Научная статья
УДК: 343.98.06+343.97

АНАЛИЗ ПРОБЛЕМ РАСКРЫТИЯ IT-ПРЕСТУПЛЕНИЙ И НАПРАВЛЕНИЯ ИХ ПРЕОДОЛЕНИЯ

Виктория Александровна Родивилина[1], Вячеслав Валентинович Коломинов[2]
[1]Восточно-Сибирский институт МВД России, г. Иркутск, Российская Федерация, 377b@bk.ru
[2]Институт государства и права Байкальского государственного университета, г. Иркутск, Российская Федерация, kolominovVV@bgu.ru

Аннотация. Статья посвящена исследованию актуальных проблем раскрытия преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, и анализу направлений повышения эффективности деятельности правоохранительных органов в данной сфере. Авторы обращают внимание на устойчивый рост числа IT-преступлений в России. В работе выделяются ключевые факторы, препятствующие эффективному расследованию: использование злоумышленниками технологий анонимизации и зашифрованных каналов связи, применение искусственного интеллекта в преступных целях, затрудненное взаимодействие правоохранительных органов с операторами связи, кредитными организациями и криптовалютными сервисами, недостаток квалифицированных специалистов и современных технических средств, а также трансграничный характер киберпреступности. В каждом из направлений анализируются научные позиции и нормативные предпосылки, приводятся аргументы о необходимости законодательных изменений. Особое внимание уделяется вопросам совершенствования нормативно-правовой базы, включая внедрение механизмов оперативного блокирования мошеннических сервисов, создание государственного реестра VPN-платформ, а также развитию цифровой криминалистики как самостоятельного направления. Авторы акцентируют важность оснащения следственных органов современными средствами фиксации электронно-цифровых следов, формирования специализированных подразделений по цифровой криминалистике и создания единой методики работы с цифровыми доказательствами. В статье обосновывается, что преодоление перечисленных проблем невозможно без комплексного подхода, сочетающего правовые, организационные и технологические меры. Перспективным направлением названы расширение международного сотрудничества, заключение двусторонних соглашений о совместном расследовании и использование лучших практик зарубежных государств. В заключение подчеркивается, что эффективное противодействие IT-преступности требует не только совершенствования уголовного законодательства, но и институционального укрепления взаимодействия

государства и частного сектора, а также развития кадрового потенциала в области цифровой криминалистики.

Ключевые слова: IT-преступления, киберпреступность, раскрытие преступлений, цифровая криминалистика, международное сотрудничество, анонимизация, мошенничество, искусственный интеллект

Для цитирования: Родивилина, В. А., Коломинов В. В. Анализ проблем раскрытия IT-преступлений и направления их преодоления // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России // Криминалистика: вчера, сегодня, завтра. 2025. Т. 35. № 3. С. 119–130.

ANALYSIS OF THE PROBLEMS OF SOLVING IT-RELATED CRIMES AND WAYS TO OVERCOME THEM

Victoria A. Rodivilina[1], Vyacheslav V. Kolominov[2]
[1]East Siberian institute of the MIA of Russia, Irkutsk, Russian Federation, 377b@bk.ru
[2]Institute of State and Law Baikal State University, Irkutsk, Russian Federation, kolominovVV@bgu.ru

Abstract. The article is devoted to the study of current issues in the detection of crimes committed using information and telecommunication technologies, as well as to the analysis of ways to improve the efficiency of law enforcement activities in this area. The authors draw attention to the steady increase in the number of IT crimes in Russia. This indicates the presence of serious systemic difficulties in investigations, which require the adaptation of traditional forensic methods to the conditions of the digital environment. The paper highlights key factors hindering effective investigations: the use of anonymization technologies and encrypted communication channels by offenders; the application of artificial intelligence for criminal purposes; the difficulties faced by law enforcement agencies in cooperating with telecommunications operators, financial institutions, and cryptocurrency services; the shortage of qualified specialists and modern technical tools; as well as the transnational nature of cybercrime. In each of these areas, scientific positions and regulatory prerequisites are analyzed, and arguments are made regarding the necessity of legislative amendments. Particular attention is paid to improving the regulatory framework, including the introduction of mechanisms for the prompt blocking of fraudulent services, the creation of a state register of VPN platforms, and the development of digital forensics as an independent field. The authors emphasize the importance of equipping investigative bodies with modern tools for recording electronic-digital traces, establishing specialized digital forensics units, and creating a unified methodology for working with digital evidence. The article argues that overcoming the above-mentioned problems is impossible without a comprehensive approach that combines legal, organizational, and technological measures. Promising directions include the expansion of international cooperation, the conclusion of bilateral agreements on

joint investigations, and the adoption of best practices from foreign states. In conclusion, it is stressed that effective counteraction to IT crime requires not only the improvement of criminal legislation but also the institutional strengthening of cooperation between the state and the private sector, along with the development of human resources in the field of digital forensics.

Keywords: IT crimes, cybercrime, crime detection, digital forensics, international cooperation, anonymization, fraud, artificial intelligence

For citation: Rodivilina, V. A., Kolominov, V. V. Analiz problem raskrytiya IT-prestuplenii i napravleniya ikh preodoleniya [Analysis of the problems of solving IT crimes and ways to overcome them]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2025, vol. 35 no. 3, pp. 119–130 (in Russ.).

Введение

Актуальность темы обусловлена включением противодействия IT-преступлениям в приоритетные направления государственной политики в сфере безопасности и цифровой трансформации[1]. Современное развитие информационных технологий привело к росту преступности в киберпространстве. За первое полугодие 2025 года из всех зарегистрированных на территории Российской Федерации преступлений свыше 40 % совершенны с использованием информационно-телекоммуникационных технологий, причем число таких деяний увеличилось на приблизительно 0,7 % по сравнению с аналогичным периодом 2024 года. Несмотря на незначительный рост числа зарегистрированных IT-преступлений, процент расследованных уголовных дел оставался крайне низким[2]. Это свидетельствует о наличии системных проблем в работе правоохранительных органов, требующих детального изучения и совершенствования существующих методик расследования.

Как отмечает А. Б. Смушкин, эффективность расследования IT-преступлений во многом зависит от уровня подготовки следователей в области цифровой криминалистики, а также их доступа к современным аналитическим инструментам [1, с. 42]. Аналогичной позиции придерживается ряд авторов, указывая, что нехватка специалистов в области цифровой криминалистики приводит к значительным пробелам в расследовании преступлений [2, с. 70].

Целью настоящей статьи является комплексный анализ причин

[1] О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы : Указ Президента Российской Федерации от 9 мая 2017 года № 203 // Собрание законодательства Российской Федерации. — 2017. — № 20. — Ст. 2901.

[2] МВД России опубликовало статистические сведения о состоянии преступности в первом полугодии 2025 года // МВД МЕДИА : сайт. URL: https://mvdmedia.ru/news/official/mvd-rossii-opublikovalo-statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-pervom-polugodii-2025-/mvd-media.ru/news/official/mvd-rossii-opublikovalo-statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-pervom-polugodii-2025-/ (дата обращения: 25.07.2025)

низкой эффективности расследования IT-преступлений в России и обоснование направлений совершенствования криминалистических методик в условиях цифровизации.

Основная часть

Можно выделить следующие проблемы раскрытия IT-преступлений:

1. Использование преступниками технологий, затрудняющих установление их личности. Злоумышленники активно применяют VPN-сервисы, анонимайзеры, а также мессенджеры с функцией сквозного шифрования (end-to-end encryption), такие как Telegram и Signal. Использование протоколов E2EE позволяет скрывать IP-адреса и обеспечивать недоступность содержимого переписки даже для операторов платформ. Подобные каналы связи значительно осложняют проведение оперативно-розыскных мероприятий и последующее доказывание в суде. Е. Р. Россинская указывает на необходимость пересмотра процессуальных подходов к сбору цифровых следов в условиях криптографической защиты информации [3, с. 165].

Использование средств анонимизации затрудняет установление личности преступника и его местоположение. По мнению Е. А. Русскевича, отсутствие централизованной системы мониторинга интернет-трафика осложняет контроль за преступной активностью в сети [4, с. 659-660]. Д. В. Бахтеев и А. А. Беляков в своей работе указывают, что современные технологии анонимизации требуют от правоохранительных органов создания новых методик цифровой криминалистики, адаптированных под постоянно изменяющуюся киберсреду [5, с. 93].

2. Использование искусственного интеллекта (далее – ИИ) в преступных целях. Как отмечает В. А. Тирранен, развитие технологий ИИ привело к появлению новых видов преступлений, таких как мошенничество с использованием deepfake, автоматизированные кибератаки и генерация вредоносного кода без участия человека [6, с. 12]. Проблема заключается в том, что правоприменительная практика не успевает за быстрым развитием технологий, что создает пробелы в квалификации преступлений. И. Н. Мосечкин подчеркивает, что возникновение преступлений, совершенных при участии автономных ИИ-систем, ставит под сомнение традиционные подходы к установлению субъекта преступления [7, с. 471]. В свою очередь, С. А. Аверинская и А. А. Севостьянова указывают, что создание ИИ-алгоритмов с целью злонамеренного использования должно рассматриваться как отдельный состав преступления, требующий внесения изменений в уголовное законодательство [8, с. 94]. Дополнительно следует учитывать, что преступники используют ИИ не только для активных атак, но и для разведки, социальной инженерии и обхода традиционных систем защиты, что требует интеграции ИИ и в профилактическую работу правоохранительных структур.

3. Ограниченное взаимодействие с операторами связи, кредитными организациями и криптовалютными сервисами. Важной проблемой при расследовании IT-преступлений является сложность получения информации от операторов связи, кредитных организаций и участников криптовалютного рынка. В большинстве случаев для следователей судебное решение для

доступа к указанным сведениям не требуется, однако оперуполномоченным в рамках проведения оперативно-розыскной деятельности необходимо получение судебного решения. В соответствии со ст. 26 Федерального закона от 2 декабря 1990 года № 395-1 «О банках и банковской деятельности»[3] следственные органы вправе запрашивать данные, составляющие банковскую тайну, на основании постановления следователя. Аналогично ст. 64 Федерального закона от 7 июля 2003 года № 126-ФЗ «О связи»[4] предоставляет правоохранительным органам возможность получать сведения об абонентах и соединениях в рамках возбужденного уголовного дела. За отказ в предоставлении информации предусмотрена административная ответственность по ст. 19.7 КоАП РФ. Тем не менее на практике взаимодействие с такими субъектами может быть затруднено из-за длительных сроков обработки запросов и опасений коммерческих организаций за возможные репутационные риски. Еще более серьезные сложности возникают при работе с криптовалютными сервисами и обменниками, большая часть которых зарегистрирована и функционирует за рубежом и не подчиняется российской юрисдикции. О. И. Русакова и С. А. Головань верно указывают, что комплексная программа борьбы с киберпреступностью должна включать совокупность действий как государственных структур, так и частного сектора экономики [9], что подтверждает необходимость пересмотра правовых механизмов взаимодействия. Отсутствие международных договоров с отдельными странами и анонимный характер блокчейн-технологий создают существенные препятствия для оперативного установления владельцев криптокошельков и блокировки транзакций.

4. Недостаток технических возможностей и специалистов. Раскрытие IT-преступлений требует применения аналитики больших данных, мониторинга даркнета, криптовалютных транзакций. В правоохранительных органах ощущается дефицит специалистов, обладающих необходимыми компетенциями. А. Б. Смушкин указывает, что подготовка специалистов в области цифровой криминалистики требует не только обучения традиционным методикам, но и освоения новых технологий, таких как машинное обучение и анализ блокчейн-транзакций [1, с. 83]. О. В. Савченко также подчеркивает, что низкая компьютерная грамотность следователей мешает эффективному расследованию преступлений [2, с. 71].

5. Международный характер преступлений. Часть преступлений организуется из-за рубежа, что усложняет проведение оперативно-розыскных мероприятий. Одной из ключевых проблем в таких случаях является получение данных от иностранных сервисов и правоохранительных органов других стран. Как подчеркивает Европол, без эффективной системы международного

[3] О банках и банковской деятельности : Федер. закон от 2 декабря 1990 года № 395-1 :: послед. ред. // КонсультатнтПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения: 25.07.2025).

[4] О связи : Федер. Закон от 7 июля 2003 года № 126-ФЗ : принят Гос. Думой 18 июня 2003 года : : одобрен Советом Федерации 25 июня 2003 года : : послед. ред. // КонсультатнтПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 25.07.2025).

обмена информацией расследование трансграничных преступлений становится практически невозможным[5]. Данную точку зрения поддерживают и ученые. Так, Е. М. Якимова и С. В. Нарутто отмечают, что важнейшим условием успешной борьбы с международной киберпреступностью является развитие системы двусторонних соглашений между государствами [10, с. 109]. Рост числа преступлений, совершаемых в киберпространстве, требует комплексного подхода к их расследованию и предупреждению. Однако, несмотря на значительное число трансграничных схем, Россия до сих пор не является полноценным участником ряда многосторонних соглашений, таких как Будапештская конвенция. Отказ от участия в подобных соглашениях создает дополнительные сложности: замедляется процесс получения международной правовой помощи, а правоохранительным органам приходится уделять больше внимания развитию национальных механизмов двустороннего сотрудничества. Это, в свою очередь, существенно увеличивает нагрузку на следственные и оперативные подразделения.

Учитывая изложенное, необходимо рассмотреть наиболее эффективные пути решения проблем, возникающих при расследовании IT-преступлений. В этой связи предлагаются следующие меры, направленные на совершенствование борьбы с киберпреступностью:

1. Совершенствование нормативно-правовой базы.

Адаптация уголовного законодательства к стремительно развивающейся цифровой среде становится одним из приоритетных направлений в борьбе с киберпрестностью. Как справедливо отмечает И. Н. Мосечкин, появление автономных систем с элементами искусственного интеллекта, способных совершать преступления без участия человека, требует внесения изменений в Уголовный кодекс Российской Федерации (далее – УК РФ) [7, с. 97].

Среди необходимых законодательных мер можно выделить:

– разработку механизмов оперативного блокирования мошеннических счетов и сервисов;

– внедрение системы оперативного межведомственного обмена информацией между правоохранительными органами, операторами связи, банками и финтех-сервисами. Согласно Указу Президента Российской Федерации от 9 мая 2017 года № 203[6] в рамках стратегии развития информационного общества предусматривается формирование единой цифровой инфраструктуры для борьбы с преступностью в сети. Эффективным шагом может стать введение обязательного порядка реагирования на запросы следственных органов в срок не более 24 часов с применением сертифицированных защищенных каналов связи;

[5] Исследования Европола по цифровой безопасности в контексте транснациональной преступности. – Брюссель, 2024. — Электронный ресурс. — URL: https://www.europol.europa.eu (дата обращения: 20.07.2025).

[6] О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы : Указ Президента Российской Федерации от 9 мая 2017 года № 203 // Гарант : сайт. URL: https://base.garant.ru/71670570/ (дата обращения: 25.07.2025).

– регламентация блокировки подозрительных транзакций и SIM-карт;

– создание нормативно закрепленного механизма контроля за использованием VPN-сервисов и других средств анонимизации. Введение централизованного государственного реестра VPN-платформ с определением критериев их правомерного применения позволит снизить число преступлений, совершаемых при сокрытии цифрового следа. Кроме того, важным шагом стало недавнее внесение изменений в уголовное законодательство: Федеральным законом от 31 июня 2025 года № 282-ФЗ[7] в ст. 63 УК РФ[8] был добавлен подп. «ф» п. 1, признающий совершение преступления с использованием программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, отягчающим обстоятельством. Это нормативное нововведение подтверждает необходимость закрепления дополнительных механизмов контроля и идентификации при использовании технологий сокрытия IP-адресов и зашифрованных каналов передачи данных.

Как указывают Д. А. Степаненко и А. А. Митрофанова, законодательство в области киберпреступлений должно оперативно адаптироваться к новым вызовам цифровой среды [11, с. 92].

2. Развитие цифровой криминалистики.

Современная криминалистика остро нуждается в обновлении методического арсенала, способного эффективно работать с цифровыми доказательствами. Как подчеркивает В. А. Ращупкина, использование автоматизированных систем анализа сетевого трафика позволяет выявлять преступные схемы на ранних стадиях их реализации, что существенно повышает эффективность расследования [12, с. 142].

В контексте цифровой трансформации представляется особенно актуальным сравнительный анализ традиционной и цифровой криминалистики. В этом аспекте заслуживает внимания работа Д. В. Воронкова, в которой детально рассмотрены методологические и структурные различия между двумя направлениями. Автор обосновывает необходимость пересмотра понятийного аппарата и подходов к построению дисциплины исходя из специфики цифровых следов и инструментов их анализа [13, с. 71-73].

В целях развития цифровой криминалистики предлагаются следующие меры:

– создание специализированных подразделений по работе с цифровыми доказательствами – в структуре Следственного комитета и МВД России должны быть отделы цифровой криминалистики, укомплектованные IT-специалистами, экспертами по блокчейн-технологиям, машинному обучению и анализу трафика;

– оснащение современными техническими средствами фиксации ЭЦС – внедрение сертифицирован-

[7] Федеральный закон от 31 июля 2025 г. N 282-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. – 2025. – 4 августа (№ 31). – Ст. 4636.

[8] Уголовный кодекс Российской Федерации : УК : принят Гос. Думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года : послед. ред. // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 25.07.2025).

ных систем копирования цифровых данных с функцией хеширования, средств анализа сетевого трафика, систем мониторинга даркнета;

– разработка единой методики работы с ЭЦС – необходимо закрепить порядок извлечения, верификации и хранения данных в виде приказа МВД/СК России с учетом международных стандартов (ISO/IEC 27037:2012);

– создание федерального реестра VPN-сервисов и анонимайзеров – с четким разграничением правомерного и неправомерного использования. Это позволит сократить правовую неопределенность и минимизировать так называемую «серую зону» – случаи, когда VPN используются вне правового контроля, но формально не подпадают под действующее регулирование (например: использование VPN для доступа к заблокированным сайтам, но не с преступной целью). При этом важно обеспечить баланс между цифровой безопасностью и защитой прав пользователей.

Е. А. Русскевич подчеркивает, что современные технологии искусственного интеллекта способны значительно повысить эффективность выявления киберугроз [4, с. 170].

3. Подготовка специалистов.

Необходимо усиление подготовки сотрудников правоохранительных органов в области цифровой криминалистики, киберразведки и анализа данных. Как отмечают А. Л. Репецкая и И. П. Родивилин, эффективная борьба с преступлениями в сфере обращения охраняемой законом информации требует не только технических, организационно-правовых мер, включая внедрение IPv6, ликвидацию технологии NAT, контроль за точками коллективного доступа к Интернету, но и подготовку специалистов [14, с. 359].

4. Укрепление международного сотрудничества.

Сложность расследования трансграничных киберпреступлений обусловлена отсутствием единых стандартов обмена данными между государствами.

Перспективные направления:

– расширение кооперации с Интерполом, Европолом, международными платежными системами и крупными IT-компаниями;

– подписание двусторонних соглашений о совместном расследовании IT-преступлений;

– развитие специализированных международных рабочих групп для анализа преступных схем.

Исследования Европола подтверждают, что объединение усилий стран-участниц значительно сокращает время на выявление преступных группировок и предотвращение их деятельности[9].

Опыт стран ЕС и США показывает, что ключевыми элементами успешного расследования киберпреступлений являются централизованные платформы обмена данными, гибкое законодательство и оперативный доступ к информации. В России такие решения пока находятся на стадии фрагментарной реализации.

Выводы и заключение

В условиях цифровизации российское общество сталкивается с устойчивым ростом числа пре-

[9] Исследования Европола по цифровой безопасности в контексте транснациональной преступности. – Брюссель, 2024. – Электронный ресурс. – URL: https://www.europol.europa.eu (дата обращения: 20.07.2025).

ступлений, совершаемых с использованием информационно-коммуникационных технологий, что требует адекватного ответа со стороны уголовной юстиции и криминалистики.

Основными проблемами, препятствующими эффективному раскрытию и расследованию IT-преступлений, являются: высокий уровень анонимности преступников, использование искусственного интеллекта в преступных целях, слабое взаимодействие с частным сектором, нехватка технических ресурсов и квалифицированных кадров, а также трансграничный характер преступной деятельности.

Анализ показал, что действующие нормы уголовного законодательства и уголовно-процессуальной практики отстают от темпов технологического развития. Это особенно проявляется в отсутствии четкого регулирования таких явлений, как автономные ИИ-системы и их участие в совершении преступлений.

Ключевыми направлениями совершенствования противодействия киберпреступности являются:

– адаптация уголовного законодательства к вызовам цифровой среды;

– развитие цифровой криминалистики с применением технологий ИИ и анализа больших данных;

– нормативное закрепление механизмов оперативного взаимодействия между правоохранительными органами и коммерческими структурами;

– укрепление международного сотрудничества в сфере трансграничного расследования.

Таким образом, успешное противодействие IT-преступности невозможно без системных и согласованных мер, охватывающих как правовую, так и техническую составляющие расследования. Требуется обновление методической базы цифровой криминалистики, законодательное закрепление новых категорий преступных деяний, связанных с искусственным интеллектом, а также институциональное развитие межведомственного и международного сотрудничества. Комплексный подход, сочетающий превентивные меры, технологические решения и правовые новации, способен повысить эффективность расследования и укрепить правопорядок в условиях цифровой трансформации общества.

СПИСОК ИСТОЧНИКОВ

1. *Смушкин, А. Б.* Криминалистические аспекты использования киберпространства и обеспечения кибербезопасности. М, 2024. 196 с.

2. *Архипов, Д. Д., Гарцева, Ю. Ю., Миллер, В. Ю.* К вопросу применения цифровой криминалистики в современных условиях // Азиатско-Тихоокеанский регион: экономика, политика, право. 2024. Т. 26. № 3. С. 158–168.

3. *Россинская, Е. Р.* Тренды развития криминалистики в условиях цифровой трансформации современной преступности // Союз криминалистов и криминологов. 2025. № 1. С. 162–173.

4. *Русскевич, Е. А.* Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной

безопасности // Journal of Digital Technologies and Law. 2023. № 7 (3). С. 650–672.

5. *Бахтеев, Д. В., Беляков, А. А.* Использование данных реестра ОС Windows для установления обстоятельств совершения компьютерного преступления // Эксперт-криминалист. 2024. № 1. С. 5–8.

6. *Тирранен, В. А.* Преступления с использованием искусственного интеллекта // Развитие территорий. 2019. № 3 (17). С. 10–13.

7. *Мосечкин, И. Н.* Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник Санкт-Петербургского университета. Право. 2019. № 3. С. 461–476.

8. *Аверинская, С. А., Севостьянова, А. А.* Создание искусственного интеллекта с целью злонамеренного использования в уголовном праве Российской Федерации // Закон и право. 2019. № 2. С. 94–96.

9. *Русакова, О. И., Головань, С. А.* Влияние киберпреступлений на банковскую систему России // Baikal Research Journal. 2021. Т. 12. № 1. URL: https://brj-bguep.ru/reader/article.aspx?id=24372 (дата обращения: 18.07.2025).

10. *Якимова, Е. М., Нарутто, С. В.* Международное сотрудничество в борьбе с киберпреступностью // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10. № 2. С. 369–378.

11. *Степаненко, Д. А., Митрофанова, А. А.* Противодействие киберпреступности как современный вызов традиционной криминалистике // Союз криминалистов и криминологов. 2022. № 3. С. 91–97.

12. *Ращупкина, В. А.* О совершенствовании процессуального порядка собирания доказательств в компьютерных сетях // Вестник Всероссийского института повышения квалификации сотрудников МВД России. 2023. № 3 (67). С. 141–145.

13. *Воронков, Д. В.* О соотношении традиционной криминалистики и цифровой криминалистики // Baikal Research Journal. 2025. Т. 16. № 1. С. 70–75.

14. *Репецкая, А. Л., Родивилин, И. П.* Предупреждение преступлений в сфере обращения охраняемой законом информации // Академический юридический журнал. 2021. Т. 22. № 4 (86). С. 352–360.

REFERENCES

1. *Smushkin, A. B.* Kriminalisticheskie aspekty ispol'zovaniya kiberprostranstva i obespecheniya kiberbezopasnosti [Forensic Aspects of the Use of Cyberspace and Ensuring Cybersecurity]. Moscow, 2024. 196 p. (in Russian).

2. *Arkhipov, D. D., Gartseva, Yu.Yu., Miller, V. Yu.* K voprosu primeneniya tsifrovoj kriminalistiki v sovremennykh usloviyakh [On the Issue of the Application of Digital Forensics in Modern Conditions]. Aziatsko-Tikhookeanskij region: ekonomika, politika, pravo. – Asia-Pacific Region: Economy, Politics, Law: Scientific Journal. 2024. vol. 26. no. 3. pp. 158-168. (in Russian).

3. *Rossinskaya, E. R.* Trendy razvitiya kriminalistiki v usloviyakh tsifrovoj transformatsii sovremennoj prestupnosti [Trends in the Development of Forensics in the Context of the Digital Transformation of Modern Crime]. Soyuz kriminalistov i

kriminologov – Union of Criminalists and Criminologists: Scientific Journal. 2025. no. 1. pp. 162-173. (in Russian).

4. *Russkevich, E. A.* Narushenie pravil tsentralizovannogo upravleniya tekhnicheskimi sredstvami protivodejstviya ugrozam informatsionnoj bezopasnosti [Violation of the Rules of Centralized Management of Technical Means of Counteracting Information Security Threats]. Journal of Digital Technologies and Law. 2023. no. 7 (3). pp. 650-672. (in Russian).

5. *Bakhteev, D. V., Belyakov, A. A*. Ispol'zovanie dannykh reestra OS Windows dlya ustanovleniya obstoyatel'stv soversheniya komp'yuternogo prestupleniya [Use of Windows Registry Data to Establish the Circumstances of a Computer Crime]. Ekspert-kriminalist – Expert-Criminalist: Scientific Journal. 2024. no. 1. pp. 5–8. (in Russian).

6. *Tirranen, V. A.* Prestupleniya s ispol'zovaniem iskusstvennogo intellekta [Crimes Using Artificial Intelligence]. Razvitie territorij – Territory Development: Scientific Journal. 2019. no. 3 (17). pp. 10-14. (in Russian).

7. *Mosechkin, I. N.* Iskusstvennyj intellekt i ugolovnaya otvetstvennost': problemy stanovleniya novogo vida sub"ekta prestupleniya [Artificial Intelligence and Criminal Liability: Problems of the Formation of a New Type of Crime Subject]. Vestnik Sankt-Peterburgskogo universiteta. Pravo – Bulletin of Saint Petersburg University. Law. 2019. no. 3. pp. 461-476 (in Russian).

8. *Averinskaya, S.A., Sevost'yanova, A.A.* Sozdanie iskusstvennogo intellekta s tsel'yu zlonamernogo ispol'zovaniya v ugolovnom prave Rossijskoj Federatsii [Creation of Artificial Intelligence for Malicious Use in the Criminal Law of the Russian Federation]. Zakon i pravo : nauch. zhurn. – Law and Legislation: Scientific Journal. 2019. no. 2. pp. 94-96. (in Russian).

9. *Rusakova, O. I., Golovan', S. A.* Vliyanie kiberprestuplenij na bankovskuyu sistemu Rossii [The Impact of Cybercrime on the Banking System of Russia]. Baikal Research Journal – Baikal Research Journal. 2021. vol. 12. no. 1. URL: https://brj-bguep.ru/reader/article.aspx?id=24372 (accessed 18.07.2025). (in Russian).

10. *Yakimova, E. M., Narutto, S. V.* Mezhdunarodnoe sotrudnichestvo v bor'be s kiberprestupnost'yu [International Cooperation in Combating Cybercrime]. Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta ekonomiki i prava : nauch. zhurn. – Criminological Journal of the Baikal State University of Economics and Law. 2016. vol. 10. no. 2. pp. 369-378. (in Russian).

11. *Stepanenko, D. A., Mitrofanova, A.A.* Protivodejstvie kiberprestupnosti kak sovremennyj vyzov traditsionnoj kriminalistike [Countering Cybercrime as a Modern Challenge to Traditional Forensics]. Soyuz kriminalistov i kriminologov – Union of Criminalists and Criminologists: Scientific Journal. 2022. no. 3. pp. 91-97. (in Russian).

12. *Rasshchupkina, V.A.* O sovershenstvovanii protsessual'nogo poryadka sobiraniya dokazatel'stv v komp'yuternykh setyakh [On Improving the Procedural Procedure for Collecting Evidence in Computer Networks]. Vestnik Vserossijskogo instituta povysheniya kvalifikatsii sotrudnikov MVD Rossii – Bulletin of the All-Russian Institute for Advanced Training of Employees of the Ministry of Internal Affairs of Russia. 2023. no. 3 (67). pp. 141-145. (in Russian).

13. *Voronkov, D. V.* O sootnoshenii traditsionnoj kriminalistiki i tsifrovoj kriminalistiki [On the Relationship Between Traditional Forensics and Digital

Forensics]. Baikal Research Journal – Baikal Research Journal. 2025. vol. 16. no. 1. pp. 70-75. (in Russian).

14. *Repetskaya, A. L., Rodivilin, I.P.* Preduprezhdenie prestuplenij v sfere obrashcheniya okhranyaemoj zakonom informatsii [Prevention of Crimes in the Sphere of Circulation of Information Protected by Law]. Akademicheskij yuridicheskij zhurnal – Academic Law Journal. 2021. vol. 22. no. 4 (86). pp. 352-360. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Родивилина Виктория Александровна, кандидат юридических наук, доцент, доцент кафедры криминалистики. Восточно-Сибирский институт МВД России. 664074, Российская Федерация, г. Иркутск, ул. Лермонтова, 110.

Коломинов Вячеслав Валентинович, кандидат юридических наук, доцент, доцент кафедры криминалистики, судебных экспертиз и юридической психологии. Институт государства и права Байкальского государственного университета. 664025, Российская Федерация, г. Иркутск, ул. Ленина, 11.

INFORMATION ABOUT THE AUTHORS

Victoria A. Rodivilina, candidate of legal sciences, Associate Professor, Associate Professor of the Department of Criminalistics. East Siberian Institute of the Ministry of Internal Affairs of Russia, 110 Lermontova St., Irkutsk, Russian Federation, 664074.

Vyacheslav V. Kolominov, candidate of legal sciences, Associate Professor, Associate Professor of the Department of Criminalistics, Forensic Examinations and Legal Psychology. Institute of State and Law, Baikal State University, 11 Lenina St., Irkutsk, Russian Federation, 664025.