Дата поступления рукописи в редакцию: 10.05.2026 г.
Дата принятия рукописи в печать: 27.05.2026 г.
DOI: 10.24412/2782-3849-2026-5-149-152

МАЙСТРЕНКО Григорий Александрович,

кандидат юридических наук, старший научный сотрудник ФКУ НИИ ФСИН России, ORCID: 0000-0001-5668-615X,

e-mail: g.maystrenko@yandex.ru,

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: ХАРАКТЕРИСТИКА, ПРИЧИНЫ, МЕРЫ ПРОТИВОДЕЙСТВИЯ

Аннотация. *Анализ результатов работы за 2025 г. показал, что несмотря на принимаемые меры количество противоправных деяний в сфере информационно-коммуникационных технологий (ИКТ) остается стабильно высоким. Кроме того, следует отметить, что посягательства в сфере ИКТ с каждым годом занимают все более заметное место в структуре зарегистрированных преступлений. Если в 2018 г. удельный вес всех рассматриваемых деяний составлял порядка 9 %, то уже в 2025 г. – более 40 %. Высокие риски несет латентность ИКТ-преступлений, поскольку отсутствие оперативной реакции в отношении противоправных актов при недостаточной эффективности выявления их оперативных путем, создает предпосылки к росту пострадавших от таких преступлений.*

Ключевые слова: *информационно-коммуникационные технологии, преступление, мошенничество, компьютерная информация, интернет, финансовые организации, лишение свободы, латентность.*

MAISTRENKO Grigoriy Aleksandrovich,

senior researcher of the PKU Research Institute of the Federal Penitentiary Service of Russia

CRIMES COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES: CHARACTERISTICS, CAUSES, COUNTERACTION MEASURES

Annotation. *The analysis of the results of work for 2025 showed that, despite the measures taken, the number of illegal acts in the field of information and communication technologies (ICT) remains consistently high, with only every fourth attack being detected. In addition, it should be noted that attacks in the field of ICT are becoming more and more prominent in the structure of registered crimes every year. In 2018, the share of all the acts under consideration was about 9%, but by 2025, it will be more than 40%. The latency of ICT crimes poses a high risk, as the lack of prompt response to illegal acts and the insufficient effectiveness of their detection create the preconditions for an increase in victims of such crimes.*

Key words: *information and communication technologies, crime, fraud, computer information, Internet, financial organizations, imprisonment, latency.*

Основным инструментом, используемым мошенниками для хищения средств у населения, по-прежнему остаются методы социальной инженерии (106,8 тыс. посягательств или 48,8 %). Причина появления такого рода мошенничества – рост популярности интернет-банкинга и онлайн-услуг, а также утечки персональных данных из-за недостаточной защиты со стороны их операторов, а иногда подкупа сотрудников таких организаций. Имеются случаи массовой дискредитации указанных инструментов, когда преступники одномоментно получают доступ к тысячам счетов и данных физических лиц.

На этом фоне наблюдается тенденция к совершению персонифицированных атак, реализации которых предшествует детальное изучение личной информации и потенциальных жертв, в том числе самостоятельно размещаемой гражданами на различных ресурсах в сети Интернет, а также к использованию злоумышленниками мессенджеров для контакта с гражданами [3, с. 362].

Также заслуживает внимания проблематика, связанная с возможностью незаконного применения технологии подделки голоса и изображения. В отдельных случаях фиксируются факты использования таких технологий в противоправных целях. Они

становятся все более доступными и могут использоваться в целях сокрытия личности, фальсификации каких-либо событий, моделирования характеристик голоса конкретного лица и др.

Продолжают иметь место создание и функционирование «финансовых пирамид», причем организация их деятельности сместилась в виртуальное пространство. В результате взаимодействия Генеральной прокуратуры Российской Федерации и Банка России ограничен доступ к более чем 4 тыс. интернет-сайтам, распространяющим сведения о деятельности таких организаций.

За первые одиннадцать месяцев 2025 года в России зарегистрировано 627 тысяч киберпреступлений. Это на 10,8% меньше, чем за аналогичный период прошлого года. Основной массив правонарушений, почти две трети (63,4%), по-прежнему составляют хищения и мошенничества — зарегистрировано 397,4 тысячи таких случаев.

Значительный объем в структуре ИКТ-преступлений занимает сбыт наркотических средств. Число преступлений, связанных с незаконным оборотом наркотиков в интернете достигло 109,2 тысячи, что на 28,5% больше, чем годом ранее. На эту категорию теперь приходится почти каждое шестое (17,4%) киберпреступление в стране.

Ключевым каналом для противоправных действий остаются мессенджеры. С их помощью совершено 244,6 тысячи преступлений, что на 17,5% больше показателя за январь-ноябрь 2024 года (тогда было 208,2 тысячи)[4].

В своем выступлении на коллегии МВД в марте 2026г. Министр внутренних дел Колокольцев В. отметил, что вместе с тем размер имущественного ущерба от противоправных посягательств остается значительным.

Его основная часть приходится на деяния, совершенные с помощью информационно-коммуникационных технологий.

Здесь последовательно вырабатывались меры правового, организационного и практического характера.

При участии Министерства принят федеральный закон о создании государственной информационной системы противодействия IT-преступлениям.

В минувшем году из теневого оборота выведено более 1,8 тысячи сим-банков и свыше трёх миллионов сим-карт различных операторов.

Совместно с Национальным координационным центром по компьютерным инцидентам заблокировано порядка полутора тысяч иностранных IP-адресов.

Через них происходило управление вредоносными программами, с помощью которых злоумышленники пытались похитить денежные средства наших граждан.

Пресекались факты сдачи недобросовестными лицами во временную аренду своих учетных записей для последующего применения в противоправных целях.

С операторами связи осуществлена блокировка более 165 тысяч привязанных к ним абонентских номеров.

Ликвидирован ряд крупных ресурсов и сервисов по продаже персональных данных.

В целом возросло число предварительно расследованных тяжких и особо тяжких IT-деяний, а также совершенных в составе организованных групп или сообществ.

Повысилась общая эффективность раскрытия киберпреступлений.

Кроме того, принятые меры позволили добиться снижения дистанционных краж, мошенничеств, фактов неправомерного доступа к компьютерной информации[11]. При исследовании учеными исследователями отмечается, что все чаще на практике в совершение таких преступлений вовлекаются несовершеннолетние [2, с. 20-21].

Раскрываемость рассматриваемого вида преступлений остается невысокой и составляла в 2021 г. – 23,4 %, в 2022 г. – 27,8 %, в 2023 г. – 26,6 %, в 2024 – 25,7 % [4]. Изучение сведений, поступивших из субъектов Российской Федерации, показало, что в определенной степени такой ситуации способствуют особенности объективной стороны совершаемых преступлений (бесконтактное хищение денежных средств с использованием систем дистанционного банковского обслуживания), а также возникающие при этом сложности в установлении информации преступниках и их местонахождении.

В то же время практика прокурорского надзора свидетельствует, что одной из основных причин низкой раскрываемости данных преступлений является отсутствие наступательности при производстве предварительного расследования со стороны следователей и дознавателей, низкая интенсивность расследования, а также ненадлежащий ведомственный контроль руководства органов расследования за своевременностью производства следственных и процессуальных действий.

На фоне роста негативных показателей в данном сегменте органами внутренних дел повсеместно допускаются факты укрытия криминальных деяний от регистрации, несвоевременное возбуждение уголовных дел, длительное непроведение следственных и иных

процессуальных действий, утрата информации, имеющей доказательственное значение [8, с. 65].

В целом принимаемые меры по выявлению и раскрытию преступлений несоразмерны оперативной обстановке в данной сфере. Отмечается нехватка специалистов по борьбе с преступлениями в сфере ИКТ; отсутствие в ряде регионов экспертных учреждений, которым может быть поручено производство наиболее востребованных экспертиз, их недостаточная оснащенность и т.д.

В первом полугодии 2025 года российские суды назначили наказание 225 осужденным за преступления в сфере компьютерной информации, следует из официальных данных Судебного департамента при Верховном суде (ВС) РФ[12], большей части из которых назначено реальное лишение свободы. При этом нередко к ответственности за мошеннические действия привлекаются лишь курьеры, непосредственно получавшие у потерпевших денежные средства, либо иные номинальные участники преступлений. По преступлениям в сфере компьютерной информации виновные лица в основном осуждаются за нелегальное копирование личных данных абонентов операторов сотовой связи и детализацию их переговоров, несанкционированный доступ к личным страницам в социальных сетях, электронным почтовым ящикам [5, с. 77].

С учетом изложенных вопросов противодействия ИКТ-преступлениям в последнее время уделяется особое внимание на всех уровнях государственной власти и управления, совместно вырабатываются дополнительные меры как профилактического характера, так и направленные на совершенствование способов выявления и раскрытия противоправных деяний [7, с. 47].

Представляется целесообразным регламентировать использование средств видео-конференц-связи (в частности, с использованием беспилотных технических средств) для проведения таких следственных действий, как осмотр места преступления в условиях военных действий, техногенных или природных катастроф и по иным направлениям, в случае если традиционный формат проведения процессуального мероприятия создает угрозу жизни или здоровья лицам в них участвующих.

Важным в противодействии ИКТ-преступности является внедрение и более активное использование современных технических средств и информационно-аналитических комплексов. В целях профилактики данного вида преступлений актуальная просветительская и справочная информация публикуется в социальных сетях и мессенджерах [1, с. 56].

В целом в Российской Федерации продолжают формироваться условия для обеспечения информационной безопасности. Вместе с тем следует констатировать, что меры информационной защиты, подобно всем мерам юридического противодействия криминальным явлениям, всегда имеют догоняющий характер [6, с. 103]. Неурегулированность общественных отношений в электронной цифровой среде способствовала активизации криминальных посягательств на имущественные права и интересы физических и юридических лиц, внедрению бесконтактных способов преступлений, а также высокой конспирации лиц их совершивших и, как следствие, латентности такого рода деяний.

Список литературы:

[1] Бойко О.А., Унукович А.С. Детерминанты латентных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Юридический вестник Самарского университета. – 2020. – №3. – С. 53-59.

[2] Букалерова Л.А., Остроушко А.В., Криез О. Преступления против информационной безопасности несовершеннолетних, совершаемые посредством информационно-телекоммуникационных сетей (включая сеть интернет) // Вестник СПбГУ. Серия 14. Право. – 2021. – №1. – С. 17-35.

[3] Гончарова С.В., Полунина Е.Н. Киберпреступления и преступления по телефону // БГЖ. – 2020. – №3 (32). – С. 359-363.

[4] Информация МВД России о состоянии преступности в январе – ноябрь 2025 года / URL: https://мвд.рф/reports/item/51988292// (дата обращения: 18.04.2026).

[5] Каримов А.М.Преступления в сфере компьютерной информации и преступления, совершаемые с использованием информационно-коммуникационных технологий: сравнительно-правовой аспект // Вестник Казанского юридического института МВД России. – 2023. – №1 (51). –

С. 75-82.

[6] Мнацаканян А.В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты: дис. … канд. юрид. наук. – М., 2015. – 216 с.

[7] Нуянзин С.В., Виноградов А.О., Тришкин С.В.Преступность в сфере информационно-телекоммуникационных технологий: современное состояние и некоторые меры по противодействию ей // Научный портал МВД России. –2020. – №4 (52). – С. 45-54.

[8] Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым

с использованием информационно-коммуникационных технологий: учеб.пособ. – М., 2018. – 115 с.

[9] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации от 17 июня 1996 г. № 25 ст. 2954 (изм. в ред. декабрь 2025г.)

[10] Федеральный закон от 26 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448 (в ред. Федерального закона от 12 декабря 2023 г. № 588-ФЗ).

[11] Выступление Владимира Колокольцева на расширенном заседании коллегии МВД России.

[12] Данные Судебного департамента при Верховном суде (ВС) РФ за 2025г.

References:

[1] Boyko O.A., Unukovich A.S. Determinants of latent crimes committed using information and telecommunication technologies//Legal Bulletin of Samara University. – 2020. – №3. - S. 53-59.

[2] Bukalerova L.A., Ostroushko A.V., Kriez O. Crimes against the information security of minors committed through information and telecommunication networks (including the Internet)//Bulletin of St. Petersburg State University. Series 14. Right. – 2021. – №1. - S. 17-35.

[3] Goncharova S.V., Polunina E.N. Cybercrimes and crimes by phone//BGJ. – 2020. – №3 (32). - S. 359-363.

[4] Information of the Ministry of Internal Affairs of Russia on the state of crime in January - November 2025/URL: https ://mvd.rf/reports/item/51988292//(date of reference: 18.04.2026).

[5] Karimov A.M. Crimes in the field of computer information and crimes committed using information and communication technologies: comparative legal aspect//Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. – 2023. – №1 (51). –

S. 75-82.

[6] Mnatsakanyan A.V. Information security in the Russian Federation: criminal legal aspects: dis.... cand. jurid. sciences. - M., 2015. - 216 s.

[7] Nuyanzin S.V., Vinogradov A.O., Trishkin S.V. Accessibility in the field of information and telecommunication technologies: the current state and some measures to counter it//Scientific portal of the Ministry of Internal Affairs of Russia. –2020. – №4 (52). - S. 45-54.

[8] E.A. Russkevich. Criminal law counteraction to crimes committed using information and communication technologies: instructional. - M., 2018. - 115 s.

[9] Criminal Code of the Russian Federation of June 13, 1996 No. 63-FZ//Collection of Legislation of the Russian Federation of June 17, 1996 No. 25, Art. 2954 (rev. December 2025)

[10] Federal Law No. 149-FZ of July 26, 2006 “On Information, Information Technologies and Information Protection “//Collection of Legislation of the Russian Federation No. 31 of July 31, 2006 (Part I) Art. 3448 (as amended by Federal Law No. 588-FZ of December 12, 2023).

[11] Speech by Vladimir Kolokoltsev at an expanded meeting of the board of the Ministry of Internal Affairs of Russia.

[12] Data of the Judicial Department under the Supreme Court of the Russian Federation for 2025