деятельность, расследование, раскрытие преступлений, средства цифровизации.*

THE USE OF INFORMATION TECHNOLOGIES IN THE INVESTIGATION OF CERTAIN TYPES OF CRIMES

Kharebin Denis Dmitrievich,
senior lecturer
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: expertus.2014@yandex.ru

Abstract: *the article deals with issues related to the use of information and computer technologies by law enforcement agencies in the process of detecting and investigating crimes.*

Keywords: *criminalistics, digital criminalistics, digital technologies, information technologies, crimes with the use of digital technologies, analogy method, computer programs, investigation, crime solution, means of digitalization.*

Повышение эффективности работы правоохранительных органов в настоящее время напрямую зависит от интеграции всех достижений науки XXI века. Поскольку «век цифровизации», привнёсший в нашу жизнь огромное количество компьютерных технологий, цифровых инструментов и гаджетов облегчает не только нашу повседневность и упрощает задачи поиска всевозможной информации, но и с лёгкостью помогает преступным элементам в их противопровной деятельности. Но не смотря на это, широкий спектр инструментов, таких как специальное программное обеспечение,

информационные базы и массивы, средства распознавания личности и многое другое, стоит на страже нашей безопасности. Они помогают следственным и оперативным работникам в процессе раскрытия и расследования преступлений направленных на различные сферы нашей жизни [1].

Использование общепринятого программного обеспечения, такого как текстовые редакторы, существенно повышает качество информационно-аналитической работы следственных органов и оперативных сотрудников. Так текстовые редакторы, позволяют повысить качество и ускорить процесс подготовки процессуальных документов. Поэтому процесс решения аналитических задач занимает не такой большой промежуток времени, которое особенно ценно для раскрытия преступлений по «горячим» следам.

Так же, для решения информационно-аналитических задач, используются всевозможные автоматизированные информационно-поисковые системы [2, с. 32], которые подразделяются на три основных типа: Автоматизированные информационно-поисковые системы оперативно-розыскного и профилактического назначения, действующие в республиках, краях и областях РФ (учеты местного уровня); Централизованные автоматизированные системы оперативно-розыскного назначения Центра криминальной информации ГИАЦ МВД РФ а так же Экспертно-криминалистические автоматизированные информационные поисковые системы (таб.1). Данные системы позволяют формировать и систематизировать информацию направленную на получение всевозможных сведений, необходимых оперативным и следственным работникам для выявления лица или лиц, причастных к совершению противоправных преступных деяний.

Таблица 1. Виды автоматизированных информационно-поисковых систем

Автоматизированные информационные поисковые системы	
Название	***Назначение***
I.Автоматизированные информационно-поисковые системы оперативно-розыскного и профилактического назначения, действующие в республиках, краях и областях РФ (учеты местного уровня)	
«АБД-область»	Предназначена для получения сведений оперативного учёта касающихся лиц, поставленных на учёт по розыскным делам и делам оперативной проверки. Так же АБД содержит в себе информацию о наличии или отсутствии материалов о проверяемом лице; биографические сведения о проверяемом лице; приметах и способах совершения преступлений и ряд другой информации.
АИПС «Дорожное движение»	Предназначена для получения сведений об автотранспортных средствах (подсистема «Автомобиль»); данных водительских удостоверений (подсистема «Водитель»); делах о ДТП (подсистема «ДТП»), данных об угонах, похищения, задержаниях автотранспортных

	средств (подсистема «Автопоиск»), а так же данных о похищенных либо утерянных тех.паспортах.
II.Централизованные автоматизированные системы оперативно-розыскного назначения Центра криминальной информации ГИАЦ МВД РФ	
АБД-Центр	Предназначена для получения сведений оперативного учёта о лицах, состоящих на действующем или архивном учетах; судимых за совершение особо опасных преступлений; нераскрытых преступлениях и пр.
АИПС «Оружие»	Предназначена для получения сведений касательно утраченного, похищенного и выявленного огнестрельного оружия, боеприпасов и взрывчатых веществ.
АИПС «Антиквариат»	Предназначена для получения сведений о похищенных, выявленных или сданных как находка предметах, представляющих историческую, художественную или научную ценность.
АИПС «ВР-оповещение»	Предназначена для получения сведений о лица, находящихся в федеральном розыске; пропавших без вести и пр.
АИПС «Опознание»	Предназначена для получения сведений о лицах, пропавших без вести; о неопознанных трупах; о неизвестных больных и детях.
АИПС «ОВИР-криминал»	Предназначена для получения сведений об иностранцах и лицах без гражданства, в том числе: совершивших преступления или административное правонарушение и пр.
АИПС «Автопоиск»	Предназначена для получения сведений о всех угнанных, задержанных, похищенных и обнаруженных бесхозных автотранспортных средствах.
АИПС «Грузы-ТМ»	Предназначена для получения сведений о хищениях, недостачах груза и багажа на железнодорожном транспорте.
АИПС «Аэропорт-2»	Предназначена для получения сведений касательно авиарейсов; утраченных паспортов и выявления разыскиваемых преступников, пытающихся покинуть территорию страны.
III.Экспертно-криминалистические автоматизированные информационные поисковые системы	
АДИС «Папилон», «Дакто», «Узор» и пр.	Предназначены для получения сведений оперативных проверок значительных массивов дактилоскопических материалов.
АИПС «Клеймо», «Пламя», «Боеприпасы», «Оружие», «Ружье», «Патрон» и пр.	Предназначены для получения сведений о маркировочных обозначения и клейма охотничьего оружия и боеприпасов; о автоматических пистолетах с фиксацией их внешнего вида а так же точным описание и характеристикам автоматических пистолетов, винтовок, автоматов и карабинов и пр.

АИПС «Облик», «Faces»	Предназначенs для получения сведений о приметах лиц, находящихся в розыске и ранее судимых.
АБД – автоматизированный банк данных; АИПС – автоматизированная информационно-поисковая система; АДИС – автоматизированная дактило-поисковая система	

Эффективная работа правоохранительных органов по раскрытию и расследованию преступлений в первую очередь зависит от сбора информации, которая необходима им для формирования образа подозреваемого, что в свою очередь способствует скорейшей идентификации и поимки виновного лица. Для решения этой проблемы правоохранители используют всевозможное программное обеспечение и оборудование. Так, экспертно-криминалистические автоматизированные информационные поисковые системы, такие как АДИС «Папилон» (рис.1) и АИПС «Faces», позволяют идентифицировать лиц, причастных к совершению преступлений на основании вещественных доказательств и информации полученной от свидетелей.

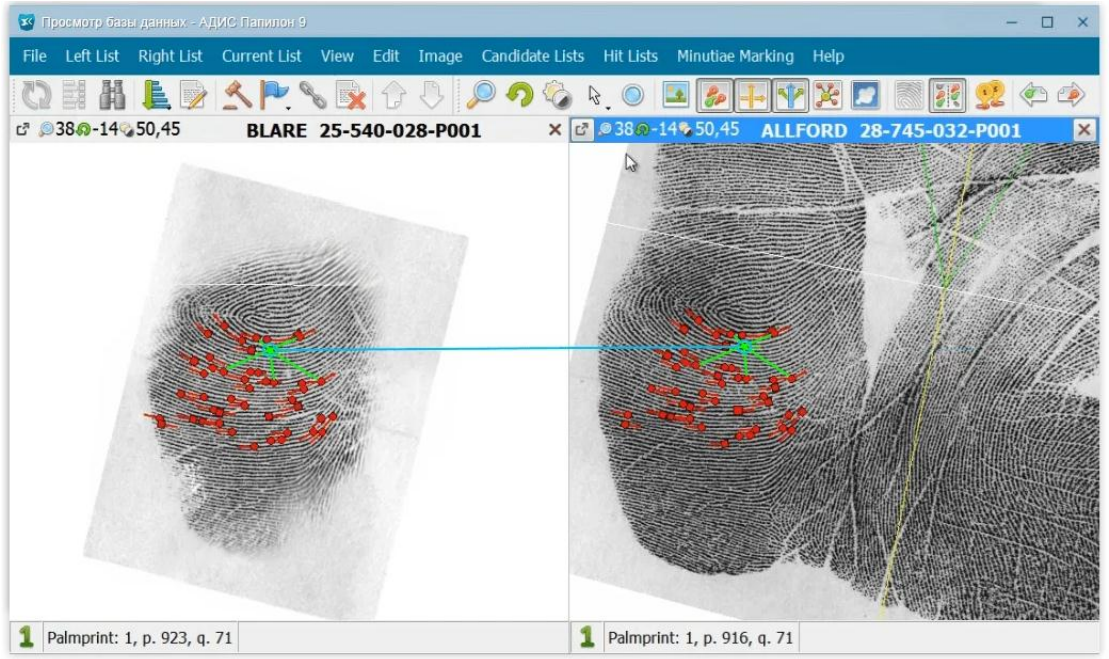


Рис. 1. Скиншот интерфейся базы данных АДИС «Папилон»

Например, информационно-поисковая система «Спрут» позволяет выявлять и моделировать преступные связи при расследовании преступлений, совершенных организованными преступными группировками. Так же для эффективного сбора криминалистически значимой информации для расследования убийств следователи используют программное обеспечение «ФОРВЕР Следователь», которая позволяет сопоставлять большой массив информации по заданным ключевым параметрам для поиска аналогичных преступлений [3].

Применение таких программ как «Digital Forensics» и «3D Свидетель» [4] позволяет производит фиксацию обстановки мест происшествия, а так же использовать визуальную реконструкцию с дальнейшим построение схем мест

происшествий. Это позволяет более детально проводить осмотры мест происшествий и является прекрасным дополнением к фото и видео фиксации, проводимым в процессе осмотра места происшествия (рис. 2).

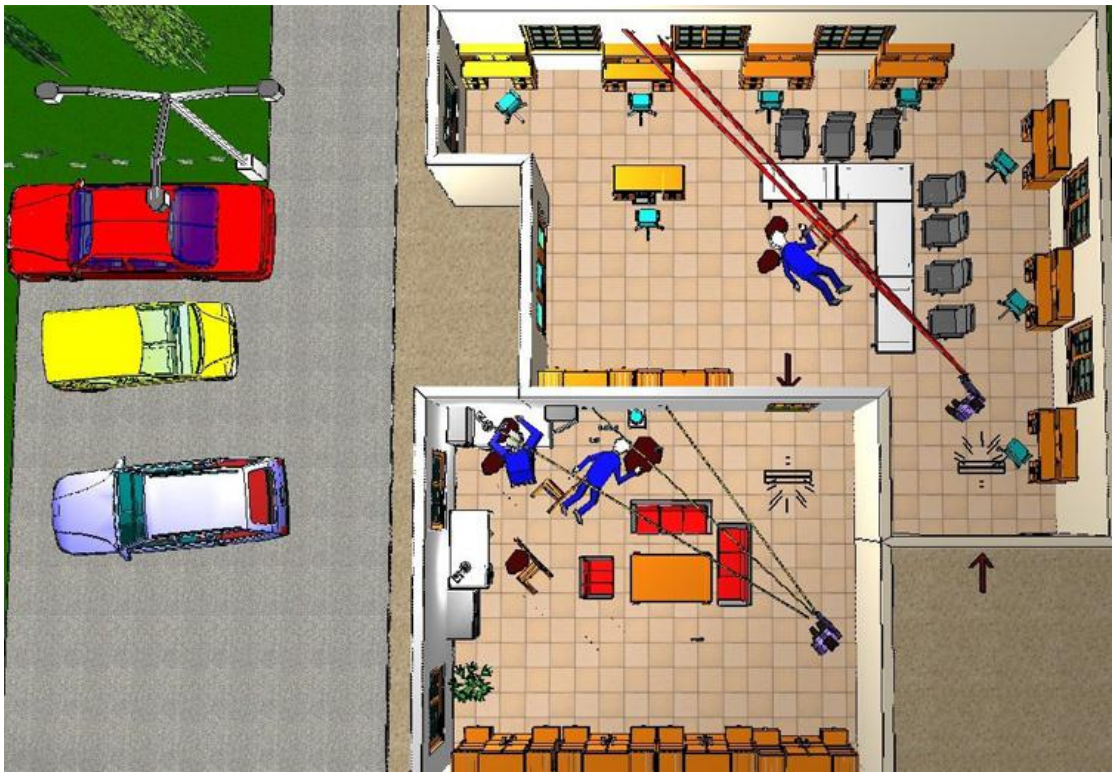


Рис. 2. Скиншот программного обеспечения «3D Свидетель» (Криммедтех) с визуальной реконструкции места преступления

Источником ценной информации для процесса расследования преступных деяний является аппаратно-программный комплекс «Безопасный город», который представляет из себя экосистему состоящую из городского видеонаблюдения, аналитики, биометрического распознавания, обнаружения, геоинформационной системы, фото и видео фиксации, датчиков охраны и многих других средств автоматизации городского пространства [2, с. 33-34].

Так же, оперативными работниками достаточно широко и успешно применяются аппаратно-комплексные программы, позволяющие исследовать мобильные телефоны, планшеты и смартфоны. Среди таких программ выделяются «Мобильный Криминалист» (рис.3) и «UFED».

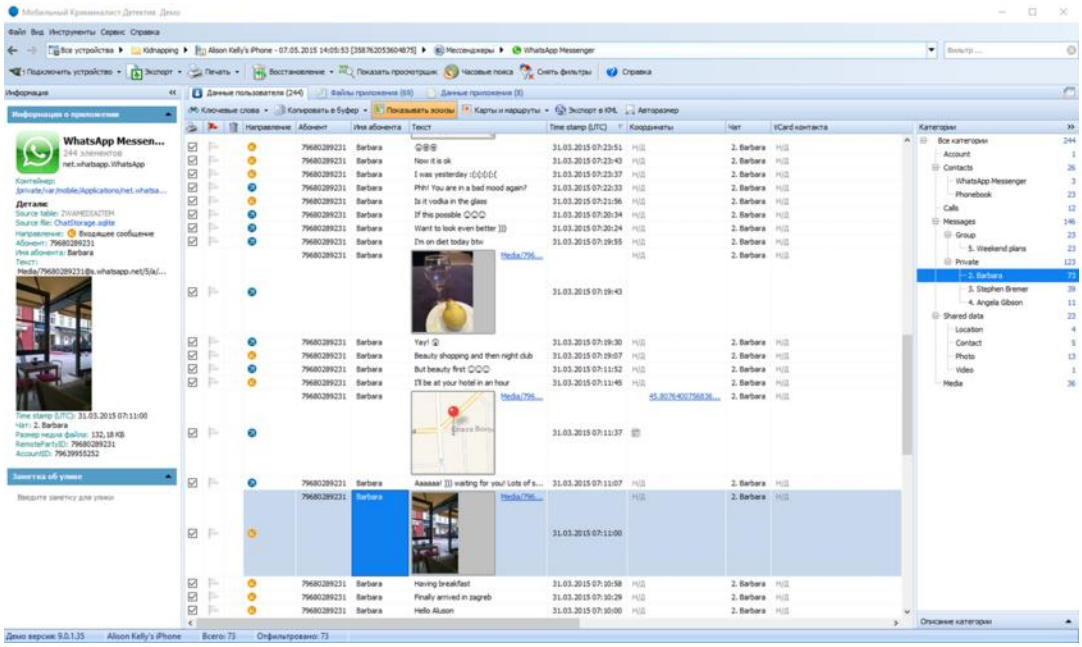


Рис.3. Просмотр данных мессенджера WhatsApp с помощью аппаратно-комплексной программы «Мобильный Криминалист»

С помощью данных аппаратно-комплексных программ возможно получение детальной информации об устройстве, исходящих и принятых звонках / SMS сообщениях / сообщениях электронной почты и мессенджеров, а так же данных адресной книги, заметок, задач, голосовых записях, логинах и паролях приложений и прочей информации хранящейся на телефоне, даже если она была заранее удалена с устройства [5, с. 163].

В заключении стоит отметить что вышеназванные инструменты не исчерпывают всего перечня инструментов направленных на помощь оперативным и следственным работниками в процессе раскрытия и расследования преступлений. Такие инструмент способствуют правильному построения тактики следственных и оперативно-розыскных мероприятий и позволяют скорейшему и успешному завершению расследований отдельных видов преступлений.

Список литературы

1. Пастухов, П.С. Использование информационных технологий для обеспечения безопасности личности, общества, государства / П.С. Пастухов, М. Лосавио // Вестник Пермского университета. Юридические науки. 2017. Вып. 36. С. 231-236.

2. Дубынин, Е.А. Возможности использования цифровых технологий в раскрытии и расследовании преступлений: практические аспекты / Е.А. Дубынин, Е.Е. Космодемьянская // Вестник Сибирского юридического института МВД России. 2022. № 1 (46). С.31-36.

3. Толстолуцкий, В.Ю. Компьютерная программа «ФОРВЕР Следователь» повышает эффективность обучения на криминалистическом полигоне / В.Ю. Толстолуцкий // Вестник Нижегородского университета им.

Н.И. Лобачевского. 2013. № 3 (2). С. 211-215.
4. Криммедтех // URL: https://kmtkazan.ru/node/256 (дата обращения 01.02.2023).
5. Соловьева, С.М. Применение цифровых технологий в криминалистике / С.М. Соловьева // Молодой ученый. 2019. № 51 (289). С. 161-164.

УДК 343

ИСПОЛЬЗОВАНИЕ ЛИПОЛЬНОГО АНАЛИЗА ДЛЯ УСТАНОВЛЕНИЯ ОБСТОЯТЕЛЬСТВ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Храмов Сергей Михайлович,
кандидат юридических наук, доцент
Брестский государственный университет им. А. С. Пушкина,
г. Брест, Республика Беларусь
e-mail: khramausiarhei@gmail.com

Аннотация: *в статье рассмотрен вопрос установления обстоятельств совершения киберпреступлений. В качестве вспомогательного инструмента использована авторская методика липольного анализа. Приводится схематичная иллюстрация действий по неправомерному доступу к компьютерной информации (ч. 1 ст. 272 УК РФ). Отмечается, что экспресс-анализ липольной схемы неправомерного доступа к компьютерной информации позволяет выявить критически важные места в рассматриваемой сфере. Делается вывод о возможности использования липольного анализа для установления обстоятельств совершения киберпреступлений. Такой анализ начинается составлением ЛП-схемы и завершается установлением существенных обстоятельств, имеющих значение для расследования уголовного дела.*

Ключевые слова*: киберпреступность, компьютерная информация, несанкционированный доступ, липольный анализ, схематизация, обстоятельства киберпреступления.*

USE OF LIPOLE ANALYSIS TO ESTABLISH THE CIRCUMSTANCES OF CYBERCRIMES

Khramov Sergey Mikhailovich,
candidate of legal sciences, associate professor
Brest State Pushkin University,
Brest, Republic of Belarus
e-mail: khramausiarhei@gmail.com

Abstract: *the article considers the issue of establishing the circumstances of the commission of cybercrimes. As an auxiliary tool, the author's method of lipolysis was used. A schematic illustration of actions for illegal access to computer information*

(part 1 of article 272 of the Criminal Code of the Russian Federation) is given. It is noted that express analysis of the lipoly scheme of illegal access to computer information makes it possible to identify critical places in the area under consideration. The conclusion is made about the possibility of using lipoly analysis to establish the circumstances of the commission of cybercrimes. Such an analysis begins with the preparation of a LP scheme and ends with the establishment of significant circumstances that are important for the investigation of a criminal case.

Keywords: *cybercrime, computer information, unauthorized access, lipoly analysis, schematization, cybercrime circumstances.*

Липольный анализ применительно к криминологии, криминалистике, уголовному праву и другим юридическим наукам разработан и апробирован автором в 2017-2018 годах. Основная разработка касалась приемов установления обстоятельств ранее совершенных преступлений. Было введено понятие «минимальная липольная система». Неологизм образован путем объединения терминов «лицо» и «поле» и кратко обозначается аббревиатурой ЛП. При этом под полем понимается сконцентрированное выражение противоправных действий. Там же находится предмет преступления. Если последствия таких действий находятся за пределами условного поля, то речь идет о материальных составах преступления.

Схематичное обозначение неправомерного доступа к компьютерной информации (ч. 1 ст. 272 УК РФ) выглядит следующим образом:

ЛП-схема ч. 1 ст. 278 УК РФ

В приведенной ЛП-схеме «Л» - лицо, совершившее преступление; «П» - поле, где сконцентрировано криминальное воздействия на предмет преступления.

Экспресс-анализ ЛП-схемы неправомерного доступа к компьютерной информации сразу же позволяет выявить критически важные места в рассматриваемой сфере.

Во-первых, это недостаточная защита компьютерной информации от неправомерного доступа.

Во-вторых, возможность в результате неправомерного доступа уничтожить, блокировать, модифицировать либо копировать охраняемую законом компьютерную информацию.

Соответственно, по результатам расследования уголовного дела о совершенном киберпреступлении на эти два момента может быть обращено внимание в Представлении об устранении причин и условий, способствовавших совершению преступления.

С точки зрения момента окончания преступления на схеме видно, что для наступления уголовной ответственности необходимы последствия в виде уничтожения, блокирования, и либо копирования компьютерной информации. Указанные признаки свидетельствуют о том, что по конструкции объективной стороны состав преступления, предусмотренный ч. 1 ст. 272 УК РФ, относится к категории материальных.

Для выявления и расследования киберпреступлений ЛП-схему, играющую роль мета-модели, необходимо условно наложить на конкретную ситуацию и затем сформулировать первоначальные следственные версии.

«Л», указанный на ЛП-схеме ч. 1 ст. 272 УК РФ, как правило, обладает необходимыми компьютерными навыками и имеет специальное образование. Может занимать должность, связанную с техническим обслуживанием компьютерного оборудования. Например, должности системного администратора, программиста, инженера. Подобные должность предполагают определенные познания в области компьютерной техники и компьютерных программ, сформировавшиеся навыки работы на персональных электронно-вычислительных машинах.

Если «Л» является специалистом, то в случае противоправных действий в отношении компьютерной информации он по должности должен быть осведомлен о незаконности нелицензионного использования объектов авторского права. Например, популярных программных продуктов «Microsoft Office».

Для совершения преступления может быть использована компьютерная информация, заведомо предназначенная для перевода программного продукта в полнофункциональный режим способом, не предусмотренным правообладателем. Такая информация обычно содержится во вспомогательных текстовых файлах наподобие «Ключ.txt» и т.п.

Такой файл с информацией для взлома лицензионной компьютерной программы может находиться в свободном доступе в сети «Интернет». Файл с информацией для взлома компьютерной программы чаще всего прямо копируется в постоянную память системного блока рабочего компьютера вместе с нелицензионной (контрафактной) версией программного продукта.

В файле типа «Ключ.txt» содержатся данные, которые позволяют нейтрализовать средства защиты компьютерной информации лицензионного программного продукта. Это делается для того, чтобы в дальнейшем беспрепятственно использовать взломанную программу в нарушение законодательства РФ об авторских правах.

Следствием взлома программы является возможность неправомерно использовать лицензионный программный продукт в полнофункциональном режиме без ограничений.

Судебная практика свидетельствует, что одним эпизодом киберпреступления во многих случаях не ограничиваются. Пример: ведущий инженер обвинялся в ряде эпизодов, связанных с совершением киберпреступлений. Так, он «находясь в помещении ООО ВСЗ «Техника», […] зная о вредоносных свойствах компьютерной информации, содержащейся в файле «Ключ.txt», позволяющих нейтрализовать средства защиты компьютерной информации - программного продукта «Microsoft Office Enterprise 2007» […] использовал […] программный продукт […] в полнофункциональном режиме без ограничений, предусмотренных правообладателем» [1].

Дополнительные возможности липольного анализа заключаются в упрощении установления юридически значимых обстоятельств, имеющих значение для расследования уголовных дел в сфере киберпреступности. В частности, на ЛП-схеме можно выделить этап «до активных действий». На этом этапе созревает умысел, приискиваются орудия и средства совершения преступления. Ответ на контрольный вопрос «В какой момент у лица возник преступный умысел на совершение киберпреступления?» имеет доказательственное значение.

Необходимо иметь в виду, что часть киберпреступлений имеет латентный, скрытый характер. Как верно отмечается в научной юридической литературе, «особенно пристального внимания с позиции противодействия киберкриминальным угрозам заслуживает проблема раннего обнаружения умысла на совершение киберпреступления…» [2, с. 67].

Пример: «В период до осени 2018 года у Б. возник преступный умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации НАО «Национальная спутниковая компания» («Триколор ТВ»), с целью модификации и копирования компьютерной информации НАО «Национальная спутниковая компания» («Триколор ТВ») из корыстной заинтересованности» [3].

Как известно, возникновение умысла само по себе не влечет уголовную ответственность. Но уголовно-процессуальное и криминалистическое исследование этого этапа важно с криминологической точки зрения для предупреждения подобных деяний впредь. Ведь речь идет о предкриминальной ситуации, причинах и условиях дальнейшего противоправного поведения субъекта. Кроме того, обнаружение умысла может рассматриваться как самостоятельная стадия развития девиантного поведения и представляет собой «выраженное словесно, письменно или путем иных действий намерение лица совершить киберпреступление…» [2, с. 68].

Далее исследуется вопрос – какие действия были предприняты для реализации преступного умысла, сознавало ли лицо общественную опасность задуманного, желало ли совершить противоправные действия, каков был мотив таких действий?

Если в дальнейшем лицо попытается сформировать «задним числом» алиби, это ему не удастся. Доказательства, подтверждающие комплекс подготовительных действий, не позволят это сделать.

Пример: Р. «в один из дней сентября 2017 года, не позднее 22 сентября 2017 года, в дневное время […], действуя из корыстной заинтересованности во исполнение своего преступного умысла, направленного на неправомерный доступ к охраняемой законом компьютерной информации, хранящейся в базе данных серверов ПАО «Почта Банк», содержащей персональные данные клиентов ПАО «Почта Банк» и их счетов, путем модификации данной информации, то есть с целью совершения операций в программном обеспечении ПАО «Почта Банк» по открытию счетов и выпуску карт на ряд физических лиц без их согласия, прибыл на работу к своей матери […] в ОПС Маркс-2 Энгельсского почтамта ФГУП «Почта России» по адресу: <адрес>, где, введя в заблуждение Потерпевший №11 и ФИО92 относительно своих истинных преступных намерений, под предлогом улучшения ОПС Маркс-2 статистических показателей и выполнения плана по выдаче неименных банковских карт ПАО «Почта Банк», уговорил Потерпевший №11 предоставить ему доступ к компьютерной информации, хранящейся в базе серверов ПАО «Почта Банк», в связи с чем Потерпевший №11, как начальник ОПС Маркс-2 Энгельсского почтамта ФГУП «Почта России», дала ФИО92 устное распоряжение открывать счета и оформлять неименные банковские карты ПАО «Почта Банк» по данным, предоставляемым Р.» [4].

На этапе «до…» может быть также обнаружена информация о возможных соучастниках преступления.

На это же этапе следует искать фактические данные, с помощью которых можно было бы отграничить длящееся преступление от серии повторных.

Исследуя начальный этап активных действий (на ЛП-схеме – между «Л» и «П»), устанавливается момент начала совершения и место совершения общественно опасного деяния, проверяются версии о наличии либо отсутствии у лица корыстной цели.

Наличие корыстной заинтересованности имеет не только доказательственное, но и уголовно-правовое значение. Неправомерный доступ к компьютерной информации, совершенный из корыстной заинтересованности, отягчает ответственность и квалифицируется по ч. 2 ст. 272 УК РФ.

Исследуя «П» (на ЛП-схеме находится в условном круге), необходимо акцентировать внимание на поиске цифровых следов, а также на установлении полного перечня технических средств и инструментов, использовавшихся в качестве вспомогательных для совершения киберпреступления. Эти же средства как материальные носители способствуют доказыванию виновности лица, совершившего киберпреступление.

Пример: «… осенью 2018 года Б., обладая познаниями в области компьютерной техники, информационных технологий и информационно - телекоммуникационных сетей, имея навыки и опыт работы на персональных ЭВМ, пользования всемирной информационно-телекоммуникационной сетью «Интернет» и различными Интернет-ресурсами, действуя умышленно,

незаконно из корыстной заинтересованности, находясь в своем жилище, расположенном по адресу: <...>, в целях просмотра закрытых телевизионных спутниковых каналов НАО «Национальная спутниковая компания» («Триколор ТВ») без абонентской платы установил и использовал ресивер марки «<данные изъяты>» NN с смарт - картой «Триколор ТВ» (индивидуальный код NN, номер карты NN На указанной карте содержится компьютерная информация (измененные сведения о подписках и сроках их действия), позволяющая осуществлять несанкционированный доступ к информации, содержащейся в системах ЭВМ и (или) сетях ЭВМ (транспортных потоках) системы спутникового телевидения НАО «Национальная спутниковая компания» («Триколор ТВ») [3].

В приведенном примере в качестве технического средства совершения киберпреступления использовался ресивер с смарт – картой.

Киберпреступления совершаются посредством компьютерных сетей и при этом посягают «на различные охраняемые законом объекты» [5, с. 257].

Если в результате киберпреступления причиняется вред двум объектам (экономическим отношениям и отношениям в сфере компьютерной безопасности), то квалифицировать действия виновного лица следует по совокупности статей 272 и 273 УК РФ «в зависимости от конкретных обстоятельств дела» [6, с. 91]. Попутно могут быть совершены и другие преступления, связанные со сферой компьютерной информации.

Пример: Р. по приговору суда признан «виновным в совершении преступлений, предусмотренных ч. 2 ст. 272, ч. 1 ст. 325.1, ч. 1 ст. 325.1, ч. 1 ст. 325.1, ч. 1 ст. 325.1, ч. 1 ст. 325.1, ч. 1 ст. 159.3 УК РФ» [4].

Таким образом, при установлении обстоятельств совершения киберпреступлений могут быть использованы возможности липольного анализа. Такой анализ начинается составление ЛП-схемы и завершается установлением существенных обстоятельств, имеющих значение для расследования уголовного дела. Прикладные возможности липольного анализа состоят в упрощении процесса выдвижения и проверки версий о совершенном киберпреступлении.

Список литературы

1. Постановление № 1-277/2020 от 29 июля 2020 г. по делу № 1-277/2020 // Архив Октябрьского районного суда г. Владимира (Владимирская область) за 2020 г.

2. Оганов, А.А. Противодействие умышленному причинению тяжкого вреда здоровью. Оперативно-розыскная деятельность и криминологический анализ: монография / А.А. Оганов. М.: ЮНИТИ-ДАНА, 2019. 143 с.

3. Приговор № 1-1-120/2020 от 29 мая 2020 г. по делу № 1-1-120/2020 // Архив Собинского городского суда (Владимирская область) за 2020 г.

4. Приговор № 1-40/2020 от 10 июля 2020 г. по делу № 1-40/2020 // Архив Марксовского городского суда (Саратовская область) за 2020 г.

5. Собольников, В.В. Криминальная психология: учебник для вузов / В.В. Собольников. 2-е изд., пер. и доп. М.: Издательство Юрайт, 2020. 379 с.

6. Простосердов, М.А. Об общественной опасности экономических киберпреступлений / М.А. Простосердов // Актуальные проблемы теории и практики применения уголовного закона: сборник материалов Четвертой Всероссийской научно-практической конференции / под ред. Ю.Е. Пудовочкина, А.В. Бриллиантова. М.: РГУП, 2017. С. 89-94.

УДК 343.1

ФИЛОСОФСКИЕ АСПЕКТЫ ВНЕДРЕНИЯ И ИСПОЛЬЗОВАНИЯ ВЫСОКИХ ТЕХНОЛОГИЙ В ПРАВЕ

Храпенкова Евгения Юрьевна,
аспирант
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: Sosna_evgeniya@mail.ru

Научный руководитель: Бертовский Лев Владимирович,
доктор юрид. наук, профессор, директор института высокотехнологичного права, социальных и гуманитарных наук
Национальный исследовательский университет «МИЭТ»,
г. Москва, Россия
e-mail: bgl1980@yandex.ru

Аннотация: *стремительное развитие технологий предполагает внедрение автоматизации и изменение характера правового регулирования. Однако, современная отрасль права не позволяет соответствовать тенденциям развития новых технологий, что делает необходимым снятие отдельных барьеров для упрощения механизма адаптации. Этот процесс, хотя и необходим обществу, может привести к серьезным негативным процессам, которые повлияют на общество во всех сферах. С этой целью необходима разработка специального механизма, который позволил бы создать условия развития права и использование в сфере его распространения высоких технологий. Право одновременно нацелено на урегулирование новых отношений в обществе, в качестве объектов которого выступают высокие технологии, и самостоятельное использование высоких технологий в целях оптимизации правовых задач, отвечая признакам логистичности, наукоемкости и технологичности, что и определяет его как отрасль высокотехнологичную.*

Ключевые слова: *высокие технологии, право, высокотехнологичность, искусственный интеллект, законодательство, юриспруденция.*

PHILOSOPHICAL ASPECTS OF THE INTRODUCTION AND USE OF HIGH TECHNOLOGIES IN LAW

Khrapenkova Evgeniya Yurievna,
postgraduate student
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: sosna_evgeniya@mail.ru

Bertovsky Lev Vladimirovich,
doctor of law, professor,
Director of the Institute of High-Tech Law,
social sciences and humanities,
National research university of electronic technology (MIET),
Moscow, Russia
e-mail: bgl1980@yandex.ru

Abstract: *the rapid development of technologies involves the introduction of automation and a change in the nature of legal regulation. However, the modern branch of law does not allow to fully comply with the trends in the development of new technologies, which makes it necessary to remove certain barriers to simplify the adaptation mechanism. Although this process is necessary for society, it can lead to serious negative processes that will affect society in all spheres. To this end, it is necessary to develop a special mechanism that would create conditions for the development of law and the use of high technologies in the sphere of its dissemination. At the same time, the law is aimed at regulating new relations in society, the objects of which are high technologies, and the independent use of high technologies in order to optimize legal tasks, meeting the signs of logistics, knowledge intensity and technology, which defines it as a high-tech industry.*

Keywords: *high technologies, law, high-tech, artificial intelligence, legislation, jurisprudence.*

В современном мире искусственный интеллект быстрыми темпами проникает во все сферы жизни, также быстро развивается и направление использования электронной демократии и культуры. В соответствии с тем, что они выступают основой для взаимодействия населения с органами государственной власти, возникает необходимость определения принципов применения права и философии права к продукции цифровизации.

Право не всегда успевает адаптироваться к меняющимся общественным отношениям, развиваясь медленно и без учета современных тенденций. В связи с тем, что юриспруденции присуща стабильность, определенность и предсказуемость, в то время, как инновации предполагают постоянные изменения. Право, стараясь достигнуть развития той или иной технологии, регулирует технологии прошлого в какой-то степени. Так как нормы, принимаемые правом, устаревают практических сразу.

Тем не менее, ряд отраслей права до сих пор придерживается консервативного подхода и не ориентируется на регулирование новых технологий. Социальные интересы являются основой права, поэтому именно они должны быть силой развития права. В некоторых случаях право препятствует распространению современных тенденций, например, существование административных барьеров по выходу на рынок в условиях распространения цифровой экономики субъекта или продукции. Так, для становления участником рынка требуется, в первую очередь, прохождение процедуры регистрации в качестве индивидуального предпринимателя или юридического лица, получение специального разрешения или лицензии. Кроме того, ограничения могут присутствовать не только со стороны государства, их могут выдвинуть и саморегулируемые организации путем определения безопасности продукции на основании получения сертификата или соответствия стандартам. Однако, данные ограничения являются необходимыми, и, хотя существует тенденция к сокращению административных барьеров, без них обойтись полностью невозможно, так как в результате на рынке будет большое количество некачественного и небезопасного товара.

Тем не менее законодательству приходится подстраиваться под новые тенденции. Особым направлением развития являются технологии «Умный город», которые позволят объединить различные системы общества в искусственно созданной среде для улучшения качества жизни населения.

Понятие «Умный город» в российском праве еще не было закреплено, но основы регулирования уже 10 лет находятся на стадии разработки технологических решений. Программа в настоящее время регулируется инициативой региональных и муниципальных властей, она должна была войти в программу «Цифровая экономика РФ», однако, требовались дополнения в виде дорожной карты и специального раздела ее регулирующего. Существует также некоторая неопределенность ее понимания властями в области правового регулирования и дальнейших отношений между регионом и муниципалитетом.

Возможной перспективной использования программы является использование решений и договоров с их формированием на базе нейронных систем, что и является будущим юридической практики. Ученые обучили искусственный интеллект распознавать ложь в процессе судебного заседания на основании запоминания эмоций человека и мимических черт. Точность распознавания составила 92% случаев, в то время как человек сможет верно отличить ложь только в 52% случаев [10].

Некоторые ученые предполагают, что уже через десять лет появятся юристы-роботы, способные принимать независимые юридические решения, однако, данный вопрос является дискуссионным, так как, считается, что роботы все еще не способны выполнять часть значимых полномочий юристов.

В конце декабря 2019 года право высоких технологий вышло на новый уровень развития. В этот период были приняты дополнения, которые легализовали сервисы проверки электронных подписей с помощью специализированных организаций [7].

Аккредитованные доверенные третьи стороны (ДТС) представляют собой специализированные организации, выполняющие функции по проверке электронной подписи в электронных документах в отношении лица, подписавшего документ [9]. Они предназначены для обеспечения доверия при обмене данными и документами и функционируют на основании Федерального закона №63-ФЗ и Федерального закона № 476-ФЗ [2, 3].

Это является важным этапом на пути к использованию в праве высоких технологий, обеспечивая трансграничное электронное взаимодействие и разработку нормативно-правовой базы для совершенствования безбумажной торговли.

Автоматизация производства, компьютеризация управления и другие важные процессы, происходящие в настоящее время в обществе, требуют регулирования и приводят к наукоемкости права. Происходит постоянное повышение научного потенциала по юридическим специальностям, число защит по ним составляет более 500 диссертаций в год с последующим возрастанием [6, С. 51]. Все чаще юристы прибегают к помощи legal technology или справочно-правовым системам («Экспресс проверка», «Конструктор договоров» и другим), которые предназначены для совершенствования юридической практики и помогают составить текст договора, проверить контрагентов или найти примеры судебной практики.

Право является логистическим, так как нормы, которые призваны регламентировать использование современных технологий, отражаются во всех современных отраслях права. Например, осужденный, содержащийся под стражей может заявить о желании присутствовать при рассмотрении апелляционной жалобы как лично, так и посредством использования конференцсвязи, согласно статье 389.12 УПК РФ.

Нарушение ПДД теперь может осуществлять путем фиксации нарушений без непосредственного участника сотрудников дорожно-патрульной службы. Кроме того, даже списание средств с баланса банковского счета для погашения штрафов не требует участия человека [8]. С 1 января 2023 года произошел переход к реестровой модели исполнительного производства, списание долгов теперь не требует оформления бумажных документов, что связано с повсеместным внедрением искусственного интеллекта.

Процедура снятия ограничений с должников, выезжающих за рубеж, ранее занимала достаточно много времени. Сейчас она составляет не более одного дня после оплаты долга. Появилась возможность обмена сведениями о должниках у Федеральной службы, Социального фонда, банков, ГИБДД, ФНС и Росреестра, а также у операторов сотовой связи в автоматическом режиме для снижения ручного сбора долгов судебными приставами. Такая система позволит избежать сокрытия доходов и имущества, а также сократит количество работы для судебных приставов.

Изменения начала года коснулись и налоговой сферы, Федеральный закон от 14.07.2022 г. № 263-ФЗ определяет создание единого налогового счета, который существенно повысить возможность контроля за поступлениями денежных средств, направленных на уплату налогов как для

налогоплательщика, так и для налоговой. Федеральный закон от 29.07.2017 г. № 242-ФЗ определяет направления развития и легализации телемедицины в области консультации больных по телефону и видеоконференцсвязи [4]. Впоследствии был принят Федеральный закон от 31.07.2020 г. № 258-ФЗ предусматривает определение правовых режимов, которые действуют в сфере цифровых технологий на территории Российской Федерации [5]. Кроме того, продолжаются исследования, направленные на унификацию процессуальных норм для дальнейшего формирования наиболее эффективного общепонятийного аппарата и единых принципов функционирования системы права наряду с быстро развивающимся обществом.

В ближайшем будущем планируется, что высокие технологии будут использоваться в праве с целью обработки заявок, дачи консультаций, а также сбора информации и выполнения других дел, в которых риск ошибки минимален за счет выполнения автоматических операций. Современное общество находится на пути обучения по применению искусственного интеллекта и стремится определить начальные этапы его внедрения, как в отрасль права, так и в другие отрасли [11]. При этом можно говорить о том, что право одновременно нацелено на урегулирование новых отношений в обществе, в качестве объектов которого выступают высокие технологии, и самостоятельное использование высоких технологий в целях оптимизации правовых задач, отвечая всем критериям высокотехнологичности: признакам логистичности, наукоемкости и технологичности.

Список литературы

1. Федеральный закон от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» // СПС «КонсультантПлюс».

2. Федеральный закон от 27 декабря 2019 года № 476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»//СПС «КонсультантПдюс».

3. Федеральный закон «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации» от 14.07.2022 г. № 263-ФЗ//СПС «КонсультантПлюс».

4. Федеральный закон от 29.07.2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья»// СПС «КонсультантПлюс».

5. Федеральный закон от 31.07.2020 г. № 258-ФЗ. «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»// СПС «КонсультантПлюс».

6. Ушакова, А.П. Сколько диссертаций защищается по юридическим наукам / А.П. Ушакова // Пролог: журнал о праве / Prologue: Law Journal, 2017. № 3. С.49-55.

7. ДТС 63-ФЗ. // URL: http://www.lht-llc.com/ (дата обращения 22.01.2023).
8. Изменения для водителей с 1 января 2023. // URL: https://avtospravochnaya.com/pdd/18506-izmeneniya-dlya-voditelej-s-1-yanvarya-2023 (дата обращения 21.01.2023).
9. Применение электронной подписи // URL: https://www.nalog.gov.ru/rn77/related_activities/el_doc/use_electronic_sign/ (дата обращения 21.01.2023).
10. Ученые обучили искусственный интеллект распознавать ложь в суде // URL: https://pravo.ru/news/view/146849/ (дата обращения 22.01.2023).
11. Бертовский, Л. В. Проблемы развития высокотехнологичного права / Л. В. Бертовский // Высокотехнологичное право: генезис и перспективы: Материалы III Международной межвузовской научно-практической конференции, Москва-Красноярск, 24–25 февраля 2022 года. Красноярск: Красноярский государственный аграрный университет, 2022. С. 26-29.

УДК 343.1

АКТУАЛЬНЫЕ ВОПРОСЫ ВЫСОКОТЕХНОЛОГИЧНОГО ПРАВА В СООТНОШЕНИИ С МЕТОДОЛОГИЕЙ ОТЕЧЕСТВЕННОЙ КРИМИНАЛИСТИКИ

Шаталов Александр Семенович,
доктор юридических наук, профессор
Московская академия Следственного комитета РФ,
г. Москва, Россия
e-mail: asshatalov@rambler.ru

Аннотация: *в статье рассмотрены взаимосвязанные вопросы формирующегося высокотехнологичного права и методологии отечественной криминалистики. Автор стремиться доказать необходимость дальнейшего обстоятельного научного исследования проблематики расследования преступлений, с использованием электронных и информационно-телекоммуникационных сетей. Он считает, что в своем нынешнем виде она безусловно претендуют на то, чтобы со временем трансформироваться в самостоятельную теоретическую концепцию, основная функция которой будет состоять в целенаправленном научном изучении способов решения конкретных задач возникающих при расследовании преступлений. С его точки зрения, разработка этой проблематики с учетом широких возможностей современных информационных технологий, изучение общетеоретических основ, принципов этой деятельности, а также профессионального опыта, вполне может претендовать на статус важнейшей задачи российской криминалистики.*

Ключевые слова: *высокотехнологичное право; информационно-телекоммуникационные сети; информационные технологии; криминалистика; расследование преступлений; уголовное судопроизводство электронные сети;*

TOPICAL ISSUES OF HIGH-TECH LAW IN RELATION TO THE METHODOLOGY OF DOMESTIC CRIMINOLOGY

Shatalov Alexander Semyonovich,
doctor of law, professor
Moscow Academy of the Investigative Committee of the Russian Federation, Moscow, Russia
e-mail: asshatalov@rambler.ru

Abstract: *the article deals with interrelated issues of emerging high-tech law and methodology of domestic criminology. The author seeks to prove the need for further thorough scientific research of the problems of crime investigation, using electronic and information and telecommunication networks. He believes that in its current form, it certainly claims to eventually transform into an independent theoretical concept, the main function of which will consist in a purposeful scientific study of ways to solve specific problems arising during the investigation of crimes. From his point of view, the development of this issue, taking into account the broad possibilities of modern information technologies, the study of general theoretical foundations, principles of this activity, as well as professional experience, may well claim the status of the most important task of Russian criminology.*

Keywords: *high-tech law; information and telecommunication networks; information technologies; criminalistics; crime investigation; criminal proceedings electronic networks*

Глобальные процессы цифровизации закономерно привели к осознанию необходимости формирования высокотехнологичного права во многих странах мира. В трудах российских криминалистов оно позиционируется в качестве наукоемкого и технологичного регулятора общественных отношений, который с одной стороны призван их регламентировать, а с другой, использовать в процессе правоприменения высокие технологии [1, с. 735-749]. В цифровом контексте, являющимся по своей природе трансграничным, само по себе определение внятных законодательных рамок для повсеместного использования технологий такого рода представляется недостаточным. Важнейшее значение приобретает, например, разработка правил киберэтики для утверждения прозрачности, лояльности и беспристрастности данного познавательного инструмента [2]. В интересах полноты, объективности и всесторонности предварительного расследования преступлений, должна быть, в частности, гарантирована достоверность методов обработки криминалистически значимой информации. Отрадно отметить, что в российской криминалистике необходимые предпосылки для этого в уже имеются.

За годы своего существования она прошла три этапа своего развития и сейчас находится на четвертом. Первый из них, принято связывать с накоплением эмпирического материала. Он начался во второй половине XIX века, и длился до середины тридцатых годов XX века. На втором этапе, начало которого совпало с выходом в свет первого советского учебника криминалистики (1935–36 г.г.), активизировалась разработка частных криминалистических теорий. Он длился около тридцати лет, т. е. примерно до середины 60-х годов XX века. Далее, вплоть до начала XXI века, осуществлялась систематизация криминалистических знаний, в основном за счет формирования общей теории криминалистики. С наступлением нового столетия работа по их систематизации не прекратилась, но в науке стал заметен акцент на программно-алгоритмической реконструкции накопленного в криминалистике научного знания, сопряженный с повсеместным внедрением и широким использованием кибернетических методов. Это привело к тому, что динамика развития криминалистической науки стала определяться не только отечественными, но и самыми разнообразными мировыми достижениями и разработками в области естественных, технических наук, а также повсеместным распространением электронных, информационно-телекоммуникационных сетей и сопутствующих им технологий.

Будучи самостоятельной отраслью научного знания советская, а затем и российская криминалистика за годы своего существования не только создавала собственный арсенал познавательных средств *(технических, тактических, технологических и методологических)*, копила опыт их использования в деле выявления, раскрытия, расследования преступлений, судебного рассмотрения уголовных дел, но и щедро делилась своими достижениями с другими науками. Сейчас в ней сложилась переходная ситуация, требующая, с одной стороны, критического пересмотра существующей системы знаний с учетом современных реалий общественного развития и правоохранительной деятельности, а с другой, ассимиляции глобальных процессов цифровизации к устоявшимся теоретическим схемам. Благодаря усилиям советских, а затем и российских криминалистов, существенно расширить методологию отечественной криминалистики смогли, в частности, кибернетические методы. Это можно и нужно считать значительным достижением, поскольку кибернетика в советское время считалась «*лженаукой*», вследствие чего, сам термин «*кибернетика*» почти не использовался и заменялся понятием «*информация*». В свою очередь само понятие «*информация*», а точнее *«криминалистически значимая информация»*, было и остается краеугольным камнем криминалистики, её научной платформой. Как следствие, она изначально позиционировалась криминалистами в зависимости от своего носителя и средств, с помощью которых могла из него извлекаться.

С недавних пор в число носителей криминалистически значимой информации стали входить электронные и информационно-телекоммуникационные сети, а для ее извлечения стали применяться современные информационные технологии, как наиболее удобные средства, имеющие большие технические возможности для ее поиска, обработки, выдачи

и хранения. Сразу нужно оговориться, что в этом плане отечественная криминалистика не является оригинальной. Во многих зарубежных странах аналогичные отрасли научного знания давно и активно развиваются в этом направлении, но преимущественно как технические дисциплины, направленные на разработку методов и средств обнаружения, изъятия, исследования следов и иных вещественных доказательств, учетно-регистрационных систем накопления и обработки криминалистически значимой информации. В то же время, в трудах зарубежных криминалистов практически не встречаются исследования, посвященные общетеоретическим, в т. ч. методологическим проблемам науки, в основном из-за того, что криминалистика ими позиционируется как прикладная дисциплина, призванная разрабатывать лишь технические рекомендации по раскрытию и расследованию преступлений. В отечественной криминалистике научные подходы несколько иные.

Методы, которые она использует, принято делить на три группы: всеобщий метод *(материалистическая диалектика)*, общенаучные и специальные [3, с. 233-266]. Их система образует целостную методологию, где в органическом единстве сочетаются научные методы, предназначенные для изучения того или иного объекта познания и методы ведения исследовательской работы. В советский и постсоветский периоды развития криминалистики основополагающим подходом к познанию всех процессов и явлений был и остается диалектический метод, призванный обеспечивать выявление всех свойств, связей и отношений, присущих изучаемому объекту. Когда в этом качестве фигурирует событие преступления, то оно объективно находится в причинно-следственной связи с другими явлениями объективной действительности. С точки зрения гносеологии это означает, что установление причинной зависимости позволяет получить фактическую основу для объяснения данного события, а также для прогнозирования хода и результатов досудебного производства по уголовному делу. Это в свою очередь влияет на определение форм и методов деятельности следователя, по расследованию преступления.

Как процесс познания, само расследование протекает от незнания к знанию, т. е. от конкретного явления, к его сущности, преследуя цель установления подлежащих доказыванию обстоятельств. Их целенаправленное познание отражает взаимосвязь диалектического метода с методами конкретных познавательных процессов. Следовательно, специфика диалектики познания не теряет изначальной общефилософской природы при использовании в досудебном и судебном производстве по уголовным делам электронных и информационно-телекоммуникационных сетей. Здесь имеется взаимосвязь категорий всеобщего, особенного и единичного, где всеобщим является диалектико-материалистический подход к сущности познаваемых явлений; особенным — возможность конкретизации его познавательного потенциала в рамках отдельно взятого акта предварительного расследования; единичным — современные информационные технологии, основанные на кибернетических методах и адаптированные для реализации в электронных и информационно-телекоммуникационных сетях.

Необходимо оговориться, что эти понятия в Уголовном кодексе Российской Федерации не разграничиваются, а сеть «Интернет» позиционируется в нем в качестве их разновидности. Под самой информационно-телекоммуникационной сетью в соответствующих статьях его Особенной части понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [4]. С точки зрения высшей судебной инстанции, для признания наличия в действиях того или иного лица признака совершения преступления с использованием электронных или информационно-телекоммуникационных сетей «… не имеют значения количество компьютерных устройств, входящих в такую технологическую систему, подключение к ней ограниченного количества пользователей или неопределенного круга лиц, а также другие ее характеристики. Таковыми могут признаваться, в частности, сети операторов связи, локальные сети организаций, домашние локальные сети, а также любые иные сети, предоставляющие возможность двум или более пользователям с помощью любых компьютерных устройств осуществлять проводной или беспроводной доступ к информации, расположенной на компьютерных устройствах, подключенных к данной сети, либо обмен информацией (передачу сообщений) между компьютерными устройствами» [5, п. 17].

Напомним, что проблематика решения криминалистических задач с помощью кибернетических методов в советское время детально изучалась в трудах Л.Г. Видонова, Н.Л. Гранат, Г.А. Густова, В.Я. Колдина, А.М. Ларина, Н.С. Полевого, А.Р. Шляхова, А.А. Эйсмана и др. Результаты их исследований позволяют сделать вывод, что непременным условием последовательного развития теоретических основ предварительного расследования преступлений, является поиск путей оптимального использования кибернетических методов и средств в этом процессе. Более того, по прошествии времени не осталось сомнений в том, что они не могут полноценно применяться в отрыве от достижений математики. Поэтому важным показателем их научной зрелости является все большее и большее использование математических методов.

Начиная с середины прошлого века криминалисты стали отмечать в своих работах, что их применение в криминалистических исследованиях открывает новые возможности для практики доказывания [6,7,8,9]. Само по себе отстаивание ими необходимости применения математических методов, как минимум свидетельствовало о достижении такого уровня развития отечественной криминалистики, когда она стала испытывать настоятельную потребность «… в тех точных методах познания своего предмета, которые может предоставить ей современная математика» [3, с. 251]. Расширение сферы применения методов этой науки в криминалистике напрямую связано с усилением процессов интеграции научного знания, призванных обеспечивать более полное качественное и количественное познание изучаемых закономерностей объективной действительности. С помощью математических методов обеспечивается высокая точность полученных результатов. Они не только расширяют и совершенствуют диапазон средств познания предмета

криминалистики, но и обогащают процесс собирания криминалистически значимой информации. При этом они не меняют своего содержания и применяются, как правило, в комплексе с другими методами. В сферу управления процессом расследования и познания его закономерностей математические методы интегрируются посредством методов кибернетических.

Хорошо известно, что многие задачи, которые приходится решать следователю, содержат элементы неопределенности. Этот феномен отчасти объясняется тем, что формирование доказательственной базы по уголовному делу происходит под влиянием множества факторов. Они весьма разнообразны, а их комбинации в каждом случае различны, вследствие чего плохо поддаются однозначной оценке. При этом любая криминалистически значимая информация выступает в качестве исходных данных и не носит такого стабильного характера, как уголовно-правовая или уголовно-процессуальная. Именно поэтому объективные закономерности, присущие массовым, однородным случайным событиям, могут и должны исследоваться при помощи математических вероятностных методов. Это может выражаться, например, в том, что при реализации следователем тех или иных криминалистических рекомендаций, случайные события, имеющие объективные предпосылки для своего появления в процессе предварительного расследования, могут произойти, а могут и не произойти. Следовательно, вероятность случайного обнаружения им источников криминалистически значимой информации может обосновываться математически, но при условии, что во внимание будут приняты самые разнообразные факторы объективного и субъективного свойства. Они пока плохо поддаются точным математическим преобразованиям, хотя попытки их осуществления имеют довольно продолжительную историю [10,11,12].

Одной из важных задач криминалистического анализа события преступления является получение научно обоснованного заключения о взаимосвязи двух и более объектов или явлений. Если их свойства проявляются случайным образом, эта задача может быть выполнена при помощи криминалистического алгоритма или программы расследования с использованием методов математической статистики, а также регрессионного и корреляционного анализа. Математизация и кибернетизация криминалистической деятельности, т. е. использование математического аппарата, а также идей, средств и методов кибернетики для решения конкретных задач предварительного расследования и построения криминалистических информационных систем неминуемо приводит к проблеме организации и управления такой деятельностью в новых условиях. Ее решение включает в себя:

- накопление значительного числа эмпирических данных, требующих научно-теоретического обоснования;

- трансформацию качественных методов криминалистики в комплексные, качественно-количественные методы исследования;

- изменение не только круга криминалистических задач, но также технологии и методики их решения;

- расширение круга специалистов, прямо или косвенно участвующих в деятельности по раскрытию и расследованию преступлений, определение их прав и обязанностей.

Эта точка зрения была сформулирована профессором Н. С. Полевым более тридцати лет тому назад [13, с. 38]. Тем не менее она является актуальной и поныне, а сама разработка теоретических основ расследования преступлений, но уже с использованием электронных и информационно-телекоммуникационных сетей все также требует специальных знаний и пока не связана с чувствительными изменениями законодательного регулирования досудебного и судебного производства по уголовным делам. В то же время развитие и внедрение новых информационных технологий рано или поздно приведет к трансформации всего уголовного судопроизводства. Российские криминалисты уже сейчас должны готовиться к такому развитию событий с высшей степенью ответственности и скрупулёзности.

Полагаем, что при анализе взаимовлияния уголовно-процессуального права и развития информационных технологий важно придерживаться индуктивного подхода с тем, чтобы понимать каким образом та или иная современная технология может повлиять на сам ход и исход защиты прав и законных интересов потерпевших от преступлений, а также подвергнутых уголовному преследованию лиц, от незаконного обвинения, осуждения, ограничения их прав и свобод. Для этого потребуется концептуальная база практического использования технологий такого рода в уголовном судопроизводстве. Представляется, что их использование не должно привести к полной дематериализации уголовного судопроизводства и к появлению, например, новых форм предварительного расследования преступлений, но несомненно повлечет за собой осовременивание его механизма. Более того, эти и некоторые другие факторы закономерно повлекут за собой изменения в теории и методологии криминалистики, что в свою очередь приведет к появлению новых теоретических концепций и дополнению понятийного аппарата (языка) науки.

Мы разделяем точку зрения Л.В. Бертовского о том, что одной из наиболее серьезных проблем является низкий уровень технической подготовленности кадров. Он правильно считает, что для ее решения необходимо обучение будущих юристов современным информационным технологиям, причем не только в качестве уверенных пользователей общеизвестного набора базовых компьютерных программ, но и лиц, осведомленных как в юридических аспектах функционирования IT в целом, так и в ее в международных стандартах и регулярно появляющихся новациях [14, с. 26-29]. В этой связи отрадно отметить, что мы становимся свидетелями последовательного создания новых основных и дополнительных инновационных профессиональных образовательных программ на стыке двух специальностей юридического и технического направления, реализуемых на базе такого многопрофильного университета, как МИЭТ.

Таким образом, мы постарались показать, что предпосылки для формирования основ новой частной теории в науке уже имеются. По нашему

глубокому убеждению, дальнейшее более обстоятельное исследование проблематики расследования преступлений, с использованием электронных и информационно-телекоммуникационных сетей, по мере продвижения и преумножения процесса цифровизации позволит выявить новые формы и направления развития криминалистического знания. Подчиняясь логико-методологическим принципам и законам диалектики, предмет отечественной криминалистики с течением времени будет конкретизироваться, наполняться новым содержанием, поскольку проблемы эти весьма и весьма многообразны. Они взаимосвязаны и безусловно претендуют на то, чтобы со временем трансформироваться в самостоятельную теоретическую концепцию, основная функция которой будет состоять в целенаправленном научном изучении способов решения криминалистических задач, с использованием электронных и информационно-телекоммуникационных сетей. Их разработка с учетом широких возможностей современных информационных технологий, изучение общетеоретических основ, принципов этой деятельности, а также уже имеющегося и регулярно появляющегося профессионального опыта, вполне может претендовать на статус важнейшей задачи российской криминалистики. Пройдя путь интеграции криминалистических знаний с данными естественных и технических наук, эта концепция достаточно давно начала формироваться в отечественной криминалистике. Поэтому в данной статье мы стремились выделить лишь некоторые ее характерные черты и показать назревшую необходимость ее дальнейшего развития.

Список литературы

1. Бертовский, Л.В. Высокотехнологичное право: понятие, генезис и перспективы / Л.В. Бертовский. Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. № 4. С. 35-749.
2. Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях. Принята на 31-м пленарном заседании ЕКЭП (Страсбург, 3-4 декабря 2018 года) // URL: https://docviewer.yandex.ru/view/1013535196/.
3. Белкин, Р.С. Курс советской криминалистики / Р.С. Белкин. Т. 1. М., 1977. 340 с.
4. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 21.11.2022 г.) // СПС «КонсультантПлюс».
5. Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. №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 сетей, включая сеть «Интернет» // URL: https://www.vsrf.ru/documents/own/31913/.
6. Винберг, А. И. Некоторые актуальные вопросы советской криминалистики / А.И. Винберг// Сов. государство и право. 1962, № 5. 250 с.

7. Шляхов, А.Р. Проблемы судебной экспертизы и задачи научно-исследовательских лабораторий судебной экспертизы / А.Р. Шляхов // Проблемы судебной экспертизы. № 1. М.: 1961. С. 3-31.

8. Эджубов, Л.Г. Об автоматизации дактилоскопической экспертизы / Л.Г. Эджубов // Советская криминалистика на службе следствия. - Вып. 14. - М., Госюриздат. 1961. С. 137-151.

9. Эйсман, А.А. Вопросы теории установления родовой принадлежности (родовой идентификации) в криминалистике / А.А. Эйсман // Проблемы судебной экспертизы. № 1. М., 1961. С.104-108.

10. Буняковский, В.Я. Основания математической теории вероятностей / В.Я. Буняковский. СПб., 1846. 502 с.

11. Курно, О. Основы теории шансов и вероятностей / О. Курно. М., 1970. 250 с.

12. Бентам, И. Трактат о судебных доказательствах / И. Бентам. Киев, 1876. 421 с.

13. Полевой, Н.С. Криминалистическая кибернетика / Н.С. Полевой. 2-ое изд. М.: Изд-во МГУ, 1989. 356 с.

14. Бертовский, Л.В. Проблемы развития высокотехнологичного права / Л.В. Бертовский // Высокотехнологичное право: генезис и перспективы: материалы III Международной межвузовской научно-практической конференции (24-25 февраля 2022 года, Москва – Красноярск). Национальный исследовательский университет «Московский институт электронной техники»; Красноярский государственный аграрный университет. Красноярск: Красноярский ГАУ, 2022. С. 26-29.

УДК 349.3

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ СОЦИАЛЬНОГО ОБЕСПЕЧЕНИЯ

Широких Светлана Викторовна,
старший преподаватель
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: diritto@mail.ru

Аннотация: *статья посвящена анализу применения информационных технологий при реализации гражданами прав на социальное обеспечение в рамках функционирования проекта «Социальное казначейство». Рассматриваются отдельные примеры законодательного закрепления беззаявительной выплаты пенсий и пособий на основе данных государственных информационных систем, а также некоторые изменения законодательства, направленные на повышение эффективности и адресности мер социальной поддержки граждан.*

Ключевые слова: *информационные технологии, социальное государство, социальное обеспечение, социальное казначейство, проактивные выплаты, проактивное информирование граждан.*

INFORMATION TECHNOLOGIES IN THE SOCIAL SECURITY SYSTEM

Shirokikh Svetlana Viktorovna,
senior lecturer
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: diritto@mail.ru

Abstract: *the article is devoted to the analysis of the use of information technologies in the implementation of citizens' rights to social security within the framework of the functioning of the project "Social Treasury". Some examples of legislative consolidation of non-explicit payment of pensions and benefits based on data from state information systems are considered, as well as some legislative changes aimed at improving the effectiveness and targeting of social support measures for citizens.*

Keywords: *information technologies, welfare state, social security, social treasury, proactive payments, proactive informing of citizens.*

Система социального обеспечения в РФ представлена достаточно широким перечнем различных мер государственной поддержки как на федеральном уровне, так и на уровне субъектов РФ. По приблизительным оценкам Минтруда РФ, на сегодняшний момент в России существует 387 видов мер социальной поддержки и эта цифра постоянно меняется в зависимости от возникновения новых обстоятельств, наступление которых влечет за собой необходимость в помощи со стороны государства (например, пандемия, стихийные бедствия и др.). Вполне естественно, что гражданам, особенно старшей возрастной группы, зачастую бывает достаточно сложно сориентироваться в большом объеме правовой информации и, как следствие, возникают сложности при реализации прав на какой-либо вид социального обеспечения. При этом основанием для представления гражданина к какому-либо виду социального обеспечения является обращение с заявлением в уполномоченный орган и подтверждение права на социальную поддержку определенным пакетом документов. То есть необходимо соблюсти определенную процедуру, что находит свое отражение и в предмете такой отрасли права как право социального обеспечения (процедурные отношения входят в предмет отрасли).

Стоит отметить, что с 2020 года (период пандемии) ситуация стала меняться в сторону упрощенного, беззаявительного назначения гражданам отдельных видов социальных выплат (например, ряд пособий семьям, имеющим детей). Данный опыт активно распространяется на иные виды социальной поддержки, что стало возможно благодаря внедрению современных цифровых технологий во все сферы общественной жизни, в том числе и в

области отношений по социальному обеспечению. Одним из способов упрощения процесса получения помощи стал запуск проекта «Социальное казначейство», реализация которого позволяет проактивно (беззаявительно) информировать граждан о положенных им мерах поддержки, а также упрощенно оформлять их без необходимости сбора подтверждающих документов, а в некоторых случаях и без заявления. Нормативно-правовой базой для внедрения данного проекта является «Концепция цифровой и функциональной трансформации социальной сферы, относящейся к сфере деятельности Министерства труда и социальной защиты Российской Федерации, на период до 2025 года», к целям которой относятся повышение адресности и эффективности предоставления мер социальной поддержки на федеральном, региональном и муниципальном уровнях; повышение эффективности использования средств бюджетов различных уровней на предоставление мер социальной поддержки гражданам РФ; оптимизация взаимодействия с гражданами при получении ими мер социальной поддержки; оптимизация процессов предоставления государственных услуг Социального фонда РФ; взаимодействия с гражданами при проведении медико-социальной экспертизы; снижение административной нагрузки на страхователей (юридических лиц), оптимизация процессов их взаимодействия с Социальным фондом РФ и др. [1].

Курс на автоматизацию назначения социальных выплат повлек за собой изменения в законодательстве, например, в части пенсионного обеспечения. В ФЗ РФ «О страховых пенсиях» включена новая статья, предусматривающая возможность назначения страховой пенсии по старости в автоматическом режиме при обращении за ней путем подачи электронного заявления через портал «Госуслуги» [2], порядок осуществления которого регламентирован Пенсионным фондом РФ в 2021 году [3]. Изменения коснулись и страховой пенсии по инвалидности, назначение которой происходит в беззаявительном порядке на основании данных Федерального реестра инвалидов. Следует отметить, что совершенствования требует также и законодательство, регулирующее назначение страховой пенсии по случаю потери кормильца в области развития взаимодействия государственных органов, обладающих необходимой информацией о получателях данного вида пенсии, например, между Социальным фондом и военкоматами в части предоставлениями последними сведений о лицах, призываемых к военной службе. Прохождение военной службы по призыву является основанием для приостановления выплаты пенсий, о чем призывник обязан сообщить в Социальный фонд, что зачастую приводит к тому, что необходимые сведения по разным причинам в орган пенсионного обеспечения не поступают, начисление пенсии продолжается, и к моменту окончания военной службы у получателей пенсии накапливается существенная задолженность, которую необходимо вернуть. Думается, что внесение соответствующих дополнений в законодательство поможет изменить ситуацию.

Еще одним направлением деятельности государственных органов, призванным усовершенствовать систему социального обеспечения РФ стало

проактивное информирование граждан о возникновении у них права на какой-либо вид социального обеспечения в зависимости от наступления конкретного социального риска [4], например, информирование Социальным фондом лиц, достигших возраста 40 лет, о сформированных к настоящему моменту пенсионных правах, о перечне мер социальной защиты, право на которые возникло у гражданина в связи с определенным жизненным событием. Осуществление подобного информирования стало возможно благодаря созданию Единого контакт-центра взаимодействия с гражданами [5], а также Единой государственной системы социального обеспечения [6].

В целом, следует отметить, что, несмотря на появление новых мер социальной поддержки, на достаточную разветвленность современной системы социального обеспечения, внедрение цифровых технологий позволяет гражданам более эффективно реализовывать свои права на меры поддержки за счет своевременного информирования, а, в некоторых случаях, беззаявительного назначения отдельных видов социального обеспечения в зависимости от конкретного жизненного события.

Список литературы

1. Распоряжение Правительства РФ от 20.02.2021 г. № 431-р «Об утверждении Концепции цифровой и функциональной трансформации социальной сферы, относящейся к сфере деятельности Министерства труда и социальной защиты РФ, на период до 2025 г.» // СПС «КонсультантПлюс».

2. Федеральный закон от 28.12.2013 г. № 400-ФЗ «О страховых пенсиях» // СПС «КонсультантПлюс».

3. Постановление Правления ПФ РФ от 28.09.2021 г. № 324п «Об утверждении Порядка назначения страховой пенсии по старости в автоматическом режиме» // СПС «КонсультантПлюс».

4. Постановление Правительства РФ от 03.12.2020 г. № 1994 «Об утверждении Правил информирования гражданина о правах, возникающих в связи с событием, наступление которого предоставляет ему возможность получения мер социальной защиты (поддержки), социальных услуг, предоставляемых в рамках социального обслуживания и государственной социальной помощи, иных социальных гарантий и выплат, а также об условиях их назначения и предоставления и о внесении изменений в Положение о Единой государственной информационной системе социального обеспечения» // СПС «КонсультантПлюс».

5. Приказ Минтруда России от 28.05.2019 г. № 360 «Об информационной системе «Единый контакт-центр взаимодействия с гражданами» (вместе с «Положением об информационной системе «Единый контакт-центр взаимодействия с гражданами») // СПС «КонсультантПлюс».

6. Постановление Правительства РФ от 16.08.2021 г. № 1342 «О Единой государственной информационной системе социального обеспечения» (вместе с «Положением о Единой государственной информационной системе социального обеспечения») // СПС «КонсультантПлюс».

УДК 343.1

К ВОПРОСУ ПРИМЕНЕНИЯ СПЕЦИАЛЬНЫХ СРЕДСТВ ДЛЯ ФИКСАЦИИ ПРАВОНАРУШЕНИЙ

Щебляков Евгений Степанович,
старший преподаватель
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: doess23@mail.ru

Аннотация: *одной из функций государства является обеспечение общественного порядка и общественной безопасности граждан, обеспечение реализации ими прав и законных интересов. В связи с этим можно сказать, что современное общество развивается также, как развиваются технологии, которые используются в целях обеспечения реализации различных функций государства, как, например, обеспечение безопасности граждан. Важно отметит, что для реализации данной функции государством используются различные средства, в том числе, и, специальные средства фиксации совершаемых правонарушений.*

Среди правонарушений, одним из наиболее распространенных правонарушений выступают правонарушения, связанные с безопасностью дорожного движения. И, здесь, необходимо отметить положительный опыт применения специальных средств при фиксации административных правонарушений в области дорожного движения. Как показывают статистические данные, применение специальных средств, работающих в автоматическом режиме и фиксирующих совершение правонарушений в области дорожного движения, позволило государству достичь снижения уровня правонарушений. Развитие в дальнейшем современных технологий позволит применять более современные средства и в других областях.

Ключевые слова: *специальные средства фиксации правонарушений, правонарушения, доказательства, современные технологии.*

USE OF SPECIAL AGENTS TO PREVENT PET THEFT

Shcheblyakov Evgeniy Stepanovich,
senior lecturer
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: doess23@mail.ru

Abstract: *one of the functions of the state is to ensure public order and public safety of citizens, ensuring the implementation of their rights and legitimate interests. In this regard, we can say that modern society is developing as well as technologies that are used to ensure the implementation of various functions of the state, such as ensuring the safety of citizens. It is important to note that for the implementation of*

this function, the state uses various means, including special means of fixing committed offenses.

Among the offenses, one of the most common offenses is road safety offenses. And, here, it is necessary to note the positive experience of using special means in fixing administrative offenses in the field of traffic. As statistics show, the use of special means working in automatic mode and recording the commission of offenses in the field of traffic, allowed the state to achieve a decrease in the level of offenses. The development of modern technologies in the future will allow the use of more modern means in other areas.

Keywords: *special means of fixing offenses, offenses, evidence, modern technologies.*

Одной из функций государства является обеспечение безопасности общественных отношений в различных сферах общественной жизни. Современные общественные отношения стремительно развиваются, также стремительно развиваются различные технологии, которые используются во всех сферах общественной жизни [1]. Необходимо отметить, что развитие современных технологий позволят государству более эффективно реализовывать различные формы регулирования общественных отношений[2]. При этом государство должно обеспечить развитие общественных отношений, обеспечить безопасность граждан при реализации ими своих прав, свобод и законных интересов.

В качестве одной из сфер, где государство активно применяет современные технологии, можно выделить сферу обеспечения безопасности в области дорожного движения. В данной сфере активно используются специальные средства фиксации правонарушений, и их применение постоянно совершенствуется с учетом развития современных технологий.

Применение специальных средств автоматической фиксации правонарушений в области дорожного движения позволило государству решить некоторые проблемы. Одной из таких проблем является проблема формирования доказательственной базы совершенного правонарушения [3]. Эта проблема решена с помощью современных технологий, так как современные комплексы фиксации правонарушений в области дорожного движения уже на сегодняшний день обеспечивают фиксацию различных правонарушений и с развитием современных технологий и дальше будут совершенствоваться. С помощью данных специальных средств облегчается работа правоприменительных органов и снижается уровень затрат на доказывание фактов совершенных правонарушений [4].

Другая проблема, решаемая с помощью специальных средств, это профилактика совершения правонарушений. Ведь именно профилактика совершения правонарушений является первичной задачей деятельности государства, так как когда человек начинает понимать необходимость соблюдения норм законодательства и осознавать их цель и задачи, тогда государство обеспечило достижение одной из своих целей, это предупреждение совершения правонарушений.

В настоящее время государству не менее важно обеспечить снижение уровня совершаемых правонарушений не только в области дорожного движения, но и в других сферах общественных отношений. Ведь проблема доказывания факта правонарушения и идентификация лиц совершивших правонарушений актуальна не только в области общественного порядка и общественной безопасности в области дорожного движения. Думается, положительный опыт применения специальных средств фиксации совершения правонарушений необходимо совершенствовать и применять при совершении правонарушений и в других областях. На современном этапе не мало областей и сфер общественных отношений, где можно использовать специальные средства фиксации правонарушений, но пока нет применяемых в правоприменительной практике. Развитие современных технологий позволит решить проблему доказывания и в других сферах общественных отношений и повысить раскрываемость других правонарушений.

Все это свидетельствует о том, что необходимо применять современные высокотехнологичные средства, что позволит ускорить время и результативность расследования правонарушений в различных областях общественных отношений.

Список литературы

1. Курбатова, С.М. Уголовно-процессуальная дееспособность: юридические и фактические аспекты проявления когнитивных особенностей личности / С.М. Курбатова // Право и законность: вопросы теории и практики. Сб. мат-в IX Всероссийской научно-практич. конф. Абакан: Изд-во ХГУ, 2019. С. 28-29.

2. Щебляков, Е.С. Криминалистические особенности хищения домашних животных (скота) / Е.С. Щебляков // Гуманитарные, социально-экономические и общественные науки. 2020. № 2. С. 192-195.

3. Щебляков, Е.С. Особенности профилактических мер борьбы с хищениями домашних животных / Е.С. Щебляков // Гуманитарные, социально-экономические и общественные науки. 2020. № 7. С. 197-199.

4. Актуальные психолого-педагогические, философские, экономические и юридические проблемы современного российского общества: колл. монография Выпуск 2. Ульяновск: изд-во «Зебра», 2017. 289 с.

УДК 343.1

ПРИМЕНЕНИЕ СПЕЦИАЛЬНЫХ СРЕДСТВ В ЦЕЛЯХ ПРЕДУПРЕЖДЕНИЯ ХИЩЕНИЙ ДОМАШНИХ ЖИВОТНЫХ

Щебляков Евгений Степанович,
старший преподаватель
Красноярский государственный аграрный университет,
г. Красноярск, Россия
e-mail: doess23@mail.ru

Аннотация: *в некоторых регионах Российской Федерации, а также в некоторых государствах, хищения домашних животных, в том числе, и, скота, причиняют значительный ущерб. Сложность расследования данных преступлений и правонарушений заключается в доказывании принадлежности домашних животных, так как не всегда возможно их идентифицировать и тем более доказать, что данное животное принадлежало конкретному лицу. Процесс доказывания является самым сложным и трудоемким. К сожалению, собственники домашних животных не всегда предпринимают необходимые меры для обеспечения идентификации и принадлежности домашних животных.*

Также одной из проблем при проведении расследований хищений домашних животных является не совершенство применяемых собственниками домашних животных средств идентификации. Большинство собственников применяют метки, клейма и иные подобные средства, которые наносятся на шкуры животных, так как они достаточно легко могут быть удалены со шкуры животного. Следствием является не возможность определить принадлежность данного животного. В связи с развитием современных технологий можно применять более современные средства идентификации домашних животных, в том числе, и скота.

Ключевые слова: *хищение домашних животных, идентификация домашних животных, современные средства идентификации домашних животных.*

USE OF SPECIAL AGENTS TO PREVENT PET THEFT

Shcheblyakov Evgeniy Stepanovich,
senior lecturer
Krasnoyarsk state agrarian university,
Krasnoyarsk, Russia
e-mail: doess23@mail.ru

Abstract: *In some regions of the Russian Federation, as well as in some states, the theft of pets, including livestock, causes significant damage. The difficulty of investigating these crimes and offenses lies in proving the ownership of pets, since it is not always possible to identify them, and even more so to prove that this animal*

belonged to a specific person. The process of proof is the most complex and time-consuming. Unfortunately, pet owners do not always take the necessary measures to ensure the identification and belonging of pets.

Also, one of the problems in conducting investigations into pet theft is not the perfection of identification tools used by pet owners. Most owners use tags, stamps and other similar means that are applied to animal skins, since they can be easily removed from the animal skin. The consequence is that it is not possible to determine the ownership of this animal. In connection with the development of modern technologies, more modern means of identifying pets, including livestock, can be used.

Keywords: *pet theft, pet identification, modern pet identification tools.*

В настоящее время собственники домашних животных не всегда используют средства идентификации домашних животных, что приводит к тому, что при потере или похищении домашнего животного не представляется возможным найти, а в случае обнаружении домашнего животного внешне похожего, доказать его принадлежность конкретному лицу. Данная проблема для правоприменительной практики создает проблему доказывания и невозможность раскрыть значительное количество правонарушений и преступлений по хищению домашних животных.

Процесс сбора доказательств совершения правонарушения или преступления всегда является очень трудоемким и требует значительных затрат времени от правоприменителя. Правоприменители при формировании доказательственной базы используют разные методы и средства доказывания обстоятельств совершения правонарушений и преступлений. В целях облегчения работы правоприменительных органов необходимо применять средства идентификации домашних животных [1].

В настоящее время к наиболее распространенных средствам идентификации домашних животных применяются следующие средства:

1. Нанесение на тело животного татуировки;
2. Также применяется такое средство, как выщипы на ушах животного;
3. Применяется такое средство, как горячее и холодное таврение на теле животного;
4. Также, одним из распространенных средств идентификации животного является биркование;
5. Также очень часто применяются металлические серьги и синтетические бирки собственниками животных, особенно владельцами домашнего скота;
6. Собственники животных, которые живут в квартирах, часто применяют ошейники;
7. Для скота и домашних птиц применяют ножные и хвостовые браслеты.

У всех вышеперечисленных форм идентификации домашних животных основная проблема заключается в несовершенстве и невозможности сохранения на теле животного нанесенных средств идентификации [2].

Лица совершающие хищения домашних животных в первую очередь удаляют нанесенные средства идентификации [3], так как они легко удаляются, и дальнейшая идентификация животного значительно осложняется для правоприменительных органов [4].

К современному средству идентификации домашних животных относится такой способ, как чипирование домашнего животного. Чипирование обладает рядом преимуществ, основным из которых является скрытый характер, что облегчает как обнаружение животного, так и последующую его идентификацию, а лица, совершающие правонарушение или преступление не предполагают о наличии чипа в теле животного и не предпринимают меры к его извлечению.

Данной проблематике посвящено много исследований, но, к сожалению, собственники домашних животных не используют существующие современные средства идентификации домашних животных, что приводит к значительному затруднению процесса расследования и доказывания хищения домашнего животного. Все это свидетельствует о том, что необходимо применять современные высокотехнологичные средства идентификации домашних животных, это позволит ускорить время расследования и результативность.

Список литературы

1. Курбатова, С.М. Уголовно-процессуальная дееспособность: юридические и фактические аспекты проявления когнитивных особенностей личности / С.М. Курбатова // Право и законность: вопросы теории и практики. Сб. мат-в IX Всероссийской научно-практич. конф. Абакан: Изд-во ХГУ, 2019. С. 28-29.

2. Щебляков, Е.С. Криминалистические особенности хищения домашних животных (скота) / Е.С. Щебляков // Гуманитарные, социально-экономические и общественные науки. 2020. № 2. С.192-195.

3. Щебляков, Е.С. Особенности профилактических мер борьбы с хищениями домашних животных / Е.С. Щебляков // Гуманитарные, социально-экономические и общественные науки. 2020. № 7. С. 197-199.

4. Актуальные психолого-педагогические, философские, экономические и юридические проблемы современного российского общества: колл. монография Выпуск 2. Ульяновск: изд-во «Зебра», 2017. 289 с.

УДК 343.14

О ПРОЦЕССНОМ ПОДХОДЕ ПРИ ПОЛУЧЕНИИ И ИССЛЕДОВАНИИ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

Яковлев Алексей Николаевич,
кандидат юридических наук, доцент
Национальный исследовательский университет
«Московский институт электронной техники» (НИУ МИЭТ),
Московский государственный технический университет
имени Н.Э. Баумана (национальный исследовательский университет),
г. Москва, Россия
e-mail: a_yakovlev@mail.ru

Аннотация: *в статье рассмотрено* многообразие именований *современной высокотехнологичной преступности, а также подход к ее исследованию и противодействия ей на основе концепции информационно-коммуникационных технологий. Раскрыто позитивное влияние выбранной концепции на возможность противодействия новому виду преступлений – атакам на технологии, констатирована неэффективность квалификации новых видов преступлений посредством имеющихся норм права. Приведен пример нового процессного подхода к получению цифровых доказательств на примере заблокированного мобильного телефона как элемента информационно-коммуникационной технологии сотовой связи.*

Ключевые слова: *преступления с использованием информационно-коммуникационных технологий, атаки на технологию, цифровые доказательства, исследование технологии, процессный подход.*

ON THE PROCESS APPROACH TO OBTAINING AND EXAMINING DIGITAL EVIDENCE

Yakovlev Aleksey Nikolaevich ,
candidate of legal sciences, associate professor
National Research University of Electronic Technology (MIET),
Bauman Moscow State Technical University
(National research university of technology),
Moscow, Russia
e-mail: a_yakovlev@mail.ru

Abstract: *the article considers a variety of names of modern high-tech crime, as well as the approach to its research and counteraction to it based on the concept of information and communication technologies. The positive influence of the chosen concept on the possibility of counteraction to a new type of crime - attacks on technology is revealed, the inefficiency of qualification of new types of crimes by the existing rules of law is stated. The example of new process approach to obtaining*

digital evidence on the example of the blocked cell phone as an element of information and communication technology of cellular communication is given.

Keywords: *information and communication technology crimes, attacks on technology, digital evidence, technology research, process approach.*

Пришло время задаться вопросом, в связи с чем в России до сих пор существует многообразие именований современной высокотехнологичной преступности, и полезно ли оно для эффективного расследования соответствующей категории преступлений? «Киберпреступления», «преступления в сфере компьютерной информации», «преступления в сфере высоких технологий», «преступления в сфере информационных технологий», и, наконец, «преступления с использованием информационно-коммуникационных технологий» – эти термины мы часто наполняем собственным или заимствованным смыслом, уводящим нас от базовых процессов обработки данных, жизненного цикла информации, которые являются фактическим предметом преступления.

Термин «киберпреступление», основываясь на замечании Л.В. Бертовского, просто лингвистическая конструкция, которая включает «приставку *кибер-* (cyber [‘saibə]; в переводе с английского *относящийся к компьютерам, информационным технологиям, Интернету*) и слово «преступление» (уголовно наказуемое деяние)» [1, с. 85]. Вместе с тем, Википедия высказывается по этому поводу более технологичнее: «Кибер- (cyber) – приставка, показывающая отношение чего-либо к кибернетике и связанным с ней явлениям» [2], и мы с этим согласны. В западной научной литературе при определении чего-то нового, как правило, используют обобщающие смысловые категории верхнего порядка, не предполагающие последующую дискуссию о тонкостях смыслов. С учетом классического определения кибернетики как науки об общих законах управления и связи в природе и обществе, а также *получении, передаче и преобразовании информации* в кибернетических системах [3, с. 93], технологические особенности термина «киберпреступление» начинают быть очевидными: киберпреступление – это преступление, связанное (сопряженное) с процессами получения, передачи и преобразования информации. Запомним это пояснение – в нем должное внимание уделено процессам, а не только их результатам.

Термин «преступления в сфере компьютерной информации» нам представляется одним из самых неудачных. Сфера здравоохранения, образования, транспортная сфера, иные, которые мы рассматриваем применительно к специфике того или иного вида преступлений, это, согласно Росстату, отрасли экономики [4], среди которых «сфера компьютерной информации» не просто отсутствует, а вообще не вписывается в какие-либо основания классификации отраслей. Если бы не помещение законодателем этого термина в наименование главы УК РФ, этот термин не имел бы шансов на повсеместное использование в научной и публицистической литературе по уголовному праву.

Термин «преступления в сфере высоких технологий» сконструирован как дань тем носителям юридических знаний, которым без погружения в технические детали мира современных технологий и процессов обработки информации необходимо самое общее обозначение чего-то малопонятного и технически сложного. Как ни странно, но интуитивная характеристика «сложное» достаточно точно соответствует фактическому определению высоких технологий в технических и иных науках. Например, в онлайн экономической энциклопедии к высоким технологиям относят наиболее новые и прогрессивные технологии современности, самые наукоёмкие отрасли промышленности, в частности, экологически чистые технологии, энергосбережение и альтернативную энергетику [5]. Как соотносятся «преступления в сфере высоких технологий» в понимании юристов и «высокие технологии» в понимании их разработчиков представить сложно, так как считать высокими технологиями особенности защиты данных средствами операционной системы или процессы функционирования файловой системы на электронном носителе информации можно было разве что четверть века тому назад. Продолжать сегодня терминологическую неразбериху с участием юристов, специалистов в области защиты информации, IT-специалистов – де-факто означает продолжать дело, начатое строителями библейской Вавилонской башни, и с тем же успехом.

Появление терминов «преступления в сфере информационных технологий» и «преступления с использованием информационно-коммуникационных технологий» явилось первой попыткой восстановления связи специалистов в области права с предметной областью рассматриваемой категории преступлений. Безусловно, термин «киберпреступление» изначально имел большой теоретический и практический потенциал, ориентированный на противодействие преступности максимально широкого спектра, не привязанной к конкретным устройствам обработки данных, конкретным типам данным и технологиям их обработки, но этот потенциал не был замечен и использован. Лишь впоследствии новая попытка раскрыть такой потенциал была поддержана на самом верхнем уровне принятия решений и закреплена Указом Президента Российской Федерации от 30 сентября 2022 года № 688, которым создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий [6].

Почему подход к исследованию высокотехнологичной преступности и противодействия ей на основе информационно-коммуникационных технологий является современным, эффективным и перспективным? Потому что он соответствует предмету преступлений, основан на полном и непротиворечивом регулировании предметной области с помощью как нормативных правовых актов (федеральных законов, постановлений Правительства Российской Федерации, ведомственных приказов), так и документов технического регулирования (межгосударственных стандартов, национальных стандартов Российской Федерации), учитывает требования к защите информации и включает информационную безопасность в состав базовых наук и практик, востребованных при расследовании преступлений, позволяет формировать

понятные гражданам требования государства к порядку использования информационно-коммуникационных технологий, предоставляет новые возможности для осуществления оперативно-розыскной деятельности, предварительного расследования, криминалистического и экспертного обеспечения расследования преступлений.

В основе такого подхода лежит система нормативно закрепленных понятий (далее приведены наиболее важные): «данные», «база данных», «обработка данных», «массив данных», «тип данных», «файл», «метаданные», «структурированные данные», «неструктурированные данные» определены в ГОСТ Р ИСО/МЭК 20546-2021 «Национальный стандарт Российской Федерации. Информационные технологии. Большие данные. Обзор и словарь» [7]; «база данных» определена в части 2 статьи 1260 ГК РФ [8]; «информация», «информационные технологии», «информационная система», «информационно-телекоммуникационная сеть», «обладатель информации», «доступ к информации», «конфиденциальность информации», «предоставление информации», «распространение информации», «электронное сообщение», «документированная информация», «электронный документ», «оператор информационной системы», «сайт в сети Интернет», «страница сайта в сети Интернет», «доменное имя», «сетевой адрес», «владелец сайта в сети Интернет», «провайдер хостинга», «поисковая система» определены в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [9], «блокирование данных», «уничтожение данных» определены в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» [10].

Верхнеуровневым понятием, объединяющим всё вышеперечисленное, является понятие «информационно-коммуникационные технологии» как совокупность информационных технологий, информационных систем и информационно-телекоммуникационных сетей, необходимых для реализации полномочий государственных органов и обеспечения их деятельности; это определение дано в пункте 2 Положения о ведомственных программах цифровой трансформации, утвержденного постановлением Правительства Российской Федерации от 10 октября 2020 г. № 1646 [11]. Понятие «информационно-коммуникационные технологии» быстро стало востребовано вне государственных информационных систем и сегодня применяется в качестве универсального, о чем свидетельствует ранее упомянутый Указ Президента Российской Федерации от 30 сентября 2022 года № 688.

Обновленный понятийно-категориальный аппарат позволяет сделать определенные выводы о сложившейся практике квалификации преступлений и особенностях доказывания на стадии предварительного расследования. Квалификация преступлений в строгом соответствии с Уголовным кодексом основывается на признаках преступного деяния, осуществляемого в отношении предмета преступления, в качестве которого выступают только отдельные компоненты информационно-коммуникационных технологий. Так видел в середине 90-х годов прошлого века IT-сферу законодатель – разрозненно, в декомпозиции, не выделяя информационные технологии в целом как предмет

преступления и не обеспечивая их правовую защиту. В результате правовой «беззащитности технологий» в настоящее время отсутствует возможность адекватной квалификации как нового вида преступлений:

– атак, направленных на технологии автоматизации инфраструктуры экономики (атаки с помощью программ-шифровальщиков на информационные системы малых и средних организаций, предприятий, крупных корпораций);

– атак с помощью аукционных роботов, направленных на технологии электронных торгов [12];

– любых иных атак, направленных на информационно-коммуникационные технологии.

Следствием стало то, что привычная квалификация деяний по принципу «похожести на…» посредством статей 272 УК РФ, 273 УК РФ и иных давно перестала соответствовать масштабу преступлений с использованием информационно-коммуникационных технологий и размеру причиненного предприятиям, учреждениям, организациям ущерба. Решение этой задачи находится не только в компетенции законодателя, но в целях проработки отдельных ее теоретических и практических аспектов – в компетенции научного сообщества.

Органами предварительного расследования не освоены и не применяются фактически имеющиеся новые технологические и правовые инструменты доказывания, основанные на понятии «информационно-коммуникационная технология» и учитывающие тот факт, что преступление оставляет единый взаимосвязанный комплекс цифровых следов не на одном электронном носителе информации устройства, с которым работает пользователь, а в той или иной степени на всех носителях информации устройств, в некоторый период времени взаимодействовавших в рамках конкретной информационно-коммуникационной технологии с этим устройством и обеспечивавших его функциональность.

Например, при выемке мобильного телефона, модель которого не поддерживается имеющимися в распоряжении экспертов аппаратно-программными комплексами, и который заблокирован, следователь с учетом извещений экспертов о невозможности получить доступ к содержимому памяти устройства принимает, как ему кажется, единственное возможное решение – не использовать в доказывании недоступные ему данные, содержащиеся в памяти мобильного устройства. Вместе с тем, мобильный телефон в процессе предшествующей эксплуатации являлся оконечным оборудованием данных одновременно для нескольких криминалистически значимых информационно-коммуникационных технологий:

– информационно-коммуникационной технологии сотовой связи;

– информационно-коммуникационных технологий обмена сообщениями (например, с помощью сервисов WhatsApp, Viber, Telegram, иных);

– информационно-коммуникационных технологий облачного хранения данных в качестве самостоятельного сервиса (Яндекс.Диск, «Облако Mail.Ru», iCloud, иных);

– информационно-коммуникационных технологий облачного хранения данных в качестве сервиса прикладной программы (Microsoft OneDrive) или сервиса как составной части пакета услуг (Google Drive).

Для информационно-коммуникационной технологии сотовой связи определенная часть данных заблокированного мобильного устройства и о нем отображена в содержимом домашнего регистра местоположения (HLR), гостевого регистра местоположения (VLR) и иных наборов (баз) данных оператора связи. Получить такую информацию возможно в порядке, предусмотренном статьей 186.1 УПК РФ, в ходе допроса сотрудника оператора связи, а также в ходе иных следственных действий, проводимых с участием специалиста в месте размещения технических средств оператора связи и соответствующих наборов (баз) данных на их носителях информации.

Для информационно-коммуникационных технологий обмена сообщениями, облачного хранения данных в качестве самостоятельного сервиса, в качестве сервиса прикладной программы или сервиса как составной части пакета услуг, возможна ситуация, когда аутентификация и авторизация в сервисе проводится при помощи SIM-карты и/или логина и пароля. В этом случае имеется техническая возможность переставить SIM-карту из интересующего устройства в иное «чистое» мобильное устройство, поддерживаемое экспертным аппаратно-программным комплексом, установить соответствующие приложения и попытаться получить доступ к сервисам, выполнив аутентификацию и авторизацию с помощью SIM-карты, а также паролей, используемых на иных устройствах пользователя (ноутбуке, компьютере, мобильных телефонах). При благоприятном стечении обстоятельств доступ к сервисам может быть получен, и если информационно-коммуникационная технология предусматривает возможность полной или частичной синхронизации данных в оконечном оборудовании данных, то такая синхронизация может быть выполнена сервисами, после чего устройство может быть исследовано. Перечисленный прием фактически является приемом подмены одного оконечного оборудования данных другим в информационно-коммуникационной технологии и является недопустимым с точки зрения привычных подходов, однако не то же ли самое мы делаем с изъятым электронным носителем информации, подключая его не к «родному» компьютерному средству, где он эксплуатировался, а совершенно к иному – ноутбуку специалиста, эксперта? Ведь и в этом случае локальная информационно-коммуникационная технология воспроизводится с новым набором ее компонент без опасений всех участников судопроизводства, что это приведет к утрате доказательства.

Таким образом, информационно-коммуникационные технологии – это не только технологическая особенность нашего времени, но и шаблоны мышления всех участников судопроизводства, преодолеть которые необходимо со временем, а также подлежащие решению силами профессионального сообщества следующие задачи: задача изучения криминалистически значимых информационно-коммуникационных технологий и выделение их технико-криминалистических особенностей; задача определения набора компонент

каждой информационно-коммуникационной технологии, необходимых для получения доступа к данным, возможно содержащим ориентирующую и доказательственную информацию по делу; задача определения действий технического характера, выполняемых специалистом или экспертом для получения доступа к данным и получения самих данных; задача определения требований к выполняемым техническим операциям, обеспечивающих относимость и допустимость доказательств; задача криминалистической фиксации проводимых действий и их результатов; задача валидации полученных результатов.

В связи с тем, что в основе концепции информационно-коммуникационных технологий лежат процессы обработки данных, мы назвали предлагаемый подход к получению цифровых доказательств процессным в отличие от объектового, когда из всех компонент информационно-коммуникационных технологий следственный интерес представляют только электронные носители информации оконечного оборудования или серверов в отрыве от конкретной информационно-коммуникационной технологии. Продуктивны ли наши предложения – покажет время и результаты совместной работы.

Список литературы

1. Бертовский, Л.В. К вопросу о понятии киберпреступления / Л.В. Бертовский // Расследование преступлений: проблемы и пути их решения. 2020. № 4 (30). С.84-88.
2. Кибер // Википедия. Свободная энциклопедия. - URL: https://ru.wikipedia.org/wiki/Кибер.
3. Воройский, Ф.С. Информатика. Введение в современные информационные и телекоммуникационные технологии в терминах и фактах: Энциклопедический словарь-справочник / Ф.С. Воройский. Москва: ФИЗМАТЛИТ, 2006. 768 с.
4. Перечень отраслей экономики // Федеральная служба государственной статистики. - URL: https://www.gks.ru/bgd/free/B99_10/IssWWW.exe/Stg/d020/i020210r.htm.
5. Высокие технологии // Экономическая энциклопедия. - URL: https://vocable.ru/termin/vysokie-tehnologii.html.
6. О внесении изменений в некоторые акты Президента Российской Федерации: указ Президента Рос. Федерации от 30 сент. 2022 г. № 688 // Официальный интернет-портал правовой информации. Москва, 30.09.2022. – URL: http://publication.pravo.gov.ru/Document/View/0001202209300029.
7. ГОСТ Р ИСО/МЭК 20546-2021. Национальный стандарт Российской Федерации. Информационные технологии. Большие данные. Обзор и словарь // СПС «КонсультантПлюс».
8. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 05.12.2022 г.) // СПС «КонсультантПлюс».

9. Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 29.12.2022) «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».

10. Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 14.07.2022 г.) «О персональных данных» // СПС «КонсультантПлюс».

11. Постановление Правительства Российской Федерации от 10.10.2020 г. № 1646 (ред. от 01.02.2023 г.) «О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти и органов управления государственными внебюджетными фондами» (вместе с «Положением о ведомственных программах цифровой трансформации»). // СПС «КонсультантПлюс».

12. Яковлев, А.Н. Уголовно-правовые меры против незаконного использования аукционных роботов / А.Н. Яковлев // Конкуренция и право. 2020. № 1. С. 21-29.

СОДЕРЖАНИЕ

ВЫСОКОТЕХНОЛОГИЧНОЕ ПРАВО: СОВРЕМЕННЫЕ ВЫЗОВЫ

Материалы IV Международной межвузовской научно-практической конференции

17-20 февраля 2023 года
Москва – Красноярск

Часть первая

Электронное издание

Издается в авторской редакции

Подписано в свет 25.05.2023 г.. Регистрационный номер 79
Редакционно-издательский центр Красноярского государственного аграрного университета 660017, Красноярск, ул. Ленина, 117