2025
№ 1

МИР КРИМИНАЛИСТИКИ

Редакционная коллегия

2025
№1

МИР КРИМИНАЛИСТИКИ

Editor's Board

2025
№ 1

МИР КРИМИНАЛИСТИКИ

СОДЕРЖАНИЕ

Свидетельство о регистрации
ПИ № ФС77-87142
от 05 апреля 2024

Учредители
ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации имени А.Я. Сухарева»
ООО «Издательство Юнити-Дана»

Главный редактор

Н. Д. Эриашвили,
доктор экономических наук, кандидат юридических наук, кандидат исторических наук, почетный работник сферы образования Российской Федерации, Лауреат премии Правительства Российской Федерации в области науки и техники, Лауреат премии Правительства Российской Федерации в области образования

В. Н. Закаидзе,
Генеральный директор
Издательства «ЮНИТИ-ДАНА»
123298 Москва,
ул. Ирины Левченко, д. 1
Тел/факс: +7(499)740-60-14/15
E-mail: unity@unity-dana.ru

www.unity-dana.ru
www.niion.org

2025
№ 1

МИР КРИМИНАЛИСТИКИ

CONTENTS

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

(Москва, 13-14 февраля 2025 года)

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

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

Модератором пленарного заседания выступил ректор Московской академии СК России имени А.Я. Сухарева Алексей Александрович Бессонов.

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

Открывая пленарное заседание, А.И. Бастрыкин выступил с докладом на тему «Роль Следственного комитета России в обеспечении информационной безопасности человечества». Он отметил, что наблюдается рост преступных 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 тысячи, что на 13,1% больше, чем в 2023 году, в том числе тяжких и особо тяжких составов увеличилось на 7,8%».

В 2024 году СК России 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.

Председатель Следственного комитета Российской Федерации А.И. Бастрыкин

Глава СК России подчеркнул, 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. Так, в 2024 году практически каждое пятое расследованное в Следственном комитете преступление в сфере информационных технологий совершено несовершеннолетними.

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 и общались на эту тематику. Также у подростков наблюдались проблемы социализации и трудности в общении со сверстниками. В связи с этим глава СК России отметил важность активизации работы по предотвращению увлечения детей идеями деструктивных движений и сообществ, подчеркнув, что сейчас продолжается 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 СК России кадеты и курсанты наравне с профильными предметами и дисциплинами изучают основы военно-патриотической подготовки, участвуют в различных мероприятиях и проектах, а также оказывают помощь и поддержку социальным учреждениям, ветеранам Великой Отечественной войны и участникам специальной военной операции.

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

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 СК России. Председатель Следственного комитета коснулся статистических данных, связанных с расследованиями 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. В настоящее время в СК России уже эксплуатируется ряд информационных систем, а также планируется создание высокотехнологичной лаборатории для проведения исследований электронных носителей информации и активное развитие систем биометрической идентификации. Кроме того, в Следственном комитете организован непрерывный мониторинг медиапространства.

«За прошлый год по материалам СМИ, социальных сетей и мессенджеров возбуждено 2 779 уголовных дел», - озвучил Александр Иванович.

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

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

Участники конференции – учащиеся ведущих образовательных организаций

С докладами также выступили: Председатель комиссии Совета Федерации Федерального Собрания РФ 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 РФ 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; начальник Института повышения квалификации и переподготовки Следственного комитета Республики Беларусь Юрий Францевич Каменецкий. В своих докладах спикеры осветили 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, а также криминалистического, оперативно-розыскного и судебно-экспертного обеспечения информационной безопасности человечества.

В первый день конференции, в том числе и в формате видеоконференцсвязи (ВКС), приняли участие сотрудники Следственного комитета, российские государственные и общественные деятели, учёные и практикующие специалисты в области кибербезопасности из Белоруссии, Казахстана, Сербии и Болгарии, а также учащиеся ведущих образовательных организаций.

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

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

В число членов президиума второго дня 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 Алексей Александрович Бессонов.

В своем приветственным 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 обозначила законодательные инициативы в этой сфере.

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, а также 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.

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

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

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

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.

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

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

На протяжении двух дней в мероприятии, в том числе в формате видеоконференцсвязи (ВКС), приняли участие свыше 500 человек, включая более 150 учёных и практиков, из которых порядка 30 докторов наук и 60 кандидатов наук. Международный формат конференции осуществлен участием в ней представителей Российской Федерации, Азербайджанской Республики, Республики Беларусь, Республики Казахстан, Республики Болгария, Республики Индия и Республики Сербия.

На конференции рассмотрены вопросы, касающиеся правового обеспечения информационной безопасности мирового сообщества, уголовно-правовой охраны информационной безопасности в России и за ее пределами, уголовно-правовых рисков развития перспективных информационных технологий, а также 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, пропаганда неонацизма, дискредитация Вооружённых Сил и органов государственной власти суверенных государств, посягательства на историческую память и преемственность поколений.

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

Об организации работы по раскрытию преступлений прошлых лет в Северо-Западном федеральном округе

Александр Иванович Бастрыкин
Председатель Следственного комитета Российской Федерации, доктор юридических наук, профессор, заслуженный юрист Российской Федерации, Почетный Председатель Президиума Международного союза криминалистов

Аннотация. В статье рассматриваются вопросы организации расследования преступлений прошлых лет в следственных органах Следственного комитета Российской Федерации по Северо-Западному федеральному округу. Приводятся статистические данные и положительные примеры расследования таких дел.
Ключевые слова: Следственный комитет Российской Федерации, организация раскрытия преступлений, преступления прошлых лет, взаимодействие.
Для цитирования: Бастрыкин А.И. Об организации работы по раскрытию преступлений прошлых лет в Северо-Западном федеральном округе // Мир криминалистики. 2025. № 1. С. 12-15

On the organization of work to solve crimes of past years in the Northwestern Federal District

Alexander I. Bastrykin
Chairman of the Investigative committee of the Russian Federation, doctor of law, professor, honored lawyer of the Russian Federation, Honorary Chairman of the Presidium of the International union of criminologists

Abstract. The article examines the issues of organizing the investigation of crimes of past years in the investigative bodies of the Investigative Committee of the Russian Federation for the Northwestern Federal District. Statistical data and positive examples of investigation of such cases are provided.
Keywords: Investigative Committee of the Russian Federation, organization of crime detection, crimes of past years, interaction.
For citation: On the organization of work to solve crimes of past years in the Northwestern Federal District // The world of criminology. 2025;(1):12-15

Одними из основных условий успеха борьбы с преступностью являются установление лиц, совершивших преступления, и привлечение их к уголовной ответственности. Без преувеличения можно сказать, что раскрытие любого преступления – это всегда результат коллективного труда, и большое значение при этом имеет оперативно-розыскное сопровождение следственных действий, умелое использование агентурного аппарата, своевременное применение экспертных возможностей.

В полной мере сказанное относится к работе по раскрытию преступлений, совершенных в прошлые годы. Указанное направление является одним из приоритетных в деятельности ведомства, в связи с чем особое внимание уделяется вопросам организации и осуществления криминалистической и судебно-экспертной деятельности, направленной на обеспечение качественного и оперативного расследования преступлений.

Эти задачи в системе ведомства выполняют Главное управление криминалистики (Криминалистический центр) и Судебно-экспертный центр, который образован в соответствии с Указом Президента РФ от 01.07.2020 № 442[1] и распоряжением Правительства РФ от 15.07.2020 № 1827-р[2].

[1] Указ Президента РФ от 01.07.2020 № 442 «О внесении изменений в Положение о Следственном комитете Российской Федерации, утвержденное Указом Президента Российской Федерации от 14 января 2011 г. № 38». «Собрание законодательства РФ», 06.07.2020, № 27, ст. 4193.

[2] Распоряжение Правительства РФ от 15.07.2020 № 1827-р «О создании федерального государственного казенного учреждения «Судебно-экспертный центр Следственного комитета Российской Федерации».

К числу их ключевых приоритетов относятся внедрение в деятельность следственных органов современных достижений науки, применение криминалистической и специальной техники при проведении следственных действий и поисковых мероприятий, психологическое сопровождение следствия, непрерывное повышение квалификации следователей и криминалистов. Благодаря такому подходу в 2024 году в целом по России раскрыто 5 296 преступлений по уголовным делам, приостановленным в прошлые годы (за 3 месяца 2025 г. – 2 030 преступлений).

Следует отметить, что на этом важном направлении работы положительные результаты достигнуты следственными органами Следственного комитета Российской Федерации (далее – СК России) по Северо-Западному федеральному округу.

Так, следователями и криминалистами совместно с органами дознания в 2024 году раскрыто 318 преступлений, из которых дела о 270 преступлениях направлены в суд (за 3 месяца 2025 г. эти показатели составили соответственно 102 и 87). В 2024 году по сравнению с 2020 годом в результате активно проведенной работы число направленных в суд дел о тяжких и особо тяжких преступлениях против личности, совершенных в прошлые годы, увеличилось почти в 4 раза.

Важно, что при проведении межведомственных совещаний и заслушиваний в ходе выездов в региональные следственные управления в Северо-Западном федеральном округе повышенное внимание уделяется организации расследования особо тяжких преступлениях прошлых лет, совершенных по найму и в составе организованных преступных групп, банд.

К примеру, собранные следственными органами СК России по Республике Коми доказательства по много эпизодному уголовному делу признаны судом достаточными для вынесения приговора лидерам и участникам преступного сообщества Ю. Пичугина.

Необходимо подчеркнуть, что расследование представляло особую сложность, обусловленную совершением преступлений в условиях неочевидности, их давностью и длительным периодом осуществления противоправных действий, значительным объемом следственных действий на территории 20 субъектов Российской Федерации. Оперативное сопровождение по уголовному делу осуществлялось сотрудниками региональных УФСБ России, МВД России, УФСИН России, Росгвардии. Практическую помощь следствию оказывали также сотрудники МЧС России. В ходе следствия допрошены более 680 свидетелей, проведены 123 судебные экспертизы, порядка 60 очных ставок, свыше 200 обысков в различных регионах Российской Федерации, осуществлены многочисленные выемки, изъятия, осмотры предметов и документов[3].

Верховный суд Республики Коми приговорил Ю. Пичугина по ч. 4 ст. 210 УК РФ (создание и руководство преступной организацией), ч. 1 ст. 209 УК РФ (бандитизм), пп. «а», «ж», «з», ч. 2 ст. 105 УК РФ, ч. 3 ст. 30, пп. «а», «ж», «з» ч. 2 ст. 105 УК РФ (убийство и покушение на убийство), ч. 3 ст. 222 УК РФ и ч. 3 ст. 222.1 УК РФ (хранение оружия и взрывного устройства), п. «а» ч. 3 ст. 163 УК РФ (вымогательство), ч. 3 ст. 291 УК РФ (дача взятки) к пожизненному лишению свободы с отбыванием в исправительной колонии особого режима.

Также к пожизненному лишению свободы приговорен один из руководителей преступной организации Х. Азизов. Другие руководители преступной организации В. Карпов и С. Вануйто приговорены к лишению свободы на срок 19 и 17 лет. Остальные 12 подсудимых приговорены к лишению свободы на срок от 7 лет 9 месяцев до 25 лет в зависимости от роли и степени участия в совершенных преступлениях[4].

---

[3] В Республике Коми вынесен приговор по уголовному делу преступного сообщества Юрия Пичугина. https://sledcom.ru/news/item/1801261/ .

[4] Создатель, лидеры и участники преступного сообщества «Пичугинские» не сумели оспорить приговор 11.07.2024 https://epp.genproc.gov.ru/web/proc_11/mass-media/news.

Из наиболее резонансных необходимо также отметить раскрытие убийства предпринимателя Константина Быкова[5].

Помимо этого, ряд уголовных дел о тяжких и особо тяжких преступлениях, совершенных в прошлые годы, в том числе в составе организованных групп и преступных сообществ, в настоящее время рассматривается по существу в суде.

Безусловно, эффективное раскрытие преступлений прошлых лет во многом от применения новейших научно-технических средств, программного обеспечения, позволяющих оперативно и качественно обрабатывать большие объемы информации, имеющей значение в расследовании преступлений.

Одним из таких достижений является АДИС Папилон-9 с программной надстройкой Папилон-АДИС-9-НейроЭксперт – усовершенствованный программно-технический комплекс, предназначенный для автоматического поиска похожих дактилоскопических и иных типов объектов в большом массиве данных, ключевое отличие которого от предыдущих версий заключается в автоматической нейросетевой экспертизе результатов.

Система позволяет создать банк данных любого объема, а накопление информации может осуществляться как сканированием дактилокарт и следов с бумажных бланков, так и путем импорта объектов бескрасковым способом с помощью программы «Живой сканер». Именно благодаря её применению в Ленинградской области раскрыто совершенное в 2009 году убийство Морозова и хищение денежных средств ООО «Альянс».

Кроме того, следственным управлением СК России по Мурманской области в результате обработки АДИС Папилон-9 следов пальцев рук, изъятых с мест происшествий в ходе расследования нескольких убийств, совершенных в 1977-2006 годах, была установлена причастность конкретных лиц к их совершению.

Необходимо также сказать о том, что в целях раскрытия преступлений прошлых лет следственными органами СК России по Северо-Западному федеральному округу активно проводится аналитическая работа, в ходе которой тщательно проверяются лица, ранее привлекаемые к уголовной ответственности за аналогичные преступления.

Так, в общей сложности к 25 годам лишения свободы приговорен приезжий из Республики Молдова, имеющий статус лица без гражданства, более 20 лет назад убивший 60-летнюю женщину и похитивший принадлежавшие ей денежные средства. Раскрыть преступление удалось благодаря работе следователей следственного управления СК России по Мурманской области, которые изучили огромный массив судебных документов об аналогичных преступлениях, имевших место на территории субъекта за полтора десятилетия. В результате была полностью доказана вина 60-летнего Богдана, ранее осужденного за совершение четырех таких же преступлений.

В результате кропотливой работы следственным управлением СК России по Вологодской области совместно с органами дознания раскрыто убийство таксиста, совершенное в 2005 году. Установлено, что нападение на мужчину совершено пассажиром с целью хищения имевшихся у водителя денежных средств. Изобличенный в содеянном злоумышленник приговорен к 25 годам лишения свободы.

Стоит отметить, что в последнее время раскрытие преступлений прошлых лет осуществляется более эффективно благодаря ольфакторной идентификации.

Например, по уголовному делу о совершении более 27 лет назад в г. Калининграде убийства двух лиц, сопряженных с изнасилованием несовершеннолетней, и покушения на убийство малолетней, сопряженного с ее изнасилованием, на орудии удушения – галстуке проведенной в 2022 году ольфакторной судебной экспертизой обнаружены запаховые следы, происходящие от Юферева. В результате ранее неоднократно судимый и отбывавший наказание за совершение убийств мужчина

[5] В Архангельске Алексей Горяшин признан виновным в убийстве организованной группой предпринимателя Константина Быкова. https://arh.sledcom.ru/news/item/679274/.

был полностью изобличен в содеянном, и путем сложения наказаний ему назначено пожизненное лишение свободы.

По уголовному делу об убийстве в 2007 году четы пенсионеров Жариковых, сопряженном с разбойным нападением, в 2022 году ольфакторной судебной экспертизой на одежде потерпевших обнаружены запаховые следы, происходящие от Зубова и Ревенко. В марте 2024 года судом оба мужчины признаны виновными в совершении данных преступлений, каждому из них назначено наказание в виде 13 лет лишения свободы.

В Новгородской области по уголовному делу о покушении на убийство, сопряженное с изнасилованием Ксенофонтовой, в 2004 году, на одежде потерпевшей в результате проведенной в 2021 году ольфакторной судебной экспертизы обнаружены запаховые следы Сомова, осужденного впоследствии к 12 годам лишения свободы.

Выводы ольфакторных экспертиз способствовали раскрытию и иных преступлений прошлых лет. В связи с этим следственные органы СК России заинтересованы в дальнейшем внедрении ольфакторной экспертизы для решения идентификационных задач, в том числе при расследовании преступлений, совершенных в условиях неочевидности. Отмечу также, что в 2024 году в СЭЦ СК России начато создание нового экспертного направления психологических исследований.

В завершение следует отметить, что в СК России постоянно обновляется ведомственная база данных о нераскрытых преступлениях, о самодельных взрывных устройствах, ведутся учеты субъективных портретов подозреваемых, используемые для организации их розыска, а также ДНК-учеты. Вместе с тем в настоящее время крайне важно наращивать слаженность информационного взаимодействия между ведомствами в электронной форме. Значимость данного направления определяется оперативностью получения необходимой следствию информации из государственных информационных систем и иных источников.

На сегодняшний день следователи ведомства активно используют сведения из баз данных МВД России, ФНС России, Росреестра, кредитных организаций и операторов сотовой связи. Использование таких сведений способствует установлению лиц, причастных к совершению преступлений, получению информации об их местонахождении и перемещении.

Список источников

1. Указ Президента РФ от 01.07.2020 № 442 «О внесении изменений в Положение о Следственном комитете Российской Федерации, утвержденное Указом Президента Российской Федерации от 14 января 2011 г. № 38». «Собрание законодательства РФ», 06.07.2020, № 27, ст. 4193.

2. Распоряжение Правительства РФ от 15.07.2020 № 1827-р «О создании федерального государственного казенного учреждения «Судебно-экспертный центр Следственного комитета Российской Федерации». «Собрание законодательства РФ», 20.07.2020, № 29, ст. 4727

УДК 343.3/.7
ББК 67.408.135

Информационная безопасность: современные реалии и перспективы уголовно-правовой защиты

Виолетта Арсеновна Агаян
Ростовский институт (филиал) ВГУЮ (РПА Минюста России), Ростов-на-Дону, Россия
Email: violletta94@mail.ru

Аннотация. В статье рассматриваются современные тенденции развития информационных технологий, которые обуславливают реалии информационной безопасности, в том числе и в поле уголовно-правовой защиты.
Ключевые слова: информационная безопасность, информация, цифровизация, информационные технологии, уголовно-правовая защита.
Научная специальность: 5.1.4. Уголовно-правовые науки
Для цитирования: Аганян В.А. Информационная безопасность: современные реалии и перспективы уголовно-правовой защиты // Мир криминалистики. 2025. № 1. С 16-21

Information security: modern realities and prospects of criminal law protection

Violetta A. Agayan
the All-Russian state university of Justice, Rostov law institute (Branch), Rostov-on-Don, Russia
Email: violletta94@mail.ru

Abstract. The article examines current trends in the development of information technology, which determine the realities of information security, including in the field of criminal law protection.
Keywords: information security, information, digitalization, information technology, criminal law protection.
For citation: Ohanyan V.A. Information security: modern realities and prospects of criminal law protection // The world of criminology. 2025;(1):16-21

Введение. Современное развитие цифровых технологий диктует обществу и государству новые условия реальности, где на первый план выдвигается информационная безопасность. Появились новые угрозы правам личности, общества и государства. Из них можно выделить следующие:

1) развитие киберпреступности. За первые 7 месяцев 2024 г. в России было зафиксировано 577 тыс. киберпреступлений[1]. Появились новые виды: фейковые свидания, голосования, телефонное мошенничество, мошеннические схемы в ритейле, фейковая работа в интернете и другие;

2) утечка персональных данных. Так, в феврале 2024 г. произошла масштабная утечка информации: в открытый доступ попало 500 миллионов строк данных о россиянах. А уже 21 января 2025 г. хакерская группировка Silent Crow сообщила о взломе базы данных компании «Ростелеком»[2]. По предварительным данным, утечка могла произойти из-за уязвимости в инфраструктуре одного из подрядчиков. «Ростелеком» официально подтвердил факт утечки данных: в базе содержалось 154 тысячи уникальных адресов электронной почты и 101 тысяча номеров телефонов;

[1] Ущерб от IT-преступлений в 2024 году составил 99 млрд рублей // Journal.sovcombank.ru. URL.: https://journal.sovcombank.ru/news/uscherb-ot-it-prestuplenii-v-2024-godu-sostavil-99-mlrd-rublei (дата обращения: 20.10.2024).

[2] Хакеры заявили о взломе баз данных «Ростелекома». // Comss.ru. URL.: https://www.comss.ru/page.php?id=15546 (дата обращения: 21.01.2025).

3) уязвимость мобильных устройств. По данным компании F.A.C.C.T., за декабрь 2024 года и январь 2025 года мошенники похитили у россиян более 40 миллионов рублей с использованием приложения NFCGate[3];

4) развитие интернет вещей (IoT). IoT — концепция сети передачи данных между физическими объектами («вещами»), оснащёнными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой, в том числе на основе интернет-сети. Так, например, в 2022 году вследствие взлома IoT-устройств Черкизовского мясокомбината произошло отключение холодильного оборудования, что повлекло значительный ущерб для компании[4];

5) риски при использовании искусственного интеллекта. На основе данной системы совершаются кибератаки, происходит нарушение авторских и личных прав, совершаются преступления с использованием беспилотных средств. Примером может послужить создание и использование дипфейков для совершения различных противоправных действий.

В связи с этим возрастает актуальность уголовно-правовой защиты информации как одного из ключевых элементов обеспечения безопасности личности, общества и государства.

Основная часть. Одним из центральных аспектов обеспечения информационной безопасности является определение его понятия.

В соответствии со ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информация - это сведения (сообщения, данные) независимо от формы их представления[5]. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» определяет информационную безопасность как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства[6].

Уголовное законодательство России предусматривает комплекс мер по защите информационной безопасности граждан, организаций и государства от противоправных действий, связанных с информационными технологиями[7]. В частности, Федеральным законом «О внесении изменений в Уголовный кодекс Российской Федерации» от 30.11.2024 № 421-ФЗ была введена уголовная ответственность за незаконный оборот компьютерной информации, содержащей персональные данные[8].

По данным Следственного комитета России, в 2024 г. было расследовано более 21 тысячи киберпреступлений, что на 12 % больше, чем в 2023 г.[9].

Так, судебные органы России регулярно рассматривают дела, связанные с нарушением информационной безопасности. Примером может послужить дело № 1-34/2018, рассмотренное Московским городским судом[10]. Гражданин Н., занимающийся разработкой программного обеспечения, был обвинен в создании и распространении вредоносной программы,

---

[3] F.A.C.C.T.: мошенники похитили 40 млн рублей, используя приложение NFCGate. // Вести.ру. URL.: https://www.vesti.ru/article/4322808 (дата обращения: 22.01.2025).

[4] Алексей Петухов, ГК InfoWatch: почему IoT-устройства стали находкой для злоумышленников. // CISOCLUB. URL.: https://cisoclub.ru/aleksej-petuhov-gk-infowatch-pochemu-iot-ustrojstva-stali-nahodkoj-dlja-zloumyshlennikov/(дата обращения: 20.10.2024).

[5] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2025) // СПС «КонсультантПлюс».

[6] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

[7] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024) // СПС «КонсультантПлюс».

[8] Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 30.11.2024 № 421-ФЗ // СПС «КонсультантПлюс».

[9] Бастрыкин: Предлагаем закрепить в УК для киберпреступников новое отягчающее обстоятельство. // RG.RU. URL.: https://rg.ru/2025/01/14/v-uk-rf-dlia-kiberprestupnikov-propishut-novoe-otiagchaiushchee-obstoiatelstvo.html (дата обращения: 14.01.2025).

[10] Приговор № 1-34/2018 от 27 июля 2018 г. по делу № 1-34/2018. // Sudact.ru. URL.: https://sudact.ru/regular/doc/qd1j7ZZFRegB/ (дата обращения: 14.01.2025).

которая использовалась для несанкционированного доступа к банковским счетам пользователей. Суд признал гражданина виновным по статье 273 УК РФ и назначил ему наказание в виде лишения свободы на четыре года.

Другой пример – дело № 2-11/2020, рассматривавшееся в Санкт-Петербургском городском суде[11]. Группа лиц была признана виновной в совершении преступлений, предусмотренных статьей 272 УК РФ, за неправомерный доступ к серверным системам крупного коммерческого банка. В результате их действий были уничтожены данные о финансовых операциях клиентов, что привело к значительным убыткам для банка. Преступники получили сроки лишения свободы от трех до шести лет.

Однако эффективность уголовно-правовых мер в борьбе с киберпреступлениями достаточно низкая. Так, по данным Министерства внутренних дел России, только 4% таких дел заканчиваются передачей материалов в суд[12].

Кроме того, несмотря на наличие правовых норм, направленных на защиту информационной безопасности, существует ряд проблем, связанных с реализацией этих положений на практике:

1) недостаточная эффективность правоприменения. Несмотря на наличие статей УК РФ, предусматривающих наказание за неправомерные действия в сфере компьютерной информации, количество уголовных дел по таким статьям остается низким. Это связано как с недостаточной квалификацией сотрудников правоохранительных органов, так и со сложностью сбора доказательств при расследовании преступлений в данной области;

2) отсутствие четких критериев квалификации деяний. В ряде случаев сложно определить, какие именно действия подпадают под те или иные статьи УК РФ. Например, понятие «неправомерного доступа» может трактоваться различными способами, что затрудняет процесс привлечения виновных лиц к ответственности;

3) низкий уровень осведомленности граждан о своих правах и обязанностях в сфере информационной безопасности. Многие не осознают всей серьезности угроз, связанных с киберпреступлениями, и не принимают необходимых мер предосторожности. Это приводит к увеличению числа инцидентов, связанных с утечкой данных и другими нарушениями информационной безопасности;

4) сложности международного сотрудничества. Киберпреступления часто носят трансграничный характер, что требует эффективного взаимодействия между правоохранительными органами различных стран. Однако отсутствие унифицированных международных стандартов и процедур обмена информацией значительно усложняет расследование и привлечение к ответственности виновных лиц;

5) необходимость модернизации законодательства. С развитием новых технологий появляются новые виды угроз, которые требуют адекватной правовой реакции. Законодательство должно оперативно реагировать на изменения в этой области, чтобы обеспечить эффективную защиту интересов государства и граждан;

6) проблема правового регулирования деятельности частных компаний в сфере информационной безопасности. Частные компании играют важную роль в обеспечении информационной безопасности, однако их деятельность зачастую слабо регламентирована законодательством. Это создает риски для потребителей услуг и снижает общий уровень защищенности информационного пространства;

7) недостаточно развитая система мониторинга и анализа киберугроз. Для эффективной борьбы с киберпреступностью необходимо иметь систему раннего обнаружения и предотвращения атак. Однако в настоящее время такие системы находятся на стадии разработки и внедрения, что ограничивает возможности государства по защите своей информационной инфраструктуры;

[11] Дело № 2-11/2020 (2-63/2019;). // Actofact.ru. URL.: https://actofact.ru/case-78OS0000-2-11-2020-2-63-2019-2019-10-23-2-0/ (дата обращения: 14.01.2025).

[12] Официальный портал: МВД Российской Федерации. URL.: https://мвд.рф/ (дата обращения: 14.01.2025).

8) недостаточное финансирование программ по обеспечению информационной безопасности. Государственные программы по развитию систем защиты от киберугроз требуют значительных финансовых вложений. Недостаточное финансирование ведет к отставанию России в этой области и снижению уровня защищенности национальной информационной инфраструктуры;

9) несовершенство системы подготовки кадров в области информационной безопасности. Для успешной реализации мер по защите информационной безопасности необходимы квалифицированные специалисты. Однако существующая система образования и профессиональной подготовки специалистов в этой области оставляет желать лучшего, что негативно сказывается на уровне защищенности государственных и коммерческих структур.

Заключение. В условиях современного мира информационная безопасность является одной из ключевых составляющих национальной безопасности любого государства. Для Российской Федерации обеспечение защиты информационных ресурсов и систем от внешних и внутренних угроз требует разработки и внедрения комплекса мер, направленных на предотвращение утечек данных, защиту критической инфраструктуры и противодействие кибератакам.

Они включают в себя:

1) законодательное регулирование. Одним из важнейших аспектов обеспечения информационной безопасности является совершенствование законодательной базы. Необходимо принятие новых законов и поправок к уже существующим нормативным актам, которые будут регулировать вопросы защиты информации, ответственность за нарушение правил обработки персональных данных и др. Предлагаем пересмотреть санкции по статьям, связанным с неправомерным доступом к компьютерной информации (ст. 272 УК РФ), созданием, использованием и распространением вредоносных программ (ст. 273–274 УК РФ). В частности, предлагается увеличить сроки лишения свободы и размеры штрафов за совершение данных преступлений, особенно, если они повлекли значительный ущерб или были совершены организованной группой лиц. Кроме того, целесообразно внести дополнения в статью 207.1 УК РФ следующего содержания: «Публичное распространение под видом достоверных сообщений заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, и (или) о принимаемых мерах по обеспечению безопасности населения и территорий, приемах и способах защиты от указанных обстоятельств, в том числе с использованием сети «Интернет»»;

2) развитие технологий защиты информации. Для повышения уровня защищенности информационных систем необходимо активно развивать отечественные технологии и программное обеспечение, предназначенные для защиты данных. Это включает создание и внедрение средств криптографической защиты, антивирусных программ, систем обнаружения вторжений и других инструментов, обеспечивающих целостность и конфиденциальность информации;

3) обучение и повышение квалификации кадров. Эффективная защита информации невозможна без квалифицированных специалистов. Поэтому важно организовать программы обучения и повышения квалификации сотрудников государственных органов, предприятий и организаций, которые работают с информацией ограниченного доступа. В рамках этих программ должны рассматриваться современные методы защиты информации, анализ рисков и управление инцидентами;

4) контроль и мониторинг информационных систем. Необходимо внедрить системы мониторинга и контроля за состоянием информационных систем, чтобы своевременно выявлять угрозы и реагировать на них. Регулярные аудиты безопасности позволят оценить уровень защищенности и выявить слабые места, требующие дополнительного внимания;

5) международное сотрудничество. Информационные угрозы носят глобальный характер, поэтому важное значение имеет международное сотрудничество в области информационной безопасности. Россия должна активно участвовать в международных форумах и инициативах,

направленных на борьбу с киберпреступностью и обмен опытом в сфере защиты информации.

Обеспечение информационной безопасности Российской Федерации требует комплексного подхода, включающего законодательные инициативы, развитие технологий, обучение кадров, контроль и мониторинг информационных систем, а также международное сотрудничество. Только при условии реализации всех перечисленных мер можно достичь высокого уровня защиты национальных интересов в информационной сфере.

Список источников

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 28.12.2024) // СПС «КонсультантПлюс».

2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2025) // СПС «КонсультантПлюс».

3. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 30.11.2024 № 421-ФЗ // СПС «КонсультантПлюс»

4. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

5. Ущерб от IT-преступлений в 2024 году составил 99 млрд рублей // Journal.sovcombank.ru. URL.: https://journal.sovcombank.ru/news/uscherb-ot-it-prestuplenii-v-2024-godu-sostavil-99-mlrd-rublei (дата обращения: 20.10.2024).

6. Хакеры заявили о взломе баз данных «Ростелекома». // Comss.ru. URL.: https://www.comss.ru/page.php?id=15546 (дата обращения: 21.01.2025).

7. F.A.C.C.T.: мошенники похитили 40 млн рублей, используя приложение NFCGate. // Вести.ру. URL.: https://www.vesti.ru/article/4322808 (дата обращения: 22.01.2025).

8. Алексей Петухов, ГК InfoWatch: почему IoT-устройства стали находкой для злоумышленников. // CISOCLUB. URL.: https://cisoclub.ru/aleksej-petuhov-gk-infowatch-pochemu-iot-ustrojstva-stali-nahodkoj-dlja-zloumyshlennikov/(дата обращения: 20.10.2024).

9. Бастрыкин: Предлагаем закрепить в УК для киберпреступников новое отягчающее обстоятельство. // RG.RU. URL.: https://rg.ru/2025/01/14/v-uk-rf-dlia-kiberprestupnikov-propishut-novoe-otiagchaiushchee-obstoiatelstvo.html (дата обращения: 14.01.2025).

10. Приговор № 1-34/2018 от 27 июля 2018 г. по делу № 1-34/2018. // Sudact.ru. URL.: https://sudact.ru/regular/doc/qd1j7ZZFRegB/ (дата обращения: 14.01.2025).

11. Дело № 2-11/2020 (2-63/2019;). // Actofact.ru. URL.: https://actofact.ru/case-78OS0000-2-11-2020-2-63-2019-2019-10-23-2-0/ (дата обращения: 14.01.2025).

12. Официальный портал: МВД Российской Федерации. URL.: https://мвд.рф/ (дата обращения: 14.01.2025).

References

1. Criminal Code of the Russian Federation of 13.06.1996 № 63-FZ (as amended on 28.12.2024) // SPS «ConsultantPlus»

2. Federal Law of 27.07.2006 № 149-FZ (as amended on 23.11.2024) «On Information, Information Technologies and Information Protection» (as amended and supplemented, entered into force on 01.01.2025) // SPS «ConsultantPlus»

3. Federal Law «On Amendments to the Criminal Code of the Russian Federation» dated November 30, 2024 №. 421-FZ // SPS «ConsultantPlus»

4. Decree of the President of the Russian Federation of 05.12.2016 № 646 «On approval of the Doctrine of information security of the Russian Federation» // SPS «ConsultantPlus»

5. Damage from IT crimes in 2024 amounted to 99 billion rubles // Journal.sovcombank.ru. URL.: https://journal.sovcombank.ru/news/uscherb-ot-it-prestuplenii-v-2024-godu-sostavil-99-mlrd-rublei (accessed: 20.10.2024).

6. Hackers announced the hacking of Rostelecom databases. // Comss.ru. URL.: https://www.comss.ru/page.php?id=15546 (accessed: 21.01.2025).

7. F.A.C.C.T.: fraudsters stole 40 million rubles using the NFCGate application. // Vesti.ru. URL.: https://www.vesti.ru/article/4322808 (accessed: 22.01.2025).

8. Alexey Petukhov, InfoWatch Group: why IoT devices have become a godsend for criminals. // CISOCLUB. URL.: https://cisoclub.ru/aleksej-petuhov-gk-infowatch-pochemu-iot-ustrojstva-stali-nahodkoj-dlja-zloumyshlennikov/ (accessed: 20.10.2024).

9. Bastrykin: We propose to enshrine a new aggravating circumstance for cybercriminals in the Criminal Code. // RG.RU. URL.: https://rg.ru/2025/01/14/v-uk-rf-dlia-kiberprestupnikov-propishut-novoe-otiagchaiushchee-obstoiatelstvo.html (accessed: 14.01.2025).

10. Sentence № 1-34/2018 of July 27, 2018 in case No. 1-34/2018. // Sudact.ru. URL.: https://sudact.ru/regular/doc/qd1j7ZZFRegB/ (accessed: 14.01.2025).

11. Case №. 2-11/2020 (2-63/2019) // Actofact.ru. URL.: https://actofact.ru/case-78OS0000-2-11-2020-2-63-2019-2019-10-23-2-0/ (accessed: 14.01.2025).

12. The official portal: Ministry of Internal Affairs of the Russian Federation. URL.: https://мвд.рф/ (accessed: 14.01.2025).

Информация об авторе

В. А. Агаян — старший преподаватель кафедры уголовного права и криминологии Ростовского института (филиала) ВГУЮ (РПА Минюста России), член Совета молодых ученых и специалистов Ростовской области.

Information about the author

V. A. Agayan — senior lecturer at the Department of Criminal Law and Criminology of the Rostov Institute (branch) VGU (RPA of the Ministry of Justice of Russia), member of the Council of Young Scientists and Specialists of the Rostov region.

УДК 343.98

Расследование по уголовным делам об убийствах, связанных с безвестным исчезновением людей, по которым труп потерпевших не обнаружен

Дмитрий Владимирович Алехин
Московская академия Следственного комитета имени А.Я. Сухарева, Москва, Россия
Email: dial@mail.ru

Аннотация. Объектом исследования является преступная деятельность лиц по совершению убийств, связанных с безвестным исчезновением людей, по которым труп потерпевших не обнаружен, а также деятельность правоохранительных органов по расследованию указанных преступлений. Предметом исследования выступают объективные закономерности преступной деятельности лиц, совершающих убийства, связанные с безвестным исчезновением людей, по которым труп потерпевших не обнаружен, а также организационно-правовые, тактические и иные средства и приемы процесса расследования. Особое внимание уделяется проблемам, возникающим на первоначальном этапе расследования убийств, связанных с безвестным исчезновением людей, когда местонахождение пропавшего не установлено, его труп не обнаружен. Методологическую основу исследования составили общенаучные методы (сравнение, анализ) и эмпирические методы (анализ материалов уголовных дел, изучение нормативной, научной и специальной литературы). Сделан вывод о том, что сложная проблемная ситуация, при которой не обнаружен труп потерпевшего, не является препятствием для привлечения к уголовной ответственности виновных лиц, если полученные доказательства позволяют прийти к обоснованному выводу о совершённом преступлении с учётом принципа свободы оценки доказательств.
Ключевые слова: убийство, безвестное исчезновение, расследование
Научная специальность: 5.1.4. Уголовно-правовые науки
Для цитирования: Алехин Д.В. Расследование по уголовным делам об убийствах, связанных с безвестным исчезновением людей, по которым труп потерпевших не обнаружен // Мир криминалистики. 2025. № 1. С. 22-25

Investigation of criminal cases of murders related to the unknown disappearance of people in which the corpses of the victims have not been found

Dmitry V. Alekhin
Sukharev Moscow Academy of the Investigative Committee, Moscow, Russia
Email: dial@mail.ru

Abstract. The object of the study is the criminal activity of persons who commit murders related to the unknown disappearance of people for whom the victims' bodies have not been found, as well as the activities of law enforcement agencies investigating these crimes. The subject of the study is the objective patterns of criminal activity of persons who commit murders related to the unknown disappearance of people for whom the corpse of the victims has not been found, as well as organizational, legal, tactical and other means and techniques of the investigation process. Special attention is paid to the problems that arise at the initial stage of the investigation of murders related to the unknown disappearance of people, when the location of the missing person has not been established, his body has not been found. The methodological basis of the research was made up of general scientific methods (comparison, analysis) and empirical methods (analysis of criminal case materials, study of normative, scientific and specialized literature). It is concluded that a complex problematic situation in which the victim's corpse is not found is not an obstacle to bringing the perpetrators to criminal responsibility if the evidence obtained allows us to come to a reasonable conclusion about the crime committed, taking into account the principle of freedom of evidence assessment.
Keywords: murder, unknown disappearance, investigation
For citation: Alekhin D.V. Investigation of criminal cases of murders related to the unknown disappearance of people in which the corpses of the victims have not been found // The world of criminology. 2025;(1): 22-25

На первоначальном этапе расследования убийств, связанных с безвестным исчезновением, возникает сложная проблемная ситуация: местонахождение пропавшего не установлено, его труп не обнаружен. Обобщение практики показало, что такая ситуация не является препятствием для привлечения к уголовной ответственности виновных лиц, если полученные доказательства позволяют прийти к обоснованному выводу о совершенном преступлении с учетом принципа свободы оценки доказательств. В основу принимаемых судебных решений закладываются такие

данные как подробное описание подсудимыми обстоятельств лишения жизни потерпевшего; свободное, добровольное, последовательное и подробное изложение способа совершения преступления в ходе проверки показаний на месте; результаты проведенных осмотров предметов и мест происшествий с указанием на обнаружение следов биологического происхождения и экспертные заключения, свидетельствующие об обнаружении крови, которая могла принадлежать пропавшему; принятие исчерпывающих мер, направленных на установление местонахождения пропавшего (активное проведение поисковых мероприятий, наличие проверок по соответствующим учетам и др.).

После получения необходимой первичной информации организуются оперативно-розыскные мероприятия, направленные на установление: возможных свидетелей преступления; мест совершения убийства и сокрытия трупа; следов и орудий преступления; автотранспорта и других вещей исчезнувшего; виновных в совершении преступления.

С учётом того, что одним из обстоятельств, устанавливаемых в ходе разрешения указанной ситуации, является подтверждение физического отсутствия человека, необходимо постоянно запрашивать и проверять информацию регистрирующих ведомств о наличии сведений о пропавшем, об используемых им предметов, имеющих идентификационные признаки (операторы мобильной связи, медицинские учреждения, адресные бюро и т.д.).

Органу дознания необходимо дать поручение на проверку возможного местонахождения разыскиваемого в местах проживания родственников или иных местах его возможного пребывания, в том числе на осуществление подворового, поквартирного обхода по примерному маршруту исчезнувшего с целью выявления лиц, которые были в контакте с ним или которые в период его исчезновения проходили по улице, а также установления наличия регистрирующих устройств электронных баз данных, способных сохранить сведения о лицах или автотранспорте, которые могли находиться на месте происшествия (например, системы видеонаблюдения предприятий, постов ГИБДД, магазинов и т.д.).

При установлении свидетелей следует подробно их допросить с целью выяснения обстоятельств, при которых они видели пропавшего: во что он был одет, в каком состоянии находился, каковы признаки внешности лиц, в окружении которых он находился. С целью уточнения маршрута, по которому вероятнее всего мог двигаться потерпевший, следует провести проверку показаний на месте с участием свидетелей, которые дают показания о возможном пути передвижения пропавшего.

Со слов свидетелей необходимо создать композиционный портрет возможного преступника и использовать его при проведении оперативно-розыскных мероприятий. Если получены данные о том, что потерпевший садился в автомобиль, следует выяснить, добровольно или принудительно осуществлялась посадка, зафиксировать данные транспортного средства, на основании которых запросить сведения о владельцах схожих по приметам автомобилей. Допрос таких свидетелей позволяет сделать выводы относительно того, является ли водитель местным жителем или нет, и получить приметы его личности.

Характеристика личности потерпевшего, его привычки и образ жизни должны постоянно оставаться в центре внимания следователя. Обстоятельства, негативно характеризующие биографию разыскиваемого лица, могут поставить под сомнение факты, которые в своей совокупности позволяют допускать его смерть (отсутствие постоянного места жительства, антиобщественный образ жизни, неоднократные случаи исчезновения, причины которых не имеют криминального характера и т.д.). Поэтому при установлении фактов неоднократного ухода пропавшего из дома путём осмотра места жительства следует выяснить наличие или отсутствие личных вещей и документов исчезнувшего. Допрос близких лиц должен быть направлен на выяснение причин и длительности как текущего, так и предыдущих исчезновений,

мест возможного нахождения, фактов сообщений о себе в период ухода, а также того, не высказывались ли им мысли о самоубийстве, не наблюдались ли странности в его поведении. Органу дознания необходимо поручить установить лиц, с которыми пропавший контактировал в период прошлых исчезновений, и допросить их о намерениях разыскиваемого, желаниях уехать куда-либо, с какой целью, на какой период и т.д.

Следователю необходимо выяснить, не было ли у пропавшего заболевания, которое могло бы обусловить скоропостижную смерть, потерю памяти, ориентирования во времени и пространстве. В этих целях должны направляться запросы в лечебные учреждения, что позволит установить, состоял ли исчезнувший на учёте, и если да, то с каким заболеванием, когда проходил лечение и как часто возникает потребность в нём. Значимую информацию можно получить путём допросов врачей, лечивших без вести пропавшего, а также выемки и последующего изучения медицинских документов. Учитывая, что человек, потерявший память, может воспользоваться общественным транспортом и уехать на значительное расстояние от места своего пребывания или проживания, необходимо установить и допросить водителей, кассиров, кондукторов транспорта местного и пригородного сообщений.

В случае исчезновения потерпевшего с крупной суммой денег начинать необходимо с допроса его ближайшего окружения. Нужно выяснить, кому было известно о наличии у пропавшего такой суммы, не высказывался ли он о том, что должен получить крупный денежный долг и от кого. Обязательному осмотру подлежит квартира разыскиваемого лица, в ходе которого могут быть обнаружены записи о должниках и долговые расписки, а также следы пребывания в квартире посторонних лиц. Допрос соседей исчезнувшего позволит установить тех, кто посещал квартиру потерпевшего незадолго до его исчезновения или уже после пропажи.

Обращаем внимание на необходимость проведения полномасштабных поисковых мероприятий. Меры, принимаемые по установлению трупов потерпевших, как по способу (в случае достоверно установленного места сокрытия), так и по охвату территории должны быть достаточными. В протоколе осмотра места происшествия необходимо отражать как долго проводились поисковые мероприятия; площадь осматриваемой территории; лиц, привлеченных к участию в поисках и технические средства; обнаружение фрагментов одежды, принадлежащей потерпевшему и пр. К протоколу следует приобщать карту местности, на территории которой проводились поиски, фотоизображения, видеозапись и т.д. О достаточности поисковых мероприятий, помимо протокола осмотра места происшествия и приложений к нему, будут свидетельствовать различные справки, ответы на запросы из учреждений и т.д. Например, при организации поисковых мероприятий на водоёмах следует приобщать к материалам уголовного дела справку от гидрологов о состоянии течения на конкретном участке, которая в последующем может свидетельствовать о невозможности отыскания трупа; справку от сотрудников гидрометцентров; заключение специалистов-микробиологов о том, что нахождение тела человека в течение интересующего периода в сильно загрязнённом водоёме способствует нарушению целостности скелета и т.д.

Одним из важных доказательств при расследовании по уголовным делам об убийствах, связанных с безвестным исчезновением людей, по которым труп потерпевших не обнаружен, является экспертное заключение. Например, проведение медико-криминалистической экспертизы позволяет установить время кремации, возможность доведения костей скелета до крайней степени уничтожения, отсутствие в золе костной ткани. Температуру горения в котлах котельной позволяет установить техническая экспертиза.

На основании материалов уголовного дела производятся и ситуационные экспертизы. Например, несмотря на отсутствие трупа, на основе данных анатомической науки и физиологии можно сделать предположительный вывод о том, что в результате нанесения потерпевшему множественных ударов кулаками и ногами по различным частям тела, в том числе в об-

ласть головы, у него могла развиться черепно-мозговая травма, относящаяся к тяжкому вреду здоровья, опасному для жизни, и это могло повлечь смерть потерпевшего.

По одному из уголовных дел суд признал виновным Щ. в совершении преступлений, предусмотренных ч.1 ст. 109, 125 УК РФ, то есть в том, что при допущенном им нарушении правил управления маломерными судами его жена во время шторма погибла в море. Труп обнаружен не был. Основой обвинения явилось экспертное заключение, согласно которому пребывание человека в воде при температуре 13 градусов и удаленности от суши от 500 до 150 м в условиях, указанных в материалах дела (время суток, скорость и направление ветра, штормовая погода, высота волн от 1,5 до 2 м, отсутствие спасательных средств), чревато высокой степенью риска наступления смерти от утопления или синдрома переохлаждения организма. Летальный исход, по мнению экспертов, мог наступить через несколько минут, при этом не исключалась возможность продержаться в воде в течение 30-40 минут, но даже в случае правильного выбора направления к берегу шансы потерпевшей доплыть до берега были маловероятны. Смерть могла наступить от механической асфиксии (утопления) вследствие закрытия дыхательных путей водой или от переохлаждения организма.

В ходе сбора доказательственного материала следователи назначают и генотипоскопические исследования, при этом, поскольку труп не обнаружен, используют образцы крови близких родственников потерпевшего.

Таким образом, обобщение практики расследования по уголовным делам об убийствах, связанных с безвестным исчезновением людей, по которым труп потерпевших не обнаружен показало, что только действия следственных органов, связанные с квалифицированным сбором и закреплением комплекса доказательств, позволяют в итоге добиться привлечения виновных лиц к уголовной ответственности.

Список источников

1. Боровиков А. П. Особенности получения криминалистически значимой информации по делам об убийствах, при которых труп потерпевшего не обнаружен или был уничтожен // Вестник Академии Следственного комитета Российской Федерации. 2019. № 2(20). С. 127-132.

2. Криминалистика: учебник в 3 ч. Часть 3 / под общей редакцией В.В. Бычкова, С.В. Харченко. М.: Проспект, 2020. С. 54-92.

3. Шувалов М.Н., Шувалова А.М. Ошибки, допускаемые следователями, при расследовании уголовных дел о без вести пропавших // Противодействие преступлениям, связанным с безвестным исчезновением граждан, и методика их расследования: Материалы Международной научно-практической конференции, Москва, 20 марта 2015 года. М.: Юнити-Дана, 2015. С. 225-229.

References

1. Borovikov A. P. Peculiarities of obtaining criminalistically significant information on murder cases in which the victim's corpse was not found or was destroyed // Bulletin of the Academy of the Investigative Committee of the Russian Federation. 2019. No. 2(20). P. 127-132.

2. Criminalistics: a textbook in 3 parts. Part 3 / edited by V.V. Bychkov, S.V. Kharchenko. Moscow: Prospekt, 2020. P. 54-92.

3. Shuvalov M.N., Shuvalova A.M. Mistakes made by investigators when investigating criminal cases of missing persons // Countering crimes related to the unknown disappearance of citizens and methods of their investigation: Proceedings of the International Scientific and Practical Conference, Moscow, March 20, 2015. Moscow: Publishing House "Unity-Dana", 2015. P. 225-229.

Информация об авторе

Д.В. Алехин — преподаватель кафедры криминалистики Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент.

Information about the author

D.V. Alekhin — lecturer of the Criminalistics Department of the Sukharev Moscow academy of the Investigative Committee, Candidate of Law, Associate Professor.

УДК: 343.3/.7
ББК 67.408.1

Социальная обусловленность установления уголовной ответственности за распространение заведомо ложной информации

Зарема Муратовна Бешукова
Адыгейский государственный университет, Майкоп, Россия
Email: Zarema_b2008@mail.ru

Маргарита Асланбиевна Меретукова
Адыгейский государственный университет, Майкоп, Россия
Email: M.meretukova@yandex.ru

Аннотация. В статье рассматривается одна из наиболее актуальных в современный период проблем – распространение ложной информации. Отмечается, что в разных странах вопрос ответственности за данное деяние решается по-разному. В некоторых государствах распространение заведомо ложной информации влечет уголовную ответственность. Сделан вывод, что в условиях глобализации и быстрого распространения информации важно создавать правовые механизмы, которые бы обеспечивали безопасность общества и государства. Введение в России уголовной ответственности за распространение заведомо ложной информации с определенным содержанием отвечает интересам и объективным потребностям современного общества и является необходимой мерой, направленной на обеспечение общественной безопасности.
Ключевые слова: ложная информация, фейкинг, интернет, пандемия, фейки, поляризация общества, специальная военная операция, манипуляция мнением, социальные сети, дезинформация, недостоверная информация, искусственный интеллект, фейковая информация.
Научная специальность: 5.1.4. Уголовно-правовые науки
Для цитирования: Бешукова З.М., Меретукова М.А. Социальная обусловленность установления уголовной ответственности за распространение заведомо ложной информации // Мир криминалистики. 2025. № 1. С.26-29

Social conditionality of establishing criminal liability for the distribution of knowingly false information

Zarema M. Beshukova
Adygea State University, Maikop, Russia
Email: Zarema_b2008@mail.ru

Margarita A. Meretukova
Adygea State University, Maikop, Russia
Email: M.meretukova@yandex.ru

Abstract. The article examines one of the most pressing problems in the modern period – the spread of false information. It is noted that in different countries the issue of responsibility for this act is resolved differently. In some states, the distribution of knowingly false information entails criminal liability. It is concluded that in the context of globalization and the rapid dissemination of information, it is important to create legal mechanisms that would ensure the security of society and the state. The introduction in Russia of criminal liability for the dissemination of knowingly false information with a certain content meets the interests and objective needs of modern society, and is a necessary measure aimed at ensuring public safety.
Keywords: false information, faking, Internet, pandemic, fakes, polarization of society, special military operation, manipulation of opinion, social networks, disinformation, unreliable information, artificial intelligence, fake information.
For citation: Beshukova Z. M., Meretukova M. A. Social conditionality of establishing criminal liability for the distribution of knowingly false information // The world of criminology. 2025;(1):26-29

Введение. Феномен распространения ложной информации существует с древних времен и был характерен для всех стран мира, о чем свидетельствуют многочисленные исторические примеры. Один из самых известных – искажение результатов битвы, произошедшей в начале XIII в. до нашей эры при Кадеше. Тогда обе стороны конфликта – египтяне и хетты, заявили о своей полной победе, хотя сражение завершилось ничьей.

В качестве средства убеждения и манипуляции общественным мнением ложная информация использовалась на протяжении многих веков, однако её массовое распространение стало возможным лишь с появлением книгопечатания и ростом уровня грамотности людей[1].

С развитием цифровых технологий скорость распространения ложной информации значительно возросла благодаря преимуществам Интернета, в числе которых высокая скорость передачи данных и растущее число пользователей[2]. Обмен информацией в виртуальной сети стал невероятно простым – достаточно всего нескольких кликов мышью. Причем, если в прошлом ложная информация была привязана к конкретному отправителю и ограниченному кругу лиц, то теперь Интернет разрушил эту бинарную структуру. Именно поэтому в настоящее время ложная информация является одной из главных проблем.

Массовая дезинформация стала настолько всепроникающей и распространенной, что в 2024 г. Всемирный экономический форум обозначил её в качестве главного глобального риска в двухгодичной перспективе. Эксперты форума подчеркнули, что, несмотря на введение некоторых нормативных актов для борьбы с дезинформацией в интернете, их темпы и эффективность пока отстают от скорости развития технологий искусственного интеллекта[3].

Основная часть. В современном мире существуют различные государственные стратегии по противодействию распространению ложной информации. В связи с этим в разных странах вопрос ответственности за распространение заведомо ложной информации решается по-разному. В некоторых государствах за подобное деяние предусмотрена уголовная ответственность в зависимости от содержания распространяемой информации.

В России рассматриваемое деяние криминализировано в 2020 г. Причем в Уголовный кодекс РФ (далее – УК РФ) были введены сразу две новые статьи – статья 207[1] «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан» и ст. 207[2] «Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия».

Если говорить о социальной обусловленности установления уголовной ответственности за распространение заведомо ложной информации, то в первую очередь необходимо отметить, что «главным социально-политическим основанием криминализации является общественная опасность деяния – то есть его способность причинить вред интересам и отношениям, охраняемым уголовным законом»[4].

В 2020 г. установление уголовной ответственности за распространение заведомо ложной информации, стало ответом на появлявшиеся со стремительной скоростью в сети «Интернет» ложные новости о ситуации и принимаемых мерах по недопущению распространения заболеваний, вызванных новой коронавирусной инфекцией[5]. Необходимо отметить, что с самого

[1] Бешукова З.М. Возраст наступления уголовной ответственности за распространение заведомо ложной информации в законодательстве России и зарубежных стран // Эпомен. 2024. № 90. С. 84–90.

[2] Бешукова З.М., Джинджолия Р.С. Противодействие экстремизму в Интернете: роль и значение федерального списка экстремистских материалов // Право и государство: теория и практика. 2023. № 4. С. 288–290.

[3] Эксперты ВЭФ назвали дезинформацию главным глобальным риском в двухгодичной перспективе. URL: https://tass.ru/mezhdunarodnaya-panorama/19707211 (дата обращения: 10.02.2025).

[4] Дулькина Л.В. Уголовная ответственность за публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации и исполнении государственными органами Российской Федерации своих полномочий: дис. … канд. юрид. наук. Ставрополь, 2023. С. 27.

[5] Трахов А.И., Бешукова З.М. Распространение заведомо ложной информации (ст. 207.1 и 207.2 УК РФ): новые составы преступлений с признаком публичности // Теория и практика общественного развития. 2020. № 6. С. 78–82.

начала пандемии её непременным спутником стала ложная информация. Отсутствие знаний о вирусе создавало идеальную почву для роста фейковых новостей и теорий заговора, а также способствовало повышению уровня тревожности и стресса у людей. И, главное, ложная информация оказывала прямое воздействие на принятие ими решений. Люди отказывались делать прививку, что, в свою очередь, представляло реальную угрозу как их собственному здоровью и жизни, так и другим лицам.

Кроме того, в кризисной ситуации ложная информация способствовала распространению паники. Например, слухи о скором дефиците продуктов провоцировали скупку товаров, в результате чего происходило их «вымывание» с полок магазинов и создавалось ложное ощущение нехватки продуктов. Впрочем, массовая скупка товаров вполне может привести к реальному дефициту, что ставит под угрозу продовольственную безопасность.

В контексте изложенного необходимо вспомнить и то, что ложная информация во время пандемии способствовала поляризации общества, усиливая разногласия между различными группами людей. Именно в период пандемии во многих странах произошел скачок роста преступлений экстремистской направленности при общем снижении уровня преступности[6]. Так, еще в мае 2020 г. Генеральный секретарь ООН охарактеризовал происходящее в мире не иначе как «цунами ненависти и ксенофобии»[7].

В контексте рассматриваемого вопроса важно отметить, что распространение информации, не соответствующей действительности, стало непременным спутником практически всех трагических событий в нашей стране, что, в свою очередь, представляет реальную опасность для общественного порядка и общественной безопасности. Доказательством этого является пожар в г. Кемерово в марте 2018 г. Тогда ложные сведения о количестве погибших, появившиеся в сети «Интернет», спровоцировали стихийный митинг, состоявшийся возле областной администрации[8].

Приведенные примеры позволяют с достоверностью утверждать, что на сегодняшний день социальная обусловленность принятия федерального закона, вносящего обозначенные выше изменения в уголовный закон, не вызывает сомнений.

Спустя два года УК РФ дополнен новой статьей 207[3], регламентирующей ответственность за публичное распространение заведомо ложной информации об использовании Вооруженных Сил РФ. Данная новелла уголовного закона стала правовым ответом на действия коллективного Запада, ведущего информационную (информационно-психологическую) войну против России, которая приобрела поистине беспрецедентные масштабы.

Заключение. Следует констатировать, что в современном мире информация играет ключевую роль в жизни общества. Она влияет на принятие решений, формирование общественного мнения и даже на политическую стабильность государств. Неконтролируемое распространение ложной информации через традиционные и новые медиа создает явную и непосредственную угрозу «ментальной безопасности» личности и всего социума в информационном пространстве[9], поэтому государства вынуждены принимать меры для борьбы с этим явлением, включая и такие жесткие, как уголовно-правовые средства.

В условиях глобализации и быстрого распространения информации важно создавать правовые механизмы, которые бы обеспечивали безопасность общества и государства. Установление уголовной ответственности за распространение заведомо ложной информации в нашей стране является необходимой мерой, можно сказать вынужденным шагом, направленным на обеспечение общественной безопасности

[6] Бешукова З.М. Механизм уголовно-правового противодействия экстремистской деятельности: содержание, структура, основные направления оптимизации: дис. … д-ра юрид. наук. Краснодар, 2020. С. 225.

[7] Трахов А.И., Бешукова З.М. Указ. соч. С. 78–82.

[8] Пандемия ненависти. // Un.org.ru URL: https://www.un.org/ru/hate-speech/impact-and-prevention/a-pandemic-of-hate (дата обращения: 10.02.2025).

[9] Дулькина Л.В. Указ соч. С.26.

Список источников

1. Бешукова З. М. Возраст наступления уголовной ответственности за распространение заведомо ложной информации в законодательстве России и зарубежных стран // Эпомен. 2024. № 90. С. 84–90.

2. Бешукова З. М. Механизм уголовно-правового противодействия экстремистской деятельности: содержание, структура, основные направления оптимизации: дис. … д-ра юрид. наук. Краснодар, 2021. 632 с.

3. Бешукова З.М., Джинджолия Р.С. Противодействие экстремизму в Интернете: роль и значение федерального списка экстремистских материалов // Право и государство: теория и практика. 2023. № 4. С. 288–290.

4. Дулькина Л.В. Уголовная ответственность за публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации и исполнении государственными органами Российской Федерации своих полномочий: дис. … канд. юрид. наук. Ставрополь, 2023. 187 с.

5. Трахов А.И., Бешукова З.М. Распространение заведомо ложной информации (ст. 207.1 и 207.2 УК РФ): новые составы преступлений с признаком публичности // Теория и практика общественного развития. 2020. № 6. С. 78–82.

6. Пандемия ненависти. // Un.org.ru URL: https://www.un.org/ru/hate-speech/impact-and-prevention/a-pandemic-of-hate (дата обращения: 10.02.2025).

References

1. Beshukova Z.M. The age of criminal liability for the dissemination of knowingly false information in the legislation of Russia and foreign countries // Epomen. 2024. № 90. P. 84–90.

2. Beshukova Z.M. The mechanism of criminal legal counteraction to extremist activities: content, structure, main directions of optimization: dis. ... doctor of Law. Krasnodar, 2021. 632 p.

3. Beshukova Z.M., Dzhindzholia R.S. Countering extremism on the Internet: the role and significance of the federal list of extremist materials // Law and State: Theory and Practice. 2023. No. 4. P. 288–290.

4. Dulkina L.V. Criminal liability for public dissemination of knowingly false information about the use of the Armed Forces of the Russian Federation and the execution by state bodies of the Russian Federation of their powers: dis. ... cand. of Law. Stavropol, 2023. 187 p.

5. Trakhov A.I., Beshukova Z.M. Dissemination of knowingly false information (Articles 207.1 and 207.2 of the Criminal Code of the Russian Federation): new offenses with publicity // Theory and practice of social development. 2020. No. 6. P. 78–82.

6. A pandemic of hate. // Un.org.ru URL: https://www.un.org/ru/hate-speech/impact-and-prevention/a-pandemic-of-hate (accessed: 10.02.2025).

Информация об авторах

З.М. Бешукова — доктор юридических наук, доцент Адыгейского государственного университета.

М.А. Меретукова — преподаватель юридического факультета Адыгейского государственного университета.

Information about the authors

Z.M. Beshukova — Doctor of Law, Associate Professor at the Adygeya State University.

M.A. Meretukova — lecturer at the Faculty of Law of the Adygeya State University.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

УДК 343.98
ББК 67.53

Роль специальных знаний в обеспечении защиты от информации экстремисткой направленности

Леонид Григорьевич Бордюгов
Федеральное государственное бюджетное учреждение «Донецкая лаборатория судебной экспертизы Министерства юстиции Российской Федерации», Донецк, Россия

Email: Leonidbrd@yandex.ru

Аннотация. Проблема экстремизма, а именно распространение идей, отличных от устоявшихся правовых и других норм социального поведения, является проблемой для всего мира. Экстремизм, под которым понимают идеологию и практику использования крайних, противоправных (нередко насильственных) мер и действий для достижения конкретной цели, существует не только в реальной жизни, а и в виртуальной. Идеи экстремизма проникают в социальные сети, в Интернет и разносятся по всему миру. Несколько лет назад распространение информации экстремистского характера осуществлялось в основном через печатные издания, сейчас же это происходит через социальные сети, через Интернет. Если раньше экстремистские проявления носили локальный характер, то в последнее время, с учетом компьютерных технологий, они переросли в глобальный. В деятельности по защите от информации экстремисткой направленности важная роль отведена судебной экспертизе. Именно использование специальных знаний правоохранительными органами и судом в деле борьбы с таким деструктивным явлением, как экстремизм, позволяет давать решительный отпор всем проявлениям этого негативного явления современности.
Ключевые слова: экстремизм, информация экстремистской направленности, расследование преступлений экстремистской направленности, специальные знания, судебная психолого-лингвистическая экспертиза.
Научная специальность: 5.1.2. Публично-правовые (государственно-правовые) науки
Для цитирования: Бордюгов Л.Г. Роль специальных знаний в обеспечении защиты от информации экстремисткой направленности // Мир криминалистики. 2025. № 1. С. 30-36

The role of special knowledge in providing protection from extremist information

Leonid G. Bordyugov
Federal State Budgetary Institution «Donetsk Laboratory of Forensic Examination of the Ministry of Justice of the Russian Federation», Donetsk, Russia

Email: Leonidbrd@yandex.ru

Abstract. The problem of extremism, namely the dissemination of ideas that differ from established legal and other norms of social behavior, is a problem for the entire world. Extremism, which is understood as the ideology and practice of using extreme, illegal (often violent) measures and actions to achieve a specific goal, exists not only in real life, but also in virtual life. Extremist ideas penetrate social networks, the Internet and spread throughout the world. Several years ago, the dissemination of extremist information was carried out mainly through printed publications, but now it happens through social networks, through the Internet. If earlier extremist manifestations were local in nature, then recently, taking into account computer technologies, they have grown into a global one. In the activities to protect against extremist information, an important role is given to forensic examination. It is the use of special knowledge by law enforcement agencies and the court in the fight against such a destructive phenomenon as extremism that allows us to give a decisive rebuff to all manifestations of this negative phenomenon of our time.
Keywords: extremism, information of extremist nature, investigation of crimes of extremist nature, special knowledge, forensic psychological and linguistic examination.
For citation: Bordyugov L.G. The role of special knowledge in providing protection from extremist information // The world of criminology. 2025;(1):30-36

Введение. Наше государство, как бы оно ни называлось — Русь, Российская империя, СССР, Российская Федерация, — на протяжении веков подвергалось нападениям со стороны западных держав. Вспомним сражения Александра Невско-

го, Петра I, Отечественную войну 1812 года, Первую мировую, Гражданскую войну, Великую Отечественную войну, а также продвижение НАТО на восток к границам России.

Уместно вспомнить слова известного русофоба Збигнева Бжезинского, который говорил: «Мы боремся с Россией – как бы она ни называлась»[1]. Эта борьба, помимо военных действий, велась и ведётся самыми уродливыми и изощренными формами, в том числе различными террористическими и экстремистскими проявлениями.

Не на последнем месте стоит и информационная война. Стремительное развитие информационных технологий только способствует этому.

Основная часть. Что такое информация и почему во все времена ей уделяется такое пристальное внимание со стороны учёных, правоохранителей, простых людей?

Информация в словарях и энциклопедиях определяется как «сведения о чём-либо»[2], «сообщение о положении дел где-либо, о каких-либо событиях»[3], «осведомление, сообщение о каком-либо событии»[4]. Примерно такое же определение понятия информации дают и другие, более современные источники[5].

Некоторые ученые считают, что эти сведения или сообщения передаются только людьми[6]. Хотя в современном мире такое мнение неприемлемо, поскольку информацию, благодаря искусственному интеллекту, может формировать, систематизировать и передавать и машина.

Информация – это и то, что человек черпает из окружающего мира с первых дней своей жизни. Теплое материнское молоко – это вкусно, солнечный зайчик в глаза – это ярко, прикосновение к крапиве – это больно и т.д. Это полезная информация, которая помогает человеку выживать.

Дальше детский сад, школа и т.д. Человек начинает черпать информацию у своих сверстников, из учебников, книг и т.п. Воздействие информации на каждого человека различно, поскольку каждый человек оценивает и воспринимает её по-своему. Поэтому даже среди братьев, казалось бы, воспитанных в одних условиях, в одном обществе, в одной семье, один может стать героем, а другой — предателем. Пример тому — литературные образы сыновей Тараса Бульбы у Н. В. Гоголя. В этом и заключается влияние, в том числе и информации, на человека.

Следует отметить, что ещё каких-нибудь 40 лет назад в нашей стране (тогда СССР) поток информации был незначительным: не только потому, что существовала цензура не только потому, что были ограничены теле- и радиовещание иностранных каналов, но и потому, что сам массив информации был гораздо меньше.

С внедрением Интернета в повседневную жизнь любой человек имеет доступ к неограниченному массиву информации, порой далеко не полезной.

Информация в современном мире — оружие, действующее не только на умы и психику людей, но и убивающее, хоть и опосредованно.

Конечно, это касается не в последнюю очередь информации экстремистской направленности.

Воздействуя на умы тысяч и тысяч людей, информация экстремисткой направленности «разъедает» их души и психику. Человек, который не способен к анализу данной информации, может стать внушае-

---

[1] Ракитянский О.В. Украинская чума: История противостояния: 1945-1955 гг. М.: Родина, 2022. С. 102.

[2] Словарь иностранных слов. – 7-е изд., перераб. М.: Русский язык, 1980. С. 205.

[3] Словарь русского языка: В 4-х т./АН СССР, Ин-т рус. яз.; Под ред. А.П. Евгеньевой. 3-е изд. стереотип. М.: Русский язык, 1985-1988. Т. I. А – Й. 1985. С. 674.

[4] Большая советская энциклопедия: [в 51 томе] / гл. ред. Б.А. Введенский. - 2-е изд. М.: Большая советская энциклопедия, 1949 - 1958. Т.18. Индекс – Истон. С.331.

[5] Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80000 слов и фразеологических выражений / Российская академия наук. Институт русского языка им. В.В. Виноградова. – 4-е изд., доп. М.: ООО «А ТЕМП», 2006. С. 250; Ушаков Д.Н. Большой толковый словарь современного русского языка. 180 000 слов и словосочетаний. М.: Альта-Принт: ДОМ. XXI век, 2009. VIII, С. 313.

[6] Философский энциклопедический словарь / Гл. ред. Л.Ф. Ильичев, П.Н. Федосеев, С.М. Ковалев, В.Г. Панов. М.: Сов. Энциклопедия, 1983. С. 217.

мой игрушкой в чужих руках, способной на любые действия, даже на преступления по приказу «хозяина».

Именно на это рассчитывают спецслужбы Украины, которые одурманивая свой народ и другие народы, взяли на вооружение геббельсовские технологии, создавая практику «фейковых» новостей, «альтернативных фактов» или «постправды»[7].

Следует отметить, что идеологией экстремизма, которая присуща современной Украине, отрицается любое инакомыслие, при этом жестко насаждается своя собственная система политических, идеологических, религиозных взглядов.

Особенно остро это стало проявляться после 2014 года, то есть после государственного переворота на Украине, когда немногочисленная, но вместе с тем активная группа так называемых «свидомых» смогла не только подчинить себе малоактивное, полуспящее большинство населения Украины, но и заставить его поверить в то, что рецепт процветания Украины – это «одна нация, один народ», несмотря на то, что на Украине, кроме украинцев, проживают также представители других национальностей и народностей, прежде всего русские, белорусы, татары, поляки, венгры, евреи и др.

Преследование за иные политические, идеологические, религиозные взгляды на Украине стало нормой государственной политики, инакомыслие выкорчевывается путем преследования неугодных, фабрикования уголовных дел и даже путем убийств. Примером может служить убийство в апреле 2015 года журналиста Олега Бузины, который выступал за сближение Украины с Россией.

От своих сторонников идеологи экстремистских формирований требуют слепого повиновения и исполнения всех, даже самых абсурдных и преступных приказов. Свидетельством этому может служить массовое убийство военнослужащими ВСУ мирных граждан в селе Русское Поречное. Несмотря на то, что это злодеяние было показано по всем каналам Российской Федерации, а также по ряду зарубежных каналов несмотря на то, что об этом узнал весь мир, международные организации, в частности ООН, Красный Крест ограничились общими фразами, по сути дела, как это было всегда «выразили озабоченность» и только.

Запад на протяжении десятилетий пытался и пытается воздействовать на умы наших граждан, особенно молодежи. Чего стоит, например, «Американская доктрина против СССР», провозглашённая директором ЦРУ Аленом Даллесом в 1945 году. В частности, в борьбе с Советским Союзом предлагалось «вдалбливать в человеческое сознание культ секса, насилия, садизма и предательства», делая основную ставку на то, что молодежь необходимо «разлагать, развращать, растлевать»[8].

Это все попадало в «благодатную» почву украинского национализма, который шел даже дальше, чем от него требовали западные наставники. Так, например, украинская экстремистская националистическая организация УНА-УНСО, возникшая в 1990 году (в том числе и при попустительстве властей), изначально основывалась на националистической идеологии (то есть на формуле «одна нация – одно государство»). Однако с середины 1990-х гг. она принимает концепцию необходимости создания украинской империи «от Адриатики до Берингова пролива» со столицей в Киеве. Позже эта идея была отвергнута, скорее всего, по указке западных кураторов, однако, глядя на происходящие в настоящее время события, не забыта.

Опасность экстремизма заключается в том, что он «способен сформировать соответствующее массовое сознание» и «манипулировать таковым»[9].

Следует отметить, что, если раньше распространение информации экстре-

[7] Борисов А.Ю. Возвращение зла: о нацизме и его наследниках // Международная жизнь. № 6. 2023. С. 53.

[8] Мартынов М.Л., Клименко П.В., Попов А.Н. Борьба за умы молодёжи в современном глобальном мире // Актуальные проблемы педагогики и психологии. 2020. Том 1. № 1. С. 6.

[9] Писаренко О.Н. Терроризм как крайняя форма выражения экстремизма // Научные проблемы гуманитарных исследований. 2010. № 10. С. 241.

мистского характера осуществлялось в основном через печатные издания, то в настоящее время это происходит через социальные сети, через Интернет. Данный процесс особенно влияет на сознание молодежи.

Если раньше экстремистские проявления носили локальный характер, то в последнее время, с учетом компьютерных технологий, они носят глобальный характер[10]. Проблемам распространения идей экстремизма через сеть Интернет и влияния данного процесса на сознание молодежи посвящен ряд работ отечественных ученых и специалистов[11].

Компьютерные технологии и Интернет предоставили фактически неограниченные возможности и ресурсы не только для свободного создания, распространения и хранения полезной информации, но и для информации деструктивного направления, совершенствования формы и методов манипулирования информацией с целью неправомерного влияния на сознание и поведение как отдельных граждан или их групп, так и социума в целом. Этим не гнушаются современные западные политики и организации (например, американское агенство USAID), науськивая своих украинских «вассалов».

В настоящее время в Украине созданы целые службы (например, центр информационно-психологических операций (ЦИПСО)), которые нацелены на разжигание ненависти ко всему русскому, на разработку и вбрасывание в прессу, в Интернет неправдивой информации. Чего только стоит история с Бучей. Служба безопасности Украины, используя методы гитлеровской охранки, путем запугивания, путем шантажа привлекает к совершению экстремистских действий, террористических актов, как граждан своей страны, так и граждан других государств, в том числе и России. Примерами могут послужить убийство военного журналиста Владлена Татарского, террористический акт в «Крокус Сити Холле». Таких примеров можно привести множество и везде «торчат уши» украинских спецслужб.

Экстремистские методы и способы борьбы пропагандируются как наиболее действенные в любой ситуации: от социальной проблемы до военного конфликта. В комплексе с социально-экономическими проблемами и политической нестабильностью распространение экстремистских идеологий способно существенно повредить реализации прав, свобод человека и гражданина, а также приостановить развитие общества и государства.

Пичкая граждан, особенно молодежь, различной информацией экстремисткой направленности, спецслужбы Украины пытаются завербовать граждан других государств, в том числе и России, для совершения на территории России различных правонарушений, в том числе и террористических актов. И следует сказать, что довольно часто это у них получается.

Всё это ещё раз указывает на необходимость системного противодействия этому явлению, на необходимость активизации процесса формирования и внедрения в следственную практику новейших методик расследования преступлений, в том числе и преступлений экстремисткой направленности.

В последнее время появилось много работ отечественных учёных (монографий, диссертаций), не говоря уже о статьях в научных журналах, посвященных вопросам противодействия преступлениям экстремистской направленности, в том числе и вопросам криминалистической методики их расследования[12].

[10] Салахутдинов А.А. Социальные сети как информационный канал экстремистского материала // Молодой ученый. 2014. № 17 (76). С. 564.

[11] Малакаев О.С. Экстремизм в социальных сетях // Вестник Института комплексных исследований аридных территорий. 2018. № 2(37). С. 83-86; Панфилова Ю.С. Экстремизм в виртуальной среде как социальная проблема: отражение в сознании молодежи // Альманах современной науки и образования. Тамбов: Грамота, 2014. Выпуск 9. С. 101-104.

[12] Петрянин А.В. Концептуальные основы противодействия преступлениям экстремистской направленности: теоретико-прикладное исследование: монография. Под редакцией А.П. Кузнецова. М.: Проспект, 2017. 335 с.; Узденов Р.М. Экстремизм: криминологические и уголовно-правовые проблемы противодействия: дис. ... канд. юрид. наук. М., 2008. 220 с.

Публикации в СМИ свидетельствуют о том, что экстремистские проявления в нашей стране происходят довольно часто. Это может оказывать влияние на политическую стабильность нашего государства. В связи с указанным, необходимо разработать и внедрить комплекс мер, которые будут уменьшать проявления экстремизма и различные связанные с этим риски. Проявления экстремизма, даже незначительные, являются серьезной проблемой для любого государства, поэтому борьба с этим негативным явлением должна стать задачей номер один для всего нашего общества. Этому вопросу должное внимание должны уделять, прежде всего, правоохранительные органы, деятельность которых в области предупреждения преступлений экстремистской направленности в первую очередь должна быть научно обоснованной и направленной на выявление обстоятельств, способствующих совершению данных преступлений.

Особая роль в этой нелёгкой, но благородной борьбе отведена и судебной экспертизе. Таким образом, важное значение для раскрытия и расследования преступлений экстремисткой направленности играет использование специальных знаний, в частности знаний в области психологии, лингвистики, культурологии, религиоведения и т.п.[13].

Примером может послужить комплексная судебная психолого-лингвистическая экспертиза. В процессе её проведения эксперты изучают представленные на исследование материалы (скриншоты, литературные произведения и т.д.), на основании чего устанавливают, содержится ли в указанных материалах информация, имеющая признаки экстремизма.

Кроме этого, решаются вопросы по установлению признаков психологического воздействия того или иного высказывания на аудиторию (при этом под аудиторией понимаются любые коммуниканты – участники митинга, слушатели выступления и т.д.), по установлению эмоционального состояния автора текста, и соответствия текста его возрасту и т.п.

Перечислять случаи назначения комплексной судебной психолого-лингвистической экспертизы нет смысла, поскольку у органов предварительного расследования и судов могут возникать самые различные вопросы.

Заключение. В настоящее время государство уделяет пристальное внимание обеспечению защиты от информации экстремистской направленности. В частности, в ряде государственных судебно-экспертных учреждениях Министерства юстиции Российской Федерации создаются отделы по исследованию материалов, имеющих признаки экстремистской направленности, сотрудники которых проводят судебно-лингвистические, комплексные судебные психолого-лингвистические экспертизы.

Именно «совместные усилия правоохранительных органов, судов, судебно-экспертных учреждений, общественности смогут не только противостоять экстремизму, но и дать решительный отпор всем проявлениям этого негативного явления современности»[14].

Список источников

1. Аминев Ф.Г. Особенности использования специальных знаний как составной части методики расследования преступлений, связанных с экстремизмом и терроризмом // Правовое государство: теория и практика. – 2017. – № 3 (49). – С. 130–137.

2. Большая советская энциклопедия: [в 51 томе] / гл. ред. Б.А. Введенский. – 2-е изд. – М.: Большая советская энциклопедия, 1949 – 1958. – Т.18. Индекс – Истон. – 620 с.

[13] Аминев Ф.Г. Особенности использования специальных знаний как составной части методики расследования преступлений, связанных с экстремизмом и терроризмом // Правовое государство: теория и практика. 2017. № 3 (49). С. 135.

[14] Бордюгов Л.Г. Применение специальных знаний в расследовании проявлений религиозного экстремизма // Антикриминальная политика: актуальные проблемы регионов: сб. статей по матер. всерос. науч.-практ. конф., (Луганск, 15 ноября 2024 года) / под ред. А.М. Моисеева, С.В. Кондратюка; Луганский юридический институт (филиал) Университета прокуратуры Российской Федерации. Самара: Самарама, 2024. С. 242.

3. Бордюгов Л.Г. Применение специальных знаний в расследовании проявлений религиозного экстремизма // Антикриминальная политика: актуальные проблемы регионов: сб. статей по матер. всерос. науч.-практ. конф. (Луганск, 15 ноября 2024 года) / под ред. А.М. Моисеева, С.В. Кондратюка; Луганский юридический институт (филиал) Университета прокуратуры Российской Федерации. – Самара: Самарама, 2024. – С. 238–242.

4. Борисов А.Ю. Возвращение зла: о нацизме и его наследниках // Международная жизнь. – № 6. – 2023. – С. 50–63.

5. Малакаев О.С. Экстремизм в социальных сетях // Вестник Института комплексных исследований аридных территорий. – 2018. – № 2 (37). – С. 83–86.

6. Мартынов М.Л., Клименко П.В., Попов А.Н. Борьба за умы молодёжи в современном глобальном мире // Актуальные проблемы педагогики и психологии. – 2020. – Том 1. – № 1. – С. 5–8.

8. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80000 слов и фразеологических выражений / Российская академия наук. Институт русского языка им. В.В. Виноградова. 4-е изд., доп. – М.: ООО «А ТЕМП», 2006. – 944 с.

9. Панфилова Ю.С. Экстремизм в виртуальной среде как социальная проблема: отражение в сознании молодежи // Альманах современной науки и образования. – Тамбов: Грамота, 2014. – Выпуск 9. – С. 101–104.

10. Писаренко О.Н. Терроризм как крайняя форма выражения экстремизма // Научные проблемы гуманитарных исследований. – 2010. – № 10. – С. 241–248.

11. Ракитянский О.В. Украинская чума: История противостояния: 1945-1955 гг. – М.: Родина, 2022. – 304 с.

12. Салахутдинов А.А. Социальные сети как информационный канал экстремистского материала // Молодой ученый. – 2014. – № 17 (76). – С. 561–564.

13. Словарь иностранных слов. – 7-е изд., перераб. – М.: Русский язык, 1980. – 624 с.

14. Словарь русского языка: В 4-х т./АН СССР, Ин-т рус. яз.; Под ред. А.П. Евгеньевой. 3-е изд. стереотип. – М.: Русский язык, 1985-1988. – Т. I. А – Й. – 1985. – 696 с.

15. Узденов Р.М. Экстремизм: криминологические и уголовно-правовые проблемы противодействия: дис. ... канд. юрид. наук: 12.00.08 / Узденов Расул Магометович; [Место защиты: Рос. акад. правосудия]. – М., 2008. – 220 с.

16. Ушаков Д.Н. Большой толковый словарь современного русского языка. 180 000 слов и словосочетаний. – М.: Альта-Принт: ДОМ. XXI век, 2009. – VIII, 1239 с.

17. Философский энциклопедический словарь / Гл. ред. Л.Ф. Ильичев, П.Н. Федосеев, С.М. Ковалев, В.Г. Панов. – М.: Сов. Энциклопедия, 1983. – 840 с.

18. Экстремизм: стратегия противодействия и прокурорский надзор / П.В. Агапов [и др.]; Акад. Генер. прокуратуры Рос. Федерации. – М.: Проспект, 2017. – 427 с.

References

1. Aminev F.G. Features of the use of specialized knowledge as an integral part of the methodology for investigating crimes related to extremism and terrorism // The rule of law: theory and practice. – 2017. – №. 3 (49). – P. 130–137.

2. Great Soviet Encyclopedia: [in 51 volumes] / editor-in-chief B.A. Vvedensky. - 2nd edition. – Moscow: Great Soviet Encyclopedia, 1949 - 1958. – Vol. 18. Index - historical. – 620 p.

3. Bordyugov L.G. Application of specialized knowledge in the investigation of manifestations of religious extremism // Anti-criminal policy: current problems of the regions: collection of articles based on the materials of the All-Russian scientific and practical conference, (Lugansk, November 15, 2024) / edited by A.M. Moiseev, S.V. Kondratyuk; Lugansk Law Institute (branch) of the University of the Prosecutor's Office of the Russian Federation. – Samara: Samara, 2024. – Pp. 238–242.

4. Borisov A.Yu. The Return of Evil: About Nazism and Its Heirs // International Affairs. – No. 6. – 2023. – Pp. 50-63.

5. Malakaev O.S. Extremism in Social Networks // Bulletin of the Institute for Comprehensive Research of Arid Territories. – 2018. – No. 2 (37). – Pp. 83–86.

6. Martynov M.L., Klimenko P.V., Popov A.N. The Struggle for the Minds of Young People in the Modern Global World // Actual Problems of Pedagogy and Psychology. – 2020. – Vol. 1. – No. 1. – Pp. 5–8.

8. Ozhegov S.I., Shvedova N.Yu. Explanatory Dictionary of the Russian Language: 80,000 Words and Phraseological Expressions / Russian Academy of Sciences. Vinogradov Russian Language Institute. – 4th ed., supplemented. – Moscow: OOO "A TEMP", 2006. – 944 p.

9. Panfilova Yu.S. Extremism in the Virtual Environment as a Social Problem: Reflection in the Consciousness of Young People // Almanac of Modern Science and Education. – Tambov: Gramota, 2014. – Issue 9. – P. 101–104.

10. Pisarenko O.N. Terrorism as an Extreme Form of Expression of Extremism // Scientific Problems of Humanitarian Research. – 2010. – No. 10. – P. 241–248.

11. Rakityansky O.V. Ukrainian plague: History of confrontation: 1945-1955. – M.: Rodina, 2022. – 304 p.

12. Salakhutdinov A.A. Social networks as an information channel for extremist material // Young scientist. – 2014. – No. 17 (76). – pp. 561–564.

13. Dictionary of foreign words. – 7th ed., revised. – M.: Russian language, 1980. – 624 p.

14. Dictionary of the Russian language: In 4 volumes/AS USSR, Institute of Russian. language; Ed. A.P. Evgenieva. 3rd ed. stereotype. – M.: Russian language, 1985-1988. – T. I. A – J. – 1985. – 696 p.

15. Uzdenov R.M. Extremism: criminological and criminal-legal problems of counteraction: dis. ... Cand. of Law: 12.00.08 / Uzdenov Rasul Magometovich; [Place of protection: Russian Academy of Justice]. – M., 2008. – 220 p.

18. Ushakov D.N. Large explanatory dictionary of the modern Russian language. 180 000 words and phrases. – M.: Alta-Print: DOM. XXI century, 2009. – VIII, 1239 p.

17. Philosophical encyclopedic dictionary / Edited by L.F. Ilyichev, P.N. Fedoseyev, S.M. Kovalev, V.G. Panov. – M.: Sov. Encyclopedia, 1983. – 840 p.

18. Extremism: strategy of counteraction and prosecutorial supervision / P.V. Agapov [et al.]; Acad. General. Prosecutor's Office of the Russian Federation. – M.: Prospect, 2017. – 427 p.

Информация об авторе

Л.Г. Бордюгов — директор Федерального государственного бюджетного учреждения «Донецкая лаборатория судебной экспертизы Министерства юстиции Российской Федерации», кандидат юридических наук.

Information about the author

L.G. Bordyugov — Director of the Federal State Budgetary Institution "Donetsk Laboratory of Forensic Examination of the Ministry of Justice of the Russian Federation", Candidate of Law.

УДК 343.3/.7
ББК 67.408.135

Ответственность за киберпреступления в международных и Российских нормах

Андрей Петрович Бохан
Ростовский филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия им. В.М. Лебедева», Ростов-на-Дону, Россия,
Email: boxan@mail.ru

Аннотация. В статье рассмотрены вопросы установления уголовной ответственности за киберпреступления как в российском уголовном законодательстве, так и в международных нормах. Автором проведён краткий сравнительный анализ, который позволил сделать вывод о том, что вопросы уголовной ответственности за рассматриваемые деяния присутствуют в российском уголовном праве и международном.
Ключевые слова: киберпреступления, киберпространство, преступления в сфере компьютерной информации, уголовное законодательство Российской Федерации, международно-правовые акты.
Научная специальность: 5.1.4. Уголовно-правовые науки
Для цитирования: Бохан А.П. Ответственность за киберпреступления в международных и российских нормах // Мир криминалистики. 2025. № 1. С. 37-41

Responsibility for cybercrimes in international and Russian norms

Andrey P. Bokhan
Russian State University Named After V.M. Lebedev, Rostov-on-Don, Russia,
Email: boxan@mail.ru

Abstract. The article considers the issues of establishing criminal liability for cybercrimes in Russian criminal legislation, as well as in international norms. The author conducted a brief comparative analysis, which made it possible to conclude that the issues of criminal liability for the acts in question are present in Russian criminal law and international law.
Keywords: cybercrimes, cyberspace, crimes in the field of computer information, criminal legislation of the Russian Federation, international legal acts.
For citation: Bokhan A.P. Responsibility for cybercrime in international and Russian norms // The world of criminology. 2025;(1):37-41

Введение. Сегодня невозможно представить нашу жизнь без использования киберпространства. Киберсреда в настоящее время проникла практически во все сферы жизни общества, в том числе в экономические, политические и иные социальные процессы. Любое предприятие, учреждение либо организация, да и в целом конкретный человек, так или иначе, связан с микро- или макрокиберсредой, в которой он проводит большую часть личного и рабочего времени, и, соответственно, в ней происходит обмен денежными средствами, информацией и иными ценностями. В связи с чем киберпространство становится объектом пристального внимания злоумышленников, посягающих на неё и её объекты с целью хищения или нанесения иного вреда. При этом, основными детерминантами совершения преступлений рассматриваемой категории выступают большие потоки денежных средств и возможность совершить преступление удалённо, находясь в другом регионе или даже в другой стране, чем обеспечивается успешное заметание своих следов преступниками.

Основная часть. Преступления данного вида не только нарушают установленный порядок работы компьютерных и

иных телекоммуникационных сетей, причиняют им организационный, имущественный и иной вред, но и представляют угрозу для правоохраняемых интересов других хозяйствующих субъектов, общества и государства в целом.

Но по-прежнему среди широкого круга учёных в области уголовной политики Российской Федерации остается дискуссионным вопрос о границах перечня преступлений, который носит окраску «совершенные в сфере информационно-телекоммуникационных технологий» и категории «киберпреступлений». Одни авторы придерживаются мнения о том, что данные понятия являются синонимами, другие, как и мы, полагают, что последние являются основной составляющей преступлений в сфере высоких технологий [1].

Следует согласиться с позицией М.А. Простосердова, который видит киберпреступления как совокупность преступных деяний, оказывающих вредоносное воздействие на общественные отношения, совершаемые дистанционно посредством применения компьютерных средств, информационно-телекоммуникационных сетей и порожденного ими киберпространства [2].

По мнению некоторых специалистов, статистическая картина киберпреступлений, совершаемых на территории России, не соответствует его реальному состоянию. Латентность этого преступления оценивается экспертами в 90 %. Таким образом, регистрируется около десяти процентов фактов киберпреступлений от их реального количества [3].

Столь высокий уровень латентности киберпреступности обусловлен целом рядом объективных и субъективных факторов, среди которых:

1) недооценка общественной опасности киберпреступности на уголовно-политическом уровне;

2) нежелание и неумение правоохранителей противодействовать киберпреступности уголовно-правовыми средствами;

3) отсутствие должного финансирования субъектов противодействия киберпреступлениям;

4) незаинтересованность граждан и «собственников» коммерческих и иных организаций в информировании правоохранительных органов обо всех фактах совершения киберпреступлений;

5) сложности проведения расследований по делам о киберпреступлениях, связанных с установлением круга виновных лиц, их организованностью, межрегиональностью и т.д.

Также необходимо отметить, что нормы уголовного закона, являющиеся основой для преследования лиц, виновных в киберпреступлениях, обладают существенными недостатками с точки зрения криминализации и пенализации этого деяния.

Проблема борьбы с киберпреступностью является одной из самых острых проблем российского государства и мирового сообщества. Она во всех её проявлениях представляет собой реальную угрозу общественным и государственным интересам всех стран.

Всё вышеизложенное указывает на актуальность темы исследования.

В статье мы хотим дать краткий анализ международным и российским нормам, предусматривающим ответственность за совершение киберпреступлений.

Киберпреступность на протяжении последних десятилетий является, пожалуй, самой трансформируемой категорией преступлений, поскольку с изменением мировых экономических процессов, развитием информационно-телекоммуникационных технологий трансформируется и вектор интересов злоумышленников, а вместе с ними способы и методы совершения ими преступлений.

Выделяют три стадии эволюционирования киберпреступлений в России, которые связаны: с появлением электронных почтовых сообщений в 80-х годах прошлого века, с развитием веб-браузеров в 90-х годах прошлого столетия и активным использованием социальных сетей в самом начале нынешнего тысячелетия. Все три стадии связаны между собой увеличением количества пользователей компьютерных устройств посредством информационно-телекоммуникационной сети

«Интернет». При этом нами отмечается ещё одна, четвёртая и, как полагается, основная стадия развития киберпреступности как в России, так и во всем мире, связанная с использованием мессенджеров на мобильных устройствах, которые являются наиболее уязвимым средством коммуникации, с которого осуществляется доступ к персональным данным пользователей и, главное, к их платежным сервисам. Четвёртая стадия киберпреступности активно развивается в стране с 2019 года по настоящее время и является наиболее масштабной и распространённой.

Особо отметим, что приоритетным направлением внутренней политики Российской Федерации является «Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы», которая определяет формирование единого информационного пространства, соответствующей ему инфраструктуры и развитие информационно-телекоммуникационных технологий [4].

В настоящее время уголовное законодательство Российской Федерации к киберпреступлениям относит составы уголовно-наказуемых деяний, содержащиеся в главе 28 УК РФ «Преступления в сфере компьютерной информации» (ст.ст. 272-274.2), где объект преступления – совокупность общественных отношений, связанных с обеспечением информационной безопасности пользователей информационно-телекоммуникационного пространства, а также нерушимая целостность критической информационной инфраструктуры Российской Федерации [5]. Иными словами, уголовно-наказуемые деяния, связанные исключительно с информационно-телекоммуникационными-технологиями.

Основной акт международно-правового реагирования на киберпреступность — Будапештская конвенция о преступности в сфере компьютерной информации [6], которая рассматривает ограниченные направления компьютерных преступлений: против конфиденциальности, целостности и доступности компьютерных систем и сетей, компьютерных данных; против злоупотребления системами, сетями и данными; связанные с нарушением авторских и смежных прав и оборотом детской порнографии. Разработка и принятие данного документа сводится к началу 2000-х годов, когда киберпреступления не были так развиты и разнообразны, как в настоящее время. Актуальных проявлений киберпреступности таких, как мошенничества с использованием IP-телефонии, фейковых «интернет-сайтов», фишинга, криптовалютных финансовых пирамид, конвенция не предусматривает.

Национальное законодательство о киберпреступлениях в зарубежных странах было разработано ещё в 70-80 годах прошлого столетия. Первооткрывателями в данном направлении выступили США, которые в 1977 году разработали законопроект, устанавливающий уголовную ответственность за компьютерные преступления, на основе которого в 1984 году был принят «Закон о мошенничестве и злоупотреблении с использованием компьютеров», положения которого и включены в ныне действующий Титул 18 Свода законов США. Нормы данного закона предусматривают уголовную ответственность за компьютерный шпионаж; несанкционированный доступ или превышение санкционированного доступа к информации из правительственного ведомства США; неравномерное воздействие на компьютер, находящийся в исключительном пользовании правительственного ведомства США; мошенничество с использованием компьютера и т.д. [7].

Следует отметить, что именно представители США сделали основной прорыв в области шифрования (двойного шифрования) данных, которые передаются посредством информационно-телекоммуникационных каналов связи. Более того, в ФБР существует специальное программное обеспечение (система наблюдения) «Carnivore», позволяющее перехватить любые звонки или электронные сообщения на территории страны, что является действенной мерой по выявлению, пресечению и раскрытию киберпреступлений.

Принятый в 1990 году парламентом Соединённого Королевства «Закон о неправомерном использовании компьютеров» остаётся титульным законом страны в области противодействия компьютерным преступлениям и послужил вдохновением для создания аналогичного законодательства в Канаде и Северной Ирландии [8].

Как правило, указанные преступления носят межрегиональный, а в последнее время и международный характер. Они характеризуются чётким распределением ролей, методами конспирации и строго выстроенной иерархией, где нижнее звено, как правило, не осведомлено о высшем.

Привлечение к ответственности участников мошеннических схем в основном квалифицируется в составе организованной преступной группы, но и в случаях, когда предоставляются в следственные органы проведенные оперативниками комплексы оперативно-розыскных мероприятий, злоумышленников привлекают в качестве участников и организаторов преступных сообществ.

Заключение. Подводя итог, следует отметить, что внутреннее законодательство России в области противодействия киберпреступности, а также используемые способы, методы и средства обнаружения и документирования следов компьютерных преступлений, по нашему мнению, являются передовыми и современными по сравнению с законодательством большинства развитых стран. Однако существуют определенные недоработки, связанные с формированием единого понятийного аппарата о киберпреступлениях, определением статуса и регулирования оборота криптовалюты в стране, а также недоработки в техническом обеспечении и формировании специальных знаний у сотрудников правоохранительных органов.

Список источников

1. Бохан А.П. Меры Уголовно-правового реагирования на хищение цифровой информации / А. П. Бохан // Юридическая деятельность в условиях цифровизации: Сборник статьей по результатам международной научно-практической конференции, Симферополь, 23 марта 2021 года // Под редакцией Е.В. Евсиковой, В.С. Тихомаевой. – Симферополь: Ариал, 2021. С. 55-58.

2. Простосердов М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дисс. ... канд. юрид. наук: 12.00.08. Москва, 2016. 232 с.

3. Бохан А.П. Особенности квалификации мошенничества с использованием электронных средств платежа по признакам объективной стороны / А. Б. Шумилина, А. П. Бохан // Правовой порядок и правовые ценности: Сборник научных статей VII Национальной научно-практической конференции с международным участием, Дивноморское, 21–23 сентября 2023 года. – Дивноморское: ДГТУ-ПРИНТ, 2023. С. 553-556.

4. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // Kremlin.ru. URL.: http://www.kremlin.ru/acts/bank/41919/page/1 (дата обращения: 27.01.2025).

5. Бохан А. П. Правовое регулирование компьютерной информации как объекта уголовно-правовой охраны / А. П. Бохан, Т. И. Лиманцева // Юристъ-Правоведъ. – 2015. – № 3(70). – С. 38-41.

6. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) URL.: https://base.garant.ru. (дата обращения: 02.02.2025).

7. Волеводз А.Г. Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран / А.Г. Волеводз, Д.А. Волеводз // Правовые вопросы связи. – 2004. – № 1. – С. 42-48.

8. Кириленко В.П., Алексеев Г.В. Гармонизация Российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Европы // Всероссийский криминологический журнал. – 2020. – № 6. – С. 897-899.

References

1. Bohan A.P. Measures of Criminal Law Response to Digital Information Theft / A.P. Bohan // Legal Activities in the Context of Digitalization: Collection of Articles Based on the Results of an International Scientific and Practical Conference, Simferopol, March 23, 2021 / Edited by E.V. Evsikova, V.S. Tikhomaeva. –Simferopol: Limited Liability Company «Publishing House» Arial, 2021. P. 55-58.

2. Prostoserdov M.A. Economic crimes committed in cyberspace and countermeasures against them: diss.... cand. jurid. Sciences: 12.00.08. Moscow, 2016. 232 p.

3. Bohan A.P. Features of qualification of fraud using electronic means of payment on the grounds of an objective side/A. B. Shumilin, A. P. Bohan//Legal order and legal values: Collection of scientific articles of the VII National Scientific and Practical Conference with international participation, Divnomorskoye, September 21-23, 2023. - Divnomorskoe: DSTU-PRINT, 2023. P. 553-556.

4. Decree of the President of the Russian Federation of 09.05.2017 № 203 «On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030» // kremlin.ru. URL.: http://www.kremlin.ru/acts/bank/41919/page/1 (accessed: 27.01.2025).

5. Bohan A.P. Legal regulation of computer information as an object of criminal law protection/A.P. Bohan, T.I. Limantseva // Lawyer-Pravoveda. – 2015. – № 3(70). – P. 38-41.

6. ETS Convention on Crime in the Field of Computer Information No. 185 (Budapest, November 23, 2001) URL.: https://base.garant.ru. (accessed: 02.02.2025).

7. Volevodz A.G. Criminal legislation on liability for computer crimes: experience of different countries / A.G. Volevodz, D.A. Volevodz // Legal issues of communication. – 2004. – № 1. – P. 42-48.

8. Kirilenko V.P., Alekseev G.V. Harmonization of the Russian criminal legislation on combating cybercrime with the legal standards of Europe // All-Russian Criminological Journal. – 2020. – № 6. – P. 897-899.

Информация об авторе

А.П. Бохан — доцент кафедры уголовного права Ростовского филиала «Российского государственного университета правосудия им. В.М. Лебедева», кандидат юридических наук, доцент.

Information about the author

A.P. Bokhan — associate professor of the criminal law department of the Rostov branch of the V. M. Lebedev Russian State University of Justice, candidate of legal sciences, and associate professor.

УДК 343.9
ББК 67.410

Деанонимизация путем мониторинга сетевого трафика при расследовании IT-преступлений как элемент обеспечения информационной безопасности

Ольга Павловна Виноградова
Уральский юридический институт МВД России, Екатеринбург, Россия

Email: olga10vin@mail.ru

Аннотация. Глобальная цифровизация активно внедряется во все сферы человеческой жизнедеятельности. Положительный характер информационной среды наряду с высокой степенью общественного комфорта снижают уровень безопасности персональных данных, охраняемой законом компьютерной информации и информационного пространства в целом. Глобальная сеть Интернет, с одной стороны, становится средством хранения, поиска, обмена и получения информации, с другой – создает условия, способствующие совершению преступлений. Анонимизация личности преступника исследуемой категории деяния затрудняет деятельность правоохранительных органов по раскрытию и расследованию преступлений. Появление новых способов совершения преступлений в информационной среде требует постоянного совершенствования средств деанонимизации злоумышленников и четкого алгоритма действий сотрудников правоохранительных органов в различных следственных ситуациях. Идентификация личности преступника, скрывающегося за анонимностью, обеспеченной возможностями сети Интернет, – одна из ключевых задач, стоящих перед современными правоохранительными органами.

Ключевые слова: IT-преступления, киберпреступник, деанонимизация, сетевые технологии, информационная безопасность, компьютерно-техническая экспертиза, трафик, информационно-телекоммуникационные технологии.
Научная специальность: 5.1.4. Уголовно-правовые науки
Для цитирования: Виноградова О. П. Деанонимизация путем мониторинга сетевого трафика при расследовании IT-преступлений как элемент обеспечения информационной безопасности // Мир криминалистики. 2025. № 1. С. 42-47

Deanonymization by monitoring network traffic in the investigation of IT crimes as an element of ensuring information security

Olga P. Vinogradova
Ural Law Institute of the Ministry of Internal Affairs of Russia, Yekaterinburg, Russia

Email: olga10vin@mail.ru

Abstract. Global digitalization is actively being implemented in all spheres of each person's life. The positive nature of the information environment, along with a high degree of public comfort, reduces the level of security of personal data, legally protected computer information and the information space as a whole. The global Internet, on the one hand, becomes a means of storing, searching, exchanging and receiving information, on the other hand, it creates conditions conducive to the commission of crimes. Anonymization of the identity of the perpetrator of the investigated category of the act makes it difficult for law enforcement agencies to detect and investigate crimes. The emergence of new ways of committing crimes in the information environment requires constant improvement of the means of deanonymization of intruders and a clear algorithm of actions implemented by the subjects of investigation in various investigative situations. Identifying the identity of a criminal hiding behind the anonymity provided by the Internet is one of the key tasks facing modern law enforcement agencies.

Keywords: IT crimes, cybercriminal, deanonymization, network technologies, information security, computer and technical expertise, traffic, information and telecommunication technologies.
For citation: Vinogradova O. P. Deanonymization by monitoring network traffic in the investigation of IT crimes as an element of ensuring information security // The world of criminology. 2025;(1): 42-47

Введение. Стремительное развитие информационно-телекоммуникационных технологий и их повсеместное распространение привели к экспоненциальному росту

киберпреступности. Киберпреступники используют анонимность сети для совершения широкого спектра преступлений: от мошенничества и кражи персональных данных до распространения вредоносного программного обеспечения, организации террористических актов и торговли наркотиками. Анонимность, обеспечиваемая современными средствами сетевой коммуникации, значительно затрудняет выявление и изобличение злоумышленников, действующих в виртуальном пространстве. Без надежной привязки противоправных действий, совершаемых в киберпространстве, к реальному человеку, стоящему за ними, невозможно эффективное расследование IT-преступлений. Это приводит к тому, что значительная часть киберпреступлений остается нераскрытой, а виновные уходят от ответственности, что, в свою очередь, стимулирует дальнейший рост киберпреступности и создает угрозу информационной и национальной безопасности [2].

Основная часть. Мониторинг сетевого трафика является одним из активных методов деанонимизации, который может использоваться сотрудниками правоохранительных органов для установления личности подозреваемого в совершении преступлений в сети Интернет. Этот метод основан на перехвате и анализе данных, передаваемых между устройством пользователя и удаленными серверами, с целью выявления идентифицирующей информации, такой как IP-адрес, MAC-адрес, идентификаторы устройства, данные геолокации и т.п.

Для успешного применения метода мониторинга трафика сотрудник полиции должен обладать достаточными техническими знаниями в области сетевых технологий и информационной безопасности. В частности, он должен хорошо разбираться в принципах маршрутизации данных в IP-сетях, структуре сетевых пакетов, протоколах прикладного уровня (HTTP, FTP, POP3, SMTP и др.), системах доменных имен (DNS) и сетевых идентификаторах (IP-адрес, MAC-адрес). Также необходимо уметь работать с программными и аппаратными инструментами перехвата и анализа трафика, такими как сниферы (Wireshark, tcpdump), анализаторы протоколов, системы обнаружения вторжений (IDS) и средства глубокого анализа пакетов (DPI).

Перед началом мероприятий по мониторингу трафика сотрудник должен убедиться в наличии необходимых правовых оснований. Перехват и анализ сетевых данных затрагивает конституционные права граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, гарантированные статьей 23 Конституции РФ. Ограничение этих прав допускается только на основании судебного решения. Таким образом, проведение мероприятий по мониторингу трафика возможно только в рамках оперативно-розыскной деятельности или следственных действий при наличии возбужденного уголовного дела и соответствующего судебного разрешения. Сотрудник должен подготовить мотивированное постановление о проведении ОРМ, получить санкцию суда, а также вынести необходимые поручения оперативно-техническим подразделениям и операторам связи.

При осуществлении мониторинга сетевого трафика подозреваемого сотрудник полиции может действовать в двух основных направлениях.

Первое – перехват и анализ входящего и исходящего трафика непосредственно на узлах и каналах связи провайдера интернет-услуг. Это потребует тесного взаимодействия с оператором связи и наличия у него технической возможности и готовности содействовать правоохранительным органам. Провайдер должен располагать оборудованием для копирования трафика (сплиттеры, коммутаторы с функцией зеркалирования портов) и выделить отдельный SPAN-порт для подключения аппаратуры правоохранительных органов. Сотрудник, в свою очередь, использует специализированные программно-аппаратные комплексы для сбора и анализа сетевых данных (например, системы оперативно-розыскных мероприятий – СОРМ).

Второе направление – перехват и анализ трафика на промежуточных узлах сети, через которые предположительно

проходят данные подозреваемого. Речь идет о компрометации точек доступа Wi-Fi, серверов VPN-провайдеров, узлов сети Tor и других промежуточных звеньев, которые пользователь задействует для анонимизации своего трафика. В этом случае сотрудник полиции должен либо получить содействие владельцев соответствующей сетевой инфраструктуры, либо осуществить её взлом собственными силами. Для этого потребуется применение специальных технических средств и методов, таких как перехват рукопожатий SSL/TLS, подмена DNS-записей, атаки человек посередине (MitM) с использованием поддельных сертификатов и т.п. Независимо от выбранного направления, ключевая задача сотрудника полиции заключается в том, чтобы выявить в массиве перехваченного трафика идентифицирующие данные, однозначно указывающие на личность подозреваемого.

К таким данным, в первую очередь, относятся:

1) *IP-адрес устройства пользователя* (хотя публичный IP обычно является динамическим и выдается провайдером на сеанс связи, сопоставление этой информации с логами провайдера и данными биллинга позволяет установить владельца интернет-подключения);

2) *MAC-адрес сетевого интерфейса* (это уникальный идентификатор, жестко привязанный к конкретному физическому устройству, который может фигурировать в заголовках сетевых пакетов канального уровня);

3) *идентификаторы мобильных устройств: IMEI, IMSI, MSISDN* (их можно извлечь из заголовков пакетов при использовании подозреваемым мобильного интернета);

4) *учётные данные пользователя* (логины, адреса электронной почты, номера телефонов), передаваемые в открытом виде в запросах к веб-сервисам и серверам аутентификации;

5) *уникальные идентификаторы, связанные с браузером и ОС пользователя*: файлы cookie, токены аутентификации, отпечатки TLS, данные WebRTC;

6) *служебная информация приложений и сервисов*: идентификаторы сессий, ключи шифрования, данные геолокации, маршруты передвижения.

Для выделения этих данных из общего потока трафика сотрудник полиции может использовать автоматизированные инструменты анализа протоколов, такие как Wireshark, NetworkMiner, Xplico. Они позволяют быстро обрабатывать большие массивы сетевых пакетов, восстанавливать сессии TCP, расшифровывать защищенный трафик, извлекать файлы и объекты из потоков HTTP/FTP, искать ключевые слова и регулярные выражения. Также полезными могут оказаться самописные скрипты и программы на языках Python, Perl, Shell, позволяющие автоматизировать рутинные операции по разбору и фильтрации сетевых данных.

Помимо автоматизированного анализа, в ряде случаев сотруднику потребуется вручную исследовать перехваченный трафик, чтобы: отследить последовательность действий подозреваемого; восстановить хронологию событий; выявить значимые улики и детали, не поддающиеся формализованному поиску. Для этого можно использовать возможности Wireshark и других сниферов по выделению и декодированию отдельных пакетов и потоков данных, применять экспертные фильтры и функции глубокой инспекции.

При анализе сетевого трафика важно фиксировать не только идентифицирующие данные, но и сопутствующий контекст: временные метки пакетов, IP-адреса и доменные имена удаленных серверов, географическое расположение узлов связи, последовательность и взаимосвязь сетевых взаимодействий. Эта информация поможет восстановить целостную картину действий подозреваемого и впоследствии использовать её в качестве доказательств.

Все выявленные в ходе мониторинга трафика идентифицирующие данные и значимые артефакты должны быть надлежащим образом задокументированы и приобщены к материалам дела. Для этого сотрудник фиксирует ход и результаты мероприятий по перехвату и анализу

сетевых данных; подробно описывает использованные технические средства и методы, временные интервалы наблюдения, объем и характер собранной информации; изготавливает копии перехваченного трафика на электронные носители с соблюдением требований к обращению с вещественными доказательствами. Для защиты подлинности данных рекомендуется использовать хеширование и электронную подпись. Результаты аналитической обработки данных оформляются в виде рапортов, справок, схем, таблиц. В документах необходимо детально описывать выявленные идентификаторы, артефакты и значимые обстоятельства, а также пояснять их смысл и значение для дела [1]. При необходимости назначается компьютерно-техническая экспертиза для подтверждения подлинности и достоверности полученных результатов, а также для решения других специальных вопросов, требующих применения экспертных знаний.

Следует отметить, что теоретическую основу данного рода экспертиз сформировали Е. Р. Россинская и А. И. Усов, определившие такие положения как понятие, предмет, объект и разновидности. Так, Е. Р. Россинская и А. И. Усов определяют компьютерно-техническую экспертизу как «самостоятельный род экспертизы, относящийся к классу инженерно-технических экспертиз, которая, в свою очередь, может быть разделена на такие разновидности, как: программно-компьютерная экспертиза; аппаратно-компьютерная экспертиза; информационно-компьютерная экспертиза; компьютерно-сетевая экспертиза» [4, 5]. В более поздней работе Е. Р. Россинская совместно с Е. И. Галяшиной выделяет наряду с обозначенными разновидностями компьютерно-технических экспертиз судебную телематическую экспертизу, которая предназначена для «установления фактических данных при исследовании электрических сетей с использованием специальных знаний об обстоятельствах расследуемого события» [6].

Кроме того, А. Б. Соколовым и А. Р. Сысенко была предложена не видовая, а родовая классификация экспертиз компьютерной техники и программного обеспечения. Так, авторами предложено отдельно выделять компьютерную и компьютерно-техническую экспертизы [7]. При этом под компьютерной экспертизой авторы понимают исследование компьютерной информации, хранящейся в электронных носителях информации, а под компьютерно-технической экспертизой – исследование аппаратной составляющей устройства с возможностью охвата его программной составляющей. На наш взгляд, в изложенной позиции имеются значительные недостатки, поскольку охват компьютерно-технической экспертизой программных составляющих устройства делает выделение отдельного рода, компьютерной экспертизы, бессмысленным. Полагаем, что подобное деление могло бы быть применимо при условии четкого разделения предложенных родов экспертиз.

Кроме того, на официальном сайте Российского федерального центра судебных экспертиз при Министерстве юстиции Российской Федерации (РФЦСЭ) указана экспертиза, которая называется компьютерно-технической, а также подразделяется на виды, которые схожи с теми, что выделяют Е. Р. Россинская и А. И. Усов. Таким образом, среди видов компьютерно-технической экспертизы РФЦСЭ при Министерстве юстиции Российской Федерации выделяет программно-компьютерную, аппаратно- компьютерную, информационно-компьютерную, компьютерно-сетевую экспертизы [8].

В свою очередь, собранные и задокументированные таким образом результаты мониторинга сетевого трафика являются основой для дальнейшей оперативной разработки фигуранта и могут быть использованы в процессе доказывания по уголовному делу. Однако сотруднику полиции следует учитывать, что сами по себе данные, полученные в результате мониторинга трафика, не всегда позволяют однозначно идентифицировать личность подозреваемого. Во многих случаях они требуют дополнительной проверки и подкрепления другими доказательствами.

Следует принимать во внимание возможное применение подозреваемым

различных средств и методов сокрытия и обфускации сетевой активности. К ним относятся: использование анонимайзеров, прокси-серверов, VPN, сети Tor для маскировки реального IP-адреса и маршрута трафика; шифрование передаваемых данных с помощью протоколов SSL/TLS, PGP, OTR, шифрованных VPN; применение средств стеганографии для скрытой передачи информации внутри легитимного трафика; тщательная фильтрация и нормализация заголовков пакетов для удаления идентифицирующих артефактов; использование эфемерных идентификаторов и одноразовых учетных записей [3]. Для преодоления этих контрмер могут потребоваться более изощренные техники перехвата и анализа трафика.

В целом, следует отметить, что мониторинг сетевого трафика является эффективным, но технически сложным и юридически чувствительным методом деанонимизации. Он требует от сотрудника полиции специальных технических знаний, строгого соблюдения процессуальных норм, тщательного документирования хода и результатов осуществляемых мероприятий. Для успешного применения этого метода сотрудник должен досконально разбираться в принципах функционирования компьютерных сетей, протоколах передачи данных, средствах анонимизации и шифрования трафика; уметь применять специализированные программно-аппаратные средства перехвата и анализа сетевого трафика; четко понимать необходимые правовые основания для осуществления оперативно-розыскной деятельности в киберпространстве и неукоснительно соблюдать предусмотренные законом ограничения и процедуры; обеспечить соответствие проводимых мероприятий по сбору и документированию доказательств требованиям уголовно-процессуального законодательства; уметь эффективно взаимодействовать с интернет-провайдерами, операторами связи, экспертными подразделениями, следственными органами; проявлять изобретательность и настойчивость в преодолении возможного противодействия со стороны подозреваемого, использующего современные средства анонимизации и шифрования.

Заключение. Сотрудники правоохранительных органов, специализирующиеся на раскрытии и расследовании преступлений в сфере информационно-телекоммуникационных технологий, должны регулярно повышать квалификацию в области методов социальной инженерии, следить за развитием ннформационных технологий, обмениваться опытом с коллегами из других подразделений и ведомств. Такая деятельность требует от сотрудника полиции развитых навыков социальной инженерии, знания психологии, технических компетенций в области веб-разработки и информационной безопасности, а также строжайшего соблюдения процессуальных норм и ограничений. Только ответственный и профессиональный подход к проведению мероприятий по деанонимизации позволит эффективно использовать этот инструмент для установления личности киберпреступников с соблюдением всех необходимых правовых и этических норм.

Кроме того, сотрудникам полиции, деятельность которых связана с противодействием IT-преступлениям, необходимо постоянно повышать свою квалификацию в области анонимных сетей и методов их деанонимизации. Это предполагает углубленное изучение архитектуры и протоколов Tor, мониторинг опубликованных уязвимостей и эксплойтов, обмен опытом с профильными экспертами и коллегами из спецслужб, активное участие в исследовательских проектах и конференциях. Регулярное обновление знаний и совершенствование технического арсенала позволит сотрудникам полиции эффективно противостоять преступникам, злоупотребляющим возможностями анонимных сетей, и обеспечить неотвратимость наказания для них.

Таким образом, только комплексный подход, сочетающий в себе высокий уровень технических и юридических знаний, процессуальную безупречность, тактическую гибкость и настойчивость, позволит эффективно использовать этот мощный инструмент для

деанонимизации и изобличения киберпреступников.

Список источников

1. Белицкий В. Ю. Проблема уголовного преследования лица, личность которого не установлена, и вариант ее решения / В. Ю. Белицкий // Юридическая наука и правоохранительная практика. – 2016. – № 2. – С. 110–116.
2. Виноградова О. П. Отдельные аспекты обеспечения информационной безопасности в условиях цифровизации общества // Thesaurus. Зборнік навуковых прац. – Магілёў, 2023. – С. 35–42.
3. Виноградова О. П. Информационная безопасность как элемент механизма государственной политики в сфере противодействия экстремизму: проблемы правового регулирования // Роль информационно-коммуникационных технологий в сфере гуманитарного образования: Сб. матер. Всерос. науч.-практ. конф. Под общ. ред. Н.В. Николаевой. – М., 2023. – С. 73–78.
4. Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза / Е.Р. Россинская, А.И. Усов. – М.: Право и закон, 2001. – 416 с.
5. Усов А. И. Судебно-экспертное исследование компьютерных средств и систем / А. И. Усов. – М.: Право и закон, 2003. – 368 с.
6. Россинская Е. Р., Галяшина Е. И. Настольная книга судьи. Судебная экспертиза. / Е. Р. Россинская, Е. И. Галяшина. – М.: Проспект, 2019. – 464 с.
7. Соколов А. Б., Сысенко А. Р. Назначение и производство компьютерной экспертизы при расследовании преступлений, совершенных с использованием сети «Интернет»: проблемы теории и практики / А. Б. Соколов, А. Р. Сысенко // Криминалистика: вчера, сегодня, завтра. – 2021. – № 1 (17). – С. 118–129.
8. Компьютерно–техническая экспертиза // Sudexpert.ru. URL: http://www.sudexpert.ru/possib/comp.php.

References

1. Belitsky V. Y. The problem of criminal prosecution of a person whose identity has not been established, and its solution / V. Y. Belitsky // Legal science and law enforcement practice. - 2016. – No. 2. – pp. 110-116.
2. Vinogradova O. P. Certain aspects of ensuring information security in the context of the digitalization of society // Thesaurus. Zbornik navukov prats. – Magiley, 2023. – pp. 35-42.
3. Vinogradova O. P. Information security as an element of the mechanism of state policy in the field of countering extremism: problems of legal regulation // The role of information and communication technologies in the field of humanitarian education: Collection of materials. All-Russian Scientific and Practical conference Edited by N. V. Nikolaeva, Moscow, 2023, pp. 73-78.
4. Rossinskaya E. R., Usov A. I. Forensic computer-technical expertise / E.R. Rossinskaya, A. I. Usov, Moscow: Pravo i zakon, 2001, 416 p.
5. Usov A. I. Forensic examination of computer tools and systems / A.I. Usov. – M.: Pravo i zakon, 2003. – 368 p.
6. Rossinskaya E. R., Galyashina E. I. The judge's table book. Forensic examination. / E. R. Rossinskaya, E. I. Galyashina. – M.: Prospekt, 2019. – 464 p.
7. Sokolov A. B., Sysenko A. R. The purpose and production of computer expertise in the investigation of crimes committed using the Internet: problems of theory and practice / A. B. Sokolov, A. R. Sysenko // Criminalistics: yesterday, today, tomorrow. – 2021. – № 1 (17). – Pp. 118-129.
8. Computer–technical expertise // Sudexpert.ru. URL: http://www.sudexpert.ru/possib/comp.php.

Информация об авторе

О. П. Виноградова — доцент кафедры криминалистики Уральского юридического института МВД России, кандидат юридических наук, доцент, полковник полиции.

Information about the author

O. P. Vinogradova — Associate professor at the Department of Criminology at the Ural Law Institute of the Ministry of Internal Affairs of Russia, Candidate of Law, Associate Professor, police Colonel.

УДК 343.1
ББК 67.410.2

Уголовно-процессуальное обеспечение применения информационных технологий в уголовном судопроизводстве

Борис Яковлевич Гаврилов
Академия управления МВД России, Москва, Россия
Email: profgavrilov@yandex.ru

Аннотация. Статья является продолжением развернувшейся в последние годы научной дискуссии о применении информационных технологий, включая искусственный интеллект в уголовном судопроизводстве. При этом в данной публикации рассматривается вопрос о применении данных технологий в уголовном досудебном производстве, где с учетом приведенных автором в публикации статистических данных отмечается высокий уровень нарушений прав и законных интересов граждан и организаций, пострадавших от совершенных в отношении них и их имущества противоправных деяний.
Подчёркивается, что внедрение искусственного интеллекта позволит более оперативно реагировать на заявления и сообщения о преступлениях и принимать по ним законные, обоснованные решения, и тем самым будет способствовать реализации предусмотренного ст. 52 Конституции Российской Федерации права граждан на доступ к правосудию и компенсацию причинённого им ущерба.
Ключевые слова: уголовный процесс, следователь, дознаватель, прокурор, суд (судья), заявление, сообщение о преступлении, отказ в возбуждении уголовного дела, возбуждение уголовного дела, искусственный интеллект, цифровизация, информационные технологии.
Научная специальность: 5.1.4. Уголовно-правовые науки
Для цитирования: Гаврилов Б.Я. Уголовно-процессуальное обеспечение применения информационных технологий в уголовном судопроизводстве // Мир криминалистики. 2025. № 1. С. 48-55

Criminal procedure support for the use of information technologies in criminal proceedings

Boris Y. Gavrilov
Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia
Email: profgavrilov@yandex.ru

Abstract. This article is a continuation of the scientific discussion that has unfolded in recent years on the use of information technologies, including artificial intelligence in criminal proceedings. At the same time, this publication examines the issue of using these technologies in criminal pre-trial proceedings, where, taking into account the statistical data provided in the publication, a high level of violations of the rights and legitimate interests of citizens and organizations that have suffered from illegal acts committed against them and their property is noted. It is emphasized that the introduction of artificial intelligence will allow for a more rapid response to statements and reports of crimes and the adoption of legal and reasoned decisions on them, and thereby will contribute to the implementation of the right of citizens to their access to justice and compensation for damage caused to them, as provided for in Article 52 of the Constitution of the Russian Federation.
Keywords: criminal proceedings, investigator, inquiry officer, prosecutor, court (judge), statement, report of a crime, refusal to initiate a criminal case, initiation of a criminal case, artificial intelligence, digitalization, information technology.
For citation: Gavrilov B.Y. Criminal procedure support for the use of information technologies in criminal proceedings // The world of criminology. 2025;(1):48-55

Сегодня наше общество переживает масштабную модернизацию, связанную с повсеместным использованием современных технологий не только в быту, но и в профессиональной деятельности. Так, Интернет, смартфоны, компьютеры и другие современные технические средства оказали глобальное воздействие на людей и

государство, в связи с чем информация, а если более детально, цифровая информация стала стратегическим и неотъемлемым атрибутом социальной, политической и экономической жизни страны и российского общества.

Активное и повсеместное их внедрение не может обойти стороной как правоохранительную, так и судебную систему, в связи с чем в научном сообществе прослеживается тенденция активного обсуждения перспектив и правовых основ внедрения цифровых технологий в деятельность органов предварительного расследования, дознания, прокуратуры и суда.

Наибольшую популярность среди информационных технологий, несомненно, получил искусственный интеллект, активно интегрировавшийся в повседневную жизнь человека (использование технологии ChatGPT, способной генерировать тексты, изображения по запросам пользователей и т.д.), а также в деятельность судебной системы, прокуратуры и других правоохранительных органов.

Обращаясь к зарубежному опыту применения технологий искусственного интеллекта в деятельности правоохранительных и судебных органов, возможно привести пример Китайской Народной Республики, где искусственный интеллект, являясь одним из ведущих направлений развития уголовного правосудия, нашёл свое применение как часть системы «умных судов», а также как отдельный инструмент, направленный на повышение эффективности следственных действий[1]. Данная система использует большие данные и машинное обучение, помогая судьям быстро находить аналогичные дела прошлых лет, подсказывать возможные статьи закона, генерировать тексты решений и сопутствующих судебных документов[2], что позволяет намного быстрее предоставлять и классифицировать доказательства, а также передавать материалы дела между судами разных инстанций.

Однако необходимо учитывать, что искусственный интеллект не является заменой интеллекта следователя, дознавателя, прокурора или судьи и их практического опыта в области расследования уголовного дела и проведения судебного разбирательства, а лишь служит им помощником и должен использоваться в рамках существующих правовых и этических норм и стандартов деятельности правоохранительных и судебных органов.

На сегодняшний день, ведя речь о возможности использования искусственного интеллекта, автор видит внедрение его элементов, в первую очередь, в стадии возбуждения уголовного дела, которая является наиболее обсуждаемой среди ученых-процессуалистов и части правоприменителей, поскольку её наличие в Уголовно-процессуальном кодексе Российской Федерации (далее - УПК РФ) порождает, во-первых, низкую эффективность уголовного судопроизводства (в суд направляется лишь от 20% до 30% от числа возбужденных уголовных дел) и, во-вторых, нарушение прав при принятии решения об отказе в возбуждении уголовного дела, что, по оценке автора и известных российских учёных-криминалистов В.В. Лунеева, О.Н. Ведерниковой, ежегодно затрагивает не менее 4 млн. пострадавших и ограничивает их доступ к правосудию и компенсацию причинённого им преступлением ущерба, что гарантируется ст. 52 Конституции Российской Федерации[3].

Так, о количестве допущенных нарушений закона в части обеспечения прав потерпевших на доступ к правосудию свидетельствуют приведённые ниже только за последнее десятилетие статистические данные о количестве ежегодно выявляемых органами прокуратуры нарушений учётной-регистрационной дисциплины при разрешении заявлений и сообщений о преступлениях (см. таблицу 1).

[1] Rusman G. et al. Features of the use of digital technologies in the criminal proceedings of the BRICS countries //BRICS Law Journal. 2023. Vol. 10. № 1. P. 51.

[2] В Китае внедрили судебный ИИ. Или нет? // URL: https://habr.com/ru/articles/677920/ (дата обращения: 06.03.2025).

[3] Гаврилов Б.Я. К вопросу о стадии возбуждения уголовного дела: законодателю пора расставить точки // Лоббирование в законодательстве. 2023. Т. 2, № 2. С. 28-34.

Период	Всего выявлено	Из них при приеме и регистрации сообщения о преступлении
2015	4 908 615	3 732 360
2016	5 067 850	3 778 553
2017	5 156 665	3 793 667
2018	5 159 080	3 730 794
2019	5 139 782	3 627 927
2020	5 086 896	3 491 902
2021	5 172 609	3 464 543
2022	4 775 939	3 111 128
2023	5 331 275	3 446 813
2024	5 436 999	3 477 520

Таблица 1. *Сведения о нарушениях закона, выявленных прокурорами на стадии возбуждения уголовного дела*[4]

В этой связи продолжающаяся научная полемика относительно места и роли стадии возбуждения уголовного дела обуславливает вектор научного анализа в части возможности применения искусственного интеллекта на данном этапе досудебного уголовного производства в целях снижения временных и трудовых ресурсов, затрачиваемых в процессе реализации процедур, регламентированных главами XIX и XX УПК РФ.

Например, искусственный интеллект способен минимизировать количество случаев принятия незаконных, необоснованных решений, связанных с отказом в возбуждении уголовного дела[5].

О наличии данной проблемы свидетельствует тот факт, что, несмотря на увеличение количества зарегистрированных заявлений, сообщений о преступлении с 10,7 млн в 2006 г. до 12,1 млн в 2024 г., более чем в два раза (с 3,3 млн до 1,5 млн) сократилось за указанный период количество возбуждённых уголовных дел при одновременном увеличении с 4,5 млн до 6,4 млн процессуальных решений об отказе в возбуждении уголовного дела, из которых ежегодно прокурорами признаются незаконными, необоснованными и отменяются от 20 % до 40 % (см. таблицу 2).

	2006	2022	2023	2024
Всего зарегистрировано сообщений о преступлениях (млн.)	10,7	11,7	11,8	12,1
Возбуждено уголовных дел (млн.)	3,3	1,6	1,6	1,5
В т.ч. удельный вес к числу сообщений о преступлениях	30,8 %	13,6%	13,6%	12,4
Количество (без повторных) «отказных» материалов (млн.)	4,5	6,0	6,2	6,4

Таблица 2. *Статистические данные о количестве возбужденных уголовных дел и «отказных» материалов*

[4] Здесь и далее. Статистические отчеты «Сведения о результатах надзора за исполнением законов на досудебных стадиях уголовного судопроизводства» по форме НСиД за 2015- 2022 гг. [Электронный ресурс] // Генеральная прокуратура Российской Федерации: официальный сайт. URL: http://genproc.gov.ru/stat/data/ (дата обращения: 18.03.2025).

[5] Гаврилов Б.Я. Влияние института возбуждения уголовного дела на состояние борьбы с преступностью // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXIV международной научно-практической конференции. Часть 1. Красноярск, 2021. С. 176.

Как следствие, из года в год фиксируется значительная регистрационно-разрешительная деятельность сотрудников органов внутренних дел Российской Федерации, эффективность которой (в виде установления лиц, совершивших данные противоправные деяния) остаётся достаточно низкой. При этом ежегодно только на подготовку (составление) 6–9 млн процессуальных решений органов предварительного расследования и органов дознания об отказе в возбуждении уголовного дела затрачивается труд порядка 20 тыс. сотрудников полиции и тысяч работников прокуратуры по отмене ежегодно до 2,5 млн (с повторными) «отказных» материалов.

Анализ приведённых в настоящей публикации статистических данных о состоянии преступности показал, что в 2024 г. из 12,1 млн сообщений о преступлениях в качестве таковых зарегистрировано всего 1 911 324 уголовно наказуемых деяния, 91,6 % из которых выявлены органами внутренних дел; в 2023 г. из 11,8 млн таких сообщений зарегистрировано 1 947 256 преступлений, 92,8 % выявлены ОВД; а в 2022 г. из 11,7 млн заявлений, сообщений зарегистрировано в качестве преступлений всего 1 966 795 (93,1 % выявлено ОВД)[6].

Таким образом, положительно повлиять на деятельность при приёме, регистрации и разрешении сообщений о преступлении за счёт её автоматизации способно программное обеспечение, работающее на основе искусственного интеллекта. Данное программное обеспечение может в значительной мере обеспечить оперативность и прозрачность выполняемой сотрудниками органов предварительного следствия и органов дознания служебной деятельности по разрешению заявлений, сообщений о преступлениях, в том числе не допускать принятия следователем, дознавателем, иным (кроме дознавателя) должностным лицом органа дознания решения об отказе в возбуждении уголовного дела по основаниям п. 2 ч. 1 ст. 24 УПК РФ при неустановлении лица, совершившего уголовно наказуемое деяние, о недопустимости чего говорится и в постановлении Конституционного Суда Российской Федерации от 22.09.2022 № 2098-О по делу И. О. Песоцкого[7].

Однако правоприменительная практика не меняется. Так, в 2024 году из числа зарегистрированных 2 039 946 заявлений, сообщений о кражах было возбуждено всего 448 925 уголовных дел, а отказано в возбуждении уголовного дела по 906 891 обращению граждан и организаций в правоохранительные органы о совершенной краже их имущества. Ещё более негативная ситуация складывается по результатам рассмотрения обращений граждан по фактам мошеннических действий. Так, в 2024 году из 2 490 567 заявлений о таких фактах было возбуждено всего 387 011 уголовных дел или 15%, а 1,3 млн потерпевшим было отказано в доступе к правосудию (см. таблицу 3). При этом «судьба» еще каждого третьего обращения о факте противоправного деяния остаётся по итогам отчетного периода неизвестной.

[6] Состояние преступности в Российской Федерации за январь-декабрь 2022-2024 гг. // URL: https://мвд.рф/reports (дата обращения: 06.03.2024).

[7] Определение Конституционного Суда РФ от 22.09.2022 № 2098-О «Об отказе в принятии к рассмотрению жалобы гражданина Песоцкого И.О. на нарушение его конституционных прав ч. 3 и 4 ст. 195, ч. 1 ст. 198, ч. 1 ст. 205 и ч. 1 ст. 206 УПК РФ, п. 13, подпунктом «а» п. 14 и подпунктом «а» п. 15 ст. 3 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации в целях совершенствования прав потерпевших в уголовном судопроизводстве». URL: https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-22092022-n-2098-o/ (дата обращения 20.02.2025).

Вид преступления	Всего поступило сообщений о преступлениях	Возбуждено уголовных дел	Отказано в возбуждении уголовного дела
Умышленное причинение тяжкого вреда здоровью (ст.111 УК РФ)	40 636	10 555	8096
Умышленное причинение средней тяжести вреда здоровью (ст.112 УК РФ)	124 360	12 937	73390
Побои (ст.116 УК РФ)	901 489	2 141	595294
Кража (ст.158 УК РФ)	2 039 946	448 925	906891
Мошенничество (ст.159 УК РФ)	2 490 567	387 011	1 294 987
Незаконные приобретение, хранение, перевозка, изготовление, переработка наркотических средств, психотропных веществ или их аналогов (ст. 228 УК РФ)	146 249	53 350	53222
Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов (ст.228.1 УК РФ)	213 513	122 167	46821

Таблица 3. *Сведения о количестве зарегистрированных сообщений о преступлений об отдельных видах противоправных действий и принятых по ним решений*[8]

Таким образом, учитывая специфику первоначального этапа уголовного судопроизводства, наиболее перспективным, по нашему мнению, видится использование искусственного интеллекта именно при реализации процедуры приема, регистрации и определения направления разрешения сообщений, заявлений о преступлениях.

При этих обстоятельствах автор считает возможным показать продвижение процесса цифровизации данного вида деятельности. Так, на законодательном уровне урегулирован вопрос об электронной форме сообщений, заявлений о преступлениях, подача которых осуществляется через порталы официальных сайтов. Способствовать реализации этой функции призвана Инструкция о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях, утвержденная приказом МВД России от 29 августа 2014 г. № 736[9]. В данном случае в алгоритм программного обеспечения заложен шаблон, который предусматривает указание обязательных реквизитов при подаче заявления и сообщения о преступлении, что позволяет обеспечивать их качество при направлении в органы внутренних дел.

С учетом изложенного предлагается существенно расширить арсенал цифрового формата регистрационно-разрешительной

[8] Сводный отчет по России о рассмотрении сообщений о преступлениях (сформирован с учетом требований приказа Генерального прокурора Российской Федерации от 03.07.2023 № 429). Форма 2-Е.

[9] Инструкция о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях, утв. приказом МВД России от 29 августа 2014 г. № 736. URL: https://www.garant.ru/products/ipo/prime/doc/70691976/ (дата обращения: 07.03.2025).

деятельности сотрудников органов предварительного следствия и органов дознания путем внедрения указанного дополнительного функционала, а именно интеграции в него искусственного интеллекта.

Арсенал функциональных возможностей программного обеспечения с искусственным интеллектом может быть дополнен следующими составляющими:

- автоматическая проверка соответствия внесенных реквизитов по базе данных (например, с помощью портала государственных услуг Российской Федерации), указанных в сообщении и заявлении, с целью выявления аналогичных обращений;
- помимо существующего формата подписания данного заявления (вывод заявления в бумажный формат и непосредственное проставление рукописной подписи) необходимо внедрение электронного способа подписания документа (например, простая электронная подпись, для создания которой требуется лишь указание номера телефона, на который в последующем будет отправлено СМС – сообщение для подтверждения данной операции);
- для реализации правила о предупреждении за заведомо ложный донос по ст. 306 Уголовного кодекса Российской Федерации необходимо ввести для заявителя этап подтверждения об ознакомлении с диспозицией данной статьи УК РФ и её последствиями путем проставления специальной отметки, не проставив которую данное лицо не будет иметь возможности перейти на следующий этап заполнения электронной формы заявления;
- при окончательном заполнении электронной формы заявления о преступлении и отправки через соответствующий портал официальных сайтов следует предусмотреть автоматизированный процесс регистрации, что позволит синтезировать первые два этапа учетно-регистрационной деятельности правоохранительного органа.

К изложенному необходимо дополнить, что данное программное обеспечение возможно использовать непосредственно на компьютере следователя или дознавателя. Безусловно, в силу недостаточности должной технической оснащённости и научно-методологической базы использования данных технологий говорить о полном переходе сотрудников органов внутренних дел на рассмотрение материалов процессуальной проверки в таком формате вряд ли целесообразно. Однако для начала можно было бы опробовать его в так называемом «демо» варианте, например, на преступлениях против собственности (кражи, мошенничества). Так, информация, поступившая непосредственно к следователю, дознавателю или содержащаяся в материалах процессуальной проверки, поступивших от оперуполномоченного полиции по факту тайного хищения чужого имущества, заносится в специальное программное обеспечение, работающее на основе искусственного интеллекта.

Помимо этого, искусственный интеллект способен помочь в изучении больших объемов данных, которые будут иметь значение для расследования преступления[10]. Также он может быть полезен и в проведении допросов, предлагая различные вопросы, подсказки, тактические комбинации или рекомендации для следователя или дознавателя, и в создании структурированных и правильно оформленных процессуальных документов (протоколы, постановления, ходатайства) для следователя или дознавателя. В перспективе искусственный интеллект должен помочь следователям и дознавателям сократить количество нарушений в квалификации

[10] Современные возможности Главного управления криминалистики (Криминалистического центра) в сфере технико-криминалистического обеспечения расследования преступлений // Вестник Главного управления криминалистики. 2022. № 11 (80). С. 7-18.

преступлений, а также снизить уровень нагрузки, дошедшей сегодня (в условиях огромного некомплекта личного состава) до рекордных показателей в ряде регионов России (Дальний Восток, Сибирь и др.).

В связи с этим следует отметить, что благодаря усилиям «Московской академии Следственного комитета Российской Федерации им. А.Я. Сухарева и сотрудников центрального аппарата Следственного комитета России, вошедших в рабочую группу с Техническим комитетом «Искусственный интеллект» (ТК-164) и Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, проводится научно-исследовательская работа по применению технологий искусственного интеллекта для автоматизации отдельных направлений деятельности по расследованию преступлений»[11].

Внедрение в деятельность органов предварительного расследования и органов дознания по проверке сообщений, заявлений о преступлениях программного обеспечения, работающего на основе искусственного интеллекта, видится достаточно перспективным, однако на данный момент нуждается в дальнейшем изучении и правовом регулировании. Это необходимо для просчёта всевозможных рисков, которые могут негативно отразиться на ходе уголовного судопроизводства. Также данная новация способна реформировать досудебную стадию уголовного процесса, а именно - реорганизовать или же вовсе ликвидировать стадию возбуждения уголовного дела, о чём автор исследования, наряду с другими представителями научного сообщества, говорит более 30 лет[12].

В заключение автор отмечает, что за последний год дискуссия о внедрении технологий искусственного интеллекта в деятельность участников уголовного процесса достигла весьма значительных масштабов. Однако этому препятствует разноречивая политика как учёных, так и правоприменителей. Одни представители научного сообщества придерживаются консервативных взглядов и считают, что никакого искусственного интеллекта не существует и изменений не требуется. Другая же часть учёных и критиков считает необходимым активное развитие данной тематики, дополнение действующего законодательства для регулирования этой новеллы и её поэтапное внедрение в деятельность следователей, дознавателей, прокуроров, судей и в целом правоохранительных органов (например, для прогнозирования и противодействия преступности, расследования преступлений, рассмотрения и разрешения уголовных дел).

Список источников

1. Rusman G. et al. Features of the Application of Digital Technology in Criminal Proceedings of the BRICS Countries //BRICS Law Journal. 2023. Т. 10. №. 1. P. 35-38.

2. Гаврилов Б.Я. К вопросу о стадии возбуждения уголовного дела: законодателю пора расставить точки // Лоббирование в законодательстве. 2023. Т. 2, № 2. С. 28-34.

3. Гаврилов Б.Я. Влияние института возбуждения уголовного дела на состояние борьбы с преступностью // Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXIV международной научно-практической конференции. Часть 1. Красноярск, 2021. С. 175-177.

[11] Бессонов А.А. К вопросу о цифровизации уголовного судопроизводства в Российской Федерации // Уголовный процесс и криминалистика: правовые основы, теория, практика, дидактика (к 75-летию со дня рождения профессора Б. Я. Гаврилова): сборник научных статей по материалам международной научно-практической конференции, Академия управления МВД России, 03 ноября 2023 года. Москва: Академия управления МВД России, 2023. С. 31; Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: монография. Москва: Проспект, 2024. 816 с.

[11] Современные возможности Главного управления криминалистики (Криминалистического центра) в сфере технико-криминалистического обеспечения расследования преступлений // Вестник Главного управления криминалистики. 2022. № 11 (80). С. 7-18.

4. Современные возможности Главного управления криминалистики (Криминалистического центра) в сфере технико-криминалистического обеспечения расследования преступлений // Вестник Главного управления криминалистики. 2022. № 11 (80). С. 7-18.

5. Бессонов А.А. К вопросу о цифровизации уголовного судопроизводства в Российской Федерации // Уголовный процесс и криминалистика: правовые основы, теория, практика, дидактика (к 75-летию со дня рождения профессора Б. Я. Гаврилова): сборник научных статей по материалам международной научно-практической конференции, Академия управления МВД России, 03 ноября 2023 года. Москва: Академия управления МВД России, 2023. С. 26-32.

6. Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: монография. М.: Проспект, 2024. - 816 с.

References

1. Rusman G. et al. Features of the use of digital technologies in the criminal proceedings of the BRICS countries //BRICS Law Journal. 2023. Vol. 10. № 1. З. 35-38.

2. Gavrilov B.Ya. On the issue of the stage of initiation of a criminal case: it's time for the legislator to put the dots // Lobbying in legislation. 2023. Vol. 2, № 2. P. 28-34.

3. Gavrilov B.Ya. The influence of the institution of criminal proceedings on the state of combating crime // Actual problems of combating crime: issues of theory and practice: proceedings of the XXIV scientific and practical international conference. Part 1. Krasnoyarsk, 2021. P. 175-177.

4. Modern capabilities of the Main Directorate of Criminalistics (Criminalistic Center) in the field of technical and criminalistic support of crime investigation // Bulletin of the Main Directorate of Criminalistics. 2022. № 11 (80). P. 7-18.

5. Bessonov A.A. On the issue of digitalization of criminal proceedings in the Russian Federation // Criminal procedure and criminalistics: legal foundations, theory, practice, didactics (on the 75th anniversary of the birth of Professor B.Ya. Gavrilov): collection of scientific articles based on the materials of the international scientific and practical conference, Academy of Management of the Ministry of Internal Affairs of Russia, November 03, 2023. Russian Russian Ministry of Internal Affairs Academy of Management, 2023. P. 26-32.

6. Bessonov A.A. Artificial intelligence and mathematical statistics in the criminalistic study of crimes: monograph. Moscow: Prospekt, 2024. - 816 p.

Информация об авторе

Б.Я. Гаврилов — профессор кафедры управления органами расследования преступлений Академии управления МВД России, доктор юридических наук, профессор.

Information about the author

B.Y. Gavrilov — is a professor at the Department of Management of Crime Investigation Bodies of the Academy of Management of the Ministry of Internal Affairs of Russia, Doctor of Law, Professor.

УДК 343.9
ББК 67.515

Хищение персональных данных: уголовно-правовой анализ и меры противодействия

Эльмира Равилевна Гафурова
Ижевский государственный технический университет им. М.Т. Калашникова, Ижевск, Россия
Email: ely_1979@mail.ru

Аннотация. В работе анализируются уголовно-правовые аспекты хищения персональных данных, выявляются проблемы законодательства и правоприменения, и выносятся предложения меры по совершенствованию противодействия данной форме киберпреступности.
Ключевые слова: хищение, персональные данные, утечка, киберпреступность, цифровизация, распространение информации.
Научная специальность: 5.1.4. Уголовно-правовые науки
Для цитирования: Гафурова Э.Р. Хищение персональных данных: уголовно-правовой анализ и меры противодействия // Мир криминалистики. 2025. № 1. С.56-60

Theft of personal data: criminal law analysis and counteraction measures

Elmira R. Gafurova
Izhevsk State Technical University named after M.T. Kalashnikov, Izhevsk, Russia
Email: ely_1979@mail.ru

Abstract. The paper analyzes the criminal and legal aspects of personal data theft, identifies problems of legislation and law enforcement, and makes proposals for measures to improve counteraction to this form of cybercrime.
Keywords: theft, personal data, leakage, cybercrime, digitalization, dissemination of information.
For citation: Gafurova E.R. Theft of personal data: criminal law analysis and counteraction measures // The world of criminology. 2025;(1):56-60

Введение. В эпоху цифровизации и глобального распространения информационных технологий персональные данные стали одним из наиболее ценных ресурсов. Однако вместе с этим возросла и угроза их незаконного присвоения. Хищение персональных данных как вид киберпреступности представляет собой серьезный вызов для современного общества и требует комплексного уголовно-правового анализа. В связи с чем необходимо понимание сущности данного феномена, выявление проблем правового регулирования и разработка эффективных мер противодействия.

Согласно ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ *«персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»* [8].

Хищение персональных данных представляет собой преступное деяние, связанное с «присвоением личности» другого лица с целью получения кредита, кредитных карт в банках или магазинах, кражи денег с существующих счетов этого лица, подачи заявок на кредиты на имя этого лица, аренды автомобилей, подачи заявок на банкротство или даже получение работы [2].

Персональные данные в современных условиях стали определенным «товаром», так как множество баз данных не способны оказать должное сопротивление злоумышленникам, а данные пользователей активно продаются на черном рынке.

Актуальность данной проблемы достаточно высока. Например, в 2024 году Роскомнадзор зафиксировал 135 случаев утечек баз данных, содержащих свыше 710 миллионов записей о россиянах [4]. А в мире в 2024 году, согласно показателям сервиса разведки уязвимостей и утечек данных DLBI, зафиксировано 382 утечки, что значительно меньше, чем 445 утечек в 2023 году. Но объем утёкших данных в прошлом году значительно вырос: в руки хакеров попало 438 млн телефонных номеров и 227 млн email-адресов, что на 70% больше, чем в 2023 году. Так, 36 % от мировых данных приходится на граждан российского государства. Все эти данные становятся объектом внимания злоумышленников, которые преследуют свои корыстные цели [7].

Основная часть. В соответствии со ст. 158 Уголовного кодекса Российской Федерации (далее – УК РФ) под хищением понимается совершение с корыстной целью противоправного безвозмездного изъятия и (или) обращения чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества [10].

На наш взгляд, хищение персональных данных не ограничивается стандартными видами преступлений против собственности, а может осуществляться в различных формах, включая:

1) *несанкционированный доступ к информационным системам*, то есть взлом баз данных, серверов, облачных хранилищ, содержащих персональные данные;

2) *мошенничество*, то есть обманное получение персональных данных путем имитации легитимных запросов от организаций или доверенных лиц;

3) *инсайдерские преступления.* В данном случае таковыми является хищение данных сотрудниками организаций, имеющими доступ к персональным данным в силу служебного положения;

4) *использование вредоносного программного обеспечения*, а именно распространение вирусов, троянов и других вредоносных программ для сбора и передачи персональных данных;

5) *кражи носителей информации* – хищение устройств, содержащих персональные данные (ноутбуков, USB-накопителей и т.п.).

Уголовная ответственность именно за хищение персональных данных в Российской Федерации прямо не предусмотрена отдельной статьей УК РФ. Однако в зависимости от конкретных обстоятельств совершенного деяния хищение персональных данных может квалифицироваться по ряду статей УК РФ, в частности: ст. 137, 159, 163, 183, 272, 272.1, 273 УК РФ и другим [6].

Обращая внимание на уголовно-правовую характеристику указанных преступлений, отметим, что персональные данные могут быть объектом преступлений. Например, по статье 272 УК РФ объектом уголовно-правовой охраны становятся персональные данные в случае их обработки в автоматизированных вычислительных системах в виде электронной информации. Непосредственным объектом в этом случае являются отношения по поводу обеспечения целостности и сохранности компьютерной информации, а также безопасности функционирования электронных информационных систем. Кроме того, персональные данные как объект преступления указаны в статье 137 УК РФ, которая предусматривает ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия. Помимо этого, статья 272.1 УК РФ предусматривает ответственность за незаконные использование, передачу, сбор и хранение компьютерной информации, содержащей персональные данные. Ст. 272.1 УК РФ была введена в действие в ноябре 2024 года в связи с ростом утечек персональных данных, а ранее незаконные действия с персональными данными квалифицировались по общим статьям [9].

Объективная сторона преступления, связанного с хищением персональных данных по УК РФ, включает в себя активные действия по присвоению и использованию персональных данных другого лица или других лиц.

Субъектом преступления хищения персональных данных может быть физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста. Также имеет место специальный субъект преступления – сотрудник организации, нарушивший правила эксплуатации средств хранения, обработки или передачи персональных данных либо информационно-телекоммуникационных сетей и оконечного оборудования, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование персональных данных.

Субъективная сторона преступлений, связанных с хищением персональных данных, как правило, характеризуется умышленной формой вины в виде прямого или косвенного умысла [6].

В большинстве случаев квалификация хищения персональных данных представляет собой значительную сложность, обусловленную:

1) отсутствием прямого состава преступления в уголовном законодательстве. Необходимость квалификации деяния по косвенным статьям УК РФ может затруднять правоприменение и не всегда адекватно отражает общественную опасность деяния;

2) размытостью понятия «существенный вред». К примеру, ст. 272 и ст. 137 УК РФ требуют установления «существенного вреда», оценка которого носит субъективный характер и вызывает сложности при доказывании;

3) трудностями при доказывании корыстной цели или иной личной заинтересованности. Для квалификации ряда преступлений (например, мошенничества, вымогательства) необходимо доказать наличие корыстной цели или иной личной заинтересованности у преступника, что не всегда представляется возможным;

4) трансграничным характером киберпреступлений. Преступники могут находиться в другой юрисдикции, что затрудняет их привлечение к ответственности.

В целом эти и другие нюансы влияют на квалификацию содеянного и повышения уровня латентности преступлений, связанных с хищением персональных данных.

Рассмотрим несколько примеров материалов о хищении персональных данных.

В начале 2024 года в Хабаровском крае задержали сотрудника отдела полиции, который продал личные данные находящегося под охраной государства свидетеля. Старший оперуполномоченный по особо важным делам регионального управления МВД России занимался защитой свидетелей и имел доступ к материалам уголовных дел. За 800 тысяч рублей он передал неустановленному лицу видео отработки рабочих версий по преступлению и протокол допроса потерпевшего, которые хранились под грифом «совершенно секретно». Силовика оперативно задержали по подозрению в совершении преступлений, предусмотренных ст. ст. 159, 286 УК РФ [1].

Районным судом <данные изъяты> было рассмотрено дело в отношении бывшего сотрудника банка, который, используя свои служебные полномочия, скопировал базу данных клиентов, содержащую персональные данные и банковскую тайну. Суд признал его виновным по ч. 2 ст. 272 УК РФ. В мотивировочной части решения суд подчеркнул общественную опасность деяния, связанную с нарушением прав большого количества граждан на неприкосновенность частной жизни и конфиденциальность банковской информации [5].

Городским судом <данные изъяты> было рассмотрено дело в отношении группы лиц, организовавших фишинговую атаку на пользователей интернет-банкинга. Преступники рассылали электронные письма, имитирующие официальные сообщения банка, с целью получения логинов и паролей от личных кабинетов. Полученные данные использовались для хищения денежных средств со счетов потерпевших. Суд квалифицировал действия обвиняемых по ч. 3 ст. 159 УК РФ [5].

Анализ судебной практики позволяет утверждать, что отсутствие отдельной нормы в уголовном законодательстве, регламентирующей ответственность за

хищение персональных данных, и последствий в результате такого хищения, а также отсутствие разъяснений судов вызывают на практике затруднения у правоприменителей при квалификации таких деяний.

По нашему мнению, необходимо разработать отдельную норму, связанную с хищением и дальнейшим оборотом персональных данных, либо усовершенствовать ст. 272.1 УК РФ, дополнив её, например, признаками мошеннических действий, вымогательства или публичного распространения персональных данных. Кроме того, следует определить меры противодействия хищению персональных данных.

Заключение. Противодействие хищению персональных данных должно быть направлено на:

1) *усиление кибербезопасности*. Внедрение и совершенствование технических и организационных мер защиты персональных данных, включая: шифрование данных, многофакторная аутентификация, регулярное обновление программного обеспечения;

2) *оценку эффективности применяемых мер* защиты и выявление уязвимостей;

3) *повышение правовой грамотности граждан.* Информирование граждан о рисках хищения персональных данных и методах защиты от киберпреступлений, включая: осторожность при предоставлении персональных данных в интернете, использование надежных паролей и их регулярная смена, установка и обновление антивирусного программного обеспечения, критическое отношение к электронным письмам и ссылкам, полученным из ненадежных источников [3].;

4) *усиление международного сотрудничества.* Развитие международного сотрудничества правоохранительных органов для эффективной борьбы с трансграничной киберпреступностью;

5) *совершенствование методов расследования киберпреступлений*. Развитие специальных подразделений в правоохранительных органах, специализирующихся на расследовании киберпреступлений, оснащение их современными техническими средствами и подготовка квалифицированных кадров.

Хищение персональных данных представляет собой серьезную угрозу для современного общества, требующую комплексных мер противодействия. Эффективная борьба с хищением персональных данных требует усилий как со стороны государства, так и со стороны граждан, направленных на повышение кибербезопасности, правовой грамотности и развитие международного сотрудничества. Введение отдельной статьи в УК РФ, предусматривающей ответственность за хищение персональных данных, могло бы стать важным шагом на пути к более эффективной защите прав граждан и организаций в цифровой среде.

Список источников

1. В российском регионе задержали сотрудника полиции за продажу данных о свидетеле. ООО «Лента.Ру». URL: https://lenta.ru/news/2024/02/02/v-rossiyskom-regione-zaderzhali-sotrudnika-politsii-za-prodazhu-dannyh-o-svidetele/ (дата обращения: 24.01.2025).

2. Кузьмин Ю.А. Кража персональных данных (криминологический аспект) // Oeconomia et Jus. 2020. №3. С. 48-57.

3. Могунова М.М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) // Вестник СГЮА. 2020. № 4 (135). С. 135-141.

4. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: https://rkn.gov.ru/ (дата обращения: 23.01.2025).

5. Судебные и нормативные акты РФ. URL: https://sudact.ru/ (дата обращения: 24.01.2025).

6. Тонян А.В. Преступления, совершаемые в отношении персональных данных: современные способы совершения и вопросы квалификации // Молодой ученый. 2022. № 4 (399). С. 251-253.

7. Утечки данных в России за 2024 год: итоги // SecureNews. URL:

https://securenews.ru/utechki-dannyh-v-rossii-za-2024-god-itogi/ (дата обращения: 23.01.2025).

8. О персональных данных: федеральный закон от 27.07.2006 № 152-ФЗ // Российская газета. URL: https://rg.ru/documents/2006/07/29/personaljnye-dannye-dok.html

9. О внесении изменений в Уголовный кодекс Российской Федерации: федеральный закон от 30.11.2024 № 421-ФЗ // Российская газета. URL: https://rg.ru/documents/2024/12/06/personalnye-dannye-dok.html

10. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

References

1. A police officer was detained in the Russian region for selling information about a witness. LLC "Lenta. <url>". URL: https://lenta.ru/news/2024/02/02/v-rossiyskom-regione-zaderzhali-sotrudnika-politsii-za-prodazhu-dannyh-o-svidetele / (accessed: 24.01.2025).

2. Kuzmin Yu.A. Theft of personal data (criminological aspect) // Oeconomia et Jus. 2020. No. 3. pp. 48-57.

3. Mogunova M.M. Technology of implementation and legal regulation of illegal possession of personal banking data (phishing) // Bulletin of the SSYAA. 2020. No. 4 (135). pp. 135-141.

4. The official website of the Federal Service for Supervision of Communications, Information Technology and Mass Communications. URL: https://rkn.gov.ru / (accessed: 01/23/2025).

5. Judicial and regulatory acts of the Russian Federation. URL: https://sudact.ru / (accessed: 01/24/2025).

6. Tonyan A.V. Crimes committed in relation to personal data: modern methods of commission and qualification issues // Young Scientist. 2022. No. 4 (399). pp. 251-253.

7. SecureNews. URL: https://securenews.ru/utechki-dannyh-v-rossii-za-2024-god-itogi / (accessed: 01/23/2025).

Информация об авторе

Э.Р. Гафурова — доцент кафедры «Юриспруденция» в Ижевском государственном техническом университете им. М.Т. Калашникова, кандидат юридических наук.

Information about the author

E. R. Gafurova — Associate Professor of the Department of Jurisprudence at Izhevsk State Technical University named after M.T. Kalashnikov, Candidate of Law.

УДК 343
ББК 67.408

О Международном союзе криминалистов 1889-1914 годов

Андрей Львович Иванов
Московская академия Следственного комитета Российской Федерации имени А.Я. Сухарева, Москва, Россия
Email: ivanoval2010@rambler.ru

Павел Тимурович Савин
Московская академия Следственного комитета Российской Федерации имени А.Я. Сухарева, Москва, Россия
Email: paulst50@gmail.com

Аннотация. В статье рассматриваются вопросы деятельности первого Международного союза криминалистов, как организации сторонников социологической школы уголовного права, поставившей своей задачей реформирование уголовного законодательства и уголовного судопроизводства в европейских странах в соответствие с основными идеями данной научной школы. Авторы статьи детально рассматривают вопросы организации деятельности данной организации, анализируют научную проблематику, которая являлась предметом обсуждения и научной дискуссии. Особое внимание в статье уделено русской секции Международного союза криминалистов, как первому всероссийскому профессиональному объединению ведущих специалистов в сфере уголовно-правовой мысли. Авторы приходят к закономерному и обоснованному выводу о том, что первый Международный союз криминалистов представлял собой не только научный форум по обмену научными идеями, но и своеобразную школу молодых ученых. В связи с этим подтверждается важность создания нового Международного союза криминалистов и в особенности его Молодежной секции.
Ключевые слова: Международный союз криминалистов; уголовно-правовые науки; социологическая школа уголовного права.
Научная специальность: 5.1.4. Уголовно-правовые науки
Для цитирования: Иванов А. Л., Савин П. Т. О Международном союзе криминалистов 1889-1914 годов // Мир криминалистики. 2025. № 1. С. 61-68

About the International Union of Criminologists 1889-1914

Andrey L. Ivanov
Sukharev Moscow Academy of the Investigative Committee of the Russian Federation, Moscow, Russia
Email: ivanoval2010@rambler.ru

Pavel T. Savin
Sukharev Moscow Academy of the Investigative Committee of the Russian Federation, Moscow, Russia
Email: paulst50@gmail.com

Abstract. The article discusses the activities of the first International Union of Criminologists, as an organization of supporters of the sociological school of criminal law, which has set itself the task of reforming criminal legislation and criminal proceedings in European countries in accordance with the basic ideas of this scientific school. The authors of the article examine in detail the issues of organizing the activities of this organization, analyze the scientific issues that were the subject of discussion and scientific discussion. Particular attention in the article is paid to the Russian section of the International Union of Criminologists, as the first all-Russian professional association of leading experts in the field of criminal legal thought. The authors come to a logical and reasonable conclusion that the first International Union of Criminologists was not only a scientific forum for the exchange of scientific ideas, but also a kind of school for young scientists. In this regard, the importance of creating a new International Union of Criminologists and especially its Youth Section is confirmed.
Key words: International Union of Criminologists; criminal law sciences; sociological school of criminal law.
For citation: Ivanov A. L, Savin P. T. About the International Union of Criminologists 1889-1914 // The world of criminology. 2025;(1): 61-68

21 апреля 2023 года в Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева состоялась международная научно-практическая конференция «Криминалистика в международном измерении». В ходе конференции в торжественной обстановке было принято решение о создании Международного союза криминалистов как основы расширения международного сотрудничества в сфере криминалистической теории и практики. Были сформулированы и основные задачи новой организации, в том числе задачи, связанной с привлечением молодых ученых и созданием возможностей для повышения их научного статуса с целью усиления их дальнейшего вклада в развитие криминалистики и иных наук уголовно-правового цикла [1]. Именно в рамках решения данной задачи 27 сентября 2024 года в Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева состоялся I Съезд Молодежной секции Международного союза криминалистов. Две секции научного форума из четырех были посвящены вопросам уголовного права: новеллам уголовного закона в свете проблем квалификации, расследования и профилактики; синергии уголовно-правовых наук в целях совершенствования практики борьбы с преступностью. Представляет особый интерес именно тот факт, что съезд Молодежной секции был первым, в то время как история Международного союза криминалистов начинается ещё в девятнадцатом столетии.

Определенный научный интерес представляет собой ознакомление с деятельностью самого первого Международного союза криминалистов. Данная организация, к сожалению, практически не упоминается в учебниках по уголовному праву, несмотря на свое истинное значение, что представляется определенного рода упущением. Необходимо по меньшей мере выяснить ряд ключевых вопросов: кто являлся учредителями первого союза; какие цели перед ним стояли; какова была роль российских ученых в его работе; по какой причине, отпраздновав 25-летний юбилей, он неожиданно прекратил свою работу.

Международный союз криминалистов был создан в 1889 г. такими известными учеными, как немецкий профессор Ф. Лист, бельгийский профессор А. Принс, голландский профессор Г. А. Ван-Гаммель. Состоялось всего двенадцать съездов, первый из которых был проведен в 1889 году в Брюсселе, а последний в 1913 в Копенгагене. В Российской Империи девятый съезд 1902 года принимал столичный Санкт-Петербург [2]. Фактически Международный союз криминалистов представлял собой не что иное, как официальный орган социологической школы уголовного права. При этом все три профессора-учредителя придерживались различных точек зрения о причинах преступности. Г. А. Ван-Гаммель, как и сторонники антропологической школы уголовного права, придерживался мнения о возможности существования неисправимых преступниках и значении детерминизма, был сторонником неопределенных приговоров. А Принс, напротив, выступал против неопределенных приговоров и придерживался мнения об относительной свободе воли. Ф. Лист занимал по отношению к своим коллегам определенную центристскую позицию. Основной задачей созданной организации, именно как органа социологической школы уголовного права, было совершенствование уголовного законодательства для борьбы с преступностью посредством последовательного реформирования уголовного права и уголовного судопроизводства. При определении причин преступности представители социологической школы придавали определяющее значение социологическим факторам [3].

В течении более чем двадцати лет Международный союз криминалистов оказывал активное воздействие на реформирование систем уголовного права, существовавших на тот момент в странах Европы. Обмен идеями осуществлялся не только посредством периодических научных съездов на международном уровне, но и посредством публикации обзоров работы различных национальных групп организации, их доведения до иностранных коллег. На 1911 год в Международном союзе криминалистов

было следующее представительство по странам: 20 членов от Бельгии, 62 от Дании, 340 от Германии, 45 от Франции и Финляндии, 7 от Греции, 3 от Италии, 34 от Хорватии, 2 от Люксембурга, 32 от Нидерландов, 17 от Норвегии, 90 от Австрии, 2 от Румынии, 291 от России, 9 от Швеции, 41 от Швейцарии, 3 от Сербии, 96 от Испании и Венгрии. Документы организационных собраний прекрасно сохранились и представляют собой определенную научную ценность. Известны четыре вопроса, предложенные для обсуждения на первой секции самого первого Съезда Международного союза криминалистов, состоявшегося в Брюсселе в 1889 году: о допустимости условного приговора (условного осуждения); о возможности применения иных уголовно-правовых методов вместо вынесения нежелательных приговоров о лишении свободы на незначительный срок; об основных недостатках современного законодательства, регламентирующего вопросы исправления рецидивистов; о воздействии на несовершеннолетних правонарушителей, включая вопросы установления возраста, до достижения которого невозможно уголовное преследование, и продления срока пребывания в исправительной школе [4].

Создание Международного союза криминалистов оказало существенное значение для развития российской уголовно-правовой мысли, так как оно послужило основой для научного объединения представителей российских уголовно-правовых наук, первые попытки которого начались несколько ранее.

В 1875 году состоялся Первый Съезд русских юристов. Съезд разделился на отделения: уголовного права и тюремного дела; гражданского и торгового права; судоустройства и уголовного судопроизводства; гражданского судопроизводства и нотариальной части. По отделению уголовного права и тюремного дела слушали выступления: заслуженного профессора В. Н. Лешкова с докладом на тему предупреждения и пресечения преступлений, как учении и учреждении, принадлежащем исключительно к области уголовного права; ординарного профессора С. М. Будзинского с докладом на тему аналогии преступности, нарушающей пределы между судебной и законодательной властью, не существующей по уложению о наказаниях; доцента (на тот момент) И. Я. Фойницкого с докладом на тему необходимости реформы постановлений русского уголовного законодательства по вопросу о лишении права; ординарного профессора Н. С. Таганцева с докладом на тему изменения системы ответственности для малолетних преступников; магистра Н. А. Неклюдова с докладом на тему расширения понятий семейных похищений; заслуженного ординарного профессора В. Н. Лешкова с докладом на тему тюремного дела, как составной части общественного, а не уголовного права; экстраординарного профессора В. В. Микляшевского с докладом на тему необходимости создания раздельных исправительных колоний и приютов для малолетних, приговоренных к наказанию, и для малолетних, освобожденных от наказания по причине совершения ими преступления «без разумения»; присяжного поверенного А. В. Лохвицкого с докладом на тему расширения права суда на понижение наказания в случае объявления подсудимого присяжными заседателями заслуживающим снисхождения [5].

В дальнейшем юридические общества Москвы, Санкт-Петербурга, Казани, Ярославля, Курска и иных городов предпринимали попытки консолидации и взаимодействия. Со временем отдельные ученые стали предпринимать и попытки международного научного участия. Первоначально представителем российских юридических обществ на международных пенитенциарных конгрессах являлось уголовное отделение Санкт-Петербургского юридического общества. В дальнейшем его преемником на международном уровне в 1897 году стала русская группа международного Союза криминалистов, созданная по инициативе профессора И. Я. Фойницкого. Деятельность данной группы была посвящена исключительно вопросам уголовного права и совершенствования уголовного законодательства. Например, российских ученых

интересовали вопросы основных начал юридической ответственности в иностранном праве и пригодности для внедрения в России института условного осуждения [6]. Соответственно, до создания Международного союза криминалистов у представителей российской уголовно-правовой науки не было единой организационной структуры, которая представляла бы все российские юридические общества на международном уровне, что вновь подчеркивает значение указанной организации.

Русская группа Международного союза криминалистов принимала участие не только в ежегодных съездах Союза, но и в различных научных мероприятиях внутри страны. Так, например, известный психиатр А. И. Сикорский, отец не менее известного авиаконструктора И. И. Сикорского, выступал на Съезде русской группы, состоявшемся в Киеве 4 января 1905 года, по вопросу оценки чувств, которые испытывают очевидцы приведения в исполнение смертной казни [7]. Представляется, что для примера можно взглянуть и на программу съезда русской группы Международного союза криминалистов в Санкт-Петербурге в 1902 году. Примечателен он тем, что председательствовал на нем Н. С. Таганцев, а среди 29 новых членов, за принятие которых собравшиеся единогласно проголосовали, указан сенатор А.Ф. Кони. Между тем, на повестке дня стояли, в том числе, и такие вопросы как: проект закона об отсрочке наказания; программа вопросов по содержанию института условного осуждения; об условном досрочном освобождении из заключения; к вопросу о преступнике по случайному поводу или соблазну; о правовой защите детей и др. [8].

В то время как учение основателя социологической школы уголовного права в России И. Я. Фойницкого демонстрировало самостоятельность российской уголовно-правовой мысли, в оценках иностранных коллег русская криминалистическая группа характеризовалась как прогрессивная и по этой причине занимала левое крыло в Международном союзе криминалистов. К её представителям можно, в частности, отнести А. А. Жижиленко, П. И. Люблинского, А. А. Пионтковского, М. Н. Гернета, А. Н. Трайнина, М. М. Исаева. Известно, что русская криминалистическая группа крайне критично относилась к теории «опасного состояния личности преступника» и предложению введения в российское уголовное законодательство соответствующего понятия. По мнению представителей российской уголовно-правовой мысли того времени, кара со стороны государства должна исходить из оценки вины, и, соответственно, меры социальной защиты от социально опасных личностей могут быть введены в законодательство исключительно при условии закрепления в нём широких прав личности. М. Н. Гернет указывал на то, что в создании теории опасного состояния личности имеет место влияние представителей антропологической школы, которых было немало в отдельных иностранных группах Международного криминалистического союза [9]. На основании ряда изученных работ можно сказать, что М. Н. Гернет по данному вопросу полагал следующее: во-первых, прирожденных преступников либо «преступников вследствие безумия» не так уж и много; однако несмотря на то, что они наименее многочисленны, они наиболее опасны [10]. Во-вторых, он же писал о том, что была бы крайне опасной ситуация, если бы в уголовных кодексах, рассматривая вопрос об угрозе жизни человека, преступников разделяли бы на опасных для общества и неопасных, определяя применяемые к виновному лицу меры исключительно на основании данной классификации [11].

Создателем теории «опасного состояния личности» выступал представитель антропологической школы уголовного права Р. Гарофало, который под данным состоянием понимал перманентную и имманентную склонность человека к совершению преступлений. Примечательно, что по итогам Брюссельского съезда Международного союза криминалистов 1910 года была принята резолюция, подчеркивавшая необходимость мер социальной защиты в уголовном праве. Речь шла о том, что часть преступников является изначально

дефективными либо из-за биологических факторов, либо из-за недостатков социального воспитания, что подразумевает собой то, что к данным лицам применять наказание, основанное на чувствах страха и расчета, крайне неэффективно [12].

Представляет определенного рода интерес и тот факт, что определенные идеи, с которыми не соглашался ряд представителей русской группы, но которые активно продвигались на Международного криминалистического союза, стали востребованы при создании нового советского уголовного законодательства, необходимость в котором возникла ввиду отмены уголовного законодательства Российской Империи после Октябрьской революции. Так, в ст. 5 УК РСФСР уже встречались слова о том, что настоящий Уголовный кодекс имеет своей задачей защиту государства от «общественно опасных элементов» и осуществляет эту задачу посредством применения к нарушителям не только наказания, но и «других мер социальной защиты» [13].

Относительно 11 съезда Международного союза криминалистов в Брюсселе в 1910 году, про который сказано выше, у П. И. Люблинского остались крайне неприятные воспоминания, связанные с его слабой организацией. К 1910 году съезды всего общества стали проходить реже, в то время как съезды национальных групп в их странах, наоборот, стали более частыми; так в Австрии и Германии они проходили несколько раз в год. Ввиду того, что у бельгийских судей за неделю до проведения мероприятия начался период отпусков, все местные юристы разъехались, и принимающая страна смогла обеспечить участие только трех бельгийцев во главе с Адольфом Принсом. Второй причиной, обусловившей низкую явку участников съезда, явилась Всемирная выставка 1910 года, проходившая в Брюсселе в те же дни, которая существенно отвлекала всеобщее внимание. За три месяца бельгийские власти решили провести сразу порядка 69 международных конгрессов. Параллельно проходили международные конгрессы железнодорожников, врачей, портных и других профессий. По данной причине съезд Международного союза криминалистов не пользовался особым вниманием у местного населения. Из 175 участвовавших человек представителей России было всего 12, в том числе несколько профессоров. При этом, кроме предусмотренных программой конгресса докладчиков, слово было предоставлено лишь 7-8 людям, и при таких условиях, которые явно не располагали к прениям. По мнению П. И. Люблинского, вопрос «об опасном состоянии преступника» привел с самого начала к взаимному непониманию, так как не разрешал споры, а скорее усложнял их [14].

Если обратить внимание на приведенные выше данные Г. А. Ван-Гаммеля, то получается, что на 1911 год в различных национальных группах Международного союза криминалистов было 1094 члена. В процентном соотношении двумя самыми крупными группами были Германия и Россия, соответственно 31 % и 26 % от всех членов. Вместе две страны составляли 57 %. При этом к 1912 году ситуация существенно изменилась. Как замечал П. И. Люблинский, в союзе состояло уже 1243 члена, из которых 405 входили в русскую группу (32 %), 315 в германскую (25 %). В январе 1914 года в Берлине состоялось грандиозное юбилейное мероприятие в честь 25-летия Международного союза криминалистов, на котором присутствовали представители германского правительства. Строились планы будущей работы организации по следующим основным вопросам: о преобразовании уголовного процесса для его соответствия новым требованиям уголовного права, в том числе «мерам социальной защиты»; об обвинительном принципе и новых проблемах; о том, на каких условиях и в каких границах допустимо применять к взрослым преступникам те начала, которые были выработаны Союзом для применения к несовершеннолетним; о системе наказаний, мерах наказания и исполнении наказания; о выработке международных определений, применимых как к Общей, так и к Особенной частям уголовного права; о территориальном принципе уголовного права и праве

выдачи; о международной регламентации права выдачи; об исследовании причин преступления; о подготовке судей [15].

Причиной окончания съездов представителей Международного Союза криминалистов явилась Первая мировая война. Российская и Германская империи прекратили свое существование в результате войны и последовавших событий. Большая часть представителей Международного союза криминалистов стала жить в абсолютно новых государствах. Что же касается представителей русской криминалистической группы, то они ещё в период существования Российской Империи придерживались достаточно прогрессивных левых взглядов по сравнению с центристами Ф. Листа. Впоследствии ряд участников русской криминалистической группы стали ведущими представителями советской уголовно-правовой науки. Так, например, под общей редакцией профессоров М. Н. Гернета, П. И. Люблинского и А. Н. Трайнина уже в 1920-е годы выпускалась серия «Криминалистика» [16]. М. Н. Гернет, П. И. Люблинский и другой бывший член русской секции Международного союза криминалистов — А.А. Жижиленко внесли существенный вклад в становление и развитие Института законодательства и сравнительного правоведения при Правительстве Российской Федерации [17].

Таким образом, следует сказать, что существенный вклад в развитие российской уголовно-правовой науки внес именно Международный союз криминалистов, как прекрасная площадка по обмену научными взглядами в сфере уголовного права, уголовно-исполнительного права, криминологии, уголовного процесса и криминалистики. Фактически это была организация представителей социологической школы уголовного права, целью которой была консолидация усилий ее сторонников в деле реформирования уголовного законодательства и уголовного судопроизводства. Для российской уголовно-правовой науки создание Международного союза криминалистов представляется несомненной удачей, так как потребовало от российских юридических обществ, расположенных по разным городам, перехода на следующую ступень взаимодействия — совместного общегосударственного представительства на международном уровне.

Представляется, что русская секция Международного союза криминалистов своим существованием была обязана не только И. А. Фойницкому, но и Н. С. Таганцеву. Данные двое учёных собрались для выступления по вопросам уголовного права на Первом Съезде русских юристов в 1875 году. Впоследствии И.А. Фойницкий инициировал создание русской секции, а Н.С. Таганцев стал ее председателем, принявшим в общество наиболее известных представителей, в том числе и А. Ф. Кони, вступившего в общество в 1902 году.

Учитывая значение первого Международного союза криминалистов и его положительный опыт, следует признать создание нового Международного союза криминалистов в 2023 году исключительно важным шагом по развитию уголовно-правовой мысли. Что же касается Молодежной секции, которая провела свой первый съезд в Московской академии Следственного комитета Российской Федерации имени А. Я. Сухарева, то можно назвать данное событие знаковым. Первый Международный союз криминалистов представлял собой своеобразную школу подготовки молодых ученых. Не исключено, что в состоявшемся первом съезде приняли участие новые Н. С. Таганцев и И. А. Фойницкий, М. Н. Гернет и А.Н. Трайнин, А. А. Жижиленко и П. И. Люблинский. При этом часть докладчиков съезда выступала с докладами, подготовленными под научным руководством авторов настоящей статьи, что, несомненно, найдет отражение в готовящемся сборнике научных публикаций. Именно так и творится история уголовно-правовой науки: вчера, сегодня и завтра.

Список литературы

1. Международный союз криминалистов // официальный сайт Московской академии Следственного комитета Российской Федерации имени А. Я. Сухарева.

URL: https://academy-skrf.ru/mskrim/ (дата обращения 04.10.2024).

2. Невский С. А. Международный союз криминалистов (из истории международного научного сотрудничества) // Международное уголовное право и международная юстиция. — 2017. — №4. — С.19-22.

3. Лоба В. Е. «Рецепты» борьбы с преступностью социологической школы уголовного права // Вестник Томского государственного университета. Право. — 2013. — №4. — С.100-107.

4. Van Hamel J. A., International Union of Criminal Law, 2 J. Am. Inst. Crim. L. & Criminology 22 (May 1911 to March 1912) // Journal of Criminal Law and Criminology. — 1911. — №2. — С.22-27 // официальный сайт Northwestern University. URL: https://scholarlycommons.law.northwestern.edu/jclc/vol2/iss1/3 (дата обращения 02.10.2024).

5. Съезд русских юристов в Москве в 1875 году: (материалы) / под ред. С. И. Баршева и др. – М.: тип. Мамонтова, 1882. — 280 с.

6. Сэруа В. С. К вопросу о межинституциональном взаимодействии в системе организации науки в России середины XIX - начала XX вв // Приволжский научный вестник. — 2015. — №3-2. — С.30-33.

7. Сикорский И. А. Чувства, испытываемые зрителем при виде смертной казни : Речь, сказ. проф. И. А. Сикорским на Съезде Русской группы Международного съезда криминалистов, в Киеве, 4 янв. 1905 г. - Киев: лито-тип. т-ва И. Н. Кушнерев и К, 1905. — 10 с.

8. Международный союз криминалистов. Русская группа. (1899-1902): (Материалы). - Санкт-Петербург, 1902. — 577 с.

9. Фейнберг Ц. М. Учение о вменяемости в различных школах уголовного права и в судебной психиатрии / Ц. М. Фейнберг; Центр. науч.-иссл. ин-т судебной психиатрии им. проф. Сербского. - М: тип. Министерства западугля СССР, 1946. — 89 с.

10. Уголовное право и социализм. Сборник статей / Пер. под ред. и с предисл. М. Н. Гернет. - М: тип. И.Д. Сытина, 1908. — 227 с.

11. Гернет М. Н. Детоубийство: Детоубийство. Социологическое и сравнительно-юридическое исследование: с приложением 12 диаграмм. / М.Н. Гернет. – М.: тип. Императорского Московского университета, 1911. — 318 с.

12. Сафронова Е. В., Лоба В. Е. «Опасное состояние личности» как криминологическая категория // Всероссийский криминологический журнал. — 2014. — №3. — С.10-17.

13. УК РСФСР 1922 // Собрание узаконений РСФСР. — 1922. № 15. — Ст. 153 (утратил силу).

14. Люблинский П. И. Брюссельский международный конгресс Союза криминалистов: (2-7 авг. 1910 г. нов. ст.) / П.И. Люблинский. - Санкт-Петербург: Сенат. тип., 1910. — 58 с.

15. Люблинский П. И. Международные съезды по вопросам уголовного права за десять лет (1905-1915) / Международные съезды по вопросам уголовного права за десять лет (1905-1915) / Проф. П.И. Люблинский. - Петроград: Сенат. тип., 1915. — 379 с.

16. Шнейкерт Г. Тайна преступника и пути к ее раскрытию: (К учению о судебных доказательствах) / Г. Шнейкерт, пер. с нем. под ред. и с предисл. П. И. Люблинского. – М.: Право и жизнь, 1925. — 64 с.

17. Незабываемые имена / официальный сайт Института законодательства и сравнительного правоведения при Правительстве Российской Федерации. URL: https://izak.ru/institute/nezabyvaemye-imena/ (дата обращения 04.10.2024).

References

1. International Union of Criminologists // official website of the Moscow Academy of the Investigative Committee of the Russian Federation named after A. Ya. Sukharev. URL: https://academy-skrf.ru/mskrim / (accessed: 04.10.2024).

2. Nevsky S. A. International Union of Criminologists (from the history of international scientific cooperation) // International criminal law and International justice. — 2017. — No. 4. — pp.19-22.

3. Loba V. E. «Recipes» for combating crime of the sociological school of criminal law // Bulletin of Tomsk State University. Right. - 2013. — No. 4. — pp.100-107.

4. Van Hamel J. A., International Union of Criminal Law, 2 J. Am. Inst. Crim. L. & Criminology 22 (May 1911 to March 1912) // Journal of Criminal Law and Criminology. — 1911. — No. 2. — S.22-27 // the official website of Northwestern University. URL: https://scholarlycommons.law. northwestern.edu/jclc/vol2/iss1/3 (accessed: 02.10.2024)

5. Congress of Russian Lawyers in Moscow in 1875: (materials) / edited by S. I. Barshev et al. – Moscow: tip. Mamontova, 1882. 280 p.

6. Serua V. S. On the issue of interinstitutional interaction in the system of science organization in Russia in the middle of the XIX - early XX centuries // Privolzhsky Scientific Bulletin. 2015. No.3-2. pp.30-33.

7. Sikorsky I. A. Feelings experienced by the viewer at the sight of the death penalty : Speech, fairy tale. I. A. Sikorsky at the Congress of the Russian Group of the International Congress of Criminologists, in Kiev, January 4, 1905 - Kiev: lit. tip. t-va I. N. Kushnerev and Co., 1905. - 10 p.

8. International Union of Criminologists. The Russian band. (1899-1902): (Materials). - St. Petersburg, 1902. — 577 p.

9. Feinberg C. M. The doctrine of sanity in various schools of criminal law and in forensic psychiatry / C. M. Feinberg; Center for Scientific Research. Institute of Forensic Psychiatry named after Prof. Serbian. - M: type. Ministries of the West of the USSR, 1946. 89 p.

10. Criminal law and socialism. Collection of articles / Translated by ed. and with a preface by M. N. Gernet. Moscow: I.D. Sytina Publishing House, 1908. 227 p.

11. Gernet M. N. Infanticide: Infanticide. Sociological and comparative legal research: with the application of 12 diagrams. / M.N. Gernet. – M.: type. Imperial Moscow University, 1911. — 318 p.

12. Safronova E. V., Loba V. E. "Dangerous state of personality" as a criminological category // All—Russian Journal of Criminology, 2014, No. 3, pp.10-17.

13. Criminal Code of the RSFSR 1922 // Collection of laws of the RSFSR. — 1922. № 15. — Art. 153 (expired).

14. Lublinsky P. I. The Brussels International Congress of the Union of Criminologists: (2-7 Aug. 1910 new art.) / P.I. Lublinsky. - St. Petersburg: Senate. tip., 1910. — 58 p.

15. Lyublinsky P. I. International congresses on criminal law for ten years (1905-1915) / International congresses on criminal law for ten years (1905-1915) / Prof. P.I. Lyublinsky. - Petrograd: Senate. tip., 1915. — 379 p.

16. Shneikert G. The mystery of the criminal and the ways to its disclosure: (To the doctrine of judicial evidence) / G. Shneikert, translated from German. edited by and with a preface by P. I. Lyublinsky. Moscow: Pravo i zhizn, 1925. 64 p.

17. Unforgettable Names / official website of the Institute of Legislation and Comparative Law under the Government of the Russian Federation, URL: https://izak.ru/institute/nezabyvaemye-imena / (accessed: 04.10.2024).

Информация об авторах

А. Л. Иванов — заведующий кафедрой уголовного права и криминологии Московской академии Следственного комитета Российской Федерации имени А. Я. Сухарева, кандидат юридических наук, доцент

П. Т. Савин — доцент кафедры уголовного права и криминологии Московской академии Следственного комитета Российской Федерации имени А. Я. Сухарева, кандидат юридических наук, доцент

Information about the authors

A. L. Ivanov — Head of the Department of Criminal Law and Criminology at the Sukharev Moscow Academy of the Investigative Committee of the Russian Federation, Candidate of Law, Associate Professor.

P. T. Savin — Associate Professor at the Department of Criminal Law and Criminology at the Sukharev Moscow Academy of the Investigative Committee of the Russian Federation, Candidate of Law, Associate Professor.

УДК 343.9.01

Киберпреступность в Беларуси: тенденции, угрозы, инновации в противодействии

Юрий Францевич Каменецкий
Учреждение образования «Институт повышения квалификации и переподготовки Следственного комитета Республики Беларусь», Минск, Беларусь

Email: kam_science@mail.ru

Аннотация. В статье исследуются состояние и тенденции киберпреступлений в Республике Беларусь, дается их криминалистическая характеристика. Обосновывается вывод, что эффективность противодействия киберпреступности предопределяется комплексным применением законодательных, организационно-практических, научно-образовательных и профилактически-просветительских мер. Описываются принятые в Беларуси законодательные новеллы в указы Президента Республики Беларусь, Уголовный и Уголовно-процессуальный кодексы, а также в Кодекс Республики Беларусь об административных правонарушениях. Приводятся положительные примеры следственной практики. На основе теории следственной профилактики и конкретных её функций предлагаются комплексы организационно-практических мер противодействия киберпреступности, аргументируются наиболее перспективные направления дальнейшего совершенствования данной сферы правоохранительной деятельности.
Ключевые слова: киберпреступность, информационно-коммуникационные технологии, следственная профилактика, функция следственной профилактики, вишинг, фишинг, кибервымогательство, блокировка, совершенствование законодательства.
Для цитирования: Каменецкий Ю.Ф. Киберпреступность в Беларуси: тенденции, угрозы, инновации в противодействии // Мир криминалистики. 2025. № 1. С. 69-77

Cybercrime in Belarus: trends, threats, innovations for counteraction

Yuri F. Kamenetsky
Educational institution «Institute of Advanced Training and Retraining of the Investigative Committee of the Republic of Belarus», Minsk, Belarus

Email: kam_science@mail.ru

Abstract. The state and trends of cybercrimes in the Republic of Belarus are considered. Its forensic characteristics is provided. The conclusion is substantiated that the efficiency of combating cybercrime is predetermined by comprehensive application of legal, institutional and practical, scientific and educational, preventive and educational measures. Legislative innovations adopted in the Republic of Belarus in Presidential Decrees, the Criminal Code, the Code of Criminal Procedure and the Code on Administrative Offences are described. Successful cases from investigative practice are provided. On the basis of the theory of investigative prevention and its particular functions, packages of institutional and practical measures of combating cybercrime are offered. Strategic pathways for further improvement of this sphere of law-enforcement activity are given.
Keywords: cybercrime, information and communication technologies, investigative prevention, function of investigative prevention, vishing, phishing, cyber extortion, blocking, improvement of legislation.
For citation: Kamenetsky Yu. F. Cybercrime in Belarus: trends, threats, innovations for counteraction // The world of criminology. 2025;(1):69-77

Введение. Киберпреступность представляет серьезную угрозу национальной безопасности Беларуси и Союзного государства. Об этом свидетельствует генезис и современное состояние данного вида преступности в Республике Беларусь, а также криминологические прогнозы её развития, основанные на национальном опыте и общемировых тенденциях.

Вопросы борьбы с киберпреступлениями активно обсуждаются в научном сообществе и нашли своё отражение в трудах А. И. Александрова, А. И. Бастрыкина, А. А. Бессонова, А. Ф. Волынского, Б. Я.

Гаврилова, В. И. Елётнова, А. М. Зинина, И. М. Комарова, О. С. Кучина, Н. П. Майлис, И. М. Рагимова, Е. Р. Россинской, А. Л. Савенка, М. В. Савич, А. Н. Савенкова, А. А. Сосновского, М. П. Шруба [1; 2; 3; 4; 5; 6; 7; 8; 9; 10; 11; 12; 13; 14; 15; 16] и др. В контексте заданного научного вектора полагаем, что глубокого теоретического осмысления требуют современное состояние противодействия киберпреступности в Беларуси, а также показавшие высокую эффективность передовые практики Следственного комитета Республики Беларусь (далее – Следственный комитет). Данное научное изыскание предлагается провести с позиции разрабатываемой нами теории следственной профилактики и конкретно функций профилактической деятельности [17], позволяющих выявлять дополнительные резервы совершенствования правоохранительной превентивной сферы.

Основная часть. Криминологическая оценка уголовно наказуемых противоправных деяний за истекший год показывает, что при общей динамике снижения преступности в Беларуси на 14,2 % доля киберпреступлений в общем числе зарегистрированных преступлений возросла с 21,8 % до 27,9 %, прибавив в сравнении с 2023 г. 9,9 % (с 18 321 до 20 137) [18].

Настоящее время отличается массовым совершением киберпреступлений в отношении населения Республики Беларусь, активизацией деятельности транснациональных организованных преступных групп, которые специализируются на хищениях путем вишинга, фишинга и кибервымогательства. Криминалистическая характеристика каждого из указанных типичных видов хищений имеет свои особенности.

В частности, субъектом вишинга являются организованные преступные группы, которые носят международный характер и связаны с образованием и деятельностью на территории Украины, России и других стран значительного количества специальных кол-центров.

Цель данных групп – завладение деньгами граждан, их шантаж ради совершения правонарушений экстремистского характера (повреждение общественного имущества, поджоги автомобилей государственных служащих и зданий государственных органов, причинение вреда сотрудникам банков, дистанционная сексуальная эксплуатация, запись экстремистских видеообращений для использования в социальных сетях и т. п.). Основным средством совершения вишинга выступает социальная инженерия, основанная на доверии граждан к государственным органам и организациям.

Фишинг также чаще совершается транснациональными организованными группами, избирающими в качестве средства преступления фишинговые интернет-ресурсы.

Способы совершения фишинга включают следующие разновидности: обман, связанный с продажей поддельных водительских удостоверений, наркотиков, оказанием сексуальных услуг, а также инвестиций в криптовалюту; обман под предлогом купли-продажи в интернет-магазинах; обман с использованием фишинговых интернет-ресурсов для знакомств, когда под предлогом встречи в кафе, кино, театре потерпевших вынуждают ввести на фишинговый сайт реквизиты банковских платежных карточек с последующим хищением денежных средств с карт-счета; обман с использованием фишинговых интернет-ресурсов банков.

Типичное кибервымогательство проявляется в виде угроз распространения полученных мошенником интимных фотографий и сообщений либо переписки экстремистского характера.

Как обоснованно отмечается в научной литературе, при совершении киберпреступлений для оказания влияния на массы активно используется тактика сетевых деструктивных технологий, когда преступниками в совокупности с информационными средствами применяются методы манипуляции сознанием людей [2].

Проведенный анализ деятельности правоохранительных органов Беларуси показывает, что эффективность противодействия киберпреступности предопределяется комплексным применением законодательных, организационно-практических,

научно-образовательных и профилактически-просветительских мер. Указанный подход принят на вооружение и успешно реализуется Следственным комитетом, о чём могут свидетельствовать следующие примеры.

В 2024 г. пресечена преступная деятельность восьми расположенных в г. Минске, г. Москве и г. Бишкеке кол-центров, входящих в структуру международной преступной организации, участники которой с октября 2018 г. осуществляли хищение под предлогом инвестирования денежных средств граждан в несуществующие сверхприбыльные финансовые компании. Для маскировки преступной деятельности фиктивно регистрировались лжефирмы, от имени которых арендовались офисы, откуда осуществлялись переписка и звонки потерпевшим. К уголовной ответственности привлечено 62 участника преступной организации.

В более чем 300 хищениях в крупном и особо крупном размерах обвиняются 29 участников преступной группы, действовавших с территории Украины (г. Кривой Рог Днепропетровской области) под видом белорусских банковских работников и сотрудников правоохранительных органов. После хищения злоумышленники цинично унижали потерпевших, склоняли их к совершению различного рода правонарушений и преступлений (повреждение общественного имущества, поджоги автомобилей государственных служащих, зданий государственных органов, причинение вреда сотрудникам банков, дистанционная сексуальная эксплуатация, запись экстремистских видеообращений для использования в социальных сетях).

Всего выявлено более 45 транснациональных организованных групп (скам-групп), совершивших более 900 тыс. хищений денежных средств с банковских карт граждан Республики Беларусь, а также Российской Федерации, Республики Казахстан, Кыргызской Республики и других стран. Общее количество вовлеченных в противоправные схемы лиц составило не менее 400 тыс. человек. Преступная деятельность пяти организованных групп полностью прекращена, задержаны и привлечены к уголовной ответственности их руководители и активные участники, в том числе на территории Российской Федерации (в рамках межведомственного сотрудничества).

Названные уголовные дела позволили выявить способствующие совершению компьютерных преступлений причины и условия, определить конкретные меры противодействия киберпреступности в контексте реализации функций следственной профилактики.

Общий анализ расследования указанных уголовных дел свидетельствует, что в его основу вместе с тактическими функциями следственной профилактики положена главным образом реализация уголовно-превентивной (определение причастности лиц к преступлению, доказывание их виновности) и предупредительно-пресекающей (предотвращение готовящегося, пресечение начавшегося деструктивного явления, оперативное принятие решений о начале досудебного производства) функций.

Базируясь на изучении практики и международном опыте противодействия киберпреступности, Следственным комитетом совместно с иными государственными органами реализованы следующие законодательные новеллы:

1) приняты положения Указа Президента Республики Беларусь от 29 августа 2023 г. № 269 «О мерах по противодействию несанкционированным платежным операциям», регламентирующие алгоритм взаимодействия территориальных подразделений Следственного комитета с органами внутренних дел, позволяющие незамедлительно блокировать до 10 суток используемые в ходе преступления карт-счета и находящиеся на них похищенные денежные средства;

2) приняты положения Указа Президента Республики Беларусь от 17 сентября 2024 г. № 367 «Об обращении цифровых знаков (токенов)», запрещающие физическим лицам и индивидуальным предпринимателям покупку и продажу криптовалюты вне белорусских криптобирж (криптообменников), способствующие развитию

транспарентного и контролируемого обращения цифровых знаков (токенов), предотвращению вывода из страны похищенных с банковских счетов граждан денежных средств путем их обмена на крипто-валюту на зарубежных криптоплощадках. Более того, внесены предложения по установлению административной ответственности за нарушение требований данного Указа;

3) внесены предложения о корректировке ст. 222 «Незаконный оборот средств платежа и (или) инструментов» Уголовного кодекса Республики Беларусь и дополнении Кодекса Республики Беларусь об административных правонарушениях ст. 12.35 «Незаконное предоставление карт доступа, реквизитов платежных инструментов», позволяющие привлекать к ответственности лиц, обеспечивающих организованные преступные группы, например, такими средствами для преступления, как банковские платежные карточки. В развитие данных норм предложено дифференцировать ответственность дропов и дроповодов на административную (при сбыте банковских платежных карточек их держателем) и уголовную (при сбыте банковских платежных карточек, оформленных на третьих лиц);

4) внесены предложения по дополнению ст. 199 «Представление об устранении нарушений закона, причин и условий, способствовавших совершению преступления» Уголовно-процессуального кодекса Республики Беларусь, расширяющие компетенцию следователя по ограничению доступа к используемым для совершения преступлений интернет-ресурсам, SIM-картам и другим средствам.

Приведенные выше меры по совершенствованию законодательства фактически воплотили в жизнь нормообразующую функцию следственной профилактики, обеспечив единство и целостность правового регулирования в области предупредительной деятельности.

Кроме того, по инициативе Следственного комитета в Уголовно-процессуальный кодекс Республики Беларусь внесены предложения и прорабатывается механизм своевременного возврата пострадавшим гражданам находящихся на счетах безналичных денежных средств, на которые наложен арест. Особо актуален этот вопрос при расследовании неочевидных преступлений, когда следствию удалось арестовать счета с похищенными деньгами, а виновные лица ещё не установлены. В данном случае речь идет о предотвращении и заглаживании вредных последствий, обеспечиваемых в ходе предупредительно-восстановительной функции следственной профилактики.

Следует отметить, **что законодательные новеллы внедряются одновременно с совершенствованием комплекса организационно-практических мер, включающего:**

1) введение специализации расследования киберпреступлений на всех уровнях (центральный аппарат, регион, район);

2) создание механизма выявления новых скам-групп, блокировки их инфраструктуры, используемых ими средств совершения преступлений, который основан на функционировании АИС «След», АИС «ГУПК», АБД «Антифишинг», АСОИ [19];

3) осуществление мониторинга интернета для выявления фишинговых и иных интернет-ресурсов, используемых в противоправной деятельности для совершения хищений денежных средств граждан и субъектов хозяйствования, кибератак в отношении государственных и иных информационных ресурсов, хищения и незаконного распространения персональных данных, экстремистских проявлений (в 2024 г. заблокировано более 2 тыс. таких интернет-ресурсов);

4) принятие мер по блокировке используемых при совершении преступлений инструментов (IP-телефония, доменные имена, аккаунты криптобиржи, социальных сетей и мессенджеров). Анализ данных мер показывает, что в их основе лежит реализация предупредительно-экспроприационной функции следственной профилактики, направленной на ограничение использования орудий и средств совершения аналогичных преступлений.

Эффективность расследования новых разновидностей преступлений в сфере информационно-коммуникационных технологий требует соответствующего научно-образовательного и кадрового обеспечения, т. е. реализации методически обеспечивающей функции следственной профилактики. В этом плане большое значение имеет сокращение времени между появлением нового вида преступления и полноценной методикой его расследования, а лучше – обеспечение предварительной готовности для расследования потенциально новых видов преступлений.

Решение данной проблемы во многом зависит от кадрового потенциала правоохранительных органов, общего уровня подготовки специалистов, вовлекаемых в расследование преступлений в сфере информационно-коммуникационных технологий, а также от наличия отвечающей современным вызовам и угрозам образовательной и научно-методической базы. В данном случае речь идет о создании образовательных и научных учреждений и объединений, их вовлеченности в практическую деятельность, обеспечении возможностей изучения современных средств и способов совершения преступлений, разработке широкого спектра востребованных обучающих узкопрофильных программ. В настоящее время обозначенные направления деятельности реализуются на базе Института Следственного комитета и в целом положены в основу обеспечения цифровизации предварительного следствия. В ведомственном учреждении образования созданы специализированные учебные курсы, дифференцированные по разновидностям киберпреступлений, включающие стажировку с участием в расследовании уголовных дел. При этом профессорско-преподавательский состав также участвует в расследовании и оперативно имплементирует передовые практики в учебные издания [19; 20] и занятия.

Не менее важным направлением противодействия киберпреступности выступают профилактически-просветительские меры, основывающиеся на реализации общевоспитательной (побуждение граждан к правомерному поведению и недопущению развития детерминант преступности) и предупредительно-информационной (обеспечение получения гражданами информации о сущности и специфических особенностях следственной профилактики, существующих угрозах противоправного поведения, средствах и методах, повышающих их защищенность от противоправного воздействия) функций следственной профилактики [17, с. 94–95]. Положительным примером в этом плане является следующая практика: информирование организаций о наиболее распространенных способах совершения киберпреступлений (подобным образом Следственным комитетом проинформировано более 200 организаций); направление в министерства информации в целях предупреждения граждан о современных угрозах киберпреступности (всего направлено 12 та-ких информаций); проведение в рамках Белорусского юридического форума тематической площадки с крупнейшими торговыми интернет-ресурсами по вопросам профилактики киберпреступлений (г. Минск, 28–29 ноября 2024 г.).

Приведенные меры противодействия киберпреступлениям в ближайшей перспективе будут способствовать решению проблем, связанных с ростом количества транснациональных преступных групп, формированием новых кол-центров для вишинга; распространением киберпреступлений как услуги, обеспечивающей экстремизм, незаконный оборот наркотических средств, совершение хищений и т. п.; применением криптовалют, а также использованием информационно-коммуникационных технологий как средств политической и военной борьбы.

Таким образом, рассмотренные посредством функций следственной профилактики меры противодействия киберпреступлениям предстают перед нами с позиции своих социального назначения и сущности правового воздействия.

Стоит отметить, что применительно к рассматриваемому виду преступлений названные функции следственной профилактики приобрели первостепенное

значение. Вместе с тем есть и иные, которые пока не получили должного развития.

В частности, дополнительной защиты от киберпреступлений требуют малый и средний бизнес, государственные организации и предприятия. Объектом следственной профилактики в данном случае выступают дефекты и недостатки в кибербезопасности, упущения в работе по её обеспечению. Решению обозначенного вопроса может способствовать предупредительно-защитная функция следственной профилактики, которая направлена на охрану заведений, организаций и учреждений, не только пострадавших от преступных посягательств, но и с высокой степенью уязвимости от криминогенных факторов, что достигается посредством внесения предложений по введению соответствующих организационно-практических мер.

Не решенной до конца проблемой в рассматриваемой сфере также выступает противодействие использованию в ходе совершения киберпреступлений искусственного интеллекта и дипфейков. В настоящее время отдельные аспекты данного направления уже проработаны. Исследование, например, сгенерированного с помощью искусственного интеллекта речевого следа получило свое развитие в криминалистическом речеведении [21]. Наряду с этим научно-технические средства распознания и ограничения использования фейкового контента также требуют своего эффективного внедрения в профилактическую деятельность. Полагаем, что воплотить в жизнь вышеизложенное возможно посредством реализации комплекса предупредительно-экспроприационной, методически обеспечивающей, общевоспитательной и предупредительно-информационной функций следственной профилактики.

Заключение. Проведенное исследование показывает, что в настоящее время для противодействия киберпреступлениям Следственным комитетом применяется комплекс законодательных, организационно-практических, научно-образовательных и профилактически-просветительских мер, который основан на реализации уголовно-превентивной, предупредительно-пресекающей, нормообразующей, предупредительно-восстановительной, предупредительно-экспроприационной, методически обеспечивающей, общевоспитательной и предупредительно-информационной функций.

Разработанные меры противодействия киберпреступлениям в ближайшей перспективе способны решать ряд проблем, связанных с ростом количества транснациональных преступных групп, формированием новых кол-центров для вишинга; распространением киберпреступлений как услуги, обеспечивающей экстремизм, незаконный оборот наркотических средств, совершение хищений и т. п.; применением криптовалют, а также использованием информационно-коммуникационных технологий как средств политической и военной борьбы.

Исходя из существующих угроз киберпреступности можно определить следующие **перспективные направления (резервы) профилактического воздействия:**

1) повышение уровня и увеличение арсенала средств кибербезопасности малого и среднего бизнеса, государственных организаций и предприятий посредством реализации предупредительно-защитной функции, подразумевающей обеспечение дополнительной защиты объектов, не только пострадавших от преступных посягательств, но и с высокой степенью уязвимости от криминогенных факторов;

2) внедрение в правоохранительную деятельность средств распознания и ограничения используемых при совершении киберпреступлений технологий искусственного интеллекта и дипфейков посредством реализации комплекса предупредительно-экспроприационной, методически обеспечивающей, общевоспитательной и предупредительно-информационной функций следственной профилактики.

Список источников

1. Александров А. И. Уголовный

процесс России – вчера и завтра / А. И. Александров // Закон и власть. – 2021. – № 1. – С. 61–65.

2. Бессонов А. А. Информационные технологии как угроза национальной безопасности и средство по ее обеспечению / А. А. Бессонов // Предварительное расследование. – 2023. – № 2(14). – С. 19–25.

3. Волынский А. Ф. Научно-техническое обеспечение уголовного судопроизводства: от привычных проблем к реалиям практики / А. Ф. Волынский // Вестник Университета прокуратуры Российской Федерации. – 2024. – № 1(99). – С. 47–56.

4. Гаврилов Б. Я. О современном состоянии Российской уголовно-процессуальной науки и ее роли в повышении эффективности отдельных институтов уголовного судопроизводства / Б. Я. Гаврилов // Предварительное расследование. – 2024. – № 1(15). – С. 21–26.

5. Елётнов В. И. Генезис и перспективы использования специальных знаний в сфере информационных технологий при расследовании преступлений / В. И. Елётнов // Следственная деятельность. – 2022. – № 2. – С. 223–235.

6. Зинин А. М. Мышление человека и искусственный интеллект в аспекте сравнительного исследования внешнего облика человека по его изображениям / А. М. Зинин, О. Г. Дьяконова // Эксперт-криминалист. – 2023. – № 3. – С. 2–5.

7. Комаров И. М. Криминалистика для обеспечения глобального равновесия будущего / И. М. Комаров, Е. С. Крюкова // Эксперт-криминалист. – 2024. – № 3. – С. 34–37.

8. Кучин О. С. Отдельные аспекты концепции комплексной методики расследования преступлений в сфере киберпространства / О. С. Кучин // Следственная деятельность. – 2024. – № 4. – С. 239–251.

9. Майлис Н. П. Экспертные ошибки, допускаемые при исследовании традиционных и цифровых следов / Н. П. Майлис // Теория и практика судебной экспертизы. – 2024. – Т. 19, № 1. – С. 20–24.

10. Рагимов И. М. О компьютерной программе определения меры наказания / И. М. Рагимов // Криминология: вчера, сегодня, завтра. – 2019.–№ 1(52). – С. 21–22.

11. Россинская Е. Р. Нейросети в судебной экспертологии и экспертной практике: проблемы и перспективы / Е. Р. Россинская // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2024. – № 3(115). –С. 21–33.

12. Савенок А. Л. Правовая оценка причинения вреда при использовании технологий искусственного интеллекта / А. Л. Савенок // Следственная деятельность. – 2021. – № 1. – С. 145–152.

13. Седых П. В. Единая автоматизированная информационная система Следственного комитета Республики Беларусь как средство решения задач следователя при назначении судебных экспертиз / П. В. Седых, М. В. Савич // Следственная деятельность. – 2023. – № 3. – С. 53–67.

14. Савенков А. Н. Актуальные направления развития общей теории криминалистики сквозь призму современных технологий / А. Н. Савенков, Е. Р. Россинская // Государство и право. – 2024. – № 10. – С. 156–168.

15. Сосновский А. А. Анализ законодательства о правовом регулировании информатизации следственной деятельности / А. А. Сосновский // Следственная деятельность. – 2022. – № 2. – С. 71–79.

16. Шруб М. П. Разработка криминалистической характеристики преступлений в сфере сексуальной эксплуатации в условиях развития современных информационных технологий / М. П. Шруб // Следственная деятельность. – 2022. – № 2. – С. 322–335.

17. Каменецкий Ю. Ф. Теория и практика следственной профилактики / Ю. Ф. Каменецкий. – Минск: СтройМедиаПроект, 2024. – 536 с.

18. О результатах работы, состоянии служебной (трудовой) дисциплины, профилактики правонарушений и происшествий в подразделениях Следственного комитета Республики Беларусь в 2024 году и задачах на 2025 год : постановление коллегии Следств. ком. Респ. Беларусь от 7 февр. 2024 г. № 1кск // ЭТАЛОН: информ.-поисковая система (дата

обращения: 11.02.2024).

19. Компьютерная информация в следственной деятельности: собирание, оценка, использование: учеб. пособие / Ю. Ф. Каменецкий, В. И. Каминский, М. В. Савич [и др.]; под общ. ред. Ю. Ф. Каменецкого; Ин-т повышения квалификации и переподгот. Следств. ком. Респ. Беларусь. – 2-е изд., перераб. – Минск, 2023. – 288 с.

20. Расследование хищений, совершенных путем фишинга организованной преступной группой: учебник / Ю. Ф. Каменецкий, А. А. Воронько, В. И. Елётнов [и др.]; под общ. Ред. Ю. Ф. Каменецкого; Ин-т повышения квалификации и переподгот. Следств. Ком. Респ. Беларусь. – Минск, 2024. – 376 с.

21. Галяшина Е. И. Криминалистическое речеведение как отрасль криминалистической техники / Е. И. Галяшина // Предварительное расследование. – 2024. – № 2(16). – С. 16–22.

References

1. Alexandrov A. I. The criminal process of Russia – yesterday and tomorrow / A. I. Alexandrov // Law and power. – 2021. – No. 1. – pp. 61-65.

2. Bessonov A. A. Information technologies as a threat to national security and a means to ensure it / A. A. Bessonov // Preliminary investigation. – 2023. – № 2(14). – Pp. 19-25.

3. Volynsky A. F. Scientific and technical support of criminal proceedings: from familiar problems to the realities of practice / A. F. Volynsky // Bulletin of the University of the Prosecutor's Office of the Russian Federation. – 2024. – № 1(99). – Pp. 47-56.

4. Gavrilov B. Ya. On the current state of Russian criminal procedure science and its role in improving the effectiveness of individual institutions of criminal justice / B. Ya. Gavrilov // Preliminary investigation. – 2024. – № 1(15). – Pp. 21-26.

5. Yetnov V. I. The genesis and prospects of using special knowledge in the field of information technology in the investigation of crimes / V. I. Yetnov // Investigative activity. - 2022. – No. 2. – pp. 223-235.

6. Zinin A.M. Human thinking and artificial intelligence in the aspect of comparative study of human appearance based on its images / A.M. Zinin, O. G. Dyakonova // Forensic expert. - 2023. – No. 3. – pp. 2-5.

7. Komarov I. M. Criminalistics to ensure the global balance of the future / I. M. Komarov, E. S. Kryukova // Criminologist expert. - 2024. – No. 3. – pp. 34-37.

8. Kuchin O. S. Selected aspects of the concept of an integrated methodology for investigating crimes in the field of cyberspace / O. S. Kuchin // Investigative activity. - 2024. – No. 4. – pp. 239-251.

9. Mailis N. P. Expert mistakes made in the study of traditional and digital traces / N. P. Mailis // Theory and practice of forensic examination. – 2024. – Vol. 19, No. 1. – pp. 20-24.

10. Ragimov I. M. On the computer program for determining the measure of punishment / I. M. Ragimov // Criminology: yesterday, today, tomorrow. – 2019.– № 1(52). – Pp. 21-22.

11. Rossinskaya E. R. Neural networks in forensic expertise and expert practice: problems and prospects / E. R. Rossinskaya // Bulletin of the O. E. Kutafin University (MGUA). – 2024. – № 3(115). – Pp. 21-33.

12. Savenok A. L. Legal assessment of harm caused by the use of artificial intelligence technologies / A. L. Savenok // Investigative activity. – 2021. – No. 1. – pp. 145-152.

13. Sedykh P. V. Unified automated information system of the Investigative Committee of the Republic of Belarus as a means of solving investigator's tasks when appointing forensic examinations / P. V. Sedykh, M. V. Savich // Investigative activity. - 2023. – No. 3. – pp. 53-67.

14. Savenkov A. N. Actual directions of development of the general theory of criminalistics through the prism of modern technologies / A. N. Savenkov, E. R. Rossinskaya // The State and Law. – 2024. – No. 10. – pp. 156-168.

15. Sosnovsky A. A. Analysis of legislation on the legal regulation of informatization of investigative activities / A. A. Sosnovsky // Investigative activities. - 2022. – No. 2. – pp. 71-79.

16. Shrub M. P. Development of criminalistic characteristics of crimes in the field of sexual exploitation in the context of the development of modern information technologies / M. P. Shrub // Investigative activity. – 2022. – No. 2. – pp. 322-335.

17. Kamenetsky Yu. F. Theory and practice of investigative prevention / Yu. F. Kamenetsky. – Minsk: StroyMediaProekt, 2024. – 536 p.

18. On the results of work, the state of official (labor) discipline, prevention of offenses and incidents in the units of the Investigative Committee of the Republic of Belarus in 2024 and tasks for 2025 : resolution of the Board of Investigative Committee. Rep. Belarus No. 1ksk dated February 7, 2024 // ETALON: inform.-search engine (accessed: 02.11.2024).

19. Computer information in investigative activities: collection, evaluation, use: textbook. manual / Yu. F. Kamenetsky, V. I. Kaminsky, M. V. Savich [et al.]; under the general editorship of Yu. F. Kamenetsky; Institute of Advanced Training and Retraining. Investigative Committee Rep. Belarus. – 2nd ed., revised. – Minsk, 2023. – 288 p.

20. Investigation of thefts committed by phishing by an organized criminal group: textbook / Yu.F. Kamenetsky, A. A. Voronko, V. I. Yetnov [et al.]; under the general editorship of Yu. F. Kamenetsky; Institute of Advanced Training and Retraining. Investigative Committee Rep. Belarus. – Minsk, 2024. – 376 p.

21. Galyashina E. I. Criminalistic speech production as a branch of criminalistic technology / E. I. Galyashina // Preliminary investigation. – 2024. – № 2(16). – Pp. 16-22.

Информация об авторе

Ю.Ф. Каменецкий — кандидат юридических наук, доцент, начальник учреждения образования «Институт повышения квалификации и переподготовки Следственного комитета Республики Беларусь», член Президиума Международного союза криминалистов, Председатель Отделения белорусских криминалистов Белорусского республиканского союза юристов.

Information about the author

Yu. F. Kamenetsky — Candidate of Law, Associate Professor, Head of the educational institution «Institute of Advanced Training and Retraining of the Investigative Committee of the Republic of Belarus», member of the Presidium of the International Union of Criminologists, Chairman of the Department of Belarusian Criminologists of the Belarusian Republican Union of Lawyers.

УДК: 343.1 / 004.42
ББК 67.9 / 32.973

Уголовные преступления против безопасности компьютерных данных

Иван Милич
Университет Нови-Сада, Нови-Сад, Республика Сербия

Email: i.milic@pf.uns.ac.rs

Аннотация. Предметом исследования в рамках данной статьи являются преступные действия против безопасности компьютерных данных в Республике Сербии. Речь идет о восьми уголовных преступлениях, которые описаны в одной из глав Уголовного кодекса Республики Сербия. Автор анализирует суть вышеуказанных преступлений, а также специальный закон, действующий в Республике Сербия, который регулирует выявление уголовных преступлений, уголовное преследование и судебное разбирательство в сфере высоких технологий.
Ключевые слова: Республика Сербия, уголовное преступление, компьютерное преступление, Уголовный кодекс.
Научная специальность: 5.1.2. Публично-правовые (государственно-правовые) науки
Для цитирования: Милич И. Уголовные преступления против безопасности компьютерных данных // Мир криминалистики. 2025. № 1. С. 78-83

The criminal offences against computer data security

Ivan Milic
University of Novi Sad, Novi Sad, Republic of Serbia

Email: i.milic@pf.uns.ac.rs

Abstract. The subject of this paper is criminal acts against the security of computer data in the Republic of Serbia. These are eight criminal acts that are prescribed in one chapter of the Criminal Code. The author points out the essence of the listed criminal acts. The author also points out a special law in force in Serbia that regulates the detection, prosecution and trial of criminal acts of high-tech crime.
Keywords: Republic of Serbia, Criminal offense, computer crime, Criminal Code.
For citation: Milic I. The criminal offences against computer data security // The world of criminology. 2025;(1):78-83

Уголовное право защищает определенные социальные ценности. Социальные ценности, защищаемые уголовным правом, претерпели изменения. Сегодня можно сказать, что наибольшей ценностью, охраняемой уголовным правом, является человеческая жизнь. Об этом также можно судить по установленной мере наказания за преступления против жизни и здоровья. По мере развития общества расширялся и перечень защищаемых уголовным правом ценностей. Например, уголовные преступления против безопасности общественного транспорта не могли быть предусмотрены до тех пор, пока не появились автомобили. То же самое относится и к уголовным преступлениям, связанным с воздушными судами. В связи с этим, зачастую Уголовный кодекс дополняется новыми составами преступлений, некоторые уголовные преступления исключаются из закона, а некоторые из них изменяются и дополняются. Изменились и способы совершения преступлений. В прошлом некоторые преступления можно было совершить только с помощью оружия, инструмента, силы или угрозы. Сегодня совершить преступление можно

и с помощью компьютерных технологий. В науке утверждается, что компьютер представляет собой одно из самых значительных и революционных достижений технического и технологического развития конца XX века. Однако, в дополнение к многочисленным и разнообразным преимуществам, которые даёт компьютер, и огромным выгодам, которые он приносит человечеству, он быстро стал средством злоупотреблений со стороны недобросовестных лиц и групп. Таким образом, компьютерная преступность выступает как особая и специфическая форма современной преступности[1]. Меняются способы совершения преступлений, и в качестве средства совершения преступлений всё чаще используются компьютеры. Некоторые преступные деяния могут быть совершены на большом расстоянии от объекта преступления. Ещё труднее становится подобные деяния выявить. По мере развития технологий совершенствуются и преступники в сфере компьютерных преступлений. Первоначально совершать преступления в сфере компьютерных технологий могли только лица, обладающие определенными знаниями. Однако сегодня можно сказать, что существует большое количество людей, которые обладают базовыми знаниями, необходимыми для работы на компьютере, и поэтому используют компьютер как средство осуществления своих преступных замыслов. Конечно, для некоторых преступных деяний, где в качестве орудия используются компьютерные технологии, требуются более глубокие знания.

Уголовный кодекс Республики Сербии[2] также предусматривает уголовную ответственность за преступления против безопасности компьютерных данных[3]. Эти уголовные преступления классифицированы в одной из глав Уголовного кодекса Республики Сербии (УК), которая так и называется — Уголовные преступления против безопасности компьютерных данных (глава двадцать седьмая Уголовного кодекса). В этой главе описано в общей сложности восемь уголовных преступлений.

1. Повреждение компьютерных данных и программ (ст. 298 УК). Это действие совершается любым лицом, которое без разрешения удаляет, изменяет, повреждает, скрывает или иным образом делает компьютерные данные или программы непригодными для использования. Данное правонарушение карается штрафом или лишением свободы на срок до одного года. Существуют также более тяжкие формы этого правонарушения, которые классифицируются, если причинен более значительный ущерб. В этом случае может быть назначено наказание в виде лишения свободы на срок до пяти лет. Учитывая грозящее ему наказание в виде лишения свободы, виновному может быть назначено условное наказание при соблюдении иных условий для его назначения. Следует также отметить, что устройства и средства, использованные для совершения уголовного преступления, если они принадлежат виновному, подлежат конфискации.

2. Компьютерный саботаж (ст. 299 УК). Данное уголовное преступление

[1] См. Драган Јовашевић, Рачунарска превара (међународни стандарди и право Републике Србије), Годишњак факултета правних наука, бр. 14/2024. С. 117.

[2] Кривични законик, "Службени гласник РС", бр. 85 од 6. октобра 2005, 88 од 14. октобра 2005 - исправка, 107 од 2. децембра 2005 - исправка, 72 од 3. септембра 2009, 111 од 29. децембра 2009, 121 од 24. децембра 2012, 104 од 27. новембра 2013, 108 од 10. октобра 2014, 94 од 24. новембра 2016, 35 од 21. маја 2019, 94 од 28. новембра 2024.

[3] Республика Сербия также ратифицировала международные документы в этой области. Так, например, в РС действует Закон о ратификации Конвенции о борьбе с преступлениями в сфере высоких технологий (с текстом Конвенции): Служебный вестник Республики Сербия – Международные договоры, № 19/2009-3; Закон о ратификации Дополнительного протокола к Конвенции о преступлениях в сфере высоких технологий, касающегося криминализации актов расистского и ксенофобного характера, совершаемых через компьютерные системы (с текстом Конвенции): Служебный вестник Республики Сербия - Международные договоры, № 19/2009-40; Закон о ратификации Второго дополнительного протокола к Конвенции о преступлениях в сфере высоких технологий о расширенном сотрудничестве и раскрытии электронных доказательств: 7/2022-18.

определяется следующим образом: тот, кто вводит, уничтожает, стирает, изменяет, повреждает, скрывает или иным образом делает непригодными для использования компьютерные данные или программы, либо уничтожает или повреждает компьютер или другое устройство для электронной обработки и передачи данных с намерением вывести из строя или существенно нарушить процесс электронной обработки и передачи данных, имеющий значение для государственных органов, общественных служб, учреждений, предприятий или других субъектов, наказывается лишением свободы на срок от шести месяцев до пяти лет.

3. Создание и внедрение компьютерных вирусов (ст. 300 УК). Первый абзац данной статьи гласит: тот, кто создает компьютерный вирус с намерением внедрить его в компьютер или компьютерную сеть другого лица, наказывается штрафом или лишением свободы на срок до шести месяцев. В этом случае бывает сложно доказать, что преступник имел намерение внедрить вирус. Второй абзац данной статьи гласит: тот, кто внедряет компьютерный вирус в компьютер или компьютерную сеть другого лица и тем самым причиняет ущерб, наказывается штрафом или лишением свободы на срок до двух лет. Также за данное правонарушение конфискуются устройство и средства, использованные для совершения преступления.

4. Компьютерное мошенничество (ст. 301 УК). Данное правонарушение совершается лицом, которое вводит неверные данные, не вводит верные данные или иным образом скрывает или представляет ложные данные, и тем самым влияет на результат электронной обработки и передачи данных с намерением получить неправомерную имущественную выгоду для себя или другого лица и тем самым причинить имущественный ущерб другому лицу. Подобное правонарушение карается штрафом или лишением свободы на срок до трёх лет. Более суровые формы предусмотрены в случае реализации имущественной выгоды в особо крупном размере. Таким образом, если преступником получена имущественная выгода, превышающая один миллион пятьсот тысяч сербских динаров, виновный будет приговорен к лишению свободы на срок от двух до десяти лет. Учитывая грозящее наказание за эту наиболее тяжкую форму, исключено назначение условного наказания. За совершение данного уголовного преступления предусмотрена и более мягкая форма, которая учитывает намерение преступника. Если деяние совершено с единственным намерением причинить вред другому человеку, виновный будет наказан штрафом или тюремным заключением на срок до шести месяцев.

5. Несанкционированный доступ к защищенному компьютеру, компьютерной сети и средствам электронной обработки данных (ст. 302 УК). Данное деяние совершается любым лицом, которое, в нарушение мер защиты несанкционированно подключается к компьютеру или компьютерной сети либо несанкционированно получает доступ к электронной обработке данных. Данное правонарушение карается штрафом или лишением свободы на срок до шести месяцев. Более серьезная форма классифицируется, если виновный записывает или использует данные, полученные «несанкционированно» — за это предусмотрен штраф или лишение свободы на срок до двух лет. Самая серьёзная форма преступления имеет место, если деяние привело к остановке или серьёзному нарушению функционирования электронной обработки и передачи данных или сети, либо к иным тяжким последствиям. Виновный будет наказан лишением свободы на срок до трёх лет.

6. Воспрепятствование и ограничение доступа к компьютерной сети общего пользования (ст. 303 УК). Это деяние совершается любым лицом, которое несанкционированно препятствует или препятствует доступу к общедоступной компьютерной сети. Данное правонарушение карается штрафом или лишением свободы на срок до одного года. Более тяжкая форма имеет место, если данное деяние совершено должностным лицом при исполнении им своих обязанностей. За более

тяжкую форму предусмотрено наказание в виде лишения свободы на срок до трех лет.

7. Несанкционированное использование компьютера или компьютерной сети (ст. 304 УК). Это правонарушение совершается любым лицом, которое несанкционированно использует компьютерные услуги или компьютерную сеть с намерением получить неправомерную имущественную выгоду для себя или другого лица. Данное правонарушение карается штрафом или лишением свободы на срок до трех месяцев. Особенностью этого правонарушения является то, что оно преследуется не ex officio (в силу занимаемой должности), а на основании частной жалобы.

8. Изготовление, приобретение и предоставление другому лицу средств для совершения преступных действий против безопасности компьютерных данных (статья 304а). Это преступление совершается тем, кто производит, продает, приобретает для использования, импортирует, распространяет и иным образом предоставляет в распоряжение:

А) устройства и компьютерные программы, предназначенные или прежде всего предназначенные для совершения уголовного преступления против безопасности компьютерных данных (уголовного преступления, предусмотренного главой двадцать седьмой УК, за исключением преступления, предусмотренного статьей 304 УК);

Б) компьютерные коды или аналогичные данные, посредством которых можно получить доступ к компьютерной системе в целом или к её части с намерением использовать их для совершения любого из уголовных преступлений против безопасности компьютерных данных (любого уголовного преступления, предусмотренного главой двадцать седьмой УК, за исключением преступления, предусмотренного статьей 304 УК). Данное правонарушение карается лишением свободы на срок от шести месяцев до трёх лет. Также данная статья предусматривает более мягкую форму преступления, когда оно совершается лицом, обладающим любым из вышеуказанных средств, с намерением использовать их в целях совершения любого из уголовных преступлений, указанных в статьях 298–303 УК.

Общая часть УК также содержит положения, имеющие отношение к этим уголовным преступлениям. Так, например, установлено, что такое компьютерные данные, компьютерная сеть, компьютерная, компьютерный вирус (ст. 112 УК).

Учитывая, что уголовные преступления в этой сфере трудно обнаружить и доказать, в Республике Сербии принят специальный закон. Это Закон «Об организации и компетенции государственных органов по борьбе с преступлениями в сфере высоких технологий»[4]. **Настоящий Закон применяется в целях выявления, преследования и вынесения судебного решения по следующим предметам:**

1) уголовные преступления против безопасности компьютерных данных, предусмотренные УК;

2) преступные деяния против интеллектуальной собственности, имущества, экономики и правового оборота, в которых компьютеры, компьютерные системы, компьютерные сети и компьютерные данные, а также их продукты в материальной или электронной форме выступают в качестве объектов или средств совершения преступных деяний, если тираж произведений, охраняемых авторским правом, превышает 2000 экземпляров или причиненный материальный ущерб превышает 1000 000 сербских динаров;

3) преступные деяния против свобод и прав человека и гражданина, половой свободы, общественного порядка и мира, конституционного строя и безопасности Республики Сербии, которые по способу совершения или использованным средствам

[4] Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, "Службени гласник РС", бр. 61 од 18. јула 2005, 104 од 16. децембра 2009, 10 од 9. фебруара 2023, 10 од 9. фебруара 2023 – др. закон.

могут считаться преступлениями с использованием высоких технологий в соответствии с пунктом 1 статьи 2 настоящего Закона.

Таким образом, хотя УК предусматривает уголовные преступления против безопасности компьютерных данных в рассмотренной выше главе, преступления в сфере высоких технологий также включают в себя и другие уголовные преступления[5]. Данный закон также предусматривает специализацию государственных органов по данным уголовным преступлениям, а именно полиции, прокуратуры и судов. Во-первых, при Высшей прокуратуре Белграда создан специальный отдел по борьбе с преступлениями в сфере высоких технологий. Во-вторых, в целях реализации задач органов внутренних дел по борьбе с указанными преступными деяниями в структуре министерства внутренних дел создана служба по борьбе с преступлениями в сфере высоких технологий. В-третьих, Верховный суд в Белграде на территории Республики Сербии наделен полномочием рассматривать дела об этих уголовных преступлениях.

По официальным данным, число подобных преступлений растет. Например, в период с 1 января 2013 года по 31 декабря 2017 года Специальной прокуратурой по преступлениям в сфере высоких технологий были предъявлены уголовные обвинения в отношении 1318 взрослых, а обвинительные заключения были предъявлены в отношении 280 взрослых[6]. Существует очевидная разница между предъявлением и прекращением уголовных обвинений, что, возможно, подтверждает идею о том, что собрать достаточные доказательства для судебного преследования непросто.

Следует также отметить, что в Республике Сербии действует Закон об информационной безопасности[7]. Настоящий закон регулирует меры защиты от рисков безопасности в информационно-коммуникационных системах, обязанности юридических лиц при управлении и использовании информационно-коммуникационных систем, а также определяет компетентные органы по реализации мер защиты, координации деятельности субъектов защиты и контролю за надлежащим выполнением предписанных мер защиты.

В какой-то степени мы можем согласится с тем, что нельзя отрицать, что Республика Сербия имеет солидную правовую базу для борьбы с компьютерной преступностью. Однако необходимо продолжить работу над поправками к нормативным актам, которые должны идти в ногу с достижениями в области информационных технологий.

Список источников

1. Закон о информационој безбедности (рус. Закон об информационной безопасности), "Службени гласник РС", бр. 6 од 28. јануара 2016, 94 од 19. октобра 2017, 77 од 31. октобра 2019.

2. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала (рус. Закон об организации и полномочиях государственного органа по борьбе с криминалом в области высоких технологий), "Службени гласник РС", бр. 61 од 18. јула 2005, 104 од 16. децембра 2009, 10 од 9. фебруара 2023, 10 од 9. фебруара 2023 – др. закон.

3. Јовашевић Д. Рачунарска превара (међународни стандарди и право Републике Србије) (рус. Компьютерное мошейничестов (междунароные стандарты и право Республики Сербия)) // Годишњак факултета правних наука. 2024. № 14. С. 115–129.

4. Кривични законик (рус. Уголовный кодекс), “Службени гласник РС“, бр. 85 од 6. октобра 2005, 88 од 14. октобра 2005 – исправка, 107 од 2. децембра 2005 - исправка, 72 од 3. септембра 2009, 111 од 29. децембра 2009, 121 од 24. децембра 2012,

[5] В этой связи наука указывает на проблемы деяний, попадающих в сферу компьютерной преступности. Об этом см. Я. Н. Мосечкин, Понятие преступлений против безопасности цифровой информации, LEX RUSSICA, Том 76, № 5 (198), май 2023 г., с. 49–59.

[6] Источник: Стратегија за борбу против високотехнолошког криминала за период 2019–2023. године, "Службени гласник РС", број 71 од 25. септембра 2018.

[7] Закон о информационој безбедности, "Службени гласник РС", бр. 6 од 28. јануара 2016, 94 од 19. октобра 2017, 77 од 31. октобра 2019.

104 од 27. новембра 2013, 108 од 10. октобра 2014, 94 од 24. новембра 2016, 35 од 21. маја 2019, 94 од 28. новембра 2024.

5. Мосечкин И.Н. Понятие преступлений против безопасности цифровой информации // Lex Russica (Русский закон). 2023. Т. 76, № 5(198). С. 49-59.

6. Стратегија за борбу против високотехнолошког криминала за период 2019–2023. године (рус. Стратегия борьбы с криминалом в области высоких технологий на 2019-2023 гг.), "Службени гласник РС", број 71 од 25. септембра 2018.

References

1. Zakon o informacionoj bezbednosti (англ. Law on Information Security), "Sluzhbeni glasnik RS", br. 6 od 28. januara 2016, 94 od 19. oktobra 2017, 77 od 31. oktobra 2019.

2. Zakon o organizaciji i nadlezhnosti drzhavnih organa za borbu protiv visokotekhnoloshkog kriminala (англ. Law on the organization and powers of the state body for combating crime in the field of high technologies), "Sluzhbeni glasnik RS", br. 61 od 18. jula 2005, 104 od 16. decembra 2009, 10 od 9. februara 2023, 10 od 9. februara 2023 – dr. zakon.

3. Jovasheviћ D. Rachunarska prevara (meђunarodni standardi i pravo Republike Srbije) (англ. Computer fraud (international standards and law of the Republic of Serbia)) // Godishnjak fakulteta pravnih nauka. 2024. № 14. S. 115-129.

4. Krivichni zakonik (англ. Criminal Code), "Sluzhbeni glasnik RS", br. 85 od 6. oktobra 2005, 88 od 14. oktobra 2005 - ispravka, 107 od 2. decembra 2005 - ispravka, 72 od 3. septembra 2009, 111 od 29. decembra 2009, 121 od 24. decembra 2012, 104 od 27. novembra 2013, 108 od 10. oktobra 2014, 94 od 24. novembra 2016, 35 od 21. maja 2019, 94 od 28. novembra 2024.

5. Mosechkin I. N. Ponyatie prestuplenij protiv bezopasnosti cifrovoj informacii (англ. The Concept of Crimes against Digital Data Security) // Lex Russica (Russkij zakon). 2023. T. 76, № 5(198). S. 49-59.

6. Strategija za borbu protiv visokotekhnolo shkog kriminala za period 2019–2023. godine (англ. Strategy for Combating High-Tech Crime for 2019-2023), "Sluzhbeni glasnik RS", broj 71 od 25. septembra 2018.

Информация об авторе

И. Милич — доцент юридического факультета Университета Нови-Сада (Нови Сад) Республика Сербия, доктор юридических наук, доцент.

Information about the author

I. Milic — Associate Professor, Faculty of Law, University of Novi Sad (Novi Sad), Republic of Serbia, Doctor of Law, Associate Professor.

УДК: 341.4
ББК 67.911.15.

Использование информационных технологий иностранцами в целях совершения преступлений в России

Семен Алексеевич Поляков
Луганская академия Следственного комитета Российской Федерации, Луганск, Россия
Email: PROCK-ROCK@MAIL.RU

Аннотация. В статье поднимается тема правового обеспечения информационной безопасности от преступных посягательств мигрантов на уровне Российской Федерации (государственный характер), стран партнеров (региональный характер) и мира (международный характер). На сегодняшний день активно развиваются информационные технологии в каждой сфере жизнедеятельности современного человека, однако не все вопросы использования и пределов действия таких технологий урегулированы на всех уровнях нормативных правовых актов. Блокчейн технологии как способ анонимности, криптовалюта как средства легализации доходов полученных преступным путем, нейротехнологии как инструмент электронного мошенничества, электронные сигареты (вейп) как способ подрыва здоровье сотен тысяч наших подростков, а также искусственный интеллект на базе американского GPT чата-бота как универсальный помощник во всех законных и незаконных вопросах. Все указанные инструменты современного мира находятся в состоянии анархической свободы и отсутствия должного контроля со стороны законодателей и правоприменителей. Искусственный интеллект (далее – ИИ), изначально наделенный в своем названии человеческими свойствами, действительно может стать смертельной проблемой для будущего поколения. Проблема урегулирования границ законного применения указанных современных технологий заключается в том, что законодательство, как правило, развивается с определенным опозданием, разрешая те или иные вызовы современности по факту наступления определенных негативных последствий. В указанной статье совершена попытка взгляда в будущее России и мира, анализа зарождающихся проблем, связанных с использованием чата GPT, а также в целом информационных ресурсов, мессенжеров (WhatsApp, Telegram, Skype for Busines, Microsoft Teams, Discord, Snapchat, Threema, Viber, WeChat) и социальных сетей (Instagram, Facebook, Twitter, Google+, Pinterest, Tumblr) коллективного Запада. Между тем вопросы контроля передачи информации мигрантами через данные ресурсы, в период проведения специальной военной операции на Донбассе (далее – СВО) стоят объективно остро.

Ключевые слова: GPT, искусственный интеллект, нейротехнологии, мигранты из недружественных стран, обеспечение международной и национальной безопасности, патриотическое воспитание.
Научная специальность: 5.1.5 Международно-правовые науки
Для цитирования: Поляков С. А. Использование информационных технологий иностранцами в целях совершения преступлений в России // Мир криминалистики. 2025. № 1. С. 84-90

Use of information technologies by foreigners for the purpose of committing crimes in Russia

Semyon A. Polyakov
Lugansk Academy of the Investigative Committee of the Russian Federation, Lugansk, Russia
Email: PROCK-ROCK@MAIL.RU

Abstract. The article raises the issue of legal support for information security from criminal attacks of migrants at the level of the Russian Federation (state character), partner countries (regional character) and the world (international character). Today, information technologies are actively developing in every sphere of modern human activity, however, not all issues of the use and limits of such technologies are regulated at all levels of regulatory legal acts. Blockchain technologies as a way of anonymity, cryptocurrency as a means of legalizing income obtained by criminal means, neurotechnologies as a tool for electronic fraud, electronic cigarettes (vape) as a way to undermine the health of hundreds of thousands of our teenagers, as well as artificial intelligence based on the American GPT chat bot as a universal assistant in all legal and illegal matters. All these tools of the modern world are in a state of anarchic freedom and lack of proper control from legislators and law enforcement officers. Artificial intelligence (AI), initially endowed with human properties in its name, can really become a deadly problem for the future generation. The problem of regulating the boundaries of the legal use of these modern technologies is that legislation, as a rule, develops with a certain delay, resolving certain challenges of our time upon the occurrence of certain negative consequences. The article attempts to

look into the future of Russia and the world, analyze emerging problems associated with the use of the GPT chat, as well as information resources, messengers and social networks of the collective West. The issues of control over the transfer of information by migrants through these resources, not controlled by our country, during the special military operation in Donbass (SMO) are objectively acute.
Keywords: GPT, artificial intelligence, neurotechnology, migrants from unfriendly countries, ensuring international and national security, patriotic education.
For citation: Polyakov S. A. Use of information technologies by foreigners for the purpose of committing crimes in Russia // The world of criminology. 2025;(1): 84-90

Введение. Современный период XXI века характеризуется глобальными изменениями мирового порядка, мнимого или действительного раскола Европы и Соединенных Штатов Америки[1], перетасовкой сфер мирового влияния и многочисленными вооруженными конфликтами на территории Европы и Азии, борьбой за независимость и самоопределение народов, угнетенных прежним правовым положением. Одной из значительных неопределенностей указанного периода можно назвать ослабление действия международного права, неспособности многих ключевых международных организаций влиять на агрессоров и нарушителей норм международных договоров.

В отсутствие эффективных международных правоохранительных организаций современные вооруженные конфликты сопровождаются использованием информационных технологий в ущерб человечеству и неофициальными гибридными войнами, создающими угрозу не только национальной безопасности отдельного государства, но и глобальной безопасности.

Специальная военная операция России началась в период технологического прорыва, приведшего законодателей и общество в тупик по вопросам правового регулирования контроля и ответственности по вопросам ИИ, цифровой валюты (криптовалюты) и использования электронных средств общения и беспилотных летательных аппаратов (далее – БПЛА) с ИИ.

Злободневной проблемой России следует одновременно считать невежество, вредительство, непринятие законов и традиций России со стороны мигрантов, прибывших с целью обогащения, а также собирания информации и данных.

Амплитуда нарушений таких иностранцев варьируется от правонарушений общественного порядка до совершения убийств, шпионажа и собирания биологических данных для ведения биологической войны против Российской Федерации.

Основная часть. Миграционное законодательство России в настоящее время находится на этапе глобального реформирования в связи с возникшими угрозами безопасности государства и защиты коренного населения Отчизны. В частности, сокращаются сроки пребывания иностранцев в России. С 1 января 2025 года максимальный срок временного пребывания без визы – 90 дней в течение года. С 5 февраля 2025 года предусмотрена высылка иностранных граждан, находящихся в России незаконно: выдворяются иностранцы по новым правилам по решению полиции, а не судебных органов. Одновременно ограничиваются сроки для постановки иностранного гражданина на миграционный учет по месту пребывания[2].

[1] Боррель сравнил кризис в отношениях США и ЕС с несогласованным разводом // Ria.ru. URL: https://ria.ru/20250219/borrel-2000304450.html (дата обращения 19.02.2025).

[2] Федеральный закон от 8 августа 2024 г. № 260-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (с изменениями и дополнениями); Указ Президента РФ от 30 декабря 2024 г. № 1126 «О временных мерах по урегулированию правового положения отдельных категорий иностранных граждан и лиц без гражданства в Российской Федерации в связи с применением режима высылки»; Федеральный закон от 8 августа 2024 г. № 248-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // СПС Гарант.

Многолетняя открытая миграционная политика в России, навеянная западными идеалами, привела к перенасыщению территории Российской Федерации иностранцами, в том числе из недружественных стран[3], которые в большинстве своем и не собирались нести какую-либо пользу нашему обществу, не желали изучать русский язык и культуру нашего народа.

В последние годы на территории Российской Федерации формируются большие социальные группы, состоящие из мигрантов, не желающих интегрироваться в российское общество, предпочитающих обособленное, компактное проживание в местах массовой резидентной концентрации – анклавах. Большое скопление на определенных территориях лиц, отличающихся от большинства российских граждан культурой, образом жизни и менталитетом, несет угрозу стабильности государства и общества, негативно влияет на социально-экономическое развитие страны и повышает уровень социальной напряженности[4].

При этом 80% таких лиц указывают недостоверную причину приезда в Россию[5], так как проживают на её территории из корыстных соображений, а также ради привлечения прибыли с целью отправки полученных (законно или незаконно) в Российской Федерации денежных средств и информации себе на родину.

Достаточно обратиться к современной статистике преступлений, совершаемых мигрантами в России, чтобы понять реальную криминогенную обстановку в стране. За 8 месяцев 2024 года иностранцы совершили более 26 тысяч преступлений, при том, что в России в настоящее время насчитывается не более 3,5 миллионов мигрантов[6].

В ходе проведенного анализа приговоров и возбужденных уголовных дел установлено, что лишь за первое полугодие 2024 года в России осуждено 70 человек за государственную измену и шпионаж в интересах коллективного Запада.

Иностранные граждане недружественных России стран активно участвуют в гибридной войне коллективного Запада против Российской Федерации, собирая сведения и отправляя их анонимно с помощью информационных технологий.

Уголовные дела о шпионаже в большинстве случаев связаны с конфиденциальным сотрудничеством сограждан и мигрантов с иностранной разведкой, включая передачу данных о фактах попадания военных снарядов ВСУ в объекты инфраструктуры, степени поражения таких объектов, прохождения и численности военной техники Вооруженных сил РФ, а также иные сведения, относящиеся к секретной информации. В сравнении с 2023 годом фиксируется значительный рост таких преступлений.

Одним из средств гибридной войны является GPT чат, с помощью которого американские разработчики пытаются создать «пятую колонну», революционные экстремистские ячейки на территории Российской Федерации.

GPT чат (Generative Pre-trained Transformer), владельцем которого является американская научно-исследовательская организация OpenAI LP, активно продвигает свою продукцию на мировом рынке информационных технологий. Средний годовой доход OpenAI LP составляет около 3,2 миллиарда американских долларов[7].

---

[3] Распоряжением Правительства РФ от 5 марта 2022 года № 430-р «Об утверждении перечня иностранных государств и территорий, совершающих в отношении РФ, российских юридических лиц и физических лиц недружественные действия» // СПС Гарант.

[4] Жубрин Р.В., Ашиткова Т.В. Противодействие созданию в Российской Федерации мест массового проживания иностранных граждан (анклавов). Вестник Университета прокуратуры Российской Федерации. 2024. № 2 (100). С. 53.

[5] Бастрыкин А.И. Противодействие преступности мигрантов – один из основных факторов укрепления безопасности России. Право и безопасность. 2009. № 2. С. 31.

[6] Иностранцы в России за восемь месяцев 2024 года совершили более 26 тыс. преступлений // Официальный сайт Следственного комитата Российской Федерации. URL: https://sledcom.ru/press/smi/item/1918181 (дата обращения 19.02.2025).

[7] OpenAI Doubles Annualized Revenue to $3.4 Billion, The Information Reports // Bloomberg L.P. URL: https://www.bloomberg.com/news/articles/2024-06-12/openai-doubles-annualized-revenue-to-3-4-billion-information (дата обращения 19.02.2025).

Работа ИИ GPT строится на обязательном соблюдении законодательства США, а также на корпоративных правилах компании.

Библиотека и автоматизированная отработка алгоритмов поиска ответов полностью зависят от разработчиков, в том числе от их политики предпочтений и проводимой цензуры, избирательного применения критериев «языка ненависти» и др. Технические задания утверждаются в соответствии с интересами собственника, инвесторов сервиса и государства, резидентами которого они являются, в том числе «групп влияния». Компания OpenAI, разработчик ChatGPT, базируется в США, как и один из крупнейших инвесторов и партнёров проекта – компания Microsoft[8].

В ходе анализа имеющейся открытой информации выяснилось, что российская платформа YandexGPT 4 Pro непосредственно связана с GPT: для некоторых типов задач она обращается к схожим источникам с GPT-4o той же американской компании.

В связи с этим возникает необходимость вести разработки российского искусственного интеллекта под строгим государственным контролем для обеспечения более эффективного расследования преступлений, совершенных иностранными гражданами.

Для выявления фактов незаконной передачи данных, совершенных мигрантами из недружественных стран коллективного Запада, а также в целях обеспечения информационной безопасности требуется совершенствование криминалистической техники при проведении поиска и анализа цифровых следов с учетом современных технологий, разработанных совместно со странами, находящимися в партнерских отношениях с Российской Федерацией.

Разработка и внедрение технологий ИИ в криминалистическую деятельность должна осуществляться под общим научным руководством или при активном участии ученых-криминалистов. Однако техническая реализация любого такого проекта требует привлечения специалистов в области программирования, компьютерной техники и коммуникаций[9].

Несмотря на рост преступлений против общественной и государственной безопасности в период проведения СВО, совершенных иностранными гражданами, на территории России продолжают проживать граждане недружественных стран, осуществляя трудовую деятельность, фотографируя, снимая на видео, пересылая файлы и конвертируя российскую валюту в криптовалюту или в иностранные денежные единицы.

Граждане указанных недружественных стран обладают рядом причин и мотивов для помощи своему родному государству и совершения преступлений против государственной власти и общества России, а проведение в отношении них следственных действий проблематично в связи с латентностью преступлений и использованием мигрантами электронных и обезличенных способов связи.

Особую опасность для России представляют граждане стран коллективного Запада: трудоспособные, обладающие хорошей физической подготовкой, знанием боевых искусств, с высшим образованием, прибывшие в Россию для осуществления интеллектуальной трудовой деятельности в сфере IT, финансов, экономики, образования, культуры и других социально значимых сферах.

Заключение. Западная идеология, привитая нашему обществу с конца 80-х годов, достигла своего апогея в начале XXI века и вылилась в открытую пропаганду ЛГБТ-отношений, childfree, смещение моральных ценностей в сторону максимального извлечения прибыли, а также уменьшение важности Родины, героев

[8] Былевский П.Г. Культурологическая деконструкция социально-культурных угроз ChatGPT информационной безопасности российских граждан // Философия и культура. 2023. № 8. С. 46–56. DOI: 10.7256/2454-0757.2023.8.43909 EDN: UZDRFW URL: https://nbpublish.com/library_read_article.php?id=43909.

[8] Головин А.Ю. Технологии искусственного интеллекта в криминалистике: задачи, которые необходимо решить. Сибирские уголовно-процессуальные и криминалистические чтения. 2024. № 2 (44). С. 30.

Великой Отечественной войны, выдающихся личностей СССР и Российской империи. Свое истинное лицо показали известные российские артисты, которые уже признаны иностранными агентами и, как правило, сегодня проживают в странах коллективного Запада.

Таким образом, следует продолжить возрождение советских (российских) традиций, развитие патриотического воспитания, института традиционных семейных ценностей и принять ошибки 00-х в части организации прозападного образовательного процесса, культурных ориентиров на коллективный Запад в жизни молодого поколения нашей страны и не допустить обратного эффекта.

Также необходимо унифицировать обширный перечень международных договоров, ратифицированных РФ[10], обеспечить эффективный миграционный контроль и взаимодействие, а также не допускать визиты иностранцев, находящихся под следствием или в розыске по уголовным делам. Активную позицию в развитии указанного положения должна занимать Генеральная прокуратура Российской Федерации, ответственная за вопросы выдачи лиц для уголовного преследования или исполнения приговора в отношении иностранцев. Для реализации указанных целей необходимо, наряду с соглашением для стран БРИКС о возврате преступных доходов[11], заключить соглашение о формировании базы данных лиц, отнесенных к иностранным агентам, подозреваемых в шпионаже и прочих потенциально опасных мигрантов для государственного строя и общества.

Совместно с государствами-партнерами разработать независимую систему ИИ, не связанную с GPT OpenAI LP для криминалистических исследований в сфере поиска и анализа цифровых следов мигрантов из недружественных стран. В том числе - в части отслеживания возможной передачи мигрантами данных в виде фото- и видеофиксации результатов атак БПЛА по объектам гражданской и военной инфраструктуры российских городов, совершаемых в интересах коллективного Запада и Украины.

Целесообразно признание правового статуса и пределов свободы самостоятельных действий ИИ на международном уровне и обеспечение национальной безопасности в России, а также в мире от его будущих преступных посягательств во II, и особенно в III и IV четвертях XXI века.

Список источников

1. Федеральный закон от 8 августа 2024 г. № 260-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (с изменениями и дополнениями) // СПС Гарант.

2. Федеральный закон от 8 августа 2024 г. № 248-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // СПС Гарант.

3. Указ Президента РФ от 30 декабря 2024 г. № 1126 «О временных мерах по урегулированию правового положения отдельных категорий иностранных граждан и лиц без гражданства в Российской Федерации в связи с применением режима высылки» // СПС Гарант.

4. Распоряжением Правительства РФ от 5 марта 2022 года № 430-р «Об утверждении перечня иностранных государств и территорий, совершающих в отношении РФ, российских юридических лиц и физических лиц недружественные действия» // СПС Гарант.

5. Бастрыкин А.И. Противодействие преступности мигрантов – один из основных факторов укрепления безопасности России // Право и безопасность. – 2009. – № 2. – С. 30–34.

[10] Перечень международных договоров Российской Федерации по вопросам правовой помощи, выдачи и передаче лиц, осужденных к лишению свободы – Официальный сайт Министерства юстиции Российской Федерации [Электронный ресурс] URL: https://minjust.gov.ru/ru/pages/perechen-mezhdunarodnyh/ (дата обращения 19.02.2025).

[10] Генеральная прокуратура России подготовила проект соглашения БРИКС о возврате нелегальных активов. // ТАСС. ру. URL: https://tass.ru/ekonomika/22172783?ysclid=m6qf43w6p9666083831 (дата обращения 19.02.2025).

6. Былевский П.Г. Культурологическая деконструкция социально - культурных угроз ChatGPT информационной безопасности российских граждан // Философия и культура. – 2023. – № 8. – С. 46–56.

7. Головин А.Ю. Технологии искусственного интеллекта в криминалистике: задачи, которые необходимо решить // Сибирские уголовно-процессуальные и криминалистические чтения. – 2024. – № 2 (44). – С. 25–33.

8. Жубрин Р.В., Ашиткова Т.В. Противодействие созданию в Российской Федерации мест массового проживания иностранных граждан (анклавов) // Вестник Университета прокуратуры Российской Федерации. – 2024. – № 2 (100). – С. 53–60.

9. Боррель сравнил кризис в отношениях США и ЕС с несогласованным разводом // Ria.ru. URL: https://ria.ru/20250219/borrel-2000304450.html (дата обращения 19.02.2025).

10. Генеральная прокуратура России подготовила проект соглашения БРИКС о возврате нелегальных активов // ТАСС. ру. URL: https://tass.ru/ekonomika/22172783?ysclid= m6qf43w6p9666083831 (дата обращения 19.02.2025).

11. Иностранцы в России за восемь месяцев 2024 года совершили более 26 тыс. преступлений // Официальный сайт Следственного комитата Российской Федерации. URL: https://sledcom.ru/ press/smi/item/ 1918181.

12. Перечень международных договоров Российской Федерации по вопросам правовой помощи, выдачи и передаче лиц, осужденных к лишению свободы // Официальный сайт Министерства юстиции Российской Федерации. URL: https://minjust.gov.ru/ru/pages/ perechen-mezhdunarodnyh/.

13. OpenAI Doubles Annualized Revenue to $3.4 Billion, The Information Reports // Bloomberg L.P. URL: https://www.bloomberg.com/news/articles/2024-06-12/openai-doubles-annualized-revenue-to-3-4-billion-information (дата обращения 19.02.2025).

References

1. Federal Law of August 8, 2024 No. 260-FZ "On Amendments to Certain Legislative Acts of the Russian Federation" (with amendments and additions) // SPS Garant.

2. Federal Law of August 8, 2024 No. 248-FZ "On Amendments to the Code of the Russian Federation on Administrative Offenses" // SPS Garant.

3. Decree of the President of the Russian Federation of December 30, 2024 No. 1126 "On temporary measures to regulate the legal status of certain categories of foreign citizens and stateless persons in the Russian Federation in connection with the application of the expulsion regime" // SPS Garant.

4. Order of the Government of the Russian Federation of March 5, 2022 No. 430-r "On approval of the list of foreign states and territories committing unfriendly actions against the Russian Federation, Russian legal entities and individuals" // SPS Garant.

5. Bastrykin A.I. Combating migrant crime is one of the main factors in strengthening Russia's security. Law and Security. 2009. No. 2. P. 30–34.

6. Bylevsky P.G. Cultural deconstruction of socio-cultural threats ChatGPT information security of Russian citizens // Philosophy and Culture. 2023. No. 8. P. 46–56.

7. Golovin A.Yu. Artificial intelligence technologies in forensics: problems that need to be solved. Siberian criminal procedure and forensic readings. 2024. No. 2 (44). P. 25–33.

8. Zhubrin R.V., Ashitkova T.V. Counteracting the creation of places of mass residence of foreign citizens (enclaves) in the Russian Federation. Bulletin of the University of the Prosecutor's Office of the Russian Federation. 2024. No. 2 (100). P. 53–60.

9. Borrell compared the crisis in US-EU relations to an uncoordinated divorce // Ria.ru. URL: https://ria.ru/20250219/ borrel-2000304450.html. (accessed: 19.02.2025).

10. The Russian Prosecutor General's Office has prepared a draft BRICS agreement on the return of illegal assets // TASS.ru. URL: https://tass.ru/ekonomika/22172783 ?ysclid= m6qf43w6p9666083831 (accessed: 19.02.2025).

11. Foreigners in Russia committed more than 26 thousand crimes in eight months of 2024 // Official website of the Investigative

Committee of the Russian Federation. URL: https://sledcom.ru/press/smi/item/1918181.

12. List of international treaties of the Russian Federation on legal assistance, extradition and transfer of persons sentenced to imprisonment // Official website of the Ministry of Justice of the Russian Federation. URL: https://minjust.gov.ru/ru/pages/perechen-mezhdunarodnyh.

13. OpenAI Doubles Annualized Revenue to $3.4 Billion, The Information Reports // Bloomberg L.P. URL: https://www.bloomberg.com/news/articles/2024-06-12/openai-doubles-annualized-revenue-to-3-4-billion-information (accessed: 19.02.2025).

Информация об авторе

С. А. Поляков — исполняющий обязанности заведующего кафедрой уголовного права, криминологии и уголовного процесса Луганской академии Следственного комитета Российской Федерации, кандидат юридических наук, подполковник юстиции.

Information about the author

S. A. Polyakov – Acting Head of the Department of Criminal Law, Criminology and Criminal Procedure of the Lugansk Academy of the Investigative Committee of the Russian Federation, Candidate of Law, Lieutenant Colonel of Justice.

УДК 343.2/.7
ББК 67.408.

Социогуманитарные вызовы цифровизации для уголовно-правовых наук

Александр Николаевич Савенков
Институт государства и права Российской академии наук, Москва, Россия
Email: director@igpran.ru

Аннотация. В статье дается анализ влияния экономических факторов и условий, роли промышленных и научно-технологических укладов, а также их существенных элементов. Подчеркивается важность совершенствования междисциплинарных подходов и исследований в русле взаимодействия права и экономики, которые ориентируются на изучение ключевых моментов развития современной политико-правовой и экономической мысли. Наличие существенных пробелов в понимании более глубоких и интенсивных связей и форм взаимодействия между правом, в том числе уголовным, и экономикой рассматривается как одно из условий, устранением которого может быть обеспечено качественно новое и значительно более эффективное развитие как правовых исследований, так и расширение познавательных горизонтов экономических работ, особенно фокусирующихся на вопросах взаимодействия с политикой и правом.
Ключевые слова: научно-технологический уклад, экономический анализ права, криминальные риски и угрозы, цифровизация, искусственный интеллект, социогуманитарные вызовы.
Научная специальность: 5.1.4. Уголовно-правовые науки
Для цитирования: Савенков А.Н. Социогуманитарные вызовы цифровизации для уголовно-правовых наук // Мир криминалистики. 2025. № 1. С. 91-99

Socio-humanitarian challenges of digitalization for criminal law sciences

Aleksandr N. Savenkov
The Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia
Email: director@igpran.ru

Abstract. The article analyzes the influence of economic factors and conditions, the role of industrial, scientific and technological structures, and their essential elements. The importance of improving interdisciplinary approaches and research in the context of the interaction of law and economics, which focus on the study of key aspects of the development of modern political, legal and economic thought, is emphasized. The presence of significant gaps in understanding the deeper and more intense connections and forms of interaction between law, including criminal law, and economics is considered as one of the conditions that can be eliminated to ensure a qualitatively new and much more effective development of both legal research and the expansion of the cognitive horizons of economic work, especially focusing on issues of interaction with politics and the right.
Keywords: scientific and technological structure, state building, economic analysis of law, criminal risks and threats, digitalization, artificial intelligence, socio-humanitarian challenges.
For citation: Savenkov A.N. Socio-humanitarian challenges of digitalization for criminal law sciences // The world of criminology. 2025;(1): 91-99

Стремительный темп изменений, связанных с новыми технологиями, становится главным фактором доминирования непредсказуемости, а значит, и опасности случайного выбора траектории развития. Современные достижения науки предоставляют фантастические возможности и меняют картину реальности. Так, интеллектуальные средства дешифрования делают открытыми любые средства коммуникаций. Потеря контроля над спутниками и электромагнитным спектром

существенно влияет на возможности их специального применения. Летальные автономные системы оружия бросают вызов давним этическим и правовым нормам. Разработка метода редактирования генома CRISPR-Cas9 была отмечена Нобелевской премией по химии за 2020 г., присужденной Эммануэль Шарпантье и Дженнифер Дудна. Однако еще на этапе разработки в 2015 г. данный метод попал в список угроз национальной безопасности.

В юридических науках результаты научно-технического прогресса в целом, а также сопряженные с этим технологические угрозы и социогуманитарные вызовы, осмысливаются пока фрагментарно, как набор частных проблем отдельных отраслевых наук, которые скорее стремятся адаптироваться к темпам изменений и предложить общее включение в обсуждение вопросов[1]. Например, в регулировании искусственного интеллекта[2] в Западной Европе и США наблюдаются в основном рамочные решения, которые скорее декларируют готовность отвечать на имеющиеся вызовы, но сами решения пока вырабатываются явно с трудом. В частности, Европейский парламент принял Закон об искусственном интеллекте[3] – первую в мире всеобъемлющую правовую базу в области ИИ и масштабный пакет мер, направленный на защиту потребителей от потенциально опасных применений искусственного интеллекта. Чиновники предприняли этот шаг на фоне опасений, что недавние достижения в области технологий могут быть использованы в неблаговидных целях, которые могут привести к слежке, дискриминации, управляемой алгоритмами, и распространению дезинформации. С одной стороны, декларируется содействие внедрению искусственного интеллекта, ориентированного на человека и заслуживающего доверия, а также обеспечение высокого уровня защиты здоровья, безопасности, основных прав, демократии и верховенства права, окружающей среды от вредного воздействия систем искусственного интеллекта при одновременном поощрении инноваций и улучшении функционирования единого рынка. С другой – этот Закон используется в идеологических целях, поскольку отдельным странам ЕС рекомендуется не принимать самостоятельных актов, что могло бы привести к фрагментации единого рынка и подорвать правовую определенность участников, разрабатывающих или использующих системы ИИ. При этом в США возможность принятия такого закона по-прежнему остаётся на стадии обсуждения.

Необходимость применения норм международного права, включая Устав ООН и гуманитарные законы, а также законы о правах человека, к автономным системам вооружений была провозглашена в резолюции Генеральной Ассамблеи ООН 78/241[4], принятой 22 декабря 2023 года 152 голосами «за», четырьмя голосами «против» и 11 голосами воздержавшихся. В ней признаются потенциальные преимущества новых технологий, а также выражается обеспокоенность по поводу связанных с ними гуманитарных, правовых, технологических и этических проблем. В резолюции выражена важность поиска различных точек зрения на смертоносные автономные системы вооружений со стороны государств-членов, наблюдателей, международных организаций, гражданского общества и промышленности.

Лидеры КНР и США Си Цзиньпин и Джо Байден 16 ноября 2024 года в ходе встречи на полях саммита Азиатско-Тихоокеанского экономического сотрудничества (АТЭС) в Лиме вновь устно договорились о том, что решения о применении теперь уже ядерного оружия должны

1 Подробно о вызовах, связанных с новым промышленным укладом, см.: Савенков А.Н. Новый технологический уклад и социогуманитарные вызовы // Государство и право. 2025. № 1. С. 14–37; Савенков А.Н. Философия права и становление российского государства-цивилизации: Монография. М.: Наука, 2024. – 739 с.

2 Далее – ИИ.

3 Regulation (eu) 2024/1689 of the european parliament and of the council of 13 June 2024. URL: https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=OJ:L_20241689 (дата обращения: 10.12.2024).

4 Резолюция, принятая Генеральной Ассамблеей 22 декабря 2023 года. URL: https://docs.un.org/ru/A/RES/78/241 (дата обращения: 11.12.2024).

оставаться за человеком, а не искусственным интеллектом[5].

Резолюция Генеральной Ассамблеи ООН 78/265 от 11 марта 2024 г. «Использование возможностей безопасных, защищенных и заслуживающих доверия систем искусственного интеллекта для устойчивого развития»[6] также призывает «разрабатывать и поддерживать нормативные правовые и организационно-управленческие подходы и рамки, относящиеся к системам искусственного интеллекта и создающие благоприятную экосистему на всех уровнях». Эта резолюция призвана содействовать разработке, внедрению и раскрытию механизмов мониторинга рисков и управления ими, механизмов защиты данных, включая защиту персональных данных и политику конфиденциальности, а также, в соответствующих случаях, оценки воздействия на протяжении всего жизненного цикла систем искусственного интеллекта. Предложение о ее принятии было инициировано Соединенными Штатами Америки и получило поддержку Китая и 121 страны. Инициатива объединяет ряд усилий правительств всего мира по влиянию на траекторию развития ИИ после запуска ChatGPT и GPT-4.

Новое соглашение ООН, возможно, является первым «глобальным» соглашением, однако оно было не первым межгосударственным актом в данной сфере. Так, за последние десятилетия были подписаны важные документы в рамках БРИКС. 23 августа 2023 г. Председатель КНР Си Цзиньпин призвал сформировать общую структуру управления ИИ в рамках БРИКС. В настоящий момент нет официальных подробностей по структуре и функциям новой рабочей группы БРИКС, тем не менее работа по институционализации такого сотрудничества продолжается уже больше восьми лет. В 2021 г. по поручению Президента РФ велась работа по разработке декларации сотрудничества стран БРИКС в сфере ИИ для вынесения данного вопроса в повестку дня саммита стран данного объединения в 2021–2022 гг.

Разработка этических документов по правилам применения ИИ является ключевым трендом их регулирования. Одним из первых таких документов стал акт, разработанный А. Незнамовым и В. Наумовым (сотрудником Института государства и права РАН) – «Модельная конвенция о робототехнике и искусственном интеллекте. Правила создания и использования роботов и искусственного интеллекта»[7].

На Саммите будущего, который проходил в Нью-Йорке 22–23 сентября 2024 г., как одно из приложений к Пакту будущего государства, члены ООН приняли Глобальный цифровой договор (ГЦД)[8], который уравнивает роль государств, гражданского общества и бизнеса, а также акцентирует правочеловеческий и гендерный нарратив в западной трактовке, прежде всего, усиливает глобальный Север, который лидирует в указанных областях. В поддержку Глобального цифрового договора проголосовало 143 государства. В настоящее время техническое управление инфраструктурой Интернета осуществляет зарегистрированная в США дочерняя структура ICANN Public Technical Identifiers (PTI), что дает Вашингтону возможность влиять на значимые политические и экономические решения, связанные с управлением Интернетом, а именно управлением системой

5 Джо Байден и Си Цзиньпин провели последнюю встречу // Ведомости. 2024. 18 нояб. URL: https://www.vedomosti.ru/politics/articles/2024/11/18/1075617-baiden-i-si-tszinpin-proveli-poslednyuyu-vstrechu (дата обращения: 11.12.2024).

6 Резолюция, принятая Генеральной Ассамблеей 21 марта 2024 года. URL: https://docs.un.org/ru/A/RES/78/265 (дата обращения: 11.12.2024).

7 Наумов В.Б., Незнамов А.В. Модельная конвенция о робототехнике и искусственном интеллекте. Правила создания и использования роботов и искусственного интеллекта // Право и информация: вопросы теории и практики. СПб., 2017. С. 210–220. Подробно по этой теме см. также: Комплексное исследование правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники / В.В. Архипов, Г.Г. Камалова, В.Б. Наумов, А.В. Незнамов. СПб., 2022. – 336 с.

8 Резолюция, принятая Генеральной Ассамблеей 22 сентября 2024 года. URL: https://docs.un.org/ru/A/RES/79/1 (дата обращения: 11.12.2024).

доменных имен и распределением блоков IP-адресов. Россия последовательно исходит из необходимости адаптировать ООН к современным реалиям многополярного мира, в том числе в цифровом пространстве. Для глобального Юга приоритетным представляется акцент на цифровом суверенитете и преодолении цифрового разрыва, борьбе с цифровым неоколониализмом и неоколониализмом данных, что позволит сделать цифровое пространство подлинно инклюзивным. Россия не поддержала Глобальный цифровой договор.

Глобальный цифровой договор затрагивает вопросы управления Интернетом, преодоления цифрового разрыва, выработки международных правил для платформ социальных сетей и регулирования искусственного интеллекта, а также ряд других смежных вопросов. Цифровое сотрудничество должно быть закреплено в правах человека и в международном праве. Правительства, технологические гиганты и соцсети должны сделать онлайн-пространство безопасным для всех, в том числе для детей, женщин и социально незащищенных групп. Именно в этом Российская Федерация видит ключевую роль данного документа.

В то же время мировая практика пока идет по иному пути. Помощь частных компаний украинской стороне в ходе конфликта с Россией говорит о наступлении новой эпохи в мировых войнах, где коммерческие компании (многие из которых американские), скорее всего, будут сами обеспечивать и защищать критически важную цифровую инфраструктуру. Ни одна из этих компаний не производит оружие, тем не менее они влияют на ситуацию на поле боя, поскольку взаимодействие Киева со Starlink Илона Маска обеспечивает украинским военным доступ к спутниковому интернету. Так, SpaceX потратила более 80 млн долл. на передачу и обслуживание терминалов Starlink; Microsoft помогла перенести правительственные данные в свои облачные системы хранения (такую же помощь оказала Amazon Web Services); Capella Space, HawkEye 360 и Maxar Technologies предоставляют сделанные из космоса снимки мест боевых действий[9].

При появлении новых модификаций ИИ, которые станут работать с фантастической скоростью, традиционные меры регулирования окажутся бесполезными. Для начала ИИ-моделям должно быть запрещено нарушать законы любого государственного образования. Ключевые особенности механизма взаимодействия между человеком и машиной должны быть абсолютно идеальными. Во-первых, нельзя обходить или же удалять защитный механизм.

Система управления должна обладать тремя ключевыми характеристиками: мощностью для обработки запросов в режиме реального времени, универсальностью для стабильной работы в любых условиях по всему миру, и гибкостью для постоянного обучения и адаптации. Наконец, нежелательное поведение компьютера (из-за случайных сбоев, непредвиденных системных взаимодействий или же преднамеренных неправомерных действий) необходимо не просто запрещать, но и полностью предотвращать[10].

Одно из решений – объявить вне закона любой разумный ИИ, который игнорирует человеческие ценности. Но опять же: что значит «человеческие ценности»? Достижение согласия по вопросу понимания того, какой смысл вкладывается в понятие ценностей, а также по вопросу, как именно ими следует оперировать на практике – это философская, дипломатическая и юридическая задача нашего века.

Можно говорить, что в целом жизнедеятельность человека радикально меняется под влиянием киберсреды. Социальные сети стали местом притяжения негатива,

9 Matt Kaplan and Michael Brown. The Private Sector on the Front Line. Big Tech and the Risky Blurring of Commercial and Security Interests. Foreign Affairs. January 31, 2025. URL: https://www.foreignaffairs.com/united-states/private-sector-front-line# (дата обращения: 11.12.2024).

10 Henry A. Kissinger, Eric Schmidt, and Craig Mundie. AI Can Save Humanity – Or End It. URL: https://www.theatlantic.com/ideas/archive/2024/11/ai-genesis-excerpt-kissinger-schmidt-mundie/680619/ (дата обращения: 30.11.2024).

лжи, дезинформации[11]. Такие понятия, как патриотизм, сотрудничество, развитие страны, духовно-нравственные ценности, задвигаются в информационной повестке, высмеиваются. Сознание людей деформируется информационными технологиями: возникают сложности с выбором правильных ориентиров, соотносящихся с морально-нравственными нормами общества и ценностными установками самой личности. Новым полем битвы становится когнитивная сфера, а новым конфликтом станет более масштабная борьба за власть и соревнование за когнитивное превосходство. Когнитивная война теперь рассматривается в НАТО как самостоятельный театр военных действий[12].

Современные технологии, сама глобальная информационно-коммуникационная инфраструктура, управляемая англосаксонскими бенефициарами, позволяют сегодня не просто осуществлять традиционное воздействие на массовое сознание, но, и агрессивно проникая через границы национальных информационных пространств, активно осуществлять сбор пользовательских данных, выступающих сегодня новым ресурсом цифрового надзорного капитализма для адаптации информационно-коммуникационной деятельности к особенностям отдельных групп населения государств и индивидов. Такого рода потенциал позволяет эффективно воздействовать на традиционное миропонимание и мировоззренческие системы, трансформируя и разрушая казавшиеся незыблемыми ценности, смыслы, символы, представления в интересах глобальных геополитических факторов. Применение технологий Big Data уже сегодня позволяет формировать индивидуальные мировоззренческие модели, порождая тем самым ценностно-смысловой конфликт на основе фрагментации мировоззрения среди различных групп населения стран-мишеней по принципу «разделяй и властвуй».

Юридическая наука в данных условиях пока не предлагает комплексного решения указанных проблем. Отечественные ученые-правоведы основной упор делают на исследование отдельных аспектов проявлений нового промышленного уклада: влиянии искусственного интеллекта на экономические и правовые процессы, внедрении новых технологий в промышленности и производстве, в сфере социальной и межличностной коммуникации, в политической практике[13]. В то же время серьезной угрозой национальной безопасности зачастую становятся криминальные проявления технологической формации, не получившие комплексного осмысления[14]. Так, за 2023 г. объем операций, совершенных без согласия граждан, составил 15,3 млрд руб. За девять месяцев 2024 г. аналогичный показатель уже достиг 17,8 млрд руб. При этом доля средств, возмещенных банками клиентам, пострадавшим от мошенничества, в третьем квартале составила лишь 11,9%, хотя это примерно вдвое выше уровня второго квартала (6,1%) и среднего значения за прошедший год (9,7%). Объем предотвращенных мошеннических операций увеличился более чем в два раза, до 4,9 трлн руб.

11 Савенков А. Н., Россинская Е. Р. Актуальные направления развития общей теории криминалистики сквозь призму современных технологий // Государство и право. 2024. № 10. С. 156–168.

12 Савенков А.Н. Историческое сознание как новый театр военных действий // Право в Вооруженных Силах – Военно-правовое обозрение. 2024. № 12 (329). С. 3–10.

13 См., например: Шестые Бачиловские чтения: Сборник статей участников Международной научно-практической конференции, Москва, 2–3 февраля 2023 года. М., 2023. – 256 с.; Полякова Т.А., Смирнов А.А. Правовые аспекты обеспечения информационной безопасности при использовании технологий искусственного интеллекта // Вестник Московского университета. Серия 26: Государственный аудит. 2024. № 3. С. 89–106; Полякова Т.А. Обеспечение национального суверенитета России в условиях развития наукоемких технологий: противодействие вызовам праву и угрозам информационной безопасности // Юридический вестник Дагестанского государственного университета. 2024. Т. 52. № 4. С. 157–165.

14 Информационные технологии в уголовно-правовой сфере: монография / О. Ю. Антонов, А. И. Бастрыкин, А. А. Бессонов [и др.]. М.: Юнити-Дана, 2023. – 279 с.

В 2024 г. Роскомнадзор зафиксировал 135 случаев распространения в Интернете баз данных, содержащих более 710 млн записей. В декабре прошлого года глава ведомства А. Липов сообщил, что совместная работа Роскомнадзора с операторами связи позволила сократить в шесть раз количество абонентов, имеющих более тысячи симок, и напомнил, что с 2025 г. россияне смогут оформить не более 20 сим-карт, иностранцы – не более 10. Он также отметил, что принятые в России новые меры ответственности будут побуждать компании серьезнее относиться к защите персональных данных[15].

Для сферы общественных наук перспективным и значимым представляется рассматривать происходящие изменения не как нечто само собой разумеющееся, а как процесс, который следует оценивать не в качестве результата, а в качестве средства и условия культурно-цивилизационного развития общества, реального инструмента обеспечения высоких и гарантированных стандартов благосостояния и социального благополучия. В настоящее же время ситуация в определенной степени развивается стихийно. Например, одна из высоких зарплат в нашей экономике сейчас у курьеров: 150 тыс. руб. в месяц предлагают населению компании – поставщики услуг. К ноябрю 2024 г. они получали больше врачей (88,4 тыс. руб.), учителей (47 тыс. руб.), а также IT-специалистов (114,2 тыс. руб.). Кроме того, по уровню оплаты труда доставщики превзошли менеджеров по логистике и ВЭД (79,5 тыс. руб.), дизайнеров (70 тыс. руб.), бухгалтеров (62,3 тыс. руб.) и журналистов (50,4 тыс. руб.). Директор департамента развития внутренней торговли Минпромторга Н. Кузнецов заявил, что сервисы доставки оттягивают из важных секторов экономики не менее 1,5 млн здоровых и физически сильных людей, при этом сами ничего не производят и убыточны. По его словам, они отучили «значительную часть потребителей от банального навыка просто ходить по магазинам»[16]. Глава сервиса по подбору сотрудников SuperJob Алексей Захаров считает, что «рынок труда у нас разбалансирован... Нужно менять налоговое законодательство, полностью закрыть тему самозанятости. Сейчас налоговые выгоды в сфере услуг при найме самозанятых – примерно 3 трлн руб. в год, возможно больше… То есть сфера услуг имеет такие налоговые преференции, которые IT-отрасли и не снились»[17].

В подобных условиях юридическая наука, как и другие общественные науки, должна быть готова к коренному изменению всей мировой системы, к необходимости базисных трансформаций. Сегодня нужна масштабная, комплексная разработка вопросов реального функционирования государства, его принципиальной роли в условиях новой научно-технологической архитектуры национальной и мировой систем.

Важным шагом в современных условиях является принятие международных актов, направленных на координацию усилий стран в парировании глобальных угроз. В августе 2024 г. специальный комитет ООН утвердил проект первой в истории всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях: «Проект конвенции Организации Объединенных Наций против киберпреступности. Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям». Уникальность конвенции определяется тем, что:

во-первых, это документ нового поколения, который учитывает актуальные

15 Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. III квартал 2024 года. 9 декабря 2024 года. Центральный банк России. // cbr.ru. URL: https://cbr.ru/statistics/ib/review_3q_2024/ (дата обращения: 30.11.2024).

16 URL: https://www.rbc.ru/society/06/12/2024/675258da9a79470b0302455 (дата обращения: 30.11.2024).

17 «У нас дефицит в 500 тыс. учителей. Зато пицца приезжает за 15 минут». Алексей Захаров о необходимости нового регулирования рынка труда // Коммерсантъ. 2024. № 232/П. URL: https://www.kommersant.ru/doc/7380789.

правовые вопросы информационной сферы, включая защиту персональных данных и сбор цифровых доказательств;

во-вторых, это первый в истории универсальный международный договор в области борьбы с информационной преступностью (Будапештскую конвенцию о киберпреступности 2001 г. Россия не подписала, как противоречащую интересам суверенных государств, п. 32b.);

в-третьих, в ней закреплен принцип государственного суверенитета, что отличает его от вышеназванной Будапештской конвенции 2001 г.;

в-четвертых, ею детально регламентирован порядок международного сотрудничества в сфере борьбы с информационной преступностью (включая киберпреступления, оказание взаимной правовой помощи по уголовным делам)[18].

Шаги в парировании новых социогуманитарных вызовов в Российской Федерации также предпринимаются. К основным нормативным актам в области обеспечения информационной безопасности России можно отнести Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[19], Доктрину информационной безопасности Российской Федерации[20] и Уголовный кодекс РФ. В России создана и успешно функционирует государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Развивается ведомственное правовое регулирование ФСБ и ФСТЭК России в сфере обеспечения безопасности критической информационной инфраструктуры. Постоянно совершенствуется законодательство в области защиты информации ограниченного доступа, включая федеральные законы «О государственной тайне»[21], «О коммерческой тайне»[22], «О персональных данных»[23] и другие. Принят Федеральный закон от 29 декабря 2022 г. № 572-ФЗ[24], регулирующий отношения, возникающие при осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных с использованием специализированной государственной информационной системы.

Вкладом в укрепление информационной безопасности Российской Федерации стало издание в 2022 г. Указа Президента России[25], которым на руководителей федеральных и региональных органов исполнительной власти, государственных корпораций (компаний), стратегических предприятий и иных организаций возложена персональная ответственность за обеспечение информационной безопасности. Указом предписано создание в каждом таком органе (организации) специализированного структурного подразделения, осуществляющего функции по обеспечению информационной безопасности, либо возложение данных функций на существующее структурное подразделение.

Одним из ключевых требований Указа является запрет на использование средств защиты информации, произведенных в недружественных иностранных государствах или компаниями, находящимися под их юрисдикцией. В 2024 г. этот запрет был распространен на иностранные сервисы (работы, услуги) по обеспечению информационной безопасности.

18 URL: https://d-russia.ru/wp-content/uploads/2024/03/v2403635.pdf (дата обращения: 20.01.2025).
19 СЗ РФ. 2006. № 31 (ч. 1). Ст. 3448.
20 Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.
21 Закон РФ от 21 июля 1993 г. № 5485-1 (ред. от 8 августа 2024 г.) «О государственной тайне» // СЗ РФ. 1997. № 41. Ст. 8220-8235.
22 Федеральный закон от 29 июля 2004 г. № 98-ФЗ (ред. от 8 августа 2024 г.) «О коммерческой тайне» // СЗ РФ. 2004. № 32. Ст. 3283.
23 Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 8 августа 2024 г.) «О персональных данных» // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.
24 Федеральный закон от 29 декабря 2022 г. № 572-ФЗ (ред. от 26 декабря 2024 г.) «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // СЗ РФ. 2023. № 1 (ч. 1). Ст. 19.
25 Указ Президента РФ от 1 мая 2022 г. № 250 (ред. от 13 июня 2024 г.) «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // СЗ РФ. 2022. № 18. Ст. 3058.

Таким образом, роль научно-технологических факторов в трансформации правового поля возрастает стремительно. Вместе с тем в современной юридической науке проблематика влияния промышленного и научно-технологического укладов изучается фрагментарно, новые комплексные модели минимизации рисков в правоведении отсутствуют. Юриспруденция в основном пытается поспеть за быстро меняющимися экономическими условиями и связанными с этим социально-экономическими вызовами. В юридической науке ещё только формируется полноценная и развернутая система теоретических взглядов на характер современной экономики и влияние происходящих в ее сфере изменений и темпов развития на право.

Сегодня особенно актуальна задача создания сбалансированной системы правовых норм и институтов, призванных отражать и развивать основы государственного строя, регулировать деятельность общественных и государственных институтов, их взаимодействие, полномочия и методы работы. Не менее важно изучение публично-правовых механизмов, определяющих права и обязанности граждан в их отношениях с государством и между собой.

Такой комплексный подход будет способствовать реализации конституционных целей развития государства и общества, укреплению суверенитета в условиях технологических и социогуманитарных изменений современности.

Список литературы

1. Henry A. Kissinger, Eric Schmidt, and Craig Mundie. AI Can Save Humanity – Or End It. URL: https://www.theatlantic.com/ideas/archive/2024/11/ai-genesis-excerpt-kissinger-schmidt-mundie/680619.

2. Matt Kaplan and Michael Brown. The Private Sector on the Front Line. Big Tech and the Risky Blurring of Commercial and Security Interests. Foreign Affairs. January 31, 2025. URL: https://www.foreignaffairs.com/united-states/private-sector-front-line#.

3. Информационные технологии в уголовно-правовой сфере: монография / О. Ю. Антонов, А. И. Бастрыкин, А. А. Бессонов [и др.]. М.: Юнити-Дана, 2023. 279 с.

4. Комплексное исследование правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники / В. В. Архипов, Г. Г. Камалова, В. Б. Наумов, А. В. Незнамов. СПб., 2022. 336 с.

5. Наумов В.Б., Незнамов А.В. Модельная конвенция о робототехнике и искусственном интеллекте. Правила создания и использования роботов и искусственного интеллекта // Право и информация: вопросы теории и практики. СПб., 2017. С. 210–220.

6. Полякова Т.А. Обеспечение национального суверенитета России в условиях развития наукоемких технологий: противодействие вызовам праву и угрозам информационной безопасности // Юридический вестник Дагестанского государственного университета. 2024. Т. 52. № 4. С. 157–165.

7. Полякова Т.А., Смирнов А.А. Правовые аспекты обеспечения информационной безопасности при использовании технологий искусственного интеллекта // Вестник Московского университета. Серия 26: Государственный аудит. 2024. № 3. С. 89–106.

8. Савенков А.Н. Новый технологический уклад и социогуманитарные вызовы // Государство и право. 2025. № 1. С. 14–37.

9. Савенков А.Н. Философия права и становление российского государства-цивилизации: Монография. М.: Наука, 2024. – 739 с.

10. Савенков А.Н., Россинская Е.Р. Актуальные направления развития общей теории криминалистики сквозь призму современных технологий // Государство и право. 2024. № 10. С. 156–168.

11. Шестые Бачиловские чтения: Сборник статей участников Международной научно-практической конференции, Москва, 2–3 февраля 2023 года. М., 2023. – 256 с.

References

1. Henry A. Kissinger, Eric Schmidt, and Craig Mundie. AI Can Save Humanity – Or End It. URL: https://www.theatlantic.com/ideas/archive/2024/11/ai-genesis-excerpt-kissinger-schmidt-mundie/680619.

2. Matt Kaplan and Michael Brown. The Private Sector on the Front Line. Big Tech and the Risky Blurring of Commercial and Security Interests. Foreign Affairs. January 31, 2025. URL: https://www.foreignaffairs.com/united-states/private-sector-front-line#.

3. Information technologies in the criminal law sphere: a monograph / O. Y. Antonov, A. I. Bastrykin, A. A. Bessonov [et al.]. Moscow: Unity-Dana, 2023. – 279 p.

4. A comprehensive study of legal and ethical aspects related to the development and application of artificial intelligence and robotics systems / V. V. Arkhipov, G. G. Kamalova, V. B. Naumov, A.V. Neznamov. SPb., 2022. – 336 p.

5. Naumov V.B., Neznamov A.V. Model convention on robotics and artificial intelligence. Rules for the creation and use of robots and artificial intelligence // Law and information: issues of theory and practice. St. Petersburg, 2017. pp. 210–220.

6. Polyakova T.A. Ensuring the national sovereignty of Russia in the context of the development of high-tech technologies: countering challenges to law and threats to information security // Law Bulletin of Dagestan State University. 2024. Vol. 52, No. 4. pp. 157–165.

7. Polyakova T.A., Smirnov A.A. Legal aspects of ensuring information security when using artificial intelligence technologies // Bulletin of the Moscow University. Series 26: State Audit. 2024. No. 3. pp. 89–106.

8. Savenkov A.N. A new technological order and socio-humanitarian challenges // State and Law. 2025. No. 1. pp. 14–37;

9. Savenkov A.N. Philosophy of law and the formation of the Russian state-civilization: a monograph. Moscow: Nauka, 2024. – 739 p.

10. Savenkov A.N., Rossinskaya E.R. Current trends in the development of the general theory of criminalistics through the prism of modern technologies // State and law. 2024. No. 10. pp. 156–168.

11. The Sixth Bachilov Readings: A collection of articles by participants of the International Scientific and Practical Conference, Moscow, February 2-3, 2023. Moscow, 2023. – 256 p.

Информация об авторе

А. Н. Савенков — директор Института государства и права Российской академии наук, член-корреспондент РАН, доктор юридических наук, профессор, Заслуженный юрист РФ.

Information about the author

A. N. Savenkov — Director of the Institute of State and Law of the Russian Academy of Sciences, Corresponding Member of the Russian Academy of Sciences, Doctor of Law, Professor, Honored Lawyer of the Russian Federation.

УДК 343.97
ББК 67.51

Догматический анализ категорий, содержащихся в ст. 205.2 УК РФ, как элемента информационной безопасности

Мария Александровна Стародубцева
Алтайский государственный университет, Барнаул, Россия

Email: starodubzewa@gmail.com

Аннотация. В данной статье автор рассматривает категории, содержащиеся в описании объективной стороны составов преступлений, предусмотренных ст. 205.2 УК РФ, с позиций криминологии и лингвистики, а также с точки зрения обеспечения информационной безопасности в области противодействия террористической деятельности.
Ключевые слова: публичные призывы, террористическая деятельность, информационная безопасность, публичное оправдание терроризма, пропаганда терроризма.
Научная специальность: 5.1.2. Публично-правовые (государственно-правовые) науки
Для цитирования: Стародубцева М.А. Догматический анализ категорий, содержащихся в ст. 205.2 УК РФ, как элемента информационной безопасности // Мир криминалистики. 2025. № 1. С. 100-105

Dogmatic analysis of the categories contained in Article 205.2 of the Criminal Code of the Russian Federation as an element of information security

Maria A. Starodubtseva
Altai State University, Barnaul, Russia

Email: starodubzewa@gmail.com

Abstract. In this article, the author examines the categories contained in the description of the objective side of the elements of crimes provided for in Article 205.2 of the Criminal Code of the Russian Federation, from the standpoint of criminology and linguistics and from the point of view of ensuring information security in the field of countering terrorist activity.
Keywords: public appeals, terrorist activity, information security, public justification of terrorism, propaganda of terrorism.
For citation: Starodubtseva M.A. Dogmatic analysis of the categories contained in Article 205.2 of the Criminal Code of the Russian Federation as an element of information security // The world of criminology. 2025;(1): 100-105

Введение. В силу ч. 2 ст. 5 Конвенции Совета Европы «О предупреждении терроризма» 2005 года Россия взяла на себя обязательство принять меры, которые могут потребоваться для признания «публичного подстрекательства к совершению террористического преступления» в качестве уголовного преступления в рамках своего внутреннего законодательства[1]. Во исполнение этого обязательства в 2006 году в Уголовный кодекс Российской Федерации была введена новая ст. 205.2, предусматривающая ответственность за публичные призывы к осуществлению

[1] Конвенция Совета Европы о предупреждении терроризма ETS № 196 (Варшава, 16 мая 2005 г.) // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru.

террористической деятельности или публичное оправдание терроризма[2].

Стоит проанализировать каждое из закрепленных в ст. 205.2 УК РФ альтернативных деяний по отдельности и начать с публичных призывов к осуществлению террористической деятельности.

Основная часть. Статья 205.2 УК РФ в части публичных призывов к осуществлению террористической деятельности предусматривает ответственность за разновидность преступного деяния, определенного ст. 282 УК РФ[3]. Такое соотношение характерно для конкуренции общей и специальной норм[4]. Согласно правилу квалификации, закрепленному в ч. 3 ст. 17 УК РФ, при наличии конкуренции применению подлежит специальная норма[5], в рассматриваемой ситуации –ст. 205.2 УК РФ.

С точки зрения науки уголовного права, перечисленные в ст. 205.2 УК РФ деяния различаются по своему предмету и не требуют квалификации по совокупности преступлений. Рассуждая о составе публичных призывов к осуществлению террористической деятельности, предметом можно определить сам призыв. Призыв понимается как побуждение, информационное сообщение, активно воздействующее на сознание и волю других лиц, преследующее цель склонения их к конкретным действиям.

Ст. 205.2 УК РФ говорит о призывах во множественном числе, однако п. 20 Постановления Пленума Верховного Суда РФ «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» обращает внимание на факт окончания анализируемого деяния с момента провозглашения (распространения) хотя бы одного обращения[6]. При этом, обращение может быть зафиксировано в любой форме. Это следует понимать как обязательный признак призыва.

Второй обязательный признак призыва связан с его целью. З.А. Шибзухов отмечает, что «призывы должны сопровождаться целью «возбудить желание» у адресатов осуществлять террористическую деятельность, а сами сообщения должны быть способны сформировать такое побуждение»[7]. О наличии подобной цели может свидетельствовать, например, использование глаголов в повелительном наклонении («сделай», «исполни» и т.д.) либо применение просьбы или совета («тебе стоит подумать над этим»)[8].

Доктрина уголовного права также отмечает неконкретизированность призывов. В противном случае речь идет о подстрекательстве к совершению конкретного преступления, а в данном случае - преступления террористического характера.

Также обязательным признаком выступает публичность. Сегодня в науке уголовного права отражено достаточно много точек зрения относительно критериев публичности. Одной из позиций выступает признание публичным обращения в отношении двух или более адресатов[9]. Признак публичности также раскрывается в Постановлении Пленума Верховного суда РФ «О некоторых вопросах судебной практики по

[2] Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации конвенции совета Европы о предупреждении терроризма» и Федерального закона «О противодействии терроризму» от 27.07.2006 № 153-ФЗ (последняя редакция) // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru.

[3] Согласно ст. 1 Федерального закона «О противодействии экстремистской деятельности», террористическая деятельность является разновидностью экстремизма.

[4] Гаухман Л.Д. Квалификация преступлений: закон, теория, практика. М.: ЮрИнфоР, 2001. С. 217.

[5] Корнеева А.В. Теоретические основы квалификации преступлений / под ред. А.И. Рарога. М.: ТК Велби, Изд-во «Проспект», 2008. С. 153.

[6] Постановление Пленума Верховного Суда РФ «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» от 09.02.2012 № 1 // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru.

[7] Шибзухов З.А. Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма: монография. М.: Юрлитинформ, 2014. С. 67.

[8] Никишин В.Д. Словесный религиозный экстремизм. Правовая квалификация. Экспертиза. Судебная практика: монография / под ред. Е.И. Галяшиной. М.: Проспект, 2022. С. 77.

[9] Бажин Д.А. К вопросу о понимании публичности в уголовном праве // Российский юридический журнал. 2011. № 2. С. 162–168.

уголовным делам о преступлениях террористической направленности», согласно которому вопрос о публичности должен разрешаться судами с учетом места, способа, обстановки и других обстоятельств дела (обращения к группе людей в общественных местах, на собраниях, митингах, демонстрациях, распространение листовок, вывешивание плакатов, распространение обращений путём массовой рассылки сообщений абонентам мобильной связи т. п.). Анализируя приведённый перечень, можно увидеть, что все примеры публичных обращений адресуются неопределённому кругу лиц, лицо обращается не к конкретным субъектам. Индивидуальные характеристики адресатов его не интересуют. Такой характер обращений является определяющим признаком публичности[10].

Наконец, с содержательной стороны, призыв должен содержать побуждение к совершению именно террористической деятельности. Однако стоит отметить существующую путаницу в терминологии рассматриваемых преступлений: «террористическая деятельность», «террористические преступления», «преступления террористического характера» и «преступления террористической направленности».

В примечании 2 к ст. 205.2 УК РФ дается ответ на вопрос о том, что следует считать террористической деятельностью для целей данной статьи. В качестве таковой следует считать совершение хотя бы одного из преступлений, предусмотренных ст.ст. 205-206, 208, 211, 220, 221, 277, 278, 279, 360, 361 УК РФ. Поскольку в рамках данного исследования автор рассматривает ст. 205.2 УК РФ, в дальнейшем мы будем придерживаться именно этого перечня.

Следующим альтернативным деянием в ст. 205.2 УК РФ выступает публичное оправдание терроризма. Его определение раскрывается в примечании 1: «под публичным оправданием терроризма понимается публичное заявление о признании идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании»[11]. Д.А. Ковлагина отмечает, что раскрытие термина «оправдание» через термин «заявление», нигде в УК РФ ни до, ни после не упоминающееся, вызывает сомнение[12].

Словарь С.И. Ожегова толкует «заявление» как «официальное сообщение»[13]. Сомнительно, что речь идет об официальном обращении о признании идеологии и практики терроризма правильными. Лингвистика предполагает считать термин «оправдание терроризма» такой «положительной оценкой (одобрение, восхваление) этого явления, в которой террористическая деятельность признается правильной, желательной и (или) необходимой»[14].

Также вызывает сомнения тот факт, что в данном составе используется термин «терроризм», чья дефиниция, как мы уже выяснили, не является уголовно-правовой, выступая в большей степени криминологической. Более того, проведенный автором анализ судебной практики и контент-анализ информационных ресурсов средств массовой информации и сети «Интернет», отражающих имеющуюся правоприменительную практику по ст. 205.2 УК РФ, доказывает, что осужденные признавали правильным не абстрактный терроризм в целом, а деятельность конкретных членов террористических организаций или террористов-одиночек, выраженную в совершении конкретных преступлений террористической направленности. Например, К. со своего мобильного телефона размещал

[10] Постановление Пленума Верховного Суда РФ «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» от 09.02.2012 № 1 // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru.

[11] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru.

[12] Ковлагина Д.А. Актуальные проблемы квалификации и применения ст. 205.2 УК РФ // Пробелы в российском законодательстве. 2020. №5. С. 154.

[13] Ожегов С.И. Толковый словарь русского языка: 80000 слов и фразеологических выражений. 4-е изд., доп. М.: ООО «ИТИТехнологии», 2014. 374 с.

[14] Никишин В.Д. Словесный религиозный экстремизм. Правовая квалификация. Экспертиза. Судебная практика: монография / под ред. Е.И. Галяшиной. М.: Проспект, 2022. С. 78.

в социальной сети изображение одного из участников диверсионно-террористической группировки с текстом, содержащим положительную оценку действий террористов при совершении террористического акта[15].

Стоит также отметить, что примечание 1 в ст. 205.2 УК РФ выделяет две альтернативные формы публичного оправдания: публичное оправдание идеологии терроризма и публичное оправдание практики терроризма.

При установлении такой формы публичного оправдания, как публичное оправдание идеологии терроризма, обращают на себя внимание трудности определения термина «идеология». Этот термин также упоминается в примечании 1.1 в ст. 205.2 УК РФ.

Сам по себе термин «идеология» не является уголовно-правовым или криминологическим и более содержательно изучается в контексте философской и политической науки. Так, Е.В. Литягин объясняет идеологию как «совокупность идей, формирующих определенный тип мировоззрения, система ценностей, идеалов, норм поведения, вносимых в общественное сознание посредством различного рода социальных институтов, и организующая всю общественную жизнедеятельность»[16]. Указанное толкование перекликается с позицией социологов, таких как С.Г. Кара-Мурза: «Идеология – это комплекс идей и концепций, с помощью которого человек понимает общество, социальный порядок и самого себя в этом обществе»[17].

Что касается второй формы публичного оправдания - публичного оправдания практики терроризма, как представляется автору, речь идет о публичном оправдании террористической деятельности в контексте примечания 2 к ст. 205.2 УК РФ. Поскольку выше автор уже рассматривал уголовно-правовые и криминологические сложности с определением термина «террористическая деятельность», подробного анализа данная форма в рамках диссертационного исследования не требует.

Само деяние, выраженное в форме пропаганды в ст. 205.2 УК РФ, неоднородно. По содержанию распространяемые материалы и информацию условно можно разделить на две разновидности.

Первой станет информация, формирующая у лица идеологию терроризма и убежденность в её привлекательности. Сразу же стоит отметить сомнения исследователей, к примеру, Г.Л. Москалева, о том, что применение подобных оценочных категорий («идеология терроризма», «убежденность», «привлекательность») означает постоянное применение на практике психолого-лингвистической экспертизы. Это, в свою очередь, может привести к искажению интерпретации информации и проявлению спекулятивного характера норм в следственной и судебной практике[18].

Второй разновидностью выступает информация, направленная на формирование у лица представления о допустимости осуществления террористической деятельности. При этом, судя по всему, террористическая деятельность рассматривается с позиции примечания 2 к ст. 205.2 УК РФ.

Заключение. В лингвистической науке нет единой точки зрения на соотношение терминов «призыв», «оправдание» и «пропаганда». В.Д. Никишин указывает, что пропаганда является родовым понятием для двух остальных и «может реализовываться в комплексе через обоснование, оправдание террористической деятельности и призывы к её осуществлению или же только через обоснование или оправдание»[19]. Также считает и Г.С. Иваненко,

[15] Апелляционное определение Верховного Суда Российской Федерации по делу № 225-АПУ19-5 от 16 января 2020 г. в отношении К. // Судебные и нормативные акты РФ. URL: https://su-dact.ru (дата обращения: 10.07.2024).

[16] Литягин Е.В. Идеология как необходимый фактор жизни современного общества: автореф. дис. ... канд. филос. наук: 09.00.11. Горно-Алтайск, 2004. С. 8.

[17] Кара-Мурза С.Г. Идеология и мать ее наука. М.: Эксмо-Пресс: Алгоритм, 2002. С. 155.

[18] Москалев Г.Л. Пропаганда терроризма (ст. 205.2 УК РФ) // Национальная безопасность / nota bene. 2018. № 6. С. 79–87.

[19] Никишин В.Д. Словесный религиозный экстремизм. Правовая квалификация. Экспертиза. Судебная практика: монография / под ред. Е.И. Галяшиной. М.: Проспект, 2022. С. 69-70.

отмечающий, что «пропаганда – понятие более широкое, чем призыв и побуждение. Пропаганда – это распространение каких-либо идей, учений, взглядов, знаний, то есть «…любое теоретическое или эмоциональное обоснование какой-либо позиции является пропагандой»[20]. Тем не менее, законодатель включил в объективную сторону ст. 205.2 УК РФ пропаганду в специально созданном для этого узком смысле. Это также может свидетельствовать об отходе от принципа системности уголовно-правовых норм.

Таким образом, автор, исходя из криминологического обоснования, приходит к выводу, что понятия «публичные призывы к осуществлению террористической деятельности», «публичное оправдание терроризма» и «пропаганда терроризма» в ст. 205.2 УК РФ соотносятся между собой как альтернативные деяния объективной стороны. Термины, содержащиеся в этих понятиях: «оправдание», «пропаганда», «идеология терроризма», «убежденность», «привлекательность», – являются оценочными категориями, выпадающими из общепринятой терминологии уголовного права и криминологии.

Список источников

1. Конвенция Совета Европы о предупреждении терроризма ETS № 196 (Варшава, 16 мая 2005 г.) // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru.

2. Гаухман Л.Д. Квалификация преступлений: закон, теория, практика. – М.: ЮрИнфоР, 2001. – С. 217.

3. Корнеева А.В. Теоретические основы квалификации преступлений // под ред. А.И. Рарога. – М.: ТК Велби, Изд-во «Проспект», 2008. – С. 153.

4. Постановление Пленума Верховного Суда РФ «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» от 09.02.2012 № 1 // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru.

5. Шибзухов З.А. Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма: монография. – М.: Юрлитинформ, 2014. – С. 67.

6. Никишин В.Д. Словесный религиозный экстремизм. Правовая квалификация. Экспертиза. Судебная практика: монография / под ред. Е.И. Галяшиной. – М.: Проспект, 2022. – С. 77.

7. Бажин Д.А. К вопросу о понимании публичности в уголовном праве // Российский юридический журнал. – 2011. – № 2. – С. 162–168.

8. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Справ.-правовая система «КонсультантПлюс». URL: http://www.consultant.ru.

9. Ожегов С.И. Толковый словарь русского языка: 80000 слов и фразеологических выражений. 4-е изд., доп. / С. И. Ожегов, Н. Ю. Шведова. – М.: ООО «ИТИТехнологии», 2014. – 374 с.

10. Апелляционное определение Верховного Суда Российской Федерации по делу № 225-АПУ19-5 от 16 января 2020 г. в отношении К. // Судебные и нормативные акты РФ. URL: https://su-dact.ru. (дата обращения: 10.07.2024).

11. Литягин Е.В. Идеология как необходимый фактор жизни современного общества: автореф. дис. ... канд. филос. наук: 09.00.11. Горно-Алтайск, 2004. С. 8.

12. Кара-Мурза С.Г. Идеология и мать ее наука / С.Г. Кара-Мурза. – М.: Эксмо-Пресс: Алгоритм, 2002. – С. 155.

13. Москалев Г.Л. Пропаганда терроризма (ст. 205.2 УК РФ) // Национальная безопасность / nota bene. – 2018. – № 6. – С. 79–87.

14. Иваненко Г.С. Лингвистическая экспертиза текста в процессах об экстремизме: учеб. пособие. – М.: ФЛИНТА, 2020. – С. 16.

References

1. Council of Europe Convention on the Prevention of Terrorism ETS N 196 (Warsaw,

[20] Иваненко Г.С. Лингвистическая экспертиза текста в процессах об экстремизме: учеб. пособие. М. ФЛИНТА, 2020. С. 16.

May 16, 2005) // Reference and legal system "ConsultantPlus". URL: http://www.consultant.ru.

2. Gaukhman L.D. Qualification of Crimes: Law, Theory, Practice. – M.: YurInfoR, 2001. – P. 217.

3. Korneeva A.V. Theoretical Foundations of Crime Qualification / edited by AI Rarog. – M.: TK Velbi, Prospect Publishing House, 2008. – P. 153.

4. Resolution of the Plenum of the Supreme Court of the Russian Federation "On Certain Issues of Judicial Practice in Criminal Cases Concerning Terrorist-Oriented Crimes" dated 02/09/2012 No. 1 // Reference and Legal System "ConsultantPlus". URL: http://www.consultant.ru.

5. Shibzukhov Z.A. Public Calls to Commit Terrorist Activities or Public Justification of Terrorism: Monograph. – M.: Yurlitinform, 2014. – P. 67.

6. Nikishin V.D. Verbal Religious Extremism. Legal qualification. Expertise. Judicial practice: monograph / edited by E.I. Galyashina. – M.: Prospect, 2022. – P. 77.

7. Bazhin D.A. On the issue of understanding publicity in criminal law // Russian Law Journal. – 2011. – № 2. – P. 162–168.

8. Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ // Reference and legal system "ConsultantPlus". URL: http://www.consultant.ru.

9. Ozhegov S.I. Explanatory dictionary of the Russian language: 80,000 words and phraseological expressions. 4th ed., suppl. / S.I. Ozhegov, N.Yu. Shvedova. – M.: OOO "ITITekhnologii", 2014. – 374 p.

10. Appellate ruling of the Supreme Court of the Russian Federation in case No. 225-APU19-5 dated January 16, 2020 in relation to K. // Judicial and regulatory acts of the Russian Federation. URL: https://su-dact.ru.

11. Lityagin E.V. Ideology as a necessary factor in the life of modern society: author's abstract. diss. ... candidate of philosophical sciences: 09.00.11. Gorno-Altaysk, 2004. – P. 8.

12. Kara-Murza S.G. Ideology and its mother science / S.G. Kara-Murza. – M .: Eksmo-Press: Algorithm, 2002. – P. 155.

13. Moskalyev G.L. Propaganda of terrorism (Article 205.2 of the Criminal Code of the Russian Federation) // National security / nota bene. – 2018. – № 6. – P. 79–87.

14. Ivanenko G.S. Linguistic examination of the text in extremism proceedings: textbook. manual. – M.: FLINTA, 2020. – P. 16.

Информация об авторе

М.А. Стародубцева — старший преподаватель кафедры уголовного права и криминологии Алтайского государственного университета.

Information about the author

M.A. Starodubtseva — Senior Lecturer at the Department of Criminal Law and Criminology, Altai State University.

УДК 343.9

Деятельность Русской группы Международного союза криминалистов в становлении отечественной криминалистики

Светлана Петровна Кушниренко
Санкт-Петербургский государственный университет, Санкт-Петербург, Россия
Email: s.kushnirenko@spbu.ru

Николай Александрович Корниенко
Санкт-Петербург, Россия
Email: office@unity-dana.ru

Аннотация. Статья посвящена истории создания и деятельности Русской группы Международного союза криминалистов, образованной в 1897 году при Юридическом обществе при Императорском Санкт-Петербургском университете. Предпосылками для её создания послужили консолидация передовых на тот исторический этап научных идей выдающихся учёных Европы — профессоров Ф. Листа, А. Принса, Г. фон Гамеля, а также проникновение в юриспруденцию идей социологической и антропологической школ, что меняло взгляд на преступление, борьбу с преступностью и наказание. Созданный ими в 1888 году Международный союз криминалистов объединял в своих рядах специалистов в области уголовного права, уголовного процесса, тюрьмоведения (уголовно-исполнительного права), криминологии и зарождающейся в эти годы криминалистики. За время своей деятельности Русская группа разрослась с 21 члена в 1897 году до 405 в 1912 году и стала самой многочисленной в Международном союзе криминалистов. Перенося идеи Союза на национальную почву, обсуждая их и предлагая решения по изменению законодательства, правоприменению, обучению студентов-юристов, группа снискала заслуженное уважение во всех слоях общества. На основании контент-анализа, исторического и сравнительно-правового методов авторы приходят к выводу об использовании идей, обсуждаемых Русской группой, высшими должностными лицами государства, благодаря чему решения в короткие сроки находили реализацию в практической деятельности, особенно в инструкциях Министерства юстиции и Министерства внутренних дел по расследованию преступлений. В статье раскрываются виды деятельности группы и делается вывод о её миссии в разработке и внедрении основ криминалистики, а также о её роли в становлении и развитии отечественной криминалистики как науки.

Ключевые слова: Русская группа Международного союза криминалистов, Императорский Санкт-Петербургский университет, история криминалистики.
Научная специальность: 5.1.4. Уголовно-правовые науки
Для цитирования: Кушниренко С.П., Корниенко Н.А. Деятельность Русской группы Международного союза криминалистов в становлении отечественной криминалистики // Мир криминалистики. 2025. № 1. С. 106-119

Activities of the Russian group of the International Union of Criminologists in the development of domestic criminology

Svetlana P. Kushnirenko
St. Petersburg State University, St. Petersburg, Russia
Email: s.kushnirenko@spbu.ru

Nikolay A. Kornienko
St. Petersburg, Russia
Email: office@unity-dana.ru

Abstract. The article is devoted to the history of the creation and activity of the Russian Group of the International Union of Criminologists, formed in 1897 at the Law Society at the Imperial St. Petersburg University. The prerequisites

for its creation were the consolidation of the leading scientific ideas of outstanding European scientists at that historical stage — Professors F. Liszt, A. Prince, and G. von Hamel, as well as the penetration of ideas from sociological and anthropological schools into jurisprudence, which changed the way crime, crime control, and punishment were viewed. The International Union of Criminologists, created by them in 1888, united specialists in the field of criminal law, criminal procedure, prison studies (penal enforcement law), criminology and criminology emerging in these years. During its activity, the Russian Group grew from 21 members in 1897 to 405 in 1912 and became the largest in the International Union of Criminologists. By bringing the Union's ideas to national soil, discussing them and proposing solutions to change legislation, law enforcement, and law student education, the group has earned well-deserved respect from all sectors of society. Based on content analysis, historical and comparative legal methods, the authors conclude that the ideas discussed by the Russian Group were used by top government officials, so that solutions could be implemented in practice in a short time, especially in the instructions of the Ministry of Justice and the Ministry of Internal Affairs on crime investigation. The article reveals the activities of the group and concludes about its mission in the development and implementation of the fundamentals of criminology, as well as its role in the formation and development of domestic criminology as a science.
Keywords: Russian group of the International Union of Criminologists, Imperial St. Petersburg University, history of criminology.
For citation: Kushnirenko S.P., Kornienko N. A. Activities of the Russian group of the International Union of Criminologists in the development of domestic criminology // The world of criminology. 2025;(1):106-119

Введение. На современном этапе развития криминалистика как синтетическая область научного знания «занимает лидирующие позиции в правовой области уголовно-правовых наук за счет многогранности своих теорий и естественно-технических решений задач по собиранию, оценке и использованию криминалистически значимой информации в судопроизводстве» [9] , что позволяет ей использовать новейшие, в том числе инновационные, достижения различных наук и проводить междисциплинарные исследования, расширяя возможности собственной науки и вырабатывая новые собственные методы исследования. В результате «методология криминалистической науки с позиций эпистемологии может рассматриваться как трансцедентальное знание, позволяющее криминалистам постигать сущность преступного деяния и предлагать наиболее эффективные приемы раскрытия и расследования преступлений» [1]. Эти два тезиса ведущих российских ученых-криминалистов подтверждают, какой значительный путь прошла наука криминалистика всего за сто с небольшим лет с момента своего формирования. Уже кажется невероятным, что совсем недавно закономерности совершения преступлений и их расследования были непостижимы, и лица, ведущие расследования, двигались в своём познании совершённого события наощупь, руководствуясь жизненным опытом и здравым смыслом.

В своем исследовании мы хотели бы обратиться к событиям конца 19 – начала 20 века, когда в России начали складываться первые научные положения криминалистической науки, претворяемые в практическую деятельность её вдохновителями и неустанными исследователями. Речь пойдет о роли Русской группы Международного союза криминалистов, способствовавших распространению криминалистических знаний, методов и техник среди работников правоохранительных органов. Именно эти соображения заставляют нас цитировать слова члена Русской группы Е.М. Кулишера о том, что «нет ничего более опасного для оценки новых идей, как их проникновение в жизнь: победоносные, они начинают казаться банальными» [5]. Действительно, за десятилетиями развития науки размываются, покрываются завесой те страсти, сомнения, дискуссии, которые бушевали при отстаивании идей, ставших обычными даже для студентов-юристов. Эти соображения заставили нас обратиться к истории науки криминалистики через призму её взаимодействия с международными научными

движениями, чтобы оценить уровень её развития в России в соответствующую эпоху и воздать должное тем энтузиастам, которые стояли у её истоков.

1. Международный союз криминалистов. Международный союз криминалистов был образован в 1889 году. Его основателями стали известные во всем мире учёные: профессор Франц фон Лист — австрийский и немецкий юрист, специалист в области уголовного и международного права; Адольф Принс — бельгийский пеналист и социолог, доктор права; Ван Гамель — голландский адвокат по уголовным делам и либеральный политик. В 1888 году ими был составлен и разослан видным представителям уголовно-правовой науки различных стран Статут Международного союза уголовного права, в котором цель создания была определена следующим образом. «Международный союз уголовного права исходит из убеждения, что преступление и наказание должны быть рассматриваемы не только со стороны юридической, но и общественной. Он посвящает себя закреплению этого принципа и его последствий в науке права и в уголовных законодательствах» (ст. I) [13]. В статье II Статута излагались положения, обозначенные как «руководящие основания работ союза», где, в частности, задачей уголовного права провозглашалась «борьба против преступности как общественного явления». Проект Статута и приглашение принять участие в Союзе были направлены Листом профессору Императорского Санкт-Петербургского университета И. Я. Фойницкому, с которым Лист познакомился во время научной командировки Ивана Яковлевича в европейские университеты Англии, Германии, Франции, Италии и Швейцарии и высоко оценивал его научную деятельность. По всей видимости, они вместе присутствовали на Первом международном пенитенциарном конгрессе в Лондоне в 1872 году, когда были заложены принципы современной пенитенциарной науки и с энтузиазмом обсуждались новые идеи об исправлении преступников. Ознакомившись со Статутом, И.Я. Фойницкий сообщил своему корреспонденту, что «не разделяет положения о неисправимых преступниках, всецело принадлежащего антропологической школе», на что Лист ответил ему, что «вступление в Союз отнюдь не означает согласия вступающего со всеми положениями ст. II Статута, которые подлежат еще рассмотрению на общих собраниях Союза… Союз не требует от своих членов присоединения к определенной уголовной теории. Оставляя в стороне чисто теоретические споры школ, он преследует цель практическую, именно постепенное преобразование действующего права в смысле полного приспособления наказания к тем целям, которые им преследуются. Каждое уголовное законодательство должно носить национальную окраску, должно сообразовываться с истинным характером государства и народа, для которого предназначается» [12].

Окончательно основные задачи Международного союза криминалистов были сформулированы следующим образом на VII съезде, состоявшемся в Лиссабоне в 1897 году: «Международный союз криминалистов защищает тот взгляд, что как преступление, так и средства борьбы с ним должны быть рассматриваемы не только с юридической, но и с антропологической и социологической точек зрения. Задачей своей союз поэтому ставит научное исследование преступления, его причин и мер борьбы с ним».

Но вернемся к истории создания Союза. Его первый съезд состоялся в 1889 году в Брюсселе. На нём обсуждались следующие вопросы:

1. Можно ли рекомендовать законодательствам, по примеру Бельгии, ввести в карательную систему институт условного осуждения?

2. Какие меры могут быть рекомендованы законодательствам для того, чтобы ограничить применение тюремного заключения в случаях осуждения за лёгкие проступки?

3. Каковы недостатки современной системы борьбы с рецидивом?

Четвёртый вопрос: «С какого возраста дети могут быть преследуемы перед судом?» — остался без рассмотрения и был перенесён на следующий съезд.

От России на съезде присутствовал один только И.Я. Фойницкий, он и дал «согласие временно принять на себя функцию быть представителем интересов союза в стране и страны перед союзом» [12]: предварительно обсуждать вопросы, намеченные для предстоящих конгрессов, взимать «скромные» членские взносы (ежегодно 5 франков), пересылать их в бюро союза, распределять в стране труды союза.

На втором съезде, состоявшемся в Берне в 1890 году, присутствовали уже 80 членов союза, из которых трое представляли Россию: И.Я. Фойницкий, профессор московского университета А.К. Вульферт и товарищ прокурора г. Брэнер. Были рассмотрены вопросы: 1) какие признаки могут быть рекомендованы законодателю для распознавания неисправимых преступников привычек и какие против них должны быть приняты меры; 2) оставшийся нерассмотренным вопрос предыдущего съезда о возрасте уголовной ответственности детей; 3) может и должен ли законодатель обратить большее, чем ныне, внимание на момент гражданского вознаграждения потерпевшего за причиненный ему преступлением вред и вообще на права потерпевшего; 4) возможно ли заменить в некоторых случаях краткосрочное лишение свободы обязательными работами без заключения? На съезде И.Я. Фойницкий выступил с докладом по вопросу об ответственности малолетних, в котором резко возражал против критерия «разумения», принятого тогда в большинстве законодательств для определения ответственности несовершеннолетних.

По итогам этих двух съездов И.Я. Фойницкий с энтузиазмом констатирует: «Международный союз уголовного права — учреждение молодое и дышащее молодостью, энергией и свежестью. Оно не может не быть весьма симпатично для всех тех, которым надоели метафизические бредни и произвольный субъективизм прежних школ. Союз стремится в постановке и разрешению жгучих вопросов уголовного права на почве действительности и насущных потребностей общежития». [12].

Воодушевленный идеями новой организации, И.Я. Фойницкий сплачивает вокруг себя единомышленников и становится «инициатором приобщения русских криминалистов к общей работе культурных стран Запада», явившись «первым представителем университетской науки в России, приобретшим европейскую известность и организовавшим научное взаимодействие русской уголовной науки с Западом» [7].

2. Русская группа Международного союза криминалистов. Русские участники сначала состояли индивидуальными членами Союза, но в 1895 году после съезда в Линце И.Я. Фойницкий был увлечен идеей создания Русской национальной группы союза и проведения в России съезда Международного союза криминалистов. Этой идеей он сумел заинтересовать Министра юстиции Н.В. Муравьева, который вместе с несколькими видными чиновниками министерства юстиции, профессорами университетов и академий записался в члены-учредители. 5 июня 1897 года Министром Народного Просвещения графом Деляновым был утвержден Устав Русской группы, в котором указывалось, что группа открывается при Юридическом Обществе, состоящем при Императорском Санкт-Петербургском университете. К слову сказать, И.Д Делянов на первом же собрании Русской группы сам вступил в число её членов. Однако решающую роль в создании группы сыграл Министр юстиции, член Санкт-Петербургского юридического общества Н.В. Муравьев. По мнению современников, организационное оформление Русской группы стало возможным именно «благодаря его энергии и посвященным стремлениям». Председателем Русской группы был избран профессор Санкт-Петербургского Императорского университета И.Я.

Фойницкий. Таким образом, именно на университетской площадке разворачивалась основная деятельность Международного союза криминалистов. Основателями группы считались русские подданные, которые до утверждения устава были членами Международного союза криминалистов. Таких по списку оказалось 21. На 1 января 1899 года в группе состояло уже более 70 членов, а на 1 августа 1902 года – 253, среди которых две организации – Курское и Ярославское юридические общества, маститые ученые, государственные деятели, присяжные поверенные, магистранты университетов и др. В состав входили и дамы, в основном, представительницы благотворительных обществ. Международный союз криминалистов также с годами расширялся и в 1912 году в него входили уже 1243 члена, объединенные в 14 национальных групп, самой многочисленной из которых стала Русская группа – 405 членов. Для сравнения, второй по численности являлась Германская группа, состоящая из 315 членов [8].

С неутомимой энергией И.Я. Фойницкий руководил группой и олицетворял её активное ядро: привлекал новых членов, организовывал съезды, выдвигал вопросы для обсуждения, отыскивал докладчиков, «направлял её деятельность в согласии с требованиями русского законодательства и научными течениями западной науки» [2].

Устав Русской группы союза определил цели организации, заключавшиеся в «*научной разработке, распространении и применении положений уголовного права, соответственно задачам Союза и условиям русской жизни*». Её деятельность определялась задачами Союза по борьбе с преступностью, которые стояли перед государственными органами. Употребление термина «уголовное право» в отмеченный период включало все уголовно-правовые дисциплины, в том числе и криминалистику, ещё не имевшую в то время самостоятельного статуса. Уровень научной мысли конца XIX века ещё не имел достаточного материала для установления и формирования её научных основ, а обобщение и анализ практики расследования преступлений ещё не собрал достаточный объем аналитической информации, позволяющий сделать вывод о её предмете, основных положениях, структуре и т.д. Естественно, что научная дисциплина в таких условиях не в состоянии предложить цели, задачи, конкретные методы и приемы противодействия преступности, способы их осуществления.

3. Внедрение в практику криминалистических знаний. Истории отечественной криминалистики до 1917 года был отведен весьма короткий отрезок времени, необходимый для развития и формирования новой дисциплины. Этот период был усложнен общественно-политическим строем и экономическим развитием: война с Японией 1904-1905 гг. с её поражениями на суше и на море, революционные события 1905-1906 гг., появление возможности участия общественных сил и политических партий только в 1905 году при созыве Государственных Дум, а затем Первая мировая война и Октябрьская революция. Всё это усложняло и тормозило становление отечественной криминалистики, тем не менее, именно в эти годы были не только заложены основы криминалистики, но и получены первые ощутимые результаты ее использования в практической деятельности по борьбе с преступностью. Мы склонны это связывать и с деятельностью Русской группы международного союза криминалистов.

В данной статье мы хотели бы подчеркнуть важную, на наш взгляд, особенность Русской группы, которая сыграла решающую роль в становлении, развитии и внедрении в практическую деятельность криминалистических научных знаний. Мы имеем в виду участие в составе группы видных должностных лиц государственных органов и служб, высоких должностных лиц Министерства юстиции, Министерства внутренних дел, Министерства просвещения и других ведомств.

Например, членами группы являлись три министра юстиции, одновременно являвшихся генерал-прокурорами Правительствующего сената: Муравьёв Н.В. (1894–1904), Щегловитов И.Г. (1906–1915), Макаров А.А. (1916); заместитель министра Веревкин А.Н., министр внутренних дел Макаров А.А., статс-секретари Государственного совета Сергеевский Н.Д., Петражицкий Л.И., Спасович В.Д., Фойницкий И.Я., Фукс Э.Я.; первоприсутствующий сенатор Уголовного кассационного департамента Сената Таганцев Н.С., обер-прокурор Уголовного кассационного департамента Сената Случевский В.Д., а также депутаты Государственной думы разных созывов и другие. Получая информацию и принимая непосредственное участие в собраниях группы, они формировали своё представление о мировых тенденциях в борьбе с преступностью и связанными с ней явлениями, воплощая его в конкретных решениях по организации и деятельности правоохранительных органов руководимых ими учреждений и служб. Одновременно они считали необходимым донести своё видение актуальных вопросов криминалистики и процессов расследования до широкой аудитории научно-педагогического сообщества, формируя тем самым почву для общественного восприятия деятельности вверенных им министерств и ведомств. Некоторые из них возглавляли комиссии по усовершенствованию действующего законодательства, учреждённые императором, работая в Государственном совете и Государственной думе. Эта особенность деятельности Русской группы практически не нашла отражения в научных публикациях; поэтому мы считаем важным акцентировать на ней внимание, поскольку именно она, по нашему мнению, позволила Русской группе быть наиболее эффективной по сравнению с другими группами и юридическими общественными образованиями. Благодаря интенсивному обмену мнениями, обсуждению наиболее актуальных проблем правоприменения в сфере борьбы с преступностью появлялись и распространялись новые знания в области практической деятельности по раскрытию и расследованию преступлений. Заметим, что в Европе в этот момент только появляются фундаментальные исследования и работы, которые лягут в основу новой науки – криминалистики. Так, в 1893 году Ганс Гросс издает свою знаменитую работу «Руководство для судебных следователей, чинов жандармерии и полиции», третье издание которой, вышедшее в 1898 году, было озаглавлено автором «Руководство для судебных следователей как система криминалистики». В 1895-1896 гг. книга в переводе на русский язык издается в России. К этому времени в России уже были изданы работы Я. И. Баршева «Основания уголовного судопроизводства, с применением к российскому уголовному судопроизводству» (1841 г.), Н. И. Стояновского «Практическое руководство к русскому уголовному судопроизводству» (1852 г.) и другие, в которых содержались научные и практические рекомендации по ведению расследования преступлений, положенные впоследствии в основу криминалистики. Членами Санкт-Петербургского юридического общества и Русской группы Международного союза криминалистов издаются значимые труды в области криминалистики, например: «Схема предварительного следствия» С. А. Алекринского (1912), «Основы уголовной техники» Н. И. Трегубова (1915), «Очерки по следственной части. История. Практика» Б. Л. Бразоля (1916) и другие. Члены Русской группы постоянно публикуют свои работы в юридической прессе: в журналах «Вестник права», «Журнал уголовного права и процесса», «Журнал Министерства юстиции», «Вестник полиции»; еженедельной газете «Право» и других изданиях, в том числе в изданиях Санкт-Петербургского юридического общества и Русской группы Международного союза криминалистов.

Заметный вклад в становление и развитие отечественной криминалистики внесли юристы, совмещавшие административную деятельность в Минюсте с

преподавательской. Так, заместитель министра юстиции Николай Иванович Стояновский, один из учредителей Юридического общества, его председатель в 1877–1895 годах, преподавал в Императорском училище правоведения и дважды издавал «Практическое руководство к русскому уголовному судопроизводству» (1852 г., 1858 г.). С. Н. Трегубов преподавал в Императорском училище правоведения и Александровской военно-юридической академии, возглавлял 1-й Департамент Министерства юстиции, являлся ревизующим сенатором, советником по военно-судным вопросам при штабе Верховного главнокомандующего в Первую мировую войну и издал «Научно-технические приёмы расследования преступлений». В 1911–1912 годах он впервые в России организовал совместно с С. М. Потаповым регулярное изучение криминалистики в Императорском училище правоведения и в Александровской военно-юридической академии.

Николай Валерианович Муравьёв (1850–1908) в 1870 году экстерном сдал экзамены на юридическом факультете Императорского Санкт-Петербургского университета. Отказавшись от педагогической деятельности, он начал службу кандидатом на судебную должность в Московском окружном суде. Пройдя все ступени карьеры, в 1894 году он занял пост министра юстиции и генерал-прокурора Правительствующего Сената. Отличный администратор сочетался в нём с талантливым юристом, автором двух солидных изданий об отечественной прокуратуре. А.Ф. Кони высоко оценивал его профессиональные качества, отмечая «развитый ум и просвещенный взгляд». В течение пяти лет он руководил комиссией по пересмотру уголовно-процессуального законодательства, но из-за войны с Японией работа комиссии была прекращена. 14 января 1905 года он оставил свою должность, а скончался послом в Италии в 1908 году. Понимая важность международного сотрудничества в борьбе с преступностью, он поддержал в 1902 году проведение в Санкт-Петербурге Международного съезда криминалистов и создание Русской группы союза, стал её членом и принял участие в заседаниях группы. Н.В. Муравьев следил за развитием криминалистических идей, всячески пропагандировал их и внедрял в деятельность правоохранительных органов. Так, им были подготовлены фундаментальный труд «Прокурорский надзор в его устройстве и деятельности» (1889) и ряд ценных ведомственных документов, содержавших практические рекомендации по раскрытию и расследованию преступлений: «Инструкция чинам полиции округа Санкт-Петербурга судебной палаты по обнаружению и исследованию преступлений» (1886), «Краткий наказ волостным и сельским начальникам по раскрытию преступлений и поимке преступников» (1885), «Руководство для судебных следователей и лиц, привлекаемых к уголовным следствиям, с разъяснениями Сената и Государственного совета» (1878), «Наказ Министра юстиции Н. Муравьева чинам прокурорского надзора судебных палат и окружных судов» (1896) и другие [11].

Много для развития криминалистики сделал член Русской группы Николай Флорианович Лучинский (1860 г. – после 1917 г.): член «консультации при министерстве юстиции учрежденной», инспектор Главного тюремного управления (ГТУ), управляющий центральным дактилоскопическим бюро (далее ЦДБ), редактор журнала «Тюремный вестник», действительный статский советник (соответствует воинскому званию генерал-майора). В 1882 году он окончил юридический факультет Новороссийского университета со степенью кандидата права. На предложение заняться научной работой и готовиться к защите докторской диссертации он отказался и с февраля 1883 года служил кандидатом на судебной должности при прокуроре Одесской судебной палаты. Дальнейшая его служба проходила в должности судьи, заместителя прокурора. С 1901 года он был инспектором тюремного ведомства, а затем и мировой судья. В 1904 году он издает работу «Основы тюремного дела». Эта и последующие печатные работы принесли ему известность в качестве специалиста по тюрьмоведению. С 1907 года

Н.Ф Лучинский является редактором журнала «Тюремный вестник», в котором систематически публикует свои работы. Известно его выступление с докладом на VIII Международном пенитенциарном конгрессе в Вашингтоне в 1910 году, в 1911 году – в Амстердаме по вопросам патроната, в 1913 году – по проблемам правовой защиты детей. Он являлся главным распорядителем III Всероссийского съезда тюремных деятелей, проходившем в Санкт-Петербурге с 27 февраля по 7 марта 1914 года, что было отмечено в журнале «Тюремный вестник». В связи с успешным распространением в Европе дактилоскопической регистрации весной 1906 года Министерство юстиции с согласия Императора командировало Ф. Н. Лучинского в Вену и Берлин. Перед ним стояла задача изучить и оценить целесообразность введения дактилоскопической регистрации в России. По результатам командировки Н. Ф. Лучинский представил обстоятельный доклад о значительных преимуществах дактилоскопии перед антропометрией и рекомендовал её использовать как средство регистрации и учета преступников. И уже 16 декабря 1906 года Министр юстиции И. Г. Щегловитов утверждает «Правила о производстве и регистрации дактилоскопических оттисков». Для ведения регистрации лиц, прошедших дактилоскопирование, при Главном тюремном управлении создается Центральное дактилоскопическое бюро со штатом 3 человека, финансирование которого началось уже с 1 января 1907 года. Постановке на учет подлежали: 1) арестованные, обвиняемые в преступлениях, карающихся лишением всех прав состояния; 2) арестованные за бродяжничество; 3) осужденные к ссылке на каторжные работы либо на поселение (в случаях, если они не подвергались ранее дактилоскопированию). Дактилоскопирование необходимо было провести в течение 1-3 суток и там, где произошло задержание. Для дактилоскопирования на места были разосланы до 1000 комплектов принадлежностей и до 10000 бланков дактилокарт, а также необходимое число «Правил для производства и регистрации дактилоскопических снимков».

После начала работы ЦДБ стали поступать запросы с просьбой провести исследование следов пальцев рук, изъятых во время «осмотра места преступления», и сравнить его с образцами дактокарты. Стоит отметить, что дактилоскопическое исследование проводилось по просьбе губернаторов, председателей и прокуроров окружных судов, судебных и военных следователей, представителей жандармерии и полиции (от весьма высокопоставленных до урядников).

Вершиной признания профессиональной деятельности Н. Ф. Лучинского следует считать персональное приглашение в апреле 1914 года на I съезд Судебной (уголовной) полиции в Монако, где он был избран Вице-президентом конгресса и сделал блестящий доклад о работе Бюро [3].

По мнению авторов, ещё одна фигура члена Русской группы заслуживает быть отмеченной в контексте вклада в становление отечественной криминалистики. Александр Александрович Макаров (1857-1919) – прокурор саратовской судебной палаты. В 1906 году назначен Министром внутренних дел П. А. Столыпиным своим заместителем, в обязанности которого с 18 мая 1906 года по 1 января 1909 года входила, в частности, и координация деятельности Департамента полиции. С организацией новых 89 сыскных отделений П. А. Столыпин поручает группе чиновников министерства под руководством А. А. Макарова подготовить служебную инструкцию для сотрудников уголовного розыска, регламентирующую их деятельность. Законом «Об организации сыскной части» от 6.07.1908 г. определялись задачи службы – «производство розыска по делам общеуголовным». Позднее «Инструкцией чинам сыскной полиции» от 9.08.1910 г. была уточнена цель её деятельности – «негласное расследование и производство дознания в виде предупреждения, устранения, разоблачения и преследования преступных деяний общеуголовного характера» (ст. 1 п. а). А. А. Макаров как

опытный юрист, профессионал, чиновник государственного мышления понимал, что для сотрудников уголовного розыска необходимо расширенное изложение цели и задач их работы. По этой причине термины и понятия «предупреждение», «устранение», «разоблачение» и «преследование» неоднократно употреблялись в тексте инструкции, преследуя цель акцентировать внимание чинов уголовного розыска на необходимость их выполнения по ходу службы.

Статья 6 Инструкции оговаривала, что исполнение поручений судебной власти (следователя) при «исследовании преступлений» (расследовании) сотрудники сыскных отделений руководствуются ст. 258 Устава уголовного судопроизводства (УУС). Данная норма определяла процессуальный порядок ведения протоколов следственных действий. Выполнение указаний прокуроров могли производиться как устно, так и письменно.

Следует отметить, что ряд терминов и понятий в Законе «Об организации сыскной части» от 6.07.1908 г. и «Инструкции чинам сыскных отделений», утвержденных главой МВД П. А. Столыпиным, восприняты УПК РФ и Законом «Об оперативно-розыскной деятельности» и действуют в современной России. К примеру, «устранение» – пресечение, «разоблачение» – раскрытие, «преследование» – комплекс оперативно-розыскных мероприятий и следственных действий. Уместно вспомнить, что только в 1950 году, спустя 50 лет, при определении предмета советской криминалистики А. И. Винберг использовал термин и понятие «предупреждение преступлений» [4].

А. А. Макаров в 1911 году был назначен товарищем министра внутренних дел, в 1912 – 1917 гг. являлся членом Государственного совета по назначению, а с 7 июля по 20 декабря 1916 г. – министром юстиции. Должность министра юстиции, «требующая беспристрастия, порядочности, спокойствия, как нельзя больше подходила к характеру Макарова. Несколько суховатый и формальный для практического деятеля, Макаров как представитель Судебного ведомства в Совете министров был на своем месте и приобрел здесь большой авторитет» [10]. Он был уволен с должности, так как планировал возбудить дело против авантюриста Манусевича – Мануйлова И. Ф. из окружения Г. Распутина. «Назначение Добровольского на место честного и безупречного Макарова вызвало прямой ропот в обществе» [10].

Неоценимый вклад внесли члены Русской группы и в развитие судебных экспертиз в Российской империи в этот период времени. Были организованы Центральное дактилоскопическое бюро (1906 г., руководитель – Н. Ф. Лучинский) и Кабинет научно-судебной экспертизы в Александровской военно-юридической академии (1912 г., организатор – С. Н. Трегубов, заместитель руководителя – С. М. Потапов). По инициативе Министра юстиции Щегловитова 28 июня 1912 года был принят закон «Об учреждении кабинета научно-судебной экспертизы при прокуроре Санкт-Петербургской судебной палаты», а Законом от 4 июля 1913 года создано ещё три аналогичных кабинета при прокурорах судебных палат в Москве, Киеве и Одессе. В результате в 1912-1913 годах появилась возможность реализовать итоги специализированных исследований в процессе расследования преступлений. Этому способствовала и «Инструкция управляющему кабинетом научно-судебной экспертизы при прокуроре Судебной палаты», утверждённая Министром юстиции 3 ноября 1912 г., которая детализировала деятельность учреждения и экспертов. Примечательно, что была предусмотрена возможность производства судебных экспертиз и для нужд гражданского судопроизводства, но на платной основе.

4. Подготовка кадров и преподавание криминалистики в высших учебных заведениях. Благодаря участию руководителей властных структур в работе общества, организовывались командировки сотрудников правоохранительных органов для ознакомления с научными и практическими достижениями в области криминалистики в страны, где существовал успешный практический опыт борьбы

с преступностью. В 1911 году под руководством действительного члена Санкт-Петербургского юридического общества С. Н. Трегубова, занимавшего в 1910-1917 гг. различные должности в Министерстве юстиции (старшего юрисконсульта, директора первого департамента), группа высокопоставленных судебных деятелей из разных судебных округов России была откомандирована Министром юстиции в Лозанну, где они прослушали лекции профессора А. Рейсса по криминалистике. Кроме того, среди слушателей был и С. М. Потапов – будущий основоположник советской криминалистики. По результатам этой поездки С. Н. Трегубовым были обработаны конспекты лекций 16 слушателей (занятия проводились на французском языке) и издан курс лекций А. Рейсса [15]. Позднее в 1915 году С. Н. Трегубов переработал лекционный курс Рейсса, «исправил ошибки и недочеты» (как сам писал в предисловии) и «внес казавшиеся полезными довольно значительные дополнения и новые отделы». В результате чего вышло в свет одно из первых в России руководств по практической криминалистике – «Основы уголовной техники. Научно-технические приемы расследования преступлений». Примечательно, что 900 экземпляров издания были бесплатно разосланы судебным следователям России для использования в практической деятельности.

В структуре издания просматриваются основы будущей системы науки. Так, *работа содержит основные положения криминалистической техники* (следы ног человека; следы пальцев – дактилоскопические отпечатки; следы разного рода – животных, колес, зубов, волос, орудий взлома; роль полицейских собак по розыску по следу; подлоги документов; подделка ценных бумаг и денежных знаков; применение ультрафиолетовых лучей; криминалистическая фотография; словесный портрет и другие), *криминалистической тактики* (следственные действия на месте преступления, производство обысков), *криминалистической методики* (расследование пожаров и поджогов, расследование железнодорожных крушений). Заметим, что С. Н. Трегубов, будучи экстраординарным профессором Военно-юридической Академии и преподавателем Императорского училища правоведения, впервые в России прочитал в этих заведениях курс криминалистики в 1911-1912 учебном году. Сам Рудольф Арчибальд Рейсс в мае 1912 года был приглашен в Россию Министром юстиции и Военным министром для прочтения в Петербурге ряда лекций для работников военно-судебного ведомства и слушателей Александровской Военно-юридической академии. В 1908 году им был создал при Лозаннском университете Институт криминалистики (Institut de police scientifique), существующий и по сей день, который начал готовить дипломированных криминалистов («Diplome de police scientifique»).

К заслуживающим внимания вопросам, рассматривавшимся на конгрессах Международного союза криминалистов, следует отнести и вопросы подготовки юристов. В частности, на конгрессе в Линце 13 августа 1895 года была принята резолюция о подготовке криминалистов-практиков. В ней было сказано: «С целью сделать более совершенной подготовку юристов и специально для того, чтобы больше подготовить их к практике, признается желательным не ограничивать образования их занятиями уголовным законом. Но желательно посредством установления необязательных курсов в университетах или специальных курсов для юристов-практиков распространить более глубокие и полные сведения об общих причинах преступления, признаках преступного мира и лучших способах выполнения наказания. Союз поручает своему бюро сделать доклад об образовательных учреждениях по криминалистике в различных странах и о способах установления такого образования» [8].

На съезде выступил Г. Гросс с докладом, посвященном обучению будущих юристов, «подготовке юристов-практиков». «Отец криминалистики», как его назвали именно на этом съезде, впрочем, ограничился сугубо практическими вопросами будущей профессиональной

деятельности, игнорируя при этом научные основы криминалистики и считая достаточным комплекс рекомендаций по расследованию уголовных дел. Содокладчиком по этому вопросу был И. Я. Фойницкий, который не согласился со своим коллегой, считая, что у этой дисциплины должна быть научная основа, теоретическая база. При всём уважении к Г. Гроссу как опытному следователю, сумевшему гармонично объединить основные положения криминалистики в единый литературный труд, ему недоставало научной эрудиции юриста, кругозора исследователя проблемы, да и педагогического опыта. К этой проблеме он подошел упрощенно. Российский педагог и ученый в своем курсе уголовного судопроизводства следующим образом определил новую науку: «криминалистика как учение о внешних следах и способах преступлений покоится на выводах самых различных прикладных наук» [14]. В этой же работе подчеркивается и значение вещественных доказательств. Важность «доказательственного материала уголовных дел заключается не в признании подсудимого, прямых свидетельских показаниях, а в признаках объективных, внешних или внутренних доказательств, доставленных нам самим делом» [14, с. 204]. Понимая важность научного подхода к расследованию преступлений, И. Я. Фойницкий даже в своем «Курсе уголовного судопроизводства» отмечает: «Криминалистика как учение о внешних следах и способах преступлений покоится на выводах самых разнообразных прикладных наук – токсикологии, химии (например, исследование пятен крови), лингвистики (воровской жаргон), фотографии (судебная фотография) и проч. Особые её отделы составляют так называемая «криминальная тактика», или учение о методах раскрытия преступлений, и учение о способах отождествления преступников, которое в свою очередь распадается на антропометрию (Бертильон), дактилоскопию (отождествление по отпечаткам концов пальцев – Гальтон), отождествление по лицевым признакам (словесный портрет). Конечно, все эти технические приемы вряд ли могут претендовать на звание науки, но ознакомление с ними может быть небезынтересно и для криминалиста-теоретика… Техника исследования вещественных доказательств в настоящее время достигла такого развития, что некоторые считают необходимым ввести её на юридических факультетах как особый предмет преподавания под именем криминалистики» [14, С. 306-307]. При этом автор ссылается на Руководство для судебных следователей Г. Гросса в переводе Л. Дудкина и Б. Зиллера (Смоленск, 1895-1897) и указывает, что «в таком духе высказался и Линцский конгресс Союза уголовного права в 1897 году».

Интерпретируя Ганса Гросса с позиций сотрудника уголовного розыска того времени, В. И. Лебедев заключает, что «ни уголовное право, ни уголовный процесс не дают нам указаний для успешного ответа … на вопросы, к разрешению которых сводится сущности деятельность по раскрытию преступлений. Какими именно способами совершаются преступления, какие бывают их мотивы и цели, как эти способы исследовать и их раскрывать, как изыскать те или другие доказательства, как дойти до них, их сохранить и использовать. Криминалистика (научная полиция) как «новая наука разрабатывает «методы обнаружения и исследования различных следов (рук, ног), выяснение виновников преступления, регистрации преступников и установки самоличности, приемы уголовного дознания, расспросы сведущих лиц и свидетелей, допросов обвиняемых и, наконец, особые методы расследования некоторых категорий преступлений профессионального свойства – словом, рассматриваются и систематизируются приемы уголовного сыска, целью которого является раскрытие преступления и выяснение истины происшедшего» [6].

Член юридического общества и Русской группы Международного союза криминалистов А. А. Левенстим, являясь

одним из руководящих лиц сообщества, в 1895 году поместил в Журнале министерства юстиции № 5 (с.132-166) изложение работы Г. Гросса «Практическое следствие по руководству д-ра Г. Гросса». Позже фрагменты отдельных глав публиковались в 1899 году в еженедельной газете «Право». Положительно оценивая объемный труд криминалиста, автор акцентировал внимание на отдельных главах монографии – допросах свидетелей и обвиняемых; значении судебной фотографии как источника точной и полной фиксации; деятельности эксперта; значении дактилоскопии. Таким образом, юридическая общественность России и сотрудники правоохранительных органов были ознакомлены с идеями «отца криминалистики» вскоре после выхода его труда в свет.

Заключение. В Русской группе Международного союза криминалистов после киевского съезда 1905 года произошел раскол, снизивший интенсивность её деятельности. В результате сменился председатель группы, длительное время не собирались съезды. На фоне революционных событий внутри страны и сложностей в международном окружении России деятельность группы начала угасать и фактически была свернута в 1914 году. Однако следует констатировать, что тот потенциал, который был наработан в годы деятельности, дал столь сильный стимул для развития криминалистики, что до 1917 года по инерции продолжали совершенствоваться криминалистические методы и их внедрение в деятельность следствия и полиции, развивались экспертные учреждения и уголовные учеты, появлялись методические рекомендации по раскрытию и расследованию преступлений. Некоторые из героев этой статьи продолжили свою службу в правоохранительных органах и занятия научной деятельностью и после Октябрьской революции, что, в свою очередь, способствовало зарождению и развитию такого феномена, как «советская криминалистика».

Список литературы

1. Галяшина Е. И. Криминалистика в многополярном мире: конкуренция или сотрудничество? // Формирование многополярного мира: вызовы и перспективы. Сборник докладов XI Московского юридического форума: в 3 частях. Ч. 3. – М.: Изд. Центр Университета имени О.Е. Кутафина (МГЮА), 2024. С. 439 ─443.

2. Кашепов В. П., Фойницкий И. Я. // История русской правовой мысли. Биографии, документы, публикации. М.: Издательство Остожье. 1998. – 603 с.

3. Корниенко Н. А. Первый Международный конгресс судебной (уголовной) полиции // КриминалистЪ. 2024. № 1 (46). С. 43 —48.

4. Криминалистика: учебник для юридических вузов. М., 1950.

5. Кулишер Е. М. Юбилей союза криминалистов // Право. 1914. № 4. С. 263 — 265.

6. Лебедев В. И. Искусство раскрытия преступлений. I. Дактилоскопия (Пальцепечатание). СПб.: Типография отдельного штаба корпуса жандармов, 1912. 2 изд., испр. и доп.

7. Люблинский П. И. Памяти И. Я. Фойницкого // Журнал Министерства народного просвещения. Новая серия. 1914. № 4. С. 45 —69.

8. Люблинский П.И. Международные съезды по вопросам уголовного права за десять лет (1905-1915). Петроград. Сенатская типография. 1915. С. 158.

9. Першин А. Н. Аддитивные технологии: новый шаг к трансформации криминалистических знаний // Формирование многополярного мира: вызовы и перспективы. Сборник докладов XI Московского юридического форума: в 3 частях. Ч. 3. – М.: Изд. Центр Университета имени О.Е. Кутафина (МГЮА), 2024. С. 482 —485.

10. Покровский Н. Н. Последний в Мариинском дворце: Воспоминания министра иностранных дел. М.: Новое литературное обозрение, 2015. – 488 с.

11. Соколов А. Указатель русской юридической литературы. Вильна. Типография И. Блюмовича 1896. Приложение к

«Практическому руководству для Судебных следователей».

12. Фойницкий И. Я. Международный союз уголовного права. СПб, 1890. – 24 с.

13. Фойницкий И. Я. Международный союз уголовного права. СПб, 1896.

14. Фойницкий И. Я. Курс уголовного судопроизводства. Т.1, Т.2. / Под ред. А.В. Смирнова СПб.: Альфа, 1996. 607 с. Печатается по третьему изданию, СПб., 1910.

15. Рейсс, Р. А. Научная техника расследования преступлений: Курс лекций, прочтен. в г. Лозанне проф. Рейссом чинам рус. судеб. ведомства летом 1911 г / Сост. под ред. С.Н. Трегубова. СПб.: Сенатская тип., 1912. — 206 с.

References

1. Galyashina E. I. Criminalistics in a multipolar world: competition or cooperation? // Formation of a multipolar world: challenges and prospects. Collection of reports of the XI Moscow Law Forum: in 3 parts. Part 3. Moscow: Publishing House of the O.E. Kutafin University Center (MGUA), 2024. pp. 439 —443.

2. Kashepov V. P., Foynitsky I. Ya. // History of Russian legal thought. Biographies, documents, publications. Moscow: Ostozhye Publishing House. 1998. – 603 p.

3. Kornienko N. A. The First International Congress of judicial (criminal) police // Criminalist. 2024. No. 1 (46). pp. 43 —48.

4. Criminalistics: textbook for law schools. Moscow, 1950.

5. Kulisher E. M. Jubilee of the Union of Criminalists // Law. 1914. No. 4. pp. 263 — 265.

6. Lebedev V. I. The art of crime detection. I. Fingerprinting. St. Petersburg: Printing house of the separate headquarters of the gendarmerie corps, 1912. 2nd ed., ispr. and add.

7. Lyublinsky P. I. In memory of I. Ya. Foynitsky // Journal of the Ministry of National Education. A new series. 1914. No. 4. pp. 45 —69.

8. Lyublinsky P. I. International congresses on criminal law for ten years (1905-1915). - Petrograd, Senate Printing House, 1915

9. Pershin A. N. Additive technologies: a new step towards the transformation of forensic knowledge // Formation of a multipolar world: challenges and prospects. Collection of reports of the XI Moscow Law Forum: in 3 parts. Part 3. Moscow: Publishing House of the O.E. Kutafin University Center (MGUA), 2024. pp. 482 —485.

10. Pokrovsky N. N. The Last One in the Mariinsky Palace: Memoirs of the Minister of Foreign Affairs. Moscow: New Literary Review, 2015. 488 p.

11. Sokolov A. Index of Russian legal literature. Vilna. Printing house of I. Blumovich 1896. Appendix to the "Practical Guide for Judicial Investigators".

12. Foynitsky I. Ya. International Union of Criminal Law. St. Petersburg, 1890. – 24 p.

13. Foynitsky I. Ya. International Union of Criminal Law. St. Petersburg, 1896.

14. Foynitsky I. Ya. Course of criminal proceedings. Vol.1, Vol.2. / Edited by A.V. Smirnov St. Petersburg: Alpha, 1996. 607 p.

15. Reiss, R. A. Scientific technique of crime investigation: A course of lectures delivered in Lausanne by Prof. According to the ranks of Russian destinies. departments in the summer of 1911 / Comp. edited by S.N. Tregubov. St. Petersburg: Senatskaya tip., 1912. — 206 p.

Информация об авторах

С. П. Кушниренко — доцент кафедры уголовного процесса и криминалистики Санкт-Петербургского государственного университета, кандидат юридических наук, доцент.

Н. А. Корниенко — кандидат юридических наук, доцент, почетный работник прокуратуры Российской Федерации.

Information about the authors

S. P. Kushnirenko — Associate Professor of the Department of Criminal Procedure and Criminalistics at St. Petersburg State University, Candidate of Law, Associate Professor.

N. A. Kornienko — Candidate of Law, Associate Professor, Honorary Employee of the Prosecutor's Office of the Russian Federation.

Вклад авторов

Н. А. Корниенко — концепция и дизайн исследования, сбор и анализ полученных данных;

С. П. Кушниренко — сбор, обработка и анализ полученных данных, написание текста.

Contribution of the authors

N. A. Kornienko — research concept and design, data collection and analysis;

S. P. Kushnirenko — data collection, processing and analysis, text writing.

УДК 340
ББК 67.4

Обеспечение информационной безопасности в современных условиях

Александр Васильевич Шаров
Московский университет МВД России имени В. Я. Кикотя, Москва, Россия
Email: a13sharidze@yandex.ru.

Аннотация. В статье рассматриваются уровни информационных угроз в зависимости от охвата территории и сфер государственной и общественной жизни, а также противопоставляемые им меры обеспечения информационной безопасности.
Ключевые слова: уровень информационной угрозы, обеспечение информационной безопасности.
Научная специальность: 5.1.2. Публично-правовые (государственно-правовые) науки
Для цитирования: Шаров А.В. Обеспечение информационной безопасности в современных условиях // Мир криминалистики. 2025. № 1. С. 120-124

Ensuring information security in modern conditions

Alexander V. Sharov
Moscow University the Ministry of Internal Affairs of Russia named after V.Ya. Kikot, Moscow, Russia
Email: a13sharidze@yandex.ru.

Abstract. The article examines the levels of information threats depending on the coverage of the territory and spheres of state and public life, as well as information security measures opposed to them.
Keywords: information threat level, information security.
For citation: Sharov A.V. Ensuring information security in modern conditions // The world of criminology. 2025;(1):120-124

Введение. Решение проблем, связанных с современными вызовами и угрозами, предполагает постановку определенных задач, продиктованных уровнем таких угроз. Несомненно, одной из первостепенных в этом ряду является информационная безопасность, которой уделено значительное внимание в сфере государственного управления. Определение уровней информационных опасностей позволит правильно понять потенциальный вред общественным отношениям.

Основная часть. Выделяемые уровни предполагаемых опасностей соответствуют системе построения межгосударственных отношений, а также принципам функционирования национальных институтов страны и общества.

По уровню охвата территории можно выделить следующие уровни с условными названиями:

1) *конвенциональный* – предполагает признание проблемы и выработку соответствующего юридически обязывающего документа на уровне Организации Объединенных Наций (далее − ООН);

2) *межгосударственный* – на уровне надгосударственных и государственных объединений на определенной территории: Союзного государства России и Беларуси, государств – участников Содружества Независимых Государств, Шанхайской организации сотрудничества, Организация Договора о коллективной безопасности, объединения государств БРИКС и т. п.;

3) *государственный* − в рамках конкретного государства.

В рамках международных отношений необходимым, определяющим и обязывающим документом могла бы стать специальная конвенция ООН об информационной безопасности (далее − Конвенция).

Концепцию соответствующего документа Российская Федерация представила еще в 2023 году[1], подтверждая последовательный подход к построению отношений на основе взаимного уважения и доверия.

В 2021 году в докладе авторского коллектива Московского государственного института международных отношений (университета) Министерства иностранных дел Российской Федерации (МГИМО) была указана «Триада угроз» международной информационной безопасности, предполагающая атаки на объекты критической инфраструктуры государств , а также использование информационно-телекоммуникационных технологий в военно-политических, террористических или преступных целях[2].

Авторы документа правильно определили направления угроз. Следует отметить, что в современных условиях фактического противостояния России и недружественных государств в сфере информационных технологий видится невозможным принятия Конвенции даже в среднесрочной перспективе. Кроме того, общеизвестны примеры фактически государственного информационного вмешательства отдельных стран в дела других государств. Достаточно рассмотреть деятельность корпорации Мета Платформс Инк[3], анонимной сети виртуальных туннелей Тор[4], созданной при поддержке государственных, в том числе военных, структур США и другие.

Особенно показательным следует признать случай организации Израилем 17 и 18 сентября 2024 года в Ливане и Сирии массовых покушений на жизнь и здоровье членов организации «Хезболла». Израиль продемонстрировал действительную силу современных информационных технологий в реализации планов государства по борьбе с его врагами, в том числе таким способом. Следует отметить, что указанный подход стал возможным не только путем реализации непосредственно информационных технологий, но и путем применения, хотя и неявно, методов социальной инженерии. В этом же ряду стоит программное обеспечение «Пегас»[5], распространяемое израильской компанией для обеспечения скрытого наблюдения за определенными лицами.

Конечно, в рамках возможного сотрудничества на уровне ООН можно упомянуть Конвенцию Организации Объединенных Наций против транснациональной организованной преступности, принятую резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года. Однако межгосударственное взаимодействие на основе взаимного уважения и невмешательства возможно только с принятием Конвенции ООН по международной информационной безопасности. В условиях современной международной ситуации реализовать предлагаемую Россией и другими государствами Конвенцию фактически нереально.

Несколько иная ситуация сложилась в сфере отношений отдельных государств в рамках двухсторонних и многосторонних

1 О концепции ООН по международной информационной безопасности. // Официальный сайт Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf (дата обращения: 02.02.2025). 15 мая Россия в соавторстве с Белоруссией, КНДР, Никарагуа и Сирией внесла концепцию конвенции ООН об обеспечении международной информационной безопасности (МИБ) в качестве официального документа 77-й сессии Генеральной Ассамблеи ООН. // Официальный сайт Министерства иностранных дел Российской Федерации. URL:https://www.mid.ru/ru/foreign_policy/news/1870609/ (дата обращения: 02.02.2025).

2 Международная информационная безопасность: подходы России / А.В. Крутских, Е.А. Зиновьева, В.И. Булва, М.Б. Алборова, Ю.А. Юдина; под ред. А.В. Крутских, Е.С. Зиновьева. Москва, 2021. 48 с. Текст: непосредственный. URL: https://mgimo.ru/library/ publications/mezhdunarodnaya-informatsionnaya-bezopasnost-podkhody-rossii/ (дата обращения: 02.02.2024). С. 6–9.

3 Meta Platforms, Inc. (Meta, до 28 октября 2021 года — Facebook Inc.) – признана экстремисткой организацией 21 марта 2022 года Тверским судом г. Москвы, 11 октября 2022 года Росфинмониторинг внес компанию Meta в перечень организаций причастных к терроризму и экстремизму.

4 Tor (англ. The Onion Router) – системы прокси-серверов, устанавливающее анонимное сетевое соединение.

5 Pegasus – шпионское программное обеспечение израильской компании NSO Group.

договоров России и других государств. Прежде всего, в рамках Союзного государства России и Республики Беларусь следует принять во внимание соответствующее Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь[6]. Указанный документ наглядно показывает возможности сотрудничества государств в области противодействия основным угрозам международной информационной безопасности, определяет общие принципы и основные направления сотрудничества, формы и механизмы его реализации и т. д.

Отдельно стоит отметить концептуальную терминологию и определения в этой сфере, которые необходимо применять и в национальном законодательстве с целью построения стройной системы правоотношений и обеспечения единообразия правоприменительной практики, приведенные в Приложении 1 указанного документа.

В Российской Федерации на государственном уровне предпринимаются значительные усилия в сфере обеспечения информационной безопасности. Обновленная Доктрина информационной безопасности Российской Федерации[7] (далее – Доктрина) определяет отношение нашей страны к указанной проблеме и предлагает не только связанные с этим понятия и определения, но и направления развития общества и государства. Она же выступает в качестве документа стратегического планирования, в котором развиваются положения Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. № 683, а также других документов стратегического планирования в указанной сфере.

Также обозначена иерархия соответствующих нормативных правовых актов, регулирующих эту сферу (пункт 4 Доктрины), и определены задачи – формирование государственной политики и развития общественных отношений, а также выработка мер по совершенствованию системы обеспечения информационной безопасности (пункт 6 Доктрины) и защите национальных интересов Российской Федерации (пункт 8 Доктрины).

В рамках государственного обеспечения информационной безопасности по сферам реализации Доктрины можно выделить деятельность государственных и негосударственных организаций, а также общественных объединений и граждан.

Наряду с технологической составляющей информационной безопасности следует обозначить психологическую. В первом случае вполне справедливо можно признать отсутствие, к сожалению, технологического суверенитета России при использовании информационных технологий и оборудования. В этом направлении, во-первых, определены пути достижения необходимого уровня независимости; во-вторых, скорейшее построение государственной системы защиты информации; и наконец, обеспечение достаточности правового регулирования указанной сферы. Принимать участие в формировании государственной политики должны не только государственные органы, но и бизнес-сообщество, а также граждане и общественные объединения.

В области психологической составляющей нельзя не упомянуть формирование устойчивости населения и адекватное реагирование на «противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание» (раздел 2 Доктрины). Пожалуй в настоящее время это одно из важнейших направлений обеспечения государственной политики в области обеспечения

6 Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности // Официальный сайт Министерства иностранных дел Российской Федерации. URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international contracts/2_contract/44274/ (дата обращения: 02.02.2025).

7 Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». // Kremlin.ru. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 02.02.2025).

информационной безопасности государства наряду с совершенствованием законодательства, на что совершенно справедливо указывают Т.А. Полякова и Н.А. Троян[8].

Здесь так же, как и при освещении уровней обеспечения информационной безопасности, можно выделить свои направления реализации. Прежде всего, повсеместная широкая пропаганда «информационной гигиены». На уровне населения и организаций практически невозможно осуществить кибератаку без применения методов социальной инженерии. Статистика преступлений и описание их способов говорит именно об этом. Чисто технологические атаки труднореализуемы и возможны, скорее всего, только на государственном уровне по типу упомянутых израильских технологий с внедрением опасных «закладок» без участия жертв, то есть на уровне изготовления и поставок оборудования.

С другой стороны, наряду с освещением проблемы применения методов социальной инженерии следует обеспечить соответствующее обучение и просвещение в образовательных учреждениях, а, с учетом возраста современного пользователя, и дошкольных учреждениях.

В рамках предпринимательской деятельности и неполной правовой урегулированности сферы, особую тревогу вызывает обеспечение сохранности персональных данных операторами таких данных, к которым, вместе с государственными организациями, относятся и негосударственные. Представляется, что проверка государственными органами таких субъектов не должно подпадать под мораторий на проверку предпринимательской деятельности, так как эта деятельность напрямую обеспечивает личную информационную безопасность. Это же касается, например, операторов сотовой связи, которые относятся к критической инфраструктуре государства.

В каждом случае частному лицу следует подробно изучать политику организации, в которую персональные данные представляются, особенно в части передачи этих данных партнерам оператора.

Заключение. Таким образом, в современных условиях определяются следующие уровни информационных угроз по охвату территории: конвенциональный, межгосударственный и государственный. Последний по сферам реализации можно подразделить на деятельность государственных и негосударственных организаций, а также общественных объединений и граждан.

Наряду с технологической составляющей реализации информационной безопасности в нашей стране можно выделить психологическую, направленную на формирование у населения устойчивого негативного отношения к методам социальной инженерии путем проведения образовательных и воспитательных мероприятий.

Список источников

1. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности. // Официальный сайт Министерства иностранных дел Российской Федерации. URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/44274/ (дата обращения: 02.02.2025).

2. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». // Kremlin.ru. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 02.02.2025).

8 Полякова Т.А. Обеспечение суверенитета в информационном пространстве − стратегическая задача национальной политики / Т.А. Полякова, Н.А. Троян // Правовая политика и правовая жизнь. 2024. № 1. С. 41-53. DOI 10.24412/1608-8794-2024-1-41-53.

3. О концепции Конвенции ООН по международной информационной безопасности. //Официальный сайт Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf (дата обращения: 02.02.2025).

4. Международная информационная безопасность: подходы России / А.В. Крутских, Е.А. Зиновьева, В.И. Булва, М.Б. Алборова, Ю.А. Юдина; под ред. А.В. Крутских, Е.С. Зиновьева. − Москва, 2021. − 48 с. − Текст: непосредственный. URL: https://mgimo.ru/library/publications/mezhdunarodnaya- informatsionnaya-bezopasnost-podkhody-rossii/ (дата обращения: 02.02.2-24).

5. Полякова, Т.А. Обеспечение суверенитета в информационном пространстве − стратегическая задача национальной политики / Т.А. Полякова, Н.А. Троян // Правовая политика и правовая жизнь. – 2024. – № 1. – С. 41-53. – DOI 10.24412/1608-8794-2024-1-41-53.

References

1. Agreement between the Government of the Russian Federation and the Government of the Republic of Belarus on cooperation in the field of international information security. Ministry of Foreign Affairs of the Russian Federation. Website. URL:https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/2_contract/44274 / (accessed: 02.02.2025).

2. Decree of the President of the Russian Federation dated 05.12.2016 No. 646 "On Approval of the Information Security Doctrine of the Russian Federation". The President of Russia. Website. URL: http://www.kremlin.ru/acts/bank/41460 (accessed: 02.02.2025).

3. On the concept of the UN Convention on International Information Security. The Security Council of the Russian Federation. Website. URL: http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf (accessed: 02.02.2025).

4. International information security: approaches of Russia / A.V. Krutskikh, E.A. Zinovieva, V.I. Bulva, M.B. Alborova, Yu.A. Yudina; edited by A.V. Krutskikh, E.S. Zinoviev. − Moscow, 2021. − 48 p. − Text: direct. URL: https://mgimo.ru/library/publications/mezhdunarodnaya-informatsionnaya-bezopasnost-podkhody-rossii / (accessed: 02.02.2-24). – pp. 6-9.

5. Polyakova, T. A. Ensuring sovereignty in the information space is a strategic task of national policy / T. A. Polyakova, N. A. Troyan // Legal policy and legal life. – 2024. – No. 1. – pp. 41-53. – DOI 10.24412/1608-8794-2024-1-41-53.

Информация об авторе

А.В. Шаров — начальник кафедры криминалистики Московского университета МВД России, кандидат юридических наук, доцент.

Information about the author

A.V. Sharov - the Head of the Criminology Department at the Kikot Moscow University of the Ministry of Internal Affairs of Russia, Candidate of Law, Associate Professor.