Научная статья
УДК 343.9.01
EDN: https://elibrary.ru/VBUOHM
NIION: 2007-0083-1/26-758
MOSURED: 77/27-005-2026-01-958

Особенности выявления и раскрытия преступлений, совершаемых с использованием информационно-телекоммуникационных технологий

Анатолий Васильевич Богданов[1], Игорь Николаевич Волосевич[2], Евгений Николаевич Хазов[3]
[1,2,3] Московский университет МВД России имени В.Я. Кикотя, Москва, Россия
[2] 89151333377in@gmail.com
[3] evg.hazow@yandex.ru

Аннотация. Проведен детальный анализ и рассмотрены особенности выявления и раскрытия преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Актуальность заключается в том, что в современной России с каждым годом возрастает количество преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Особое внимание уделено причинам, условиям и особенностям выявления и раскрытия преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Ключевые слова: оперативно-розыскная деятельность, преступления в сфере информационно-телекоммуникационных технологии, организованные преступные группы, особенности выявления и раскрытия преступлений, совершенных организованными преступными группами

Для цитирования: Богданов А. В., Волосевич И. Н., Хазов Е. Н. Особенности выявления и раскрытия преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Криминологический журнал. 2026. № 1. С. 14–21. EDN: VBUOHM.

Original article

Features of detection and disclosure of crimes committed using information and telecommunication technologies

Anatoly V. Bogdanov[1], Igor N. Volosevich[2], Evgeny N. Khazov[3]
[1,2,3] Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Moscow, Russia
[2] 89151333377in@gmail.com
[3] evg.hazow@yandex.ru.

Abstract. A detailed analysis has been carried out and the features of the detection and disclosure of crimes committed using information and telecommunication technologies have been considered. The relevance lies in the fact that in modern Russia the number of crimes committed using information and telecommunication technologies is increasing every year. Special attention is paid to the causes, conditions and features of the detection and disclosure of crimes committed using information and telecommunication technologies.

Keywords: operational investigative activities, crimes in the field of information and telecommunication technology, organized criminal groups, features of detection and disclosure of crimes committed by organized criminal groups

For citation: Bogdanov A. V., Volosevich I. N., Khazov E. N. Features of detection and disclosure of crimes committed using information and telecommunication technologies. Criminological Journal. 2026;(1):14–21. (In Russ.). EDN: VBUOHM.

Главным вызовом для органов внутренних дел стали преступления в сфере информационно-телекоммуникационных технологий (ИТТ). Всеобщая цифровизация, информационные технологии и искусственный интеллект обнаружили очень опасные и уязвимые точки, связанные с безопасностью граждан и государства. Не было бы интернета, не было бы информационной безопасности как индустрии. Не было бы Интернета, не было бы и информационной безопасности как индустрии [1].

До 1992 г. в СССР и России не обучали защите информации в гражданских вузах. Эта система была уделом ограниченного количества «закрытых вузов» и негражданских государственных организаций. С появлением Интернета в России появились новые классы угроз. А самое главное, если раньше существовала изолированная компьютерная сеть в рамках одного здания, какого-нибудь оборонного предприятия или министерства, то подключение к Интернету автоматически сделало сети компаний и организаций доступными всему миру. Чем больше Интернет-сервисов, тем больше различных угроз [2].

В настоящее время цифровое пространство превратилось в способ зарабатывания денег. Невозможно сохранить всемирную паутину от кибервторжений. Киберпреступность в сети Интернет непобедима. Внедрение информационно-телекоммуникационных технологий в различные области общественной жизни, появление новых технических средств, формирование цифрового пространства в качестве платформы, обеспечивающей гармоничное взаимодействие между различными субъектами юридических отношений, а также развитие искусственного интеллекта (ИИ) — это реалии современного информационного (цифрового) общества [3].

С каждым годом расширяется сфера применения искусственного интеллекта в системе МВД РФ. Внедрение ИИ поможет снизить нагрузку на оперативные подразделения. ИИ никогда не сможет полностью заменить оперативного сотрудника — это еще и индивидуальный подход, умение принимать решения в сложных и нестандартных ситуациях: в выявлении и раскрытии преступлений.

Способов, которыми кибермошенники стараются изъять деньги у населения, сегодня великое множество. Даже эксперты и правоохранительные органы сбились со счета. Едва раскроют одну схему, тут же появляется следующая, еще более хитроумная. Однако и старые методы мошенничества продолжают работать. Кибермошенники применяют все новые и новые формы социальной инженерии, которые подвергаются систематической трансформации в следствии, изменяющихся внутренних и внешних социально-экономических и политических обстоятельств и проведении специальной военной операции (СВО).

Обозначенные выше процессы диктуют обязательную потребность по переосмыслению возникших угроз в сфере информационно-телекоммуникационных технологий (ИТТ), а также обусловленных ею возникших проблем, не только с теоретических и правовых позиций, но и с уголовной и правовой защиты граждан и организаций, но также и с точки зрения и позиции оперативно-розыскной деятельности. Один из безусловных приоритетов органов внутренних дел это борьба с преступлениями с использованием ИТТ [4].

Используя методы социальной инженерии и искусственного интеллекта (ИИ), киберпреступники легко завоевывают доверие тех, кто совсем не привык жить в мире цифровых угроз. В 2024 г. в России, зарегистрировано 765,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или сфере компьютерной информации, что на 13,1 % больше чем в 2023 г. [5].

По данным Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России (УБК МВД России) только по итогам 2024 г. общая сумма составила 203 млрд руб. Жертвами стали 132,4 тыс. пенсионеров (23,4 % от общего количества потерпевших); 6,9 тыс. несовершеннолетних (1,2 %) [6].

Использование локальных решений и проверенных облачных платформ снижает уровень безопасности утечки персональных данных. Утечки персональных данных ИИ-сервисов могут происходить из-за кибератак или ошибок на этапе разработки сервиса. Злоумышленники могут похитить учетные данные пользователей от аккаунтов в ИИ-сервисах и получить доступ к конфиденциальным данным, которыми те обмениваются с нейросетью. Программы-шифровальщики остаются одной из самых опасных киберугроз. Злоумышленники продолжают активно использовать социальную инженерию — набор методик манипулирования людьми с целью получения конфиденциальной информации и несанкционированного доступа к серверам и персональным компьютером [7].

В 2023 г. общий объем прибыли хакеров, действующих в России странах СНГ превысил 1 млрд долларов. Ежегодно на территории Российской Федерации помимо сохранения тенденции увеличения количества регистрируемых преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, фиксируется растущий уровень сложности документирования данных преступлений в связи с постоянным развитием информационных технологий, что в свою очередь совершенствует и инструменты совершения данных преступлений, увеличивая их количество. В настоящее время в Перечне № 25 статей УК РФ IT-преступлений (действующего в редакции совместного указания Генеральной прокуратуры России и МВД России от 27 декабря 2024 г. № 952/11/3) — 83 состава, из них к компетенции оперативных подразделений органов внутренних дел относится 78 составов, из них к латентным (скрытым) составам, которые подлежат выявлению, относятся более 60 %. Наибольшей латентностью обладают преступления, отнесенные к Главе 28 УК РФ, из них 80–85 % преступлений, связанных с неправомерным доступом к охраняемой законом компьютерной информации, а факты обнаружения незаконного доступа к информационным ресурсам на 90 % носят случайный характер. При этом треть IT-преступлений, отнесенных к компетенции подразделений по борьбе с киберпреступлениями квалифицируются по совокупности со ст. 272 и (или)

273 УК РФ, а именно: ст. 137, 146, 158, 159, 159.3, 163, 165, 183, 187 УК РФ [8].

Увеличение количества регистрируемых IT-преступлений, в том числе по тяжким и особо тяжким составам обусловлено постоянным ростом использования сети Интернет в качестве средства коммуникации и ведения хозяйственной деятельности, а также приспосабливаемостью преступников к принимаемым правоохранительными органами мерам по противодействию. Современные информационные технологии позволяют многим преступникам успешно скрывать свою личность, а высокая латентность не позволяет получить достоверные статистические данные о масштабе проблемы, что в свою очередь не дает возможности реализовать принцип неотвратимости наказания, безнаказанности, и порождает рост рецидива [9].

Оперативная обстановка свидетельствует о том, что ранее имущественные IT-преступления совершались преимущественно из «мест лишения свободы» под предлогами «сын попал в беду» или «путем направления смс-сообщения от имени родственника», а в последние годы распространение получили дистанционные хищения, совершаемые от имени сотрудников правоохранительных органов, служб безопасности банков, медицинских или социальных работников.

Типичными предлогами мошенников для совершения противоправных деяний являются: проведение операции по задержанию преступников; защита денежных средств от кражи путем перевода на «безопасный» счет; попытка злоумышленниками завладения правами на квартиру (дом); необходимость получения кредитов для предотвращения их оформления мошенниками; получение компенсаций за ранее приобретенные товары, медикаменты; получение социальных выплат; необходимость проведения дорогостоящей медицинской операции; сообщить код из SMS-сообщения для блокировки карты.

В настоящее время чаще всего хищения совершается лицами, находящимся за пределами Российской Федерации. Все сервисы находятся за пределами нашей страны. Немалое влияние оказывают события, связанные с проведением специальной военной операции. Огромные кол-центры по мошенническому хищению денег у россиян посредством Интернета сосредоточены сегодня на Украине. В 2022–2024 гг. мошенники перешли от количества совершаемых преступлений к «качеству», а именно: конечной целью преступников является завладение денежными средствами в особо крупном размере. Преступники стали склонять потерпевших к реализации имущества посредством заключения договоров купли-продажи в риэлтерских агентствах и получению кредита или займа в кредитно-финансовых организациях [10].

Кроме того, массовость совершения имущественных IT-преступлений обуславливается высоким уровнем организации участников преступных групп и преступных сообществ. Их деятельность в настоящее время носит «сервисный» характер и характеризуется устойчивыми связями участников групп, организованностью действий, созданием условий для совершения преступлений, разделом сфер преступного влияния с общей целью извлечения преступного дохода. В настоящее время большинство имущественных IT-преступлений совершаются международными организованными группами [11].

Структура участников ОГиПС составляет: организаторы, которые имеют один или несколько колл-центров; лица, работающие в колл-центре, которые непосредственно вступают в контакт с потерпевшими путем телефонного разговора. Данные лица получают четкие указания, т. е. методические рекомендации, как совершать преступления данного характера, а также обладают психологическими навыками; лица, входящие в структуру сервиса по обналичиванию денежных средств, добытых преступным путем. Если колл-центры в большинстве случаев находятся за рубежом, то лица, входящие в систему сервиса по обналичиванию денежных средств, осуществляют свою преступную деятельность на территории Российской Федерации.

Пример: дистанционные хищения, совершаемые от имени сотрудников банка — группа преступников путем аренды серверов создает инфраструктуру для «обзвона» граждан, в которую входит удаленный доступ к личному кабинету мошенника с базой клиентов банков, заготовленными спичами. Данная инфраструктура продается в виде франшизы лицу, которое готово организовать работу колл-центра (арендовать здание, купить компьютеры и обеспечить их соединение с интернетом, набрать персонал). Далее, в ходе обмана работники колл-центра должны куда-то переводить денежные средства, добытые преступным путем. Данные услуги предлагает, так называемый, «обнал сервис», работа которого организована на территории Российской Федерации. Главный доход указанного сервиса — процент от суммы за перевод денежных средств. Мошенники-обнальщики конвертируют похищенные денежные средства в криптовалюту, затем переводят их на различные электронные кошельки или биржи, чтобы скрыть их источник. В настоящее время денежные средства, проведенные через криптобиржи либо электронные кошельки, невозможно вернуть через процедуру «чарджбэк».

Существует несколько проблем с обнаружением незаконных криптовалютных транзакций, включая анонимный характер криптовалютных операций: использование сложных криптовалютных сетей и методов запутывания, а также отсутствие в настоящее время в Российской Федерации полного и исчерпывающего законодательного регулирования оборота криптовалют. Лишь отдельные элементы содержатся в Федеральных законах «Об информации, информационных технологиях и о защите информации» [12] и «О цифровых финансовых активах» [13].

В последнее время имущественные IT-преступления в большей степени стали совершаться с использованием кроссплатформенных мессенджеров («WhatsApp», «Viber», «Telegram» и т. д.), подключенных на «виртуальные номера». Так, в 2024 г., примерно, в 70 % имущественных IT-преступлений совершены с использованием указанных интернет-ресурсов.

IT-преступления с использованием кроссплатформенных мессенджеров совершаются участниками организованных групп и преступных сообществ. Доступ к указанным мессенджерам приобретается удаленно, через специализированные платные интернет-сервисы (сайты) с использованием SIM-банков (SIM-бокс / GSM-шлюзов) путем приобретения или аренды виртуальных абонентских номеров для SMS-активации.

Лица, предоставляющие услуги по аренде или приобретению виртуальных номеров, зачастую, используют SIM-банки (SIM-боксы). SIM-банк представляет собой устройство-репозиторий SIM-карт и используется для незаконного подключения к телефонным сетям. Устройство конвертирует международные звонки в локальные звонки домашнего региона (соединяющее сети VoIP и GSM / UMTS). Обычно они используются для совершения звонков через несколько SIM-карт, установленных в устройстве. Мошенники используют его для незаконной терминации международного голосового трафика через местные SIM-карты в сети, тем самым, это сетевое устройство с возможностью считывать данные банка для SIM-карт, а затем обмениваться данными с устройствами GSM для установления виртуальных соединений между SIM-картами и устройствами GSM. Это позволяет устанавливать SIM-банки в одном месте, тогда как устройства GSM устанавливаются в разных местах.

Основным поставщиком на территорию Российской Федерации SIM-банков является Китайская Народная Республика. Данные технические средства ввозятся уже заранее модифицированными («перепрошитыми»), а именно, дополненными различными функциями, облегчающими использование SIM-банков в преступных целях, такими как способность генерировать различные омерные емкости IMEI («динамический IMEI»), что затрудняет их идентификацию.

Лица, предоставляющие услуги доступа к данным ресурсам, находятся на территории Российской Федерации и их местонахождение возможно установить путем получения сведений об используемых для активации мессенджеров.

В целях выработки законодательных предложений по регулированию данной деятельности, а также по внесению изменений и (или) дополнений в нормативные правовые акты, целесообразно на площадках различных межведомственных рабочих групп и координационных совещаниях:

рассмотреть вопрос и дать правовую оценку деятельности лиц, администрирующих площадки по предоставлению удаленного доступа к мессенджерам и сервисам и лиц, использующих SIM-боксы в преступных целях, для выработки соответствующих предложений о внесении законодательной инициативы о регулировании данной деятельности, в том числе по привлечению к уголовной ответственности по ст. 33 УК РФ, как соучастие в совершении преступлений;

рассмотреть вопрос об обязательной регистрации и сертификации SIM-банков (SIM-бокс/GSM-шлюзов), вести учет лиц, которые осуществляют ввоз данных технических средств из-за рубежа.

Также в настоящее время основными проблемами при расследовании уголовных дел по IT-преступлениям являются: широкое использование злоумышленниками средств анонимизации в сети «Интернет» (прокси-сервера, VPN-сервисы, TOR-сети); межрегиональный характер, требующий значительных временных затрат на подготовку и проведение необходимых оперативно-розыскных мероприятий и следственных действий, направленных на документирование и раскрытие преступлений указанной категории; отсутствие контроля операторов сотовой связи за юридическими лицами, осуществляющими реализацию «SIM-карт» в больших количествах, а также отсутствие реальной идентификации лиц, на которых они зарегистрированы; низкая оперативность при получении информации в иностранных организациях, находящихся вне юрисдикции правоохранительных органов Российской Федерации, предоставляющих услуги связи (операторы связи и провайдеры), регистрации и хостинга доменных имен; установление конечного Интернет-пользователя при использовании злоумышленниками промежуточных виртуальных серверов, в том числе российских хостинг-провайдеров; невозможность возмещения ущерба и наложения ареста в случае преобразования похищенных денежных средств в криптовалюту, отсутствие действенных норм законодательства Российской Федерации по регулированию данного вопроса; несвоевременное проведение следственных и оперативно-розыскных мероприятий, направленных на закрепление доказательственной базы (осмотры мест происшествий, изъятие сотовых телефонов и иной оргтехники; получение скриншотов сообщений, переписки с неустановленными лицами); несвоевременное заполнение базы данных ПТК «ИБД-Ф», в связи с чем невозможно проверить факты совпадений по реквизитному составу, либо внесение неполных сведений в базу данных.

В целях повышения эффективности своевременного установления лиц, участвующих в схеме совершения хищений («обнальщики», «дропы», «дроповоды»), необходимо налаживать механизм оперативного получения из территориальных подразделений ГУ МВД информации по всем фактам мошеннических действий, связанных с переводом денежных средств посредством банкоматов (токены) для последующего получения в течении суток от оператора платежных систем АО «Национальная система платежных карт»

и банковских организаций (ПАО «СберБанк России», ПАО «ВТБ») информации о полных номерах банковских карт, на которые потерпевшими переводились денежные средства [14].

С 15 мая вступил в силу закон, ограничивающий возможность дропперов (людей, через чьи банковские карты за определенную комиссию мошенники прогоняют деньги: именно реквизиты дроппера получает жертва обмана) для вывода и обналичивания денег. Теперь они не смогут переводить сами себе и другим людям более 100 тыс. руб. в месяц. Новая мера против дропперов — это часть закона о периоде охлаждения по кредитам и займам принятого в феврале. Данные по данной дропперам попадают в базу Банка России о мошеннических операциях, эти сведения недоступны всем банкам и правоохранительным органам. Сама база формируется на основе сведений банков о случаях и попытках мошенничества (это финансовые операции, по которым клиенты банка заявили о своем несогласии). Если сведения о клиенте попадают в базу данных ЦБ, то банк может приостановить ему действие карты или услуги онлайн-банкинга.

В основном дропперы — это молодые люди в возрасте от 18 до 25 лет, но в настоящее время ими становятся несовершеннолетние. Несовершеннолетние воспринимают такие услуги как легкий способ заработать финансовые средства. В подростковой среде информация распространяется очень быстро. Несовершеннолетний получает предложение легко заработать, соглашается, получив деньги, а потом рассказывают об этом своим одноклассникам, как он их легко заработал [15].

С 1 июля 2025 г. у Росфинмониторинга появятся полномочия самостоятельно блокировать карты дропперов. Можно останавливать операции до 10 дней при наличии подозрений в отмывании денег. Внесены поправки в ст. 187 УК РФ, которая предусматривает наказания за передачу карты третьим лицам (штраф от 100 до 300 тыс. руб., исправительные работы, лишение свободы до двух лет).

Дело и в том, что не всегда люди становятся дропперами осознанно. Иногда дропперами становятся случайно. Мошенники придумывают разные уловки и люди просто не знают, что становятся соучастниками преступной схемы. Чтобы не попасть в такую ситуацию, ни в коем случае не передавать свою банковскую карту посторонним, не использовать ее для переводов (в том числе в банкомате) по просьбе чужих людей, не предоставлять никому доступ к своему онлайн-банкингу, а также не переводить никому ошибочно поступившие на ваш счет деньги. В этом последнем случае нужно обратиться в свой банк и сообщить ему о таком переводе. Попадание в базу данных ЦБ и последующую блокировку карты можно обжаловать. Для этого существует два способа. Первый — нужно обратиться с заявлением в любой из банков, клиентом которого вы являетесь. Заявление должны перенаправить ЦБ максимум на следующий рабочий день. Второе — направить заявление в банк России через интернет-приемную выбрав в качестве темы обращения «Информационная безопасность».

Также в целях совершенствования проводимой работы необходимо налаживать взаимодействие с иными правоохранительными и контролирующими органами, с кредитно-финансовыми организациями и операторами связи [16]. Так, в целях снижения количества правонарушений связанных с незаконной деятельности по реализации идентификационных модулей абонентов (SIM-карт) от имени операторов связи лицами, не имеющими соответствующих полномочий на заключение договора об оказании услуг подвижной радиотелефонной связи и без включения в договор на услуги указанного вида связи сведений об абоненте, совместно с органами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций необходимо разработать разъяснения по организации и проведению мероприятий, направленных на пресечение фактов реализации юридическими и физическими лицами SIM-карт с нарушением действующего законодательства с учетом Правил оказания услуг телефонной связи, утвержденных Постановлением Правительства Российской Федерации от 24 января 2024 г. № 59 [17].

В целях снижения количества IT-преступлений, совершаемых с использованием специального оборудования «SIM-боксы» необходимо налаживать взаимодействие и обмен информацией с руководством «OZON» и «Wildberries» по получению информации о лицах, осуществляющих сбыт и оптовую покупку «SIM-карт».

В рамках взаимодействия с представителями ООО «Коинкит» (сервис для проверки криптовалютных транзакций и кошельков), на постоянной основе получать точки удаленного доступа для использования возможностей сервиса.

Наладить взаимодействие с представителями ООО «Ф.А.К.К.Т.» (российский разработчик технологий для борьбы с киберпреступлениями) для проведения мероприятия по сбору и обработке цифровых доказательств.

Для обмена оперативной информацией и выработки плана совместных мероприятий по повышению эффективности борьбы с преступностью в IT-сфере на постоянной основе проводить рабочие встречи с представителями различных кредитно-финансовых организаций и операторов связи (ПАО «СберБанк России», ПАО «Теле2», ПАО «Почта России», АО «АльфаБанк», ПАО Банк «ФК Открытие», АО «Т-Банк», ПАО «ВТБ»), в том числе в рамках участия в межбанковских рабочих группах.

В целях повышения уровня информированности населения о наиболее распространенных способах совершения IT-преступлений, в том числе о рисках хищений с применением инструментов социальной инженерии и методов защиты от них проводить ком-

плекс соответствующих агитационно-профилактических мероприятий. Размещать материалы на официальных сайтах государственных учреждений и в средствах массовой информации. В местах массового пребывания граждан размещать информационно-профилактические материалы (памятки, информационные листовки).

Организовывать проведение оперативно-профилактических мероприятий (ОПМ): ОПМ направленных на пресечение незаконной деятельности по реализации идентификационных модулей абонентов («SIM-карт») от имени операторов связи лицами, не имеющими соответствующих полномочий на заключение договора об оказании услуг подвижной радиотелефонной связи и без включения в договор на услуги подвижной радиотелефонной связи сведений об абоненте, в нарушение Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» [18]; ОПМ направленных на снижение мошенничеств, совершаемых с использованием IT-технологий, в том числе фактов повторных мошеннических действий в отношении граждан («мошенничеств двойного круга») путем соответствующей профилактической работы с гражданами, пострадавшими от мошеннических действий в 2023–2024 гг.

Налаживать взаимодействие с различными молодежно-добровольческими и волонтерскими организациями, институтами гражданского общества и иными организациями в IT-сфере для организации и проведения профилактических мероприятия (лекции, беседы) в различных образовательных и иных государственных учреждениях.

Для устранения причини и условий совершения киберпреступлений был принят Федеральный закон от 1 апреля 2025 г. № 41-ФЗ [19]. Данный закон направлен на то, чтобы дать людям инструменты для самозащиты. Он также призван лишить кибермошенников возможности использовать их методы обмана. В законе порядка 30 мер, которые были разработаны Правительством РФ, совместно с правоохранительными органами, бизнесом и депутатами. Важно понимать, что все эти меры направлены на одно: защиту человека и его безопасность в цифровом пространстве [20].

Важнейшую роль в борьбе с преступлениями в сфере информационно-коммуникационных технологий играет профилактика. Во исполнение поручения Президента Российской Федерации УБК МВД России разработана и Правительством Российской Федерации утверждена концепция государственной системы противодействия противоправным деянием в сфере информационно-коммуникационных технологий [21].

Таким образом, в условиях увеличения числа киберпреступлений и колоссального объема пострадавших большую роль в выявлении и раскрытии преступлений играют оперативные подразделений органов внутренних дел. Что позволяет обеспечить защиту прав и законных интересах граждан, пострадавших от преступлений в сфере ИТТ.

Список источников

1. Гасанов К. К., Гуреев В. А., Егоров С. А. и др. Национальная безопасность: учебник для студентов высших учебных заведений. М., 2025.
2. Богданов А. В., Ильинский И. И., Хазов Е. Н. Информационно-телекоммуникационные технологии и их роль обеспечение безопасности личности, общества и государства // Мировая экономика: проблемы безопасности. 2021. № 1. С. 17–23.
3. Богданов А. В., Хазов Е. Н., Артамонов И. В. Киберпреступность как угроза национальной безопасности России // Международный журнал гражданского и торгового права. 2023. № 2. С. 39–43.
4. Кузьмин Н. А., Тузов Л. Л., Богданов А. В. и др. Оперативно-розыскная деятельность: учебник для студентов вузов. М., 2024.
5. Состояние преступности в России за январь–декабрь 2024 года // URL: https://мвд.рф/reports/item/12167987
6. Глебов М. Преступность уходит в цифру // Газета МВД России. 24 апреля 2025. № 15 (1943). С. 8
7. Богданов А. В., Завьялов И. А., Ильинский И. И., Михайлов Б. П. и др. Особенности противодействия киберпреступности подразделениями уголовного розыска. М., 2016.
8. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 21 апреля 2025 г.) // Собрание законодательства Российской Федерации. 17 июня 1996. № 25. Ст. 2954.
9. Богданов А. В., Ильинский И. И., Хазов Е. Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. 2020. № 1. С. 15–20.
10. Михайлова Е. В., Хазов Е. Н. Роль средств массовой информации в обеспечении национальной безопасности России: сборник мат. Всероссийской науч.-практ. конф. (Старотеряево, 12 апреля 2024 г.). Старотеряево, 2024. С. 403–409.
11. Лобзов К. М., Богданов А. В., Ильинский И. И. и др. Экстремистские организации: сущность, идеология, тактика их деятельности. Новосибирск, 2021.
12. Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 23 ноября 2024 г.) (с изм. и доп., вступ. в силу с 1 января 2025 г.) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 31 июля 2006. № 31. Ч. 1. Ст. 3448.
13. Федеральный закон от 31 июля 2020 г. № 259-ФЗ (ред. от 25 октября 2024 г.) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законода-

тельные акты Российской Федерации» // Собрание законодательства Российской Федерации. 3 августа 2020. № 31. Ч. 1. Ст. 5018.
14. Папазова Ю. В., Богданов А. В., Хазов Е. Н. Обеспечение информационной безопасности правоохранительными органами России // Право. Безопасность. Чрезвычайные ситуации. 2021. № 3 (52). С. 45–52.
15. Богданов А. В., Папазова Ю. В., Хазов Е. Н. Роль и значение информационных систем и банков данных в деятельности правоохранительных органов // Уголовное судопроизводство: проблемы теории и практики. 2021. № 2. С. 27–33.
16. Богданов А. В., Бражников Д. А., Бычков В. В. и др. Оперативно-розыскная деятельность. М., 2023.
17. Постановление Правительства РФ от 30 декабря 2024 г. № 1994 «Об утверждении Правил оказания услуг телефонной связи и перечня организаций, имеющих право осуществлять подтверждение сведений об абоненте — физическом лице» // Собрание законодательства Российской Федерации. 6 января 2025. № 1. Ст. 42.
18. Федеральный закон от 7 июля 2003 г. № 126-ФЗ (ред. от 26 декабря 2024 г.) (с изм. и доп., вступ. в силу с 1 апреля 2025 г.) «О связи» // Собрание законодательства Российской Федерации. 14 июля 2003. № 28. Ст. 2895.
19. Федеральный закон от 1 апреля 2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. 7 апреля 2025. № 14. Ст. 1574.
20. Богданов А. В., Виноградов Е. А., Хазов Е. Н. Телекоммуникационные технологии и компьютерная грамотность как средство профилактики киберпреступлений // Образование и право. 2021. № 8. С. 231–236.
21. Проект Постановления Правительства РФ «О реализации пилотного проекта по оперативному взаимодействию и информационному обмену уполномоченных государственных органов и организаций при противодействии правонарушениям, совершаемым с использованием информационно-телекоммуникационных технологий» // URL: https://regulation.gov.ru

References

1. Hasanov K. K., Gureev V. A., Egorov S. A. et al. National security: a textbook for students of higher educational institutions. M., 2025.
2. Bogdanov A. V., Ilyinsky I. I., Khazov E. N. Information and telecommunication technologies and their role in ensuring the security of individuals, society and the state // World Economy: security problems. 2021. No. 1. P. 17–23.
3. Bogdanov A. V., Khazov E. N., Artamonov I. V. Cybercrime as a threat to Russia's national security // International Journal of Civil and Commercial Law. 2023. No. 2. P. 39–43.
4. Kuzmin N. A., Tuzov L. L., Bogdanov A. V. et al. Operational investigative activity: a textbook for university students. M., 2024.
5. The state of crime in Russia in January–December 2024 // URL: https://мвд.рф/reports/item/12167987
6. Glebov M. Crime goes into numbers // Newspaper of the Ministry of Internal Affairs of Russia. April 24, 2025. No. 15 (1943). P. 8
7. Bogdanov A. V., Zavyalov I. A., Ilyinsky I. I., Mikhailov B. P. et al. Features of countering cybercrime by criminal investigation units. M., 2016.
8. Criminal Code of the Russian Federation No. 63-FZ dated June 13, 1996 (as amended on April 21, 2025) // Collection of Legislation of the Russian Federation. June 17, 1996. No. 25. Art. 2954.
9. Bogdanov A. V., Ilyinsky I. I., Khazov E. N. Cybercrime and remote fraud as one of the threats to modern society // Criminological Journal. 2020. No. 1. P. 15–20.
10. Mikhailova E. V., Khazov E. N. The role of mass media in ensuring Russia's national security: collection of materials of the All-Russian Scientific and Practical conference (Staroteryaevo, April 12, 2024). Staroteryaevo, 2024. P. 403–409.
11. Lobzov K. M., Bogdanov A. V., Ilyinsky I. I. et al. Extremist organizations: the essence, ideology, tactics of their activities. Novosibirsk, 2021.
12. Federal Law No. 149-FZ of July 27, 2006 (as amended on November 23, 2024) (as amended and supplemented, intro. effective January 1, 2025) «On Information, information technologies and information Protection» // Collection of Legislation of the Russian Federation. July 31, 2006. No. 31. P. 1. Art. 3448.
13. Federal Law No. 259-FZ of July 31, 2020 (as amended on October 25, 2024) «On Digital Financial Assets, Digital Currency and on Amendments to Certain Legislative Acts of the Russian Federation» // Collection of Legislation of the Russian Federation. August 3, 2020. No. 31. P. 1. Art. 5018.
14. Papazova Yu. V., Bogdanov A. V., Khazov E. N. Ensuring information security by law enforcement agencies of Russia // Right. Safety. Emergency situations. 2021. No. 3 (52). P. 45–52.
15. Bogdanov A. V., Papazova Yu. V., Khazov E. N. The role and importance of information systems

and data banks in the activities of law enforcement agencies // Criminal justice: problems of theory and practice. 2021. No. 2. P. 27–33.
16. Bogdanov A. V., Brazhnikov D. A., Bychkov V. V. et al. Operational search activity. M., 2023.
17. Decree of the Government of the Russian Federation dated December 30, 2024 No. 1994 «On Approval of the Rules for the Provision of Telephone Services and the List of organizations authorized to confirm information about an Individual Subscriber» // Collection of Legislation of the Russian Federation. January 6, 2025. No. 1. Art. 42.
18. Federal Law No. 126-FZ of July 7, 2003 (as amended on December 26, 2024) (as amended and supplemented, intro. effective from April 1, 2025) «On Communications» // Collection of legislation of the Russian Federation. July 14, 2003. No. 28. Art. 2895.
19. Federal Law No. 41-FZ of April 1, 2025 «On the Creation of a State information system for Countering Offenses Committed using Information and Communication Technologies and on Amendments to Certain Legislative Acts of the Russian Federation» // Collection of Legislation of the Russian Federation. April 7, 2025. No. 14. Art. 1574.
20. Bogdanov A. V., Vinogradov E. A., Khazov E. N. Telecommunication technologies and computer literacy as a means of preventing cybercrime // Education and Law. 2021. No. 8. P. 231–236.
21. Draft Decree of the Government of the Russian Federation «On the implementation of a pilot project on operational interaction and information exchange of authorized state bodies and organizations in countering offenses committed using information and telecommunication technologies» // URL: https://regulation.gov.ru

Информация об авторах

А. В. Богданов — доцент кафедры оперативно-розыскной деятельности и специальной техники Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент;

И. Н. Волосевич — доцент кафедры оперативно-разыскной деятельности и специальной техники Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент;

Е. Н. Хазов — профессор кафедры конституционного и муниципального права Московского университета МВД России имени В.Я. Кикотя, доктор юридических наук, профессор.

Information about the authors

A. V. Bogdanov — Associate Professor of the Department of Operational Investigative Activities and Special Equipment of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Candidate of Legal Sciences, Associate Professor;

I. N. Volosevich — Associate Professor of the Department of Operational Investigative Activities and Special Equipment of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Candidate of Legal Sciences, Associate Professor;

E. N. Khazov — Professor of the Department of Constitutional and Municipal Law of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Doctor of Legal Sciences, Professor.

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.

Статья поступила в редакцию 03.06.2025; одобрена после рецензирования 10.06.2025; принята к публикации 17.06.2025.

The article was submitted 03.06.2025; approved after reviewing 10.06.2025; accepted for publication 17.06.2025.