Дата поступления рукописи в редакцию: 26.03.2026 г.
Дата принятия рукописи в печать: 30.04.2026 г.
DOI: 10.24412/2076-1503-2026-4-867-876

СКВОРЦОВ Константин Васильевич,
кандидат технических наук, доцент,
доцент кафедры специальной техники и информационных технологий юридического факультета ВЮИ ФСИН России,
г. Владимир, ORCID: 0000-0001-8611-3353,
e-mail: k-skv@yandex.ru

СИЛЕНКОВ Виктор Иванович,
кандидат педагогических наук, доцент,
начальник кафедры гуманитарных и социально-экономических дисциплин инженерно-технического факультета Университета ФСИН России, г. Санкт Петербург,
ORCID: 0000-0002-4806-0737,
e-mail.: silenkov61@gmail.com

КИБЕРПРЕСТУПНОСТЬ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ИСТОРИКО-КРИМИНОЛОГИЧЕСКИЙ АНАЛИЗ (2000–2025 гг.)

Аннотация. *Статья посвящена комплексному анализу эволюции киберпреступности в Российской Федерации за период с 2000 по 2025 год. На основе статистических данных МВД РФ, Генеральной прокуратуры, результатов исследований российских учёных, а также новостных СМИ, прослежена трансформация структуры, масштабов и методов совершения киберпреступлений в РФ. Выявлена периодизация развития данного феномена, включающая этап зарождения (2000–2010), этап экспоненциального роста (2011–2019), «пандемический скачок» (2020–2022) и современный этап системной зрелости (2023–2025). Проанализированы ключевые законодательные инициативы по противодействию киберпреступности и перспективы снижения киберпреступной активности. Сделан вывод о переходе от экстенсивного роста киберпреступности к формированию институциональных механизмов противодействия, требующих дальнейшего развития прогнозных моделей и межведомственного взаимодействия.*

Ключевые слова: *киберпреступность, информационная безопасность, цифровизация, социальная инженерия, уголовное законодательство, критическая информационная инфраструктура, кибермошенничество, уголовно-исполнительная система, ФСИН России.*

SKVORTSOV Konstantin Vasilyevich,
PhD in Technical Sciences,
Associate Professor of the Department of Special Equipment and Information Technologies of the Faculty of Law VUI of the Federal Penitentiary Service of Russia, Vladimir

SILENKOV Viktor Ivanovich,
Candidate of Pedagogical Sciences,
Associate Professor Head of the Department of Humanities and Socio-Economic Disciplines, Faculty of Engineering and Technology, University of the Federal Penitentiary Service of Russia, Saint Petersburg

CYBERCRIME IN THE RUSSIAN FEDERATION: A HISTORICAL AND CRIMINOLOGICAL ANALYSIS (2000–2025)

Annotation. *This article presents a comprehensive analysis of the evolution of cybercrime in the Russian Federation from 2000 to 2025. Based on statistical data from the Ministry of Internal Affairs of the Russian Federation, the Prosecutor General's Office, research findings by Russian*

scholars, and news media reports, the transformation of the structure, scale, and methods of committing cybercrimes in Russia is traced. A periodization of the development of this phenomenon is identified, including the emergence stage (2000–2010), the exponential growth stage (2011–2019), the "pandemic surge" (2020–2022), and the current stage of systemic maturity (2023–2025). Key legislative initiatives to counteract cybercrime and the prospects for reducing cybercriminal activity are analyzed. The conclusion is drawn about a transition from the extensive growth of cybercrime to the formation of institutional counteraction mechanisms, which require further development of predictive models and interagency cooperation.

Key words: *cybercrime, information security, digitalization, social engineering, criminal legislation, critical information infrastructure, cyber fraud, penal enforcement system, Federal Penitentiary Service of Russia.*

Введение.

Стремительная цифровизация всех сфер жизни российского общества в XXI веке сопровождается столь же стремительным ростом преступлений, совершаемых с использованием информационно-коммуникационных технологий (далее – ИКТ). Проблематика киберпреступности находится в фокусе внимания российских ученых на протяжении последних двадцати лет. Фундаментальные основы понятия, состояния и уголовно-правовых мер борьбы были заложены в работах В.А. Номоконова и Т.Л. Тропиной [1; 2]. Вопросы взаимосвязи цифровой трансформации и криминала поднимаются в трудах В.П. Кириленко, Г.В. Алексеева [3] и Ю.Ю. Комлева [4], который обосновывает необходимость развития цифровой девиантологии. Организованный характер современной киберпреступности исследуют В.С. Овчинский и Ю.Н. Жданов [5]. Эволюцию методов и структуры преступлений анализируют Л.П. Зверянская [6], Д.В. Жмуров [7] и специалисты профильных компаний [8; 9]). Комплексный обзор современной криминогенной ситуации, включая анализ ущерба и судебной практики, представлен в работе К.В. Мордвинова и У.А. Удавихиной [10]. Однако, несмотря на обилие публикаций, комплексные историко-криминологические исследования, охватывающие весь период эволюции (2000–2025 гг.) и рассматривающие проблему в единстве ее технических, социальных, правовых и пенитенциарных аспектов, остаются фрагментарными.

Особого внимания заслуживает тот факт, что киберугрозы проникли во все элементы правоохранительной системы, включая уголовно-исполнительную систему (УИС). Учреждения ФСИН России, с одной стороны, сталкиваются с использованием своего контингента для совершения дистанционных мошенничеств, а с другой – сами всё чаще становятся объектом целенаправленных атак на критическую информационную инфраструктуру, что создает дополнительные риски для безопасности и требует адекватного институционального ответа.

Цель настоящего исследования – провести комплексный историко-криминологический анализ эволюции киберпреступности в Российской Федерации, выявить основные этапы и закономерности её развития, оценить эффективность законодательных мер противодействия и определить перспективные направления борьбы с данным видом преступности.

Исследование основано на системном и сравнительно-правовом подходах. Эмпирическую базу составляют новостные ленты федеральных СМИ, статистические данные МВД Российской Федерации, Генеральной прокуратуры и Следственного комитета РФ о состоянии преступности за период 2014–2025 годов. Так же, использованы аналитические отчёты организаций Positive Technologies, F6, «Лаборатории Касперского» и данные Банка России. Теоретическую базу составили работы российских учёных в области уголовного права, криминологии и информационной безопасности.

Периодизация эволюции киберпреступности в России

На основании анализа нормативно-правовой базы, статистических данных и научных публикаций можно выделить четыре основных этапа эволюции киберпреступности в Российской Федерации.

1. **Этап зарождения (до 2010): от хакерского хулиганства к кардингу.**

Как отмечает Л.П. Зверянская [6], предпосылки для формирования киберпреступности в России были заложены ещё в 1990-х годах, когда хакерство носило преимущественно хулиганский характер – взлом программ для обхода защиты авторских прав, написание вирусов с демонстрационным функционалом. Первым известным «хакером» в истории СССР стал выпускник МГУ Мурат Уртембаев, который в 1983 году внёс изменения в код программы на заводе «АвтоВАЗ», что привело к остановке конвейера на три дня [11].

С массовым распространением интернета в России (число пользователей выросло с 47 млн в

2009 году до 70 млн в 2012 году) произошла криминализация киберпространства. В этот период возникли первые подпольные форумы (Carderplanet и др.), специализирующиеся на обмене украденными данными банковских карт. Громкие дела – взлом Citibank Владимиром Левиным (1994), деятельность русскоязычных кардинговых группировок – сделали «русских хакеров» одним из устойчивых медийных образов [12].

Правовое реагирование на новые угрозы нашло отражение в принятии главы 28 УК РФ «Преступления в сфере компьютерной информации» со статьями 272 (Неправомерный доступ к компьютерной информации), 273 (Создание, использование и распространение вредоносных программ) и 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей). В 2000 году была утверждена первая Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 N ПР-1895), определившая стратегические направления защиты национальных информационных ресурсов.

2. Этап экспоненциального роста (2011–2019): формирование индустрии киберпреступности.

Второе десятилетие XXI века характеризуется трансформацией киберпреступности из сферы деятельности отдельных хакеров-одиночек в полноценную криминальную индустрию. Как отмечают В.П. Кириленко и Г.В. Алексеев киберпреступность стала теснейшим образом связана с процессами цифровой трансформации общества [3]. Экосистема IT-преступлений стала базироваться на разделении ролей: разработчики вредоносного ПО, операторы ботнетов, продавцы эксплойтов, обнальщики и иные «специалисты» формировали целый теневой рынок [13]. Статистика демонстрирует взрывной рост: если в 2013 году БСТМ МВД фиксировал порядка 11 тыс. компьютерных преступлений, то к 2017 году – уже 90,6 тыс. (4,4% всех преступлений), к 2019 году – 294,4 тыс. (+68,5% к 2018 году). По данным Следственного комитета, за период с 2014 по 2022 год число IT-преступлений выросло более чем в 50 раз [14].

Важнейшим законодательным ответом на растущие угрозы стало принятие в декабре 2016 года обновлённой Доктрины информационной безопасности РФ (Указ Президента РФ от 05.12.2016 № 646), заменившей документ 2000 года. Новая Доктрина ввела актуальные понятия и термины, а её целью стала защита интересов человека, общества и государства от угроз, связанных с использованием ИКТ в военных и политических целях. В 2017 году был принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», установивший правовые основы защиты объектов КИИ от компьютерных атак и определивший полномочия государственных органов в данной сфере. Одновременно УК РФ был дополнен ст. 274.1, предусматривающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

3. «Пандемический скачок» (2020–2022): кризис как катализатор.

Пандемия COVID-19 стала мощнейшим катализатором роста киберпреступности в России. Массовый переход на удалённый режим работы и обучения, расширение использования онлайн-сервисов при одновременно низком уровне цифровой грамотности населения создали идеальные условия для кибермошенников [15,16]. По данным Генпрокуратуры РФ, в 2020 году число киберпреступлений увеличилось на 73,4% и составило 510,3 тыс., а их доля в структуре преступности возросла до 25%. Наиболее значительный рост зафиксирован в Санкт-Петербурге – на 780% (с 2,2 тыс. в 2019 году до 19,5 тыс.). Как констатировал начальник главного организационно-аналитического управления Генпрокуратуры А. Некрасов, число киберпреступлений достигло масштабов, «позволяющих говорить о них как об угрозе национальной безопасности» [17]. В 2021 году рост замедлился до 1,4% (~518 тыс.), а в 2022 году впервые с 2017 года наблюдалось незначительное снижение – до ~510–522 тыс. Однако эксперты RTM Group оценили ущерб от действий хакеров по итогам 2021 года в 150 млрд рублей, а рост результативных атак составил 35% – преимущественно за счёт телефонного мошенничества и схем социальной инженерии [18]. Этот период стал переломным в понимании природы киберпреступности: из технического феномена она превратилась в социальную проблему государственного масштаба. Как показали, рассмотренные выше, исследования, ключевыми факторами стали: низкий уровень цифровой грамотности населения, недостаточная эффективность антифрод-инфраструктуры и невысокий процент раскрываемости (менее 25%).

4. Этап системной зрелости (2023–2025): рекорды и первые признаки перелома.

Период 2023–2025 годов характеризуется, с одной стороны, достижением рекордных показателей киберпреступности, а с другой – появлением первых позитивных тенденций. Статистические данные [14,19,20] свидетельствуют о следующей динамике:

Год	Число зарегистрированных IT-преступлений	Динамика к предыдущему году	Доля в общей преступности	Ущерб (млрд руб.)
2022	~522 тыс.	–1,9%	26,5%	–
2023	677 тыс.	+29,7%	~35%	156
2024	765,4 тыс.	+13,1%	40%	200
2025	675 тыс.	–11,8%	38%	—

Рост в 2023 году на 29,7% частично объясняется расширением перечня преступлений, относящихся к категории IT-преступлений в статистическом учёте МВД. Тем не менее именно 2024 год стал пиковым: 765,4 тыс. зарегистрированных преступлений, 40% в общей структуре преступности – максимум с 2020 года. Министр внутренних дел В. Колокольцев констатировал: «Если пять лет назад в общем массиве криминальных проявлений киберпреступления занимали седьмую часть, то сейчас они уже занимают 40%».[14]. Вместе с тем финансовые потери продолжают расти: средний ущерб от дистанционных хищений увеличился на 5% в 2025 году, а число пострадавших несовершеннолетних выросло почти вдвое [21].

Трансформация структуры и методов киберпреступности.

Анализ эволюции методов киберпреступлений выявляет устойчивый тренд смещения от чисто технических атак к методам психологического манипулирования. По данным Positive Technologies, в IV квартале 2024 года социальная инженерия оставалась ведущим методом атак: на организации – в 50% случаев, на частных лиц – в 88%. Рост фишинговых атак в 2024 году составил 50%, а ущерб от вишинга (телефонного мошенничества) достиг 250 млрд рублей [22, 23]. По данным, ведущего разработчика технологий для борьбы с киберпреступностью, компании «F6» [9], в 2025 году в публичный доступ попало более 767 млн строк с персональными данными российских пользователей, а рекорд суммы выкупа за зашифрованную компанию достиг 500 млн рублей.

Особую тревогу вызывает рост атак на критическую информационную инфраструктуру (КИИ). По данным Positive Technologies, на промышленность в период с июля 2024 года по сентябрь 2025 года пришлось 17% всех успешных кибератак (рост на 6 п.п. по сравнению с 2023 годом), на государственные учреждения – 11%, на IT-компании – 9%. Компания F6 прогнозирует сохранение высокого уровня угроз для промышленности и госсектора в 2026 году. По прогнозам, число успешных кибератак в 2025 году может увеличиться на 20–45%, а в 2026 году – ещё на 30–35% [24]. Президент РФ В.В. Путин в феврале 2026 акцентировал внимание на необходимости внедрения инновационных методов борьбы с киберугрозами [25]. В качестве ключевой задачи было определено дальнейшее совершенствование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) [26].

Эволюция киберугроз в адрес пенитенциарной системы.

Особым и недостаточно изученным аспектом эволюции киберпреступности в России является её проявление в рамках уголовно-исполнительной системы Российской Федерации (далее – УИС). Анализ ее роли позволяет выделить два взаимосвязанных, но разнонаправленных вектора. С одной стороны, учреждения ФСИН России могут выступать в качестве среды, потенциально благоприятствующей совершению киберпреступлений. Как отмечают исследователи [27], отдельные категории осужденных, несмотря на изоляцию, демонстрируют способность адаптироваться к современным технологическим реалиям. Речь идет о преступлениях в сфере телекоммуникаций и мошенничеств, совершаемых с использованием мобильной связи и сети Интернет. Статистика изъятия средств связи в исправительных учреждениях свидетельствует о сохраняющейся латентной угрозе использования пенитенциарной системы как плацдарма для противоправной деятельности в цифровом пространстве. В связи с этим перед УИС стоит задача постоянного совершенствования режимных требований и профилактических мер, направленных на нейтрализацию данного вида вызовов. С другой стороны, сама

уголовно-исполнительная система все чаще становится объектом противоправного вмешательства извне. В современной научной литературе [28], обоснованно выделяются основные направления киберугроз в адрес учреждений и сотрудников УИС. К ним относятся попытки несанкционированного доступа к ведомственным базам данных, содержащим персональные данные сотрудников и спецконтингента, а также атаки на критическую информационную инфраструктуру. Компрометация таких сведений создает риски для безопасности учреждений и может быть использована для оказания давления на сотрудников, дестабилизации обстановки или сокрытия иных правонарушений. Масштаб и системность данных угроз подтверждаются практикой последних лет. Крупные киберинциденты, затронувшие официальные ресурсы ведомства в 2021 и 2022 годах, когда хакеры взломали сайты ведомства и разместили сообщения политического характера [29; 30]. По данным заместителя директора ФСИН С.В. Щербакова, в 2024 году зафиксировано более 600 значимых киберинцидентов, среди которых 46 попыток внедрения вредоносного программного обеспечения, более 1 тыс. DDoS-атак и свыше 10 тыс. различных событий информационной безопасности. С.В. Щербаков подчеркнул, что речь идёт о целенаправленной работе против системы: «Такие атаки не совершаются группой студентов – это коллективы людей, иногда и сотрудников спецслужб иностранных государств» [31]. Признавая высокую значимость данных угроз, государством предпринимаются последовательные институциональные меры. Во исполнение Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», в центральном аппарате ФСИН и территориальных органах УИС созданы структурные подразделения, ответственные за обеспечение информационной безопасности, обнаружение, предупреждение и ликвидацию последствий компьютерных атак [32]. Таким образом, роль уголовно-исполнительной системы в контексте противодействия киберпреступности характеризуется комплексностью и требует дальнейшего осмысления. Представляется обоснованным рассматривать УИС одновременно в двух качествах: как объект преступных посягательств, нуждающийся в надежной эшелонированной защите, и как субъект профилактики, призванный пресекать использование собственной инфраструктуры в киберпреступных целях. Дальнейшее укрепление информационной безопасности УИС видится не только как ведомственная задача, но и как важный элемент обеспечения национальной безопасности в целом. В этой связи представляется необходимым продолжение работы по гармонизации законодательства, внедрению передовых технологических решений и углублению межведомственного взаимодействия для эффективного реагирования на современные киберугрозы, источником или целью которых становится пенитенциарная система.

Формирование системы нормативно-правового противодействия киберпреступности.

Законодательная база противодействия киберпреступности в России претерпела значительную эволюцию. Ключевые нормативно-правовые акты можно систематизировать следующим образом:

Год	Нормативный акт	Содержание
1996	Глава 28 УК РФ (ст. 272–274)	Базовые составы преступлений в сфере компьютерной информации
2000	Доктрина информационной безопасности	Первый стратегический документ в сфере информационной безопасности
2011	Федеральный закон от 07.12.2011 N 420-ФЗ	Модернизация ст. 272 УК РФ
2016	Доктрина информационной безопасности (новая)	Актуализация стратегии информационной безопасности с учётом новых угроз
2017	Федеральный закон от 26.07.2017 № 187-ФЗ + ст. 274.1 УК РФ	Защита КИИ и уголовная ответственность за атаки на неё
2024	Федеральный закон от 30.11.2024 № 421-ФЗ (ст. 272.1 УК РФ)	Уголовная ответственность за незаконный оборот персональных данных

Особого внимания заслуживает введение в декабре 2024 года статьи 272.1 УК РФ, установившей уголовную ответственность за незаконное использование, использование и (или) передача, 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. Максимальное наказание по наиболее тяжкому составу – лишение свободы на срок до 10 лет со штрафом в размере до трех миллионов рублей. Как указывает И.Г. Чекунов в диссертационном исследовании [33], ключевой задачей является переход от экстенсивных к интенсивным криминологическим мерам предупреждения киберпреступности на основе разработки специализированных информационных систем. Генеральный прокурор И. Краснов в 2024 году отметил снижение раскрываемости IT-преступлений до 25,9%, раскритиковав «шаблонность, безынициативность и отсутствие наступательности» в оперативной работе. Так же, президент В.В. Путин на коллегии МВД в марте 2025 года указал, что раскрываемость киберпреступлений снизилась до 23%, а ущерб за 2024 год превысил 200 млрд рублей, при этом четверть пострадавших составляют пенсионеры [35].

Ситуация, озвученная на высшем уровне, потребовала немедленной реакции и консолидации усилий правоохранительных органов и законодателей, что, по-видимому, и обеспечило долгожданный эффект. Так, итоги 2025 года демонстрируют перелом негативной динамики, когда впервые за последние годы зафиксировано снижение числа IT-преступлений на 11,8% – до 675 тыс [36]. Количество дистанционных краж уменьшилось на 23,6%, дистанционных мошенничеств – на 9%, преступлений в сфере компьютерной информации – на 42,2% [37]. Замминистра цифрового развития И. Лебедев отмечает, что по отдельным составам киберпреступлений снижение достигло 30% [38]. Число нераскрытых преступлений снизилось на 13,5% – до 494,3 тыс [39]. Этому способствовали:

– вступление в силу комплексных мер по борьбе с кибермошенничеством (сентябрь 2025 года); - активизация деятельности специализированных подразделений МВД по борьбе с IT-преступлениями;
– международное сотрудничество: в 2025 году направлено 215 запросов о правовой помощи в 28 стран;
– развитие антифрод-систем: банки во II квартале 2025 года предотвратили почти 38,7 млн попыток хищений на сумму 3,4 трлн рублей [40].
– формирование ГосСОПКА как единой системы реагирования на компьютерные инциденты.

Заключение. Проведённое исследование позволяет констатировать, что киберпреступность в Российской Федерации за период 2000–2025 годов прошла путь от маргинального явления до одной из ключевых угроз национальной безопасности. Рост числа IT-преступлений более чем в 70 раз за десять лет (с ~10 тыс. в 2014 до 765,4 тыс. в 2024 году), увеличение совокупного ущерба до 200 млрд рублей ежегодно и проникновение киберпреступных элементов в 40% всей структуры преступности свидетельствуют о системном характере проблемы. Важным выводом исследования является то, что киберпреступность затрагивает все элементы правоохранительной системы, включая уголовно-исполнительную систему, которая одновременно является источником киберпреступлений (мошенничества осуждённых) и объектом целенаправленных кибератак со стороны иностранных злоумышленников.

Вместе с тем данные 2025 года дают основания для осторожного оптимизма: впервые зафиксировано снижение числа IT-преступлений, что связано как с законодательными мерами (в том числе принятием в 2024 году УК РФ Статья 272.1. и комплексных антимошеннических мер), так и с развитием институциональных механизмов противодействия. Как подчеркнул Председатель Государственной Думы В. Володин, «правоохранительные органы впервые за последние годы фиксируют сокращение преступлений, совершённых с использованием информационно-телекоммуникационных технологий» [41].

Перспективные направления научных исследований в данной области могут включать: разработку криминологических прогнозных моделей на основе анализа больших данных (в русле предложений Ю.Ю. Комлева о методологической триангуляции эмпирических методов и вычислительных алгоритмов [4]); совершенствование механизмов оперативного информационного обмена между правоохранительными органами и финансовыми организациями; развитие виктимологического направления профилактики; исследование влияния технологий искусственного интеллекта на трансформацию методов киберпреступности; а также совершенствование системы информационной безопасности учреждений и органов УИС, включая внедрение технологий искусственного интеллекта, многоуровневой аутентификации и организацию межведомственного взаимодействия МВД, ФСИН с ФСТЭК и профильными IT-компаниями.

Список литературы:

[1] Номоконов В.А., Тропина Т.Л. Киберпреступность: угрозы, прогнозы, проблемы борьбы // Information Technology and Security. 2013. № 1(3).

[2] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: диссертация на соискание ученой степени кандидата юридических наук / Тропина Татьяна Львовна. – Владивосток, 2005. – 235 с. – EDN NNKIKF

[3] Кириленко В.П., Алексеев Г.В. Киберпреступность и цифровая трансформация // Теоретическая и прикладная юриспруденция. 2021. № 1(7). С. 39–53. DOI: 10.22394/2686-7834-2021-1-39-53.

[4] Комлев Ю.Ю. От цифровизации социума к киберпреступности, кибердевиантности и развитию цифровой девиантологии // Российский девиантологический журнал. 2022. Т. 2. № 1. С. 17–26.

[5] Жданов Ю.Н. Киберполиция XXI века. Международный опыт / Ю.Н. Жданов, В.С. Овчинский. - Москва: Международные отношения, 2020. - 288 с. - ISBN 978-5-7133-1652-5.

[6] Зверянская Л.П. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений // Концепт. 2016. Т. 15. С. 881–885.

[7] Жмуров Д.В. От иерархии к сетям: децентрализация в криминальной среде // Российский следователь. 2025. № 4. С. 56–60. DOI: 10.18572/1812-3783-2025-4-56-60

[8] Positive Technologies. Лидер результативной кибербезопасности. URL: https://ptsecurity.com/(дата обращения 15.02.2026).

[9] F6. Киберугрозы-2025: F6 назвала основные тренды вымогателей, утечек и фишинга // CISO Club. – 2025. – 16 дек. – URL: https://cisoclub.ru/kiberugrozy-2025-f6-nazvala-osnovnye-trendy-vymogatelej-utechek-i-fishinga/ (дата обращения 15.02.2026)

[10] Мордвинов К.В., Удавихина У.А. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. 2022. № 1(11). С. 83–88. DOI: 10.22394/2686-7834-2022-1-83-88.

[11] «Русские хакеры» действительно существуют. Откуда они появились, как стали звездами и почему их боится Запад? // Lenta.ru. – 2021. – 20 авг. – URL: https://lenta.ru/articles/2021/08/20/russians_are_coming (дата обращения 20.02.2026)

[12] Петухов С. Дело хакера №1: Подробности величайшего ограбления века // Коммерсантъ. – 1999. – 14 февр. – URL: https://www.kommersant.ru/doc/2286437 (дата обращения 20.02.2026)

[13] Трущенков, И. В. Киберпреступность в России: векторы изменений / И. В. Трущенков, И. Г. Трущенкова // Advances in Law Studies. – 2022. – Т. 10, № 2. – С. 31-35. – DOI 10.29039/2409-5087-2022-10-2-31-35. – EDN QEWFOH.

[14] Число киберпреступлений в России URL: https://www.tadviser.ru/index.php/Статья:-Число_киберпреступлений_в_России (дата обращения 01.02.2026).

[15] Швыряев, П. С. Киберпреступность в России: новый вызов для общества и государства / П. С. Швыряев // Государственное управление. Электронный вестник. – 2021. – № 89. – С. 184-196. – DOI 10.24412/2070-1381-2021-89-184-196. – EDN KFWYZW.

[16] Шикула, И. Р. Киберпреступность в Российской Федерации: основные методы борьбы и проблемы противодействия / И. Р. Шикула, Е. Н. Куркин // Международный журнал экспериментального образования. – 2023. – № 1. – С. 37-41. – DOI 10.17513/mjeo.12119. – EDN CESTGI.

[17] В Генпрокуратуре заявили, что киберпреступность стала представлять угрозу нацбезопасности // ТАСС. – 2021. – 24 мая. – URL: https://tass.ru/obschestvo/11451173 (дата обращения: 15.03.2026).

[18] Послwoвская Ю., Буйлов М. Взлом высоких технологий: Годовой ущерб от киберпреступлений растет // Коммерсантъ. – 2022. 17 февр. URL: https://www.kommersant.ru/doc/5218254 (дата обращения: 10.02.2026).

[19] В России в 2024 году IT-преступления достигли пика за последние пять лет // ТАСС. – 2024. – URL: https://tass.ru/proisshestviya/22978955 (дата обращения: 21.02.2026).

[20] В РФ в 2024 году ущерб от IT-преступлений вырос почти на 40 % и составил 200 млрд рублей // Независимая газета. – 2024. – URL: https://www.ng.ru/news/811035.html (дата обращения: 21.02.2026).

[21] В России средний ущерб от киберпреступлений вырос на 5 %. При этом число потерпевших уменьшилось // ТАСС. – 2025. – URL: https://tass.ru/obschestvo/26009207 (дата обращения: 21.02.2026).

[22] Диреев И.Д. Социальная инженерия в контексте информационной безопасности / И.Д. Диреев // Международный научно-исследовательский журнал. – 2025. – №3 (153). – URL: https://research-journal.org/archive/3-153-2025-march/10.60797/IRJ.2025.153.121 (дата обращения: 28.02.2026)

[23] Социальная инженерия, вооруженная ИИ: как защитить себя? // Билайн: Big Data – URL: https://bigdata.beeline.ru/blog/articles/socialnaya-inzheneriya-i-big-data (дата обращения: 02.02.2026)

[24] Forbes Staff. Взлеты и нападения: кибератак на Россию будет все больше // Forbes. – 2025. – 7 окт. – URL: https://www.forbes.ru/tekhnologii/547308-vzlety-i-napadenia-kiberatak-na-rossiu-budet-vse-bol-se (дата обращения: 10.03.2026).

[25] Путин призвал внедрять новые методы противодействия киберпреступности // Финмаркет. – 2026. – 24 февр. – URL: https://www.finmarket.ru/news/6566900 (дата обращения: 10.03.2026).

[26] Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации/ URL: https://gossopka.ru/ (дата обращения: 01.03.2026).

[27] Скворцов, К. В. О мерах профилактики киберпреступлений в уголовно-исполнительной системе Российской Федерации / К. В. Скворцов, В. И. Силенков // Профессиональное юридическое образование и наука. – 2024. – № 3(15). – С. 61-63. – EDN USZQFG.

[28] Скворцов, К. В. Кибератаки как угроза информационной безопасности учреждениям и органам уголовно-исполнительной системы Российской Федерации / К. В. Скворцов, В. И. Силенков, А. В. Печенин // Профессиональное юридическое образование и наука. – 2025. – № 1(17). – С. 48-51. – EDN EPQAVA.

[29] Сайт ФСИН заработал после призыва основателя Gulagu.net к хакерам остановить атаку // Коммерсантъ. – 2021. – URL: https://www.kommersant.ru/doc/5152575?tg (дата обращения: 01.03.2026).

[30] Хакеры взломали сайты Минцифры, ФАС, ФСИН и других российских ведомств // Российская газета. – 2022. – 8 марта. – URL: https://rg.ru/2022/03/08/hakery-vzlomali-sajty-minci-fry-fas-fsin-i-drugih-rossijskih-vedomstv.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 01.03.2026).

[31] Замглавы ФСИН рассказал, кто стоит за кибератаками на системы службы // РИА Новости. – 2025. – 21 марта. – URL: https://ria.ru/20250321/fsin-2006348431.html (дата обращения: 01.03.2026).

[32] Щербаков, С. Проблемы с колл-центрами в учреждениях ФСИН не существует / С. Щербаков // РИА Новости. – 2025. – 21 марта. – URL: https://ria.ru/20250321/scherbakov-2006375882.html (дата обращения: 01.03.2026).

[33] Чекунов, И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: автореферат диссертации на соискание ученой степени кандидата юридических наук / Чекунов Игорь Геннадьевич. – Москва, 2013. – 22 с. – EDN ZPBUOJ.

[34] Интернет-мошенники в 2024 г. отобрали у россиян более 150 миллиардов // CNews. – 2024. – 5 дек. – URL: https://www.cnews.ru/news/top/2024-12-05_summa_ushcherba_ot_dejstvij (дата обращения: 02.03.2026).

[35] Путин: ущерб от кибермошенничества превысил 200 млрд рублей в 2024 году. Как сообщил президент, раскрываемость таких преступлений снизилась и составила порядка 23 % // ТАСС. – 2025. – 5 марта. – URL: https://tass.ru/politika/23313189 (дата обращения: 01.03.2026).

[36] Число IT-преступлений в России в 2025 году сократилось до 675 тыс. // ТАСС. – 2026. – 9 февр. – URL: https://tass.ru/obschestvo/26385451 (дата обращения: 15.03.2026)

[37] В России в 2025 году IT-преступлений стало меньше почти на 12% // ТАСС. – 2026. – 29 янв. – URL: https://tass.ru/obschestvo/26280465 (дата обращения: 15.03.2026)

[38] В Минцифры заявили о снижении числа киберпреступлений в России // Интерфакс. – 2026. – 9 февр. – URL: https://www.interfax.ru/digital/1071821 (дата обращения: 10.03.2026)

[39] МВД: число киберпреступлений в России снизилось на 12 % в 2025 году // Коммерсантъ. – 2025. – URL: https://www.kommersant.ru/doc/8442339 (дата обращения: 21.02.2026).

[40] Обзор отчётности об инцидентах информационной безопасности при переводе денежных средств. II квартал 2025 года // Центральный банк Российской Федерации. – 2025. – 7 августа. – URL: https://cbr.ru/statistics/ib/ (дата обращения: 11.02.2026).

[41] Вячеслав Володин: ГД 10 февраля рассмотрит комплекс новых мер по противодействию кибермошенничеству // Государственная Дума. – 2026. – 9 февр. – URL: http://duma.gov.ru/news/62978/ (дата обращения: 15.03.2026)

References:

[1] Nomokonov VA, Tropina TL Cybercrime: threats, forecasts, problems of struggle//Information Technology and Security. 2013. № 1(3).

[2] Tropina T. L. Cybercrime: concept, state, criminal law measures of struggle: specialty 12.00.08 “Criminal law and criminology; criminal executive law”: dissertation for the degree of candidate of legal sciences/Tropina Tatyana Lvovna. - Vladivostok, 2005. – 235 c. – EDN NNKIKF

[3] Kirilenko V.P., Alekseev G.V. Cybercrime and digital transformation//Theoretical and applied jurisprudence. 2021. № 1(7). S. 39-53. DOI: 10.22394/2686-7834-2021-1-39-53.

[4] Komlev Yu. Yu. From digitalization of society to cybercrime, cyberdeviance and the development of digital deviantology//Russian Deviantological Journal. 2022. VOL. 2. № 1. S. 17-26.

[5] Zhdanov Yu.N. Cyber police of the XXI century. International experience/Yu.N. Zhdanov, V.S. Ovchinsky. - Moscow: International Relations, 2020. - 288 p. - ISBN 978-5-7133-1652-5.

[6] Zveryanskaya L.P. Historical analysis of the stages of development of cybercrime and the features of modern cybercrimes//Concept. 2016. VOL. 15. S. 881-885.

[7] D.V. Zhmurov. From hierarchy to networks: decentralization in the criminal environment//Russian investigator. 2025. №4. S. 56-60. DOI: 10.18572/1812-3783-2025-4-56-60

[8] Positive Technologies. Leader of effective cybersecurity. URL: https://ptsecurity.com/ (date of contact 15.02.2026).

[9] F6. Cyber threats-2025: F6 named the main trends in ransomware, leaks and phishing// CISO Club. – 2025. – 16 дек. – URL: https://cisoclub.ru/kiberugrozy-2025-f6-nazvala-osnovnye-trendy-vymogatelej-utechek-i-fishinga/ (дата обращения 15.02.2026)

[10] Mordvinov K.V., Udavikhina U.A. Cybercrime in Russia: current challenges and successful practices in the fight against cybercrime//Theoretical and applied jurisprudence. 2022. № 1(11). S. 83-88. DOI: 10.22394/2686-7834-2022-1-83-88.

[11] "Russian hackers" do exist. Where did they come from, how did they become stars and why is the West afraid of them ?// Lenta.ru. – 2021. - Aug 20 - URL: https://lenta.ru/articles/2021/08/20/russians_are_coming (contact date 20.02.2026)

[12] Petukhov S. Hacker case No. 1: Details of the greatest robbery of the century//Kommersant. – 1999. - Feb. 14 - URL: https://www.kommersant.ru/doc/2286437 (date of contact 20.02.2026)

[13] Schulenkov, I.V. Cybercrime in Russia: vectors of change/I.V. Schulenkov, I.G. Schulenkov// Advances in Law Studies. – 2022. - T. 10, NO. 2. - S. 31-35. – DOI 10.29039/2409-5087-2022-10-2-31-35. – EDN QEWFOH.

[14] Number of cybercrimes in Russia URL: https://www.tadviser.ru/index.php/Статья: Number of _ cybercrimes _ in _ Russia (date of contact 01.02.2026).

[15] Shvyryaev, P. S. Cybercrime in Russia: a new challenge for society and the state/P. S. Shvyryaev//Public Administration. Electronic bulletin. – 2021. – № 89. - S. 184-196. – DOI 10.24412/2070-1381-2021-89-184-196. – EDN KFWYZW.

[16] Shikula, I. R. Cybercrime in the Russian Federation: basic methods of struggle and problems of counteraction/I. R. Shikula, E. N. Kurkin//International Journal of Experimental Education. – 2023. – № 1. - S. 37-41. – DOI 10.17513/mjeo.12119. – EDN CESTGI.

[17] The Prosecutor General's Office said that cybercrime began to pose a threat to national security//TASS. – 2021. - May 24. - URL: https://tass.ru/obschestvo/11451173 (access date: 15.03.2026).

[18] Poslavskaya Yu., Buylov M. Hacking high technologies: Annual damage from cybercrimes is growing//Kommersant. – 2022. Feb. 17 URL: https://www.kommersant.ru/doc/5218254 (access date: 10.02.2026).

[19] In Russia in 2024, IT crimes have peaked over the past five years//TASS. – 2024. - URL: https://tass.ru/proisshestviya/22978955 (access date: 21.02.2026).

[20] In the Russian Federation in 2024, the damage from IT crimes increased by almost 40% and amounted to 200 billion rubles//Nezavisimaya Gazeta. – 2024. - URL: https://www.ng.ru/news/811035.html (access date: 21.02.2026).

[21] In Russia, the average damage from cybercrimes increased by 5%. At the same time, the number of victims decreased//TASS. – 2025. - URL: https://tass.ru/obschestvo/26009207 (access date: 21.02.2026).

[22] Direev I.D. Social Engineering in the Context of Information Security/I.D. Direev//International Research Journal. – 2025. – №3 (153). - URL: https://research-journal.org/archive/3-153-2025-march/10.60797/IRJ.2025.153.121 (Accessed: 28.02.2026)

[23] AI-armed social engineering: how to protect yourself ?//Beeline: Big Data - URL: https://bigdata.beeline.ru/blog/articles/socialnaya-inzheneriya-i-big-data (Accessed: 02.02.2026)

[24] Forbes Staff. Ups and attacks: there will be more and more cyber attacks on Russia//Forbes. – 2025. – 7 окт. – URL: https://www.forbes.ru/tekhnologii/547308-vzlety-i-napadenia-kiberatak-na-rossiu-budet-vse-bol-se (дата обращения: 10.03.2026).

[25] Putin called for the introduction of new methods of countering cybercrime//Finmarket. – 2026. - Feb. 24 - URL: https://www.finmarket.ru/news/6566900 (access date: 10.03.2026).

[26] State System for Detection, Prevention and Elimination of Consequences of Computer Attacks on Information Resources of the Russian Federation/ URL: https://gossopka.ru/ (accessed on: 01.03.2026).

[27] Skvortsov, K. V. On measures to prevent cybercrime in the penal system of the Russian Federation/K. V. Skvortsov, V. I. Silenkov//Professional legal education and science. – 2024. – № 3(15). - S. 61-63. – EDN USZQFG.

[28] Skvortsov, K.V. Cyberattacks as a threat to information security to institutions and bodies of the penal system of the Russian Federation/K.V. Skvortsov, V.I. Silenkov, A.V. Pechenin//Professional legal education and science. – 2025. – № 1(17). - S. 48-51. – EDN EPQAVA.

[29] The FSIN website started working after the Gulagu.net founder called on hackers to stop the

attack//Kommersant. – 2021. - URL: https://www.kommersant.ru/doc/5152575?tg (access date: 01.03.2026).

[30] Hackers hacked the websites of the Ministry of Digital Science, the Federal Antimonopoly Service, the Federal Penitentiary Service and other Russian departments//Rossiyskaya Gazeta. – 2022. - March 8. – URL: https://rg.ru/2022/03/08/hakery-vzlomali-sajty-mincifry-fas-fsin-i-drugih-rossijskih-vedomstv.html?utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 01.03.2026).

[31] The deputy head of the FSIN told who is behind the cyber attacks on the service systems//RIA Novosti. – 2025. - March 21. - URL: https://ria.ru/20250321/fsin-2006348431.html (access date: 01.03.2026).

[32] Shcherbakov, S. There are no problems with call centers in FSIN institutions/S. Shcherbakov// RIA Novosti. – 2025. - March 21. - URL: https://ria.ru/20250321/scherbakov-2006375882.html (access date: 01.03.2026).

[33] Chekunov, I. G. Criminological and criminal legal support for the prevention of cybercrime: specialty 12.00.08 “Criminal Law and Criminology; criminal executive law”: abstract of the dissertation for the degree of candidate of legal sciences/Igor Gennadievich Chekunov. - Moscow, 2013. – 22 c. – EDN ZPBUOJ.

[34] Internet scammers in 2024 took away more than 150 billion from Russians//CNews. – 2024. - Dec 5 - URL: https://www.cnews.ru/news/top/2024-12-05_summa_ushcherba_ot_dejstvij (Accessed: 02.03.2026).

[35] Putin: the damage from cyber fraud exceeded 200 billion rubles in 2024. According to the president, the detection rate of such crimes decreased and amounted to about 23 %//TASS. – 2025. - March 5. - URL: https://tass.ru/politika/23313189 (access date: 01.03.2026).

[36] The number of IT crimes in Russia in 2025 decreased to 675 thousand//TASS. – 2026. - Feb. 9 - URL: https://tass.ru/obschestvo/26385451 (accessed on: 15.03.2026)

[37] In Russia in 2025, IT crimes decreased by almost 12 %//TASS. – 2026. - Jan 29 - URL: https://tass.ru/obschestvo/26280465 (Accessed: 15.03.2026)

[38] The Ministry of Digital Industry announced a decrease in the number of cybercrimes in Russia// Interfax. – 2026. - Feb. 9 - URL: https://www.interfax.ru/digital/1071821 (accessed on: 10.03.2026)

[39] Ministry of Internal Affairs: the number of cybercrimes in Russia decreased by 12% in 2025// Kommersant. – 2025. - URL: https://www.kommersant.ru/doc/8442339 (access date: 21.02.2026).

[40] Information Security Incident Reporting Review for Funds Transfers. II quarter of 2025//Central Bank of the Russian Federation. – 2025. - August 7. - URL: https://cbr.ru/statistics/ib/ (access date: 11.02.2026).

[41] Vyacheslav Volodin: On February 10, the State Duma will consider a set of new measures to counter cyber fraud//State Duma. – 2026. - Feb. 9 - URL: http://duma.gov.ru/news/62978/ (accessed on: 15.03.2026)