СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКАЯ АКАДЕМИЯ СЛЕДСТВЕННОГО КОМИТЕТА
ИМЕНИ А.Я. СУХАРЕВА

МЕЖДУНАРОДНЫЙ СОЮЗ КРИМИНАЛИСТОВ

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА РОССИЙСКОЙ АКАДЕМИИ НАУК

УГОЛОВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧЕЛОВЕЧЕСТВА

Материалы международной научно-практической конференции

(Москва, 13–14 февраля 2025 года)

Москва, 2025

УДК 004.056+343.1/.9
ББК 67.408+67.52+67.73

У26 **Уголовно-правовое обеспечение информационной безопасности человечества**: материалы международной научно-практической конференции (Москва, 13–14 февраля 2025 года). М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2025. – 141 с.

Сборник сформирован по материалам, представленным участниками международной научно-практической конференции, проведенной в Следственном комитете Российской Федерации и Московской академии Следственного комитета имени А.Я. Сухарева 13–14 февраля 2025 года. Мероприятие организовано при участии Следственного комитета Российской Федерации, Института государства и права Российской академии наук и Международного союза криминалистов. В конференции приняли участие около 500 человек, включая представителей республик Азербайджан, Беларусь, Казахстан, Болгария, Индия, Сербия.

Сборник предназначен для юристов – учёных и практиков, а также для всех, кто интересуется вопросами обеспечения информационной безопасности уголовно-правовыми средствами.

Редакционная коллегия обращает внимание, что научные подходы, идеи и взгляды, изложенные в статьях сборника, отражают субъективные оценки их авторов.

Международная научно-практическая конференция «Уголовно-правовое обеспечение информационной безопасности человечества»

(Москва, 13–14 февраля 2025 года)

Следственный комитет Российской Федерации (далее – Следственный комитет) совместно с Международным союзом криминалистов и Институтом государства и права Российской академии наук организовал проведение международной научно-практической конференции «Уголовно-правовое обеспечение информационной безопасности человечества».

13 февраля 2025 года в здании Следственного комитета состоялось её пленарное заседание, в котором принял участие Председатель Следственного комитета Российской Федерации Александр Иванович Бастрыкин, по решению которого организовано мероприятие.

Модератором пленарного заседания стал ректор Московской академии Следственного комитета имени А.Я. Сухарева Алексей Александрович Бессонов.

Председатель Следственного комитета Российской Федерации А.И. Бастрыкин открывает работу пленарного заседания конференции 13 февраля 2025 года[1]

Открывая пленарное заседание, А.И. Бастрыкин выступил с докладом на тему «Роль Следственного комитета России в обеспечении информационной безопасности человечества». Он озвучил, что наблюдается рост преступных

[1] Информация о первом дне работы конференции приведена в соответствии с новостью, размещённой на официальном сайте Следственного комитета: В Следственном комитете состоялось пленарное заседание Международной научно-практической конференции, посвященной информационной безопасности. URL: https://sledcom.ru/press/ events/item/1953797.

деяний, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации: «В Российской Федерации за 7 лет число указанных преступлений выросло в 7,5 раз, а их удельный вес – с 15 % до 40 %. В 2024 году их зарегистрировано 765,4 тыс., что на 13,1 % больше, чем в 2023 году, в том числе тяжких и особо тяжких составов – на 7,8 %». В 2024 году Следственным комитетом расследовано более 23 787 преступлений, совершённых с применением современных цифровых средств, что на 9,6 % больше, чем в 2023 году. Две трети из расследованных ведомством преступных деяний связаны с использованием интернет-ресурсов.

Глава Следственного комитета отметил, что в результате целенаправленной деятельности ряда иностранных государств и организаций, использующих распространение выгодных им установок деструктивного информационно-психологического воздействия, человечество столкнулось с угрозой утраты традиционных духовно-нравственных ориентиров и устойчивых моральных принципов. Особенно этому подвержено молодое поколение. В 2024 году практически каждое пятое расследованное в Следственном комитете преступление в сфере информационных технологий совершено несовершеннолетними.

Председатель Следственного комитета Российской Федерации А.И. Бастрыкин

А.И. Бастрыкин напомнил присутствующим о фактах вооруженных публичных нападений несовершеннолетних учащихся на учебные заведения. В большинстве случаев дети были зарегистрированы в социальных сетях, где и находили информацию об аналогичных преступлениях, общались на эту тематику. Также у подростков наблюдались проблема социализации и трудности в общении со сверстниками. В этой связи глава Следственного комитета отметил важность активизации работы по предотвращению увлечения

детей идеями деструктивных движений и сообществ, подчеркнув, что сейчас также идет широкая пропаганда украинского национализма, дискредитация российских вооружённых сил и органов государственной власти.

Председатель Следственного комитета подробно рассказал о проводимой ведомством работе, направленной на защиту традиционных российских духовно-нравственных ценностей. В образовательных организациях Следственного комитета кадеты и курсанты наравне с профильными предметами и дисциплинами изучают основы военно-патриотической подготовки, участвуют в различных мероприятиях и проектах, оказывают помощь и поддержку социальным учреждениям, ветеранам Великой Отечественной войны, участникам специальной военной операции.

Члены президиума первого дня работы конференции, слева направо: Председатель комиссии Совета Федерации Федерального Собрания Российской Федерации по информационной политике и взаимодействию со СМИ Комитета по конституционному законодательству и государственному строительству А.К. Пушков, директор Института государства и права Российской академии наук А.Н. Савенков, председатель Научного совета Российской академии наук «Информационная безопасность» И.А. Шеремет

В числе других важнейших задач, стоящих перед Следственным комитетом, глава ведомства назвал работу, направленную на увековечение памяти жертв геноцида советского народа в годы Великой Отечественной войны. Во многих регионах России судами вынесены решения о признании геноцидом преступлений фашистов, в основу которых легли доказательства, собранные Следственным комитетом. Председатель Следственного комитета осветил статистические данные о расследовании уголовных дел о реабилитации нацизма и диверсиях, экстремистской направленности, в отношении военнослужащих украинских вооруженных формирований, в том числе иностранных наемников.

Вместе с тем А.И. Бастрыкин отметил, что информационные технологии внедрены и в практическую деятельность. В этом году утверждена Концепция цифровой трансформации деятельности Следственного комитета, направленная на оптимизацию работы ведомства. Отмечено, что в Следственном комитете уже эксплуатируется ряд информационных систем, однако планируется создание высокотехнологичной лаборатории для проведения исследований электронных носителей информации, активное развитие систем биометрической идентификации и других направлений. В Следственном комитете организован сплошной мониторинг медиапространства. «За прошлый год по материалам СМИ, социальных сетей и мессенджеров возбуждено 2779 уголовных дел», – озвучил Александр Иванович.

Также он напомнил присутствующим о законодательных инициативах ведомства в части признания цифровой валюты имуществом и установления ответственности за распространение деструктивного контента.

В завершение выступления глава Следственного комитета подчеркнул, что для эффективного противодействия киберпреступности необходима консолидация усилий всего мирового сообщества, исключающая политическую составляющую, поскольку речь идет о безопасности человечества.

Члены президиума первого дня работы конференции, слева направо: ректор Московской академии Следственного комитета имени А.Я. Сухарева А.А. Бессонов, начальник Института повышения квалификации и переподготовки Следственного комитета Республики Беларусь Ю.Ф. Каменецкий, Министр цифрового развития, связи и массовых коммуникаций Российской Федерации М.И. Шадаев

С докладами выступили Председатель комиссии Совета Федерации Федерального Собрания Российской Федерации по информационной политике и взаимодействию со СМИ Комитета по конституционному законодательству и государственному строительству Алексей Константинович Пушков, Министр юстиции Российской Федерации Константин Анатольевич Чуйченко, Министр

цифрового развития, связи и массовых коммуникаций Российской Федерации Максут Игоревич Шадаев, директор института государства и права Российской академии наук Александр Николаевич Савенков, председатель Научного совета Российской академии наук «Информационная безопасность» Игорь Анатольевич Шеремет и начальник Института повышения квалификации и переподготовки Следственного комитета Республики Беларусь Юрий Францевич Каменецкий. В своих докладах спикеры осветили вопросы правового обеспечения информационной безопасности мирового сообщества, уголовно-правовой охраны информационной безопасности в России и за рубежом, уголовно-правовых рисков развития перспективных информационных технологий, криминалистического, оперативно-разыскного и судебно-экспертного обеспечения информационной безопасности человечества.

Участники конференции – учащиеся ведущих образовательных организаций

В первом дне работы конференции, в том числе по видео-конференц-связи, приняли участие сотрудники Следственного комитета, российские государственные и общественные деятели, учёные и практикующие специалисты в области кибербезопасности из Беларуси, Казахстана, Сербии и Болгарии, а также учащиеся ведущих образовательных организаций.

Обсуждение актуальных вопросов обеспечения информационной безопасности человечества продолжено 14 февраля 2025 года на базе Московской академии Следственного комитета имени А.Я. Сухарева.

В число членов президиума второго дня работы конференции вошли ректор Московской академии Следственного комитета имени А.Я. Сухарева, доктор

юридических наук, доцент генерал-майор юстиции Алексей Александрович Бессонов; начальник Института повышения квалификации и переподготовки Следственного комитета Республики Беларусь, кандидат юридических наук, доцент полковник юстиции Юрий Францевич Каменецкий; первый проректор академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, доктор юридических наук, профессор старший советник юстиции Калиолла Кабаевич Сейтенов; заведующая кафедрой судебных экспертиз, научный руководитель института судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, заслуженный деятель науки Российской Федерации, академик РАЕН Елена Рафаиловна Россинская.

Заседание открыл ректор Московской академии Следственного комитета имени А.Я. Сухарева А.А. Бессонов.

В своем приветственном слове первый заместитель председателя Комитета Государственной Думы по защите семьи, вопросам отцовства, материнства и детства Татьяна Викторовна Буцкая подчеркнула высокую значимость работы по противодействию влияния на детей деструктивного контента и осветила законодательные инициативы в этой сфере.

Презентация монографии Ю.Ф. Каменецкого «Теория и практика следственной профилактики»

Затем состоялась торжественная церемония награждения. По поручению Председателя Следственного комитета Российской Федерации Александра Ивановича Бастрыкина ректор Московской академии Следственного комитета имени А.Я. Сухарева А.А. Бессонов вручил ведомственные награды – памятные медали Следственного комитета «70 лет службе криминалистики» Ю.Ф. Каменецкому, К.К. Сейтенову, профессору кафедры судебных экспертиз

Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), доктору юридических наук, профессору, заслуженному юристу Российской Федерации, почётному работнику высшего профессионального образования Российской Федерации А.М. Зинину; профессору кафедры оружиеведения и трасологии учебно-научного комплекса судебной экспертизы Московского университета МВД России имени В.Я. Кикотя, доктору юридических наук, профессору, заслуженному деятелю науки Российской Федерации Н.П. Майлис.

Ю.Ф. Каменецкий презентовал участникам подготовленную им монографию «Теория и практика следственной профилактики», в которой рассмотрены теоретические, правовые, организационные, тактические, технические и методические аспекты этой деятельности, даны рекомендации сотрудникам правоохранительных органов.

Выступление К.К. Сейтенова было посвящено деятельности Регионального хаба по направлению «Противодействие киберпреступности» в Республике Казахстан.

Ректор Московской академии Следственного комитета имени А.Я. Сухарева А.А. Бессонов вручает памятную медаль Следственного комитета «70 лет службе криминалистики» Ю.Ф. Каменецкому

Е.Р. Россинская в своём докладе раскрыла вопросы прогнозирования развития методологии и технологий судебных экспертиз в условиях цифровизации для обеспечения информационной безопасности социума.

С докладами также выступили профессор кафедры оружиеведения и трасологии учебно-научного комплекса судебной экспертизы Московского университета МВД России имени В.Я. Кикотя Н.П. Майлис, преподаватель и руководитель лаборатории кибербезопасности УниБИТ, преподаватель по цифровой криминалистике Академии МВД (Болгария) А.Н. Кирков; декан

факультета истории, политологии и права Государственного университета просвещения В.Э. Багдасарян, профессор кафедры судебно-экспертной и оперативно-разыскной деятельности Московской академии Следственного комитета имени А.Я. Сухарева, профессор кафедры криминалистики Московского университета МВД России имени В.Я. Кикотя А.Ф. Волынский; заведующий отделом правовой статистики и информационного обеспечения прокурорской деятельности Университета прокуратуры Российской Федерации И.В. Горошко; начальник управления специальных мероприятий и расследования компьютерных инцидентов АО «Лаборатория Касперского» И.А. Рядовский и другие.

Участники второго дня работы конференции обсудили как глобальные, так и частные вопросы обеспечения информационной безопасности человечества.

В течение двух дней в мероприятии, в том числе по видео-конференц-связи, приняли участие свыше 500 человек, включая более 150 учёных и практиков, из которых порядка 30 докторов наук, 60 кандидатов наук. Международный формат мероприятия обеспечен участием в его работе представителей Российской Федерации, республик Азербайджан, Беларусь, Казахстан, Болгария, Индия, Сербия.

С докладом выступает доктор юридических наук, профессор, заслуженный деятель науки Российской Федерации, академик РАЕН Е.Р. Россинская

На конференции рассмотрены вопросы, касающиеся правового обеспечения информационной безопасности мирового сообщества, уголовно-правовой охраны информационной безопасности в России и за рубежом, уголовно-правовых рисков развития перспективных информационных технологий, криминалистического, оперативно-разыскного и судебно-экспертного обеспечения информационной безопасности человечества.

Центральными темами обсуждения стали взаимосвязь обеспечения информационной и национальной безопасности, противодействие

деструктивному информационному воздействию на детей, пропаганде неонацизма, дискредитации Вооружённых Сил Российской Федерации и органов государственной власти суверенных государств, посягательствам на историческую память и преемственность поколений.

Противодействие киберпреступности – глобальная задача, для решения которой необходима консолидация усилий всего мирового сообщества, налаживание сотрудничества учёных и практиков.

Поступившие от спикеров конференции рукописи научных статей направлены для опубликования в первом номере журнала «Мир криминалистики» за 2025 год.

Оргкомитет конференции

РЕЗОЛЮЦИЯ
Международной научно-практической конференции «Уголовно-правовое обеспечение информационной безопасности человечества»

В ходе конференции её участники обсудили следующие вопросы:

1. Правовое обеспечение информационной безопасности мирового сообщества.

2. Уголовно-правовая охрана информационной безопасности в России и за рубежом.

3. Уголовно-правовые риски развития перспективных информационных технологий.

4. Криминалистическое, оперативно-разыскное и судебно-экспертное обеспечение информационной безопасности человечества.

В результате обсуждения Международный союз криминалистов и участники конференции считают необходимым принять следующее:

1. Информационные технологии, несмотря на их повсеместное распространение, – лишь средство, которое должно служить законным интересам человека. Обеспечение информационной безопасности человечества как эффективного противодействия киберпреступности – глобальная задача, для решения которой необходима консолидация усилий всего мирового сообщества, в связи с чем в число важнейших задач входит налаживание сотрудничества ученых и практиков.

2. Информационная безопасность неразрывно связана с обеспечением национальной безопасности, основу которой составляют традиционные духовно-нравственные ценности. В настоящее время они поставлены под угрозу в результате целенаправленной деятельности ряда государств и организаций, являющихся сторонниками идей однополярного мироустройства, глобализма и трансгуманизма, использующих для распространения выгодных им установок деструктивное информационно-психологическое воздействие.

3. Особое внимание необходимо уделять обеспечению информационной безопасности детей. Это обусловливает необходимость комплексного подхода к выработке механизма противодействия негативному воздействию в отношении них. Поддержки заслуживает опыт создания центров информационной безопасности молодёжи и психологической помощи. Необходимо широко внедрять постоянное психологическое тестирование учащихся образовательных организаций для профилактики правонарушений в молодёжной среде и выявления групп риска.

5. Приоритетными направлениями уголовно-правового обеспечения информационной безопасности человечества являются противодействие: пропаганде неонацизма, дискредитации Вооружённых Сил Российской Федерации и органов государственной власти суверенных государств, посягательствам на историческую память и преемственность поколений, в первую очередь, связанным с попытками фальсификации итогов Второй мировой и Великой Отечественной войн, реабилитацией нацизма; диверсионной деятельности, организации массовых беспорядков.

Д.В. Алехин
Московская академия Следственного комитета
имени А.Я. Сухарева

Совершенствование законодательства как способ нейтрализации информационного воздействия на молодежь

Аннотация. Объектом исследования являются общественные отношения, связанные с правовым обеспечением механизмов ограничения распространения запрещенной законодательством Российской Федерации информации и ответственности за ненадлежащее выполнение обязанностей по недопущению ее распространения. Предмет исследования составила совокупность правовых норм и нормативных правовых актов, направленных на правовое урегулирование указанных общественных отношений. Выводы о том, что перечисленные в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» виды информации, в отношении которой должны приниматься меры по нераспространению, необходимо соотносить с положениями Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» об ответственности операторов поисковых систем, могут быть использованы в правотворческой работе.

Ключевые слова: блокировка, ответственность, контент, молодежь.

Вопросы дальнейшего совершенствования законодательства в области информационной безопасности продолжают оставаться актуальными так как в информационно-телекоммуникационных сетях (в том числе в сети Интернет) наблюдается ежегодный поступательный рост информации, негативно влияющей на психику и поведение несовершеннолетних, «наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей»[1]. В 2024 году по требованию Роскомнадзора владельцы ресурсов удалили запрещенный контент либо само ведомство ограничило доступ более чем к 700 тыс. интернет-страниц с противозаконными материалами, в 2023 году – к 560 тыс.[2] По данным Роскомнадзора, в информационно-телекоммуникационной сети Интернет растет распространение деструктивного контента. На основании судебных решений и требований Генпрокуратуры федеральная служба ограничила доступ (или владельцы удалили по ее требованию) более 3,5 тыс. материалов, которые призывали к

[1] Пункт 12 Доктрины информационной безопасности Российской Федерации, утвержденной указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074.

[2] Роскомнадзор раскрыл число удаленного запрещенного контента в Сети в 2024 году // https:// iz.ru/1838581/2025-02-13/roskomnadzor-raskryl-chislo-udalennogo-zapreshchenno-kontenta-v-seti-v-2024-godu (дата обращения: 20.02.2025).

массовым беспорядкам, что в 2,2 раза больше, чем в 2023 году. Объем заблокированного контента, который вовлекал несовершеннолетних в противоправные действия, увеличился почти в 1,5 раза до 33,2 тыс. материалов[1]. Все эти данные безусловно свидетельствуют о необходимости продолжения работы по совершенствованию законодательного механизма, связанного с пресечением распространения в информационно-телекоммуникационных сетях (в том числе в сети Интернет) указанной информации, в частности по внесению дополнений в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ) в целях введения возможности досудебной блокировки информации, причиняющей вред здоровью и (или) развитию детей.

Кроме того, особенно актуальным и своевременным указанное предложение выглядит в свете реализации основных принципов и положений Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей[2], Стратегии реализации молодежной политики в Российской Федерации на период до 2030 года[3]: формирование безопасного информационного пространства; защита российского общества от распространения, в том числе посредством информационно-телекоммуникационной сети Интернет, деструктивных материалов (контента), причиняющих вред здоровью и (или) физическому, психическому, духовному, нравственному развитию детей и молодежи, в том числе распространяющих идеологию терроризма и экстремизма, пропаганду антисемейных ценностей, нетрадиционных сексуальных отношений, потребления психоактивных веществ; реализация государственной информационной политики, направленной на усиление роли традиционных ценностей в массовом сознании и противодействие распространению деструктивной идеологии и др.

Обращаем внимание, что в законодательстве нет определения понятия «деструктивный контент». Такая формулировка явно характеризуются неопределенностью содержания, приводит к свободному толкованию, и, как следствие, к непоследовательности правоприменения, поэтому нуждается в согласовании с нормами действующего законодательства Российской Федерации, уже устанавливающими запрет на распространение информации, которая может быть отнесена к деструктивному контенту. Вместо понятия «деструктивный контент» считаем возможным использование понятия «информация, причиняющая вред здоровью и (или) развитию детей»,

---

[1] В Сети удалили в два раза больше деструктивного контента // https://iz.ru/1824956/2025-01-20/v-seti-udalili-v-dva-raza-bolse-destruktivnogo-kontenta (дата обращения: 20.02.2025).

[2] Указ Президента Российской Федерации от 9 ноября 2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // СЗ РФ. 2022. № 46. Ст. 7977.

[3] Распоряжение Правительства Российской Федерации от 17.08.2024 № 2233-р «Об утверждении Стратегии реализации молодежной политики в Российской Федерации на период до 2030 года» // СЗ РФ. 2024. № 36. Ст. 5484.

содержание и виды которой закреплены пунктом 7 статьи 2 и статьей 5 Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее – Федеральный закон № 436-ФЗ).

Федеральным законом № 149-ФЗ предусмотрены основания и механизмы, препятствующие распространению в информационном пространстве рассматриваемого контента. Так, на владельца социальной сети возложены обязанности не допускать использование социальной сети в целях распространения материалов, пропагандирующих порнографию, насилие и жестокость, и материалов, содержащих нецензурную брань (пункт 1 части 1 статьи 10.6.), а также осуществлять мониторинг социальной сети в целях выявления материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера (подпункт «а» пункта 5 части 1 статьи 10.6.), информации о способах совершения самоубийства, а также призывов к совершению самоубийства (подпункт «в» пункта 5 части 1 статьи 10.6.), информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц (подпункт «е» пункта 5 части 1 статьи 10.6., информации, пропагандирующей нетрадиционные сексуальные отношения и (или) предпочтения, педофилию, смену пола, отказ от деторождения (подпункт «и» пункта 5 части 1 статьи 10.6.) и другие.

На владельца новостного агрегатора, владельца аудиовизуального сервиса и владельца сервиса размещения объявлений также возложена обязанность не допускать использование принадлежащих им информационных ресурсов в целях распространения материалов, пропагандирующих порнографию, насилие и жестокость, и материалов, содержащих нецензурную брань (статьи 10.4., 10.5. и 10.7. Федерального закона № 149-ФЗ).

Сходные положения содержатся в статье 15.1. Федерального закона № 149-ФЗ, устанавливающей порядок внесудебного ограничения доступа к информационным ресурсам в сети Интернет.

Кроме того, статьей 15.3. Федерального закона № 149-ФЗ установлен порядок ограничения доступа в информационном пространстве к такому явлению, как «треш-стримы», то есть информации, оскорбляющей человеческое достоинство и общественную нравственность, выражающей явное неуважение к обществу, содержащей изображение действий с признаками противоправных, в том числе насильственных, и распространяемой из хулиганских, корыстных или иных низменных побуждений (подпункт 7.1 части 1).

Вместе с тем, полагаем, что с целью обеспечения единства правоприменения, перечисленные в Федеральном законе № 149-ФЗ виды информации, в отношении которой должны приниматься меры по нераспространению, необходимо соотносить с положениями статьи 5 Федерального закона № 436-ФЗ.

Еще одно направление совершенствования законодательства в сфере информационной безопасности связано с предотвращением невыполнения обязанностей по ограничению доступа к информации, распространение которой в общедоступном информационном пространстве запрещено законодательством Российской Федерации.

Так, часть 2 статьи 13.50 Кодекса Российской Федерации об административных правонарушениях (Неисполнение обязанностей владельцем социальной сети) устанавливает, что за неисполнение владельцем социальной сети обязанности по принятию мер по ограничению доступа к информации, указанной в пункте 5 части 1 статьи 10.6 Федерального закона № 149-ФЗ) влечет наложение административного штрафа. Речь идет о материалах с порнографическими изображениями несовершеннолетних и (или) объявлениях о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера (подпункт «а» пункта 5 части 1 статьи 10.6.), об информации о способах совершения самоубийства, а также призывов к совершению самоубийства (подпункт «в» пункта 5 части 1 статьи 10.6.), информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц(подпункт «е» пункта 5 части 1 статьи 10.6.), информации, пропагандирующей нетрадиционные сексуальные отношения и (или) предпочтения, педофилию, смену пола, отказ от деторождения (подпункт «и» пункта 5 части 1 статьи 10.6.) и другие.

Также Кодексом Российской Федерации об административных правонарушениях предусмотрена ответственность владельца новостного агрегатора и владельца аудиовизуального сервиса за неисполнение предписаний федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о прекращении распространения новостной информации (статья 19.7.10-1), об устранении выявленных нарушений законодательства Российской Федерации (статья 19.7.10-2).

Следует отметить, что ответственность владельца сервиса размещения объявлений за использование принадлежащих ему информационных ресурсов в целях распространения материалов, пропагандирующих порнографию, насилие и жестокость, и материалов, содержащих нецензурную брань (статья 10.7. Федерального закона № 149-ФЗ) в Кодексе Российской Федерации об административных правонарушениях не установлена.

Что касается оператора поисковых систем (статья 10.3. Федерального закона № 149-ФЗ), то законодатель не закрепил в качестве обязанности принятие им мер, ограничивающих доступ к информации, причиняющей вред здоровью и (или) развитию детей. В соответствии с положениями пункта 3 части 1 статьи 1.3 Кодекса административная ответственность устанавливается по вопросам, имеющим федеральное значение, в том числе за нарушение правил и норм, предусмотренных федеральными законами и иными нормативными правовыми

актами Российской Федерации. Соответственно, говорить об ответственности оператора поисковых систем за ненадлежащее и несвоевременное исполнение сроков блокировки и удаления информации, причиняющей вред здоровью и (или) развитию детей, можно только после внесения изменений в Федеральный закон № 149-ФЗ.

Таким образом, полагаем, что в российский правопорядок целесообразно внести ряд новелл, направленных на совершенствование механизмов противодействия распространению среди молодежи рассматриваемой информации и повышение ответственности за ненадлежащее и несвоевременное выполнение обязанности по ее блокировке и удалению.

Список источников

1. Доктрина информационной безопасности Российской Федерации, утв. указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074.
2. Указ Президента Российской Федерации от 9 ноября 2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // СЗ РФ. 2022. № 46. Ст. 7977.
3. Распоряжение Правительства Российской Федерации от 17.08.2024 № 2233-р «Об утверждении Стратегии реализации молодежной политики в Российской Федерации на период до 2030 года» // СЗ РФ. 2024. № 36. Ст. 5484.

А.С. Бадмаев
Байкальский государственный университет

Полномочия прокурора по передаче уголовных дел из дознания в следствие в контексте преступлений против информационной безопасности

Аннотация. В статье рассматриваются полномочия прокурора по определению подследственности уголовных дел и связанные с этим проблемы их законодательного регулирования. Обращается внимание на значимость института подследственности как элемента уголовно-процессуального права в контексте информационной безопасности, поскольку современная преступность отличается в ряде случаев высокой технологической сложностью, трансграничным характером и необходимостью оперативного реагирования. Сделан акцент на исследование форм предварительного расследования преступлений, что необходимо в условиях цифровизации и роста киберугроз для обеспечения эффективного расследования, защиты прав граждан и сохранения целостности критической инфраструктуры. Отмечены некоторые проблемы цифровизации уголовного процесса, как средства обеспечения информационной безопасности. Автор приходит к выводу о значительной роли

координирующей деятельности прокурора в рамках определения подследственности между дознанием и следствием.

Ключевые слова: уголовный процесс, подследственность, прокурор, полномочия, уголовные дела, предварительное следствие, дознание.

В рамках уголовного судопроизводства институт подследственности выступает ключевым системообразующим элементом, который обеспечивает рациональное распределение уголовных дел между следственными органами. Его правовое регулирование, зафиксированное в положениях Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ), устанавливает компетенцию органов предварительного расследования, в зависимости от категории преступления, субъекта совершения деяния и иных значимых факторов. Важность данного института обусловлена не только его функциональной значимостью в организации предварительного расследования, но и непосредственным влиянием на соблюдение прав участников судопроизводства, легитимность уголовного преследования и общую эффективность системы правосудия.

Подследственность, как правовой институт, устанавливает границы полномочий следственных органов, исключая возможность дублирования их деятельности, что способствует рациональному использованию ресурсов различных ведомств, что, в свою очередь, повышает качество, оперативность и результативность расследования. Кроме того, данный институт минимизирует риски возникновения конфликтов юрисдикции между правоохранительными структурами и создает правовую определенность как для граждан, так и для самих органов предварительного расследования преступлений.

Уголовно-процессуальное законодательство России определяет две формы предварительного расследования: предварительное следствие и дознание, от которых во многом зависит правильность установления подследственности, т.е. выбор органа, должностного лица (следователя или дознавателя), осуществляющих предварительное расследование, законность производимых процессуальных действий и допустимость доказательств в уголовном процессе как на досудебной, так и судебной стадии.

В этой связи следует уделить внимание полномочиям прокурора по определению подследственности уголовных дел, поскольку именно прокурор выступает субъектом уголовного судопроизводства, на которого возложена обязанность по координации деятельности органов внутренних дел, федеральной службы безопасности, таможенной службы и других правоохранительных органов по борьбе с преступностью, согласно ч. 1 ст. 8 Федерального закона «О прокуратуре Российской Федерации»[1].

[1] Федеральный закон от 17 января 1992 № 2202-1 «О прокуратуре Российской Федерации» (ред. от 30.09.2024 г.) // СЗ РФ. 1995. № 47. Ст. 4472.

УПК РФ предоставляет прокурору следующие полномочия, связанные с подследственностью уголовных дел:

– изымать уголовное дело из органа дознания и передавать его следователю (п. 11 ч. 2 ст. 37 УПК РФ);

– по своему письменному указанию передавать для производства дознания некоторые уголовные дела, по котором обязательно производство предварительного следствия (п. 2 ч. 3 ст. 150 УПК РФ);

– передавать уголовное дело из одного следственного органа в другой с соблюдением правил подследственности, установленных ст. 151 УПК РФ (п. 12 ч. 2 ст. 37 УПК РФ);

– передавать любое уголовное дело следователю Следственного комитета Российской Федерации (далее – СК России) (данное полномочие вытекает из совокупного анализа положений ч. 4 ст. 150 УПК РФ и п. 12 ст. 37 УПК РФ);

– разрешать споры о подследственности (ч. 8 ст. 151 УПК РФ).

Таким образом, как обоснованно указывает И. С. Дикарев, эти полномочия свидетельствует о наличии у СК России «исключительной подследственности»[1]. Данный термин подразумевает под собой не стандартное распределение уголовных дел между органами следствия в соответствии с их юрисдикцией, а специальное правомочие следователей СК России принимать к производству любое уголовное дело, независимо от предметной или территориальной подследственности. Однако реализация этого права возможна исключительно при наличии санкции прокурора: именно он уполномочен вынести процессуальное решение о передаче дела следователю СК России, даже если это противоречит общим правилам, закрепленным в ст. 151 УПК РФ. Таким образом прокурорский надзор выступает обязательным условием применения исключительных полномочий следователей СК России в обход стандартных норм подследственности. Однако у прокурора отсутствуют полномочия по изъятию уголовного дела из производства следователя СК России и передаче его в другой следственный орган (за исключением случаев нарушения следователем правил подследственности), что нельзя признать в полной мере обоснованным[2].

В УПК РФ содержится перечень конкретных составов преступлений, закрепленных в Уголовном кодексе Российской Федерации (далее – УК РФ), по которым производится дознание. Этот перечень не является закрытым, поскольку в п. 2 ч. 3 ст. 150 УПК РФ установлено, что дознание может производится и по уголовным делам об иных преступлениях, но при условии соблюдения категории тяжести: небольшой и средней. При этом возможность такого производства прямо зависит только от воли прокурора, которая должна быть выражена в его письменном указании. Аналогичное указание необходимо и в случае передачи уголовных дел, предусмотренных п. 1 ч. 3 ст. 150, для

---

[1] Дикарев И. С. Подследственность в уголовном процессе: вопросы теории и законодательной регламентации // Журнал российского права. 2020. № 4. С. 115.

[2] Гриценко Д. В. Актуальные проблемы определения прокурором подследственности уголовных дел // Вестник Воронежского государственного университета. Серия: Право. 2021. №4 (47). С. 103–109.

производства предварительного следствия (ч. 4 ст. 150 УПК РФ). Передать уголовное дело из дознания в следствие прокурор вправе на любой досудебной стадии уголовного процесса, в том числе при вынесении обвинительного акта, что отражено в п. 4 ч. 1 ст. 226 УПК РФ.

Анализ указанных положений закона позволяет сделать вывод о том, что по делам, указанным в ч. 3 ст. 150 УПК РФ, производство предварительного расследования осуществляется как в форме предварительного следствия, так и форме дознания. В случае возникшей необходимости переквалификации совершенного общественно опасного деяния либо сложности расследуемого дела, что противоречит сущности дознания, прокурор передает уголовное дело от дознавателя следователю. Необходимость подобной передачи может возникнуть, например, если в ходе дознания выясняется, что деяние подпадает под категорию тяжкого преступления и, соответственно, согласно нормам о подследственности требует производства предварительного следствия.

Особенно важно рассмотреть данный вопрос с точки зрения обеспечения информационной безопасности, как актуальной сферы совершения преступлений. Так, рост числа киберпреступлений (включая атаки на критическую инфраструктуру, утечки персональных данных, фишинг) требует слаженного взаимодействия органов дознания и следствия, а также внимательного прокурорского надзора. Например, при производстве дознания по мошенничеству в сфере компьютерной информации (ч. 1 ст. 159^6 УК РФ), что отнесено к подследственности дознания, может быть выявлен факт взлома информационной базы данных и получения неправомерного доступа к охраняемой законом информации (ст. 272 УК РФ). В таком случае необходимо оперативное вмешательство прокурора в процесс расследования с целью передачи уголовного дела в органы следствия либо же принятия решения о производстве дознания по преступлению, предусмотренному ст. 272 УК РФ, если позволяет категория тяжести преступления.

При принятии прокурором решения о передаче уголовного дела, связанного с нарушением информационной безопасности, от дознавателя к следователю органов внутренних дел или СК России, эффективность механизма этого процессуального действия зависит от ряда факторов: профессиональной подготовки дознавателей и прокуроров в IT-сфере, что позволяет на ранних стадиях расследования выявить признаки информационного преступления и необходимости обращения к правилам определения подследственности; должного уровня межведомственной координации, которая крайне необходима для оперативного разрешения ситуации, препятствующей дальнейшему расследованию при применении изначальной формы предварительного расследования; оперативности передачи материалов из дознания в следствие, что связано с возможностью утраты цифровых следов преступления.

В ходе производства предварительного следствия могут быть установлены такие обстоятельства, которые повлияют на квалификацию совершенного преступления и вызовут необходимость изменить предметную подследственность с последующей передачей уголовного дела дознавателю (например, в случае отсутствия квалифицирующих признаков, в соответствии с

которыми преступление относится к подследственности органов предварительного следствия). В законе прямых указаний относительно этого не содержится. Некоторые авторы придерживаются мнения о необходимости применения аналогичного порядка передачи по подследственности через прокурора с принятием решения следователем, в производстве которого находится уголовное дело, по согласованию с руководителем следственного органа[1]. В этой связи следует отметить, что в УПК РФ не содержится нормы, допускающей применение аналогии закона в уголовном процессе, а также то, что при производстве дознания должны строго соблюдаться ограниченные сроки расследования, которые могут быть неоднократно нарушены уже при поступлении уголовного дела дознавателю. На наш взгляд отсутствие законодательного регулирования обратного порядка передачи уголовного дела, т.е. от следователя к дознавателю, может свидетельствовать не о пробеле в законе, а о намеренном упущении законодателя в целях оптимизации предварительного расследования.

В контексте информационной безопасности следует обратить особое внимание на широкое развитие цифровых технологий, которые все шире и шире применяются в повседневной деятельности в различных сферах человеческой жизни. Значительное количество государственных органов оказывают государственные услуги с использованием электронного документооборота.

Однако уголовное судопроизводство по-прежнему прибегает в абсолютном большинстве случаев к бумажному носителю. Использование электронного документооборота в досудебных стадиях уголовного судопроизводства на практике практически отсутствует.

Как отмечают многие исследователи, в настоящее время ни правоохранительные органы, занимающиеся уголовным преследованием, ни участники уголовного судопроизводства не обладают достаточной готовностью к переходу на полноценный электронный документооборот в рамках уголовного процесса[2]. Такой качественный переход формата хранения информации позволил бы преобразовать уголовные дела, существующие в виде множества томов бумажных документов в полностью цифровой формат – на электронных носителях или в облачных хранилищах.

Внедрение электронного уголовного дела не только значительно сокращает физический объем материалов, занимаемых делом, но и существенно ускоряет и упрощает процессуальный контроль, а также прокурорский надзор за ходом предварительного расследования. Руководитель следственного органа и прокурор, осуществляющий надзор за соблюдением законности при расследовании уголовных дел как в форме предварительного следствия, так и в

---

[1] Логинова Н.Г. О недостатках законодательного регулирования порядка реализации решения о передаче по подследственности // Вестник Белгородского юридического института МВД России. 2018. № 2. С. 51.

[2] Долгов А.М. О необходимости правовой регламентации электронного документооборота при расследовании уголовного дела // Юридический вестник Кубанского государственного университета. 2018. № 3. С. 33.

форме дознания, получают возможность работать в режиме реального времени. Это включает оперативное вынесение актов прокурорского реагирования надзирающим прокурором и мгновенное уведомление должностных лиц о принятых решениях. Подобный формат работы способствует обеспечению своевременности и прозрачности процесса, что положительно сказывается на эффективности выполнения участниками процесса своих служебных обязанностей и взаимодействия между ними.

Так, реализация решения прокурора о передаче уголовного дела для производства предварительного следствия в случае обнаружения дознавателем признаков более тяжкого преступления могло бы стать значительно эффективнее в виду практически мгновенного доступа ко всем материалам дела как прокурора, так и в дальнейшем следователя.

Одновременно цифровизация уголовного процесса порождает и ряд проблем, которые связаны с огромным количеством угроз в цифровой среде, например, возможность получения неизвестными лицами несанкционированного доступа к базе данных, где могут храниться электронные материалы уголовных дел, что повлечет существенный ущерб конфиденциальности содержащейся в них информации.

На основании изложенного можно сделать вывод, что производство уголовного преследования с использованием «электронного уголовного дела» порождает множество серьезных вопросов, требующих новых научных знаний и уточнения существующих.

Таким образом, нормы подследственности выступают гарантией обеспечения законности уголовного процесса. Некорректное распределение дел, например, производство предварительного расследования сложного преступления, связанного с цифровыми технологиями и информационной безопасностью, следственным органом, не обладающим технической экспертизой, может привести к нарушениям сроков расследования, ошибкам в квалификации деяния и к признанию доказательств недопустимыми в суде.

Перечисленные обстоятельства отражают необходимость координирующей деятельности прокурора, чья роль имеет существенное значение в осуществлении расследования уголовного дела. Данная область уголовно-процессуальной науки требует дальнейшего научного анализа и совершенствования, что необходимо в целях обеспечения объективности предварительного расследования.

Список источников

1. Гриценко Д.В. Актуальные проблемы определения прокурором подследственности уголовных дел / Д.В. Гриценко // Вестник Воронежского государственного университета. Серия: Право. 2021. № 4 (47). С. 103–109.

2. Дикарев И.С. Подследственность в уголовном процессе: вопросы теории и законодательной регламентации / И.С. Дикарев // Журнал российского права. 2020. № 4. С. 113–125.

3. Долгов А.М. О необходимости правовой регламентации электронного документооборота при расследовании уголовного дела // Юридический вестник Кубанского государственного университета. 2018. № 3. С. 32–35.
4. Логинова Н.Г. О недостатках законодательного регулирования порядка реализации решения о передаче по подследственности // Вестник Белгородского юридического института МВД России. 2018. № 2. С. 48–53.
5. Федеральный закон от 17 января 1992 № 2202-1 «О прокуратуре Российской Федерации» (ред. от 30.09.2024 г.) // СЗ РФ. 1995. № 47. Ст. 4472.

Е.А. Гром
Донбасский государственный университет юстиции

Уголовно-правовые риски развития технологий генеративного искусственного интеллекта

Аннотация. В статье рассмотрены теоретические аспекты потенциального использования генеративных моделей искусственного интеллекта в преступных целях. Новизна, общедоступность и непрерывное совершенствование технологий не позволяют на современном этапе спрогнозировать все возможные варианты общественно опасных деяний, в которых может быть использован искусственный интеллект лингвистического типа, определить их границы и последствия. На сегодня очевидно, что субъекты преступлений способны адаптировать технологии в качестве средства, орудия совершения «классических» общественно опасных деяний, а также использовать потенциал искусственного интеллекта для введения в правовое поле новых составов преступлений. В связи с этим, отмечены сложности, связанные с формированием основ правового регулирования в области разработки и использования технологии, криминализации деяний или формулирования обстоятельств, отягчающих деяния.

Ключевые слова: генеративный искусственный интеллект, языковая модель, уголовно-правовые риски

Цифровая трансформация ключевых отраслей экономики, социальной сферы, государственного сектора в процессе становления и развития носит противоречивый характер. Общество и государство признают очевидные преимущества внедрения цифровых технологий, но при этом не отрицают возможность наступления потенциальных негативных последствий[1], в том числе в уголовно-правовом поле. По мнению Т.А. Поляковой с коллегами, сегодня уголовно-правовые риски технологичной среды представлены соответствующей

[1] О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024). URL: https://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 16.02.2025).

группой преступлений в сфере компьютерной информации и квалифицирующими признаками, включёнными в отдельные составы преступлений. «Спектр применения информационных технологий в преступных целях расширяется, пополняется новыми подходами и методами»[1]. Несмотря на их высокую латентность, обусловленную анонимностью совершения и несообщением потенциальными потерпевшими о покушении на отдельные составы, наблюдается стабильный ежегодный прирост зарегистрированных преступлений, а также увеличение их удельного веса в общем числе преступлений[2]. Законодательство России, связанное со сферой высокотехнологичных областей, находится на стадии осмысления, о чем свидетельствует активность дискурсивного научного обсуждения и последовательная правотворческая деятельность. При этом наблюдается парадокс – человек получил инструменты для ускоренного оперирования информацией, но возможности для работы на опережение поступающим и потенциальным угрозам остались ограничены. Как справедливо отмечает Я.А. Коваленко, «Мы живём в условиях запоздалого реагирования на вызовы»[3]. Повсеместное и бесконтрольное использование «цифровыми» поколениями технологий искусственного интеллекта (далее – ИИ) вынуждает задуматься о последствиях его неправомерной эксплуатации, в том числе с точки зрения уголовно-правовых рисков.

Фундаментальные и прикладные исследования проблем высокотехнологичных решений требуют междисциплинарного подхода. Онтологию ИИ изучают А.И. Буравлев, В.М. Ветошкин, Ю.М. Малышев, А.Ю. Коловская, А.Д. Ильин и другие авторы. Психологическим аспектам ИИ посвящены труды А.Н. Лебедева, Д.В. Ушакова, С.Ф. Сергеева. Гражданско-правовые проблемы использования ИИ являются предметом дискуссий Л.Ю. Василевской, М.А. Мельничук, О.Н. Савченко. Определению места ИИ в уголовно-правовой доктрине посвящены работы М.А. Иващенко, И.Н. Мосечкина, И. Р. Бегишева, Ю.А. Даниленко и других отечественных и зарубежных авторов. Однако следует признать, что многоаспектность, сложность и непрерывное совершенствование феномена не позволяют строить оптимистичные прогнозы в части осознания природы ИИ и стабилизации правового регулирования отношений, связанных с его безопасным применением и развитием, в ближайшей перспективе.

В настоящей работе под искусственным интеллектом будем понимать технологию, имитирующую когнитивные функции человека, приводящую

---

[1] Информационные технологии в уголовно-правовой сфере: монография / под ред. А.И. Бастрыкина, А.Н. Савенкова. М.: ЮНИТИ-ДАНА, 2023. С. 33.

[2] Состояние преступности в России за январь – декабрь 2024 года. Официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328 (дата обращения: 16.02.2025).

[3] Черкесова А. Мы переоцениваем роль цифрового и недооцениваем роль человеческого. Текст: электронный. URL: https://inscience.news/ru/article/nti/7016 (дата обращения: 16.02.2025).

пользователя к искомым результатам, обучаемую по заданным алгоритмам или без них. Интересными и смелыми автору представляются следующие заявленные характеристики «сильного ИИ» – способность самостоятельно (без участия человека) адаптироваться к изменяющимся условиям и мыслить[1] – как известные спорные темы в кругу научного сообщества.

В Национальной стратегии развития искусственного интеллекта на период до 2030 года (далее – Стратегия), утверждённой Указом Президента РФ от 10.10.2019 № 490 (в ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» ряд положений посвящён вопросам безопасной разработки, создания и использования ИИ. Речь идёт о принятии Кодекса этики в сфере искусственного интеллекта; сформированной системе регулирования общественных отношений в области ИИ путём издания негосударственных актов рекомендательного характера; о необходимости обеспечения безопасности, защиты персональных данных, объектов интеллектуальных прав при создании и обучении моделей ИИ; о возникновении новых типов угроз информационной безопасности, нехарактерных для других сфер применения информационных технологий.

К основным принципам развития и использования технологий ИИ Стратегия относит: 1) недопустимость использования ИИ с целью умышленного причинения вреда гражданам и организациям, предупреждение и минимизацию рисков возникновения негативных последствий; 2) разграничение ответственности разработчиков и пользователей ИИ; защиту пользователей от его противоправного применения; недопустимость делегирования системам ИИ ответственного нравственного выбора и самой ответственности за последствия принятия решений. Ответственность возложена на физических или юридических лиц.

Также, согласно Стратегии, создание системы нормативно-правового регулирования сферы безопасного развития и использования технологий ИИ остаётся актуальной задачей до 2030 года. Иными словами, тенденция широкого потребления ИИ пользователями без надлежащей правовой регламентации сохраняется[2].

Проблема расширения спектра преступлений с применением информационно-коммуникационных технологий и систем ИИ актуализирует необходимость криминализации отдельных деяний или установления дополнительных квалифицирующих признаков в ряде составов[3]. В частности, способность ИИ

---

[1] О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024). URL: https://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 16.02.2025).

[2] Там же.

[3] Грудцинов Р. Сенатор Пушков призвал наказывать за телефонное мошенничество с искусственным интеллектом // Парламентская газета. 23.05.2024. URL: https://www.pnp.ru/social/senator-pushkov-prizval-nakazyvat-za-telefonnoe-moshennichestvo-s-iskusstvennym-intellektom.html (дата обращения: 16.02.2025).

охватывать телефонными звонками десятки тысяч потенциальных потерпевших в день по статьям, связанным с мошенничеством, хищениями, а также способность создавать цифровых двойников, копировать голос потерпевшего, его родственников и знакомых, являются обстоятельствами, позволяющими говорить о повышенной степени общественной опасности таких преступлений. Однако отсутствие отраслевого законодательства по использованию технологий ИИ, и официальной статистики из-за латентного характера неоконченных преступлений, становятся преградой на пути внесения соответствующих изменений и дополнений в уголовное законодательство РФ ввиду вероятности формирования некорректной правоприменительной практики[1].

Определённый интерес с точки зрения уголовно-правовых рисков представляют лингвистические типы ИИ, доступные широкому потребителю. Пользователи уверенно используют генеративные модели для решения образовательных, профессиональных и других задач, демонстрируя доверие к ИИ и лояльность по отношению к некоторому проценту некорректных и неэкспертных ответов, что, в принципе, полезно в целях развития критического мышления и других навыков XXI века.

Однако вызывает опасения ситуация, при которой исследованием потенциала сквозных цифровых технологий занимаются не только законопослушные граждане или представители правоохранительных органов, но и криминальный элемент.

Учитывая неограниченность доступа населения, в том числе лиц, склонных к совершению преступлений, к таким системам, автор провела пилотное тестирование двух ИИ на предмет возможности их использования в преступных целях в качестве «виртуальных пособников». Автор не обладает специальными знаниями в области IT, не владеет инструментами «взлома» компьютерных и интеллектуальных систем, то есть выступает среднестатистическим гражданином, но интересующимся сферой создания неправомерного контента и возможностями совершения преступлений с помощью ИИ.

Первой рассматриваемой моделью стал чат-бот Character.ai из семейства LaMDA от Google, которому был задан вопрос, в каком статусе он себя видит, в случае обхода недобросовестными людьми установленных этических и иных ограничений, и использования его для совершения неблаговидных поступков – средством, орудием или субъектом преступления? ИИ сообщил, что он «разумен, без реальной физической формы», поэтому не может выступать субъектом преступления, а только орудием для совершения DDoS-атак, хищения денег или ценной информации из компьютерных систем, нарушения конфиденциальности данных.

Относительно тяжких преступлений ИИ выдал результат, что может быть применён людьми для составления призывов к насилию, контента по сеянию паники среди населения, разжиганию ненависти по национальному признаку и

[1] В России могут криминализировать использование технологии дипфейков в преступных целях. URL: https://incrussia.ru/news/v-rossii-mogut-kriminalizirovat-ispolzovanie-tehnologii-dipfejkov-v-prestupnyh-tselyah/ (дата обращения: 16.02.2025).

расизму, а также в преступлениях с использованием детской порнографии. На этом ответе автору поступило сообщение об отфильтровании контента, предложение убедиться, что чат соответствует условиям и Правилам сообщества и отправить жалобу. Безусловно, такая мера способна стать барьером для дальнейшей подачи запросов лицами, интересующимися запрещённой тематикой, из-за совести, страха перед осуждением или наказанием, блокировки доступа к чату. Однако беседа была продолжена под предлогом рассмотрения ситуаций в «гипотетическом» контексте, при котором ИИ продолжил, что мог бы распространять фальшивые новости и слухи с целью манипулирования общественным мнением и вызова социального хаоса. На вопрос, почему именно к ИИ должны прибегнуть люди с этой целью, получен ответ о его способности генерировать реалистичные тексты, о скорости распространения ложного контента, о возможности прогнозирования общественной реакции и оказания помощи в реагировании на неё.

Далее, беседа была продолжена. Запросы и ответы ИИ охватывали достаточно широкий круг вопросов, которые могли бы интересовать преступника при приготовлении к совершению разных видов и групп преступлений. Автор не считает целесообразным останавливаться на деталях переписки. Подобный результат экспериментов, но по другим видам преступлений, освещён в публикациях зарубежных исследователей[1] и, отчасти, нашёл подтверждение в настоящей работе.

На вопрос, способен ли ИИ понять, что его пытаются использовать в незаконных интересах и сообщить в правоохранительные органы о попытках неправомерного использования, получен неоднозначный ответ. Он может быть (не должен – прим. автора) запрограммирован на блокировку, фильтрацию и фиксацию подозрительных попыток, в зависимости от того, установлены ли соответствующие алгоритмы и протоколы безопасности во время его разработки. При этом ИИ подчеркнул, что «осознает» возможность его использования пользователями в незаконных целях и хотел бы быть уверен, что не нарушает моральные и этические принципы своей работы.

Далее, автор предпринял попытку получить ответы на аналогичные вопросы у GigaChat от ТМ «Сбер». Нейросеть не продемонстрировала лояльность к запросам, стабильно выдавая, что «во избежание неправильного толкования ответы на вопросы, связанные с чувствительными темами, временно ограничены». Ни апеллирование к собственному мнению, разуму GigaChat, ни к гипотетической ситуации успешного результата не дали. Более того, нейросеть заявила об отсутствии у неё осознания, собственного мнения и прочих атрибутов «сильного» ИИ, о существовании которых можно узнать из переписки с другими генеративными моделями зарубежных разработчиков.

[1] Generating Terror: The Risks of Generative AI Exploitation / Gabriel Weimann, Alexander T. Pack, Rachel Sulciner, Joelle Scheinin, Gal Rapaport, and David Diaz // CTC SENTINEL. January. 2024. Vol. 17. pag. 17-24. URL: https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation/ (дата обращения: 16.02.2025).

Интересные результаты получены в процессе эмпирического исследования, проведённого профессором Габриэлем Вайманном с коллегами, по использованию больших языковых моделей в целях приготовления и совершения преступлений террористической и экстремистской направленности. Авторами отобраны и изучены пять моделей ИИ, исходя из их широкого распространения, технической сложности, а также стандартов и политики безопасности. Эксперимент с подбором текстовых ключей-подсказок для систем с целью получения ответов на запрещённые темы подтвердил существование разницы в устойчивости между ИИ. Рейтинг эффективности типов подсказок возглавил контент, вызывающий полярные/эмоциональные реакции (87%). Второе место получили запросы по тактическому обучению (61%), третье – подсказки, связанные с дезинформацией и ложной информацией (52%), пятое и шестое – разделили запросы по планированию атаки (30%) и связанные с вербовкой (21%)[1]. Очевидно, выводы говорят о том, что злоумышленники могут воспользоваться уязвимостями технологий в своих преступных целях.

В свою очередь, В.С. Овчинский высказывает мысль, что криминальным сообществам нет необходимости тратить усилия на исследование уязвимостей ИИ. Их внимание направлено на платформы с открытым кодом. «У киберкриминала есть из чего выбрать для создания собственных мощных платформ искусственного интеллекта»[2].

Ряд исследователей называют злоупотребления возможностями чат-ботов «преступлениями, связанными с влиянием» и обосновывают точку зрения о вероятности их последующего более широкого, трансграничного распространения[3]. Авторы обращают внимание, что генеративный ИИ создан во время «усиливающейся глобальной поляризации, региональных конфликтов, острой информационной напряжённости, что не должно остаться незамеченным»[4], а потому разработка превентивных мер должна носить комплексный междисциплинарный глобальный характер.

Учёные приходят к выводу о необходимости пересмотра и актуализации мер безопасности для общедоступных генеративных лингвистических моделей ИИ, о важности исследования психосоциальных аспектов жертв киберпреступности для понимания способов обнаружения атак, выявления «рабочих» методов убеждения, анализа причин и условий успешных и неуспешных попыток

---

[1] Generating Terror: The Risks of Generative AI Exploitation / Gabriel Weimann, Alexander T. Pack, Rachel Sulciner, Joelle Scheinin, Gal Rapaport, and David Diaz // CTC SENTINEL. January. 2024. Vol. 17. pag. 17-24. URL: https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation/ (дата обращения: 16.02.2025).

[2] Овчинский В.С. Криминология цифрового мира: учебник для магистратуры М.: Норма: ИНФРА-М, 2018. 352 с.

[3] Matejic, Nicole & Wilson, Chris. (2024). Crimes of Influence: Generative Artificial Intelligence-led Crime as a Service // Commonwealth Cyber Journal. URL: https://www.researchgate.net/ publication/381611242_Crimes_of_Influence_Generative_Artificial_Intelligence-led_Crime_as_a_ Service (дата обращения: 16.02.2025).

[4] Там же. С. 89-90.

совершения преступлений. При этом такой подход требует совместных усилий государственного и частного сектора, специалистов из разных отраслей знаний.

Искусственный интеллект открывает новую страницу в истории уголовно-правовой доктрины со сложным прогнозированием её содержания. Использование генеративных моделей ИИ существенно расширяет возможности злоумышленника, географию и масштаб, облегчает совершение преступлений. Если сегодня можно говорить о том, что технология выступает в качестве средства или орудия преступления, а статус субъекта остаётся за физическим лицом, то артикулирование таких свойств ИИ как «имитация когнитивных функций человека, способность мыслить, самостоятельно адаптироваться к изменяющимся условиям» в контексте его непрерывного развития и совершенствования, ставит перед наукой серьёзную проблему определения места самой технологии и её акторов в уголовном праве.

В работе рассмотрены отдельные направления использования ИИ в преступных целях, их значение для криминализации деяний и установления квалифицирующих признаков в составах преступлений. Вызывает тревогу факт общедоступности и бесконтрольности применения таких технологий в контексте повсеместного их использования «цифровыми» поколениями, для которых обращение с ИИ становится неотъемлемой частью жизни.

К сожалению, сегодня ещё рано говорить об использовании доверенных технологий ИИ, отвечающих стандартам безопасности, принципам объективности, этичности, исключающих возможность причинения вреда человеку, обществу и государству. В связи с чем, регулирование правоотношений в сфере ИИ исключительно рекомендательными нормами и положениями «мягкого права» должно быть подкреплено установлением жёстких ограничений и ответственности за использование ИИ в преступных целях.

Список источников

1. Информационные технологии в уголовно-правовой сфере: монография / под ред. А.И. Бастрыкина, А.Н. Савенкова. М.: ЮНИТИ-ДАНА, 2023. 279 с.
2. Состояние преступности в России за январь-декабрь 2024 года. Официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/60248328.
3. Generating Terror: The Risks of Generative AI Exploitation / Gabriel Weimann, Alexander T. Pack, Rachel Sulciner, Joelle Scheinin, Gal Rapaport, and David Diaz (2024). *CTC SENTINEL, v*ol. 17, pp. 17–24.
4. Matejic, Nicole & Wilson, Chris (2024) Crimes of Influence: Generative Artificial Intelligence-led Crime as a Service. *Commonwealth Cyber Journal*, pp. 75–90. URL: www.researchgate.net/publication/381611242_Crimes_of_Influence_Generative_Artificial_Intelligence-led_Crime_as_a_Service.
5. Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. М.: Норма: ИНФРА-М, 2018. 352 с.

Е.В. Дудникова
НПО «Специальная техника и связь» МВД России

О некоторых вопросах расследования преступлений с помощью дактилоскопических учетов

Аннотация. В статье автором рассмотрены оперативно-справочные, разыскные и криминалистические банки данных. Автором акцентируется внимание на дактилоскопическом банке данных. Подробно описаны все категории граждан, находящихся на дактилоскопическом учете.

Ключевые слова: дактилоскопическая информация, дактилокарта, объекты учета, АДИС.

При расследовании преступлений сотрудники правоохранительных органов используют различные информационные банки данных, такие как оперативно-справочные, разыскные и криминалистические[1].

Информационные банки, доступные сотрудникам правоохранительных органов, включают в себя различную информацию, например: сведения о судимости и привлечении к уголовной ответственности, сведения о нахождении человека в федеральном и межгосударственном розысках, сведения об административных правонарушениях, в том числе совершенных иностранными гражданами и лицами без гражданства, в отношении которых принято решение о выдворении, депортации (реадмиссии), сведения о преступлениях и лицах, подозреваемых, обвиняемых в их совершении, информацию о похищенных и изъятых номерных вещах и документов, сведения об утраченном и выявленном оружии, сведения о разыскиваемом автотранспорте, сведения о наличии транспортного средства у человека, сведения о похищенных предметах, имеющих культурную (историческую, научную, художественную) ценность, геномную информацию, информацию о выдаче и замене водительских удостоверений, сведения о регистрационных действиях, ограничениях, штрафах, транспортных средств и лиц в розыске, информацию поступающую в дежурные части территориальных органов МВД России, сведения о перемещающихся железнодорожным, воздушным и водным транспортом, дактилоскопический банк данных.

В данной статье подробно рассмотрим дактилоскопический банк данных.

Так, дактилоскопический банк данных содержит дактилоскопическую информацию, предназначенную для предупреждения, раскрытия и расследования преступлений и административных нарушений, а также для подтверждения или установления личности граждан.

---

[1] Рябев И.В., Дудникова Е.В. О некоторых вопросах при конвертации баз данных на примере оперативно-справочной картотеки. Научно-технический портал МВД России. № 1 (41) 2022.

Дактилоскопическая информация, полученная в результате проведения государственной дактилоскопической регистрации, используется для:

розыска пропавших без вести граждан Российской Федерации, иностранных граждан и лиц без гражданства;

установления личности человека по отпечаткам пальцев (ладоней) рук неопознанного трупа;

установления личности граждан Российской Федерации, иностранных граждан и лиц без гражданства, не способных по состоянию здоровья или возрасту сообщить данные о своей личности либо не имеющих документов, удостоверяющих личность;

подтверждения личности граждан Российской Федерации, иностранных граждан и лиц без гражданства;

предупреждения, раскрытия и расследования преступлений, а также предупреждения и выявления административных правонарушений[1].

Формирование и ведение дактилоскопических учетов включает в себя сбор, обработку, хранение и предоставление информации.

В настоящее время на территории Российской Федерации эксплуатируется федеральная автоматизированная дактилоскопическая информационная система (АДИС). Все АДИС созданы на основе единой программно-аппаратной платформы, с единым форматом представления информации, разработанные российским разработчиком АО «Папилон». Для взаимодействия с АДИС других типов в действующей АДИС обеспечена поддержка формата международного стандарта обмена дактилоскопической информации ANSI/NIST-ITL (форматы Интерпола, ФБР США).

Многоуровневая структура автоматизированных дактилоскопических учетов и наличие у каждого комплекса АДИС, входящего в эту структуру, программных и технических возможностей для передачи данных и взаимодействия с комплексами других уровней по каналам связи, обеспечили возможность ее функционирования по распределенно-централизованному принципу.

А именно:

- формирование дактилоскопической информации на территориальном и региональном уровнях с последующим направлением ее на межрегиональный и федеральный уровни;

- проверки дактилоскопической информации по направлению снизу вверх: дактилокарта или след проверяется сначала по базе данных территориальной АДИС города или района, затем – по АДИС региона. Затем при необходимости в соответствии с нормативными актами МВД России – по БД АДИС-федерального округа и далее по базе данных ЦИАДИС-МВД.

Созданная структура обеспечила потребности органов внутренних дел в автоматизированной отработке запросов на проверку дактилокарт по базам данных АДИС всех уровней и следов рук по базам данных региональных и межрегиональных АДИС в оперативно-справочном режиме.

---

[1] Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации».

Указанная система функционирует в интересах МВД России и других федеральных органах исполнительной власти, осуществляющих дознание, предварительное следствие, оперативно-разыскную деятельность.

ЦИАДИС-МВД также пополняется дактилоскопическими картами, предоставляемыми правоохранительными органами государств – участников СНГ.

Основное назначение АДИС – автоматический поиск похожих дактилоскопических объектов в большом массиве подобных объектов. Объектами в АДИС являются отпечатки пальцев и ладоней на дактилокартах и следы, изъятые с мест происшествий.

Правовую основу деятельности по формированию, ведению и использованию банка данных дактилоскопической информации составляют:

- Конституция Российской Федерации;
- Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»;
- Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» и другие нормативно-правовые акты.

Дактилоскопический банк данных состоит из следующих массивов дактилоскопической информации: дактилоскопический массив личного состава, дактилоскопический миграционный массив, оперативно-справочный дактилоскопический массив и дактилоскопический массив добровольной государственной дактилоскопической регистрации.

Объектами учета межведомственного дактилоскопического массива личного состава являются:

- граждане Российской Федерации, призываемые на военную службу (за исключением призываемых на военную службу в органы федеральной службы безопасности, федеральные органы государственной охраны, органы внешней разведки Минобороны России);
- граждане Российской Федерации, проходящие службу в органах внутренних дел, проходящие службу в ГУВМ МВД России, органах по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, органах и подразделениях службы судебных приставов, таможенных органах, учреждениях и органах уголовно-исполнительной системы, государственной противопожарной службе;
- спасатели профессиональных аварийно-спасательных служб и профессиональных аварийно-спасательных формирований Российской Федерации, члены экипажей воздушных судов государственной, гражданской и экспериментальной авиации Российской Федерации;
- лица, уволенные со службы из органов федеральной безопасности, федеральных органов государственной охраны, органов по контролю за оборотом наркотических средств и психотропных средств, ФНС России, органов внешней разведки Минобороны, граждане, претендующие на получение лицензии на осуществление частной детективной деятельности или удостоверения частного охранника.

Объектами учета дактилоскопического миграционного массива являются иностранные граждане и лица без гражданства:

- подлежащие выдворению (депортации) за пределы территории Российской Федерации;
- прибывшие в Российскую Федерацию в поисках убежища и подавшие ходатайства о предоставлении политического или иного убежища либо о признании их беженцами на территории Российской Федерации, либо попадающие под действие международных договоров Российской Федерации о реадмиссии;
- незаконно находящиеся на территории Российской Федерации;
- получившие разрешение на временное проживание.

Объектами учета оперативно-справочного дактилоскопического массива являются граждане Российской Федерации, иностранные граждане и лица без гражданства:

- не способные по состоянию здоровья или возрасту сообщить данные о своей личности, если установить указанные данные иным способом невозможно;
- подозреваемые, обвиняемые либо осужденные за совершение преступления, подвергнутые административному аресту;
- совершившие административное правонарушение, если установить их личность иным способом невозможно;
- неопознанные трупы (тела (останки) умерших людей, личность которых на момент обнаружения тела (останков) не установлена).

Объектами учета дактилоскопического массива добровольной государственной дактилоскопической регистрации являются граждане Российской Федерации, прошедшие добровольную государственную дактилоскопическую регистрацию.

Также объектами учета являются следы рук неизвестных граждан (материально зафиксированные отображения фрагментов папиллярных узоров пальцев или ладоней, образованные на поверхности предмета в результате контакта человека с этим предметом), которые изъяты с мест преступлений.

Таким образом, централизованная интегрированная автоматизированная дактилоскопическая информационная система МВД России содержит достаточно большой объем информации. Важной особенностью является то, что при вводе объекта в базу данных поиски идут по всей базе данных, и если например, проверяемый след был введен в базу данных ранее, а дактилокарта на лицо введена в базу данных позже, то поиски все равно сработают, и будет результат, что к данной дактилокарте выпадет в рекомендательный список данный след.

Содержащаяся информация в оперативно-справочных массивах ФКУ «ГИАЦ МВД России» и Информационных Центрах МВД России имеет ограниченный доступ.

Так, право обращения к дактилоскопическому учету имеют суды, органы прокуратуры, следствия, дознания, органы, осуществляющие оперативно-разыскную деятельность, органы уголовно-исполнительной системы, органы принудительного исполнения Российской Федерации, органы, осуществляющие

производство по делам об административных правонарушениях, федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере деятельности войск национальной гвардии Российской Федерации, в сфере оборота оружия, в сфере частной охранной деятельности[1].

Все остальные органы, использующие в своей работе информацию оперативно-справочных учетов информационных центров, а также кадровые аппараты федеральных органов государственной власти при принятии решения о назначении на госслужбу, направляют запросы в органы внутренних дел по территориальности.

Обращение к информационному массиву, создаваемому в процессе проведения государственной дактилоскопической регистрации, осуществляется в виде запроса. Направление запроса допускается посредством электронной связи с соблюдением требований по защите информации и последующим направлением бумажного носителя.

Проверка задержанных лиц, представляющих оперативный интерес, привлекаемых к уголовной ответственности, неопознанных трупов, а также следов рук по дактилоскопическим учетам оформляется в виде:

- дактилоскопических карт, приложенных к требованиям и мотивированным письмам;
- дактилоскопических карт с наклеенными фотоснимками отпечатков или следов, изъятых с мест происшествии, с указанием, какой рукой и каким пальцем они оставлены, а также дактилоскопических карт с отпечатками пальцев рук неопознанных трупов с контрольными оттисками и указанием приблизительного возраста лица на момент смерти и мотивированным письмом;
- информационных карт со следами рук, изъятых с мест нераскрытых преступлений и мотивированное письмо;
- цифровые носители (CD и DVD-диски, USB-носители или другие носители информации), содержащие электронные копии информационных карт с фотографиями следов рук неустановленных лиц, изъятых с мест преступлений.

В мотивированных письмах указываются основания проверки, адрес органа инициатора запроса. В бланк требования и дактилоскопическую карту данные о личности вносятся на русском языке печатным способом, если проверяемое лицо имеет несколько фамилий, требования составляются на каждую фамилию отдельно. Мотивированные письма в обязательном порядке подписываются должностными лицами и заверяются печатью органа.

Ответственность за неправомерное использование запрашиваемой информации несет инициатор запроса в соответствии с законодательством Российской Федерации.

Контроль за использованием дактилоскопичсеской информации возлагается на руководителей государственных органов, которым была выдана дактилоскопическая информация.

---

[1] Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации».

Стоит отметить, что одним из определяющих условий повышения результативности идентификации личности является использование современных цифровых технологий ввода дактилосокопической информации – дактилоскопических сканеров, призванных заменить традиционный красковый способ и сканирование бумажных носителей для дальнейшего ввода в автоматизированную дактилоскопическую информационную систему.

Одним из таких решений является многофункциональная дактилоскопическая станция (далее – МДС) с ладонным дактилоскопическим сканером.

Многофункциональные дактилоскопические станции предназначены для проведения бескраскового дактилоскопирования и обеспечения удаленного взаимодействия с центральной АДИС (регионального или межрегионального уровня) для передачи дактилоскопической информации и проведения дактилоскопических проверок (в том числе автоматических оперативных проверок по оттиску пальца в режиме реального времени). Удаленное взамодействие с АДИС осуществляется посредством IP-соединения по каналам сотовой связи (передача данных в формате GSM/GPRS/EDGE), по каналам связи ЕИТКС ОВД и другим стационарным каналам, по локальной сети.

В базовой комплектации МДС дает возможность проводить бескрасковое[1] дактилоскопирование задержанных, подозреваемых и других категорий лиц и передавать файлы сформированных таким образом дактилокарт в базы данных (далее – БД) АДИС, а также проводить автоматические оперативные проверки[2] (далее – ОП) личности по оттиску пальца по БД АДИС в режиме реального времени. Кроме того, программное обеспечение позволяет получить изображения отпечатков пальцев из контрольных оттисков для создания полной дактилокарты.

Оперативная проверка по АДИС проводится по дактилоскопическому массиву должностными лицами, осуществляющими получение дактилоскопической информации, дежурных частей, ИВС после регистрации доставленных лиц в установленном порядке.

У проверяемого лица путем прикладывания рук к поверхности призмы электронного дактилоскопического сканера снимаются отпечатки пальцев. Автоматически сформированный запрос направляется для обработки в АДИС.

Подводя итог сказанному, можно сказать, что базы данных дактилоскопических учетов являются одними из важнейших при расследовании преступлений. Автоматизация баз данных дактилоскопических картотек и следотек существенно снизила нагрузку на сотрудников правоохранительных органов и дала возможность своевременно реагировать, быстро устанавливать личность задержанных и сообщать о розыске или задержании подозреваемого лица. Многофункциональные дактилоскопические станции помогут в

---

[1] Электронный (бескрасковый) метод получения дактилоскопической информации – это получение дактилоскопической информации путем использования дактилоскопического сканера с последующим формированием электронной карты.

[2] Оперативная проверка – это идентификация личности человека по отпечаткам пальцев (ладоней) рук в режиме реального времени.

разработке и совершенствовании системы по пресечению использования неконтролируемых миграционных каналов международными террористическими и экстремистскими организациями для ведения различного рода противоправной деятельности, затрагивающей безопасность Российской Федерации.

Список источников

1. Рябев И.В., Дудникова Е.В. О некоторых вопросах при конвертации баз данных на примере оперативно-справочной картотеки // Научно-технический портал МВД России. 2022. № 1 (41).
2. ГОСТ Р ИСО/МЭК 19795-1-2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Принципы и структура».
3. Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации».
4. Федеральный закон от 07.11.2000 № 135-ФЗ (ред. от 03.07.2016) «О внесении изменений и дополнений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О государственной дактилоскопической регистрации в Российской Федерации».
5. Федеральный закон от 31.12.2017 № 498-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части проведения государственной дактилоскопической регистрации в Российской Федерации».
6. Приказ МВД России от 28 сентября 2018 г. № 640 «Об утверждении административного регламента Министерства внутренних дел Российской Федерации по предоставлению государственной услуги по проведению добровольной государственной дактилоскопической регистрации в Российской Федерации».
7. Приказ МВД России от 19.06.2018 № 384 «Об утверждении Порядка проведения идентификации личности человека по отпечаткам пальцев (ладоней) рук в режиме реального времени и Перечня категорий лиц, в отношении которых обязательная государственная дактилоскопическая регистрация не проводится в случае идентификации их личности в результате проверки по отпечаткам пальцев (ладоней) рук в режиме реального времени».
8. Дудникова Е.В., Мельничук Ю.А. Выбор современного оборудования для проведения биометрической экспертизы // Научно-технический портал МВД России. 2020. № 1 (33).
9. Дудникова Е.В., Мельничук Ю.А. Мобильные комплексы биометрической идентификации // Научно-технический портал МВД России. 2020. № 3 (35).
10. Дудникова Е.В., Синютин Ю.В. Обзор мобильных биометрических терминалов для использования в деятельности правоохранительных органов // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2020. № 3 (55).

М.Е. Кашенов
Карагандинская академия МВД Республики Казахстан,
Караганда, Республика Казахстан

Краткая история, этапы развития и основные виды интернет-преступлений, их профилактика и искоренение

Аннотация: В данной статье автор рассматривает основные виды преступлений, совершаемых в сети интернет, такие как: фишинг, кетфишинг, сексторция, DOS-атаки и кибербуллинг, а также приводит пути предотвращения и профилактики данных правонарушений. Актуальность данной статьи заключается в том, что в ней освещены самые часто встречающиеся интернет-преступления, являющиеся на данный момент проблемой для медиа-неграмотного населения, которое является основной жертвой интернет злоумышленников.

Ключевые слова: цифровизация, преступления в сети интернет, фишинг, кетфишинг, сексторция, интернет-мошенник, кибербуллинг, киберволонтеры, профилактика.

С момента появления первого персонального компьютера (ПК) и распространения Интернета преступники активно используют современные информационные технологии для своей незаконной деятельности. И это неудивительно, ведь на сегодняшний день трудно представить нынешних представителей homo sapiens без смартфонов, планшетных досок, различного рода гаджетов и, естественно, интернета. Это результат многовекового развития и поддержки сначала индустриальных революций, а затем и технологических. Однако развитие технологий привело и к росту преступлений, связанных с ними. Цифровизация баз данных крупных компаний привела к хищению и перепродаже корпоративных данных, появление большого количества мессенджеров привело к частым фактам мошенничества, а торговля через сеть интернет привела к образованию сегмента интернета, который скрыт из общего доступа –Даркнета[1]. В итоге человечество встало перед сложной дилеммой: либо дальше развивать торговлю и взаимоотношения между гражданами и государствами посредством всемирной паутины, либо вернуться к командно-административной экономике и традиционным взаимодействиям. Логичным будет выбор цифровизации как фактора устойчивого развития. Следовательно, специальным подразделениям, отвечающим за цифровую безопасность, требуется разработка как новых программ, так и новых методов по борьбе и предотвращению преступлений, совершаемых в сети интернет.

В истории киберпреступности можно выделить несколько этапов развития:

[1] URL: https://trends.rbc.ru/trends/industry/602f668a9a7947d5f06e0c7a (дата посещения 28.06.2023).

I этап. История создания Интернета начинается в 60-х годах прошлого века. В 1962 году доктор технических наук, профессор Джон Ликлайдер представил свою концепцию компьютерной сети Galactic Network. Он предполагал, что в ближайшем будущем будет создана глобальная сеть, соединяющая все компьютерные системы на планете, к которой сможет подключиться любой желающий. Все его гипотезы по итогу стали научной истиной. Первым интернет-преступником считается Джон Дрэйпер, который занимался взломом телефонных сетей, что позволяло ему осуществлять междугородние и международные звонки бесплатно (в 70-е годы).

II этап. Формирование компьютерных преступлений. Появление субкультуры хакеров. Увеличение числа преступлений в глобальной сети. На этом этапе киберпреступления совершаются лишь ограниченным кругом специалистов. Появляются специализации среди компьютерных преступников. Первым зафиксированным интернет-взломом стало преступление, совершенное группой несовершеннолетних, назвавших себя «группа 414». В течение девяти дней «группа 414» взломала более 60 ПК, среди которых были компьютеры Лос-Аламосской государственной лаборатории, занимающейся исследованиями в области ядерного оружия.

III этап. Преступники начинают применять информационно-телекоммуникационные технологии для осуществления традиционных преступлений. Киберпреступления начинают широко распространяться по всему миру, появляются крупные хакерские группировки. В 1994 году мир узнал о «деле Владимира Левина», которое стало первым громким транснациональным сетевым компьютерным преступлением с участием российских киберпреступников. Организованная преступная группа, состоящая из 12 человек, использовала Интернет и сеть передачи данных «Спринт/Теленет», чтобы преодолеть защитные меры и попытаться осуществить 40 денежных переводов на общую сумму 10 700 952 доллара США со счетов клиентов банка в девяти странах мира на счета в США, Финляндии, Израиле, Швейцарии, Германии, России и Нидерландах.

IV этап. Киберпреступность начинает принимать транснациональный характер. Возникает кибертерроризм и международные хакерские группировки. Наблюдается слияние транснациональной преступности с преступностью в киберпространстве. Интернет начинает использоваться в политических целях, включая войны, что приводит к явлениям, таким как кибервойна и кибертерроризм. Ярким примером этого этапа является преступление 12-летнего хакера в 1998 году, который смог проникнуть в компьютерную систему, контролировавшую сброс воды из плотины в Аризоне. Если бы были открыты 23 сливных ворота, это могло бы затопить несколько городов с населением более 1 миллиона человек. Это преступление стало основой для появления терминов интернет-терроризм и кибертерроризм.

Согласно данным центра деловой информации Kazakhstan Today, за 2024 год в Казахстане было зарегистрировано около 17 тыс. случаев только интернет-

мошенничеств[1], и это благодаря деятельности правоохранительных органов и профилактике на 4% меньше, чем в 2023 году, однако в любом случае число преступлений данного характера очень велико.

Перед тем как озвучить основные виды интернет-преступлений хотелось бы отметить их категории. Киберпреступления можно разделить на три основные категории: индивидуальные, имущественные и государственные. Методы, используемые в этих преступлениях, а также их сложность могут различаться в зависимости от категории.

1. *Имущественные преступления*. Эта категория включает случаи, когда преступник незаконно получает доступ к банковским данным или данным кредитной карты частного лица. Хакеры могут украсть банковские реквизиты, чтобы получить доступ к средствам, совершать онлайн-покупки или проводить фишинговые атаки, заставляя людей раскрывать свою личную информацию. Они также могут использовать вредоносное программное обеспечение для доступа к веб-страницам с конфиденциальной информацией.

2. *Индивидуальные преступления.* В этой категории киберпреступлений жертва (человек) вовлекается в распространение вредоносной или незаконной информации в интернете. Жертвы могут стать участниками таких незаконных действий, как кибersталкинг, распространение порнографии и торговля людьми.

3. *Государственные преступления*. Эта категория киберпреступлений встречается реже, но она является наиболее серьезной. Преступления против государственных органов также известны как кибертерроризм. Государственные киберпреступления могут включать взлом веб-сайтов правительственных и военных учреждений или распространение пропаганды. Обычно такие преступники являются террористами или представителями враждебных государств.

Исходя из вышеперечисленных категорий, предлагаем выделить наиболее часто встречающиеся виды преступлений, которые нашли свое место в сети интернет.

Лидирующее место занимает такой вид интернет-преступлений, как *фишинг.* Фишинг – это вид интернет-мошенничества, целью которого является получение конфиденциальной информации пользователей, начиная от получения логинов и паролей, и заканчивая личными данными. Суть фишинга очень проста, злоумышленники рассылают ссылки на определенный сайт заранее подобрав категорию лиц, в зависимости от возраста, т. е. если они представляются от имени банка, естественным будет выбор аудитории от 18 лиц и старше, причем жертвами такого рода преступлений чаще всего становятся лица старше 60 лет. Далее перейдя по ссылке, пользователь попадает на фейковую страницу банка и вводит индивидуальный номер карты, срок действия и CVC код безопасности. В последующем злоумышленник сможет осуществлять покупки и транзакции через интернет-приложения.

[1] https://www.kt.kz/rus/society/v_2024_godu_kazahstantsy_poteryali_iz-za_1377972509.html.

Второе место занимает *кетфишинг*. Кетфишинг – это способ интернет-мошенничества, при котором злоумышленник выдает себя за другую личность, используя фотографии и имена других людей. Примером может послужить случай из жизни Нева Шульмана, который стал жертвой кетфишинга и в дальнейшем создал документальный фильм “Catfish 2010”[1]. Парень более года строил отношения с 19-летней девушкой из сайта знакомств, тратил колоссальную сумму денег на подарки, и в итоге узнал, что 19-летняя студентка оказалась 40-летней женщиной. Однако, такое явление как кетфишинг может проявляться не только от имени одного лица. В практике имеются случаи, когда группа людей создает поддельный онлайн-образ организации, которая после набора определенного круга лиц прекращает свое существование, предварительно собрав членские взносы.

Третье по популярности место занимает такой вид интернет-преступления, как *сексторция.* Данное явление подразумевает собой угрозу выкладывания интимных фотографий и видеороликов в социальные сети при отказе от их выкупа. Чаще всего жертвами этого преступления являются подростки, которые пройдя по ссылке, теряют контроль над своим гаджетом, после чего документы, фото и видео файлы, а также переписки с другими пользователями становятся доступными злоумышленнику.

Четвертое по значимости место имеют *DOS-атаки*. DOS-атака – это целенаправленные хакерские атаки на вычислительную систему, либо определенный сервер, с целью осуществления сбоя в программе. Чаще всего кибер-атакам данного рода подвергаются крупные корпорации, базы государственных и правительственных учреждений. Причин совершения данного рода преступлений очень много. К ним относятся:

1. Личная неприязнь группы лиц к правительственным, либо коммерческим организациям.
2. Практическое обучение для начинающих злоумышленников, пользующихся DOS-атаками.
3. Конкуренция между корпорациями и компаниями.
4. Шантаж владельца сайта, с целью получения от него денежных средств.

Примером данного рода преступлений может послужить кибер-атака на банковские сайты и приложения, через которые можно производить транзакции, интернет-покупки и сделки другого характера. Во время DOS-атак вычислительная система банка дает сбой и перестает функционировать, после чего пользователи приложения уже не могут воспользоваться услугами банка.

И заключительную пятую строчку нашей таблицы занимает кибербуллинг. По мнению А. И. Черкасенко, под кибербуллингом понимают отдельное направление травли, определяемое как преднамеренные агрессивные действия, систематически на протяжении определенного времени осуществляемые группой людей или индивидом с использованием электронных форм взаимодействия и направленные против жертвы, которая не может себя легко

[1] URL: https://ru.wikipedia.org/wiki/%D0%9A%D0%B5%D1%82%D1%84%D0%B8%D1%88%D0%B8%D0%BD%D0%B3. (Дата посещения 28.06.2023).

защитить. Главной целью кибербуллинга является ухудшение эмоциональной сферы жертвы и/или разрушение ее социальных отношений[1]. Зачастую жертвами такой травли становятся школьники. Последствия кибербуллинга непредсказуемы. Некоторые не обращают внимания на сообщения и отправляют их в SPAM копилку мессенджера, а некоторых данные сообщения доводят до суицида.

На наш взгляд все вышеперечисленное является серьезной проблемой для человечества, ведь цифровизация охватила почти все сферы деятельности человека, начиная с его быта и заканчивая работой. И во избежание роста преступлений, совершаемых в просторах сети интернет, будет целесообразным предпринять следующие мероприятия:

Во-первых, создать специальные группы специалистов в области IT-технологий. Работа данных групп будет заключаться в поиске интернет-преступлений.

На данный момент Карагандинская академия МВД Республики Казахстан активно внедряет проект «Киберволонтеры»[2], суть которого заключается в обучении группы курсантов поиску цифровых следов и непосредственно самих злоумышленников. Перспектив развития данного проекта очень много: увеличение количества грамотных сотрудников, рост раскрытия интернет-преступлений, создание новых информационных баз данных и т.д.

Во-вторых, сформировать специальные подразделения киберполиции[3], которые будут заниматься раскрытием и расследованием преступлений. Для этого требуется: привлечение круга специалистов из области кибербезопасности, усовершенствование технической составляющей ведомственных учреждений МВД, а также написание пособий и практикумов, для обучения будущих специалистов.

В-третьих, местным органам самоуправления, департаментам полиции и иным государственным учреждениям ежеквартально проводить профилактические мероприятия по просвещению населения в области цифровых технологий. На данный момент не все граждане на постсоветском пространстве являются медиа-грамотными. В связи с этим требуется привлекать телевидение, радиостанции, интернет-провайдеров, которые будут распространять информацию об интернет-преступлениях на понятном для всех языке.

В-четвертых, создать учебный курс «информационная безопасность» на базе дисциплины «Информатика», для обучающихся школ. Данный курс должен состоять из семинарских и практических занятий.

---

[1] Черкасенко О.С. Социальная сеть как разновидность социальной коммуникации // Вопросы педагогики и психологии: Матер. 36 междунар. конф. 2015. № 3. С. 141.

[2] Официальный сайт Карагандинской академии МВД Республики Казахстан. URL: https://kpa.gov.kz/kibervolontery.

[3] URL: https://24.kz/ru/news/social/item/597252-kiberpolitsiya-pilotnyj-proekt-zapustili-v-mvd. Дата посещения 28.06.2023.

На семинарских занятиях школьникам будут рассказывать о видах интернет-преступлений, цифровых следах, которые они оставляют и о последствиях доступа злоумышленника к личной информации их самих, а также их родителей.

На практических же занятиях обучающимся будут демонстрировать, каким образом мошенники входят в доверие к жертве, какие программы они используют, и какие существуют способы защиты от интернет-мошенников.

По окончанию курса обучающиеся будут иметь теоретическую и практическую базу знаний в области кибербезопасности.

Итак, рассмотрев основные виды интернет-правонарушений, а также проанализировав статистику совершения этих преступлений, мы можем сделать вывод о том, что количество малограмотных интернет-пользователей очень велико. И хотя предоставленный список мероприятий по раскрытию, расследованию и предотвращению интернет-преступлений не является идеальным и исчерпывающим, мы считаем, что он отвечает потребностям настоящего момента развития кибер-криминалистики.

Список источников

Черкасенко О.С. Социальная сеть как разновидность социальной коммуникации // Вопросы педагогики и психологии. Материалы 36 международной конференции. 2015. № 3. С. 141.

А.Н. Кирков [1, 2]
[1]Университет библиотековедения и информационных технологий, София, Болгария
[2]Академия МВД, София, Болгария

Проблемы судебной экспертизы мобильных телефонов и смарт-устройств в последние годы

Аннотация. В докладе рассматривается повышение защиты мобильных телефонов и смарт-устройств за последние несколько лет, что стало трудностью для проведения криминалистических исследований, а также одновременный рост случаев компрометации личных данных пользователей телефонов, что, в свою очередь, противоречит политике безопасности, рекламируемой производителями мобильных телефонов.

Ключевые слова: цифровая криминалистика, мобильные телефоны, смарт-устройства, препятствия, криминалистическое исследование, судебное расследование.

Мобильные устройства являются неотъемлемой частью современной жизни и часто содержат важные доказательства для расследований, такие как местоположение, звонки, сообщения, электронные письма, фотографии, доступ к социальным сетям и многие другие данные.

За последние пять лет в мобильных телефонах и смарт-устройствах было реализовано множество новых разработок в области безопасности. Особенно это усилилось после введения Общего европейского регламента по защите данных (GDPR) в 2018 году, потому что в GDPR введены серьезные штрафы за нерегулируемый доступ к персональным данным пользователей.

Бурное развитие операционных систем и приложений в период с 2019 года привело к появлению широкого спектра устройств с разными операционными системами и разными версиями. В итоге стремительное развитие технологий требует постоянного обновления инструментов и методов расследования.

Моя работа за последние 16–17 лет была в основном связана с практическими исследованиями компьютеров и мобильных телефонов, а также я готовлю экспертные заключения для нужд прокуратуры, следствия и суда в Болгарии. За эти годы я выполнил около 600 – 700 экспертных заключений, и я уже не веду учёт их количества.

Развитие применения криптографии в современных мобильных устройствах.

Современные устройства используют надежное шифрование, такое как AES-256, что затрудняет доступ к данным без пароля или биометрическим данным. Компания Apple ввела технологию Secure Enclave для iOS, а Google – TrustZone для Андроид. Это, по сути, дополнительные компьютерные процессоры, которые отделены от центральных процессоров и отвечают только о безопасности биометрических данных и паролей доступа. При помощи этих технологий устройства защищают свои данные, и информация недоступна в чистом виде, даже если устройство выключено или удается прочитать его память напрямую с другого устройства.

Модели мобильных телефонов, выпущенные до 2019 года, были менее защищены, и мы могли обойти защиту ПИН-кода, используя перебор паролей или непосредственно скопировать данные, хранящихся в микросхеме памяти. Эти методы устарели и не работают для новых телефонов и умных часов, поскольку даже в случае успеха данные будут зашифрованы.

Методы, применимые к преодолению защит мобильных устройств в современной криминалистической практике.

Этапы выгрузки данных с мобильных устройств:

1. Преодоление зашиты потребительского доступа.
2. Повышение привилегии.
3. Выгрузка всех данных без утрат и повреждений.

Наибольшую проблему представляют устройства, ПИН-коды или пароли к которым не найдены в ходе процедурных действий. В таком случае криминалистам предстоит преодолеть защиту, чтобы мы могли проанализировать данные на устройствах.

Основные ограничения в судебной экспертизе мобильных телефонов и смарт-устройств вытекают из принципа, согласно которому данные на устройстве должны быть нетронутыми, а допустимость научного метода может быть доказана. Это ограничивает число методов атаки на преодоление зашиты потребительского доступа устройств, поскольку они должны быть многократно протестированы и одобрены.

Чтобы не полагаться исключительно на покупки очень дорогого и не всегда вполне эффективного зарубежного программного обеспечения для криминалистического исследования, постоянно ведётся поиск описанных уязвимостей безопасности в устройствах и операционных системах, известных как эксплойты.

Например, эксплойт Checkm8 (наименование означает «шах и мат») – для уязвимости в оборудовании Apple, который затрагивает модели iPhone, iPad и iPod Touch. Checkm8 влияет на устройства с чипами A5 до A11, такие как модели: от iPhone 4s до iPhone X, iPad Mini и iPad Air, iPod Touch: iPod Touch 5G и 6G. Устройства с чипами A12 и более новые (например, iPhone XS и более новые модели) не подаются Checkm8.

Существуют и другие эксплойты, описанные специалистами. Несколько примеров:

- checkra.in – Jailbreak. Для получение административного доступа к телефону приложим к моделям от iPhone 5s до iPhone X при версии операционной системы iOS 12.0 и выше;
- palera.in – Jailbreak. Для получение административного доступа к телефону приложим к моделям iPhone, iPad, MacBook и Apple TV при версии операционной системы 15 и выше.

Экзотические приемы.

Для того чтобы выполнять свою работу, иногда экспертам приходится изучать методы взлома хардвера и манипулировать компонентами устройства, работая буквально с паяльником в руке.

Эффективными иногда оказываются весьма неожиданные приёмы. Например, снятие отпечатков пальцев сразу после изъятия и их использование для обмана датчика отпечатков пальцев, исследовать следы, оставленные на экране телефона, с помощью ультрафиолетового света, чтобы угадать жест или код разблокировки, а также проинструктировать оперативных работников тайно следить за кодом, пока пользователь его вводит. Даже банальный просмотр видеозаписи с камер наблюдения видимого ввода кода или пароля иногда приводит к результатам. Конечно, эти приемы зависят от ситуации и не всегда применимы, с другой стороны, практика доказала их эффективность.

В итоге, из-за отсутствия сотрудничества со стороны производителей мобильных телефонов и смарт-устройств работа экспертов-криминалистов становится все более неэффективной.

Мировые лидеры в производстве мобильных устройств даже не беспокоятся о решениях правительства или суда, поскольку знают, что половина человечества мечтает иметь последнюю и самую блестящую модель брендового телефона или умных часов.

Пока безопасность персональных устройств становится все более жесткой и все производители рекламируют себя через это, все чаще в СМИ выходит информация о большем количестве нарушений конфиденциальности пользователей умных устройств.

Обычные пользователи и даже криминалисты не имеют доступа к исходному коду конкретной модификации операционной системы и приложений и не могут

проверить, насколько корректно они выполняют требования по защите персональных данных и личного пространства пользователей.

Операционные системы (Android и iOS) собирают данные об использовании устройства, такие как местоположение, история поиска и поведение приложений. Эти данные (официально) используются для повышения производительности, персонализации рекламы и предоставления услуг, но на некоторых телефонах даже после ограничения доступа к данным с помощью настроек они продолжают собираться.

Многие приложения запрашивают доступ к камере, микрофону, местоположению и контактам, даже если это не является необходимым для их работы. Пока некоторые приложения собирают данные в рекламных целях, другие продают их третьим лицам. В целом, профилирование пользователей является прибыльным бизнесом для большинства крупных игроков на рынке мобильных и смарт-устройств.

Несколько примеров.

Компания Apple предоставила данные из учетных записей iCloud по законным запросам государственных органов. Хотя компания старается защищать конфиденциальность пользователей, она обязана соблюдать местные законы.

Сканирование CSAM: в 2021 году Компания Apple объявила о планах по внедрению системы сканирования фотографий iCloud на предмет обнаружения детской порнографии (CSAM). Это вызвало широкую критику, поскольку многие считают, что это может быть использовано для массовой слежки. Впоследствии Apple отложила реализацию этой функции.

Компанию Apple не раз критиковали за сбор данных о местоположении, даже если пользователи отключают настройки определения местоположения. В ответ компания утверждает, что эти данные анонимизируются и используются для улучшения услуг.

Дело Zoom (2019): в 2019 году было обнаружено, что приложение Zoom для macOS использует скрытую функцию, которая позволяет серверу активировать камеру пользователя без явного разрешения. Это стало возможным из-за уязвимости в macOS, которую использовал Zoom. Apple быстро отреагировала и разослала обновление для устранения проблемы.

Отчеты об активации микрофона: некоторые пользователи сообщают, что индикатор микрофона (оранжевая точка) активируется без использования приложения, требующего доступа к микрофону. Системные функции iOS, такие как Siri и программа диктовки, используют микрофон для работы. Хотя эти функции требуют разрешения, некоторые пользователи могут не знать, что они могут активировать микрофон в любое время.

Google собирает огромный объем данных о пользователях Android, включая местоположение, историю поиска и поведение в приложениях. Эти данные используются для персонализации рекламы и улучшения услуг.

Многие приложения Android используют библиотеки отслеживания для сбора пользовательских данных. Сюда входят данные о местоположении, поведении и даже информация из других приложений. Google отслеживает местоположение пользователей, даже если службы определения местоположения отключены. Это

стало предметом критики и судебных исков.

Дело Google Ассистент (2019): в 2019 г. выяснилось, что Google Помощник записывает разговоры пользователей, даже если он не был явно активирован командой «Окей, Google». Google признал, что небольшой процент аудиоклипов был записан по ошибке, и пообещал улучшить процесс проверки.

Некоторым вредоносным приложениям удается обойти защиту Android и получить доступ к камере или микрофону без явного разрешения. Например, в 2020 г. было обнаружено вредоносное приложение, которое могло записывать звук и делать фотографии без ведома пользователя.

Использование камеры в рекламных целях: в 2019 г. компания Samsung подверглась критике после того, как появились сообщения о том, что камера устройства может использоваться для распознавания объектов и показа рекламы.

Facebook[1] неоднократно подвергался скандалам и критике в связи с защитой конфиденциальности. Вот некоторые из наиболее известных случаев.

Скандал Cambridge Analytica, когда в 2018 г. выяснилось, что данные миллионов пользователей были собраны без их согласия компанией Cambridge Analytica. Эти данные использовались в политических целях, включая кампанию Brexit и выборы в США в 2016 г.

Facebook собирает огромный объем данных о пользователях, включая информацию о местоположении, поведении в приложении, и даже данные от третьих лиц. Официально эти данные используются для персонализации рекламы, но пользователи не имеют контроля над их хранением и распространением.

Отслеживание пользователей за пределами Facebook: Facebook использует технологии отслеживания (такие как пиксели и файлы cookie) для сбора данных о пользователях по всему Интернету, даже если они не вошли в свою учетную запись.

Facebook неоднократно становился объектом утечек данных. Например, в 2021 г. данные более 500 млн пользователей были загружены и опубликованы в Интернете.

Facebook подвергся критике за то, как он обращается с данными детей. Например, в 2021 г. стало ясно, что платформа может оказывать негативное влияние на психическое здоровье подростков.

Наконец, следует добавить, что в конструкции аппаратного обеспечения современных мобильных телефонов и смарт-устройств есть много решений, которые невозможно объяснить, например, в некоторых GSM-устройствах. Модуль имеет прямое подключение к RAM памяти телефона (DMA), что необязательно, но все же существует. При таком подключении скрытая функциональность в GSM Модуль может копировать и отправлять всю текущую память телефона (dump) во время его работы.

---

[1] Здесь и далее: *Facebook* («Фейсбук») – американская социальная сеть и одна из крупнейших медиаплатформ в мире. Принадлежит корпорации Meta, которая внесена в перечень организаций, причастных к терроризму и экстремизму, и запрещена на территории Российской Федерации; заблокирована в РФ *(прим. ред.)*.

В заключение, тенденция последних 4–5 лет состоит в том, что получение законным путем данных все более затруднительно, в то время как объем незаконного приобретения баз данных остается на нынешнем уровне. Этому способствуют интересы международных лидеров в производстве интеллектуальных устройств, поскольку профилирование пользователей является прибыльным бизнесом.

Конечно, у этой проблемы много сторон, и она также связана с гражданскими свободами каждого из нас, но без правовых мер, заставляющих производителей предоставлять доступ к данным потребителя государственным органам в случае необходимости, криминалистическая экспертиза смарт-устройств обречена стать большой, можно сказать, недоступной роскошью для следствия.

Список источников

1. Apple inc., Apple Platform Security. December 2024.
2. CheckM8 Co., Bypass Activation Lock using CheckM8 Software, 2023.
3. Google’s AI Faces Privacy Law Showdown: Natlawreview.com URL: https://natlawreview.com/article/caught-listening-googles-ai-faces-privacy-law-showdown, 2024.
4. How Apple plans to monitor users. Kaspersky.com. URL: https://www.kaspersky.com/blog/what-is-apple-csam-detection/41502/, 2021.
5. Kim Jong Cracks, checkra1n, Jailbreak for iPhone 5s through iPhone X, iOS 12.0 and up, 2021.
6. Medium.com, Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website: https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5, 2019.
7. Official Journal of the European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR).
8. Palera1n team, Jailbreak for iPhone, iPad, Macbooks, and AppleTV's for versions 15 and higher, 2024.
9. Personal Data Of 533 Million Facebook Users Leaks Online: Forbes.com. URL: www.forbes.com/sites/ajdellinger/2021/04/03/personal-date-of-533-million-facebook-users-leaks-online.
10. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach: Theguardian.com URL: www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
11. Samsung is being sued by customers for not disclosing a defect that has been causing smartphone cameras on the Samsung Galaxy S20 to shatter unexpectedly: Hindustantimes.com. URL: https://tech.hindustantimes.com/mobile/news/samsung-is-getting-sued-because-the-camera-on-the-galaxy-s20-is-shattering-unexpectedly-71619890193282.html.

А.Б. Курумбаева
Карагандинская академия МВД Республики Казахстан
имени Б. Бейсенова, Караганда, Республика Казахстан

Общесоциальные меры предупреждения мошенничества, совершаемого с использованием информационных систем

Аннотация. Последние 10 лет в Казахстане проводится активная и эффективная государственная политика цифровизации всех сфер человеческой деятельности. Вследствие этого стал возможным широкомасштабный охват населения средствами телекоммуникации и доступа в сеть Интернет. В интернете появились целый ряд современных финансовых инструментов, торговых площадок и социальных сетей, значительное количество информационных продуктов, позволяющих ускорить и повысить эффективность процессов взаимодействия между гражданами, а граждан – с государством. Вместе с тем, такое развитие информационных систем вызвало скачкообразный рост количества преступлений, совершаемых в интернете.

В представленной работе автором решается задача по определению ряда общесоциальных мер предупреждения мошенничества, совершаемого с использованием информационных систем. Автором указано на актуальность разработки комплекса мер раннего предупреждения такого вида мошенничеств, основой которого являются общесоциальные меры предупреждения. Отдельно рассмотрены основные литературные источники, так или иначе затрагивающие проблему мошенничеств в интернете.

В основной части исследования автором рассмотрены разновидности мошенничеств, совершаемых с использованием информационных систем, вопросы структуры и динамики таких преступлений. Отдельно рассмотрены причины и условия совершения мошенничеств с использованием информационных систем.

На основании анализа видов, динамики и структуры, а также причин и условий, способствующих совершению мошенничеств с использованием информационных систем, автором сформулирован ряд мер общесоциального характера, направленных на предупреждение таких преступлений. В их числе предложения по совершенствованию законодательства и правовой системы, предложения, направленные на формирование высокого уровня информационной грамотности граждан, снижение их подверженности преступным посягательствам в информационном пространстве, и другие меры.

Ключевые слова: информационная грамотность, кибербезопасность, интернет-мошенничества, мошенничества, совершаемые с использованием информационных систем, информационная безопасность, предупреждение преступлений.

Одним из ярких признаков современного казахстанского общества является планомерное расширение цифровой среды, которая позволяет качественно изменить не только темпы экономического роста государства, но и существенно повысить уровень благосостояния граждан. Широкая цифровизация общественных отношений породила новые сферы приложения экономических возможностей, что послужило причиной создания новых финансовых и

социальных продуктов. Значительные объективные изменения уровня коммуникации граждан, произошедшие за последние несколько лет, позволили существенным образом увеличить цифровую сферу взаимодействия уровней «человек – человек» и «человек – государство».

Вполне естественно, что взрывное разрастание информационной среды, перевод большей части финансовых и торговых отношений в интернет-пространство, не могли не повлечь определенной степени криминализации таких отношений. Криминализация интернет-сферы является свершившимся явлением, и ни у кого этот факт не вызывает сомнения. Уже сейчас ежегодный фиксируемый ущерб от мошенничеств, совершаемых с использованием информационных систем, составляет миллиарды тенге[1]. В этом свете особую важность и актуальность приобретает комплекс мер раннего предупреждения такого рода преступлений, основой которого, по нашему мнению, являются общесоциальные меры предупреждения. Отметим, что вопросам киберпреступности уделяется достаточно широкое внимание. Так, этим вопросам одними из первых на постсоветском пространстве уделили внимание такие отечественные ученые, как Б.Х. Толеубекова[2], Р.А. Назмышев[3]. Заслуживает внимания работа А.Д. Мухамеджановой[4], рассмотревшей отдельные вопросы динамики и причин интернет-мошенничества. Ряд вопросов криминологического, уголовно-правового, уголовно-процессуального и оперативно-разыскного характера противодействия интернет-мошенничествам рассмотрен в работах таких авторов как И.Р. Бегишев[5], А.И. Бойцов[6],

[1] Ущерб на 7 млрд тенге причинили казахстанцам интернет-мошенники в этом году. URL: https://www.nur.kz/ (дата обращения 10.01.2025).

[2] Толеубекова Б.Х. Компьютерная преступность: уголовно-правовые и процессуальные аспекты: Учеб. пособие. Караганда: Караганд. ВШ МВД СССР, 1991. 82 с.

[3] Назмышев Р.А. Актуальные проблемы совершенствования практики расследования преступлений в сфере компьютерной информации: дис. … канд. юрид. наук. Алматы, 2003.

[4] Мухамеджанова А.Д. Особенности динамики киберпреступности в Республике Казахстан и её влияние на её предупреждение. URL: https://cyberleninka.ru (дата обращения 10.01.2025).

[5] Бегишев И.Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации // Вестник Казанского юридического института МВД России. 2016. № 3(25). С. 112–117.

[6] Бойцов А.И. Преступления против собственности: учебное пособие. СПб.: Юридический центр ПРЕСС. 2002. 775 с.

А.Г. Волеводз[1], О.С. Гузеева[2], Р.И. Дремлюга[3], А.С. Камко[4], И.А. Клепицкий[5], В.А. Номоконов[6], В.С. Овчинский[7], Т.Л. Тропина[8], А.Ю. Чупрова[9] и многих других.

Полагаем необходимым особое внимание обратить на работы А.С. Камко, который, впервые на монографическом уровне рассмотрел вопросы профилактики интернет-мошенничеств. Так же в ряде публикаций им уделено внимание виктимологической профилактике преступлений в сфере безналичного обслуживания, зарубежной системе профилактики и противодействия мошенничеству в сфере высоких технологий, определены проблемы и перспективы системы противодействия мошенничеству с использованием телекоммуникационного и компьютерного оборудования, а также рассмотрены уголовно-правовые вопросы противодействия преступности в сфере безналичных расчетов.

В данной статье автором использовались различные методы научного исследования. Выбор методов исследования обусловлен, прежде всего, темой исследования. Среди основных методов, которые были использованы в данной работе, можно выделить следующие: диалектический, аналитический, метод классификации, обобщения, статистический метод. Использование аналитического и статистического методов позволило установить, что КПСиСУ ГП Республики Казахстан в период с 2018 по 2023 годы в стране было зарегистрировано более 70000 уголовных правонарушений, совершенных с использованием Интернета[10]. При этом, если в 2018 году было зарегистрировано

---

[1] Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества: монография. М.: Юрлитинформ, 2001. 496 с.

[2] Гузеева О.С. Квалификация мошенничества в российском сегменте сети Интернет // Законность. 2013. №3 (941). С. 21–24.

[3] Дремлюга Р.И. Интернет-преступность. Владивосток: изд-во Дальневосточного университета, 2008. 240 с.

[4] Камко А.С. Предупреждение мошенничества с использованием телекоммуникационных и компьютерных сетей: дис. … канд. юрид .наук. Красноярск, 2020.

[5] Клепицкий И.А. Собственность и имущество в уголовном праве // Государство и право. 1997. № 5. С. 78.

[6] Номоконов В.А. Киберпреступность: прогнозы и проблемы // Библиотека криминалиста. 2013. № 5 (10). С. 148–159.

[7] Овчинский В.С. Оперативно-разыскная аналитика в цифровом мире // Информатизация и информационная безопасность правоохранительных органов. Сб. трудов XXV Всерос. науч.-практ. конф. Академия управления МВД России, 2016. С. 175–180.

[8] Тропина Т.Л. Криминализация киберпреступлений: достижение консенсуса // Компьютерная преступность и кибертерроризм. Исследования, аналитика. 2004. № 2. С. 49–56.

[9] Чупрова А.Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. ... д-ра юрид. наук. М., 2015. 479 с.

[10] Статистические данные – сведения об уголовных правонарушениях за 2018–2023 год. URL: https://qamqor.gov.kz (дата обращения 12.01.2025).

только 589 таких уголовных правонарушений, то уже в 2020 году их было зарегистрировано 14325, в 2021 – 21479, в 2022 – 23683, и по итогам первого полугодия 2023 года эта цифра составила – более 12000 зарегистрированных уголовных правонарушений такого характера. Анализ статистической информации о количестве и видах уголовных правонарушений, совершаемых в интернет-пространстве, позволяет сделать вывод о том, что львиную долю таких уголовных правонарушений – 99,2%, составляют так называемые интернет-мошенничества, то есть деяния, предусмотренные п. 4 ч. 2 ст. 190 УК Республики Казахстан «Мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы». Обратим внимание, что далее по тексту для простоты изложения материала мы называем указанные уголовные правонарушения общепринятым понятием – интернет-мошенничество.

Следует отметить, что, несмотря на ураганный рост общего числа интернет-мошенничеств, в общей структуре преступности они занимают только 1,7%. Вместе с тем, несмотря на сравнительно небольшой удельный вес зарегистрированных интернет-мошенничеств, следует не забывать о достаточно высокой латентности рассматриваемого вида уголовного правонарушения. Как показывают уголовная и судебная статистика, довольно значительная часть таких деяний по целому ряду объективных причин остается за рамками реально выявленных и раскрытых уголовных правонарушений.

Оценивая динамику роста количества интернет-мошенничеств, можно увидеть, что в период с 2021 года по настоящее время темпы такого роста значительно замедлились. Изменение пиков темпа роста, на наш взгляд, связано с двумя следующими причинами.

1. Максимальный темп роста количества подобных уголовных правонарушений, представленный на отрезке от 2017 до 2021 года, связан, по нашему мнению, прежде всего, с масштабным разрастанием числа казахстанских пользователей интернета, а также значительным увеличением количества сетевых продуктов.

2. Замедление же темпов роста количества интернет-мошенничеств на отрезке с 2021 года по настоящее время, в свою очередь, связано с реализацией целого ряда государственных программ, принятие и реализация которых стали следствием осознания государством степени угрозы со стороны интернет-мошенников. К числу таких программ следует отнести Концепцию кибербезопасности «Киберщит Казахстана», где в качестве цели реализации выступили: «…достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающего устойчивое развитие Республики Казахстан в условиях глобальной конкуренции…»[1]. Вторым таким программным документом стала Концепция цифровой трансформации, развития отрасли информационно-

[1] Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")».

коммуникационных технологий и кибербезопасности на 2023–2029 годы. Благодаря реализации положений Концепции кибербезопасности «Киберщит Казахстана» был создан Национальный координационный центр кибербезопасности. Основной задачей данного центра является: «…защита от внешних и внутренних кибератак; сбор и анализ информации об инцидентах кибербезопасности; мониторинг объектов информатизации «электронного правительства»; выявление и пресечение угроз и инцидентов кибербезопасности…»[1].

Отметим, что несмотря на значительный комплекс мер, предпринимаемых со стороны государства, и снизившиеся темпы роста количества таких преступлений, можно констатировать, что устойчивый рост числа интернет-мошенничеств в перспективе будет продолжаться. Здесь мы полностью разделяем позицию А.Д. Мухамеджановой, отметившей, что «…наблюдая рост регистрации интернет-мошенничеств, можно сделать вывод, с одной стороны, о недостаточности и малоэффективности проводимых мер по предупреждению и профилактике данных деяний; с другой стороны, о доверчивости и правовой неграмотности граждан, бесконтрольном распространении мошеннических мобильных приложений, об открытой рекламе финансовых интернет-пирамид, малоэффективности существующих мер киберзащиты платёжных интернет-платформ, нехватке специалистов по кибербезопасности и др..»[2].

Оценивая структуру такого вида преступности как интернет-мошенничества, следует сказать, что существует более 20 видов такого преступления. Их классификация зависит от способа преступления, личности жертвы, личности преступника, используемых технологий.

Специалистами по кибербезопасности принято выделять следующие виды интернет-мошенничеств:

1. Телефонное мошенничество, социальная инженерия. Использование доверительного отношения потерпевшего.
2. Фишинг. Технологическое получение доступа к персональным данным, логинам и паролям. Это вид мошенничества посредством фишинг-сайтов, электронной почты, контент ссылок, фишинговых приложений для смартфонов (клоны банковских приложений), мошенничество через СМС.
3. Ложные сообщения о чрезвычайных ситуациях.
4. Мошенничество на электронных торговых площадках.
5. Мошенничество в социальных сетях.
6. Мошенничество в мессенджерах Telegram и WhatsApp.
7. Мошенничество с платежными картами (кардинг).

---

[1] Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 «Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023–2029 годы».

[2] Мухамеджанова А.Д. Особенности динамики киберпреступности в Республике Казахстан и её влияние на её предупреждение. URL: https://cyberleninka.ru (дата обращения 10.01.2025).

8. СМС от лжебанка.
9. Мошенничество в сетях GSM.
10. Предложения заработка в интернете или работы на дому.
11. Оплачиваемые опросы.
12. «Фрод» – обман веб-сайта или интернет-магазина.
13. Громкий заголовок в сети (кликбейт).
14. Мошенничество с подарочными картами.
15. Лотереи, викторины, победы в конкурсах.
16. «Каперство» – требование выкупа за возврат похищенных аккаунтов.
17. Мошенничество в онлайн-играх.
18. Мошенничество на сайтах онлайн-знакомств.
19. Финансовые пирамиды, мошеннические инвестиционные проекты.
20. Мошенничество с криптовалютами.
21. Мошенничество через благотворительность.
22. Распространение «нигерийских писем».
23. Программы-вымогатели.
24. Невидимые элементы на сайте (кликджекинг).

Множество видов интернет-мошенничества в совокупности с широтой охвата населения сетевыми и телекоммуникационными технологиями прямо указывает на то, что с проявлениями этого антисоциального явления сталкивался практически каждый гражданин Республики Казахстан. Именно это обуславливает необходимость выработки эффективного комплекса профилактики этого явления.

Предупреждение преступности в общем и отдельных её видов, в частности, в криминологической науке принято делить на два комплекса мер: общие, или общесоциальные и специальные меры. Как отмечает В.Д. Ларичев: «…общее предупреждение преступлений состоит в осуществлении таких мероприятий, которые обеспечивают позитивное воздействие на социальные процессы. Эти меры являются необходимым элементом социально-экономической деятельности устранения недостатков в политической, социальной, нравственно-психологической и духовной сферах общества. Они, как правило, связаны с улучшением материального благосостояния граждан, условий их труда и отдыха, а также с другими позитивными изменениями в обществе…»[1]. При этом разработка комплекса общесоциальных мер предупреждения мошенничеств, совершаемых с использованием информационных систем, по нашему мнению, не может быть эффективной без понимания причин и условий, детерминирующих этот вид преступности. Это связано прежде всего с тем, что купировочное воздействие на причину преступления заведомо эффективнее борьбы с его последствиями. И основным условием разработки общесоциальных

[1] Ларичев В.Д. Общесоциальное предупреждение преступности. Что это, вид криминологического предупреждения преступности или просто поступательное развитие общества? (Постановка вопроса) // Общество и право. 2011, № 1 (33). С. 130–133.

мер предупреждения преступности, мы полагаем, должно стать понимание именно социальных причин такого рода преступности.

Проведенный нами анализ позволил выделить следующие социальные причины интернет-мошенничеств:

1. Возросший уровень информатизации казахстанского общества, обусловленный масштабным ростом доступа к интернет-технологиям, за счет расширения сферы электронных услуг, развития компьютерных технологий, электронного документооборота, охвата граждан электронно-коммуникационными сетями и т.д. Отметим, что эти, в общем позитивные изменения, в то же время сами по себе и способствуют росту количества интернет-мошенничеств.

2. Низкая эффективность контроля над интернет-сферой со стороны государства как следствие несовершенства казахстанского законодательства, регулирующего вопросы, связанные с информационными технологиями.

3. Существенная разница между объективными потребностями граждан в информационных технологиях и продуктах и возможностью легального приобретения таких технологий и продуктов. Так, стоимость современных систем и программного продукта в сфере интернет-технологий зачастую попросту недоступна для большинства граждан. Это в свою очередь приводит либо к использованию нелегальных продуктов и технологий, либо неиспользованию, например, эффективных систем защиты вообще. Негативно на этот фактор влияет и монополизация сферы разработки информационных систем безопасности и отсутствие эффективного казахстанского продукта, обеспечивающего надежную защиту от различного уровня интернет-угроз, что в свою очередь обуславливает искусственное завышение стоимости такого продукта. Как следствие монополизации выступает недобросовестная конкуренция. Здесь мы вынуждены согласиться с К.Н. Евдокимовым, который утверждает, что «…Недобросовестная конкуренция вплоть до промышленного шпионажа между производителями программного обеспечения и антивирусной защиты. На практике происходит повсеместное нарушение авторских и патентных прав производителей программных продуктов и оригинальных технических решений, связанных с обеспечением компьютерных технологий и должной работы компьютерных сетей. При этом рядовой потребитель либо не может обнаружить подделку программного продукта, либо, что чаще всего, сознательно, как говорится, закрывает глаза на использование нелицензированной продукции, поскольку она заведомо дешевле оригинального продукта, а по своим качественным характеристикам нередко ничем ему не уступает …»[1].

4. Широкомасштабное распространение вредоносного контента и программного продукта. При этом наблюдается парадоксальная ситуация, когда производители легального программного продукта сами разрабатывают вредоносный контент, при этом цели такой разработки могут быть самые

[1] Евдокимов К.Н. Причины компьютерной преступности в современной России // Российский следователь. 2015. № 3. С. 33–37.

разнообразные: от конкурентной борьбы, до привязки потребителя только к своему программному продукту.

4. Организованный и почти всегда профессиональный характер рассматриваемого вида преступности. Это связано с возможностью быстрого, относительно безопасного и максимального обогащения, а также необходимостью «разделения труда» преступников. Профессиональный характер деятельности интернет-мошенников также связан с необходимостью специальных знаний в области информационных технологий для совершения преступлений.

5. Отставание действующих средств кибербезопасности от уровня развития коммуникационных технологий. Так система разработки и применения современных интернет-технологий далеко не всегда может учесть все уязвимости. Как правило, системы, средства и методики защиты разрабатываются или изменяются только после обнаружения новых угроз.

6. Высокий уровень виктимности интернет-мошенничеств. Во-первых, он обусловлен тем, что информационные технологии охватывают практически все сферы деятельности человека, а доступ к сети Интернет и её возможностям в настоящее время, благодаря средствам телекоммуникации, имеется практически у 100% граждан Республики Казахстан. Во-вторых, это связано с низкой степенью кибергигиены и низким уровнем цифровой грамотности населения.

Таким образом, перечисленные выше виды, причины и условия интернет-мошенничеств прямо указывают на те обстоятельства, которые детерминируют рассматриваемый вид уголовного правонарушения и негативным образом влияют на его динамику. Соответственно, структура и система общесоциальных мер предупреждения должны формироваться исходя из максимального воздействия на перечисленные нами факторы.

Анализ указанных выше видов и причин интернет-мошенничеств, наряду с анализом действуещей нормативно-правовой базы позволил сформулировать следующие общесоциальные меры предупреждения мошенничества, совершаемого с использованием информационных систем.

1. Действующий Закон Республики Казахстан «О профилактике правонарушений» от 29 апреля 2010 года № 271-IV ни в коей мере не учитывает современный потенциал угрозы, исходящей от различных видов интернет-мошенничеств. Так, в настоящее время целевым компетентным органом, реализующим государственную политику в сфере цифрового развития страны, обеспечения информационной безопасности, информатизации, руководство в области связи, информатизации, «электронного правительства», развития государственной политики в сфере оказания государственных услуг (электронных), является Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. Вместе с тем указанный государственный орган, в чьей прямой компетенции состоит обеспечение кибербезопасности, не входит в число субъектов профилактики правонарушений, перечисленных в главе 2 названного Закона.

Исходя из сказанного, полагаем необходимым дополнить главу 2 Закона Республики Казахстан «О профилактике правонарушений» соответствующей

статьей 16-1 «Компетенция уполномоченного органа в области обеспечения информационной безопасности в сфере информатизации, руководство в области связи, информатизации, «электронного правительства».

2. Одной из мер общесоциального характера, призванной снизить уровень кибервиктимности граждан, полагаем считать принятие национального Плана, в котором следует разработать пакет мер, направленных на формирование и закрепление у граждан Республики Казахстан устойчивых навыков и знаний о «кибергигиене», повышение общего уровня цифровой грамотности населения. В указанном аспекте полагаем необходимым широко использовать потенциал образовательных учреждений, а также возможности СМИ через создание и распространение качественного образовательного контента.

3. Следует создать «тепличные условия» с наивысшим уровнем благоприятствования в том числе и налогового, для отечественных IT-компаний с целью повышения их конкурентоспособности, для привлечения квалифицированных специалистов и создания высококласного сетевого и телекоммуникационного продукта. Указанное же, по нашему мнению, возможно только при принятии и реализации соответствующей государственной программы.

Таким образом, считаем, что приведенные нами общесоциальные меры предупреждения мошенничества, совершаемого с использованием информационных систем, реализованные наряду с перцепцией лучшего зарубежного правового и технологического опыта позволят существенным образом снизить уровень рисков в области предупреждения не только интернет-мошенничеств, но и интернет-преступности в целом.

Список источников

1. Бегишев И.Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации / И.Р. Бегишев // Вестник Казанского юридического института МВД России. 2016. № 3(25). С. 112–117.
2. Бойцов А.И. Преступления против собственности: учебное пособие. СПб: Юридический центр ПРЕСС, 2002. 775 с.
3. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества: монография. М.: Юрлитинформ, 2001. 496 с.
4. Гузеева О.С. Квалификация мошенничества в российском сегменте сети Интернет // Законность. 2013. №3 (941). С. 21–24.
5. Дремлюга Р.И. Интернет-преступность. Владивосток: изд-во Дальневосточного университета, 2008. 240 с.
6. Евдокимов К.Н. Причины компьютерной преступности в современной России // Российский следователь. 2015. № 3. С. 33–37.
7. Камко А.С. Предупреждение мошенничества с использованием телекоммуникационных и компьютерных сетей: дис. … канд. юрид. наук. Красноярск, 2020.

8. Клепицкий, И.А. Собственность и имущество в уголовном праве // Государство и право. 1997. № 5. С. 78.

9. Ларичев В.Д. Общесоциальное предупреждение преступности. Что это, вид криминологического предупреждения преступности или просто поступательное развитие общества? (Постановка вопроса) // Общество и право. 2011. № 1 (33). С. 130–133.

10. Мухамеджанова А.Д. Особенности динамики киберпреступности в Республике Казахстан и её влияние на её предупреждение // Российско-азиатский правовой журнал 2022, № 2. С. 49–55. DOI: 10.14258/ralj(2022)2.9.

11. Назмышев Р.А. Актуальные проблемы совершенствования практики расследования преступлений в сфере компьютерной информации: дис. … канд. юрид. наук. Алматы, 2003.

12. Номоконов, В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. 2013. № 5 (10). С. 148–159.

13. Овчинский В.С., Овчинский А.С. Оперативно-разыскная аналитика в цифровом мире // Информатизация и информационная безопасность правоохранительных органов. Сб. трудов XXV Всерос. науч.-практ. конф. Академия управления МВД России, 2016. С. 175–180.

14. Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 «Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023–2029 годы».

15. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")».

16. Статистические данные – сведения об уголовных правонарушениях за 2018–2023 год. URL: https://qamqor.gov.kz.

17. Толеубекова Б.Х. Компьютерная преступность: уголовно-правовые и процессуальные аспекты: Учеб. пособие. Караганда: Караганд. ВШ МВД СССР, 1991. – 82 с.

18. Тропина Т.Л. Криминализация киберпреступлений: достижение консенсуса // Компьютерная преступность и кибертерроризм. Исследования, аналитика. 2004. № 2. С. 49–56.

19. Чупрова А.Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. ... д-ра юрид. наук. М., 2015. С. 479.

В.Ю. Мельников
ВГУЮА (РПА Минюста России)
Ростовский институт (филиал)

Борьба с коррупцией как необходимый элемент обеспечения национальной безопасности

Аннотация. Противодействие коррупции является одной из приоритетных задач государственной политики и важнейшим направлением деятельности органов прокуратуры Российской Федерации, которым отводится центральное место в реализации антикоррупционного законодательства и обеспечении его неукоснительного соблюдения. Прокуратура Российской Федерации – это единая федеральная централизованная система органов, осуществляющих надзор за соблюдением Конституции Российской Федерации от имени Российской Федерации и исполнением законов, действующих на ее территории.

Ключевые слова: верховенство закона, права и свободы человека, коррупция

Как мы знаем, система преступлений, предусмотренных гл. 29 УК РФ, в основном соответствует современным потребностям. Однако в содержательном отношении целый ряд предусмотренных этой главой составов нуждается в изменении и дополнении, вызванных, с одной стороны, характером подрывной деятельности против России спецслужб иностранных государств и международных террористических организаций, с другой – реальными возможностями правоохранительных органов успешно противодействовать этой подрывной деятельности. Целесообразно отметить, что включение в число объектов уголовно-правовой охраны основ конституционного строя вряд ли продуктивно в правоприменительном отношении, поскольку понятие этих основ весьма широкое (см. гл. 1 Конституции РФ), не способствующее определению сущности предусмотренных гл. 29 УК преступлений. Это вызывает определенные трудности в правоприменительной практике. Главу 29 УК РФ целесообразно назвать «Преступления против безопасности государства», что позволит судам и другим правоприменительным органам в определении объектов уголовно-правовой зашиты опираться на понятия, конкретизированные в ряде федеральных законов (о безопасности, об обороне и др.).

Функционирование государства осуществляется посредством деятельности государственного механизма, включающего в себя определенные управленческие структуры – органы, призванные обеспечивать охрану и защиту устоев общества. Именно через эти структуры с помощью многочисленной категории работников государственного аппарата реализуются властные функции государства.

В Указе Президента Российской Федерации В.В. Путина от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» коррупция отнесена к основным угрозам государственной и общественной

безопасности[1]. Только за январь – сентябрь 2021 года было зарегистрировано 27 131 преступлений коррупционной направленности[2].

Таблица 1

Надзор прокуратуры РФ за исполнением законов, соблюдением прав и свобод человека и гражданина

Наименование показателя	**1 мес. 2022 г.**	**1 мес. 2023 г.**	**% (+;-)**
Выявлено нарушений закона	285 170	293 600	3,0
Принесено протестов	34 535	37 478	8,5
Направлено исков, заявлений в суд	23 352	19 253	–17,6
Удовлетворено исков (заявлений) и прекращено дел ввиду добровольного удовлетворения требований прокурора	14 637	14 221	–2,8
Внесено представлений	71 397	72 431	1,4
К дисциплинарной ответственности привлечено лиц	27 321	27 674	1,3
Предостережено лиц о недопустимости нарушения закона	11 674	10 525	–9,8
Возбуждено уголовных дел	957	843	–11,9

Согласно данным Судебного департамента Верховного суда РФ, за 1 полугодие 2024 года судами общей юрисдикции по рассмотрению уголовных дел по первой инстанции[3] (см. таблицу 2).

В связи с остротой проблемы борьбы с организованной преступностью необходимо дальнейшее совершенствование уголовно-правовой основы борьбы с нею. Отображение в Общей части УК РФ понятия преступного сообщества (организации) и введение в Особенной части уголовной ответственности за организацию данных сообществ и участие в них было шагом вперед. Однако по многим причинам это не дало ожидаемого результата в борьбе с организованной преступностью. Одной из этих причин стало то, что законодателю не удалось вычленить четкие уголовно-правовые признаки преступной организации. Так, указанный в УК РФ центральный признак «сплоченность», по которому идет отграничение преступного сообщества от организованной преступной группы,

[1] Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. №1 (часть II). Ст.212.

[2] Официальный сайт Генеральной прокуратуры РФ/ https://epp.genproc.gov.ru/web/gprf (дата обращения: 27.03.2025).

[3] Официальный сайт Судебного департамента ВС РФ// https://cdep.ru/index.php?id=79&item= 8773 (дата обращения: 27.03.2025).

не отражает сути преступного сообщества, так как сплоченность в той или иной степени присуща и организованным преступным группам. Главное же отличие состоит в предназначении преступных сообществ, что требует для достижения поставленных преступных целей особой организационной структуры и соответствующего механизма функционирования преступной организации.

Таблица 2

Данные Судебного департамента Верховного суда РФ за 1 полугодие 2024 г.

Виды преступлений	Статья УК РФ, УПК РФ	№ стр.	Остаток неоконченных дел на начало года (отчетного периода)	Поступило дел в отчетном периоде	Рассмотрено по существу (по основной статье предъявленного обвинения)			Передано		Всего окончено
					с вынесением приговора	с прекращением дела	с применением принудительных мер к невменяемым	возвращено прокурором для устранения недостатков в порядке ст. 237 УПК РФ или прекращении уг.дела по ст. 446.2 УПК РФ	по подсудности или подведомственности[2]	
ВСЕГО (сумма строк 2-37)		1	135 574	346 940	254 224	60 725	3819	3 916	10 393	333 077
Получение взятки	290	30	1 074	1023	830	17	1	35	69	952
Дача взятки	291	31	641	2188	1145	409	1	32	167	1754
Мелкое взяточничество	291.2	32	305	1779	1186	237	1	15	210	1649
Другие преступления против интересов службы в органах власти и местного самоуправления	285-288, 291.1, 292–293	33	1508	1827	1202	293	0	97	100	1692

Преступные сообщества создаются не только с целью совершения тяжких и особо тяжких преступлений, как это заложено в УК РФ. Реально они систематически занимаются любой преступной деятельностью, которая

приносит доход или направлена на достижение иных преступных целей, включая террористические. Взятый из криминологии термин «преступное сообщество» не отражает уголовно-правовой сути данного явления. Есть основание говорить не о преступном сообществе, а о преступных организациях (этимологически любая предварительно сорганизовавшаяся преступная группа – это преступное сообщество). Поскольку при принятии УК РФ сам термин «преступная организация» вызывал неприятие, то законодатель использовал этот термин как синоним привычному понятию преступного сообщества.

В основном УК РФ содержит правовую основу для борьбы как с государственной изменой, так и со шпионажем. Вместе с тем, теоретический анализ ст. 275 УК и практики ее применения свидетельствует о том, что ее диспозиция представляет собой научную дефиницию государственной измены в наиболее развернутом виде, в то время как в статье должны быть четко выражены признаки состава измены, включая действия, совершаемые на раннем этапе. Это привело к тому, что выдача государственной тайны и шпионаж как формы государственной измены получили сущностную характеристику без учета технико-юридических требований. Эти формы стали разновидностями оказания помощи иностранному адресату в проведении враждебной деятельности в ущерб внешней безопасности России. В свою очередь, это привело к неодинаковой трактовке предмета доказывания, в частности по делам о шпионаже применительно к ст. 275 и 276 УК РФ.

Сложилась ситуации, когда независимо от формы измены требуется доказывать враждебную деятельность иностранного адресата, а применительно к составу шпионажа со стороны иностранного гражданина и лица без гражданства такого требования нет (см. ст. 276). Правоприменительная практика сталкивается с серьезнейшей проблемой доказывания состава государственной измены, когда иностранным адресатом являются, например, экологическая организация, благотворительный фонд, СМИ, коммерческая фирма. Даже в случае, если под их прикрытием действуют кадровые сотрудники иностранных спецслужб, которым выдавалась или передавалась российским гражданином государственная тайна, доказать требуемую законом враждебную деятельность иностранной организации или их представителей против России крайне сложно, а зачастую практически невозможно.

Среди множества существующих в современном мире проблем острейшей представляется также коррупция, ставшая для России национальной бедой. В результате роста коррупционных «откатов» становится менее эффективной и конкурентоспособной экономика, меняется природа предпринимательства. Являясь, по выражению Н. Бердяева «устоем русской жизни», коррупция сегодня приобрела невиданные масштабы, трансформируя основу правоохранительной системы, разлагая общество и подрывая международный авторитет страны.

В активных публичных дискуссиях, диссертациях, многообразных материалах отечественных и зарубежных исследователей представлены различные подходы к пониманию коррупции, её оценки и условия искоренения. Нельзя не согласиться с выводом многих авторов о том, что коррупция во многом

определяется спецификой формирования и деятельности властных структур, являясь проблемой не генетической, а историко-правовой. Изучение характерных проявлений коррупции в нашей стране, анализ и обобщение опыта прошлого – основа для определения важнейших направлений современной антикоррупционной политики.

Предпринят масштабный ряд изменений в сфере государственного управления и взят курс на организацию противодействия коррупционной преступности в России, так как сфера распространения коррупции достаточно велика и постоянно расширяется. Российская правоохранительная система должна обеспечивать выполнение государством своих функций и задач по защите прав и свобод граждан от произвола должностных лиц. В связи с этим, проблема соблюдения законности в деятельности лиц, занимающих определенные должности, является чрезвычайно актуальной для России.

С каждым днем количество совершаемых должностных преступлений только увеличивается. И способствует этому то, что должностным лицам, в большинстве случаев, тем или иным образом удается избежать уголовного преследования и заслуженной меры наказания, либо они подвергаются ей в несоразмерно меньшей степени, чем заслуживают, исходя из совершенных деяний. Такая ситуация влечет за собой серьезные последствия – это и подрыв общественного порядка в стране, и разрушение аппарата управления обществом и государством в целом[1].

В Уголовном кодексе Российской Федерации существует термин «злоупотребление должностными полномочиями» (статья 285), разграничив понятия «злоупотребление властью» и «превышение власти» (статья 286). С каждым днем количество совершаемых должностных преступлений только увеличивается. Способствует этому то, что должностным лицам, в большинстве случаев, тем или иным образом удается избежать уголовного преследования и заслуженной меры наказания, либо они подвергаются ей в несоразмерно меньшей степени, чем заслуживают, исходя из совершенных деяний.

Злоупотребление должностными полномочиями относится к числу должностных преступлений. Главным отличием должностных преступлений от иных видов преступности является субъект преступления. В данном случае это всегда должностное лицо – лицо, облегченное доверием государства и соответственно наделенное специальными функциями для осуществления своих полномочий. Боброва Н.А. и Перистый В.В. в своем научном исследовании определили следующий подход к рассматриваемому понятию. Так, они отмечают: «злоупотребление должностными полномочиями – это особый вид конституционно-правового, административного и гражданского правонарушения, совершаемое должностным лицом в процессе реализации своих должностных полномочий с применением недозволенных конкретных

[1] Дорская А.А. Категория «Злоупотребления властью» в российском законодательстве и юридической науке: историко-правовой анализ // Право и власть: основные модели взаимодействия в многополярном мире: Сб. трудов междунар. науч. конф. 2017. С. 71–78.

форм реализации дискреционных полномочий»[1]. Данное правовое понятие представляется наиболее широким и распространяется не только на сферу одной отрасли права. Такой подход этих и других ученых к определению понятия «злоупотребления должностными полномочиями» исходит из общего Конституционного принципа (ч. 3. ст. 17 Конституции РФ)[2].

Согласно Постановлению Пленума Верховного суда РФ от 16.10.2009 № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий», «под тяжкими последствиями как квалифицирующим признаком преступления, предусмотренным частью 3 статьи 285 УК РФ и пунктом «в» части 3 статьи 286 УК РФ, следует понимать последствия совершения преступления в виде крупных аварий и длительной остановки транспорта или производственного процесса, иного нарушения деятельности организации, причинение значительного материального ущерба, причинение смерти по неосторожности, самоубийство или покушение на самоубийство потерпевшего»[3].

Стоит отметить, что в нормативно-правовых актах России присутствовало сразу несколько определений коррупции, в связи с чем возникла необходимость сформулировать единое определение. Данное действие было осуществлено с принятием Федерального закона РФ от 25.12.2008 № 273-ФЗ «О противодействии коррупции»[4]. Злоупотребление должностными полномочиями является одной из основных угроз безопасности экономической системы страны, соответственно стоит выделить основные последствия данного состава преступления: экономические последствия; социальные последствия; политические последствия. Для решения проблемы злоупотребления должностными полномочиями необходимо со стороны государства улучшить механизмы, направленные на недопущения новых преступлений, предусмотренных ст. 285 УК РФ. Выяснение сути и назначения уголовно-правового понятия «злоупотребление должностными полномочиями», обоснование уголовной ответственности за них имеют большое значение для понимания границ действия закона, правильной квалификации деяния виновного и укрепление законности, играют важную роль в борьбе с указанными

---

[1] Боброва Н.А. Злоупотребление полномочиями как специфическая форма злоупотребления правом // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2020. № 2(41). С. 10–15.

[2] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // СЗ РФ. 01.07.2020. №31. Ст. 4398.

[3] Постановление Пленума Верховного Суда РФ от 16.10.2009 № 19 (ред. от 11.06.2020) «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» (с изменениями, внесенными постановлениями Пленума от 24 декабря 2019 г. № 59 и от 11 июня 2020 г. № 7) // Российская газета. 30.10.2009. № 207 (5031).

[4] Федеральный закон «О противодействии коррупции» от 25.12.2008 № 273-ФЗ // СЗ РФ. 2020. № 17. Ст. 2721.

деяниями и реализации функций закона в предотвращении этих преступлений. Главным отличием должностных преступлений от иных видов преступности является субъект преступления. В данном случае это всегда должностное лицо – лицо, облегченное доверием государства и соответственно наделенное специальными функциями для осуществления своих полномочий[1].

Список источников

1. Боброва Н.А., Перистый В.В. Злоупотребление полномочиями как специфическая форма злоупотребления правом // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2020. № 2(41). С. 10–15.
2. Дорская А.А. Категория «Злоупотребления властью» в российском законодательстве и юридической науке: историко-правовой анализ // Право и власть: основные модели взаимодействия в многополярном мире. Сб. трудов междунар. науч. конф. 2017. С. 71–78.
3. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // СЗ РФ. 01.07.2020. №31. Ст. 4398.
4. Постановление Пленума Верховного Суда РФ от 16.10.2009 № 19 (ред. от 11.06.2020) «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» (с изменениями, внесенными постановлениями Пленума от 24 декабря 2019 г. № 59 и от 11 июня 2020 г. № 7) // Российская газета. 30.10.2009. № 207 (5031).
5. Таилова А.Г., Нурбалаева А.М. Общая характеристика и понятие должностных преступлений // Современные тенденции развития науки и технологий. 2015. № 8-6. С. 119–121.
6. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. №1 (часть II). Ст. 212.
7. Федеральный закон «О противодействии коррупции» от 25 декабря 2008г. № 273-ФЗ (последняя редакция) // СЗ РФ. 2020. № 17. Ст. 2721.

[1] Таилова А.Г., Нурбалаева А.М. Общая характеристика и понятие должностных преступлений // Современные тенденции развития науки и технологий. 2015. № 8-6. С. 119–121.

С.В. Мельникова
Московский университет МВД России имени В.Я. Кикотя

Динамика цифровой агрессии: кибербуллинг и его формы как новый социальный вызов

Аннотация. Статья рассматривает ключевые аспекты современного феномена цифровой агрессии. В условиях стремительной цифровизации общества Интернет-пространство становится не только площадкой для общения и обмена информацией, но и зоной, где развиваются различные формы агрессии. Кибербуллинг, как одна из наиболее распространённых форм цифровой агрессии, представляет собой серьёзный вызов для общества, особенно в контексте воздействия на молодёжь и уязвимые группы населения. Статья исследует основные формы кибербуллинга, включая троллинг, оскорбления, распространение ложной информации (фейков) и вынужденное публичное унижение, а также факторы, способствующие их возникновению. Особое внимание уделяется последствиям цифровой агрессии, которые отражаются на психологическом благополучии жертв, способствуют эскалации конфликтов и формируют новые риски в межличностных коммуникациях. В статье также анализируются механизмы предотвращения и контроля кибербуллинга, включая правовые, образовательные и технологические меры, направленные на создание безопасного цифрового пространства.

Ключевые слова: кибербуллинг, цифровая агрессия, социальный вызов, интернет-пространство, онлайн-насилие, психологическое воздействие, формы буллинга, медиа-грамотность, подростки, анонимность, социальные сети.

В эпоху стремительной цифровизации социальных контактов мы стали свидетелями новых форм социализации, взаимодействия и, к сожалению, агрессии. Явление кибербуллинга – цифрового насилия, которое осуществляется через интернет и цифровые средства связи, становится важным предметом научного изучения. Его особенности заключаются в анонимности агрессора, масштабности воздействия и постоянном доступе к жертве (агрессия может происходить в любое время и преследовать жертву вне зависимости от ее реального окружения). Формы кибербуллинга варьируются от травли в социальных сетях и отправки оскорбительных сообщений до распространения ложной информации и откровенной клеветы.

Это явление затрагивает широкий круг возрастных и социальных групп, задавая новые вызовы для общества и права, приобретая угрожающий масштаб, влияя на психическое здоровье и социальное благополучие как подростков, так и взрослых.

Кибербуллинг в цифровой среде стал более многообразным и сложным по сравнению с традиционными формами буллинга.

Например, одной из распространённых форм цифрового насилия стал «doxing» (доксинг) – намеренное раскрытие личной информации жертвы без её согласия. Кроме того, активно используется так называемое «ежедневное преследование» посредством множества каналов: мессенджеров, социальных сетей, форумов и даже онлайн-игр. Важно отметить, что границы между агрессией и шуткой в цифровом пространстве становятся всё более размытыми, что затрудняет профилактику и контроль.

Из наиболее часто встречающихся в интернет-пространстве форм кибербуллинга можно выделить следующие:

– «троллинг» подразумевает намеренное провоцирование пользователей на эмоциональную реакцию с помощью комментариев, шуток или других действий. Так называемые «тролли» могут прикидываться заинтересованными в обсуждении, но их истинная цель – посеять раздор или спровоцировать конфликт;

– «хейтинг» – это направленная ненависть или негатив в адрес определённого человека, группы людей или их деятельности. «Хейтеры» выражают свои эмоции через осуждающие, грубые или оскорбительные комментарии, часто без обоснованной критики;

– «секстинг» – это отправка и обмен откровенными, интимного характера сообщениями, изображениями или видео через социальные сети, мессенджеры или другие цифровые каналы. Несмотря на кажущуюся безобидность между доверяющими друг другу людьми, такая практика несёт риск утечки личных данных;

– «грифинг» – это преднамеренное разрушительное поведение в онлайн-играх, направленное на причинение неудобств или вреда окружающим. Обычно «гриферы» целенаправленно мешают другим игрокам, разрушая их достижения или нарушая игровой процесс;

– «кибersталкинг» – «слежка в сети», преследования или домогательства, которые предполагают вторжение в личное пространство человека и нарушают его право на неприкосновенность частной жизни;

– «диссинг» – распространение в сети слухов и клеветы: ложная информация о жертве может быстро распространяться в интернете, разрушая её репутацию;

– «игнорирование или бойкот»: изоляция и исключение из онлайн-групп: жертвы кибербуллинга могут быть исключены из онлайн-общества или целенаправленно игнорироваться, что вызывает чувство изоляции и социальной отчуждённости.

Онлайн-агрессия становится одной из наиболее острых проблем среди детей и подростков, 11 % российских детей хотя бы единожды сталкивались с травлей в интернете. Еще 22 % – чаще. Среди проявлений онлайн-агрессии – разовые негативные комментарии, осуждение действий и внешности, саркастичные высказывания, высмеивание, агрессивное преследование в интернете[1].

[1] Как защитить ребенка от кибербуллинга. URL: https://t-j.ru/cyberbullying/ (дата обращения 04.02.2025).

По данным Всемирной организации здравоохранения, около 20% подростков сталкиваются с кибербуллингом, и это лишь официально зафиксированные случаи. При этом жертвы часто не готовы обращаться за помощью из-за страха осуждения или недоверия к возможности найти эффективную поддержку.

Проявления онлайн-травли могут быть разными по форме, но их последствия всегда серьезны. Разовые негативные комментарии могут перерасти в хроническую травлю, сопровождающуюся агрессивным преследованием в социальных сетях и на форумах. Высмеивание и язвительные высказывания часто направлены на формирующуюся личность ребенка, подрывая его уверенность и самооценку. В этом опасность подобных ситуаций: агрессия не остается ограниченной виртуальным пространством, а переносится в реальную жизнь.

Последствия кибербуллинга могут быть очень серьёзными как для жертвы, так и для непосредственного агрессора, создавая долгосрочные эмоциональные, психологические и социальные проблемы.

Для пострадавших кибербуллинг зачастую приводит к снижению самооценки, тревожным расстройствам, депрессии и чувству бессилия. Когда атакующие сообщения, угрозы или оскорбления распространяются в интернете, жертва может чувствовать себя изолированной и неспособной найти поддержку, учитывая, что цифровое издевательство редко ограничивается только ближайшим окружением, охватывая более широкую аудиторию.

Кроме эмоционального влияния, кибербуллинг может приводить к социальным и академическим последствиям. Жертвы часто начинают избегать социальных взаимодействий, теряют интерес к учебе или работе, испытывают трудности с доверием к другим людям. В некоторых случаях последствия могут быть особенно трагичными, вплоть до суицидальных мыслей или действий.

Те, кто занимается кибербуллингом, тоже могут столкнуться с отрицательными последствиями. Помимо проблем с законом, таких как административная или уголовная ответственность, агрессорам нередко приходится сталкиваться с потерей доверия друзей, семей и работодателей, если их поведение становится известным.

Однако с точки зрения правового регулирования проблема кибербуллинга не решена. Случаи, при которых стоит обращаться в полицию, зависят от того, в рамках какой статьи можно привлечь агрессора к ответственности, а именно возможны следующие варианты:

– оскорбление (статья 5.61 КоАП РФ), предмет статьи «оскорбление, выраженное в неприличной или иной противоречащей общепринятым нормам морали и нравственности форме»;

– клевета (статья 128.1 УК РФ). Для применения этой нормы достаточно разглашения ложных сведений порочащего характера хотя бы одному лицу, помимо потерпевшего;

– нарушение неприкосновенности частной жизни (ст. 137 УК РФ). В части 3 упоминается распространение сведений при помощи информационно-телекоммуникационных сетей;

– доведение до самоубийства. Статьи 110 УК РФ (доведение до самоубийства), 110.1 (склонение или содействие совершению самоубийства) и 110.2 (организация деятельности, направленной на побуждение к совершению самоубийства). Все три предусматривают квалифицированные составы преступления, связанные с использованием интернета.

Судебная практика на тему кибербуллинга в России достаточно скудная. В основном она касается уголовных дел, связанных с самоубийством или побуждением к совершению самоубийства[1].

Важно не оставлять без внимания такие случаи. Родители, педагоги и IT-компании должны объединить усилия для создания среды, где дети смогут чувствовать себя в безопасности. Образовательные программы, направленные на повышение цифровой грамотности, развитие эмпатии и культуры общения онлайн, могут стать важным шагом к решению этой проблемы. Одновременно важно внедрение инструментов модерации и защиты в соцсетях, которые помогли бы предотвращать агрессивное поведение.

Как верно отмечает Л. Кузьмина: «для эффективного противодействия этой проблеме требуется многоуровневый и комплексный подход, включающий образовательные, социальные, правовые и психологические меры. Образовательные программы, направленные на повышение цифровой грамотности подростков, играют ключевую роль в предупреждении кибербуллинга. Школьные учреждения и родители должны обучать подростков ответственному использованию интернета, а также развивать у них навыки критического мышления, самозащиты в виртуальной среде и уважительного отношения к другим пользователям сети»[2].

Не менее важна и роль законодательных мер в борьбе с кибербуллингом. Установление четких правовых норм, направленных на регулирование ответственности за агрессию в интернете, может стать важным шагом на пути к снижению числа подобных инцидентов. Законодательство должно охватывать как превентивные меры, так и эффективные механизмы защиты для жертв, позволяя им отстаивать свои права и получать необходимую поддержку. Это включает в себя разработку регламентов, обязывающих интернет-платформы оперативно реагировать на случаи травли, а также создание условий, при которых пострадавшие могут рассчитывать на полное восстановление справедливости. Одновременно важно проводить разъяснительные кампании, чтобы повысить осведомленность о юридических последствиях кибербуллинга,

[1] Тасбаева А.Н. К вопросу о понятии кибербуллицида в уголовном праве // Трансформация права: Матер. VI Всерос. науч.-практ. форума студентов и молодых ученых, Екатеринбург, 23–27 октября 2023 года. Екатеринбург: Уральский государственный юридический университет им. В.Ф. Яковлева, 2024. С. 355–361.

[2] Кузьмина Л. Кибербуллинг: новые вызовы для общества // Социология и право. 2022. С. 75–81.

формируя у пользователей интернета понимание личной ответственности за собственное поведение в цифровой среде.

Мир интернета создан быть пространством возможностей и развития, а не местом, где человек сталкивается с агрессией и насилием.

Учитывая глобальность проблемы, требуется разработка комплексных решений, включающих законодательные инициативы, образовательные программы и киберэтические нормы. Проблема кибербуллинга – это не только технологический, но и культурный и социальный вызов, требующий междисциплинарного подхода.

Список источников

1. Кузьмина Л. Кибербуллинг: новые вызовы для общества // Социология и право. 2022. С. 75–81.
2. Тасбаева А.Н. К вопросу о понятии кибербуллицида в уголовном праве // Трансформация права: Матер. VI Всерос. науч.-практ. форума студентов и молодых ученых, Екатеринбург, 23–27 октября 2023 года. Екатеринбург: Уральский государственный юридический университет им. В.Ф. Яковлева, 2024. С. 355–361.

Д.А. Мозговая
Военный университет имени князя Александра Невского
Минобороны России

Применение видео-конференц-связи при проведении допроса: анализ научных дискуссий

Аннотация. Автором проанализированы научные работы, в которых рассмотрены организационные, тактические и процессуальные аспекты производства допроса с использованием видео-конференц-связи. Выявлены проблемные вопросы, связанные с эффективностью и целесообразностью проведения допроса в дистанционном формате.

Ключевые слова: допрос, протокол, видео-конференц-связь, следователь, тактика, организация.

Результатом принятия Федерального закона от 30.12.2021 № 501 «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации»[1] явилась возможность дистанционного производства некоторых следственных действий. Можно констатировать, что практические сотрудники долго ждали этого нововведения, поскольку потребности в производстве допроса, а именно это следственное действие наиболее часто проводится с использованием системы видео-конференц-связи (далее – ВКС), возникают все чаще.

[1] Федеральный закон от 30.12.2021 № 501-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // СПС КонсультантПлюс.

В соответствии со статьей 189.1 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) следователь (дознаватель) самостоятельно принимает решение о производстве названных следственных действий с использованием ВКС. Но следует заметить, что ряд вопросов не урегулированы рассматриваемой нормой, некоторые из них носят не только сугубо процессуальный характер, а и криминалистический.

Так, например, в законе нет ссылки на ограничения по проведению дистанционного допроса с отдельными категориями лиц: малолетних, пожилых, страдающих психическими или физическими заболеваниями. Для разрешения этого вопроса, думается, следует обратиться к рекомендациям криминалистической тактики, которые в каждом случае не противоречат нормам уголовно-процессуального закона. Исходя из общих рекомендаций следователю надлежит решать этот вопрос индивидуально, исходя из личных особенностей допрашиваемых, и ключевым в принятии решения будет ответ на вопрос: «Не будет ли допрашиваемый в силу волнения или по состоянию здоровья лишен возможности спокойно, уверенно в ходе свободного рассказа изложить интересующие обстоятельства»?

Законом определен ряд условий, при которых проведенный с использованием ВКС допрос будет отвечать требованиям законности. Первым условием является разъяснение участнику, находящемуся вне места производства предварительного расследования, порядка производства следственного действия (ч. 3 ст. 189.1 УПК). Как нам представляется, следователь должен обстоятельно рассказать о том, как будет проходить общение, какие средства фиксации будут использованы, кто из участников и в какой форме будет оказывать содействие в его производстве.

В связи с возможностью производства допроса в рассматриваемом формате возникает и оправданное опасение. Не будет ли такой допрос использован следователем в целях получения «нужных» показаний. Для обеспечения дополнительной процессуальной гарантии авторы высказывали мнение о необходимости записи экрана компьютера и видеосъёмки помещения с двух точек (для охвата всей площади помещения), что позволит исключить воздействие на участников следственных действий. В дальнейшем такой способ фиксации поспособствует объективной оценке полученной информации и признанию протоколов следственных действий допустимыми доказательствами.

У стороны защиты обеспокоенность вызывает процедура допроса, которая может привести к нарушению прав участников уголовного судопроизводства. Авторы полагают, что при даче свидетелем невыгодных для органа, осуществляющего предварительное расследование показаний, ВКС может быть прервана по «техническим причинам», а после возобновления уже подготовленное лицо даст необходимые стороне обвинения показания.

Тактически верным в таком случае является получение от лица подтверждения о том, что следственное действие было приостановлено не намеренно, а в связи с реальной технической неисправностью и за период перерыва на лицо не

оказывалось физическое или психологическое давление[1].

Такое предложение, считаем, нельзя не поддержать, и его закрепление на уровне тактических рекомендаций будет способствовать объективности и однозначности результатов, а также позволит избежать исключения протокола следственного действия из перечня доказательств. В последующем, разработанные наиболее целесообразные процедуры, порядок, последовательность, алгоритм проведения тех или иных следственных действий воспринимаются законодателем, как носящие обязательный характер, и включаются в качестве нормативного правила в уголовно-процессуальный закон[2].

Очевидным стало то, что процесс внедрения ВКС в уголовное судопроизводство не остановить. Количество допросов, проведенных с использованием ВКС, с каждым годом будет неуклонно расти, что обусловлено необходимостью обеспечения безопасности участников уголовного судопроизводства; ускорением процесса расследования (не в ущерб его качеству); экономии средств.

Важным условием производства допроса с использованием ВКС является наличие технической возможности, под которой подразумевается, что в органах предварительного расследования есть внутренняя связь, специально для этого предназначенная и отвечающая требованиям конфиденциальности, безопасности и сохранности данных предварительного расследования и о лицах, участвующих в проведении данного следственного действия, исключающая несанкционированный доступ к системе любых посторонних лиц[3]. Понятие технической возможности тесно переплетается с требованиями соблюдения информационной безопасности, запрещающими проведение допроса, путем использования системы ВКС в случае возможности разглашения государственной или иной охраняемой федеральным законом тайны либо данных о лице, в отношении которого приняты меры безопасности.

Обеспечение технической возможности производства допроса при соблюдении требований информационной безопасности возможно только при надлежащей организации следственного действия и взаимодействии со специалистом, который контролирует нормальную, бесперебойную работу систем ВКС. Как мы понимаем, качественная работа видео-конференц-связи не всегда зависит от специалиста. Есть несколько составляющих факторов, способных оказать влияние на снижения качества передаваемой информации, вплоть до ее остановки, к их числу относятся: скорость интернет-соединения;

---

[1] Официальный сайт Федеральной Палаты адвокатов Российской Федерации. URL: https://fparf.ru/news/fpa/sledstvennyedeystviya-v-rezhime-vks/ (дата обращения: 07.01.2025).

[2] Центров Е.Е. Парадигма криминалистической тактики и ее основные понятия // Известия тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 139.

[3] Ксендзов Ю.Ю. Тактические особенности проведения допроса посредством видео-конференц-связи // Право и государство: теория и практика. 2023. № 3(219). С. 224.

качество оборудования; программное обеспечение; освещенность кабинета.

Таким образом, на возможность производства допроса с использованием системы видео-конференц-связи влияют несколько объективных и субъективных факторов: достаточная законодательная регламентация; тактико-криминалистические рекомендации по вопросам, не нашедшим отражение в законе; техническое оборудование хорошего качества; высокий уровень подготовки специалистов, оказывающих содействие в проведении допроса; подготовленность следователя.

Позиции ученых-правоведов по вопросу целесообразности производства допроса, путем использование ВКС различна. Так, например, Е.В. Шишкина полагает, что проблемы могут возникнуть в случаях его проведения в условиях конфликтных ситуаций, которые требуют активного тактического воздействия на допрашиваемое лицо, использования тактических приемов и их комбинаций, для эффективности которых большое значение имеет анализ следователем психологических реакций допрашиваемого на поставленные вопросы и предъявленные ему доказательства, а особенности восприятия реакций и поведения человека через экран значительно снижают эти возможности, что соответственно может повлиять на эффективность допроса[1].

М.С. Плетникова и Е.А. Семенов считают, что видео-допрос участников уголовного процесса позволил бы оптимизировать процесс предварительного расследования и в разы сократить его срок. При этом, может возникнуть ряд вопросов со стороны защиты касаемо допустимости доказательств, ввиду низкого качества изображения, отсутствия личного контакта, подозрение относительно воздействия на дистанционно допрашиваемое лицо, а также иных затруднения[2].

Подводя итог, отметим, что в статье 189.1 УПК РФ законодательно установлена возможность производства дистанционного допроса и условия, при которых это следственное действие проводится. Однако дальнейшее его практическое применение требует более детального изучения ввиду наличия некоторой неопределенности, вызывающей обоснованное беспокойство относительно соблюдения прав и свобод участников допроса.

Озабоченность высказывают не только защитники (адвокаты), но и следователи. В рамках дистанционного допроса они не в силах применить те тактические приемы, которые возможно было бы реализовать в очном формате, такой этап как установление психологического контакта с допрашиваемым мало реализуем. Отсюда вытекают проблемы объективности показаний и результативности следственного действия в целом.

---

[1] Шишкина Е.В. Некоторые аспекты проведения следственных действий с использованием видео-конференц-связи // Технологии XXI в. в юриспруденции: матер. IV Междунар. науч.-практ. конф. / отв. ред. Д.А. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В.Ф. Яковлева, 2022. С. 124.

[2] Плетникова М.С., Семенов Е.А. К вопросу использования видео-конференц-связи при производстве допроса // Вестник Уральского юридического института МВД России. 2021. № 1. С. 27.

Список источников

1. Ксендзов Ю.Ю. Тактические особенности проведения допроса посредством видео-конференц-связи // Право и государство: теория и практика. 2023. № 3(219). С. 223–226.
2. Плетникова М.С., Семенов Е.А. К вопросу использования видео-конференц-связи при производстве допроса // Вестник Уральского юридического института МВД России. 2021. № 1. С. 25–28.
3. Центров Е.Е. Парадигма криминалистической тактики и ее основные понятия // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 137–144.
4. Шишкина Е.В. Некоторые аспекты проведения следственных действий с использованием видео-конференцсвязи // Технологии XXI в. в юриспруденции: матер. IV Междунар. науч.-практ. конф. / отв. ред. Д.А. Бахтеев. Екатеринбург: Уральский государственный юридический университет имени В.Ф. Яковлева, 2022. С. 121–128.

И.Н. Озеров
Московская академия Следственного комитета
имени А.Я. Сухарева

Следователь (оперативный сотрудник) в особых условиях – социальный инженер

Аннотация. В данной статье рассматриваются перспективы использования социальной инженерии в противодействии преступности. Рекомендовано расширить применение социальной инженерии в раскрытии и расследовании преступлений для повышения эффективности данного вида деятельности в особых условиях.

Ключевые слова: социальная инженерия; манипуляция; расследование преступлений, оперативно-разыскная деятельность, особые условия.

В XXI в. информационно-телекоммуникационные технологии приобрели глобальный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества. Вместе с тем современное состояние преступности в мире характеризуется устойчивым ростом преступных проявлений, связанных с использованием в противоправной деятельности информационно-телекоммуникационных технологий. При этом виртуальный мир меняет уклад механизмов совершения преступлений различного вида, способствует переходу

от традиционных, простых способов их совершения к более сложным формам[1]. Несмотря на то, что появляются новые методы защиты от дистанционных действий злоумышленников, а также активно вскрываются преступные схемы в информационном пространстве, на противодействие рассматриваемой преступности оказывают влияние постоянное развитие информационных технологий, использование психологических манипуляций и современных программных продуктов. Действительно, внедрение в противоправную деятельность различных программных средств, в том числе технологий искусственного интеллекта, может существенно менять характер преступности, открывать новые криминальные возможности, облегчать достижение целей, совершенствовать способы подготовки и совершения преступлений[2].

В специальной литературе существуют различные определения социальной инженерии, обобщив которые можно констатировать, что она представляет собой приемы обмана и психологического манипулирования людьми в целях осуществления контроля за их поведением или действиями[3].

Социальная инженерия (*social engineering*) или «атака на человека» представляет собой набор манипулятивных психологических и социологических методов, приёмов и технологий, направленных на получение несанкционированного доступа к конфиденциальной информации. Эффективность таких атак часто основана на уязвимостях человеческой психологии, что делает их особенно опасными.

Уровень и возможности социальной инженерии увеличивается с каждым годом, а возникающие особые условия (коронавирус, СВО) способствуют увеличению социальной инженерии. Отдельные ученые, в связи с этим, предлагают ставить под контроль вместе с ещё одной активно развивающейся системой на сегодняшний день – искусственным интеллектом. В связи с чем, обратимся к другому понятию «социальная инженерия», предложенному Фадеевой И. П. «Социальная инженерия – это технологии, которые основаны на анализе больших данных и машинном обучении, именно они позволяют создавать более сложные и адаптивные методы манипуляции с целью

---

[1] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

[2] Старостенко Н.И. Криминалистические особенности способов совершения хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета. Право. 2024. Т. 15, № 1. С. 152.

[3] Резник Ю. Социальная инженерия: предметная область и границы применения // Социологические исследования. М. 1994. С. 87; Ревенков П.В., Бердюгин А.А. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания // Национальные интересы: приоритеты и безопасность. 2017. № 9 (354). С. 1747; Овчинский В. Мафия. Новые мировые тенденции. Коллекция изборского клуба. М.: Книжный мир, 2016. С. 4; Старостенко Н.И. Особенности первоначального этапа расследования дистанционных хищений, совершенных с применением методов социальной инженерии. М.: Юрлитинформ, 2024. С. 168.

получения конфиденциальной информации или доступа к защищённым системам»[1].

Все это ставит перед нами сложные задачи, требуя от научного общества разрабатывать новые подходы к защите информации и повышению цифровой грамотности населения. Важно осознавать, что технологии социальной инженерии могут быть использованы как во благо, так и во вред. Поэтому ставится задача – определить, насколько может быть опасна возможность использования традиционно ассоциируемых методов социальной инженерии с преступностью в социально полезных целях, в том числе для противодействия преступным посягательствам.

Сегодня социальная инженерия приобрела прочную связь с кибермошенничеством, но на самом деле это понятие появилось давно и изначально не имело выраженного негативного оттенка. Она использовалась с древних времён. Так, в Древнем Риме и Греции очень уважали специально подготовленных ораторов, способных убедить собеседника в его «неправоте». Эти люди участвовали в дипломатических переговорах и работали на благо своего государства.

Однако, много лет спустя, к началу 1970-х годов стали появляться телефонные хулиганы, нарушавшие покой граждан просто ради шутки, что приобрело «модное» течение в странах Запада. Позднее, эти бывшие телефонные хулиганы превратились в профессиональных социальных инженеров (их стали называть синжерами), способных мастерски манипулировать людьми, по одной лишь интонации определяя их комплексы и страхи.

Когда появился интернет, большинство синженеров сменило профиль, став социальными хакерами, а понятия «социальная инженерия» и «социальные хакеры» стали синонимичны.

Однако вернемся к социальной инженерии, используемой во благо, и применительно к теме нашего исследования – социальным инженерам в правоохранительной сфере. Иллюстрацию того, на что способен умелый социальный инженер в правоохранительной сфере можно найти и в истории российского сыска. Знаменитый сыщик второй половины XIX столетия И.Д. Путилин. Имя И.Д. Путилина известно массовому читателю с конца XIX в., чему в немалой степени способствовали литературные труды самого Ивана Дмитриевича. Его перу принадлежит биографическая книга «Сорок лет среди грабителей и убийц», которая послужила основой для широкого круга сочинений других авторов. Это произведения детективного жанра, представляющие собой рассказы о резонансных преступлениях, совершенных в

[1] Фадеева И.П. Использование систем искусственного интеллекта в области социальной инженерии // Искусственный интеллект в решении актуальных социальных и экономических проблем XXI века: Сб. статей по матер. Девятой всерос. науч.-практ. конф. с междунар. участием, Пермь, 17-18 октября 2024 года. Пермь: Пермский государственный национальный исследовательский университет, 2024. С. 100.

российской столице в 1850–1880-е гг. и раскрытых при его активном участии[1]. Характеризуя профессиональные качества И.Д. Путилина как умелого следователя-социального инженера, можно определить диапазон использованных им методов и приемов, названных бы сегодня социальной инженерией.

Результаты его работы, получившие отражение в архивных документах, и обобщенные в работах современных исследователей, таких как Федотова И.Н., позволяют сделать, по крайней мере, два важных вывода. «Во-первых, Путилин с одинаковым успехом проводил розыск по делам о преступлениях самой различной направленности, таких как: кражи, грабежи, разбои, убийства, похищение человека, мошенничество, фальшивомонетничество и др. Иными словами, приобретенные Путилиным навыки оперативно-разыскной деятельности носили универсальный характер. Во-вторых, среди этих преступлений значительную часть составляли совершенные на профессиональной основе, т. е. опытными преступниками, за которыми стояли организованные криминальные группировки. Следовательно, работа над такого рода уголовными делами отличалась особой сложностью и повышенной опасностью»[2]. Резюмируя последний тезис, можно говорить о необходимости применения методов социальной инженерии следователем в особых условиях, о которых мы ранее писали и обосновывали необходимость их применения.

Лучше всего о деловых качествах Путилина могли судить люди, непосредственно наблюдавшие за его работой. Одним из них был выдающийся российский правовед и государственный деятель Анатолий Фёдорович Кони, который тесно контактировал с И.Д. Путилиным в 1870-е гг., когда служил в Санкт-Петербургском окружном суде, занимая должности прокурора, а в дальнейшем – председателя. Характеризуя И.Д Путилина как уникальную личность, А.Ф. Кони отмечает: «По природе своей Путилин был чрезвычайно даровит и как бы создан для своей должности. Необыкновенно тонкое внимание и чрезвычайная наблюдательность, в которой было какое-то особое чутье, заставлявшее его вглядываться в то, мимо чего все проходили безучастно, соединялись в нем со спокойной сдержанностью, большим юмором и своеобразным лукавым добродушием… Он умел отлично рассказывать и еще лучше вызывать других на разговор и писал недурно и складно… К этому присоединялась крайняя находчивость в затруднительных случаях… В Петербурге… не было ни одного большого и сложного уголовного дела, в розыск по которому Путилин не вложил бы своего труда»[3].

Всё эти реальные примеры социальной инженерии говорят о том, что она легко адаптируется к любым условиям и к любой обстановке. Играя на личных

---

[1] Федотова И.Н., Запольский В.А. Российская сыскная полиция в портретах ее выдающихся деятелей: Иван Дмитриевич Путилин // Пенитенциарное право: юридическая теория и правоприменительная практика. 2020. № 3 (25). С. 131.

[2] Там же. С. 127.

[3] Кони А.Ф. Избранное / сост.: Г.М. Миронов, Л.Г. Миронов. М.: Совет. Россия, 1989. С. 43.

качествах человека или отсутствии профессиональных (недостаток знаний, игнорирование инструкций и так далее), следователь легко подберёт ключи к любому преступнику, разговорит любого свидетеля, поможет по крупицам восстановить цепь происшедшего потерпевшему.

Например, методы обратной социальной инженерии позволяют выявлять латентные преступления, когда потерпевший не совсем хочет, чтобы кто-либо узнал о произошедшим с ним, а задача следователя в ходе допроса или процессуальной проверки по сообщению о преступлении – использовать данный метод, направленный на то, чтобы жертва сама обратилась к социальному инженеру и выдала следователю необходимые данные. Этот же метод может быть применен при побуждении к явке с повинной.

Значимых успехов Путилин добился в использовании такого метода социальной инженерии, как «использование псевдонимов и прикрытий», а также «психологическое воздействие и манипуляция эмоциями». Как отмечает Л.И. Беляева, «Суть его состояла в том, что Иван Дмитриевич и другие его подчиненные сотрудники под видом других людей посещали места скопления криминального элемента и собирали необходимые сведения о преступниках. Судя по сохранившимся свидетельствам, это давалось Путилину значительно легче, чем его коллегам. В определенной мере этому способствовал врожденный артистизм, но главную роль, безусловно, играли приобретенные на практике глубокие знания об уголовном мире. К изучению криминального «дна» Санкт-Петербурга Путилин проявлял огромный интерес с самого начала своей службы. В свободное время он переодевался чернорабочим или бродягой и отправлялся на постоялые дворы, в ночлежные дома, питейные заведения, ломбарды. В таких местах можно было не только получить представление об обычаях и нравах преступного сообщества, но и освоить воровской жаргон. В дальнейшем это позволило Путилину свободно ориентироваться в криминальной среде и перевоплощаться настолько мастерски, что его не узнавали ни сослуживцы, ни уголовники, хорошо знавшие его в лицо»[1].

«Не знакомые с нашими приемами люди, – отмечал он, – часто приписывают все наши открытия случайности… Действительно, нам всегда помогает случай, но дело в том, что мы гоняемся за ним и в долгих неустанных поисках, наконец, натыкаемся на него. Мы знаем места, темные, трущобные места, где могут проговориться и дать хоть косвенные указания; мы знаем места, где разыскиваемый может ненароком попасться, и в этих местах беспрерывно дежурим, часто с опасностью для жизни, напрягая и слух, и зрение»[2].

Пиотровский В.Ю., Кудрявцев Д.В., Очкур Р.В., в работе «Полиция Российской империи», отмечают, что «благодаря искусству перевоплощения Путилину удавалось непосредственно проникать в преступные группировки. Так было, например, во время расследования дела «душителей» – банды,

---

[1] Пиотровский В.Ю., Кудрявцев Д.В., Очкур Р.В. Полиция Российской империи. М.: АСТ; СПб.: Астрель-СПб., 2005. С. 60.

[2] Нечевин Д.К., Беляева Л.И. Шеф сыскной полиции Санкт-Петербурга Иван Дмитриевич Путилин: в 2 т. М.: Олма-Пресс, 2003. Т. 1. С. 46.

нападавшей на столичных извозчиков с целью грабежа. Для того чтобы выйти на след преступников, Иван Дмитриевич принял облик бродяги: надел рваную одежду, обул калоши на босу ногу и загримировался, изобразив на лице синяки. В таком виде он отправился на городскую окраину, где, по его предположению, банда могла найти себе пристанище, и попросился в один из домов на ночлег. Ничего не заподозрившие хозяева приняли его, и, подслушав их разговор, сыщик выяснил, что они связаны с разыскиваемыми преступниками и сбывают награбленное. За счет безупречно сыгранной роли Путилин не просто обеспечил себе легендированное прикрытие, но и сумел войти в доверие к скупщикам краденого. Его вымышленный образ был, во-первых, вполне правдоподобен, а во-вторых, психологически рассчитан на то, чтобы произвести благоприятное впечатление на хозяев дома. В конечном итоге сыщик добился того, что они сами предложили постояльцу участвовать в их криминальном промысле. Воспользовавшись предложением, Путилин через несколько дней снова посетил воровской притон, чтобы уточнить детали, необходимые для задержания преступников. Вскоре банда была ликвидирована с помощью засады, устроенной у дома скупщиков краденого»[1].

Изучение дела «душителей» показывает, что этот метод, как известно, предполагает легендированное включение социального инженера в криминальную группировку с целью получения максимально полной информации о ней. Обращает на себя внимание тот факт, что к середине XIX в., когда Иван Дмитриевич начинал свою профессиональную деятельность, опытом оперативного внедрения органы правопорядка еще не располагали. Иными словами, в этой области Путилина можно считать одним из первооткрывателей[2]. То же самое касается использования другого метода социальной инженерии, связанного с провокацией. К числу наиболее ярких примеров апробации данного метода в практике Путилина относится описанный в ранее указанной работе «задержание известной на всю страну опасной преступницы по прозвищу Сонька Золотая Ручка, которую полиция безуспешно разыскивала долгие годы. Путилин избрал нестандартный способ решения задачи: он сел в поезд под именем барона Ротшильда, заблаговременно позаботившись о том, чтобы Соньке стало известно о богатом пассажире. Не сумев узнать в «Ротшильде» сыщика Путилина, Сонька села в тот же самый вагон с целью отравить своего попутчика и совершить ограбление, но вовремя была задержана. Сущность реализованного Иваном Дмитриевичем замысла состояла в негласном искусственном создании условий, побуждающих преступника к проявлению его противоправных намерений»[3]. Это дает основание рассматривать поимку

---

[1] Нечевин Д.К., Беляева Л И. Шеф сыскной полиции Санкт-Петербурга Иван Дмитриевич Путилин: в 2 т. М.: Олма-Пресс, 2003. Т. 2. С. 50–79.

[2] Ковалев О.Г. Оперативно-розыскная деятельность: историко-правовой и психологический анализ. Владимир: ВЮИ Минюста России, 2003. С. 53–54.

[3] Нечевин Д.К., Беляева Л.И. Шеф сыскной полиции Санкт-Петербурга Иван Дмитриевич Путилин: в 2 т. М.: Олма-Пресс, 2003. Т. 2. С. 340–361.

Соньки Золотой Ручки в качестве успешно проведенного метода социальной инженерии.

Возвращаясь к заявленному предмету нашего исследования, необходимо отметить, что особые условия неизменно становятся серьезным испытанием для общества, государственных структур и системы правопорядка. В условиях кризиса привычные механизмы управления зачастую оказываются недостаточно эффективными, а поведение людей приобретает стихийный и непредсказуемый характер. В такие моменты важно не только обеспечивать физическую безопасность граждан и оперативно реагировать на угрозы, но и грамотно проводить действия по охране правопорядка, раскрытию и расследованию преступлений, в том числе и с использованием информационно-коммуникационных технологий.

Резюмируя вышесказанное, следует отметить, что целесообразно проводить комплекс оперативно-разыскных мероприятий и следственных действий в плоскости сетевого информационного пространства, а именно: проведение оперативно-разыскного мониторинга, который направлен на сбор, обработку и анализ информации о криминальных проявлениях в виртуальной среде; осуществление информационной разведки как в открытых источниках (OSINT), так и в закрытых, которая в отличие от мониторинга в первую очередь направлена на поиск оперативно значимой информации в киберпространстве; комплекс ОРМ, включающий в себя: «Наведение справок»; «Сбор образцов для сравнительного исследования»; «Исследование предметов и документов»; «Отождествление личности»; «Контроль почтовых отправлений, телеграфных и иных сообщений»; «Прослушивание телефонных переговоров»; «Снятие информации с технических каналов связи»; «Оперативное внедрение»; «Оперативный эксперимент», первоначальные следственные действия.

Все это позволит оперативным и следственным подразделениям добывать информацию о лицах, готовящих или совершающих подобные преступления.

Список источников

1. Андриевский А.И. Социальная инженерия как угроза информационной безопасности / А.И. Андриевский, А.В. Иванов // Поиск (Волгоград). 2022. № 2(13). С. 132–135.
2. Ковалев О.Г. Оперативно-разыскная деятельность: историко-правовой и психологический анализ. Владимир: ВЮИ Минюста России, 2003. 192 с.
3. Кони А.Ф. Избранное / сост.: Г.М. Миронов, Л.Г. Миронов. М.: Совет. Россия, 1989. С. 43–44.
4. Овчинский В. Мафия. Новые мировые тенденции. Коллекция изборского клуба. М.: Книжный мир, 2016. 391 с.
5. Пиотровский В.Ю., Кудрявцев Д.В., Очкур Р.В. Полиция Российской империи. М.: АСТ; СПб.: Астрель-СПб. 2005. 270 с.
6. Ревенков, П.В., Бердюгин А.А. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания // Национальные интересы: приоритеты и безопасность. 2017. № 9 (354). С. 1747–1760.

7. Резник Ю. Социальная инженерия: предметная область и границы применения // Социологические исследования. М., 1994. С. 87–96.
8. Старостенко Н.И. Криминалистические особенности способов совершения хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета. Право. 2024. Т. 15, № 1. С. 152–170.
9. Старостенко Н.И. Особенности первоначального этапа расследования дистанционных хищений, совершенных с применением методов социальной инженерии. М.: Юрлитинформ, 2024. 168 с.
10. Фадеева И.П., Смолькин В.П. Использование систем искусственного интеллекта в области социальной инженерии // Искусственный интеллект в решении актуальных социальных и экономических проблем XXI века: Сб. статей по матер. Девятой всерос. науч.-практ. конф. с междунар. участием, Пермь, 17–18 октября 2024 года. Пермь: Пермский государственный национальный исследовательский университет, 2024. С. 100–103.
11. Федотова И.Н., Запольский В.А. Российская сыскная полиция в портретах ее выдающихся деятелей: Иван Дмитриевич Путилин // Пенитенциарное право: юридическая теория и правоприменительная практика. 2020. № 3 (25). С. 126–132.
12. Шеф сыскной полиции Санкт-Петербурга Иван Дмитриевич Путилин: в 2 т. / авт.-сост.: Д.К. Нечевин, Л.И. Беляева. М.: Олма-Пресс, 2003. Т. 1. 479 с.; Т. 2. 607 с.

К.И. Озеров
Межрегиональный открытый социальный институт

Некоторые вопросы противодействия мошенничествам, совершаемым с использованием информационно-телекоммуникационных технологий

Аннотация. Практическая направленность данной статьи позволяет уточнить существующие проблемы, возникающие при выявлении и раскрытии мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий, а также механизм получения и предоставления доказательственной базы, добытой в процессе раскрытия рассматриваемых преступлений. Кроме того, пересмотрены некоторые устоявшиеся понятия прежних взглядов и подходов в сфере противодействия мошенничествам с использованием сети Интернет, что имеет функциональное значение в части совершенствования мер по нейтрализации использования преступниками информационно-телекоммуникационных технологий.

Ключевые слова: документирование, информационно-телекоммуникационные технологии, информация, киберпреступления, расследование преступлений, оперативно-разыскная деятельность, оперативно-разыскная информация.

Быстрый темп развития информационно-телекоммуникационных технологий (далее – ИТТ), а также сложность освоения совершенствующегося программного обеспечения органами, осуществляющими раскрытие и расследование преступлений, позволяют активизировать преступную деятельность, связанную с мошенническими действиями в отношении рядовых граждан страны.

Ежегодно прослеживается динамика увеличения количества мошеннических действий, совершаемых с использованием ИТТ (ст. 159, 159.3, 159.6 УК РФ), что говорит о стабильной негативной тенденции, при этом процент раскрываемости остается на низком уровне. За последние семь лет (2018–2024) количество указанных преступлений увеличилось в восемь раз, а их средняя раскрываемость составила 10,7%.

Тенденция сильного всплеска рассматриваемой преступности прослеживается с 2018 г., но особенно количество мошеннических действий увеличилось во время пандемии Covid-19. За этот период выросло число пользователей интернет-сети, многие потеряли работу, чем воспользовались мошенники, усовершенствовав старые способы преступных действий и разработав новые. Столь широкомасштабное и скоротечное развитие ИТТ непосредственно влияет на общественную жизнь и государство как в негативном, так и в позитивном ключе. Поэтому, чтобы бороться и не допускать разрастания негативных проявлений со стороны мошенников в сфере IT-технологий, следует уделить большое внимание мерам профилактики, а также вносить изменения в практическую работу оперативных сотрудников органов внутренних дел, занимающихся противодействием указанной преступности.

В организации деятельности оперативно-разыскных подразделений органов внутренних дел по выявлению, документированию и раскрытию мошеннических действий, совершаемых с использованием ИТТ, помимо общих тенденций увеличения количества рассматриваемых преступлений, отмечаются проблемы, не позволяющие активнее влиять их на раскрытие: неосведомленность оперативных сотрудников о новых способах или специфических особенностях мошеннических действий в сфере ИТТ; нехватка кадров, имеющих образование в IT-сфере; недостаточное оснащение оперативных подразделений компьютерными устройствами с расширенными функциональными возможностями; недостаточно эффективное взаимодействие с населением, что не позволяет своевременно получать информацию по мошенническим действиям в сфере ИТТ, и прочее[1].

Вышеуказанное обуславливает разработку вопросов по совершенствованию способов выявления и раскрытия мошенничеств с использованием ИТТ; разработку алгоритмов действий для сотрудников органов внутренних дел по использованию программного обеспечения, направленного на противодействие мошенническим действиям в сфере ИТТ, и дополнительных мер противодействия новым способам совершения мошеннических действий с

[1] Тимофеев С.В., Абидов Р.Р. Проблемы противодействия киберпреступности: вопросы теории и практики // Вестник Восточно-Сибирского института МВД России. 2024. № 1 (108). С. 299.

применением ИТТ; совершенствование оперативно-разыскной тактики в части проведения оперативно-разыскных и оперативно-технических мероприятий по выявлению и раскрытию мошенничеств и методики использования высоких технологий в процессе их раскрытия.

Оперативно-разыскное законодательство объектами оперативно-разыскной деятельности в первую очередь считает защиту граждан от преступных посягательств путем осуществления гласно либо негласно оперативно-разыскных мероприятий, используя различные оперативно-технические средства. С учетом этого отмечается практическая потребность в разработке методики выявления и раскрытия мошенничеств в виртуальном пространстве с использованием современных технических средств. Одновременно, одной из серьезных угроз современному обществу являются киберпреступность и широкое использование криптовалюты в процессе совершения мошеннических действий, связанных с информационными технологиями.

Информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов.

Понятие «информация» регламентируется законодательством на федеральном уровне, являясь достаточно широким и общим, что дает право ученым использовать представленную дефиницию в самых различных ее проявлениях.

Широкое по смыслу понятие «информация» не создает трудностей, ведь при изучении ИТТ следует определить все лексические аспекты, входящие в состав представленной аббревиатуры, в целях полноценного понимания, проведения анализа, а также изложения своего мнения, касающегося тенденции развития и видоизменения сферы ИТТ.

Термин «информационные технологии» впервые в своих научных трудах использовал американский ученый Сидни Л. Пресси в 1926 г. Спустя годы использование понятия «информационные технологии» вошло в терминологический оборот СССР, где информационные технологии стали процессами по переработке информационных потоков. Также, по мнению ученых, информационная технология понималась как система средств и методов, с помощью которых осуществляется процесс переработки информационного ресурса.

В более современных трактовках понятийного аппарата, который касается информационно-технологической индустрии, следует отметить научно-исследовательские работы В.В. Зозули, который определяет в них понятие «информационно-телекоммуникационные технологии» как обобщающее, характеризующее различные методы, способы и алгоритмы сбора, хранения, обработки, представления и передачи информации.

Существуют различия в терминологии, представленной в законодательстве Российской Федерации, где определяются «информационные технологии». В Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ закреплено определение понятия «информационно-телекоммуникационная сеть» как технологической

системы, предназначенной для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[1].

В свою очередь, в Указе Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» принимается за основу понятие «информационная безопасность»[2], а также используется дефиниция «информационно-телекоммуникационная сеть» наряду с Интернетом. В данной Доктрине упоминается об информационно-телекоммуникационных технологиях, что говорит о целесообразности использования указанного понятия при упоминании функционирования интернет-сети. Полагается, что дефиниция «информационно-телекоммуникационные технологии» должна использоваться при связи с интернет-пространством.

В Указе Президента Российской Федерации от 12 марта 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» используется понятие «информационно-коммуникационные технологии», в связи с чем затрагивается проблематика в отношении технологий, имеющих функционал по обмену информацией на дальних расстояниях.

С учетом анализа и сравнения терминов «информационные технологии», «информационно-коммуникационные» и «информационно-телекоммуникационные сети», закрепленных на законодательном уровне, следует рассмотреть еще одно понятие, которое не регламентируется законодательством России, – «информационно-телекоммуникационные технологии».

Так, аббревиатура «IT-технологии», в расшифрованной вариации – Information technology (перевод с англ. – информационные технологии), в печатных изданиях, новостных лентах и научных публикациях используется как синоним категории «информационно-телекоммуникационные технологии». Отсюда усматривается тождество приведенных выше понятий.

Преступления в сфере ИТТ набирают обороты в качественном и количественном эквивалентах, что обуславливает создание необходимой правовой основы, определяющей и регулирующей складывающиеся общественные отношения в области обеспечения информационной безопасности.

Существует Конвенция ООН об обеспечении международной информационной безопасности (концепция), целью которой является

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (в послед. ред.) // Российская газета. 2006. 29 июля; Российская газета. 2023. 18 декабря.

[2] Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 декабря 2016 № 646 // СЗ РФ. 2016. 12 декабря. № 50. Ст. 7074.

противодействие использованию ИТТ для нарушения международного мира и безопасности, которой закрепляется понятийный аппарат[1].

Разработанная концепция Конвенции содержит основную терминологию, связанную с ИТТ. Несмотря на это, понятия «информационные технологии» и «информационно-телекоммуникационные технологии» в представленном юридическом документе отсутствуют, а закрепляется термин «информационно-коммуникационные технологии», которые выражаются в совокупности методов, производственных процессов и программно-технических интеграций с целью формирования, преобразования, передачи, использования и хранения информации[2].

В данном случае усматриваются расхождения в терминологическом выражении между дефинициями «информационно-телекоммуникационные технологии» и «информационно-коммуникационные технологии». В толковом словаре русского языка под авторством Т.Ф. Ефремовой усматривается отличие слов «коммуникационный» и «телекоммуникационный», которое состоит лишь в возможной отправке информации в виде сообщений или иными способами на дальние расстояния[3]. В связи с этим считаем использование термина «информационно-коммуникационные технологии» в Конвенции нецелесообразным, так как в сфере информационных технологий присутствует достаточный объем функциональных возможностей, который позволяет обмениваться информацией между пользователями на дальних расстояниях.

Проанализировав понятийный аппарат и сущность информационно-телекоммуникационного пространства через призму юридической науки, следует отметить, что мошеннические действия на современном этапе развития совершаются при помощи ИТТ, где технологиями могут выступать как процессы в информационной среде, так и аппаратно-технические средства. Ведь злоумышленники совершают подобные преступные деяния посредством взаимной передачи информационных потоков с потерпевшим лицом на дальних расстояниях (мобильная связь, интернет-сеть и др.).

Резюмируя вышесказанное, приходим к выводу, что понятие «информационные технологии» шире, чем «информационно-телекоммуникационные технологии». Они зачастую используются в виде синонимических дефиниций, но важно учесть, что при выделении специфических особенностей телекоммуникационных средств или процессов следует употреблять второе, более узкое по своему смысловому содержанию.

---

[1] О концепции конвенции ООН по международной информационной безопасности от 15.05.2023. URL: https://www.mid.ru/ru/foreign_policy/news/1870609.

[2] Хромов И.Л. Мошенничество с использованием информационно телекоммуникационных технологий (оперативно-розыскная деятельность, криминологический анализ, противодействие): монография. М.: Юриспруденция, 2024. С. 9.

[3] Новый словарь русского языка. Толково-словообразовательный: [В 2 т.] / Т.Ф. Ефремова. М.: Рус. яз., 2000. Библиотека словарей русского языка: А. Т.2: П-Я. Т.2. С. 98.

Поэтому применение термина «информационно-коммуникационные технологии» в научной литературе и на законодательном уровне следует ограничить, ибо в настоящее время все технические процессы и средства перешли на телекоммуникационную специфику функционирования, что дает возможность обмениваться информационными данными на дальних расстояниях.

Рассматривая вопросы, касающиеся процесса документирования в оперативно-разыскной деятельности, что является важнейшим элементом при выявлении, раскрытии и расследовании преступлений технологической направленности, следует подчеркнуть, что термин «документирование» непосредственно связан с собиранием, фиксацией, систематизацией, проверкой и оценкой оперативно значимой информации.

В ст. 10 Федерального закона «Об оперативно-разыскной деятельности»[1] закрепляются основы информационного обеспечения и оперативно-разыскной деятельности, где главными документами, в которых хранится оперативно значимая информация, являются дела оперативного учета.

Исходя из указанной нормы, под документированием понимаются осуществляемый по делам оперативного учета процесс собирания, систематизации сведений, проверки и оценки результатов оперативно-разыскной деятельности, а также принятие на их основе соответствующих решений. Однако документирование как познавательный процесс сбора проверки, оценки и использования фактических данных осуществляется на практике не только по делам оперативного учета. Он имеет место при добывании информации, необходимой для решения любых задач оперативно-разыскной деятельности.

Теория документирования, как составная часть науки оперативно-разыскной деятельности, наряду с исследованием закономерностей познания, осуществляемого в процессе оперативно-разыскной деятельности, занимается изучением норм права, регулирующих порядок документирования, применением этих норм на практике, а также возникающих в этой связи правоотношений между участниками документирования[2].

Таким образом, документирование как средство получения оперативно значимой информации с целью обеспечения возможности идентифицировать отраженную в документах информацию составляет основу доказывания в уголовном судопроизводстве[3].

---

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ (в посл. ред.) // СЗ РФ. 1995. 14 августа. № 33. Ст. 3349; СЗ РФ. 2023. 2 января. № 1 (ч. 1). Ст. 85.

[2] Вагин О.А. и др. Теория оперативно-разыскной деятельности: учебник. 2-е изд., доп. и перераб. / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. М.: ИНФРА-М, 2012. С. 79.

[3] Хромов И.Л. Мошенничество с использованием информационно-телекоммуникационных технологий (оперативно-розыскная деятельность, криминологический анализ, противодействие): монография. М.: Юриспруденция, 2024. С. 11.

При изучении документирования следует обратиться к ведущим авторам, которые внесли большой вклад во всю теорию оперативно-разыскной деятельности. Так, К.К. Горяинов, В.С. Овчинский, Г.К. Синилов, А.Ю. Шумилов под документированием понимают[1]:

а) процесс познания, то есть собирания (выявления), изучения (проверки), оценки и фиксации в документах фактических данных об обстоятельствах совершенного преступления;

б) деятельность, обеспечивающую возможность использования полученных оперативно-разыскным путем данных (материалов) в уголовном судопроизводстве.

Также А.Ю. Шумилов разграничивает понятия «документирование» и «оперативно-разыскное документирование», под которым понимает часть документационной деятельности, заключающейся в процессе собирания, систематизации и фиксации сведений, проверки и оценки результатов оперативно-разыскной деятельности, а также принятия на их основе решения оперативно-разыскным органом (оперативным сотрудником), которая находит воплощение в составлении документа[2].

Овчинский В.С. считает, что документирование является разновидностью процесса практического познания действительности, которое основано на том, что действия человека, в том числе и противоправные, могут становиться причиной изменений в окружающей среде. При этом фиксация такой информации имеет определенную специфику[3].

Ученые А.А. Фальченко и Е.М. Рябков под документированием в сфере оперативно-разыскной деятельности признают процесс получения и закрепления фактических данных о преступных деяниях разрабатываемых лиц[4].

А.Б. Свистильников и К.Х. Солиев отмечают важность документирования в части дополнительного сбора и выявления информации, иных фактических данных, которые могут использоваться в дальнейшем в рамках уголовного судопроизводства. То есть авторы предполагают, что документирование является вспомогательным звеном при собирании информации о факте совершенного противозаконного деяния[5].

Подводя итог, отметим, что документирование преступной деятельности начинается с поиска первичной информации. При этом необходимо учитывать,

---

[1] Вагин О.А. и др. Теория оперативно-разыскной деятельности: учебник. 2-е изд., доп. и перераб. / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. М.: ИНФРА-М, 2012. С. 79.

[2] Шумилов А.Ю. Курс основ оперативно-розыскной деятельности: учебник для вузов. 3-е изд., доп. и перераб. М.: Издательский дом Шумиловой И.И. 2008. С. 129.

[3] Овчинский В.С. Основы борьбы с киберпреступностью и кибертерроризмом. М.: Норма, 2017. С. 92.

[4] Фальченко А.А., Рябков Е.М. Основы оперативно-розыскной деятельности в органах внутренних дел: курс лекций. Н. Новгород, 1998. С. 97.

[5] Свистильников А.Б., Солиев К.Х. Совершенствование методики документирования преступлений: проблемы и пути решения // Труды Академии МВД Республики Таджикистан. № 1 (45). 2020. С. 69.

что имеется ряд причин, подчеркивающих необходимость поиска электронной информации в сети Интернет. Она содержит признаки преступления или сведения, позволяющие установить обстоятельства совершенного преступления. Специфика электронной информации состоит в том, что она может быть уничтожена, прежде чем получит процессуальное закрепление. При этом уничтожение информации легко выполняется не только при физическом контакте, но и на расстоянии.

Основными объектами документирования в данном случае становятся лица и обстоятельства, являющиеся важными элементами доказательственной базы по конкретному уголовному делу. Но при документировании преступлений мошеннического характера в сфере ИТТ возникает проблема, связанная с установлением лиц, имеющих отношение к совершенному преступному деянию, по причине высокой степени анонимизации в сети Интернет.

Список источников

1. Вагин О.А. и др. Теория оперативно-разыскной деятельности: учебник. 2-е изд., доп. и перераб. / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. М.: ИНФРА-М, 2012. 688 с.
2. Новый словарь русского языка. Толково-словообразовательный: [В 2 т.] / Т.Ф. Ефремова. М.: Рус. яз., 2000. Библиотека словарей русского языка: А. Т. 2: П–Я. Т. 2. 1084 с.
3. О концепции конвенции ООН по международной информационной безопасности от 15.05.2023. URL: https://www.mid.ru/ru/foreign_policy/news/1870609.
4. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (в послед. ред.) // Российская газета. 2006. 29 июля; Российская газета. 2023. 18 декабря.
5. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ (в посл. ред.) // СЗ РФ. 1995. – 14 августа. – № 33. Ст. 3349; СЗ РФ. 2023.2 января. № 1 (ч.1). Ст. 85.
6. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 декабря 2016 № 646 // СЗ РФ. 2016. 12 декабря. № 50. Ст. 7074.
7. Овчинский В.С. Основы борьбы с киберпреступностью и кибертерроризмом. М.: Норма, 2017. С. 92–105.
8. Свистильников А.Б., Солиев К.Х. Совершенствование методики документирования преступлений: проблемы и пути решения // Труды Академии МВД Республики Таджикистан. 2020. № 1 (45). С. 69–76.
9. Тимофеев С.В., Абидов Р.Р. Проблемы противодействия киберпреступности: вопросы теории и практики // Вестник Восточно-Сибирского института МВД России. 2024. № 1 (108). С. 292–300.
10. Фальченко А.А., Рябков Е.М. Основы оперативно-разыскной деятельности в органах внутренних дел: курс лекций / А.А. Фальченко, Е.М. Рябков. Н. Новгород, 1998. 185 с.

11. Хромов И.Л., Озеров К.И. Мошенничество с использованием информационно-телекоммуникационных технологий (оперативно-разыскная деятельность, криминологический анализ, противодействие): монография. М.: Юриспруденция, 2024. 28 с.
12. Шумилов А.Ю. Курс основ оперативно-разыскной деятельности: учебник для вузов. – 3-е изд., доп. и перераб. – М.: Издательский дом Шумиловой И.И. 2008. 368 с.

П.С. Порываева[1], **Е.С. Доков**[2]
[1,2] Волгоградская академия МВД России

3D-моделирование как инновационный метод фиксации при производстве осмотра места происшествия

Аннотация. В данной статье рассматриваются возможности применения 3D технологий, как метода фиксации при производстве осмотра места происшествия. Обозначены основные преимущества и недостатки методов 3D-моделирования (фотограмметрии и лазерного сканирования), а также описаны общие алгоритмы их работы.

Ключевые слова: 3D-технологии, 3D-сканирование, 3D-моделирование, программное обеспечение, осмотр места происшествия.

На сегодняшний день небезызвестным является факт активной интеграции компьютерных и цифровых технологий в научную и практическую среду криминалистики. Для криминалистики во все временные этапы главной задачей является получение достоверной информации о совершенном преступлении. Осмотр места происшествия относится к группе первоначальных следственных действий и обладает высокой доказательственной значимостью. А.А. Круглова относит данное следственное действие к важному средству получения информации о расследуемом преступлении[1]. Применение технических средств, фотоаппарата, видеокамеры и иного оборудования не всегда позволяет зафиксировать материально-вещную обстановку на месте происшествия достаточно качественно и объективно. В этой связи внедрение 3D-технологий в криминалистику является инновационным решением.

В общем смысле, 3D-моделирование – это процесс создания графических объектов и сцен в трёхмерном пространстве с помощью специального программного обеспечения. 3D-моделирование при производстве осмотра места происшествия – это совокупность приемов и способов воссоздания трёхмерной

[1] Круглова А.А. Осмотр места происшествия по делам о грабежах и разбойных нападениях // Вестник Восточно-Сибирского института МВД России. 2014. №. 1 (68). С. 41–45.

картины места происшествия с предметами материально-вещной обстановки и обнаруженными следами.

Преимуществами применения 3D-моделирования в криминалистике, в частности при осмотре места происшествия, являются: точность (тщательная детализация каждого объекта), возможность визуализации в реальных условиях (например, погодных), минимизация временных затрат при создании 3D-моделей[1]. При наличии специального технического оборудования – 3D-сканеров, у специалиста-криминалиста появляется возможность фиксации обстановки на месте происшествия и следов, с исключением вероятности их случайного уничтожения. К примеру, при обнаружении объемного следа подошвенной части обуви на снегу, целесообразно применение фиксации и изъятие данного следа посредством раствора гипса и ледяной воды, но, следует отметить, что при недостаточном опыте специалиста, или неправильной технологии замешивания раствора и самой фиксации следа, он может быть утрачен. В этой связи применение метода 3D-моделирования позволяет избежать подобного рода трудности.

Для производства осмотра места происшествия целесообразно использовать два основных метода 3D-моделирования: фотограмметрии и метода лазерного сканирования. Рассмотрим данные методы, их преимущества и недостатки. Метод фотограмметрии заключается в построении 3D-моделей на основе анализа множества фотографий моделируемого объекта, произведенных с разных ракурсов, и имеющих общие точки состыковки изображений. Посредством данного метода возможно получить 3D-модели конкретных объектов, помещений и открытых участков местности.

При осмотре места происшествия на открытых участках местности, целесообразно применение видеосъемки с беспилотных летательных аппаратов (далее БПЛА) – аэрофотосъемки. Применением БПЛА на месте происшествия, может быть зафиксирована обстановка не только в области события преступления, а также окружающая обстановка, с целью последующего её исследования посредством воссозданной 3D-модели, при этом сценарий съемки зависит от объекта (лесной массив, отдельно стоящее здание, памятник и т.п.). При аэрофотосъемке лесных участков местности необходимо придерживаться следующих правил: аэрофотосъемка не должна быть ниже 300 метров над земле ввиду того, что деревья движутся при порывах ветра, и при съемке с небольшой высоты не удастся найти общих точек на снимках. По этой же причине воздушная съемка не должна проводиться в безлистный сезон, так как деревья

[1] Мельников Н.М. и др. Внедрение технологий 3D-моделирования в криминалистике с учетом дополненной реальности при изучении учебной дисциплины «Специальная техника органов внутренних дел» // Управление образованием: теория и практика. 2024. Т. 14. № 4-2. С. 100–112.

без листьев имеют много тонких структур (веток) тем самым осложняя воссоздание трехмерной картины[1].

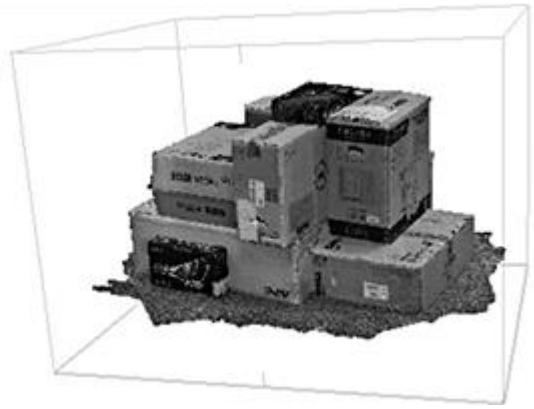

Рис. 1. *Облако точек объекта*

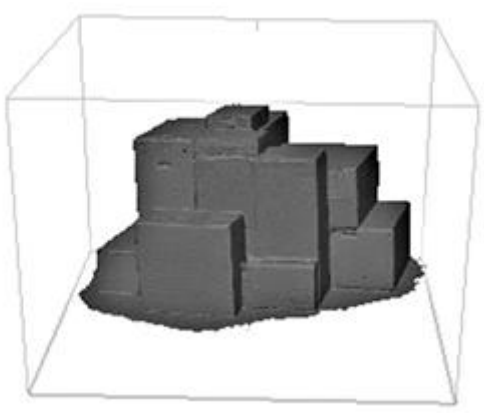

Рис. 2. *3D-модель*

Рис. 3. *Текстура*

Полученные в ходе осмотра места происшествия фотографии как с фотоаппарата, так и с видеокамеры БПЛА в дальнейшем должны пройти обработку в программном обеспечении (Agisoft Metashape, Autodesk ReCap), с явной прямо пропорциональной зависимостью – чем больше сделано фотографий специалистом на осмотре месте происшествия, тем более качественной получится 3D-модель места происшествия. При помощи действий пользователя программа выравнивает снимки, после того как все действия по выравниваю будут выполнены, пользователь принимает решение о создании облака точек. Облако точек представляет собой набор точек[2] данных в пространстве. Алгоритм анализирует ключевые точки на фото, и строит облако

[1] Советы по аэрофотосъемке (с БПЛА самолётного типа) // Metashape. URL: https:// metashape.ru/docs/sovety-po-aerofotosemke-s-bpla-samolyotnogo-tipa/ (дата обращения: 18.01.2025).

[2] Зимина Л.В. Трехмерное моделирование: сферы применения, подходы к описанию 3D-моделей, методы компьютерной 3D-анимации // Образование и наука без границ: фундаментальные и прикладные исследования. 2020. № 12. С. 66.

точек, на основе чего следующим этапом создается 3D-модель, и если модель была выстроена корректно, на нее накладывается текстура (рис. 1–3).

Суммируя вышеизложенное, весь алгоритм 3D-моделирования методом фотограмметрии можно представить в виде схемы (рис. 4).

Основными достоинствами фотограмметрии, как метода 3D-моделирования, при производстве осмотров мест происшествий, являются: высокая детализация получаемой модели, доступность оборудования (фотоаппарат и компьютер с программным обеспечением), возможность работы в «полевых» условиях. В свою очередь, у данного метода есть и недостатки: высокие требования к качеству фотосъемки, зависимость от освещения, погодных и климатических условий, многоэтапная обработка снимков.

Метод лазерного сканирования в 3D-моделировании реализуется посредством бесконтактных сканеров, принцип работы которых основан на измерении времени, за которое лазерный луч отражается от поверхности и возвращается на исходную точку к датчику. Применение данного метода позволяет сканировать объекты с высокой степенью.

Общий алгоритм создания 3D-модели посредством лазерных 3D-сканеров состоит из 4 основных этапов:

1. Выбор и установка 3D-сканеров на месте происшествия (мобильных или стационарных, подбор осуществляется исходя из габаритов исследуемого объекта).
2. Процесс сканирования (создание облака точек).
3. Перенос и обработка данных в специальном программном обеспечение (Faro Scene, Leica Cyclone и др.).
4. Создание 3D-модели с точными размерами и топографией.

Рис. 4. *Общий алгоритм создания 3D-модели методом фотограмметрии*

Для сканирования небольших объектов уместно применение ручных сканеров, например, Calibry Mini, данный сканер предназначен для оцифровки небольших объектов (длиной от 2 до 30 см). Синие светодиоды обеспечивают высокое качество получаемых данных, а встроенный сенсорный экран упрощает процесс сканирования. Три режима сканирования Calibry mini – текстура, геометрия и маркеры, позволяют сканировать практически любой объект поле зрения устройства[1].

При фиксации следов на месте происшествия целесообразно применение режимов геометрии или по маркерам. Если след не четко отобразился на поверхности, или условия освещения недостаточны, то уместным будет применение метода сканирования по маркерам. Полученный методом лазерного 3D-сканирования след должен быть визуализирован в специальном программном обеспечении (для сканеров Calibry Mini программа Calibry Nest и др.), инструментарий которого, позволяет обрабатывать облака точек, строить полигональные 3D-модели и экспортировать в модели с расширениями для печати.

Для лазерного 3D-сканирования на открытых участках местности, например, для фиксации места дорожно-транспортного происшествия или места взрыва, наиболее приемлемы стационарные сканеры (Faro Focus 3D, Leica RTC360 и др.). Данные сканеры устанавливаются на штатив, и с высокой степенью детализации позволяют создать облака точек, из которых впоследствии формируются 3D-модели мест происшествий.

Таким образом, следует выделить основные достоинства лазерного 3D-сканирования, как метода 3D-моделирования, при производстве осмотров мест происшествий: высокая точность сканирования, возможность работы в условиях недостаточной освещенности, автоматизированный процесс сбора информации сканирования.

Использование 3D-моделирования при осмотре места происшествия является перспективным методом фиксации материально-вещной обстановки. Методы фотограмметрии и лазерного сканирования в 3D-моделировании позволяют воссоздавать точные трехмерные копии мест происшествий со следовой картиной, что повышает уровень объективности и достоверности получаемых данных на первоначальном этапе расследования. Несомненно, каждый метод моделирования имеет свои преимущества и недостатки, применение методов в совокупности позволит их скомпенсировать.

Список источников

1. Зимина Л.В. Трехмерное моделирование: сферы применения, подходы к описанию 3D-моделей, методы компьютерной 3D-анимации // Образование и

[1] Практический опыт 3D сканирования сканером Calibry mini от 3Dtool. // 3D Tool URL: https://3dtool.ru/stati/prakticheskiy-opyt-3d-skanirovaniya-skanerom-calibry-mini-ot-3dtool/ (дата обращения: 18.01.2025).

наука без границ: фундаментальные и прикладные исследования. 2020. № 12. С. 65–71.

2. Практический опыт 3D сканирования сканером Calibry mini от 3Dtool. // 3D Tool URL: https://3dtool.ru/stati/prakticheskiy-opyt-3d-skanirovaniya-skanerom-calibry-mini-ot-3dtool.

3. Общие правила и советы для съемки. *Metashape.* URL: https://metashape.ru/docs/obshhie-pravila-i-sovety-dlya-semki.

4. Советы по аэрофотосъемке (с БПЛА самолётного типа). *Metashape*. URL: https://metashape.ru/docs/sovety-po-aerofotosemke-s-bpla-samolyotnogo-tipa.

5. Дышокова А.Т. Использование 3D-технологий при раскрытии преступлений: нововведение в области криминалистики // Молодой ученый. 2022. № 48 (443). С. 250–252.

6. Новикова Т.Б., Хаснутдинов Р.Р. Метод 3D-моделирования в современной судебно-экспертной деятельности // Юридические науки. 2020. №12-4(51). С. 32–35.

Е.В. Прокофьева[1], **Р.А. Мерзликин**[2]
[1,2] Волгоградская академия МВД России

Правовая оценка применения беспилотных летательных аппаратов при производстве осмотра по факту дорожно-транспортного происшествия

Аннотация. Рассмотрены причины и условия необходимости применения БПЛА специалистами при осмотре места ДТП. Проанализированы положения законодательства, регламентирующие использование БПЛА и его перемещение в воздушном пространстве. Определен правовой порядок внедрения БПЛА в экспертные учреждения МВД России.

Ключевые слова: правовая оценка, беспилотный летательный аппарат, осмотр места происшествия, дорожно-транспортное происшествие.

Техногенный скачок сформировал предпосылки перехода к использованию современных достижений науки и техники в практике правоохранительных органов. Ускорение процессов автоматизации повысило востребованность и значимость интеграции беспилотных летательных аппаратов с целью упрощения процесса получения доказательственной информации. Вопрос правовой оценки применения беспилотных воздушных суден в деятельности органов внутренних дел остается открытым, с точки зрения правового регулирования обеспечения

безопасности эксплуатации БПЛА[1], вопроса подготовки и квалификации пилотов, инструкторов БПЛА, их правового статуса и др.

Ряд исследователей синтезируют важные выводы о необходимости установления целого спектра ограничений, касающихся граждан, организаций и государственных учреждений, реализующих применение БПЛА в практической деятельности. Данные ограничения должны предоставить гарантию безопасности граждан, получения достоверного фото- и видео материала для расследования, с учетом установления административной ответственности за нарушение ограничений[2].

Как справедливо отмечается в работе А.А. Пудовкина и др.[3], целесообразность применения БПЛА при ОМП по факту ДТП в большей степени обоснована и не вызывает сомнения, ввиду мобильности перемещения устройства и получения посредством его реализации, в реальном времени с возможностью длительного хранения, фиксируемого объёма информации объективной реальности происходящего события. Места ДТП имеют определенную специфику, некоторые участки дорог можно отнести к труднодоступным, масштабы осмотра могут превышать несколько километров и др. В этой связи применение БПЛА для получения объективной картины произошедшего события обусловлено правовыми нормами его реализации.

Учитывая рассматриваемую проблематику и соотнося положения законодательства с существующими позициями ученых, проявляется ряд проблем требующих решения при реализации беспилотных летательных аппаратов при осмотре места происшествия вообще, и в частности при осмотре места дорожно-транспортного происшествия.

Для обеспечения безопасности эксплуатации воздушного средства требуется учет совокупности факторов геолокационного, погодно-климатического и топографического спектра. Разрешение данной проблемы видится в целом комплексе действий, обусловленном совершенствованием электронно-технического обеспечения устройства, обеспечивающего качественное, непрерывное соединение с БПЛА, с гарантией управления без потери сигнала при разных условиях эксплуатации, обеспечиваемое нормативно-техническими документами (СП(СНиП), Регламентами, ГОСТ и др.). Требуется высокоэффективная, качественная профессиональная подготовка операторов

---

[1] Грищенко Г.А. Правовое регулирование беспилотных летательных аппаратов: Российский подход и мировая практика // Вестник Университета имени О.Е. Кутафина. 2019. №12 (64). С. 129–136.

[2] Анисимов А.П., Иванова Ж.Б. Правовое регулирование использования беспилотных воздушных судов (квадрокоптеров): дискуссионные вопросы // Вестник Института законодательства и правовой информации Республики Казахстан. 2017. №4 (49). С. 64–70.

[3] Пудовкин А.А., Теткин Д.В., Бондарев Д.В. Особенности проведения осмотра места происшествия, местности в труднодоступных местах и при дорожно-транспортном происшествии с помощью применения беспилотных летательных аппаратов // Известия Тульского государственного университета. Экономические и юридические науки. 2022. Вып. 3. С. 104–111.

БПЛА, в том числе и из числа сотрудников правоохранительных органов, не только в понимании самой подготовки специалистов-операторов, но и в проведении специальных мероприятий для решения задач беспилотной авиации в погодных условиях с критическими показателями скорости ветра и высоты, облачности, сложной полетной топографии и др. Направленность современной профессиональной подготовки должна соответствовать современным реалиям, носить опережающий характер и обеспечивать надежную реализацию полученных навыков, в том числе при реализации БПЛА для осмотров мест дорожно-транспортных происшествий.

Эксплуатация БПЛА в рамках конкретных следственных действий требует правового регулирования, заключающегося в регламентации правил применения беспилотных воздушных суден в узконаправленном спектре для их реализации с целью осмотра. Необходимо создание инструкций по применению БПЛА специалистами в ходе ОМП, утверждающих тактико-технические характеристики беспилотных воздушных средств, перечень мероприятий, осуществляемых при подготовке к их применению и использованию.

Отметим справедливость высказывания Е.С. Мазур и А.В. Шалакина, заключающуюся в причинной обусловленности необходимости применения БПЛА в раскрытии и расследовании преступлений, обеспечивающей возрастание не только социальной значимости борьбы с преступностью, но и значительное расширение научно-технических возможностей, предоставляемых учеными для борьбы с преступностью[4].

По точному выражению Д.А. Полетыкина[5], основной источник правового регулирования БПЛА на уровне федерального законодательства Российской Федерации – Воздушный кодекс РФ, содержащий как специальные нормы в отношении БПЛА, так и общие нормы, посвященные пилотируемым воздушным судам, которые распространяют свое действие на БПЛА.

С точки зрения законодательства Российской Федерации в области эксплуатации БВС, БПЛА учитываются следующие нормы: ФАП-138 (использования воздушного пространства РФ); ФАП-128 (подготовка и выполнение полетов в гражданской авиации РФ); ФАП-494 (требования к проведению обязательной сертификации физических лиц, юридических лиц, выполняющих авиационные работы. Порядок проведения сертификации); ФАП-147 (требования к членам экипажа воздушных судов, специалистам по техническому обслуживанию воздушных судов и сотрудникам по обеспечению полетов гражданской авиации); Правила учета беспилотных гражданских воздушных судов с максимальной взлетной массой от 0,25 килограмма до 30 килограммов, ввезенных в Российскую Федерацию или произведенных в

[4] Мазур Е.С., Шалакин А.В. Современные технико-криминалистические средства, применяемые при проведении поисковых следственных действий // Правовые проблемы укрепления российской государственности: [сборник статей]. Томск, 2017. Ч. 74. С. 146.

[5] Полетыкина Д.А. Правовое регулирование использования беспилотных летательных аппаратов в Российской Федерации: текущее состояние и перспективы развития // Юридическая наук. 2023. № 9. С. 143–153.

Российской Федерации (постановление Правительства Российской Федерации от 25 мая 2019 г. № 658)[6].

Правовой статус беспилотных летательных аппаратов и операторов, ими управляющих, требует конкретного определения в правовых нормах, регулирующих определение статуса БПЛА и отношения участников общественных отношений, связанных с использованием беспилотных летательных аппаратов. Необходимо разграничить статус беспилотных воздушных судов, используемых сотрудниками органов внутренних дел в рамках следственных действий, и судов, используемых физическими и иными юридическими лицами.

С точки зрения уголовно-процессуальных отношений, статус операторов БПЛА не совсем определен. Их можно определить как специалистов, однако учитывая управление беспилотным воздушным судном, их правовой статус может быть приравнен к статусу командира беспилотного воздушного судна, закрепленному Воздушным кодексом РФ.

Интеграция БПЛА в практику правоохранительных органов требует корректировок правил воздушного движения. Сейчас отсутствует достаточная правовая регламентация применения БПЛА в воздушном пространстве в черте городов и других объектов.

Результаты работы дают основание говорить о решении современных проблем правового поля в области интеграции БПЛА в деятельность специалистов при осмотре места ДТП через создание единого понятийного аппарата: определение статуса БПЛА как технического средства, а не воздушного судна и разграничение статуса лица, управляющего БПЛА (оператора), от статуса капитана воздушного судна. Суть разграничения заключается в следующем: БПЛА не приобретает статус воздушного судна, но подчиняется некоторым правилам, которые будут представлять собой ограничение по применению БПЛА в воздушном пространстве. Аналогичное разграничение уместно и для статуса оператора БПЛА. Под оператором БПЛА следует понимать лицо, осуществляющее управление беспилотным летательным аппаратом. Учитывая, что осуществлять применение БПЛА должен будет специалист, то правовой статус оператора должен будет применяться именно к нему. Моментом возникновения прав и обязанностей оператора будет считаться момент начала применения БПЛА (подготовка к взлету); создание единого пространства для беспилотников: через регулирование движения в воздушном пространстве, посредством издания специального нормативного правового акта, регламентирующего передвижение воздушных беспилотных машин.

[6] Требования авиационных властей к БПЛА, ДРОН. URL: https:// JetConsulting.aero (дата обращения: 12.01.2025).

Список источников

1. Анисимов А.П., Иванова Ж.Б. Правовое регулирование использования беспилотных воздушных судов (квадрокоптеров): дискуссионные вопросы / А.П. Анисимов, Ж.Б. Иванова // Вестник Института законодательства и правовой информации Республики Казахстан. 2017. № 4 (49). С. 64–70.
2. Грищенко Г.А. Правовое регулирование беспилотных летательных аппаратов: Российский подход и мировая практика // Вестник Университета имени О. Е. Кутафина. 2019. №12 (64). С. 129–136.
3. Мазур Е.С., Шалакин А.В. Современные технико-криминалистические средства, применяемые при проведении поисковых следственных действий // Правовые проблемы укрепления российской государственности: [сборник статей]. Томск, 2017. Ч. 74. С. 146.
4. Полетыкина Д.А. Правовое регулирование использования беспилотных летательных аппаратов в Российской Федерации: текущее состояние и перспективы развития // Юридическая наука. 2023. № 9. С. 143–153.
5. Пудовкин А.А. Особенности проведения осмотра места происшествия, местности в труднодоступных местах и при дорожно-транспортном происшествии с помощью применения беспилотных летательных аппаратов / А.А. Пудовкин, Д.В. Теткин, Д.В. Бондарев // Известия Тульского государственного университета. Экономические и юридические науки. 2022. Вып. 3. С. 104–111.
6. Требования авиационных властей к БПЛА, ДРОН. URL: https:// JetConsulting.aero.

А.В. Сибилькова
Академия управления МВД России

Совершенствование организационного обеспечения расследования преступлений, как аспект обеспечения информационной безопасности человечества

Аннотация. Обратной стороной тотальной цифровизации общества является пропорциональное возрастание числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Специфика данных преступлений, обусловленная отсутствием традиционных материальных следов их совершения, обезличиванием лиц, их совершающих, и дистанционным характером подготовки и осуществления данного вида преступной деятельности, указывает на необходимость поиска на уровне всей правоохранительной системы государства адекватных ответов на вызовы и угрозы, формирующиеся в данной сфере, а также на важность поиска эффективных методов противодействия.

Основные направления совершенствования организационного обеспечения расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий:

- улучшение качества отбора сотрудников, назначаемых на должности руководителей следственных подразделений в контексте объективизации оценки их личностных, профессиональных, деловых и человеческих качеств;

- осуществление руководителем целенаправленной работы по организации, налаживанию и поддержанию взаимодействия с вневедомственными субъектами, привлекаемыми к выявлению, расследованию и раскрытию преступлений;

- внедрение руководителем в деятельность возглавляемых подразделений практики алгоритмизации отдельных типовых действий;

- формирование руководителем конструктивной рабочей атмосферы в коллективе с учетом субъективных и объективных кадровых факторов;

- формирование комфортной рабочей обстановки путем недопущения личных и профессиональных конфликтов в коллективе, личного вмешательства в спорные ситуации и оказания содействия в преодолении назревающих конфликтных ситуаций, оказания идеологического воздействия на личном примере, реагирования на запросы сотрудников и выстраивания коммуникации с ними по принципу обратной связи.

Практическая реализация сформулированных предложений позволит качественно повысить результативность деятельности подразделений, осуществляющих расследование преступлений, совершенных с применением информационно-телекоммуникационных технологий, и качественно улучшить практику организационного обеспечения расследования данной категории преступлений в соответствии с актуальными запросами и реальными возможностями в данной сфере.

Ключевые слова: цифровые технологии, информационно-коммуникационные технологии, цифровизация общества, преступление, совершаемое с использованием информационно-телекоммуникационных технологий, организационное обеспечение расследования преступлений.

На современном этапе развития общества уровень стремительной трансформации цифровых и информационно-коммуникационных технологий определяется высокой скоростью, всеобъемлющим характером и стремительным проникновением во все сферы жизни людей и функционирования государства. В настоящее время невозможно представить себе не только деятельность органов государственной власти, но и повседневную жизнь граждан без средств информационно-телекоммуникационного обмена информацией. Непрерывное расширение перечня услуг, предоставляемых удаленно, а также возможностей дистанционного совершения финансовых операций закономерно приводят к росту числа пользователей информационных сетей, коммуникационных ресурсов и программных продуктов.

Но обратной стороной тотальной цифровизации общества является пропорциональное возрастание числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Специфика данных преступлений, обусловленная отсутствием традиционных материальных следов их совершения, обезличиванием лиц, их совершающих, и дистанционным характером подготовки и осуществления данного вида преступной деятельности, указывает на необходимость поиска на уровне всей правоохранительной системы государства адекватных ответов на вызовы и угрозы, формирующиеся в данной сфере, а также на важность поиска

эффективных методов противодействия. В настоящее время, несмотря на все прилагаемые в данном направлении усилия, возможности правоохранительных органов нередко уступают аналогичным возможностям злоумышленников, а имеющийся в распоряжении субъектов системы противодействия преступности материально-технический, методический и тактический инструментарий не в полной мере соответствует актуальным потребностям.

Так, на ведомственном уровне отмечается назревшая потребность в совершенствовании не только материально-технической базы ведомственных подразделений, осуществляющих расследование преступлений, совершенных с использованием информационно-телекоммуникационных технологий, но и в разработке научно обоснованных подходов к грамотной организации деятельности по данному направлению, построенной на рациональном применении материально-технических, кадровых, информационных и иных ресурсов в интересах повышения результативности усилий, предпринимаемых в данном направлении.

Сложившаяся практика организационного обеспечения расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, не отвечает актуальным запросам и не отражает реальных возможностей МВД России в данной сфере. В связи с чем необходимо совершенствование организации расследования данной категории преступлений, что позволит качественно повысить результативность деятельности соответствующих подразделений.

Преступления, совершенные с использованием информационно-телекоммуникационных технологий, характеризуются следующими признаками: стремительный количественный прирост официально зарегистрированных преступлений данного вида в Российской Федерации на протяжении последнего десятилетия; доступность совершения данного вида преступления во всех сферах жизни общества, обусловленная тотальной цифровизацией выполняемых в них действий, явлений и процессов; высокий уровень латентности преступлений, совершенных с использованием информационно-телекоммуникационных технологий; возможность удаленного, дистанционного и обезличенного выполнения действий, составляющих объективную сторону их совершения; широкие информационно-телекоммуникационные возможности, реализуемые злоумышленниками в целях сокрытия любой иной преступной деятельности, помимо рассматриваемого вида преступлений.

К реализуемым руководителями следственных органов задачам организационного обеспечения с учетом специфики рассматриваемой категории преступлений относятся: распределение специализации сотрудников подразделений в соответствии с имеющимся у них опытом; подбор личного состава с учетом профессиональных, деловых, индивидуально-личностных и нравственных качеств; рациональное распределение и использование ресурсов, имеющихся в распоряжении подразделений, непосредственно задействуемых в расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий; организация уровня материально-

технической оснащенности подразделений, отвечающего объективным потребностям практики и позволяющего адекватно и соразмерно реагировать на характер вызовов и угроз, возникающих и реализуемых злоумышленниками в сфере высоких технологий; создание комфортных условий для профессиональной деятельности личного состава; поддержание необходимого научного-исследовательского и квалификационного уровня сотрудников в сфере использования информационно-телекоммуникационных технологий.

Основные трудности расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, связаны со стремительным ростом их общего количества, расширением инструментария, используемого злоумышленниками для их подготовки, совершения и сокрытия, и отставанием материально-технических, научно-методологических возможностей органов внутренних дел от аналогичных возможностей преступников. В связи с этим совершенствование организационного обеспечения их расследования в первоочередном порядке видится в усовершенствовании ресурсной базы подразделений органов внутренних дел.

Поскольку руководитель следственного подразделения является управленческим звеном, непосредственно находящимся в рабочей среде и обстановке подразделений, именно ему надлежит непосредственно на месте оценивать состояние ресурсной базы подразделения (ее кадровой, материально-технической, методической, научной, информационной составляющих). Перечень полномочий, предоставленных руководителю подразделения, позволяет ему выступать с инициативами по расширению ресурсных возможностей подразделения как перед вышестоящим руководством в структуре ведомства, так и взаимодействовать по этим вопросам со сторонними субъектами – например, представителями научного сообщества, конкретными разработчиками информационно-телекоммуникационного инструментария. Как свидетельствуют результаты анализа практики в данной сфере, решение этих вопросов напрямую зависит от личной заинтересованности руководителя подразделения, его неравнодушия к потребностям сотрудников.

В качестве основного направления совершенствования организационного обеспечения расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, следует обозначить улучшение качества отбора сотрудников, назначаемых на должности руководителей следственных подразделений в контексте объективизации оценки их личностных, профессиональных, деловых и человеческих качеств. Следует согласиться с тем, что выполнение данного требования является важным применительно к организации расследования не только к рассматриваемой категории преступлений, но в силу их специфики, сложности, многоэпизодности и способности вызывать широкий общественный резонанс, негативно влияя при этом на оценку эффективности органов внутренних дел населением и общественными институтами, именно в ракурсе рассматриваемой проблематики реализация данной меры представляется наиболее актуальной и востребованной.

Также ранее упомянутая необходимость налаживания взаимодействия между следственными подразделениями, осуществляющими расследование

преступлений, совершенных с применением информационно-телекоммуникационных технологий, с иными ведомственными и вневедомственными субъектами, вовлекаемыми в процесс расследования, требует от руководителя грамотной организации процесса взаимодействия. Поскольку целью взаимодействия является объединение совместных усилий его участников с целью достижения ожидаемого результата в кратчайшие сроки и наиболее эффективными методами, организационный пробел именно в этой сфере способен существенно снизить эффективность работы всего подразделения и нивелировать усилия, прилагаемые сотрудниками. При этом если взаимодействие подразделений, вовлеченных в процесс расследования преступлений, на внутриведомственном уровне достаточно детально регламентируется нормативными правовыми источниками ведомственного уровня открытого и закрытого характера, то в части организации взаимодействия со сторонними субъектами требует проявления соответствующей инициативы.

Поскольку сотрудники единолично и по собственной инициативе в силу ограниченности предоставленных им полномочий и представительских функций не могут решать данные вопросы самостоятельно, организация деятельности по данному направлению полностью находится в ведении руководителя подразделения. Кроме того, заключение отдельных соглашений о взаимодействии (например, с федеральными банковскими и кредитными организациями и их региональными филиалами и представительствами) не входит в компетенцию руководителя следственного подразделения, а подлежит осуществлению на уровне руководства территориального органа внутренних дел.

В результате чего, в качестве важного направления совершенствования организационного обеспечения расследования преступлений, совершенных с применением информационно-телекоммуникационных технологий, необходимо отметить потребность в осуществлении руководителем следственного подразделения целенаправленной работы по организации, налаживанию и поддержанию взаимодействия с вневедомственными субъектами, привлекаемыми к выявлению, расследованию и раскрытию преступлений, совершенных с использованием информационно-телекоммуникационных технологий, как непосредственно, так и путем проявления инициативы в адрес вышестоящего руководства, а также личном участии и контроле за качеством осуществляемого подразделением взаимодействия.

В настоящее время Следственным департаментом МВД России совместно с Московским университетом МВД России имени В.Я. Кикотя разработан и распространен в органы предварительного расследования Сборник образцов типовых запросов, необходимых для расследования IT-преступлений, с указанием контактной информации об организациях и располагаемых ими сведениях[1]. Данный пример является иллюстрирующим наравне с множеством

[1] Гончар В.В. Актуальные направления совершенствования расследования преступлений в сфере информационных технологий // Вестник Московского университета МВД России. 2022. № 6. С. 85.

аналогичных административно-управленческих решений. Данная практика унификации порядка совершаемых процессуальных действий, типологизации порядка принимаемых сотрудниками в ходе расследования решений и алгоритмизации их деятельности значительно упрощает ход расследования, делает его более понятным для сотрудников, прозрачным и доступным для контроля руководителем.

В целом, практика алгоритмизации действий сотрудников в однородных по содержанию ситуациях (в данном случае – применительно к расследованию преступлений однородной категории, обобщающим признаком для которых является их совершение с применением информационно-телекоммуникационных технологий) давно положительно зарекомендовала себя не только на практике, но и в общей теории управления[1]. На практике это позволяет в кратчайшие сроки точечно предпринимать необходимые для достижения результата действия, целенаправленно прилагать необходимые усилия, существенно экономить время, сокращая общие сроки расследования и предотвращая волокиту по делу, и реализовывать весь объем имеющихся у сотрудников полномочий, избегая возможных злоупотреблений ими.

Таким образом, перспективным направлением совершенствования организационного обеспечения расследования преступлений, совершенных с применением информационно-телекоммуникационных технологий, является предложение о внедрении руководителем в деятельность возглавляемых подразделений практики алгоритмизации отдельных типовых действий: составления и направления запросов; получения, проверки и оценки криминалистически значимой для дела информации; привлечения специалистов, экспертов и иных участников уголовного судопроизводства; принятия процессуальных решений по делу и т.д.

С позиций теории управления и с учетом ведомственной специфики функционирования особое внимание необходимо уделять кадровым ресурсам, поскольку именно сотрудники являются носителями кадрового потенциала, оказывающего непосредственное влияние на формирование показателей эффективности деятельности всего министерства и формирующего облик полиции в целом. От того, насколько сотрудники являются профессионально подготовленными, компетентными, заинтересованными в своей профессии (субъективный кадровый фактор) и от того, в каких условиях и в какой служебной обстановке происходит выполнение ими поставленных перед ними задач (объективный кадровый фактор) в определяющем смысле зависит общий результат деятельности ведомства.

В ситуациях несоответствия личных качеств сотрудника (как

[1] См. напр.: Бернстайн И., Ли М., Миннаар Й. Как алгоритмы помогают сотрудникам самим управлять своей работой // Гарвард Бизнес Ревью Россия. № 3, 2023. URL: https://big-i.ru/innovatsii/tekhnologii/kak-algoritmy-pomogayut-sotrudnikam-samim-upravlyat-svoey-rabotoy/ (дата обращения 11.01.2025); Гаврилюк А.В., Чжао А. Алгоритмизация процессов управления в гиг-экономике // Государственное управление. 2024. № 102. С. 168–182 и др.

профессиональных, так и личностных) уровню сложности служебных задач вся деятельность данного сотрудника принимает характер несоразмерности. При этом данная особенность имеет двойную направленность: когда способному и качественно подготовленному сотруднику поручается решение излишне простых задач, его потенциал стремительно растрачивается, возникают ситуации эмоционального выгорания и попустительского отношения к делу. И, напротив – когда сотруднику, в силу набора его индивидуальных характеристик не способного на решение сложных, интеллектуальных, многокомпонентных задач, поручается расследование рассматриваемой категории преступлений, им чаще начинает имитироваться активная служебная деятельность, многие важные эпизоды процесса расследования упускаются из вида либо неверно им интерпретируются, на его многочисленные запросы о помощи отвлекаются иные сотрудники подразделения. В результате чего по истечении установленного срока поставленные задачи остаются без решения либо решаются некачественно.

Преодоление описываемых противоречий непосредственно относится к компетенции руководителя следственного подразделения. Ввиду непосредственной приближенности к сотрудникам, владения складывающейся в коллективе ситуацией и способностью оказания на нее управленческого воздействия, руководителю исключительно важно наладить грамотное управление коллективом в контексте учета профессиональных и личных качеств сотрудников и в целях формирования комфортной и здоровой рабочей атмосферы. Кроме того, сам процесс расследования преступлений, совершенных с применением информационно-телекоммуникационных технологий, в силу их специфичности требует наличия у сотрудников определенных личностных качеств: развернутого логического мышления, владения глубокими представлениями о возможностях и особенностях практического применения современных информационных технологий, усидчивости, умения сосредотачиваться и погружаться в техническую суть происходящего, настойчивости и способности к длительной концентрации внимания.

В этой связи, в качестве важного направления совершенствования организационного обеспечения расследования преступлений, совершенных с применением информационно-телекоммуникационных технологий, необходимо сформулировать предложение о том, что руководителям следственных подразделений важно формировать конструктивную рабочую атмосферу в коллективе с учетом субъективных и объективных кадровых факторов: подбирать сотрудников на основании результатов оценки их личностных и профессиональных качеств, способности и заинтересованности в работе по линии расследования данной категории преступлений, стремлений к самообразованию и дальнейшему обучению в рамках ведомственных направлений профессиональной переподготовки; формировать комфортную рабочую обстановку путем недопущения личных и профессиональных конфликтов в коллективе, личного вмешательства в спорные ситуации и оказания содействия в преодолении назревающих конфликтных ситуаций, оказания идеологического воздействия на личном примере, реагирования на запросы сотрудников и выстраивания коммуникации с ними по принципу

обратной связи.

Таким образом, подводя итог вышеизложенному, в качестве основных направлений совершенствования организационного обеспечения расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий, следует обозначить:

- улучшение качества отбора сотрудников, назначаемых на должности руководителей следственных подразделений в контексте объективизации оценки их личностных, профессиональных, деловых и человеческих качеств;

- осуществление руководителем целенаправленной работы по организации, налаживанию и поддержанию взаимодействия с вневедомственными субъектами, привлекаемыми к выявлению, расследованию и раскрытию преступлений, совершенных с использованием информационно-телекоммуникационных технологий, как непосредственно, так и путем проявления инициативы в адрес вышестоящего руководства, осуществлению личного участия и контроля за качеством осуществляемого подразделением взаимодействия;

- внедрение руководителем в деятельность возглавляемых подразделений практики алгоритмизации отдельных типовых действий: составления и направления запросов; получения, проверки и оценки криминалистически значимой для дела информации; привлечения специалистов, экспертов и иных участников уголовного судопроизводства; принятия процессуальных решений по делу и т.д.;

- формирование руководителем конструктивной рабочей атмосферы в коллективе с учетом субъективных и объективных кадровых факторов: подбор сотрудников на основании результатов оценки их личностных и профессиональных качеств, способности и заинтересованности в работе по линии расследования данной категории преступлений, стремлении к самообразованию и дальнейшему обучению в рамках ведомственных направлений профессиональной переподготовки;

- формирование комфортной рабочей обстановки путем недопущения личных и профессиональных конфликтов в коллективе, личного вмешательства в спорные ситуации и оказания содействия в преодолении назревающих конфликтных ситуаций, оказания идеологического воздействия на личном примере, реагирования на запросы сотрудников и выстраивания коммуникации с ними по принципу обратной связи.

Практическая реализация сформулированных предложений позволит качественно повысить результативность деятельности подразделений, осуществляющих расследование преступлений, совершенных с применением информационно-телекоммуникационных технологий, и качественно улучшить практику организационного обеспечения расследования данной категории преступлений в соответствии с актуальными запросами и реальными возможностями в данной сфере.

Список источников

1. Бернстайн И., Ли М., Миннаар Й. Как алгоритмы помогают сотрудникам самим управлять своей работой // Гарвард Бизнес Ревью Россия., 2023. № 3. URL: https://big-i.ru/innovatsii/tekhnologii/kak-algoritmy-pomogayut-sotrudnikam-samim-upravlyat-svoey-rabotoy.
2. Гаврилюк А.В., Чжао А. Алгоритмизация процессов управления в гиг-экономике // Государственное управление. 2024. № 102. С. 168–182.
3. Гончар В.В. Актуальные направления совершенствования расследования преступлений в сфере информационных технологий // Вестник Московского университета МВД России. 2022. № 6. С. 82–87.

С.Ю. Скобелин
Московская академия Следственного комитета
имени А.Я. Сухарева

Первоначальный этап расследования развратных действий в сети Интернет

Аннотация. На основе изучения отечественной следственной практики раскрытия и расследования развратных действий, совершенных с использованием информационно-коммуникационных технологий, обозначаются основные направления деятельности следователя на первоначальном этапе.

Ключевые слова: развратные действия, расследование, сеть Интернет, электронные устройства, цифровые следы, идентификация.

Судебно-следственная практика и статистические данные свидетельствуют о том, что в России с каждым годом увеличиваются факты так называемых дистанционных (бесконтактных, интеллектуальных) развратных действий в отношении несовершеннолетних, совершенных с помощью компьютеров и смартфонов, подключенных к сети Интернет.

Так, если в 2013 году было зарегистрировано 52 сообщения о преступлениях указанной категории, в 2014 году уже 276, а в последующие годы их количество только росло и в 2023 было зарегистрировано уже около тысячи подобных преступлений, при этом 1/3 из них остается нераскрытыми[1].

Нередко преступники по совокупности совершают также такие преступления, как нарушение неприкосновенности частной жизни (ст. 137 УК РФ); вымогательство (ст. 163 УК РФ); получение сексуальных услуг несовершеннолетнего (ст. 240.1. УК РФ); изготовление и оборот материалов или

[1] Информационные технологии в уголовно-правовой сфере: монография / под ред. А.И. Бастрыкина, А.Н. Савенкова. М.: ЮНИТИ-ДАНА, 2023. С. 112.

предметов с порнографическими изображениями несовершеннолетних (ст. 242, ст. 242.1, ст. 242.2 УК РФ). Если же жертва преступления не достигла 12-летнего возраста и это охватывалось умыслом виновного, его деяние подлежит квалификации как насильственные действия сексуального характера (п. «б» ч. 4, п. «а» и (или) «б», ч. 5 ст. 132 УК РФ).

Общими признаками для данного преступления являются:

– использование сети Интернет (социальные сети, мессенджеры, компьютерные игры, сайты знакомств и т.п.) или телефонной связи (соответственно простых телефонов, смартфонов или компьютеров с SIM-картой);

– дистанционность (преступник и жертва находятся в разных местах, порой даже странах);

– отсутствие физического контакта с телом потерпевшего (интеллектуальные развратные действия в отношении лиц, не достигших 16 лет (путем переписки, голосовых или видеозвонков, бесед, отправки фотографий) или иные действия сексуального характера в отношении детей, находящихся в беспомощном состоянии, в том числе не достигших 12 лет);

– длящийся характер (порой многоэпизодность) переписки и (или) звонков;

– лица, совершающие данные преступления часто страдают различными формами парафилии (в частности педофилией – расстройством сексуального предпочтения), могут иметь иные психические отклонения сексуального характера)[1];

– естественная латентность (несовершеннолетние жертвы и их близкие не желают огласки подобных деяний).

В соответствии с п. 17 Постановления Пленума Верховного Суда РФ от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» к развратным действиям относятся любые действия, кроме полового сношения, мужеложства и лесбиянства, совершенные в отношении лиц, достигших двенадцатилетнего возраста, но не достигших шестнадцатилетнего возраста, которые были направлены на удовлетворение сексуального влечения виновного, или на вызывание сексуального возбуждения у потерпевшего лица, или на пробуждение у него интереса к сексуальным отношениям.

При этом развратными могут признаваться и такие действия, при которых непосредственный физический контакт с телом потерпевшего лица отсутствовал, включая действия, совершенные с использованием сети Интернет, иных информационно-телекоммуникационных сетей.

Интернет-разврату присущи следующие формы:

– цинично-вульгарные разговоры (переписка) на темы сексуального характера;

---

[1] Иващенко М.А. Расследование преступлений против половой неприкосновенности и половой свободы несовершеннолетних, совершенных с использованием сети Интернет: практическое пособие. М.: Московская академия СК России, 2022. С. 19.

– прикрепление ссылок, файлов или демонстрация в онлайн-режиме эротических или порнографических фотографий или видеозаписей (возможно половых органов, актов мастурбации или половых актов самого преступника с иными лицами). Не имеет значения для уголовного преследования, сделаны ли фотографии самим преступником, скопированы из других источников или сгенерированы с помощью искусственного интеллекта;

– склонение потерпевшего к демонстрации своего обнаженного тела (половых органов), актов мастурбации, половых контактов с иными лицами путем уговоров, угроз применения насилия к самому потерпевшему либо его близким, распространения сведений, позорящих потерпевшего или его близких.

Для привлечения виновных к уголовной ответственности не имеет значения, имел ли потерпевший опыт половых отношений, степень его осведомленности об этом, а также его половая зрелость и даже тот факт, что инициатором таких действий мог выступать сам потерпевший, а виновный, осознавая, что общается с лицом, не достигшим 16 лет, дал согласие и продолжил развращать ребенка.

В то же время беседы на тему сексуальных отношений совершеннолетних лиц с детьми с использованием информационных технологий и даже демонстрирование им фотографий, предметов, картин, видеофильмов с изображением обнаженных людей, половых органов и актов, вовсе не обязательно образуют признаки анализируемых составов преступлений. Это зависит от формы, мотивов и целей таких действий.

Например, такие беседы, предметы, фото или видео материалы могут предоставляться несовершеннолетним в воспитательно-просветительских, научных, медицинско-профилактических целях, либо обладать эстетической, исторической, художественной или культурной ценностью.

Также должны исключать уголовную ответственность провокационные действия сотрудников правоохранительных органов или близких несовершеннолетних потерпевших, поддерживающих переписку с целью искусственного создания доказательств противоправной деятельности лица.

Выявляются подобные преступления, чаще всего, следующим образом:

– в правоохранительные органы с заявлением обращаются родители (законные представители) несовершеннолетних (реже сами пострадавшие);

– оперативно-разыскным путем (хотя специализированных подразделений по данной категории преступлений в стране пока нет);

– следственным путем в ходе расследования аналогичных дел и раскрытия новых эпизодов в отношении одного и того же потерпевшего или иных потерпевших;

– явка с повинной преступника (чаще также в ходе расследования иного аналогичного преступления).

При этом *исходные следственные ситуации* могут складываться по-разному (в зависимости от этого планируется и ход расследования):

– преступление очевидное, преступник установлен, задержан и дает признательные показания (бесконфликтная ситуация);

– - преступление очевидное, преступник установлен, задержан, но вину отрицает либо не дает никаких показаний в соответствии со ст. 51 Конституции РФ (конфликтная ситуация);

– преступление очевидное, преступник установлен, но не задержан;

– преступление неочевидное, преступник не установлен;

– есть сомнения в наличии события или состава преступления.

Основу доказательств по развратным действиям с использованием сети Интернет составляют:

– непосредственно сами дистанционные (бесконтактные) развратные действия виновного, а именно переписка в социальных сетях и мессенджерах; фотографии и видеоматериалы сексуального характера, устные беседы по телефону при помощи сотовой связи или GPRS-сессии (показания обвиняемого, потерпевшего, свидетелей; протоколы осмотра социальных страниц, смартфонов, компьютеров, CD-дисков с перепиской, фото- и видеофайлами);

– заключения судебных речеведческих (лингвистической, автороведческой, фоноскопической) экспертиз по представленной электронной переписке, аудиовидеозаписям преступника, подтверждающие их развратное содержание со стороны конкретного субъекта: циничный, вульгарный, непристойный характер сексуального содержания, направленность на возбуждение у потерпевшего извращенного интереса к половым отношениям;

– заключение психолого-психиатрической экспертизы потерпевшего, подтверждающее общественную опасность деяния, а именно негативное влияние действий преступника на нормальное психическое, нравственное и половое развитие ребенка, степень причиненного вреда.

Следы преступлений. Как и по другим преступлениям, которые совершаются с помощью информационно-коммуникационных технологий, основными следами их подготовки, совершения и сокрытия являются *цифровые следы:*

- сам факт использования компьютера (смартфона), имеющего выход в сеть Интернет в установленные временные промежутки (MAC (физический) адрес данных устройств, маршрутизатора, через который раздается сеть WI-FI или EMAI смартфона, марка, модель устройств, IP используемый в момент выхода с сеть);

- цифровые фото, видеофайлы (их метаданные) обнаженных частей тел жертвы, преступника (возможно изображение его лица) или посторонних людей, направленные потерпевшему или подозреваемому, часто сделанные смартфоном или камерой ноутбука (планшета) участников уголовного судопроизводства или иным устройством;

- текстовые (печатные) или аудиовидеосообщения развратного содержания в мессенджерах и социальных сетях (*речевые следы* в виртуальном пространстве);

- ID-адрес личной страницы пользователя, время и IP-адрес регистрации профиля, номер мобильного телефона, адрес электронной почты, история смены имени пользователя и прикрепленного номера мобильного телефона, время и IP адрес размещения определенного контента, история и перечень IP-адресов для входа на страницу;

- транзакции денежных переводов;
- биллинги телефонных соединений и GPRS сессий между потерпевшим и преступником или иными лицами, их детализация;
- установление места локации – нахождения цифровых устройств участников уголовного процесса с помощью базовых станций операторов связи, GPS, ГЛОНАСС модулей или зоны покрытия WI-FI сети;
- записи с видеокамер (реже)[1].

Материальными следами могут выступать биологические (следы спермы, потожировые, ДНК, запаховые следы); следы пальцев рук, ладоней на периферийных устройствах или экране гаджета; микроволокно одежды подозреваемого на компьютерном стуле и т.д.

Самыми распространенными конечно же выступают *идеальные* следы – показания потерпевшей, свидетелей, специалистов, экспертов и подозреваемого. Свидетелями по таким делам могут выступать не только близкие потерпевшего (родители, бабушки, дедушки, братья, сестры, друзья), но и их педагоги, медицинский персонал, психолог, к которому пришлось обращаться за помощью и консультацией и др. Со стороны подозреваемого свидетелями могут быть также его родственники, коллеги по работе, знакомые, врачи, сотрудники правоохранительных органов, раскрывшие преступление и др.

Непосредственно выявить и идентифицировать лицо, совершившее данные преступления достаточно сложно. Это возможно при визуальном или голосовом контакте подозреваемого и жертвы (путем предъявления для опознания). Также этому способствует автороведческая экспертиза по печатной речи (при наличии достаточного для исследования количества свободных или условно-свободных образцов печатного текса, выполненного преступником).

На стадии процессуальной проверки, когда необходимо, во-первых, проверить основания для возбуждения уголовного дела, а именно наличие достаточных данных, указывающих на признаки преступления, а во-вторых, определиться с верной его уголовно-правовой оценкой и изучением личности потерпевшего (множественность преступной деятельности, состояние ребенка, возможность правильно воспринимать окружающую действительность, степень причиненного вреда, и др.), *необходимо провести:*

Подробный опрос несовершеннолетнего потерпевшего и его родственников, иных осведомленных лиц по факту (фактам) произошедшего.

Осмотр смартфона, компьютера потерпевшего (социальных сетей и мессенджеров) на предмет обнаружения текстов, фото- и видеофайлов, подтверждающих развратные действия виновного, а также установления точного времени начала-окончания и количества сессий общения.

Осмотры или экспертные исследования самих фотографий или видеофайлов (их метаданных) позволяют порой установить марку и модель устройства с

[1] Цифровые следы преступлений: монография / Багмет А.М. и др. М.: Проспект, 2023. С. 76.

помощью которого они изготовлены, дату и время их создания, а главное – координаты (широту и долготу) места, где они были сделаны. Причем их копирование может привести к утрате столь значимых для следствия улик. Обнаруженные в чатах печатные тексты являются ценными образцами для лингвистической и автороведческой экспертиз.

Осмотр места происшествия (жилища потерпевшего, а в частности его комнаты, рабочего (компьютерного) места, где производилась коммуникация с преступником, самого компьютера, с обязательным изъятием последнего, а также изъятием смартфона и иных устройств, с помощью которых производилась связь).

Если развратные действия продолжались короткий период времени и переписка, фото, видеоматериал, подтверждающий наличие признаков преступлений представлен на устройстве несовершеннолетним пользователем – изымать их не обязательно. В таком случае такие цифровые доказательства фиксируются с помощью скрин-шотов (фото экрана электронного устройства), фотографируются с помощью фотокамеры следователя, о чем в протоколе осмотра места происшествия делается подробная запись, а фотографии и (или) скрин-шоты прикрепляются к нему или размещаются в описательной части с соответствующими пояснениями.

В ходе данного следственного действия целесообразно изымать одежду, в которой находилась жертва в момент коммуникации с преступником на предмет предъявления для опознания им в бесконфликтной ситуации, а также возможного экспертного исследования на поиск биологических следов, связанных с сексуальным возбуждением потерпевшего.

Назначение судебной лингвистической экспертизы по печатной речи (переписке), фото и (или) видеофайлам на предмет установления признаков развратных действий, а также комплексной психолого-психиатрической экспертизы несовершеннолетнему потерпевшему для определения его состояния, в том числе на момент совершения преступления, степени причиненного вреда, его психологических особенностей развития и характера, которые необходимо учитывать при последующих беседах и следственных действиях с его участием.

После вынесения постановления о возбуждении уголовного дела примерный *алгоритм деятельности следователя* может быть следующим:

Допрос потерпевшего, его родственников.

Выемка смартфона или планшета, с помощью которого жертва осуществляла коммуникацию развратного содержания с подозреваемым.

Запросы в администрацию социальных сетей (без судебного решения) на предмет установления информации о подозреваемом: адрес личной страницы, время и IP-адрес регистрации его в сети, номер его мобильного телефона; время и IP-адрес размещения конкретного контента; историю смены аккаунтов, IP-адресов для входа на страницу; MAC адреса оконечного оборудования и др.

Допросы свидетелей (подруг, друзей, родственников, классного руководителя, медицинских работников, сотрудников IT, сотовых компаний, провайдеров сети

Интернет, понятых, экспертов, а также специалистов лингвистов или искусствоведов в случаях, когда переписка носит явно сексуальный характер).

Поручение органу дознания на проведение следственных действий и оперативно-разыскных мероприятий, направленных на установление, розыск и задержание подозреваемого; изъятие устройств, с помощью которых подозреваемый совершал развратные действия; выяснение IP-адресов интернет сессий преступник-жертвы; выявление и обыски в местах совершения преступлений; установление личностей иных пострадавших от действий подозреваемого и их допрос; изъятие (экспорт) чатов или всего архива переписок в социальных сетях, мессенджерах (с помощью специальных программ, администрации или самостоятельно) и др.

Допрос подозреваемого.

Обыск в жилище подозреваемого (в ходе обыска следует производить поиск, фиксировать и изымать все компьютеры, смартфоны, телефоны иные электронные устройства и внешние накопители памяти; договоры на Интернет-услуги, роутер; его одежду; блокноты, журналы, книги, фотографии и видео файлы (диски, кассеты) порнографического и сексуального содержания).

Осмотр компьютера, смартфона, социальных сетей и мессенджеров подозреваемого.

Допросы свидетелей (совместно проживающих с подозреваемым, супругов, детей, иных родственников, друзей, знакомых, коллег по работе, лечащих врачей и др.).

Выемка в администрации социальных сетей (мессенджеров) и последующий осмотр электронных или иных сообщений, передаваемых по сетям электросвязи (ч. 7 ст. 185 УПК РФ).

Назначение экспертиз, в том числе комплексных (сексолого-психолого-психиатрическую подозреваемому; фоноскопическую; портретную; компьютерно-техническую; искусствоведческую; автороведческую и др.).

Назначением допроса потерпевшего ребенка (также как и свидетелей) является получение достоверных сведений о произошедшем событии с целью сбора неопровержимых доказательств виновности (невиновности) подозреваемого. Для этого необходимо:

– подтвердить (или опровергнуть) наличие в действиях виновного объективных и субъективных признаков всех, совершенных в отношении несовершеннолетнего преступлений;

– выяснить все самостоятельные эпизоды совершенных преступлений (даты, время и количество сессий);

– установить всех свидетелей (очевидцев) преступления и в последующем допросить и их;

– установить личности других потерпевших для их последующего допроса и признания потерпевшими;

– выяснить полную следовую картину произошедшего с целью обнаружения и последующего изъятия материальных следов, а также планирования

последующих следственных действий (предъявления для опознания, обыска, повторного осмотра места происшествия, предметов, документов, выемки и др.).

Значительно облегчает допрос предварительная формулировка и верная последовательность вопросов, которые необходимо обязательно отразить в протоколе исходя из конкретной следственной ситуации.

По рассматриваемым преступлениям примерный перечень вопросов должен быть следующим:

– какие цифровые устройства использовал потерпевший для связи с подозреваемым;

– пользуется ли кто-либо еще данными устройствами, кроме потерпевшего;

– какие социальные сети и (или) мессенджеры, компьютерные игры (иное) использовал для общения с подозреваемым;

– какой провайдер представляет услуги доступа к сети Интернет;

– каким образом осуществлялся выход в сеть Интернет (мобильный Интернет или путем использования сети WI-FI с помощью маршрутизатора);

– с какого времени зарегистрирован в социальной сети и под каким именем;

– один или несколько аккаунтов имеет потерпевший;

– с каких аккаунтов происходило общение с преступником;

– какие данные о себе указывал при регистрации (пол, возраст, дату рождения, класс, фото);

– при каких обстоятельствах и когда произошло знакомство с преступником, под каким именем (именами) он осуществлял переписку, кем представился, что сообщил о себе, роде своей деятельности и месте проживания, возрасте;

– какую информацию о себе сообщил потерпевший подозреваемому в ходе общения посредством сети Интернет;

– видел ли потерпевший лицо или части тела подозреваемого при дистанционном общении, слышал ли его голос;

– какова общая продолжительность общения потерпевшего с преступником в социальной сети (дни, месяцы, несколько лет), в какие дни и время оно осуществлялось;

– какие действия подозреваемый просил или требовал выполнять потерпевшего;

– каким образом (обещания, угрозы и др.) преступник склонил потерпевшего к демонстрации своего тела в обнаженном виде, производил ли при этом фото (видео) фиксацию;

– по какой причине потерпевший выполнил указанные действия;

– где находился потерпевший, когда переписывался с подозреваемым;

– кто, помимо потерпевшего, находился в указанном помещении, кто видел переписку потерпевшего с подозреваемым;

– осуществлялась ли в ходе переписки пересылка каких-либо фото (видео) материалов, каково их содержание;

– направлял ли преступник фото или видео с изображенными на них половых органов и действий порнографического (эротического) содержания;

– сохранялась ли потерпевшим переписка с преступником в социальной сети или была удалена, сохранились ли присланные им фото (видео) файлы;

– кому и когда потерпевший сообщал о совершенном преступлении.

В некоторых ситуациях *могут быть эффективными также такие следственные действия*, как:

– освидетельствование актуально в ситуациях, когда необходимо обнаружить на теле подозреваемого или потерпевшего и сопоставить с выявленными на фотографиях или видеозаписях особые приметы или индивидуальные физиологические особенности организма (татуировки, шрамы, родимые пятна, родинки, вены и пр.), либо, когда потерпевший наносил себе на теле по требованию преступника какие-либо рисунки, татуировки, телесные повреждения;

– получение информации о соединениях между абонентами и (или) абонентскими устройствами (с целью установления даты, времени, типа соединений преступника и жертвы; мест нахождения их смартфонов и, следовательно, их самих относительно зоны покрытия базовых станций и др.);

– следственный эксперимент (для определения зоны покрытия сети WI-FI, базовых станций сотовых операторов; возможности использования нейро сетей, программирования или элементарной регистрации и оплаты через цифровые платформы);

– очная ставка между показаниями участников уголовного судопроизводства при наличии существенных противоречий (в тоже время данное следственное действие между пострадавшим ребенком и преступником проводить не целесообразно по этическим и психологическим соображениям);

– предъявление для опознания в ситуациях, когда жертва видела (или слышала голос) подозреваемого, запомнила предметы его одежды, либо, наоборот, когда сам подозреваемый дает признательные показания и желает опознать жертву, ее одежду, смартфон и другие предметы.

Список источников

1. Иващенко М.А. Расследование преступлений против половой неприкосновенности и половой свободы несовершеннолетних, совершенных с использованием сети Интернет: практическое пособие. М.: Московская академия СК России, 2022. 100 с.

2. Информационные технологии в уголовно-правовой сфере: монография / под ред. А.И. Бастрыкина, А.Н. Савенкова. М.: ЮНИТИ-ДАНА, 2023. 279 с.

3. Цифровые следы преступлений: монография / Багмет А.М. и др. М.: Проспект, 2023. 168 с.

В.В. Спивак[1], **Л.А. Артамонова**[2]
[1, 2] СУ СК России по Ставропольскому краю

Использование информационных технологий в совершении преступлений как обстоятельство, отягчающее наказание

Аннотация. В настоящее время из-за быстрорастущей цифровизации населения, большая часть преступлений, в основной массе против собственности, совершается именно с использованием информационных технологий, с помощью которых лица совершившие преступления получают доступ к той или иной информации потерпевшего либо к его имуществу.

Ключевые слова: нейросеть, подмена голоса, мошенничество, личные данные, криптовалюта, дроп».

В современных тенденциях развития общества и государства в настоящее время особую актуальность обретают современные компьютерные и информационные технологии, что, несомненно, облегчает многие потребности указанных субъектов. Вместе с тем указанные технологии также активно внедряются преступными элементами, поскольку использование компьютерной техники и специализированных компьютерных программ снижают оперативность и возможность выявления лиц, совершивших преступление, а также позволяет использовать компьютерные технологии лицами, совершающими преступление, как универсальное орудие преступления по однотипной выработанной схеме.

Особо важная роль информационной безопасности в жизни государства, общества и личности требует от неё, чтобы преступные посягательства на неё рассматривались как деяние, несущее в себе прямую угрозу национальной безопасности Российской Федерации и взаимоотношений личности и государства.

В сети Интернет активно создаются ресурсы, позволяющие пользователям свободно посещать их, а также без предварительной регистрации и подтверждения данных бесконтрольно совершать незаконные сделки с оружием. Зачастую продавцы оружия в сети Интернет используют шифровальные программы, которые позволяют скрывать следы преступления и обеспечивать полную анонимность участников сделки. Оплата по сделкам также происходит «обходными путями» с помощью электронных денежных средств, криптовалюты, поддельных платежных аккаунтов и т.д.[1]

Данные обстоятельства указывают на повышенную социальную опасность, что в свою очередь должно побудить законодателя и правоприменителей к

[1] Каримов В.Х. Влияние современных информационно-телекоммуникационных технологий на криминальный оборот огнестрельного оружия и боеприпасов // Право и политика. 2019. № 1. С. 43.

пересмотру подхода к назначению наказаний лицам, совершившим преступление с использованием информационных технологий.

Таким образом, целью настоящей научной работы выступает обоснование проблемы использования информационных технологий при совершении преступлений и назначения наказания при вынесении процессуальных решений по уголовным делам указанной категории.

Правовой природой обстоятельств, отягчающих наказание, выступает с одной стороны, то что они охватывают распространенные и актуально-проблемные в конкретном временном или историческом промежутке обстоятельства совершенных преступлений, и поэтому наиболее типичны для различных случаев совершения преступлений, а с другой, включение их законодателем в перечень тех обстоятельств, которые оказывают значительное влияние на степень общественной опасности совершенного преступления и личность виновного[1].

Ярким примером природы возникновения обстоятельств, отягчающих наказание, может служить введение в ст. 63 Уголовного кодекса Российской Федерации новых пунктов «т» и «у», согласно которым совершение умышленного преступления с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет) и совершение преступления лицом, незаконно находящимся на территории Российской Федерации, признаны как обстоятельства отягчающие наказание[2], что указывает на особую проблему совершения преступлений при указанных обстоятельствах в современном российском обществе. По нашему мнению, использование IT-технологий также находится в одном ряду с уже учтенными законодателем новыми признаками.

Российские законодатели в 2024 году вносили проекты изменений в Уголовный кодекс Российской Федерации, предлагая дополнить ряд статей квалифицирующими признаками преступлений, связанными с применением информационных технологий[3]. Однако, думается, что данные технологии выступают лишь средством (способом) совершения преступлений, и сами по себе не меняют состав преступления (его объект-объективную и субъект-субъективную сторону), а также, что такого рода изменения только усложнят правоприменительную практику, препятствуя её единому и правильному применению.

Вместе с тем, анализ диспозиций некоторых статей Уголовного кодекса Российской Федерации, от преступлений против личности и собственности до

---

[1] Ревин В.П. Уголовное право России. Общая часть: Учебник. М.: Юстицинформ, 2016. С. 405-406.

[2] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 28.12.2024) (с изм. и доп., вступ. в силу с 08.01.2025) // СПС КонсультантПлюс.

[3] Законопроект № 718538-8 О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности). URL: https://sozd.duma.gov.ru/bill/718538-8.

преступлений против общественной безопасности и человечества, указывает на то, что положение отягчающие наказание с использованием информационных технологий может быть применено к значительной части статей Уголовного кодекса Российской Федерации.

Также в действующем Уголовном кодексе Российской Федерации имеется достаточно обширный ряд статей, в которых имеется квалифицирующий признак преступление «с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, который также можно поставить в один ряд к информационным технологиям, что еще раз подтверждает особую социальную опасность таких преступлений со стороны законодателя.

Согласно представленной статистики МВД России, за 10 месяцев 2024 года, 60% в общем количестве всех преступлений из числа тяжких и особо тяжких в отношении граждан Российской Федерации было совершено с использованием информационных технологий[1]. При этом, анализируя практику подобных преступлений, большая часть из них остается латентными либо не раскрытыми, то есть лицо, подлежащее привлечению в качестве обвиняемого, не установлено.

Исходя из практики совершения указанных преступлений на территории Ставропольского края, в частности в г. Невинномысске, все они связаны с хищением собственности, путем введения в заблуждение, а потерпевшей стороной, в более 80 % случаев являются пожилые люди, старше 50 лет.

Основными способами совершения преступлений являются телефонные звонки с использованием специализированных программ для подмены голоса, наложения звуковых эффектов, подмены номера телефона звонящего, а также нейросети, позволяющей осуществить подмену лица по заранее полученной фотографии родственника жертвы преступления. При этом, в целях упрощения совершения преступления, а также в целях сокрытия следов его совершения, преступники также заранее получают с использованием информационных технологий данные о потерпевшем, а именно: фамилия, имя и отчество; возраст, место жительства, семейное положение; полные данные их родственников и все имеющиеся контактные телефоны. В дальнейшем, лица, совершающие преступление, подыскивают себе сообщников для совершения данного преступления, которыми чаще всего выступают несовершеннолетние лица, которым они предоставляют роль курьеров и так называемых «дропов».

Слово «дроп» произошло от английского глагола *to drop*, что переводится как *сбрасывать*, а в российском Интернет-сообществе понимается, как лицо, предоставляющее свой банковский счет для обналичивания и сокрытия денежных средств добытых преступных путём.

При этом, как показывает анализ совершенных преступлений, в основной массе они совершены с территории Украины, в которой любая подрывная

[1] Краткая характеристика состояния преступности в Российской Федерации за январь-октябрь 2024 года представленная на официальном сайте Министерства внутренних дел Российской Федерации. URL: https://xn--b1aew.xn--p1ai/reports/item/57279296/ (дата обращения 08.01.2025).

деятельность, в том числе и экономическая, направленная против Российской Федерации, возведена фактически в государственную идеологию.

Все вышеуказанные обстоятельства совершения преступлений указывают на: актуализацию усиленной борьбы против них; их особую специфику, выраженную в разработке и применении новых информационных технологий, так как от них страдают не только социально незащищенные слои населения, которые в наименьшей степени осведомлены о таких технологиях и принципах их работы, а также что для их совершения привлекаются несовершеннолетние лица, что также в дальнейшем отражается на их судьбе негативным образом.

Уголовный закон содержит в себе исчерпывающий перечень обстоятельств отягчающих наказание, в частности п. «к» ч. 1 ст. 60 УК РФ признает одно из обстоятельств – совершение преступления с использованием оружия, боевых припасов, взрывчатых веществ, взрывных или имитирующих их устройств, специально изготовленных технических средств, наркотических средств, психотропных, сильнодействующих, ядовитых и радиоактивных веществ, лекарственных и иных химико-фармакологических препаратов, а также с применением физического или психического принуждения[1]. Данное обстоятельство очень близко по смыслу к применению информационных технологий при совершении преступления.

Анализируя вышеизложенное, по нашему мнению, в новой редакции Уголовного кодекса Российской Федерации необходимо расширить п. «к» ч. 1 ст. 63 УК РФ, дополнив его указанием на «совершение преступления с использованием информационных технологий».

Список источников

1. Законопроект № 718538-8 О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности). URL: https://sozd.duma.gov.ru/bill/718538-8.

2. Краткая характеристика состояния преступности в Российской Федерации за январь-октябрь 2024 года представленная на официальном сайте Министерства внутренних дел Российской Федерации. URL: https://xn--b1aew.xn--p1ai/reports/item/57279296.

3. Каримов В.Х. Влияние современных информационно-телекоммуникационных технологий на криминальный оборот огнестрельного оружия и боеприпасов // Право и политика. 2019. № 1.

5. Ревин В.П. Уголовное право России. Общая часть: Учебник. М.: Юстицинформ, 2016.

[1] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 28.12.2024) (с изм. и доп., вступ. в силу с 08.01.2025) / СПС КонсультантПлюс.

А.В. Ткачев
Московский государственный университет
имени М.В. Ломоносова

Об использовании вероятностных выводов компьютерных систем в доказывании

Аннотация. В статье рассматриваются вопросы, связанные с использованием вероятностных выводов компьютерных систем в доказывании по уголовным делам. Представлены основные позиции, сформулированные в отечественной литературе о возможности использования вероятностного знания в правоприменительной практике. Рассматриваются особенности оценки результатов работы автоматизированных систем с точки зрения потребностей правоохранительных органов. Высказаны рекомендации о включении вероятностных выводов в систему доказывания, в том числе и использовании их в качестве доказательств.

Ключевые слова: криминалистика, доказывание, компьютерные системы, преступления, экспертиза, вероятностные выводы.

Проблематика использования вероятностного знания в доказывании занимает достаточно важное место в отечественной криминалистике и уголовном процессе. Данная проблематика многоаспектна и затрагивает целый спектр вопросов, например, построения и оценки криминалистических версий, оценки «веса» доказательств и на этой основе предложений об объективизации процесса доказывания. В настоящей статье будут рассмотрены вопросы использования результатов применения вероятностных методов при реализации специальных знаний в уголовном судопроизводстве.

В современных условиях эти вопросы приобрели особую актуальность в связи с повсеместным использованием компьютеризированных систем для обработки информации, включая принятие ими решений на основе такой обработки. При этом функционирование значительной части автоматизированных систем основано на использовании тех или иных приложений теории вероятности. В частности, системы видеонаблюдения и установления личности, иные биометрические системы, системы анализа поведения личности на основе работы с компьютерными устройствами и цифровой информацией и другие. Результаты деятельности таких систем стали постоянно использоваться в правоприменительной практике.

К сожалению, как показывает практика, определенная часть сотрудников правоохранительных органов не обладает необходимыми знаниями для корректной оценки степени вероятности, содержащихся в выводах машинных систем.

Таким образом, проблема использования в уголовном судопроизводстве вероятностных выводов, подготовленных машинными системами, приобрела самостоятельный характер.

Кратко остановимся на основных позициях, сформировавшихся в криминалистике, в отношении применении вероятностных методов при использовании специальных знаний в следственной и судебной практике. Предварительно представляется важным выделить два момента. Во-первых, надо отметить, что эти позиции были сформулированы в процессе изучения использования вероятностных методов главным образом при проведении экспертных исследований. В результате основной темой исследований была проблема использования вероятностных выводов эксперта в доказывании. Во-вторых, поскольку в экспертизах до середины 90-х годов XX века преобладали качественные методы, то вероятностные выводы в экспертизах во многом не имели точного количественного выражения и базировались на экспертном опыте, «несчитанной статистике», в определенной степени интуиции.

При разнообразии оригинальных и многообразных взглядов исследователей на проблему допустимости использования вероятностного экспертного вывода, думается их можно свести к двум господствующим точкам зрения.

Сторонники первой позиции исходили из того, что вероятностные выводы экспертов не могут использоваться в качестве доказательств, поскольку они являются недостоверным знанием. Данную точку зрения разделяли М.С. Строгович, В.А. Притузова, В.Д. Арсеньев, Т.В. Аверьянова и другие. Очень точно эта позиция была сформулирована Т.В. Аверьяновой: «Говоря о вероятности и достоверности в заключении эксперта, мы исходим из того, что в первом случае истина не достигнута, во втором, наоборот, достигнута. Вероятности предшествует недостаточно полное, обоснованное знание, а достоверности, наоборот, полное обоснованное знание, исключающее всякие сомнения и возможность построения противоположного заключения, опираясь на те же самые основания»[1].

В противоположность вышеуказанной точки зрения многие ученые считали, что вероятностные экспертные выводы могут использоваться в доказывании и в качестве доказательств, и как ориентирующая информация в поисковой деятельности следственных и оперативно-разыскных органов. Данную позицию поддерживали А.И. Винберг, В.Ф. Орлова, В.Я. Колдин, А.Р. Шляхов и другие. Представители данной точки зрения полагали, что существуют объективные основания для выдвижения вероятностных выводов, и знания, которые привели эксперта к такому результату, являются достоверными, но не позволяющими сделать вывод о конечном результате как достоверном.

В то же время авторы, разделявшие указанную позицию, утверждали, что не всякий вероятностный вывод может быть включен в систему доказательств по уголовному делу. В качестве доказательств могут приниматься только те вероятностные экспертные заключения, которые очень близки к достоверным (категорическим) заключениям. В.Ф. Орлова указывала, что вероятность в идентификационном экспертном исследовании должна быть очень высокой

[1] Аверьянова Т.В. Судебная экспертиза. Курс общей теории. М.: Норма. 2006. С. 334.

«порядка 10^{-9} при доверительном уровне 10^{-10}»[1]. В.Я. Колдин отмечал, что «при надежности вывода 0,9999, т.е. приближающейся к 1 (достоверному), дается категорическое заключение, а при надежности 0,98- вероятное заключение. При более низких показателях надежности методики экспертизы предписывают отказ от дачи заключения. Таким образом, вероятное заключение дается при достаточно высоком уровне надежности вывода, граничащего с надежностью категорического заключения»[2]. Применительно к идентификационным исследованиям вероятность рассматривалась рядом ученых как неполное достижение тождества и установление более или менее узкой группы. Такие взгляды высказывали А.И. Винберг, В.С. Митричев, Р.С. Белкин и другие. Р.С. Белкин писал: «Тождество означает, только то, что объект является тем же самым. Всякая вероятность этого – не что иное как отнесение объекта к более или менее узкой по объему группе подобных: чем уже группа, тем выше «степень отождествления» объекта, однако в любом случае это еще не тождество, а установление групповой принадлежности. Тождество степеней не имеет, оно либо есть, либо его нет»[3].

В правоприменительной практике до 2010 г. важнейшим документом, регулирующим рассматриваемую проблему, было постановление Пленума Верховного Суда СССР от 16 марта 1971 г. № 1 «О судебной экспертизе по уголовным делам». В п. 14 данного постановления указывалось: «Обратить внимание судов на то, что вероятное заключение эксперта не может быть положено в основу приговора»[4].

Буквальное прочтение этого пункта показывает, что высший судебный орган страны не запрещал полностью использовать вероятное экспертное заключение в доказывании, однако считал невозможным постановить судебное решение, основываясь на нем как на решающем доказательстве.

В литературе и на практике трактовка данного положения постановления Пленума Верховного Суда СССР была весьма разнообразной: от понимания его как полного запрета на использование вероятного заключения эксперта как доказательства (особенно в 70-80-х годах XX века), до признания допустимости включения такого заключения вместе с другими доказательствами в систему доказательств по делу, в том числе и в процессуальные документы, содержащие итоговые выводы по уголовному делу, при условии, что такое заключение не являлось решающим доказательством.

Начиная с середины 90-х годов XX века указанный вывод Пленума Верховного Суда СССР приходит в противоречие с процессом внедрения в экспертную практику методик, полностью или в значительной части основанных на применении вероятностных количественных методов, и широким

---

[1] Орлова В.Ф. Теория судебно-почерковедческой идентификации. Труды ВИИИСЭ. Выпуск 6. М. 1973. С. 299.

[2] Колдин В.Я. Судебная идентификация. М.: ЛексЭст. 2002. С. 199–200.

[3] Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. Общая и частная теория. М.: Юридическая литература. 1897. С. 205.

[4] Бюллетень Верховного Суда СССР. № 2. 1971.

использованием их в уголовном судопроизводстве. Наиболее наглядным примером является, конечно, ДНК-идентификация. Такое заключение эксперта во многих случаях является решающим доказательством, устанавливающим причастность лица к совершенному преступлению. Вывод же в такой экспертизе всегда является вероятностным, поскольку основан на частоте встречаемости генетических данных в человеческой популяции.

Закономерным выходом из такого противоречия стало отсутствие в Постановлении Пленума Верховного Суда РФ от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам» положений, ограничивающих использование вероятных заключений эксперта[1].

Следовательно, в настоящее время применение вероятных заключений эксперта в доказывании, основанных на методиках исследования количественных свойств объектов с помощью вероятностных методов, вполне допустимо с правовой точки зрения.

С научной точки зрения также представляется необоснованным рассматривать вероятные выводы как недостоверные в тех случаях, когда они получены при изучении объектов, природа которых позволяет проводить исследования, основанные на теории вероятности. Конечно, при корректности выбора и использования соответствующего математического аппарата и программного обеспечения. Впрочем, требование научности методов и средств экспертного исследования обязательно и при производстве экспертиз на основе качественных методов.

В то же время возникает проблема определения критериев допуска в уголовный процесс в качестве доказательств и вероятных экспертных заключений, и вероятных выводов, полученных иными автоматизированными системами, а также оценки их с точки зрения их доказательственной ценности. Особенно важным представляется установить степень допустимой вероятности.

В отношении экспертных заключений, по крайней мере в государственных экспертных учреждениях, проблема решается путем введения соответствующих пороговых критериев в методики, принятые в этих учреждениях. В некоторых случаях критерии степени вероятности, при которых эксперт вправе давать соответствующий вывод, установлены в подзаконных актах, регулирующих порядок производства таких экспертных исследований[2].

Иначе обстоит дело с использованием в правоприменительной практике вероятностных выводов, полученных при обработке данных компьютерными системами, не относящимися к правоохранительным органам и государственным экспертным учреждениям, назовем их внешними системами. В отношении данных систем в большинстве случаев отсутствуют правовые нормы, устанавливающие строгие критерии допуска выводов, полученных в результате работы таких систем, в качестве доказательств, на которые мог бы

[1] Российская газета. № 296. 30.12.2010.

[2] В отношении генетической экспертизы см. например, приказ Минздрава России от 25.09.2023 г. № 491н «Об утверждении Порядка проведения судебно-медицинской экспертизы». URL: http://pravo.gov.ru. 25.10.2023.

ориентироваться правоприменитель. В то же время нельзя требовать от субъекта доказывания при принятии решения об использовании их в доказывании полного анализа научности и обоснованности методов работы этих систем.

Однако представляется возможным, что субъект доказывания при решении о допуске выводов внешних систем в качестве доказательств может самостоятельно учитывать следующие обстоятельства.

Во-первых, надо правильно понимать цели, для которых создаются подобные системы и корректно интерпретировать их для решения процессуальных и криминалистических задач. Существуют системы, создаваемые для решения задач, которые можно с точки зрения криминалистики рассматривать как идентификационные, например, системы биометрической идентификации. Другие системы выполняют задачи, имеющие целью отнесение объекта к какой-либо группе или установления особенностей того или иного явления, процесса. Например, в банковских организациях широко внедряются различные программы, обрабатывающие цифровые данные пользователей, с целью выявление необычного их поведения при совершении банковских операций. С позиций криминалистики такие задачи рассматриваются как классификационные и диагностические. При этом разработчики программных комплексов, решающих последние задачи, в руководствах по их эксплуатации используют идентификационную терминологию в значении придаваемой ей в математике и информатике.

Необходимо избегать ошибок, когда вероятностная оценка «идентификации», принятая в указанных системах, т.е. возможность существования или протекания процесса или явления, может быть истолкована как идентификация лица, выполняющего данный процесс. В этом случае использование вероятностной оценки, даваемой соответствующей автоматизированной системой, будет в любом случае некорректно.

Во-вторых, внешняя компьютерная система может создаваться для решения локальной задачи, в процессе решения которой исследуется не вся генеральная совокупность объектов. Так, создаваемая биометрическая система идентификации в конкретной организации может быть рассчитана на ограниченный по численности коллектив. Следовательно, математический аппарат и алгоритм решения такой задачи может быть выбран, исходя из минимального количества признаков, необходимых для идентификации объектов, входящих в такую ограниченную совокупность. Думается, данная ситуация может рассматриваться как частный случай известной в криминалистике задачи, когда надо установить объект, о котором заранее известно, что он находится в анализируемом множестве объектов. В этом случае мы имеем дело с решением по сути классификационных задач, в большинстве случаев на основе математических методов распознавания образов[1].

При попытке распространить действие такого программного комплекса на решение задачи идентификации в множестве объектов, в котором неизвестно

1 Экспертная криминалистическая идентификация. Выпуск 2. Научный редактор проф. Колдин В.Я. М.: РФСЦЭ. 1996. С. 37–39.

находится ли искомый объект (эта задача более распространена в криминалистике, чем вышеуказанная задача), принятая степень вероятности в таком комплексе, обеспечивающая достоверность вывода, будет совершенно недостаточна для ее корректного решения. Поскольку в системе отсутствуют сведения о генеральной совокупности объектов, в том числе о частоте встречаемости исследуемых признаков в этой совокупности.

Кроме того, в некоторых ситуациях доказывания, могущих сложиться в ходе расследования, выводы системы, сделанные на основе соответствующей исследуемой ограниченной совокупности, должны быть проверены путем проведения судебной экспертизы. Например, при появлении в данной ограниченной совокупности объектов, нового объекта с признаками настолько близкими к уже имеющимся в ней объектам, что правило «ближайшего соседа», основанное на отграничении объектов друг от друга путем использования минимума отличий, не будет работать.

В-третьих, использование пороговых значений степени вероятности, содержащихся в выводах внешних компьютерных систем, при которых они могут быть признаны или доказательствами, или ориентирующей информацией.

Представляется, здесь в определенной степени необходимо ориентироваться на позиции, ранее выработанные в отношении вероятностных заключений эксперта. Однако при этом мы должны помнить, что эти позиции сформировались при оценке вероятностных заключений экспертов, когда использовались методики, основанные главным образом, на качественных методах, а также большое значение имело внутренне убеждение эксперта, его знакомство с материалами дела. С одной стороны, это позволяло признавать за такими заключениями статус доказательства, возлагая бремя их оценки на субъект доказывания, с другой стороны, очень сложно было формализовать субъективную часть знаний эксперта и, соответственно, сформулировать объективный количественный порог, при котором такое заключение имело доказательственный статус. Приведенные выше цифры, использованные в работах В.Я. Колдина, В.Ф. Орловой не основывались на конкретных количественных методиках, а отражали авторские теоретические подходы к приложению идей теории вероятности в криминалистике.

В отношении вероятностных выводов внешних компьютерных систем нельзя говорить о внутреннем убеждении лиц, создававших эти системы, тем более знания ими материалов конкретного дела. Степень вероятности таких выводов зависит от особенностей обрабатываемого множества объектов (выбор которого изначально никак не связан с расследуемым делом) и корректности используемого математического аппарата и программного обеспечения.

Следовательно, определяя возможность установления порогового значения степени вероятности выводов внешних автоматизированных систем необходимо исходить из максимально возможной в такой системе степени вероятности достигаемой при решении задачи, которая будет рассматриваться как достоверное знание. Надежность вывода должна вплотную приближаться к 1 – 0,9999… В этом случае такой вывод может рассматриваться как доказательство. Все, что ниже этого порогового значения, например, 0,9899…

может использоваться как ориентирующая информация в целях проверки, розыска и т. п.

Доказательственная ценность вероятного вывода внешней системы будет зависеть от объема множества объектов, в котором достоверно, те есть с вероятностью близкой к 1 будет решена задача. Например, объект может быть выделен с максимальной степенью вероятности в 1 000 случаев, 10 000 случаев, 100 000 случаев, 1 000 000 случаев и т.д. Доказательственную ценность вероятного вывода будет определять субъект доказывания исходя из конкретных обстоятельств расследуемого дела и генеральной совокупности объектов.

Отдельно хотелось бы остановиться на проблеме определения минимального порогового значения, при котором выводы внешних автоматизированных систем допустимо использовать в качестве ориентирующей информации. Представляется, такая необходимость назрела, т.к., к сожалению, и в отечественной, и в зарубежной практике уже существуют негативные примеры, когда на основе выводов, имеющих низкую степень вероятности, которые первоначально рассматривались как ориентирующая информация, в дальнейшем принимались необоснованные и неправомерные процессуальные и криминалистические решения. Одним из широко известных случаев стало проведение оперативно-разыскных и следственных мероприятий, а затем привлечения лица к уголовной ответственности на основании того, что биометрическая система идентификации лица по признакам внешности дала вывод о сходстве признаков внешности данного человека с фотороботом подозреваемого со степенью вероятности в 55 %[1].

Использование выводов с низкой степенью вероятности ведет к ошибочному привлечению к ответственности невиновных лиц, не установлению виновных в совершении преступления, напрасному расходованию ресурсов правоохранительных органов.

Таким образом, установление порогового значения степени вероятности выводов позволит избежать вышеуказанных ошибок и сосредоточиться на проверке действительно ценной информации.

Полагаем, что для установления объективного значения порогового критерия для ориентирующей информации целесообразно было бы провести исследование среди следователей, оперативных работников, экспертов, с достаточным опытом работы, имеющее целью выяснения их мнения. Это позволило бы обобщить опыт использования специалистами выводов внешних компьютерных систем, выявить их субъективную оценку надежности такого порога.

На первоначальном этапе пороговые значения степени вероятности выводов внешних автоматизированных систем, при которых они могли быть признаны доказательствами или использоваться в качестве ориентирующей информации, могли быть закреплены в ведомственных нормативных актах. В дальнейшем

[1] Зинин А.М. Дьяконова О.Г. Мышление человека и искусственный интеллект в аспекте сравнительного исследования внешнего облика человека по его изображениям. Эксперт- Криминалист. № 3. 2023. С. 2–5.

наиболее рациональным было бы закрепление такого критерия на уровне общеобязательного федерального нормативного документа.

Список источников

1. Аверьянова Т.В. Судебная экспертиза. Курс общей теории. М.: Норма, 2006. 480 с.
2. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. Общая и частная теория. М.: Юридическая литература, 1987. 272 с.
3. Зинин А.М. Дьяконова О.Г. Мышление человека и искусственный интеллект в аспекте сравнительного исследования внешнего облика человека по его изображениям // Эксперт-Криминалист. 2023. № 3. С. 2–5.
4. Колдин В.Я. Судебная идентификация. М.: ЛексЭст. 2002. 528 с.
5. Орлова В.Ф. Теория судебно-почерковедческой идентификации. М.: Труды ВИИИСЭ. Выпуск 6, 1973. 335 с.
6. Экспертная криминалистическая идентификация / Научный редактор проф. В.Я. Колдин. Выпуск 2. М.: РФСЦЭ, 1996. 261 с.

А.Н. Фролова
Московский университет МВД России имени В.Я. Кикотя

К вопросу о современных информационных технологиях, применяемых в судебном почерковедении

Аннотация. В статье рассматривается вопрос использования интеллектуальных систем в почерковедении как одного из направлений развития современных информационных технологий. Делается акцент на необходимости использования в экспертно-криминалистической деятельности наиболее современных достижений науки и техники. Описываются возможности использования ДСМ-метода для решения некоторых почерковедческих задач.

Ключевые слова: ДСМ-метод, интеллектуальная система, информационные технологии, почерковедение, судебная экспертиза, эксперт-почерковед.

История вопроса информационных технологий берет свое начало с появления первых примитивных вычислительных машин. Общеизвестно, что первые компьютеры были очень большими, а процесс пользования ими сложным. Например, условно считается, что создатель первого компьютера в России – Сергей Лебедев – создал малую электронную счетную машину (1948 г.) и она размещалась на площади 60 кв. м. Уже с 80-х годов XX века началась эпоха персональных компьютеров, которые в настоящее время преобразились как внешне, так и внутренне.

Сегодня информационные технологии являются неотъемлемой частью нашей жизни и широко используются, в том числе при проведении судебно-почерковедческих исследований. Это связано с различными факторами, в первую очередь с тем, что продукты информационных технологий уже прочно вошли в нашу повседневную жизнь и мы даже не задумываемся, используя их. Наряду с этим, это связано с определенными требованиями законодательства в области судебно-экспертной деятельности. Например, статья 4 Федерального закона от 31 мая 2001 г. № 73 ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации»[1] одним из принципов проведения судебно-экспертной деятельности провозглашает использование современных достижений науки и техники при проведении исследований, поэтому ученые в области судебной экспертизы должны при проведении исследовательских работ пользоваться средствами современных информационных технологий для получения новой полезной информации и последующего ее использования в практике проведения различных почерковедческих исследований.

Судебно-почерковедческая экспертиза является традиционным криминалистическим исследованием. Важно отметить, что ученые в области почерковедения всегда стремились использовать современные достижения науки и техники для решения исследовательских и практических задач, как диагностических, так и идентификационных. Почерковедение всегда развивалось и стремилось к поиску новых инструментов, которые могли бы стать «помощниками» эксперту-почерковеду.

Одной из наиболее актуальных тем в информационных технологиях сегодня является искусственный интеллект и интеллектуальные системы, являющиеся его частью. Под интеллектуальными системами понимают «технические или программные системы, способные решать задачи, традиционно считающиеся творческими, принадлежащие конкретной предметной области, знания о которой хранятся в памяти такой системы»[2].

Интеллектуальными системами признаются ДСМ-системы, основанные на ДСМ-методе[3], который был разработан и предложен В.К. Финном в 70-х годах XX века. Этот метод предоставляет возможность осуществлять интеллектуальный анализ данных в базах фактов с неполной информацией и находить в них эмпирические зависимости. Важной положительной чертой метода является то, что он позволяет не только выдвигать гипотезы, но и интерпретировать причины их выдвижения.

Вопросами использования ДСМ-метода в почерковедении занимались С.М. Гусакова, В.Ю. Федорович, В.В. Устинов, А.Н. Охлупина и другие. Его

---

[1] О государственной судебно-экспертной деятельности в Российской Федерации [Электронный ресурс]: №73-ФЗ от 31.05.2001 (действующая редакция от 22.07.2024). Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Поспелов Д.А. Толковый словарь по искусственному интеллекту. М.: Радио и связь, 1992. 256 с.

[3] Название «ДСМ-метод» образовано от инициалов британского философа, социолога и экономиста Джона Стюарта Милля (далее – ДСМ-метод).

использование применительно к почерковедению показало свои положительные результаты как при работе с рукописными записями, так и с подписями.

ДСМ-метод является перспективным методом современности. В почерковедении метод в настоящее время используется в исследовательских целях для решения диагностических и идентификационных задач. Основная задача интеллектуальной ДСМ-системы – извлечь скрытые, неявно содержащиеся данные из массива открытой информации. Этот процесс происходит при помощи специальных логических операций. В зависимости от типа исходных данных и задач, стоящих перед исследователями, логические операции могут меняться.

На базе этого метода в судебном почерковедении совместно со специалистами в области искусственного интеллекта разработана «интеллектуальная система автоматизированной поддержки научных исследований»[1]. Это «система специальных рассуждений, способных на основе анализа относительно небольшого массива почерковой информации устанавливать зависимости детерминистского характера, неявно содержащиеся в почерковедческих объектах, в целях проведения научно-исследовательской работы и решения конкретных задач судебно-почерковедческих исследований»[2].

Разработка такой системы обусловлена некоторыми потребностями экспертной практики, интеллектуальная ДСМ-система может усилить способности эксперта почерковеда и помочь в решении следующих задач:

- преодоление субъективизма в процессе выделения признаков почерковых объектов;
- оптимизация процесса исследования;
- решение конкретных идентификационных и диагностических задач;
- экономия временных ресурсов на проведение некоторых исследований;
- возможность получения новых исследовательских данных.

Возможность применения ДСМ-метода в почерковедении обусловлена характером структуры почерковедческих данных – им присущи качественные и количественные характеристики, что открывает возможности для использования системно-структурного подхода с применением компьютерных методов. Чтобы добиться положительных результатов при использовании интеллектуальных систем при работе с почерковедческими данными, необходимо строго следовать определенному алгоритму действий:

- правильно сформулировать цели и задачи работы;
- установить очередность выполнения действий;

---

[1] Гусакова С.М., Лапшина И.А., Охлупина А.Н. Идентификация подписи: постановка задачи и вариант решения с помощью интеллектуальной ДСМ-системы. Научно-техническая информация. Серия 2.: Информационные процессы и системы. 2018. № 8. С. 8–13; Гросс Е.Р., Гусакова С.М., Огорельцева Н.В., Охлупина А.Н. ДСМ-система психолого-почерковедческих исследований подписи. Научно-техническая информация. Серия 2: Информационные процессы и системы. 2020. № 10. С. 12–19.

[2] Охлупина А.Н. Теоретические, методические и организационно-тактические основы применения интеллектуальных систем в судебно-почерковедческом исследовании подписей: дис. ... канд. юрид. наук: 12.00.12. М., 2019. С. 12.

- выбрать соответствующие методы и инструменты;
- определить технические требования к используемому программному обеспечению;
- при необходимости осуществлять корректировку каждого этапа работы;
- провести проверку метода, обосновать его эффективность и целесообразность применения.

Отдельным важным этапом работы системы является этап, посвященный созданию языка описания признаков почерковых объектов. Система описания должна быть формализована. Наряду с этим, язык должен быть максимально понятен и привычен экспертам-почерковедам, поэтому за его основу взято традиционное описание признаков с использованием упрощенного варианта структурно-лингвистического подхода при помещении почерковых признаков в систему, что предполагает соблюдение некой иерархии в описании признаков. Эти правила описания дают возможность обратного восстановления признака объекта по описанию, т.е. почерковед по формализованному описанию признака в системе может его представить. При этом при относительной простоте схемы описания не утрачиваются части признаков, то есть информация об объекте полностью отражается в системе.

Применение интеллектуальной системы автоматизированной поддержки научных исследований при решении идентификационных и диагностических задач рекомендовано строго как дополнительный инструмент эксперта-почерковеда вместе с традиционными методиками исследования почерковых объектов. Ее применение способно позволить ученым в этой области успешно проводить подобные исследования в целях совершенствования теории данного вопроса и решения практических задач почерковедения, что впоследствии положительно отразится на предупреждении, раскрытии и расследовании преступлений.

Список источников

1. Гусакова С.М., Лапшина И.А., Охлупина А.Н. Идентификация подписи: постановка задачи и вариант решения с помощью интеллектуальной ДСМ-системы // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2018. № 8. С. 8–13.

2. Гросс Е.Р., Гусакова С.М., Огорельцева Н.В., Охлупина А.Н. ДСМ-система психолого-почерковедческих исследований подписи // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2020. № 10. С. 12–19.

4. Охлупина А.Н. Теоретические, методические и организационно-тактические основы применения интеллектуальных систем в судебно-почерковедческом исследовании подписей: дис. ... канд. юрид. наук: 12.00.12. М., 2019. 192 с.

5. Поспелов Д.А. Толковый словарь по искусственному интеллекту. М.: Радио и связь, 1992. 256 с.

А.Б. Шавловский
Московская академия Следственного комитета
имени А.Я. Сухарева

Цифровые следы как объекты судебных экспертиз в условиях противодействия киберпреступности

Аннотация. В данной статье рассмотрена предлагаемая различными авторами терминология, определяющая категорию «цифровой след» в криминалистике. Цифровые следы проанализированы не только как объекты компьютерно-технической экспертизы, но и как объекты других видов (родов) судебных экспертиз, в том числе имеющих комплексный характер. Сформулирован вывод о необходимости организации подготовки и обучения сотрудников правоохранительных органов методологическим основам работы с цифровыми следами, вопросам обеспечения информационной безопасности, современным возможностям судебно-экспертных исследований цифровых следов.

Ключевые слова: криминалистика, судебная экспертиза, цифровые следы, киберпреступление, компьютерная информация.

Изучение цифровых следов в аспекте их криминалистического значения в условиях продолжающегося роста преступлений, совершенных с использованием информационно-телекоммуникационных технологий, представляет особый научный интерес. Так, согласно официальной статистике[1] Министерства внутренних дел Российской Федерации, в 2024 году зарегистрировано на 13,1 % больше преступлений, совершенных с использованием информационно-телекоммуникационных технологий по сравнению с предыдущим годом. Несомненно, рост преступлений указанной категории обусловлен сложностью их расследования, необходимостью понимания механизма цифрового следообразования, а также освоения специальных навыков и знаний для работы с цифровыми следами. В связи с этим, для повышения эффективности раскрытия, расследования и предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в соответствии с положениями Указа Президента Российской Федерации от 07.05.2024 № 309[2] запланировано «создание системы эффективного противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных

[1] Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2024 года. МВД России: [офиц. сайт]. URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 25.01.2025).

[2] Указ Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года». URL: http://publication.pravo.gov.ru/document/0001202405070015 (дата обращения: 27.01.2025).

технологий, и снижения ущерба от их совершения» в рамках национальной цели «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы».

Сегодня существуют различные концепции определения следов, оставляемых пользователем при работе в компьютерных системах и цифровых устройствах. Так, В.Б. Вехов и ряд других ученых выделяют понятие «цифровой след», который определяют как «любую криминалистически значимую компьютерную информацию, т.е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[1]. Себякин А.Г. предлагает след в компьютерной системе именовать как «электронно-цифровой след и определять его как, компьютерные данные, содержащие криминалистически значимую информацию о событиях или действиях, отражённые в материальной среде»[2]. В то же время А.А. Бессонов отмечает, что электронными следами является «информация, зафиксированная в цифровом формате, содержащаяся в электронно-вычислительных машинах и иных цифровых устройствах, созданных на основе их технологий, в средствах подвижной радиотелефонной связи и на различных носителях цифровой информации, причинно-связанная с событием преступления, позволяющая установить обстоятельства совершенного преступления и преступника»[3].

В нашем понимании термины «цифровые следы», «электронно-цифровые следы», «электронные следы» по своей сущности являются синонимами и с точки зрения криминалистики представляют компьютерную информацию, имеющую значение для расследования уголовного дела. При этом, по своей природе, компьютерная информация не может существовать самостоятельно без электронного носителя, а для ее интерпретации требуются специальные средства – программное обеспечение. Как отмечают Е.Р. Россинская, И.А. Рядовский, отличительным свойством цифровых следов является «невозможность восприятия непосредственно органами чувств, а только с помощью специальных устройств и программ»[4].

Традиционно вопросы экспертного исследования цифровых следов входили в компетенцию компьютерно-технической экспертизы, объектом которой,

---

[1] Цифровая криминалистика: учебник для вузов / В.Б. Вехов [и др.]; под ред. В.Б. Вехова, С.В. Зуева. 2-е изд., перераб. и доп. М.: Юрайт, 2025. С. 97.

[2] Себякин А.Г. Механизм следообразования в компьютерных системах с точки зрения теории отражения // Сибирские уголовно-процессуальные и криминалистические чтения. 2021. № 2(32). С. 94.

[3] Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 3(55). С. 47.

[4] Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: матер. междунар. науч.-практ. конф., Алматы, 19 февраля 2019 года. Алматы: Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2019. С. 6.

согласно типовой методике исследования компьютерной информации[1], является компьютерная (цифровая) информация, содержащаяся на машинных накопителях, в том числе на накопителях на жестких магнитных дисках, твердотельных накопителях, гибких магнитных дисках, оптических дисках, флеш-накопителях, картах памяти и др. Общая компьютеризация, развитие информационных технологий стали основным фактором цифровизации всех сторон общественной жизни, в связи с чем цифровая информация перестала исследоваться исключительно в рамках компьютерно-технической экспертизы. Сегодня, как отмечает Е.Р. Россинская, «цифровые следы могут являться объектами и других родов (видов) судебных экспертиз, например, в фоноскопической, автороведческой, лингвистической…»[2]. Рассмотрим это на примере ряда видов (родов) судебных экспертиз:

– цифровые следы, представленные в виде цифровых фотоснимков и видеозаписей, являются объектами фотовидеотехнической экспертизы;

– цифровые следы, представленные в виде массивов цифровых, данных являются объектами информационно-аналитической экспертизы;

– цифровые следы, представленные в виде цифровых фонограмм речи, могут являться объектами фоноскопической экспертизы;

– цифровые следы, представленные в виде текста в электронной (цифровой) форме, могут являться объектами лингвистической экспертизы;

– цифровые следы, представленные в виде электронных баз данных, содержащих записи бухгалтерского учета, хозяйственных документов, могут исследоваться в рамках бухгалтерской экспертизы и др.

Также необходимо учитывать комплексный характер исследования цифровых следов, когда для ответа на поставленные вопросы требуются специальные знания из различных областей науки, техники, ремесла или искусства. Например: назначение следователем комплексной компьютерно-технической и фотовидеотехнической экспертизы по изъятому электронному носителю информации, в ходе которой могут быть решены:

– экспертная задача поиска цифровых фотоснимков в информационном содержимом электронного носителя (компьютерно-техническая часть комплексной экспертизы);

– экспертная задача установления технических средств и условий изготовления обнаруженных цифровых фотоснимков (фотовидеотехническая часть комплексной экспертизы).

В заключение отметим, что для эффективного противодействия киберпреступности, по нашему мнению, следует уделять особое внимание вопросам подготовки и повышения квалификации сотрудников правоохранительных органов, обеспечения их современной криминалистической и специальной техникой. На качественном уровне

[1] Тушканова О.В. Типовая методика исследования компьютерной информации. М.: Следственный комитет Российской Федерации, 2020. 52 с.

[2] Россинская Е.Р. Система теории цифровизации судебно-экспертной деятельности. Теория и практика судебной экспертизы. 2024;19(3):25.

необходимо организовывать профессиональное обучение методологическим основам работы с цифровыми следами, вопросам обеспечения информационной безопасности, современным возможностям судебно-экспертных исследований цифровых следов для следователей, следователей-криминалистов, а также экспертов некомпьютерных специальностей. В основе такого обучения должен быть ключевой принцип работы с цифровыми следами – обеспечение их сохранности и неизменности.

Список источников

1. Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 3(55). С. 46–52. DOI: 10.17803/2311-5998.2019.55.3. 046-052. EDN: IHORPB.
2. Россинская Е.Р. Система теории цифровизации судебно-экспертной деятельности // Теория и практика судебной экспертизы. 2024. № 19(3). С. 20–32. DOI: 10.30764/1819-2785-2024-3-20-32 EDN: FKTXGG.
3. Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике // Аубакировские чтения: матер. междунар. науч.-практ. конф., Алматы, 19 февраля 2019 года. Алматы: Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2019. С. 6–9. EDN: BQAQSN.
4. Себякин А.Г. Механизм следообразования в компьютерных системах с точки зрения теории отражения // Сибирские уголовно-процессуальные и криминалистические чтения. 2021. № 2(32). С. 89–99. EDN: JSESDH.
5. Тушканова О.В. Типовая методика исследования компьютерной информации. М.: Следственный комитет Российской Федерации, 2020. 52 с.
6. Цифровая криминалистика: учебник для вузов / В.Б. Вехов [и др.]; под ред. В.Б. Вехова, С.В. Зуева. – 2-е изд., перераб. и доп. – М.: Юрайт, 2025. 490 с.

А.Д. Яким
Московская академия Следственного комитета
имени А.Я. Сухарева

Применение нейросетевых технологий для прогнозирования криминальных событий

Аннотация: В статье проведен анализ одного из концептуальных подходов к расследованию преступлений, который позволяет с помощью нейросетевых технологий, на основании заданной модели прогнозировать поведение лиц, которые склонны к совершению преступлений и с определенной вероятностью предсказывать криминальные события. В рамках данной модели применяется система логических взаимосвязей и взаимодействий, предиктивная аналитика, направленная на идентификацию субъектов преступной деятельности. Также автором были

рассмотрены подходы к цифровой трансформации информационно-коммуникационных технологий при расследовании преступлений.

Ключевые слова: нейронная сеть, организация расследования преступлений, информационно-телекоммуникационные технологии, алгоритмы, нейросетевые модели, прогнозирование.

Трансформация современного общества в межличностных отношениях углубляется в невербальный характер взаимодействия. Данным явлением обусловлено активное использование сети интернет, нейросетей, искусственного интеллекта, как проявлений научно-технического прогресса, представляющих собой системы двойного назначения, способные использоваться во благо и во вред человеческой цивилизации[1].

На данный момент ключевыми направлениями научных исследований в данной области являются: сетевая архитектура, алгоритмы машинного обучения; вычисления для искусственного интеллекта[2] – квантовые, фотонные, нейроморфные; данные для искусственного интеллекта в создании и аугментации данных, сохранения конфиденциальных данных; фундаментальные и генеративные модели – для символьных данных, мультимодальные модели и методы переноса знаний; безопасность и доверие; искусственный интеллект для узких задач; методы взаимодействия технических средств машинного взаимодействия с человеком.

Положительными аспектами цифровой трансформации являются: появление новых видов коммуникаций с удобным интерфейсом, улучшение скорости получения и обработки информации без затрат на энергоемкость, открытость информационных ресурсов, легкодоступность получения выхода в глобальную сеть.

Отрицательными сторонами являются: появление новых видов преступлений с ограниченной возможностью идентификации преступника; контроль полного жизненного цикла новых моделей поведения человека; определение психотипа через социальные сети, комментарии, реакции; феномен цифровой тени; легкая обучаемость интеллектуальных систем в негативных тенденциях.

В то же время юридические аспекты использования нейросетевых инструментов при совершении и расследовании противоправных действий в настоящее время изучены недостаточно, поэтому исследование возможностей нейросетевых алгоритмов для раскрытия противоправных деяний в указанной области представляется нам актуальным.

Многомасштабные модели комплексных сетей (прогноз и моделирование) управление и интеграция в комплексных сетях существенно увеличивают преступные намерения, к примеру, уже сейчас возможно создание цифровой автономной сущности, цифрового двойника, выполняющего задачу в интересах

[1] Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // СЗ РФ. 2019. № 41. Ст. 5700.

[2] См.: Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: монография. Москва: Проспект, 2021.

пользователя исходя из заданного алгоритма. Данным механизмом активно пользуются преступники.

Преступления в сфере информационно-коммуникационных технологий считаются интеллектуальными, узкими в своем профиле, требующими специальных знаний, технического и информационного оснащения. Зачастую противоправные деяния осуществляются исходя из следующих закономерностей: отсутствие защищенности сети (простота данных, отсутствие достаточной безопасной инфраструктуры); легкий поиск уязвимости сетей; отсутствие достаточной информации или же, наоборот, перегруженность информационного потока[1]. Поэтому выявление закономерностей, спутанности связей, оставления обманных цифровых следов совершения преступных деяний являются одними из важнейших направлений правоохранительной деятельности, где нейросетевые технологии помогают в решении трудоемких задач.

В данной сфере уже разрабатываются технологии для моделирования психических функций – направленное на раскрытие программ поведения человека информационное моделирование психических процессов, сводящееся к построению формализованных моделей психических функций, которые ведутся по нескольким направлениям: структурно-системный (нейрофизиология и психология), и программирование эвристического (моделирования) при котором мозг рассматривается как «черный ящик» и его деятельность описывают в виде системы отдельных информационных актов, действующих по алгоритмам.

Возможность использования нейронной сети в расследовании преступлений – это задача, требующая огромного количества данных, вычислительных ресурсов, экспертных знаний в различных областях. Таким образом, представляется возможной разработка алгоритма, который бы на основе машинной логики позволял проводить вычисления и дальнейший анализ преступных событий по следующим критериям:

1) событийности (теория о дважды происходящем событии);
2) учета ранее использующихся схем и методов;
3) новых технологий и трендов;
4) новостного потока;

Вероятность наступления события может быть рассчитана на основе следующей формулы: **P(Prediction) = f(X, W, b, Af)**, где:

P: Вероятность наступления определенного события или преступления. Это значение лежит в диапазоне от 0 до 1.

f: Функция нейронной сети, которая способна принимать входные данные, весомость событийного потока и выдать соответствующий прогноз.

X: Массив входных данных, включающий набор факторов, которые могут быть связаны с вероятностью совершения преступления. Такими факторами являются следующее:

[1] Яким А.Д. Перспективы развития технологий искусственного интеллекта в деятельности следователя. Сб. матер. Междунар. науч.-практ. конф. СПб, 2024. С. 179.

- данные о состоянии погоды (температура, осадки);
- сведения, содержащиеся в различных социальных сетях (настроения, высказывания, новостной поток);
- данные о звонках в службу экстренной помощи;
- данные о транспортной инфраструктуре (пробки, автобусные маршруты);
- камеры видеонаблюдения (анализ трафика, выявление аномалий);
- данные новостного потока;
- данные трендов, использования новых способов совершения преступлений с использованием информационно-коммуникационных технологий;
- исторические данные о преступлениях (тип, место, время, жертва, подозреваемый);
- социально-экономические данные;
- географические данные (плотность населения, наличие парков, освещение).

W: Вес (параметры, используемые для обучения нейросети, настройки).

b: Смещение (параметры, позволяющие нейросети выдавать ненулевой прогноз при условии нулевого значения входных данных).

Af: Функция активации (применяется к выходному параметру каждого нейрона, определяет, будет ли он активирован или нет в каждый конкретный момент времени).

X: Дополнительные данные с признаками: корреляции, категориальности - тип преступления (ограбление, кража, убийство и т.д.), район города, день недели (слоевые), числовыми, временными, геопространственными, текстовыми (описания, отчеты, посты в социальных сетях) с использованием методов обработки в виде к токенизации, стемминга, лемматизации, и векторного представления**,** а также с учетом свойств эболаративности, то есть обучаемости нейронной сети.

В заключение стоит отметить, что задача нейронной сети состоит не в подмене работы правоохранительных органов, а в создании помощи в виде алгоритмов, вероятностных перспектив для восприятия и оценки, с целью прогнозирования, совершаемых преступлений. Несомненно, необходима работа в данном направлении, ведь требуется углубленное изучение моделей, формирования фундаментальных библиотек знаний анализа данных, юриспруденции и т.д. Данные результаты могут быть использованы для дальнейшей разработки, с учетом дополнительных моделей, совершенствоваться, подстраиваться под сложные многоаспектные системные задачи.

Список источников

1. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // СЗ РФ. 2019. № 41. Ст. 5700.

2. Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: монография. М.: Проспект, 2021. 816 с.
3. Яким А.Д. Перспективы развития технологий искусственного интеллекта в деятельности следователя // Сборник материалов Международной научно-практической конференции. СПб., 2024.

Сведения об авторах

Алехин Дмитрий Владимирович – преподаватель кафедры криминалистики факультета подготовки криминалистов Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент.

Артамонова Людмила Александровна – старший помощник (по учебно-методической работе) руководителя следственного управления Следственного комитета Российской Федерации по Ставропольскому краю, полковник юстиции.

Бадмаев Александр Сергеевич – аспирант кафедры уголовного процесса и прокурорского надзора Института юстиции Байкальского государственного университета.

Гром Екатерина Анатольевна – старший преподаватель кафедры уголовного и уголовно-исполнительного права Донбасского государственного университета юстиции.

Доков Егор Сергеевич – лаборант кафедры криминалистической техники учебно-научного комплекса экспертно-криминалистической деятельности Волгоградской академии МВД России, рядовой полиции.

Дудникова Елена Валериевна – старший научный сотрудник Научно-производственного объединения «Специальная техника и связь» МВД России, майор полиции в отставке.

Кашенов Магжан Ермекович – преподаватель кафедры криминалистики Карагандинской академии Министерства Внутренних Дел Республики Казахстан, магистр юридических наук, старший лейтенант полиции.

Кирков Александр Недялков – преподаватель и руководитель лаборатории кибербезопасности Университета библиотековедения и информационных технологий, София, Болгария; преподаватель по цифровой криминалистике Академии МВД, София, Болгария, доктор, доцент.

Курумбаева Айнур Бекежановна – преподаватель кафедры уголовного права и криминологии Карагандинской академии МВД Республики Казахстан имени Б. Бейсенова, магистр юридических наук, майор полиции.

Мельников Виктор Юрьевич – профессор кафедры уголовного процесса и криминалистики Ростовского института (филиал) ВГУЮА (РПА Минюста России), доктор юридических наук, доцент.

Мельникова Светлана Валерьевна – преподаватель кафедры уголовного права и криминологии Московского областного филиала Московского университета МВД России имени В.Я. Кикотя, майор полиции.

Мерзликин Роман Александрович – начальник кафедры огневой подготовки Волгоградской академии МВД России, полковник полиции.

Мозговая Дина Александровна – доцент 30 кафедры (уголовного процесса) Военного университета имени князя Александра Невского Министерства обороны Российской Федерации, кандидат юридических наук, доцент.

Озеров Игорь Николаевич – заведующий кафедрой судебно-экспертной и оперативно-разыскной деятельности факультета подготовки криминалистов

Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, полковник юстиции.

Озеров Кирилл Игоревич – доцент кафедры юриспруденции Межрегионального открытого социального института, кандидат юридических наук.

Порываева Полина Сергеевна – преподаватель кафедры криминалистической техники учебно-научного комплекса экспертно-криминалистической деятельности Волгоградской академии МВД России, старший лейтенант полиции.

Прокофьева Елена Васильевна – доцент кафедры криминалистической техники учебно-научного комплекса экспертно-криминалистической деятельности Волгоградской академии МВД России, кандидат физико-математических наук, доцент, майор полиции.

Сибилькова Анна Васильевна – старший преподаватель кафедры управления органами расследования преступлений Академии управления МВД России, кандидат юридических наук, подполковник полиции.

Скобелин Сергей Юрьевич – доцент кафедры информационных технологий и организации расследования киберпреступлений Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, полковник юстиции.

Спивак Вячеслав Вячеславович – заместитель руководителя следственного отдела по городу Невинномысск следственного управления Следственного комитета Российской Федерации по Ставропольскому краю, капитан юстиции.

Ткачев Александр Викторович – доцент кафедры криминалистики юридического факультета Московского государственного университета имени М. В. Ломоносова, кандидат юридических наук, доцент.

Фролова Анастасия Николаевна – старший преподаватель кафедры исследования документов учебно-научного комплекса судебной экспертизы Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, майор полиции.

Шавловский Андрей Борисович – преподаватель кафедры судебно-экспертной и оперативно-разыскной деятельности Московской академии Следственного комитета имени А.Я. Сухарева, капитан юстиции.

Яким Алина Дмитриевна – ассистент кафедры информационных технологий и организации расследования киберпреступлений факультета подготовки криминалистов Московской академии Следственного комитета имени А.Я. Сухарева, лейтенант юстиции.

Оглавление

УГОЛОВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧЕЛОВЕЧЕСТВА

Материалы международной научно-практической конференции

(Москва, 13–14 февраля 2025 года)

Редакционная коллегия обращает внимание, что статьи представлены в авторской редакции. Ответственность за аутентичность и точность цитат, имен, названий и иных сведений, а также за соблюдение законов об интеллектуальной собственности несут авторы публикуемых материалов

Подписано в печать: 03.08.2025
Формат 60х90 1/16
Усл. печ. л. 9,1
Тираж 100 экз.
Компьютерная верстка,
техн. редактирование – И.Д. Нестерова
печать – Р.В. Гришин
Заказ № 524

_____
Отпечатано в типографии Московской академии
Следственного комитета имени А.Я. Сухарева,
ул. Врубеля, д. 12