Мария Юрьевна ТАРАСОВА,
кандидат юридических наук, доцент
Волгоградская академия МВД России (г. Волгоград)
доцент кафедры оперативно-разыскной деятельности и специальной техники
tarasovawo.mariya@yandex.ru

Михаил Александрович БУГЕРА,
доктор юридических наук, доцент
Краснодарский университет МВД России (г. Краснодар)
профессор кафедры уголовного права и криминологии
ma.bugera@mail.ru

Научная статья
УДК 343.85:[343.9.024:004]

ПРОТИВОДЕЙСТВИЕ ЦИФРОВОЙ ПРЕСТУПНОСТИ: ТРИ ВЕКТОРА ЗАКОНОДАТЕЛЬНЫХ ИНИЦИАТИВ

КЛЮЧЕВЫЕ СЛОВА. Противодействие преступности, цифровая преступность, киберпреступление, информационно-телекоммуникационные технологии, средства сотовой связи, беспилотное воздушное судно.

АННОТАЦИЯ. ***Введение***. *Цифровая преступность стала магистральным вектором эволюции противоправной деятельности: от массовых телефонных мошенничеств до атак на критически важную инфраструктуру. Особое место в ней занимают операции с SIM-картами и смартфонами, включая кражи устройств с последующей легализацией через изменение IMEI-номеров. Новая угроза связана с расширением использования в криминальных целях беспилотных воздушных судов, управление которыми нередко осуществляется через сети сотовой связи. Противодействие таким вызовам со стороны преступного мира требует от государства не точечных, а системных мер.* ***Методы***. *В ходе исследования, результаты которого представлены в статье, применялся общенаучный диалектический метод познания окружающей действительности, предполагающий полное и всестороннее изучение явлений, рассмотрение связей и противоречий между ними. Кроме того, были востребованы абстрагирование, обобщение и статистический метод.* ***Результаты***. *В 2025 году в России впервые удалось добиться снижения числа цифровых преступлений. В качестве ключевого инструмента была использована государственная информационная система, объединившая данные правоохранительных органов, операторов связи и регуляторов. Внедрен механизм временной блокировки иностранных SIM-карт, а все беспилотные воздушные суда оснащаются средствами удаленной идентификации с интеграцией в систему «ЭРА-ГЛОНАСС». Законодательным ответом на хищения смартфонов стало создание единого реестра IMEI с привязкой к SIM-карте. Тем не менее сохраняется значительный правовой пробел – отсутствие уголовной ответственности за перепрограммирование IMEI. В связи с этим авторами предлагаются направления совершенствования законодательства с учетом зарубежного опыта и рисков переходного периода.*

ВВЕДЕНИЕ

Современный уровень технической оснащенности преступной деятельности не позволяет рассматривать сегодня цифровую преступность в качестве частной криминалистической проблемы или второстепенного явления. Напротив, данный криминальный сегмент выступает одним из магистральных векторов эволюции преступности в XXI веке. Деяния, совершаемые с применением информационно-коммуникационных технологий (далее – ИКТ), трансформировались из экзотических форм в повседневную реальность, охватывая спектр от массовых веерных телефонных мошенничеств до целевых атак на объекты критической инфраструктуры [1, с. 76]. Особое место в структуре цифровой преступности занимают противоправные операции, непосредственно связанные с использованием SIM-карт и смартфонов: фишинговые рассылки, хищения денежных средств со счетов граждан, а также кражи самих мобильных устройств с последующей их «легализацией» через изменение идентифи-

Maria Yu. TARASOVA,
Cand. Sci. (Jurisprudence), Associate Professor
Volgograd Academy of the Ministry of the Interior of Russia (Volgograd, Russia)
Associate Professor of the Department of Operational Investigative Activities and Special Equipment
tarasovawo.mariya@yandex.ru

Mikhail A. BUGERA,
Doctor of Law, Associate Professor
Krasnodar University of the Ministry of the Interior of Russia (Krasnodar, Russia)
Professor of the Department of Criminal Law and Criminology
ma.bugera@mail.ru

COUNTERING DIGITAL CRIME: THREE VECTORS OF LEGISLATIVE INITIATIVES

KEYWORDS. Countering crime, digital crime, cybercrime, cellular communications, unmanned aerial vehicles, information and telecommunications technologies.

ANNOTATION. ***Introduction***. *Digital crime has become the main vector of the evolution of illegal activity: from mass telephone fraud to attacks on critical infrastructure. A special place in this trend belongs to transactions with SIM cards and smartphones, including the theft of devices followed by legalization by changing IMEI numbers. A new threat is associated with the increasing use of unmanned aerial vehicles for criminal purposes, which are often controlled via cellular networks. Countering such challenges from the criminal underworld requires systemic rather than targeted measures from the state.* ***Methods***. *The study, the results of which are presented in the article, employed a general scientific dialectical method of understanding reality, which involves a complete and comprehensive study of phenomena, examining the connections and contradictions between them. Abstraction, generalization, and statistical methods were also required.* ***Results***. *In 2025, Russia achieved a reduction in the number of digital crimes for the first time. The key tool was a state information system that combined data from law enforcement agencies, telecom operators, and regulators. A temporary blocking mechanism for foreign SIM cards has been implemented, and all unmanned aerial vehicles are equipped with remote identification systems integrated into the ERA-GLONASS system. The legislative response to smartphone theft has been the creation of a unified IMEI registry linked to SIM cards. However, a significant legal gap remains: the lack of criminal liability for IMEI reprogramming. Therefore, the authors propose areas for legislative improvement, taking into account international experience and the risks of the transition period.*

кационных номеров (IMEI) [2, с. 25]. Принципиально важно, что те же каналы сотовой связи и те же инструменты (SIM-карты, идентификаторы устройств) всё чаще используются для совершения преступлений других видов. Параллельно с эскалацией классических киберугроз в последние годы обозначился качественно новый вызов – применение беспилотных воздушных судов (далее – БВС) в криминальных целях, включая разведывательные и ударные операции со стороны недружественных государств. Управление такими аппаратами нередко осуществляется дистанционно через сети сотовой связи, что делает контроль за SIM-картами и мобильными устройствами критически значимым и для противодействия беспилотной угрозе. Оба описанных выше явления (и связанные с ними хищения средств сотовой связи) требуют не разрозненных, точечных мер, а системной, внутренне согласованной работы, адекватной масштабу угроз.

Проведенное нами исследование имело следующие цели: выявить специфику цифровых преступлений, совершаемых с использованием SIM-карт и смартфонов; оценить системы защиты от противоправного применения БВС (с учетом того, что они управляются через сети сотовой связи) и механизмы пресечения хищений средств сотовой связи; определить, какие организационные, материально-технические и правовые затруднения возникают при реализации законодательных инициатив, ориентированных на противодействие цифровой преступности; обосновать перспективные пути реформирования российского законодательства в рассматриваемой сфере.

МЕТОДЫ

В ходе исследования, результаты которого представлены в статье, в качестве общенаучной основы познания применялся диалектический метод. Это позволило рассмотреть законодательные инициативы и противоправные явления (киберпреступления, причиняющее вред использование БВС, хищения средств сотовой связи) комплексно, во взаимосвязях, развитии и противоречиях, что способствовало формированию целостного, а не фрагментарного взгляда на предмет исследования. Метод абстрагирования и обобщения позволил выделить ключевые, существенные признаки анализируемых законодательных новелл и сформулировать общие выводы о логике государственной политики в сфере цифровой безопасности без отвлечения на частные и второстепенные детали. Статистический метод был применен для изучения динамики преступлений, совершаемых с использованием ИКТ и в сфере компьютерной информации (в частности для констатации факта снижения количества таких преступлений в 2025 году), что позволило эмпирически обосновать эффективность принятых мер.

РЕЗУЛЬТАТЫ

На расширенных заседаниях коллегии МВД России последних лет неизменно обсуждается блок вопросов, касающихся противодействия цифровой преступности. В 2024 году Президент Российской Федерации В.В. Путин, выступая на оче-

редном из таких заседаний, одну из стратегических целей органов внутренних дел сформулировал следующим образом: требуется переломить имеющуюся негативную тенденцию и обеспечить устойчивое снижение уровня цифровых преступлений[1]. Министр внутренних дел В.А. Колокольцев в марте 2026 года отчитался перед главой государства с трибуны коллегии о выполнении данного поручения[2]: в 2025 году число преступлений, совершенных с применением ИКТ, снизилось. С учетом того, что в предшествовавшее десятилетие наблюдался неуклонный рост киберпреступности, данный факт имеет важное политическое и криминологическое значение. Впервые зафиксированное снижение годового показателя свидетельствует о том, что совокупность принимаемых мер приобрела системный характер, а выбранные правовой и организационный векторы государственной политики в сфере борьбы с цифровой преступностью являются верными.

Ключевым инструментом достижения такого результата стало выстраивание эффективного межведомственного взаимодействия МВД России с Банком России, ФСБ, Росфинмониторингом и операторами связи – институтами, без координации работы с которыми противодействие киберугрозам объективно невозможно. Практика показала, что изолированные усилия каждого ведомства по отдельности в данной сфере ранее закономерно приводили к ограниченным результатам.

В ходе осуществленных мероприятий в 2025 году из незаконного оборота было изъято свыше 1800 SIM-банков (устройств для массовых мошеннических обзвонов) и более трех миллионов SIM-карт. Совместно с Национальным координационным центром по компьютерным инцидентам нейтрализовано порядка 1500 зарубежных IP-адресов, использовавшихся для управления вредоносным программным обеспечением. Качественным шагом вперед стало принятие Федерального закона от 1 апреля 2025 г. № 41-ФЗ[3], которым в России впервые была создана специализированная государственная информационная система, ориентированная исключительно на противодействие правонарушениям, совершаемым с применением ИКТ. Принципиальным в данном случае является переход от реагирования на отдельные инциденты к непрерывному мониторингу и межведомственной координации. Система объединила в общем контуре сведения, поступающие из правоохранительных органов, от операторов связи и регуляторов, чего ранее невозможно было добиться. Ее создание позволило наконец скоординировать усилия по всем перечисленным выше направлениям противодействия киберпреступности: прежде работа осуществлялась по ним в рамках решения отдельных, изолированных оперативных задач. В частности, пресечена аренда аккаунтов у недобросовестных граждан, заблокировано свыше 165 тысяч абонентских номеров, связанных с мошенниками, прекращено функционирование онлайн-площадок, созданных для торговли персональными данными [3, с. 13; 4, с. 123].

Вместе с тем необходимо отметить, что в 2025 году российские операторы связи запустили новый механизм противодействия одному из наиболее распространенных инструментов телефонного мошенничества – использованию иностранных SIM-карт. Суть новации заключается в том, что при попадании в Россию SIM-карта, зарегистрированная за рубежом, автоматически лишается доступа к сети Интернет и SMS-сообщениям на 24 часа; разблокировка требует верификации личности пользователя. Хотя внешне мера выглядит как ограничение для туристов, ее реальная цель – разрушить типичную схему, в условиях которой мошенники, физически находящиеся в России, используют зарегистрированные за ее пределами номера, не отслеживаемые отечественными операторами связи [5, с. 12]. Дополнительным эффектом оказывается создание препятствий для дистанционного управления БВС с задействованием зарубежных SIM-карт.

В целях обеспечения безопасности Постановлением Правительства Российской Федерации от 2 февраля 2026 г. № 83 с 1 марта 2026 года введена обязанность оснащать все БВС, допущенные к полетам на территории России, аппаратно-программными средствами удаленной идентификации с последующей интеграцией в государственную автоматизированную информационную систему «ЭРА-ГЛОНАСС», изначально разработанную для экстренного реагирования на дорожно-транспортные происшествия. Расширение ее функций на воздушное пространство является логичным шагом с учетом роста числа инцидентов с беспилотниками. Реализация новой нормы имеет большое значение для правоохранительной практики, так как данные о местонахождении и маршруте аппарата передаются в режиме реального времени. Это открывает возможность производства оперативно-разыскных мероприятий (в соответствии с Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности») в отношении операторов, противоправно использующих БВС. Фактически закладывается инфраструктурная основа для этого направления оперативно-разыскной деятельности [6, с. 62].

Отдельной проблемой, тесно связанной с контролем за мобильными устройствами, остаются хищения средств сотовой связи. Несмотря на повсеместное распространение биометрической защиты (сканеры отпечатков пальцев, системы распознавания лиц, двухфакторная аутентификация), криминальный интерес к смартфонам не снижа-

[1] Путин потребовал улучшить борьбу с преступлениями в сфере IT // ГОСТономика: сайт. 02.04.2024 // URL: https://gostonomica.ru/putin-potreboval-uluchshit-borbu-s-prestuplenijami-v-sfere-it/.

[2] Расширенное заседание коллегии МВД России // Президент России: сайт. 04.03.2026 // URL: http://www.kremlin.ru/events/president/transcripts/deliberations/79255.

[3] Федеральный закон от 01.04.2025 № 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».

ется. Только в Москве ежедневно регистрируется свыше 150 заявлений о кражах телефонов, по большей части это дорогостоящие флагманские модели. Типичные места совершения таких преступлений – объекты транспортной инфраструктуры и массового пребывания людей (метро, торговые центры, парки, рестораны) [7, с. 27]. Устойчивый спрос на похищенные гаджеты объясняется двумя факторами: во-первых, после изменения IMEI-номера их можно реализовать в качестве готовых к использованию устройств; во-вторых, активно развивается теневой рынок запасных частей (дисплеев, аккумуляторов, материнских плат), которые обращаются в «серой» зоне экономики независимо от правового статуса устройства-донора [8, с. 211]. Оба канала сбыта обеспечивают высокую рентабельность криминального бизнеса рассматриваемого вида.

Ответом государства на обострение проблемы стала подготовка законопроекта, предусматривающего создание единого реестра идентификационных номеров мобильных устройств (IMEI), включенного во второй пакет антикибермошеннических мер[1]. Он был одобрен обеими палатами парламента и направлен 17 июня 2026 года Президенту Российской Федерации на подписание. IMEI (International Mobile Equipment Identity) – уникальный 15-значный код, присваиваемый каждому мобильному устройству, который автоматически передается в сеть оператора при регистрации аппарата. Именно этот идентификатор является ключевым инструментом, используемым при розыске похищенных телефонов и проведении специальных технических мероприятий [9, с. 118]. Новый законодательный механизм предполагает внесение каждого ввозимого в нашу страну устройства сотовой связи в федеральный реестр (порядок его ведения определяет Правительство Российской Федерации). Операторы смогут оказывать телекоммуникационные услуги только тем абонентам, IMEI телефонов которых зафиксированы в этой базе данных. При заключении договора об услугах связи оператор обязан будет фиксировать в нем идентификатор конкретного устройства и привязку SIM-карты к данному аппарату. Повторное оформление карты, уже закрепленной за другим телефоном, станет технически невозможным.

Код IMEI для оперативно-разыскной деятельности важен еще и тем, что этот идентификатор позволяет устанавливать факт нахождения устройства в зоне действия определенной базовой станции, а также маршруты его перемещения и соотносить их с данными о личности пользователя [10, с. 159]. Привязка SIM-карты к IMEI в рамках единого реестра сформирует сквозную идентификационную цепочку «устройство – абонент – абонентский номер», что существенно повысит результативность поисковых мероприятий [11, с. 216]. Это в полной мере соответствует целям таких оперативно-розыскных мероприятий, предусмотренных ст. 6 Федерального закона «Об оперативно-розыскной деятельности», как наблюдение, прослушивание телефонных переговоров, снятие информации с технических каналов связи.

Однако именно возможность перепрограммирования IMEI-кода позволяет злоумышленникам «обнулять» идентификацию похищенного устройства, фактически легализуя его для последующего использования или перепродажи. В отечественном уголовном законодательстве в настоящее время такие действия не рассматриваются в качестве самостоятельного состава преступления [12, с. 24]. Уголовный кодекс Российской Федерации содержит нормы об ответственности за неправомерный доступ к компьютерной информации (ст. 272); за незаконные использование и (или) передачу, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272.1); за создание вредоносных программ (ст. 273). Но эти нормы не охватывают перепрограммирования идентификатора устройства сотовой связи.

Полагаем, было бы правильно дополнить Уголовный кодекс статьей 272.2 «Незаконные изменение, уничтожение или подделка идентификационного номера мобильного устройства (IMEI)». Это позволило бы устранить существующий ныне пробел. Тем более что практика ряда зарубежных государств предлагает готовые законодательные модели. Так, в США специального закона, прямо запрещающего изменение IMEI, не существует, однако использование чужого идентификационного номера для доступа к сети с 2020 года квалифицируется как мошенничество и наказывается лишением свободы на срок до 10 лет. В Республике Беларусь уголовная ответственность за изменение IMEI введена еще в 2008 году (ст. 350 УК РБ «Уничтожение, блокирование или модификация компьютерной информации»). В Индии функционирует Центральная база данных оборудования (CEIR), позволяющая блокировать похищенные устройства всем операторам одновременно. Аналогичные реестры действуют в Пакистане, ряде государств Африки и Юго-Восточной Азии. В России же акцент сделан на привязку IMEI к конкретной SIM-карте. Такой подход воспринимается участниками рынка как прецедент в мировой практике.

Предложенный российским законодателем единый реестр IMEI представляет собой не столько инструмент блокировки устройств (как в Индии), сколько механизм оперативно-разыскного характера, ориентированный на сквозную идентификацию абонента посредством привязки устройства к SIM-карте. Именно эта особенность определяет его практическое назначение и отличает от зарубежных аналогов. Нормативно-правовой фундамент такой идентификации абонента

[1] Законопроект № 1110676-8 «О внесении изменений в отдельные законодательные акты Российской Федерации (в части противодействия преступлениям, совершаемым с использованием информационных и коммуникационных технологий)» // Система обеспечения законодательной деятельности: сайт // URL: https://sozd.duma.gov.ru/bill/1110676-8.

заложен Федеральным законом от 31 июля 2020 г. № 248-ФЗ[1], который регулирует государственный контроль над хозяйствующими субъектами (речь о плановых и внеплановых проверках бизнеса). Впрочем, сам по себе факт нарушения оператором связи требований, касающихся идентификации абонентов, не является основанием для контрольной проверки. Выявление такого рода нарушений, если они сопряжены с преступной деятельностью, относится к компетенции правоохранительных органов: ч. 3 ст. 1 названного закона прямо выводит из сферы его действия оперативно-разыскную деятельность, дознание и предварительное следствие. Поэтому единый реестр IMEI – это инструмент не надзора за рынком, а оперативно-разыскной деятельности, что принципиально важно для определения его практического назначения. Соответственно, требуется криминализация нарушений, о которых идет речь.

Еще одним базовым нормативно-правовым актом, ориентированным на противодействие киберпреступности, является Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который за два десятилетия своего действия претерпел многочисленные изменения, каждый раз адаптируясь к новым вызовам цифровой среды. Данный закон регулирует распространение информации, порядок доступа к ней и ответственность за противоправные действия в цифровом пространстве.

Существенным элементом правовой системы обеспечения информационной безопасности стал Указ Президента Российской Федерации от 1 мая 2022 г. № 250[2]. Продекларированный им подход к проблеме принципиально отличается от традиционных. Ответственность за состояние информационной безопасности персонально возлагается на руководителей органов государственной власти и организаций, благодаря чему вопрос переводится из сугубо технической плоскости в управленческую. Кроме того, указ запрещает применение средств защиты информации, произведенных в недружественных государствах, что следует расценивать не только как меру безопасности, но и как стимул для развития отечественной отрасли информационной защиты. В совокупности с правоохранительными инструментами формируется двухуровневая модель: профилактика на организационном уровне плюс уголовно-правовое реагирование.

Здесь отметим, что развитие превентивной составляющей системы противодействия цифровой преступности нашло отражение в законопроекте о совершенствовании профилактики киберпреступлений[3] (одобрен Государственной Думой Российской Федерации и направлен 24 июня 2026 года в Совет Федерации). В частности, предлагается дополнить Федеральный закон от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» положением о таком самостоятельном направлении деятельности, как противодействие правонарушениям в сфере компьютерной информации и информационно-коммуникационных технологий, включая работу по выявлению и устранению причин и условий, способствующих их совершению. В законопроекте необходимо выделить три ключевые новеллы. Во-первых, противодействие киберпреступлениям приобретает самостоятельный статус в перечне направлений профилактики, что создает для региональных органов власти правовое основание для разработки и финансирования соответствующих целевых программ. Во-вторых, на федеральные ведомства и субъекты федерации возлагается обязанность информировать граждан о правилах цифровой безопасности посредством максимально широкого спектра каналов: платежные квитанции, SMS от операторов, национальный мессенджер «Макс», портал «Госуслуги», банковские офисы, МФЦ, отделения Социального фонда России. Для пожилых людей предусматриваются специальные форматы разъяснительной работы. В-третьих, Минцифры совместно с Минпросвещения наделяются полномочиями по выработке конкретных форматов информирования и координации деятельности субъектов системы профилактики. С точки зрения уголовно-правовой науки данная инициатива заслуживает положительной оценки: переход от традиционного реагирования на уже совершённые деяния к превентивной парадигме соответствует современным криминологическим представлениям о приоритете предупреждения преступлений [13, 14, 15]. Вместе с тем практическая эффективность закона будет во многом определяться качеством подзаконного регулирования и реальным финансовым обеспечением соответствующих программ.

ЗАКЛЮЧЕНИЕ

Государство последовательно переходит от реагирования на отдельные преступления к созданию инфраструктуры, в рамках которой совершение цифровых и сопряженных с ними преступлений объективно затруднено. Прежде всего речь о государственной информационной системе противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, которая закрывает каналы анонимной связи. Реестр IMEI лишает смысла хищение телефонов, идентификация БВС делает невозможным анонимное управление им. Каждая из этих мер по отдельности – лишь инструмент; в совокупности они образуют среду, создающую условия, при которых совершение цифровых пре-

[1] Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».
[2] Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
[3] Законопроект № 1106687-8 «О внесении изменения в статью 6 Федерального закона «Об основах системы профилактики правонарушений в Российской Федерации» (в части совершенствования государственной политики в сфере профилактики правонарушений)» // Система обеспечения законодательной деятельности: сайт // URL: https://sozd.duma.gov.ru/bill/1106687-8.

ступлений существенно затрудняется. Вместе с тем выявленный нами законодательный пробел – отсутствие самостоятельного состава преступления, связанного с изменением IMEI-номера, – остается уязвимым местом этой системы. Опыт США, Беларуси и Индии показывает: без криминализации этого деяния защитный потенциал реестра окажется ниже предполагавшегося уровня. Его будут обходить так же, как обходят любые другие идентификационные ограничения – путем перепрограммирования IMEI-кода. Устранение этого пробела должно стать важным шагом законодателя на пути противодействия цифровой преступности в России. ■

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алексеева А.П. Киберпреступность: насколько реальна угроза // Научно-методический электронный журнал «Концепт». 2017. № Т31. С. 76-80.

2. Глубоковских Р.В., Гринева Д.А. Характеристика оперативно-розыскного инструментария при раскрытии хищения денежных средств с банковских счетов // XIII Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2025. С. 25-27.

3. Алексеева А.П., Анисимова Т.В. Законодательные инициативы в сфере установления уголовной ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные: проблемы и перспективы // Уголовное законодательство: вчера, сегодня, завтра: Материалы международной научно-практической конференции. Спб: СПбУ МВД России, 2024. С. 13-15.

4. Катков С.В., Семененко Г.М., Костенко Н.С., Алексеева А.П. О мерах совершенствования организации работы оперативных и следственных подразделений МВД России по выявлению, раскрытию и расследованию хищений денежных средств с использованием банковских карт на территории Российской Федерации // Вестник Волгоградской академии МВД России. 2020. № 4 (55). С. 123-128.

5. Алексеева А.П. Кибермошенничество как объект криминологического исследования: анализ способов совершения и стратегий противодействия // Актуальные проблемы современного российского государства и права: Материалы всероссийской научно-практической конференции. Калининград: КФ СПбУ МВД России, 2025. С. 11-13.

6. Попов С.В. О некоторых вопросах развития оперативно-розыскной науки // XI Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2023. С. 62-63.

7. Алексеева А.П., Ничуговская О.Н. Киберпреступность: основные черты и формы проявления // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2017. № 1. С. 27-34.

8. Поляков А.В., Гринева Д.А. О возможностях использования информационных технологий в решении задач оперативно-розыскной деятельности // Межведомственный научно-практический Петербургский оперативно-розыскной форум: Материалы межведомственной научно-практической конференции. СПб: СПбУ МВД России, 2025. С. 211-215.

9. Контемирова Ю.В., Тарасова М.Ю. Современное состояние деятельности оперативных подразделений по противодействию хищениям денежных средств граждан, совершаемым с использованием информационно-телекоммуникационных технологий // Вестник Волгоградской академии МВД России. 2021. № 1 (56). С. 118-126.

10. Желудков М.А., Алексеева А.П. Обеспечение защищенности биометрических персональных данных от использования в криминальных целях // Вестник Санкт-Петербургского университета МВД России. 2025. № 2 (106). С. 159-169.

11. Попов С.В. К вопросу об особенностях обнаружения признаков мошеннических действий в сети Интернет // Межведомственный научно-практический Петербургский оперативно-розыскной форум: Материалы межведомственной научно-практической конференции. СПб: СПбУ МВД России, 2025. С. 216-219.

12. Алексеева А.П. Перспективы развития уголовного законодательства в киберсфере // Подготовка сотрудников полиции к использованию информационных технологий в борьбе с преступностью: Сборник научных трудов по материалам всероссийской межвузовской научно-практической конференции. Вып. 2. Волгоград: Волгоградская академия МВД России, 2017. С. 24-31.

13. Решняк О.А., Алексеева А.П. Использование IT-технологий в раскрытии и расследовании незаконного сбыта наркотических средств, совершаемого современными способами // Вестник Волгоградской академии МВД России. 2021. № 4 (59). С. 125-130.

14. Алексеева А.П. Цифровизация наркопреступлений и меры противодействия им // Межведомственный научно-практический Петербургский оперативно-розыскной форум: Материалы межведомственной научно-практической конференции. СПб: СПбУ МВД России, 2025. С. 16-19.

15. Герасимов А.В., Поляков А.В. К вопросу информационного воздействия на объекты оперативной заинтересованности // X Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии»: Материалы международной научно-практической конференции. Калининград: КФ СПбУ МВД России, 2022. С. 60-61.

REFERENCES

1. Alekseyeva A.P. Kiberprestupnost': naskol'ko real'na ugroza // Nauchno-metodicheskiy elektronnyy zhurnal «Kontsept». 2017. № T31. S. 76-80.
2. Glubokovskikh R.V., Grineva D.A. Kharakteristika operativno-rozysknogo instrumentariya pri raskrytii khishcheniya denezhnykh sredstv s bankovskikh schetov // XIII Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: KF SPbU MVD Rossii, 2025. S. 25-27.
3. Alekseyeva A.P., Anisimova T.V. Zakonodatel'nyye initsiativy v sfere ustanovleniya ugolovnoy otvetstvennosti za nezakonnyye ispol'zovaniye i peredachu, sbor i khraneniye komp'yuternoy informatsii, soderzhashchey personal'nyye dannyye: problemy i perspektivy // Ugolovnoye zakonodatel'stvo: vchera, segodnya, zavtra: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Spb: SPbU MVD Rossii, 2024. S. 13-15.
4. Katkov S.V., Semenenko G.M., Kostenko N.S., Alekseyeva A.P. O merakh sovershenstvovaniya organizatsii raboty operativnykh i sledstvennykh podrazdeleniy MVD Rossii po vyyavleniyu, raskrytiyu i rassledovaniyu khishcheniy denezhnykh sredstv s ispol'zovaniyem bankovskikh kart na territorii Rossiyskoy Federatsii // Vestnik Volgogradskoy akademii MVD Rossii. 2020. № 4 (55). S. 123-128.
5. Alekseyeva A.P. Kibermoshennichestvo kak ob"yekt kriminologicheskogo issledovaniya: analiz sposobov sovershеniya i strategiy protivodeystviya // Aktual'nyye problemy sovremennogo rossiyskogo gosudarstva i prava: Materialy vserossiyskoy nauchno-prakticheskoy konferentsii. Kaliningrad: KF SPbU MVD Rossii, 2025. S. 11-13.
6. Popov S.V. O nekotorykh voprosakh razvitiya operativno-rozysknoy nauki // XI Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: KF SPbU MVD Rossii, 2023. S. 62-63.
7. Alekseyeva A.P., Nichugovskaya O.N. Kiberprestupnost': osnovnyye cherty i formy proyavleniya // Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy. 2017. № 1. S. 27-34.
8. Polyakov A.V., Grineva D.A. O vozmozhnostyakh ispol'zovaniya informatsionnykh tekhnologiy v reshenii zadach operativno-rozysknoy deyatel'nosti // Mezhvedomstvennyy nauchno-prakticheskiy Peterburgskiy operativno-rozysknoy forum: Materialy mezhvedomstvennoy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2025. S. 211-215.
9. Kontemirova Yu.V., Tarasova M.Yu. Sovremennoye sostoyaniye deyatel'nosti operativnykh podrazdeleniy po protivodeystviyu khishcheniyam denezhnykh sredstv grazhdan, sovershayemym s ispol'zovaniyem informatsionno-telekommunikatsionnykh tekhnologiy // Vestnik Volgogradskoy akademii MVD Rossii. 2021. № 1 (56). S. 118-126.
10. Zheludkov M.A., Alekseyeva A.P. Obespecheniye zashchishchennosti biometricheskikh personal'nykh dannykh ot ispol'zovaniya v kriminal'nykh tselyakh // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2025. № 2 (106). S. 159-169.
11. Popov S.V. K voprosu ob osobennostyakh obnaruzheniya priznakov moshennicheskikh deystviy v seti Internet // Mezhvedomstvennyy nauchno-prakticheskiy Peterburgskiy operativno-rozysknoy forum: Materialy mezhvedomstvennoy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2025. S. 216-219.
12. Alekseyeva A.P. Perspektivy razvitiya ugolovnogo zakonodatel'stva v kibersfere // Podgotovka sotrudnikov politsii k ispol'zovaniyu informatsionnykh tekhnologiy v bor'be s prestupnost'yu: Sbornik nauchnykh trudov po materialam vserossiyskoy mezhvuzovskoy nauchno-prakticheskoy konferentsii. Vyp. 2. Volgograd: Volgogradskaya akademiya MVD Rossii, 2017. S. 24-31.
13. Reshnyak O.A., Alekseyeva A.P. Ispol'zovaniye IT-tekhnologiy v raskrytii i rassledovanii nezakonnogo sbyta narkoticheskikh sredstv, sovershayemogo sovremennymi sposobami // Vestnik Volgogradskoy akademii MVD Rossii. 2021. № 4 (59). S. 125-130.
14. Alekseyeva A.P. Tsifrovizatsiya narkoprestupleniy i mery protivodeystviya im // Mezhvedomstvennyy nauchno-prakticheskiy Peterburgskiy operativno-rozysknoy forum: Materialy mezhvedomstvennoy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2025. S. 16-19.
15. Gerasimov A.V., Polyakov A.V. K voprosu informatsionnogo vozdeystviya na ob"yekty operativnoy zainteresovannosti // KH Baltiyskiy yuridicheskiy forum «Zakon i pravoporyadok v tret'yem tysyacheletii»: Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kaliningrad: KF SPbU MVD Rossii, 2022. S. 60-61.

Авторы заявляют об отсутствии конфликта интересов.
Авторами внесён равный вклад в написание статьи.
The authors declare no conflicts of interests.
The authors have made an equal contribution to the writing of the article.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Тарасова М.Ю., Бугера М.А, Противодействие цифровой преступности: три вектора законодательных инициатив // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2026. № 2 (84). С. 43-49.