

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Пензенский государственный университет»

Юридический институт
дисциплин»

Кафедра «Государственно-правовых
(наименование)

Направление подготовки

40.03.01
(код)

Юриспруденция
(наименование)

Профиль «Правозащитная деятельность»
(наименование)

БАКАЛАВРСКАЯ РАБОТА

по теме: «Киберпреступления в современной России.
Типология правонарушений и методы противодействия»

Студент 22ЮЮ1
номер группы

подпись, дата

Щербаков Андрей Максимович
фамилия, имя, отчество полностью

Научный руководитель К.И.Н., доцент
должность

ПГУ, каф. ГПД
наименование организации

подпись, дата

Костин В.Е.
фамилия, инициалы

Консультанты:

по _____
наименование раздела, звание, должность

подпись, дата

фамилия, инициалы

по _____
наименование раздела, звание, должность

подпись, дата

фамилия, инициалы

по _____
наименование раздела, звание, должность

подпись, дата

фамилия, инициалы

Нормоконтролер: К.Ю.Н., доцент
должность

подпись, дата

Елистратова О.В.
фамилия, инициалы

Работа допущена к защите в (протокол заседания кафедры от _____ 2026 № __)

Заведующий кафедрой «Г.П.Д.»
название

подпись, дата

С.Ю. Суменков
фамилия, инициалы

Работа защищена с оценкой _____ (Протокол от _____ 2026 г. № __)

Секретарь ГЭК

подпись, дата

Антипкина Е.Г.
фамилия, инициалы

Пенза, 2026 г.

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Юридический институт

Направление 40.03.01 «Юриспруденция»

Профиль «Правозащитная деятельность»

УТВЕРЖДАЮ

Зав. кафедрой «Государственно-правовых дисциплин»

_____/ С.Ю. Суменков /
(подпись) (ф.и.о. фамилия)

____ 2026г.

ЗАДАНИЕ

на выпускную квалификационную работу студента гр. № 22 ЮЮ1

Щербакова Андрея Максимовича

1. Тема работы: Киберпреступления в современной России. Типология правонарушений и методы противодействия

2. Научный руководитель: к.ю.н., доцент каф. ГПД Костин В.Е.

3. Дата выдачи задания: 25.12.2025 г.

4. Срок сдачи студентом законченной работы: 18.05.2026 г.

5. Перечень подлежащих разработке вопросов:

5.1 Понятие и признаки киберпреступлений в Российской Федерации

5.2 Типология киберпреступлений в Российской Федерации

5.3 Нормативно-правовое регулирование противодействия киберпреступлениям в Российской Федерации

5.4 Показатели и структура киберпреступлений, расследуемых правоохранительными органами

5.5 Характеристика основных видов киберпреступлений по данным Следственного комитета Российской Федерации

5.6 Методы противодействия и расследования киберпреступлений Российской Федерации

6. Консультанты по работе, с указанием относящихся к ним разделов работы:

Раздел	Консультант	Подпись, дата	
		Задание выдал	Выполненное задание принял
Введение		03.02.2026 г. Костин В.Е.	21.02.2026 г. Костин В.Е.
Теоретико-правовые основы киберпреступлений в российской федерации		21.02.2026 г. Костин В.Е.	21.03.2026 г. Костин В.Е.
Статистический анализ киберпреступлений и методы противодействия		21.03.2026 г. Костин В.Е.	18.04.2026 г. Костин В.Е.
Выводы		18.04.2026 г. Костин В.Е.	19.05.2026 г. Костин В.Е.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	5
1. Теоретико-правовые основы киберпреступлений в российской федерации	8
1.1. Понятие и признаки киберпреступлений в Российской Федерации .	8
1.2. Типология киберпреступлений в Российской Федерации.....	14
1.3. Нормативно-правовое регулирование противодействия киберпреступлениям в Российской Федерации	25
2. Статистический анализ киберпреступлений и методы Противодействия.....	30
2.1. Показатели и структура киберпреступлений, расследуемых правоохранительными органами	30
2.2. Характеристика основных видов киберпреступлений по данным Следственного комитета Российской Федерации	37
2.3. Методы противодействия и расследования киберпреступлений Российской Федерации.....	52
ЗАКЛЮЧЕНИЕ	61
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	66
ПРИЛОЖЕНИЯ	72

ВВЕДЕНИЕ

Актуальность темы. Актуальность темы исследования киберпреступлений в современной России обусловлена стремительной цифровизацией общества и постоянным ростом масштабов противоправной деятельности в информационной сфере. За 11 месяцев 2025 года в России было зарегистрировано 627 тысяч киберпреступлений, что на 10,8 % меньше, чем за аналогичный период 2024 года. При этом некоторые категории преступлений показали свой рост, а именно почти 2/3 (64,3 %) зарегистрированных киберпреступлений - хищения и мошенничество (397,4 тысячи случаев). Число преступлений, связанных с незаконным оборотом наркотиков в интернете достигло 109,2 тысячи, что на 28,5 % больше, чем за 2024 год. На данную категорию приходится почти шестое (17,4 %) киберпреступление в стране. Мессенджеры остаются основным каналом для противоправных действий. С их помощью совершено 244,6 тысячи преступлений – на 17,5 % больше, чем за январь-ноябрь 2024 года (208,2 тысячи). К 2026 году сложность и частота кибератак достигли беспрецедентного уровня. Технологические достижения, к сожалению, работают в обе стороны, вооружая преступников новыми инструментами. Киберпреступники используют поддельные письма, СМС- сообщения и веб-сайты. Данная тенденция 2025 года сохраняется и в начале 2026 года. Например, фишинг, как вид интернет-мошенничества и социальной инженерии, целью которого является получение доступа к конфиденциальным данным пользователей, перестал быть просто «письмом с ошибками». Отправляя 10 персонализированных фишинговых писем (*Spear Phishing*), киберпреступник имеет 90 % шанс, что как минимум, один сотрудник перейдет по ссылке или загрузит вложение. На долю фишинга приходится от 30 % до 40 % всех угроз, связанных с электронной почтой. Значимость темы усиливается тем, что атаки на инфраструктуру, информационные системы и корпоративные сети несут прямую угрозу национальной безопасности, способны нарушить работу основных отраслей - энергетики, транспорта, здравоохранения.

Актуальность рассматриваемой темы определяется не одним обстоятельством, а их сочетанием. В российской практике противодействия киберпреступности заметным ограничением остается нехватка подготовленных специалистов в области информационной безопасности и цифровой криминалистики; из-за этого снижается как качество выявления таких деяний, так и результативность их предупреждения. Одновременно проблема находится в фокусе государственного внимания: Президент Российской Федерации неоднократно относил борьбу с киберпреступностью к числу безусловных приоритетов правоохранительной деятельности. По этой причине исследование киберпреступлений в современной России имеет не только теоретическую ценность, но и прикладное значение, поскольку предполагает выработку адаптивных подходов к защите в условиях быстро изменяющейся цифровой среды.

Объектом исследования выступают общественные отношения, складывающиеся в процессе использования информационных технологий и цифровых ресурсов, а также связанные с этим процессы совершения, обнаружения и предупреждения киберпреступлений в современной России.

Предмет исследования образуют виды и типологические группы киберпреступлений, их характерные признаки, способы совершения и сокрытия, нормы правового регулирования и особенности практического применения мер противодействия, включая деятельность государственных органов, организаций и специалистов в сфере информационной безопасности.

Цель работы состоит в комплексном изучении киберпреступлений в современной России - их типологии, нормативно-правовых оснований противодействия и используемых методов - для выявления специфики и оценки эффективности правоприменительной практики.

Задачи исследования:

1. Рассмотреть понятие, признаки и особенности киберпреступлений в Российской Федерации.
2. Провести анализ типологии киберпреступлений, классифицировать основные виды киберпреступлений в цифровой среде.
3. Изучить нормативно-правовое регулирование, направленное на противодействие киберпреступлений в Российской Федерации.
4. Проанализировать статистические показатели и структуру киберпреступлений, расследуемых правоохрнительными органами.
5. Охарактеризовать основные виды киберпреступлений на основе данных Следственного комитета Российской Федерации.
6. Исследовать методы противодействия и расследования киберпреступлений в Российской Федерации, оценить их эффективность.

Гипотеза исследования - предполагается, что современная система противодействия киберпреступлениям в Российской Федерации требует комплексного подхода, включающего как совершенствование нормативно-правовой базы, так и применение современных методов расследования и профилактики, что позволит повысить эффективность выявления пресечения цифровых правонарушений.

Методы исследования – аналитический метод: изучение научной и учебной литературы, нормативно-правовых актов, статистических данных и материалов судебной практики; сравнительно-правовой метод; статистический метод для обработки и анализа данных правоохрнительных органов; системный метод; метод обобщения и классификации для систематизации видов киберпреступлений, их признаков и способов совершения; метод контент-анализа нормативных документов.

Практическая значимость исследования - возможность использования полученных данных и выводов для совершенствования методов выявления, расследования, профилактики киберпреступлений, а также в подготовке специалистов по информационной безопасности и правоохрнительной деятельности.

Структура исследования: введение, две главы, заключение, список источников.

1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ КИБЕРПРЕСТУПЛЕНИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

1.1. Понятие и признаки киберпреступлений в Российской Федерации

Киберпреступление в Российской Федерации - уголовно наказуемое деяние, связанное с использованием компьютерных технологий, информационных сетей или цифровой инфраструктуры для совершения противоправных действий, посягающее на информационную безопасность, права личности, общественные отношения в сфере компьютерной информации и других охраняемых законом интересов, отмечает Х.А. Аккаева¹.

Киберпреступность определяется как преступление, когда компьютер является объектом преступления или используется как основной инструмент для совершения преступлений. Киберпреступником используются устройства для доступа к личной информации пользователя, для доступа к конфиденциальной деловой информации, к правительственной информации или для отключения данных устройств. Киберпреступления можно разделить на две категории: преступления, направленные на сети или устройства (вирусы, вредоносные программы, DoS-атаки) и преступления, использующие устройства для осуществления преступной деятельности (фишинговые письма, кибер-сталкинг, кража онлайн-личности)². Необходимо отметить, что к киберпреступлениям также относится продажа или получение указанной выше информации в Интернете.

¹ Аккаева Х.А. Киберпреступления: криминологический анализ / Х.А. Аккаева // Право и управление. 2025. № 1. С. 317.

² Клишков В.Б., Стебенева Е.В., Яковлева М.А. Киберпреступность: понятие, признаки, основные направления противодействия/ В.Б Клишков, Е.В. Стебенева, М.А. Яковлева // Вестник Нижегородского университета им. Н. И. Лобачевского. 2022. № 4. С. 107.

В правовом контексте термин «киберпреступление» часто отождествляют с понятиями «преступления в сфере компьютерной информации» (гл. 28 УК РФ) и «преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей», отмечает А.О. Апухтина¹.

Согласно Постановлению Пленума Верховного Суда РФ от 15 декабря 2022 года №37, к киберпреступлениям относятся как деяния в сфере компьютерной информации, так и преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая интернет². Е.А. Астахова³ отмечает, что основным признаком киберпреступлений является использование информационных технологий или компьютерной техники в качестве средства совершения преступлений. Т.М. Бормотова и соавторы⁴ добавляет наличие двух объектов посягательства: первый - общественные отношения в сфере безопасности компьютерной информации, второй - общественные отношения реального мира (например, отношения собственности, жизни и здоровья граждан, государственной безопасности). Р.Х. Кочесоков⁵ подчеркивает, что субъект киберпреступления обладает специальными знаниями в сфере информационных технологий и использует программные комплексы для совершения противоправных действий. П.Н. Кобец⁶ выделяет умышленный характер действий,

¹ Апухтина А.О. Киберпреступность: понятийно-содержательный аспект / А. О. Апухтина // Молодой ученый. 2024. № 45 (544). С. 229.

² О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37. URL: <https://normativ.kontur.ru/document?moduleId=7&documentId=439211&ysclid=mkz0c4b54590851850> (дата обращения 27.01.2026).

³ Астахова Е.А. Перспективы противодействия использованию ИКТ в преступных целях / Е.А. Астахова // Правовая политика и правовая жизнь. 2025. № 1. С. 58.

⁴ Бормотова Т.М., Ильин А.Е., Белянский Е.Б., Макаров В.В. Киберпреступность в России: состояние и методология анализа / Т.М. Бормотова и [др.] // Этносоциум и межнациональная культура. 2023. № 10 (184). С. 61.

⁵ Кочесоков Р.Х. Киберпреступность в России: тенденции и методы борьбы / Р.Х. Кочесоков // Пробелы в российском законодательстве. 2023. Т. 16. №5. С. 243.

⁶ Кобец П.Н. Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт / П.Н. Кобец // Научный вестник Омской академии МВД России. 2022. № 2. С. 103

повышенную скрытность и возможность трансграничного характера преступлений.

Основные признаки киберпреступлений обусловлены особенностями цифровой среды и технологическим особенностям таких преступлений:

- использование информационно-телекоммуникационных технологий - ключевой признак (киберпреступления совершаются с применением компьютеров, сетей, программного обеспечения, интернет-ресурсов и других цифровых инструментов¹;

- преступления нацелены на нарушение целостности (изменение или уничтожение данных), доступности (блокировка доступа к системам) или конфиденциальности (незаконный доступ к охраняемой информации) компьютерной информации. Объектом могут выступать информационные инфраструктуры (энергетика, транспорт, здравоохранение);

- киберпреступник и жертва часто находятся на значительном удалении друг от друга, а действия могут пересекать государственные границы, что усложняет расследование и привлечение к ответственности;

- злоумышленники используют методы маскировки, а именно шифрование данных, подмену IP-адресов, публичные точки доступа, чужие учетные записи, что затрудняет идентификацию виновных;

- киберпреступления совершаются быстро (в режиме реального времени), могут затрагивать множество жертв одновременно (например, при DDoS-атаках, массовых фишинговых рассылках)²;

- значительная часть киберпреступлений остается невыявленной, что связано с тем, что жертвы не всегда осознают факт преступления (например, при незаметном хищении данных) или не сообщают о нем в

¹ Гекк Б.В. Борьба с киберпреступностью в РФ: анализ явления и законодательные меры противодействия / Б. В. Гекк // Молодой ученый. 2024. № 8 (507). С. 149..

² Киберпреступность в 2026 году: новые схемы утечек данных. URL:<https://falcongaze.com/ru/pressroom/publications/informacionnaya-bezopasnost/> (дата обращения 27.01.2026).

правоохранительные органы и латентность обусловлена сложностью обнаружения следов преступления в цифровой среде¹;

- при киберпреступлении используются специальные технические средства и методы (вредоносное ПО (вирусы, трояны, шпионские программы), эксплойты, ботнеты, инструменты для социальной инженерии (фишинг, смишинг, вишинг);

- киберпреступления посягают на несколько объектов одновременно: например, на безопасность компьютерной информации и на имущественные права граждан, права личности, национальную безопасность (в случае кибертерроризма или шпионажа)²;

- действия киберпреступления происходят в цифровой среде, что создает иллюзию безнаказанности и облегчает сокрытие следов и помимо финансовой выгоды (мошенничество, кража данных), киберпреступления могут преследовать политические, идеологические или деструктивные цели (кибертерроризм, распространение экстремистской информации, нарушение работы критической инфраструктуры)³. Киберпреступления представляют собой специфический вид противоправной деятельности, тесно связанный с развитием цифровых технологий и требующий специальных подходов к расследованию и противодействию⁴. В 2025–2026 годах понятие и признаки киберпреступлений в Российской Федерации развиваются под влиянием технологического прогресса, трансформации криминальных практик и усиления правового регулирования, отмечает Е.А. Сычева⁵.

¹ Булохов И.И. Понятие и признаки киберпреступления / И.И. Булохов. - Текст: непосредственный // Молодой ученый. - 2022. - № 46 (441). - С. 182.

² Мозжерина Е.С. Кибератаки и киберпреступления: современные тренды и методы предотвращения / Е.С. Мозжерина // Молодой ученый. 2024. № 48 (547). С. 6.

³ Михайлюк В.А. Киберполиция - современный правоохранительный орган в борьбе с интернет-преступностью / В.А. Михайлюк // Вестник Уфимского юридического института МВД России. 2023. № 1(99). С. 75.

⁴ Никульченкова Е.В. О необходимости введения дефиниции «киберпреступление» в уголовный закон Российской Федерации/ Е.В. Никульченкова // Вестник Омского университета. Серия. Право. 2022. Т. 19. № 3. С. 99.

⁵ Сычева Е.А. История развития киберпреступности в России / Е.А. Сычева// Проблемы совершенствования российского законодательства: Сборник тезисов Всероссийской (с международным участием) научной конференции курсантов, слушателей и студентов, Барнаул, 12–13 апреля 2021 года.

Суть киберпреступления по-прежнему заключается в общественно опасном деянии, совершаемом с использованием компьютерных технологий, информационно-телекоммуникационных сетей (включая интернет) и направленном на нарушение целостности, доступности или конфиденциальности компьютерной информации либо на использование цифровых средств для иных противоправных целей, подчеркивает А.А. Ройхра¹. Однако содержание этого понятия и его ключевые признаки заметно усложнились. Одним из главных технологических факторов стало массовое внедрение искусственного интеллекта в преступную деятельность.

В 2026 году киберпреступники активно применяют ИИ для генерации персонализированных фишинговых сообщений, которые практически не отличаются от легитимных; автоматизации разработки и адаптации вредоносного ПО; создания дипфейков и дипвойсов, повышающих эффективность социальной инженерии; а также для ускоренной разведки и поиска уязвимостей². Наряду с этим распространяется техника ClickFix, когда жертва под видом системного уведомления выполняет вредоносную команду, и инъекции в промпты (Prompt injection) - манипуляции с ИИ-моделями, ведущие к компрометации корпоративных систем. Эти новшества придают киберпреступлениям масштабность, персонализацию и сложность, затрудняя их выявление и квалификацию, отмечает Р.Н. Сомов³. Законодательная база также претерпела существенные изменения.

Барнаул: Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Барнаульский юридический институт Министерства внутренних дел Российской Федерации», 2022. С. 282.

¹ Ройхра А.А. Зарождение киберпреступности и этапы ее последующего генезиса: российский и зарубежный опыт / А.А. Ройхра // Молодой ученый. 2025. № 13 (564). С. 130.

² Новые тенденции в борьбе с киберпреступностью: уголовно-правовые меры. URL: <https://companies.rbc.ru/news/bFD5SBdC24/novyie-tendentsii-v-borbe-s-kiberprestupnostyu-ugolovno-pravovyye-meryi/?ysclid=mkbbp5r8g1941400558> (дата обращения 15.01.2026).

³ Сомов Р.Н. Киберпреступность: основные проявления и особенности противодействия / Р. Н. Сомов // Молодой ученый. 2024. № 42 (541). С. 185.

В 2025 году Федеральный закон от 24.06.2025 № 176-ФЗ¹ внес поправки в ст. 187 УК РФ, установив ответственность за передачу электронных средств платежа (карт, ключей доступа) третьим лицам и совершение по их указанию незаконных операций, что особенно актуально в борьбе с «дропперами».

ФЗ РФ от 31.07.2025 № 282-ФЗ добавил в УК РФ новые статьи: ст. 274.4 предусматривает уголовную ответственность за организацию передачи абонентских номеров (SIM-карт) в нарушение закона, а ст. 274.5 - за передачу информации, необходимой для регистрации или авторизации пользователей в интернете (логинов, паролей, кодов). С 1 сентября 2025 года действует обновленная редакция закона 187-ФЗ, ужесточающая требования к защите стратегически важных объектов в цифровой сфере. Также с 1 марта 2026 года запускается государственная информационная система (ГИС) для противодействия кибермошенничеству, в которой будет аккумулироваться информация о злоумышленниках и их абонентских номерах (закон от 01.04.2025 № 41-ФЗ)². В результате этих изменений признаки киберпреступлений дополнились новыми характеристиками. Использование ИИ и автоматизированных систем стало самостоятельным квалифицирующим признаком, способным усиливать ответственность. Атаки все чаще носят целенаправленный и многоэтапный характер, особенно в фишинге и атаках на владельцев смартфонов. Распространились эксплойты «нулевого дня» (zero-day), для которых еще нет патчей. Преступники активно задействуют сторонние сервисы по модели Ransomware-as-a-Service («вымогательство как услуга»), что позволяет даже лицам без технических знаний проводить сложные атаки.

¹ О внесении изменений в отдельные законодательные акты РФ: федеральный закон РФ от 31.07.2025 № 282-ФЗ// принят Государственной Думой 22.07.2025, одобрен Советом Федерации 22.07.2025.

² О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации»: федеральный закон от 01.04.2025 № 41-ФЗ // принят Государственной Думой 25.03.2025, одобрен Советом Федерации 27.03.2025 (за исключением положений ст. 1 ФЗ № 41-ФЗ (вступит с 01.03.2026).

В-пятых, наблюдается тенденция к использованию легитимных инструментов (например, ПО для удаленного управления) для проникновения в корпоративные сети. Таким образом, в 2025–2026 годах киберпреступления в России отличаются технологическим усложнением за счет ИИ и автоматизации, расширением круга субъектов ответственности (включая дропперов и организаторов инфраструктуры) и усилением правового регулирования.

Понятие киберпреступления теперь охватывает не только традиционные деяния, но и действия, связанные с новыми технологиями и организационными схемами, а его признаки дополнились критериями, отражающими использование ИИ, многоэтапность атак и эксплуатацию современных уязвимостей. Это требует от правоохранительных органов и экспертов постоянного мониторинга технологических трендов и адаптации методов противодействия. Следовательно, киберпреступление - уголовно наказуемое деяние трансграничного характера, направленное против общественных отношений, охраняемых законом, совершенное с помощью средств вычислительных знаний в области информационных технологий, проецируемые в реальном или виртуальном мире.

1.2. Типология киберпреступлений в Российской Федерации

В современной России проблема киберпреступности приобретает все большую актуальность вследствие повсеместного внедрения информационных технологий в экономическую, правовую и частную сферы. Доступ к сети сам по себе делает возможными цифровые посягательства, ориентированные и на причинение ущерба гражданам, организациям, государственным структурам, и на извлечение незаконной выгоды - как финансовой, так и нематериальной. При этом спектр таких действий необычайно широк, что заставляет трактовать киберпреступность как совокупность разнородных практик, а не единичный тип правонарушений. Технологическая «опора» здесь выступает центральным

признаком: задействуются компьютерные системы, сетевая инфраструктура, мобильные устройства, а также иные цифровые платформы.

Иначе говоря, именно инструментальная среда предопределяет способы реализации атак. Отсюда же вытекает и проблема атрибуции.

Анонимизация, распределение ролей, удалённое управление (в том числе через промежуточные узлы) позволяют злоумышленникам длительно сохранять инкогнито, а правоохранным органам - тратить больше усилий на установление личности и доказательной базы. Масштаб же часто приобретает транснациональные очертания: физические границы теряют прежнюю «запирающую» функцию, когда достаточно лишь интернет-доступа.

Отдельного внимания требует темп изменений: техники атак постоянно усложняются и подстраиваются под меры защиты. Регулярного пересмотра требуют и инструменты противодействия, и подходы к подготовке специалистов, которым приходится работать в условиях непрерывной эволюции преступных схем.¹ Законодательное регулирование сферы противодействия цифровым правонарушениям строится как на внутринациональной, так и на международной базе правовых актов. Наиболее значимым международным инструментом является Будапештская конвенция о киберпреступности 2001 года, служащая моделью для формирования нормативных подходов во многих государствах и обеспечивающая платформу для координации глобальных антикриминальных инициатив². В современной криминалистике приняты различные основания для классификации киберпреступлений.

Принято выделять преступления по сфере воздействия, способу осуществления, вовлеченным технологиям, а также по видам причиненного ущерба. Среди наиболее изученных категорий можно отмечать цифровые

¹ Никиташенко В.В. Понятие и признаки киберпреступности / В.В. Никиташенко// Молодой ученый. 2021. № 14 (356). С. 251.

² Конвенция Организации Объединенных Наций против киберпреступности: резолюция Генеральной Ассамблеи. 2024. № 79/243.

преступления против безопасности информации: несанкционированное проникновение (взлом) в информационные системы, внедрение вредоносных программ, атаки на отказ в обслуживании (DDoS), которые парализуют функционирование ресурсов.

К числу киберпреступлений, ориентированных на извлечение материальной выгоды, Д.А. Баишев относит интернет-мошенничество, неправомерное получение и использование персональных данных, а также действия с криптовалютными активами, совершаемые в целях незаконного обогащения за счёт манипулирования чужими ресурсами¹. Однако в структуре цифровой деликтности значительное место занимают и посягательства, затрагивающие личные права. В пределах электронных коммуникаций сюда включаются как открытые площадки сетевого взаимодействия, так и закрытые каналы обмена сообщениями. Кибербуллинг связан с продолжительным психологическим воздействием; киберсталкинг — с навязчивым отслеживанием поведения лица в цифровой среде, нередко сопровождаемым угрозами; сексторшн основан на использовании интимных фото- и видеоматериалов как средства давления, посредством которого потерпевшего побуждают к действиям, отвечающим интересам злоумышленника. Самостоятельный блок образуют правонарушения, связанные с распространением запрещённого контента: речь идёт о материалах с детской порнографией, публикациях экстремистского характера, а также пиратской продукции, нарушающей авторские и смежные права. В более ранних исследованиях эта группа, впрочем, также выделялась достаточно устойчиво. Е.О. Бондарь обращает внимание на то, что разграничение видов киберпреступлений придаёт правоприменению большую определённость: точнее организуется поиск и фиксация цифровых следов, проще соотнести аналитические инструменты с конкретным типом угрозы, сужаются пределы неопределённости при квалификации деяний.

¹ Баишев Д.А. Проблемы противодействия киберпреступности / Д.А. Баишев // Молодой ученый. 2025. № 20 (571). С. 379.

Практическая значимость такой систематизации не сводится к расследованию. Она заметна и в подготовке специалистов по информационной безопасности, поскольку именно при упорядоченном представлении о типах киберугроз формируется не набор изолированных навыков, а целостное понимание механизмов их возникновения, предупреждения и пресечения.

Отсюда вытекает и прикладной эффект для проектирования средств защиты: структурированное описание ландшафта угроз позволяет разрабатывать специализированные решения, рассчитанные на выявление и нейтрализацию повторяющихся сценариев атак. А.М. Арипшев предлагает рассматривать данную связь шире, чем совокупность отдельных ответных действий: не только блокирование несанкционированного доступа, но и построение многоуровневых систем мониторинга, функционирующих в режиме реального времени. Одновременно возрастает значение просветительской составляющей. Распространение базовых практик личной и коллективной информационной безопасности, даже на уровне повседневного цифрового поведения, повышает киберграмотность населения и в известной мере уменьшает восприимчивость к приёмам социальной инженерии.

С методологической точки зрения типологизация киберпреступлений формирует основу для комплексного конструирования политики кибербезопасности и для адаптации правовых механизмов к ускоряющимся технологическим изменениям. Выигрыш в таком случае получают не только государственные структуры. Для бизнеса и граждан корректное выделение признаков цифровых посягательств также имеет прямое значение: появляется возможность точнее оценивать риск, заранее определять способы сокращения ущерба, включая организационные меры, которые нередко оказываются не менее существенными, чем технические.

При этом современная среда цифровых угроз характеризуется не просто количественным ростом, а одновременным усложнением их внутренней структуры. Технологическое развитие меняет базовые категории киберпреступности, и это достаточно отчётливо отражено в экспертных

оценках и отраслевых прогнозах на 2025–2026 годы. Особенно показателен сегмент компрометации корпоративных и государственных информационных систем с помощью фишинговых кампаний нового типа.

Если прежде преобладали массовые рассылки и сравнительно простые поддельные веб-ресурсы, то в текущих сценариях доминируют персонализация, сочетание методов социальной инженерии и использование искусственного интеллекта для генерации сообщений, имитирующих деловую переписку, в том числе в схемах Business Email Compromise. По оценкам экспертов, дальнейшее развитие этих практик будет связано со способностью языковых моделей воспроизводить стилистику и поведенческие шаблоны конкретных сотрудников. В такой ситуации выявление мошеннических действий заметно осложняется: отдельные признаки могут не восприниматься как подозрительные сами по себе и обнаруживаются лишь при сопоставлении совокупности косвенных индикаторов¹.

В сфере экономических преступлений наблюдается распространение взломов аккаунтов, связанных с финансовыми платформами. Примером может служить кража средств через получение доступа к личным кабинетам пользователей онлайн-банкинга. За 2025 год в России уже было зафиксировано десятки тысяч попыток несанкционированного входа с целью вывода денежных средств на фишинговые счета и обналичивания через криптовалютные обменники. Ожидается, что в 2026 году злоумышленники будут активнее использовать вредоносное ПО, специально нацеленное на мобильные платформы, что приведет к росту числа подобных преступлений, а также появлению новых моделей мошеннических приложений для поддельного инвестирования или страхования². Сохранится (и даже усилится) акцент на киберпреступления против личности.

¹ Взять цифровой след. Как раскрываются преступления в МБД. URL: <https://secpost.ru/vzyat-czifrovoj-sled-kak-raskryvayut-kiberprestupleniya-v-rossii-v-2025-godu?ysclid=mkzbfmvsdj486492345> (дата обращения 28.01.2026).

² Киберпреступность в 2026 году: новые схемы утечек данных. URL: <https://falcongaze.com/ru/pressroom/publications/informacionnaya-bezopasnost/> (дата обращения 27.01.2026).

Уже сейчас резонанс получают случаи так называемого deepfake-шантажа: распространение реалистичных цифровых подделок фото и видео на основе нейросетевых технологий все чаще становится инструментом вымогательства.

В 2026 году такие инциденты станут более массовыми, особенно в отношении публичных персон и топ-менеджмента компаний, что заставляет пересматривать стратегию личной цифровой безопасности и методы аутентификации контента. Отдельного анализа заслуживает блок рисков, возникающих на стыке криптовалютной экономики и блокчейн-инфраструктуры. В российской практике последних лет фиксируются эпизоды хищения активов через взломы смарт-контрактов и DeFi-платформ (децентрализованных финансовых сервисов). И именно рост объёма операций в подобных экосистемах (параллельно с усложнением их программной архитектуры) создаёт условия, при которых атаки приобретают экономически рациональный масштаб. На 2026 год аналитики прогнозируют появление более изощрённых сценариев эксплуатации уязвимостей в коде, а также фишинговые кампании, нацеленные на пользователей NFT и токенизации активов.

В числе актуальных тенденций выделяют технологическое «пиратство» с опорой на облачные хранилища и распространение запрещённых материалов через зашифрованные мессенджеры и пиринговые сети - там, где привычные инструменты идентификации администраторов и логистики контента работают хуже, а цепочки распространения намеренно дробятся. Существенно усложняется выявление организаторов незаконных сетей. И это усложнение носит не только технический, но и организационно-правовой характер (поскольку границы юрисдикций и фрагментация цифровых следов начинают играть роль дополнительного «щита»).

Отдельной линией проходит рост посягательств на объекты критической инфраструктуры, когда под удар попадают системы, обеспечивающие жизненно важные сервисы. Резкий сдвиг в сторону сложных, опирающихся на искусственный интеллект схем, демонстрирует типология киберпреступности

в контексте 2026 года; по этой причине уголовно-правовая оценка требует развернутого анализа каждого конкретного проявления, а не шаблонной квалификации.

За пределы стандартных средств обнаружения выводит злоумышленников использование вредоносных программ на базе ИИ: они способны обходить автоматизированные средства защиты и почти мгновенно подстраиваться под контекст цифровой среды. Сложнее становится экспертиза. И реконструкция способа совершения посягательства тоже.

Для уголовно-правовой практики России это означает необходимость пересмотра подходов к доказыванию умысла и более точной и законодательно закреплённой нормы об ответственности за несанкционированный доступ, поскольку «поведение» атаки все чаще формируется автоматически (и в материалах дела это не всегда очевидно без углублённой технической интерпретации). Особого внимания требует использование ИИ для повышения эффективности персонализированного фишинга и программ-вымогателей: целенаправленные воздействия на конкретных должностных лиц, синтез фишинговых сообщений на базе анализа личных и профессиональных связей жертвы заметно увеличивают криминальный потенциал информационного нападения. Возрастает и сложность отнесения подобных эпизодов к определённой статье УК РФ. Появляются ситуации, где квалификация упирается в освоение новых цифровых категорий доказательств и понятий, включая модели генерирования текста, алгоритмы подмены идентичности и способы встраивания вредоносной логики в легитимные коммуникации.

Расширяют спектр социальных посягательств состязательные ИИ-системы, вредоносные языковые модели и технология дипфейков: расследование дел о мошенничестве, шантаже и вмешательстве в частную жизнь сталкивается с тем, что источник вреда может оставаться фактически неочевидным, а круг потерпевших - неопределённым. На горизонте 2026 года выглядит тревожно и перспектива квантовых вычислений: возможная утрата стойкости привычных механизмов цифровой подписи и шифрования бьёт по

целостности доказательственной базы в уголовном судопроизводстве, где электронные доказательства становятся опорными.

Реальную угрозу создаёт концепция отложенной расшифровки («Harvest Now, Decrypt Later»), допускающая ретроспективную компрометацию массивов данных, ранее считавшихся защищёнными. В современную типологию вписываются и атаки на цепочки поставок, и эксплуатация IoT-устройств, когда доступ к целевой системе обеспечивается не напрямую, а через доверенных контрагентов, внешних исполнителей либо уязвимые устройства с минимальной защитой. Развития требуют правоприменительные подходы к распределению ответственности между участниками инфраструктурной «экосистемы», а также экспертные критерии оценки уровня защищённости (без которых трудно отделить преступную небрежность от добросовестной ошибки управления риском). Параллельно расширяется модель «вымогательство как услуга» (RaaS), которая фактически снижает порог входа в киберпреступность: атаки становятся доступнее и для лиц без глубоких технических компетенций, что усиливает массовость преследования и подталкивает к появлению новых криминалистически значимых ролей в преступных группах.

В поле охраны цифровых интересов личности и экономики всё большее беспокойство вызывают инсайдерские эпизоды и эксплуатация уязвимостей нулевого дня. Обладая легитимными полномочиями внутри организаций, инсайдеры нередко обходят традиционные инструменты форензики; затрудняется не только фиксация самого факта посягательства, но и доказательство субъективной стороны (когда мотив, цель и осознание последствий приходится восстанавливать по косвенным цифровым признакам). В совокупности это показывает: передовые информационные технологии всё теснее переплетаются с классическими моделями преступного поведения, а от уголовного права требуется способность к быстрой адаптации — через обновление квалифицирующих признаков, развитие цифровой криминалистики и законодательную модернизацию.

Показательным кейсом, получившим общественный резонанс, стала попытка компрометации систем управления городской энергетикой с применением программ-вымогателей (ransomware): в 2025 году подобные инциденты затрагивали отдельные регионы России, где из-за воздействия на операторов электросетей или водоснабжения отключалась часть сервисов.

К 2026 году состав и внутренняя дифференциация киберпреступности в Российской Федерации заметно усложняются. Уже не отдельные эпизоды, а целые группы новых атак формируют ситуацию, при которой прежние подходы к наблюдению, расследованию и правовому реагированию оказываются недостаточными. В уголовно-правовом измерении это особенно ощутимо: развитие цифровых технологий порождает такие способы совершения деяний, которые не всегда своевременно получают нормативное выражение в Особенной части УК РФ¹. Отсюда возникают не только теоретические затруднения. Практика сталкивается с менее определенными границами состава, с проблемами при квалификации, с осложнениями в доказывании и, в ряде случаев, с неочевидностью выбора соразмерной санкции.

Базовое регулирование сосредоточено в гл. 28 УК РФ, где предусмотрены ст. 272 УК РФ, устанавливающая ответственность за неправомерный доступ к компьютерной информации, ст. 273 УК РФ, посвященная созданию, использованию и распространению вредоносных компьютерных программ, ст. 274 УК РФ о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а также ст. 274.1 УК РФ, предусматривающая ответственность за неправомерное воздействие на критическую информационную инфраструктуру РФ.

¹ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 20.01.2026) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

Эти нормы охватывают основные посягательства на конфиденциальность, доступность и целостность информации, однако в правоприменении сохраняется известная неполнота описания конкретных способов совершения преступления и критериев, по которым оценивается причиненный вред. Наряду с этим к регулированию цифровой преступности привлекаются и иные положения Кодекса: ст. 159.3 УК РФ и ст. 159.6 УК РФ применяются при хищениях, совершаемых с использованием электронных средств платежа и компьютерной информации, а ст. 187 УК РФ — в делах, связанных с неправомерным оборотом средств платежей, включая операции с поддельными платежными инструментами. В 2025 году законодатель усилил этот блок норм: Федеральным законом от 31.07.2025 № 282-ФЗ в УК РФ включены ст. 274.4 и ст. 274.5, направленные на пресечение передачи абонентских номеров в нарушение закона, а также на ограничение оборота сведений, необходимых для регистрации или авторизации пользователей в сети «Интернет»¹. По существу, речь идет о попытке охватить уголовно-правовыми средствами инфраструктурное содействие преступной деятельности, в том числе действия так называемых дропперов.

Вместе с тем часть актуальных угроз не имеет однозначного нормативного соответствия. Пока отсутствуют прямые уголовно-правовые конструкции, специально ориентированные на использование искусственного интеллекта для создания дипфейков, проведения автоматизированных фишинговых кампаний или воздействия на ИИ-модели посредством prompt injection. Проблема здесь связана не столько с исключительностью указанных способов, сколько с тем, что традиционная модель описания объективной стороны преступления не всегда позволяет точно уловить их техническую специфику. Есть и другая группа практик — формально они могут охватываться действующими составами, но при этом меняют привычные

¹ Проблемы противодействия киберпреступности: материалы II Международной научно-практической конференции (Москва, 26 апреля 2024 года) / Под общ. ред. О.Ю. Антонова, Э.Б. Хатова. - М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2024. – С. 78.

представления о способе совершения деяния и распределении ролей между участниками.

К таким явлениям относится Ransomware-as-a-Service, а также использование уязвимостей zero-day, когда разработчик инструмента, оператор атаки и организатор схемы выступают как разные субъекты. В подобных случаях сложнее установить не только механизм соучастия, но и соотнести действия каждого участника с конкретной формой вины. Иногда — и с конкретным способом посягательства.

Отдельный пласт трудностей связан с трансграничным характером киберпреступности. Даже при наличии применимых норм УК РФ расследование может упираться в неопределенность юрисдикции, проблемы получения цифровых доказательств, их процессуального закрепления и последующего использования, а также в ограниченные возможности экстрадиции, особенно если инфраструктура атаки распределена по нескольким государствам. По этой причине востребовано не только внутреннее уточнение уголовного законодательства, но и развитие международного взаимодействия, прежде всего в части процессуальных механизмов и обмена цифровыми доказательствами. Сохранять эффективность уголовно-правовой защиты в таких условиях возможно лишь при регулярном мониторинге технологических изменений и при формировании более гибких юридических конструкций, способных учитывать новые киберугрозы без постоянного запаздывающего пересмотра норм.

Адаптация действующей типологии киберпреступлений к современным технологическим условиям остается одной из актуальных задач. Для повышения результативности противодействия представляется необходимым уточнение диспозиций составов преступлений с учетом использования искусственного интеллекта, облачных сервисов и криптовалют, введение квалифицирующих признаков для деяний, совершаемых организованными группами либо с применением специализированных сервисов, а также согласование положений УК РФ с международными стандартами и развитие

правовых инструментов расследования трансграничных инцидентов. Без такого обновления нормативная система будет воспроизводить отставание от реальной динамики преступных практик.

Системный учет особенностей цифровой преступности в этих условиях имеет не частное, а общее значение: он усиливает защиту интересов личности, общества и государства и поддерживает устойчивость развития национальной уголовно-правовой системы России.

1.3. Нормативно-правовое регулирование противодействия киберпреступлениям в Российской Федерации

Нормативно-правовое регулирование противодействия киберпреступлениям в Российской Федерации представляет собой многоуровневую систему международных и национальных правовых актов, направленных на обеспечение информационной безопасности и пресечение противоправных действий в цифровой среде. Основополагающим международным документом выступает Конвенция Организации Объединенных Наций против киберпреступности, принятая резолюцией Генеральной Ассамблеи ООН № 79/243 от 24.12.2024 года¹. Этот глобальный договор устанавливает базовые принципы противодействия киберпреступности, включая механизмы международного сотрудничества при расследовании преступлений и обмене электронными доказательствами, а также определяет меры по предупреждению незаконного перехвата данных и использования вредоносных программ. На национальном уровне ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»² регламентирует отношения, связанные с поиском,

¹ Конвенция Организации Объединенных Наций против киберпреступности: резолюция Генеральной Ассамблеи. 2024. № 79/243.

² О персональных данных: федеральный закон от 27.07.2006 г. № 152-ФЗ (в ред. от 01.09.2025)// Собрание законодательства РФ.2006. № 31 (часть I). Ст. 3451.

получением, передачей, производством и распространением информации, закрепляет принципы свободы информации и устанавливает требования к ее защите.

Особое значение имеет ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», который формирует правовую основу обработки персональных данных и предусматривает защиту данных от несанкционированного доступа, устанавливает принципы их обработки, запрещает обработку без согласия субъекта. Исключения закреплены в п.2 ст. 6 гл.2 «Принципы и условия обработки персональных данных ФЗ РФ № 152-ФЗ и обязывает операторов обеспечивать конфиденциальность информации. Для защиты несовершеннолетних применяется ФЗ РФ от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», который запрещает распространение среди детей информации, побуждающей к причинению вреда здоровью, самоубийству, содержащей насилие, порнографию и иные опасные материалы¹.

Особую роль в противодействии киберугрозам занимает ФЗ РФ от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который определяет понятия компьютерной атаки и инцидента, устанавливает порядок функционирования государственной системы обнаружения и ликвидации последствий атак, предусматривает категорирование объектов критической информационной инфраструктуры (КИИ) и государственный контроль за их безопасностью².

Необходимо отметить изменения в законодательстве, внесенные ФЗ РФ от 01.04.2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений

¹ О защите детей от информации, причиняющей вред их здоровью и развитию: федеральный закон от 29.12.2010 г. № 436-ФЗ (в ред. от 01.03.2024)// Собрание законодательства РФ. 2011. № 1. Ст. 48.

² О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26.07.2017 г. № 187-ФЗ (в ред. от 01.09.2025)// Собрание законодательства РФ. 2017. № 31 (часть I). Ст. 4736

в отдельные законодательные акты Российской Федерации», который предусматривает создание специализированной ГИС для оперативного выявления и пресечения киберправонарушений.

Включает хранение данных о лицах, совершивших противоправные действия с использованием сетей связи, и обеспечение взаимодействия органов власти, банков и операторов связи¹.

ФЗ РФ от 31.06.2025 г. № 282-ФЗ «О внесении изменений в отдельные законодательные акты РФ» внес изменения в УК РФ и УПК РФ², установив ответственность за незаконное использование абонентских терминалов пропуска трафика, организацию передачи абонентских номеров с нарушением законодательства, а также за передачу информации, необходимой для регистрации или авторизации в интернете. К отягчающим обстоятельствам отнесено использование VPN-сервисов при совершении преступлений.

Необходимо отметить судебную практику по делам о киберпреступлениях формирует Постановление Пленума ВС РФ от 15.12.2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» содержит разъяснения по квалификации преступлений, предусмотренных ст. 272–274.1 УК РФ, и помогает судам применять нормы уголовного закона³. Совокупность указанных нормативных актов формируют комплексную

¹ О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации»: федеральный закон от 01.04.2025 № 41-ФЗ // принят Государственной Думой 25.03.2025, одобрен Советом Федерации 27.03.2025 (за исключением положений ст. 1 ФЗ № 41-ФЗ (вступил с 01.03.2026).

² О внесении изменений в отдельные законодательные акты РФ: федеральный закон РФ от 31.07.2025 № 282-ФЗ// принят Государственной Думой 22.07.2025, одобрен Советом Федерации 22.07.2025.

³ О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37. URL: <https://normativ.kontur.ru/document?moduleId=7&documentId=439211&ysclid=mkz0c4b54590851850> (дата обращения 27.01.2026).

систему противодействия киберпреступлениям, сочетающую международно-правовые обязательства, уголовно-правовые запреты, административные меры регулирования и технологические механизмы защиты информационной инфраструктуры.

Анализ нормативно-правового регулирования в сфере противодействия киберпреступлениям в Российской Федерации показывает, что действующая система законодательства находится в стадии постоянного развития, реагируя на технологические вызовы современности.

Повышение эффективности нормативного регулирования требует своевременного обновления законодательства, развития специальных институтов судебной и правоохранительной практики, а также широкого внедрения профилактических и образовательных мер. Таким образом, совершенствование нормативно-правовой базы противодействия киберпреступлениям представляется неотъемлемой частью национальной стратегии цифрового развития и обеспечивает более высокий уровень защиты интересов граждан, бизнеса и государства в условиях постоянной трансформации цифровых угроз.

Вывод по первой главе исследования.

Проведённое в первой главе исследование позволяет зафиксировать исходную рамку: в российском уголовно-правовом дискурсе киберпреступления понимаются как общественно опасные посягательства, реализуемые посредством информационных технологий и сетей, прежде всего через информационно-телекоммуникационную инфраструктуру. Характерные черты такой криминальной активности проявляются устойчиво — специфичен объект посягательства, дистанционен способ совершения, высока степень анонимизации субъекта. Существенно влияет и трансграничность (особенно в условиях «размытых» цифровых границ), поскольку она усложняет квалификацию и организацию расследования.

Широта поля противоправных действий проясняется через структурную классификацию: в ней группируются посягательства на конфиденциальность,

целостность и доступность информации, а также деяния, совершаемые с применением цифровых инструментов в экономической сфере, в области личных прав и в иных сегментах общественных отношений.

Не только систематизация норм получает от типологизации практический эффект - легче выявляются новые формы преступной активности, быстрее настраиваются механизмы противодействия под изменяющиеся сценарии угроз. Анализ нормативно-правовой базы показывает, что в Российской Федерации складывается комплекс мер противодействия, опирающийся на уголовные, административные и специальные регулятивные акты. При этом сохраняются пробелы, обусловленные ускорением технологического развития и появлением новых форм атак.

Отсюда - приоритетная задача, а именно адаптация правовых предписаний к обновляющейся цифровой реальности. И параллельно - гармонизация российского регулирования с международными стандартами, без чего эффективное реагирование на транснациональные киберпреступления остаётся затруднённым.

2. СТАТИСТИЧЕСКИЙ АНАЛИЗ КИБЕРПРЕСТУПЛЕНИЙ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ

2.1. Показатели и структура киберпреступлений, расследуемых правоохранительными органами

Максимум зарегистрированных преступлений цифрового характера пришелся на 2023 год: правоохранительными органами было учтено 677 тыс. таких деяний, что почти на треть выше показателя 2022 года. При этом увеличение массива объясняется не только фактическим расширением криминальной активности, но и пересмотром подходов к статистическому учету, а также более широкой уголовно-правовой квалификацией соответствующих посягательств¹. Внутри общей структуры заметнее всего представлены дистанционные мошеннические схемы: свыше 52% киберпреступлений в 2023 году были связаны с использованием информационных технологий. Кражи, совершаемые с применением ИТ-инструментов, по-прежнему сохраняют значительное место, хотя их доля уже не выглядит доминирующей, поскольку быстрее распространяются иные формы противоправного поведения². Одновременно увеличивается число преступлений, сопряженных с незаконным оборотом наркотических средств, где цифровые платформы используются и для коммуникации, и для сокрытия участников сделки, что заметно усложняет саму конфигурацию преступной деятельности. Технологический профиль этих деяний также сместился. В 2023 году почти 78% преступлений совершались с использованием интернет-среды, еще 44,7% были связаны с мобильной связью; уже в 2024 году интернет

¹ СК РФ. Официальный сайт. URL: <https://tass.ru/obschestvo/24573429?ysclid=mkzh42p83834667093>. (дата обращения 27.01.2026)

² Степанов Е.А. Пути совершенствования расследования и раскрытия компьютерных преступлений / Е.А. Степанов // Вестник науки. 2025. № 1 (82). С. 455.

фигурировал в 84,8% зафиксированных случаев, а значение мобильных технологий стало еще более существенным.

Наиболее уязвимыми остаются дистанционные финансовые операции, обработка персональных данных и электронная торговля. Дополнительные сложности создает распространение атак, где применяются инструменты искусственного интеллекта, дипфейк-технологии и квантовое шифрование; традиционные модели расследования в таких условиях работают заметно менее эффективно¹. Территориальное распределение в 2024 году не было равномерным: в Мордовии, Марий Эл, Татарстане, Югре, Чувашии, Кировской и Томской областях удельный вес IT-преступлений превышал 49–63% общего числа правонарушений (Приложение 1 - рис.1)². В южных субъектах, напротив, коэффициенты цифровой преступности оставались ниже, что обычно связывают с неодинаковым уровнем информатизации и рядом социокультурных особенностей. За одиннадцать месяцев 2025 года общее количество датированных преступлений сократилось до 627 тыс., однако основа структуры почти не изменилась: более 63% составляли хищения и мошенничества. Одновременно на 28,5% вырос массив преступлений, связанных с наркотиками, а мессенджеры стали еще более значимым каналом взаимодействия между участниками преступных групп (Приложение 1 - рис.2).

Острее всего проблема проявляется в сфере раскрываемости. В 2023 году до завершения удалось довести лишь 26,6% дел, причем по мошенничествам показатель не поднимался выше 11%³. Между регистрацией преступлений и их фактическим раскрытием формируется все более заметный разрыв; его определяют анонимизация преступников, трансграничный характер действий, применение программ для маскировки цифровых следов и процессуальные

¹ Черенцова Р.С. Проблемы правового регулирования киберпреступности в современной России / Р.С. Черенцова // Актуальные исследования. 2025. №21 (256). ч. III. С. 56.

² Киберпреступность в 2026 году: новые схемы утечек данных. URL: <https://falcongaze.com/ru/pressroom/publications/informacionnaya-bezopasnost/> (дата обращения 27.01.2026).

³ Швыряев П.С. Проблема киберпреступности в России: актуальное состояние и перспективы решения/ П.С. Швыряев // Уровень жизни населения регионов России. 2023. Том 19. № 4. С. 618.

затруднения при истребовании сведений из иностранных юрисдикций.

К этому добавляется высокая латентность: опросные данные показывают, что к правоохранительным органам обращается лишь небольшая доля граждан, столкнувшихся с цифровыми посягательствами, поэтому официальная статистика отражает ситуацию лишь частично¹. В уголовно-правовом смысле само понятие раскрытия киберпреступления охватывает очень разные по сложности случаи — от установления исполнителя сравнительно простого электронного мошенничества до изобличения многоуровневой международной атаки. Именно поэтому даже приближение раскрываемости к рубежу 30% следует оценивать как индикатор определенного укрепления возможностей специализированных подразделений МВД России и других силовых структур: сказались и техническое переоснащение, и профессиональная подготовка сотрудников, и расширение взаимодействия с коммерческими организациями, работающими в сфере информационной безопасности.

Особое место в этой системе занимают подразделения «К», традиционно рассматриваемые как одни из наиболее подготовленных в техническом отношении, наряду со структурами экономической безопасности. Помимо МВД России, в противодействии цифровым угрозам участвует и Центр информационной безопасности ФСБ России. Практика последних лет включает ряд сложных оперативно-разыскных мероприятий, в том числе в 2025 году — выявление коррупционного эпизода с участием сотрудника БСТМ, задержание группы хакеров, осуществлявших атаки на государственные порталы, пресечение деятельности лиц, связанных с иностранными спецслужбами и использовавших схемы телефонного мошенничества, а также нейтрализацию групп, причастных к созданию

¹ Шикула И.Р., Куркин Е.Н. Киберпреступность в Российской Федерации: основные методы борьбы и проблемы противодействия/ И.Р. Шикула, Е.Н. Куркин // Международный журнал экспериментального образования. 2023. № 1. С. 38.

вредоносного программного обеспечения и атак на банковскую инфраструктуру¹.

Вместе с тем для следствия сохраняются одни и те же узловые трудности: анонимность субъектов, трансграничность цифровой активности, активное использование шифрования, ограниченный доступ к носителям информации и сложность извлечения пригодных для доказывания цифровых данных². Сбор и интерпретация цифровых следов остаются центральным элементом расследования, однако объем информации, который в принципе удастся установить, как отмечают специалисты, редко превышает 30% совокупности обстоятельств, а доля сведений, способных быть непосредственно связанной с конкретным лицом в доказательственном порядке, еще меньше³. Здесь и проявляется главное противоречие современной уголовно-процессуальной практики: количественный рост таких дел уже очевиден, а адаптация следственных механизмов к изменяющейся цифровой среде все еще не завершена. В практике выявления и документирования киберпреступлений используется разнородный набор средств. Речь идет не только о сетевом контроле, включая комплексы класса «Сорм-3», предназначенные для исследования интернет-трафика, но и о специализированных экспертных решениях для анализа цифровых следов, извлечения сведений из устройств, восстановления удаленной информации. Существенное место занимают и методы киберразведки: работа в закрытых онлайн-сообществах преступной направленности, исследование блокчейн-цепочек, фиксация данных о криптовалютных переводах; в ряде случаев к таким мероприятиям подключаются внешние технические специалисты. Практическая отдача от этих инструментов, однако, ограничивается рядом факторов. Наиболее

¹ Аккаева Х.А. Киберпреступления: криминологический анализ / Х.А. Аккаева // Право и управление. 2025. № 1. С. 321.

² Гильмутдинова Ю.Ю. Проблемы уголовно-правовой квалификации киберпреступлений по законодательству РФ / Ю.Ю. Гильмутдинова // Lex criminalis scientiarum. 2025. № 1 (3). С. 52.

³ Взять цифровой след. Как раскрываются преступления в МБД. URL: <https://secpost.ru/vzyat-czifrovoj-sled-kak-raskryvayut-kiberprestupleniya-v-rossii-v-2025-godu?ysclid=mkzbfmvsdj486492345> (дата обращения 28.01.2026).

значимы здесь анонимизирующие технологии, широкое применение шифрования, а также размещение ключевых элементов преступной инфраструктуры вне российской юрисдикции.

Дополнительную сложность создает ситуация, при которой участники преступных схем действуют с территории государств, не предусматривающих экстрадицию, либо из стран, где проведение необходимых процессуальных действий фактически блокируется. Из-за этого инициирование выдачи и организация следственных мероприятий нередко оказываются затрудненными почти до предела. Отдельно следует учитывать и политически обусловленные обстоятельства: некоторые иностранные юрисдикции, по существу, допускают организованное функционирование мошеннических call-центров. Международная правовая помощь в подобных делах обеспечивается на основании специальных норм УПК РФ, двусторонних соглашений и международных конвенций; параллельно расширяется обмен оперативными сведениями между компетентными органами государств СНГ, в том числе при участии Интерпола¹. Значимую помощь правоохрнительным структурам оказывают и специалисты по информационной безопасности: ими выявляются отдельные атакующие инфраструктуры, локализуются и исследуются ботнеты, обеспечивается техническое сопровождение дел, связанных с вымогательством, фишингом и кардингом.

При этом наиболее результативные эпизоды такой работы нередко остаются вне публичного поля — сказываются оперативные ограничения и режим неразглашения. Отдельные расследования, особенно по делам о международных организованных группах мошенников, длятся годами. В подобных производствах привлекаются междисциплинарные команды, выполняющие комплексный технический анализ, реконструирующие маршруты передачи данных, выстраивающие графы сетевой инфраструктуры; именно такая, несколько трудоемкая, модель работы заметно повышает шансы

¹ СК РФ. Официальный сайт. URL: <https://tass.ru/obschestvo/24573429?ysclid=mkzh42p83834667093>. (дата обращения 27.01.2026)

на установление конечных бенефициаров преступной схемы и доведение уголовного преследования до практического результата.

По оценкам, основанным на статистике МВД за 2023–2025 годы и с учетом продолжающейся цифровизации российского общества, в 2026 году количество выявленных киберпреступлений, вероятно, достигнет примерно 695 тысяч случаев¹. Ожидается именно устойчивое увеличение, без скачкообразной динамики. Его предпосылки достаточно очевидны: расширяются дистанционные финансовые сервисы, усиливается интенсивность интернет-коммуникаций, новые цифровые инфраструктуры внедряются практически во все сферы социальной и экономической жизни. Внутри общего массива существенных структурных изменений не прогнозируется. Лидирующее положение сохранит мошенничество — около 55 % от числа зарегистрированных киберпреступлений. На долю краж, совершенных с использованием информационных технологий, предположительно придется около 15 %, причем их удельный вес продолжит снижаться. Иная траектория характерна для деяний, связанных с незаконным оборотом наркотических средств через цифровые каналы: здесь ожидается дальнейший рост, вплоть до 9 % совокупного объема. Примерно 55 % всех киберпосягательств, по предварительным расчетам, по-прежнему будут относиться к тяжким и особо тяжким деяниям, что указывает на сохраняющийся высокий уровень общественной опасности². Более 87 % таких преступлений в 2026 году, как и ранее, будут совершаться с использованием сети Интернет, а около половины всех эпизодов окажется связано с эксплуатацией мобильной связи. Одновременно расширяется набор применяемых преступниками средств: от систем искусственного интеллекта и

¹ Киберпреступность в 2026 году: новые схемы утечек данных. URL: <https://falcongaze.com/ru/pressroom/publications/informacionnaya-bezopasnost/> (дата обращения 27.01.2026).

² Киберпреступность в 2026 году: новые схемы утечек данных. URL: <https://falcongaze.com/ru/pressroom/publications/informacionnaya-bezopasnost/> (дата обращения 27.01.2026).

дипфейк-технологий до сложных схем шифрования и блокчейн-инструментов. Для аналитической и следственной деятельности это создает дополнительные, не всегда быстро преодолимые, барьеры.

Показатель раскрываемости, по прогнозу, может увеличиться до 33 %. Основания для такого ожидания связаны с наращиванием технической оснащённости ведомств, повышением квалификации сотрудников, а также с более тесным взаимодействием государственных органов и высокотехнологичного частного сектора. Вместе с тем улучшение данного коэффициента не устраняет базовых ограничений: сохраняются анонимность преступников, трансграничный характер их активности, постоянное совершенствование методов сокрытия цифровых следов, трудности получения доказательственной информации из зарубежных информационных систем. Устойчива и территориальная дифференциация. Наиболее высокие показатели распространенности киберпреступности фиксируются в регионах с развитой ИТ-средой — в Мордовии, Марий Эл, Татарстане, Югре, Чувашии, Кировской и Томской областях, где удельный вес таких деяний в общей структуре уголовных дел находится в диапазоне от 52 % до 66 %¹. На ближайшую перспективу ключевые риски, связанные с цифровой преступностью, не утратят значения. По этой причине противодействие киберпреступности требует не только дальнейшего внедрения новых технологических решений и усиления межведомственной кооперации, но и повышения цифровой грамотности населения, обновления нормативной базы, подготовки специалистов, способных вести ИТ-расследования на должном уровне. При переходе от общей динамики к анализу видовой структуры необходимо учитывать методологическое расхождение официальной статистики. СК РФ отражает число уголовных дел, расследованных, направленных в суд либо находящихся в производстве, тогда как МВД России учитывает

¹ СК РФ. Официальный сайт. URL: <https://tass.ru/obschestvo/24573429?ysclid=mkzh42p83834667093>. (дата обращения 27.01.2026)

зарегистрированные сообщения о преступлениях, то есть первичные обращения, не каждое из которых получает последующее процессуальное развитие.

Именно этим объясняются различия в численных показателях: МВД фиксирует весь массив поступивших заявлений, включая материалы без принятого процессуального решения, а в отчетности СК РФ представлены уже установленные факты преступной деятельности. Поэтому при исследовании структуры киберпреступности требуется сопоставление данных МВД России и СК России — только так формируется более целостное представление о масштабах и содержании рассматриваемого явления.

2.2. Характеристика основных видов киберпреступлений по данным Следственного комитета Российской Федерации

Для киберпреступлений, если соотносить их с традиционными формами преступной деятельности, типичны иные базовые характеристики. На первый план здесь выходят затруднённая идентификация субъекта, трансграничный характер совершаемых деяний, ускоренное изменение применяемых способов и инструментов, а также масштаб последствий, который нередко оказывается существенным. Причём речь идёт не только о прямых финансовых потерях. Существенное значение имеют и репутационные издержки, иногда менее очевидные на начальном этапе, но сопоставимые по своему воздействию. Именно это сочетание — анонимности, территориальной рассредоточенности и высокой адаптивности методов — заметно отличает киберпреступления от традиционных преступлений. Для практики Следственного комитета Российской Федерации расследование киберпреступлений связано не только с применением уголовно-процессуальных норм, но и с работой в среде цифровых следов, где значение имеют технические детали фиксации и последующей интерпретации данных. Отправной точкой выступает прием сообщения о преступлении и его проверка: уже на этой стадии анализируются

журналы сетевых подключений, снимки экранных интерфейсов, выгрузки переписки из мессенджеров, а также сведения, предоставляемые операторами связи.

Существенным в момент решения вопроса о возбуждении уголовного дела по ст. 146 УПК РФ становится наличие достаточного массива данных, позволяющего усмотреть признаки конкретного состава. Речь может идти об обнаружении вредоносного программного обеспечения, необычных операций с криптовалютой, признаках несанкционированного проникновения в информационные системы. Само по себе такое установление не всегда формируется одномоментно: отдельные цифровые фрагменты сначала выглядят разрозненными, однако именно их процессуально корректное сопоставление приобретает определяющее значение.

В дальнейшем, в рамках предварительного следствия, осуществляемого по правилам гл. 22 УПК РФ, используются специальные процессуальные и криминалистические механизмы, ориентированные на обращение с электронными доказательствами. К их числу относится выемка электронных носителей по ст. 183 УПК РФ, назначение компьютерно-технических экспертиз в порядке ст. 195 УПК РФ, проведение допросов с фиксацией цифровых материалов, а также арест электронных активов, включая криптовалютные кошельки. Отдельного внимания требует соблюдение цепочки сохранности доказательств (chain of custody): каждое действие с носителем подлежит документированию, сопровождается видеофиксацией, при необходимости — с участием понятых. Именно такая процессуальная последовательность снижает риск признания полученных сведений недопустимыми, хотя в реальной следственной практике наибольшие сложности возникают как раз на стыке техники и процедуры.

Среди киберпреступлений, расследуемых СК РФ, заметное место занимают деяния, объединенные в гл. 28 УК РФ, посвященной преступлениям в сфере компьютерной информации. В этом массиве центральное значение имеет неправомерный доступ к компьютерной информации, предусмотренный

ст. 272 УК РФ. Его содержание охватывает несанкционированное проникновение в информационные системы, базы данных и отдельные устройства, если целью выступают копирование сведений, их изменение либо уничтожение.

Формально конструкция состава выглядит определенной, но в следственной работе ее наполнение зависит от качества цифровой фиксации и от того, насколько убедительно установлены способ доступа, объем затронутой информации и характер последствий. Существенный массив киберпреступлений связан с применением вредоносного программного обеспечения, ответственность за которое предусмотрена ст. 273 УК РФ. В эту группу включаются компьютерные вирусы, троянские модули, средства скрытого наблюдения, программы-вымогатели, в том числе шифрующие данные, а также иные программные решения, изначально ориентированные на дестабилизацию функционирования информационных систем, неправомерное получение сведений либо вымогательство. Подобные действия нередко предшествуют более тяжким посягательствам — хищению, шантажу, промышленному шпионажу, на что указывает О.Г. Шляхтова¹. Распространение получили и иные криминальные модели: незаконное использование чужих вычислительных мощностей для добычи криптовалюты, обычно обозначаемое как криптоджекинг, а также сервисы формата Ransomware-as-a-Service (RaaS). Последние заметно снижают порог вхождения в преступную деятельность, поскольку позволяют осуществлять атаки и лицам, не обладающим сколько-нибудь значительной технической подготовкой.

Особого рассмотрения требуют посягательства на критическую информационную инфраструктуру, охватываемые ст. 274.1 УК РФ. Речь идет об атаках на системы энергетики, транспортный комплекс, здравоохранение, оборонную сферу и иные объекты, нарушение работы которых способно

¹ Шляхтова О.Г. О подходах к пониманию и классификации преступлений в сфере компьютерной безопасности / О.Г. Шляхтова// Молодой ученый. 2024. № 10 (509). С. 243.

вызвать масштабные социально-экономические последствия; именно этот аспект специально выделяет О.Г. Шляхтова¹.

Для таких деяний, как правило, характерны направленность и организационная сложность, вследствие чего в расследование вовлекаются несколько подразделений СК РФ, нередко при взаимодействии со смежными ведомствами. Значительное место занимает и расследование дистанционных хищений, а также мошенничества, совершаемого с использованием информационных технологий. Наиболее типичны здесь приемы социальной инженерии: фишинговые сообщения в электронной почте и SMS, телефонное мошенничество в форме вишинга, подмена маршрутизации с выводом пользователя на фиктивные интернет-ресурсы, то есть фарминг. Отдельно следует назвать дипфейки — синтезированные аудио- и видеоматериалы, воспроизводящие голос или внешний облик должностных лиц, что заметно усложняет как предупреждение, так и последующую квалификацию подобных эпизодов.

В статистических материалах Следственного комитета РФ заметное место занимают эпизоды, связанные с незаконным получением и распространением персональных данных. Речь идет о доступе к информационным массивам организаций, из которых извлекаются паспортные сведения, адреса, платежные реквизиты, а также учетные данные пользователей — логины и пароли. Далее эти сведения используются неодинаково: часть из них становится инструментом последующих атак, часть реализуется на теневых площадках. И.Р. Шикула и Е.Н. Куркина указывают, что подобные схемы позволяют склонять потерпевших к переводу денежных средств, побуждать их сообщать банковские данные либо открывать доступ к своим учетным записям². Нарушение в данном случае не исчерпывается вторжением в частную сферу.

¹ Шляхтова О.Г. Компьютерные преступления: историко-правовой аспект / О.Г. Шляхтова // Известия Гомельского государственного университета им. Ф. Скорины. 2023. № 2 (137).

² Шикула И.Р., Куркин Е.Н. Киберпреступность в Российской Федерации: основные методы борьбы и проблемы противодействия/ И.Р. Шикула, Е.Н. Куркин // Международный журнал экспериментального образования. 2023. № 1. С. 38.

А.Ю. Трофимов обращает внимание на иной аспект: незаконный оборот таких данных затрагивает конституционно охраняемую неприкосновенность частной жизни и одновременно формирует основу для новых противоправных действий, включая мошеннические посягательства и шантаж¹.

К числу наиболее сложных высокотехнологичных угроз относится и кибершпионаж, предполагающий неправомерное получение доступа к государственным, военным либо корпоративным сведениям ограниченного характера. Субъектный состав здесь неоднороден: такие деяния совершаются как отдельными лицами, так и организованными структурами, в ряде случаев — при участии иностранных элементов. Мотивировка также варьируется, хотя в ее основе обычно находятся извлечение конкурентных преимуществ, дестабилизация либо компрометация стратегически значимых объектов, а иногда передача полученной информации заинтересованным третьим лицам за вознаграждение. Отдельно СК РФ отмечает увеличение количества преступлений, в которых используются криптовалюты и анонимные платежные механизмы. В эту группу входят легализация преступных доходов, финансовое обеспечение незаконной деятельности, проведение расчетов в рамках вымогательства и оборота запрещенных товаров. Расследование таких дел сталкивается с дополнительными затруднениями: децентрализованный характер криптовалютных систем и ограниченные возможности отслеживания движения средств заметно осложняют установление как маршрута транзакций, так и круга причастных лиц. К числу сопутствующих рисков относятся не только DoS- и DDoS-воздействия, ориентированные на перегрузку серверной и сетевой инфраструктуры с последующим нарушением ее работоспособности.

¹ Трофимова А.Ю. История развития уголовного законодательства в части регламентации оснований ответственности за преступления в сфере компьютерной информации / А.Ю. Трофимова// Молодой ученый. 2021. № 53 (395). С. 128.

Не меньшую проблему создают уязвимости нулевого дня (Zero-day), для которых на момент эксплуатации еще отсутствуют исправления, а также инсайдерский фактор — как преднамеренное содействие, так и неосторожные действия работников, допущенных к информационным системам. В этой группе угроз особенно заметна их разнородность: часть из них реализуется извне, часть связана с внутренним контуром организации, и это усложняет не столько формальную квалификацию, сколько выбор адекватных процессуальных и технических средств реагирования.

Расследование киберпреступлений затрудняется рядом устойчивых обстоятельств. Злоумышленники, как правило, используют инструменты цифровой маскировки: шифрование, VPN-сервисы, подмену IP-адресов, анонимные учетные записи. Существенное значение имеет и трансграничный характер таких деяний, при котором получение значимой информации нередко зависит от взаимодействия с иностранными правоохранительными структурами. Отдельную сложность формирует высокая изменчивость самих атакующих практик: обновляются программные средства, модифицируются сценарии проникновения, все чаще применяются системы искусственного интеллекта — для создания дипфейков, автоматизированного фишинга, обхода защитных механизмов. При этом сбор цифровых доказательств остается процессуально и технически сложной задачей, обычно требующей участия специалистов узкого IT-профиля, и не во всех ситуациях такой ресурс доступен немедленно.

В ответ на указанные вызовы Следственный комитет Российской Федерации развивает специализированные подразделения, располагающие средствами исследования цифровых следов, анализа сетевых транзакций и изучения вредоносного программного обеспечения. Значимым остается межведомственный формат работы с ФСБ России, МВД России, Роскомнадзором и операторами связи; параллельно сохраняется участие в международных механизмах противодействия киберпреступности.

Отдельно следует выделить взаимодействие с Банком России при расследовании хищений денежных средств с банковских счетов, а также с операторами связи — в целях ограничения функционирования мошеннических номеров и фишинговых ресурсов. С 2025 года действует единая межведомственная платформа обмена данными: сроки предоставления сведений сократились с 30 до 3–5 дней. Это заметно ускорило ход предварительного следствия, хотя сама зависимость от скорости межведомственного обмена, по сути, лишь стала более очевидной.

В материалах III Международной научно-практической конференции¹ обращается внимание на то, что в правоприменительном и исследовательском обороте понятие «киберпреступления» давно уже не сводится к перечню составов, закрепленных в гл. 31 УК РФ. Обычно в этот массив включают и деяния экономической направленности: незаконное предпринимательство², осуществляемое без лицензии (ст. 233 УК РФ), уклонение от уплаты налогов и сборов (ст. 243 УК РФ), а также посягательства, сопряженные с изъятием чужого имущества, — мошенничество (ст. 209 УК РФ), вымогательство (ст. 208 УК РФ), хищение имущества посредством изменения компьютерной информации (ст. 212 УК РФ). Тем же контуром охватываются преступления, связанные с незаконным оборотом наркотических средств (ст. 328 УК РФ), и иные составы, в которых цифровая среда меняет сам способ совершения деяния: повышает скрытность, позволяет действовать в большем масштабе, иногда придает посягательству качественно иную форму.

Структура таких преступлений в 2023 г. была выражена достаточно отчетливо. Наибольший удельный вес пришелся на мошенничество: 52,18%, или 353 291 зарегистрированный случай, квалифицированный по ст. 159 УК РФ.

¹ Проблемы противодействия киберпреступности: материалы III Международной научно-практической конференции (Москва, 4 июня 2025 г.). М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2025. – С. 167.

² Проблемы противодействия киберпреступности: материалы II Международной научно-практической конференции (Москва, 26 апреля 2024 года) / Под общ. ред. О.Ю. Антонова, Э.Б. Хатова. - М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2024. – С. 78.

Далее следовали кражи, совершенные с использованием цифровых инструментов, — 17,61% (119 212 эпизодов по ст. 158 УК РФ); по сравнению с предшествующим годом их количество несколько увеличилось. Еще одна крупная категория — незаконный оборот наркотических и психотропных веществ, а равно их аналогов (ст. 228.1 УК РФ): 81 520 преступлений, что составило 12,04% общего числа. После них по распространенности располагались неправомерные доступы к компьютерной информации по ст. 272 УК РФ; зафиксировано 36 788 таких инцидентов¹. Иначе говоря, ядро киберпреступности формируется не только за счет собственно посягательств на информационные системы, но и за счет традиционных составов, перенесенных в цифровую среду. В 2024 г. рост сохранился. По сведениям СК РФ, число выявленных преступлений, связанных с использованием интернета и компьютерных технологий, достигло 765,4 тыс., что на 13,1% выше уровня предыдущего года; одновременно на 7,8% возросла доля тяжких и особо тяжких деяний. Среди наиболее употребимых способов совершения назывались контакты с потенциальными потерпевшими через интернет-мессенджеры, операции с пластиковыми картами для получения доступа к денежным средствам, а также фишинговые схемы — рассылка ложных уведомлений от имени организаций, которым обычно доверяют, с последующим изъятием платежных реквизитов. Число подобных ресурсов за год достигло 350 тыс., увеличившись на 67%². Этим перечень не исчерпывался: значимое место занимали программы-вымогатели класса ransomware, незаконное получение платежной и персональной информации, кибершпионаж, ориентированный на закрытые ведомственные массивы

¹ Статистика киберпреступности по данным МВД России. URL: <https://www.ec-rs.ru/blog/novosti/statistika-kiberprestupnosti-v-rossiyskikh-regionakh-dannye-mvd-za-2024-god/?ysclid=mkzazhqlux584169377> (дата обращения 27.01.2026).

² СК РФ. Официальный сайт. URL: <https://tass.ru/obschestvo/24573429?ysclid=mkzh42p83834667093>. (дата обращения 27.01.2026)

данных и объекты критической государственной инфраструктуры, атаки с целью влияния на общественное сознание.

Около 15% всех кибератак 2024 г. были адресованы государственным органам, включая избирательную систему. Такая динамика, наряду с усложнением самих уголовных дел, потребовала институционального реагирования. В структуре Главного следственного управления СК РФ создан специализированный отдел, использующий отечественные технологические решения для работы с большими массивами сведений, выявления и интерпретации цифровых следов, а также для расследования операций, совершаемых с применением криптовалюты.

В практике расследования дел, связанных с цифровыми следами, заметно возросло значение организационных и кадровых решений. Приоритет отдан не столько формальному расширению компетенций, сколько прикладной подготовке сотрудников: проводятся программы повышения квалификации, создаются профильные методические материалы, осваиваются инструменты анализа и обнаружения электронных доказательств. Речь идет, в частности, об автоматизированных системах отбора релевантных сведений, средствах поиска в неструктурированных открытых источниках, а также о технических решениях, применяемых при исследовании компьютерных устройств и ситуаций, осложненных использованием шифрования. Существенную роль в этой работе играет отечественная программная платформа, ставшая базовым элементом при расследовании преступлений с цифровой составляющей. Параллельно был выстроен электронный документооборот с государственными органами, что сократило сроки получения значимой информации, хотя сам эффект здесь определяется не только скоростью обмена, но и устойчивостью межведомственных процедур. Отдельное значение приобрела международная кооперация, без которой расследование киберпреступлений, имеющих трансграничный характер, фактически утрачивает необходимую полноту. Следственный комитет Российской Федерации участвует как в выработке международно-правовых подходов,

включая работу над соответствующей конвенцией ООН, так и в практическом взаимодействии с зарубежными и негосударственными структурами.

Поддерживаются рабочие контакты с Интерполом и Европоллом при розыске лиц, скрывающихся за пределами страны; заключаются двусторонние соглашения о взаимной правовой помощи с правоохранительными органами Китая, Индии и ОАЭ; иницируются экстрадиционные процедуры по делам о банковских взломах и незаконном обороте персональных данных. Характерным эпизодом стало задержание в 2025 году участников группы, распространявшей Ransomware-as-a-Service: часть серверной инфраструктуры размещалась в Европе, тогда как организаторы находились в Юго-Восточной Азии, и это потребовало координации действий нескольких государств¹.

По данным Следственного комитета РФ на октябрь, за девять месяцев число таких посягательств увеличилось на 120% по отношению к аналогичному периоду предыдущего года. Одновременно меняется и сама конфигурация преступного воздействия: используемые злоумышленниками сценарии становятся более адаптированными к возрастным особенностям детей, а конечной целью нередко выступает изъятие денежных средств из семейного бюджета. В первом полугодии 2025 года выявлено свыше 3,5 тысячи эпизодов, в которых дети использовались как средство обмана родителей для хищения денег; совокупный ущерб семьям превысил 600 миллионов рублей, при этом средний размер потерь по одному случаю за год увеличился вдвое². Не менее показателен и масштаб контакта несовершеннолетних с киберпреступными практиками вообще: по итогам года 81% детей и подростков сталкивались с теми или иными их проявлениями. Наиболее распространенными оставались ложные звонки от «сотрудников банков» — 56%, обращения от лиц, представлявшихся сотрудниками МВД и

¹ Новые тенденции в борьбе с киберпреступностью: уголовно-правовые меры. URL: <https://companies.rbc.ru/news/bFD5SBdC24/novyie-tendentsii-v-borbe-s-kiberprestupnostyu-ugolovno-pravovyye-meryi/?ysclid=mkbbp5r8g1941400558> (дата обращения 15.01.2026).

² СК РФ. Официальный сайт. URL: <https://tass.ru/obschestvo/24573429?ysclid=mkzh42p83834667093>. (дата обращения 27.01.2026)

иных официальных структур, — 40%; подозрительные сообщения от незнакомых пользователей получали 53% респондентов, от аккаунтов знакомых — 41%. Кроме того, 39% переходили по сомнительным ссылкам, распространявшимся через телеграм-каналы и социальные сети.

В этих условиях профилактические и просветительские меры заняли устойчивое место в стратегии СК РФ по противодействию киберпреступности. Для населения подготавливаются информационные материалы, посвященные актуальным мошенническим схемам; они распространяются через средства массовой информации и социальные сети, дополняются памятками по защите учетных записей. Бизнесу адресуются методические рекомендации по соблюдению базовых требований кибергигиены, включая своевременное обновление программного обеспечения и применение многофакторной аутентификации. В образовательной среде проводятся занятия по цифровой безопасности с разбором практических ситуаций, в том числе типового сценария «звонка от службы безопасности банка». Здесь важен не только объем информирования, но и регулярность повторения таких мер, поскольку преступные модели меняются быстрее, чем закрепляются навыки безопасного поведения.

За первые семь месяцев 2025 года число преступлений, совершенных с использованием информационно-телекоммуникационных технологий в России, приблизилось к 425 тыс. На этом фоне в 2025 году был введен в действие портал «Кибербезопасность для всех», через который пользователь может проверить сомнительную ссылку, направить сообщение о фишинговом ресурсе и получить экспертную консультацию¹. Отдельную тревогу вызывает участие самих несовершеннолетних в цифровой преступности: около 16,4 тыс. правонарушений в сфере компьютерной информации были совершены подростками, а к маю 2025 года уже каждая пятая киберугроза в стране исходила от лиц, не достигших совершеннолетия.

¹ Степанов Е.А. Пути совершенствования расследования и раскрытия компьютерных преступлений / Е.А. Степанов // Вестник науки. 2025. № 1 (82). С. 459.

По оценке ректора Московской академии Следственного комитета РФ им. А. Сухарева А. Бессонова, значительная доля таких подростков вовлекается взрослыми участниками, причем последствия подобного вовлечения не сводятся к единичному противоправному эпизоду и затрагивают физическое, эмоциональное и моральное состояние несовершеннолетних¹. Более 70% преступлений против детей совершается в социальных сетях, прежде всего во «ВКонтакте» и «Одноклассниках»; остальная часть приходится на мессенджеры, включая Telegram, WhatsApp, Likee и иные платформы, также активно используемые в противоправных целях. Практика последних месяцев показывает достаточно устойчивый набор угроз: требования сообщить коды из СМС с последующим психологическим давлением, ложные предложения о поступлении или продаже ответов на экзамены, особенно в период после ЕГЭ, а также вовлечение в незаконную деятельность — от распространения запрещенных материалов до участия в мошеннических схемах². Статистические данные за конец 2025 — начало 2026 года пока не опубликованы вследствие незавершенности отчетного периода, однако сама динамика, судя по имеющимся материалам, сохраняет направленность на рост и усложнение рисков (Приложение 1 — рис. 3).

В качестве приоритетного профилактического решения представляется обоснованным развитие интегрированных сервисов на основе искусственного интеллекта, ориентированных именно на защиту несовершеннолетних в цифровой среде. Речь идет не просто о техническом мониторинге, а о маркировании признаков имитации общения со взрослыми: выявлении недостоверных сведений о возрасте и местонахождении, использовании поддельных фотографий, искусственно сгенерированных либо ненатуральных аудиосообщений, иных индикаторов мошеннического поведения.

¹ Проблемы противодействия киберпреступности: материалы III Международной научно-практической конференции (Москва, 4 июня 2025 г.). М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2025. – С. 111.

² Проблемы противодействия киберпреступности: материалы II Международной научно-практической конференции (Москва, 26 апреля 2024 года) / Под общ. ред. О.Ю. Антонова, Э.Б. Хатова. - М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2024. – С. 117.

Наряду с этим сохраняет актуальность идея специализированного государственного координатора по кибербезопасности, который обеспечивал бы согласованное реагирование различных служб на выявленные инциденты и аккумулировал сведения о преступности в цифровой среде с опорой на механизмы государственно-частного партнерства. Здесь возникает и другой аспект. Расследование киберпреступлений в современных условиях требует соединения правовых процедур с экспертными техническими знаниями, причем в институциональной форме, а не эпизодически.

В системе Следственного комитета РФ уже действуют специализированные экспертные подразделения — Экспертно-криминалистический центр и сеть региональных лабораторий, располагающие инструментами и методиками для анализа цифровых следов¹. Их организация построена по принципу территориального присутствия: подразделения компьютерно-технических исследований функционируют как в центральном аппарате, так и в ряде городов, среди которых Санкт-Петербург, Симферополь, Казань, Ессентуки, Красноярск, Хабаровск, Благовещенск, Воронеж, Иркутск, Кемерово, Нижний Новгород, Новосибирск, Омск, Барнаул, Екатеринбург. Такая конфигурация позволяет распределять компетенции между площадками и обеспечивать оперативное реагирование на инциденты различного масштаба по всей территории страны. В следственной практике выделяется несколько направлений компьютерно-технических исследований: изучение аппаратных средств, включая персональные компьютеры, серверное оборудование, носители информации и виртуальные объекты; анализ цифровых сетей; исследование мобильных и носимых устройств — смартфонов, планшетов, фитнес-браслетов, «умных» часов; экспертиза фото- и видеоматериалов, а также информационно-аналитическая обработка значительных массивов данных.

¹ Проблемы противодействия киберпреступности: материалы III Международной научно-практической конференции (Москва, 4 июня 2025 г.). М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2025. – С. 115.

Примечательно, что информационно-аналитическая экспертиза как самостоятельное направление была закреплена Минюстом только в 2020 году, после предварительной апробации внутри системы СК РФ. Использование цифровых доказательств при этом подчинено строгим процессуальным требованиям.

Сама процедура исследования обычно строится на двух уровнях. Первый — первичный, ускоренный осмотр с обязательной видеофиксацией, необходимый для отбора перспективных объектов и базовой фильтрации информации. Второй связан уже с углубленной экспертизой, где применяются специализированные программные комплексы для восстановления удаленных либо зашифрованных данных, вскрытия защищенных архивов, интерпретации сведений, извлекаемых из специальных контейнеров. Существенно и то, что изменился характер самих объектов экспертного анализа: граница между компьютерной техникой и бытовой электроникой сегодня почти стерта. Источником значимой информации могут выступать подключенные к сети бытовые устройства, интеллектуальные автомобильные мультимедийные системы, различные виды носимой электроники, содержащие конфиденциальные сведения. Именно поэтому современная экспертиза вынуждена работать с крайне разнородными носителями и постоянно расширяющимся кругом объектов исследования¹.

Цифровая безопасность повышается, одновременно растет и сложность защиты информации. В устройствах активно внедряются системы шифрования, регулярно используются пароли, а современные носители данных обладают огромной емкостью. Прежние методы (например, J-Tag, Chip-OFF), которые еще недавно были эффективны при извлечении информации с микросхем, теряют актуальность из-за тотального шифрования.

¹ Проблемы противодействия киберпреступности: материалы III Международной научно-практической конференции (Москва, 4 июня 2025 г.). М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2025. – С. 121.

Даже подбор простых паролей в ряде случаев занимает до полугода интенсивной работы.

Используемое программное обеспечение, как отечественное (Эскиз В, Зверобой, Следопыт, Октопус, Мобильный криминалист и др.), так и зарубежное (Belkasoft, FTK, Magnet, X-Ways, UFED, Passware и другие), покрывает широкий спектр задач, а именно поиск и фильтрация файлов, анализ текстовых и графических материалов, восстановление переписок и изучение интернет-истории. Проблемы остаются нерешенными (выявление и декодирование зашифрованных архивов, нестандартные расширения, удаленные текстовые массивы, а также работы с узкоспециализированными программами и нетиповыми устройствами (например, GPS-навигаторами, автомобильными блоками, камуфлированной электроникой). Важнейшая составляющая экспертной деятельности - уровень профессионализма специалистов. Эксперты должны не только найти все цифровые следы, но и грамотно подобрать программные решения с учетом меняющихся тактик злоумышленников. Проблемными моментами остаются устаревшие стандарты (ГОСТы), нехватка типовых методик для анализа новых видов устройств и высокая степень зависимости от зарубежных производителей ПО, что создает риски при прекращении их поддержки на территории РФ. Дальнейшее развитие требует совершенствования отечественных программных комплексов, активного обучения экспертов работе с нетипичными устройствами, внедрения ИИ для автоматизации обработки больших массивов данных и расширения международного обмена передовыми методиками. Экспертно-криминалистическая инфраструктура СК РФ остается ключевым элементом государственного механизма противодействия киберпреступности.

Однако дальнейшее успешное функционирование этой системы возможно лишь при условии регулярного обновления инструментов, повышения уровня подготовки кадров и совершенствования процессуальных процедур обращения с цифровыми доказательствами¹.

¹ Киберпреступность в 2026 году: новые схемы утечек данных. URL: <https://falcongaze.com/ru/pressroom/publications/informacionnaya-bezopasnost/> (дата обращения 27.01.2026).

Среди ключевых проблем остаются дефицит квалифицированных кадров, устаревшие процессуальные нормы и санкционные ограничения. Для их преодоления СК РФ расширяет сеть региональных лабораторий ЭКЦ СКР, организует стажировки в ИТ-компаниях и программы переподготовки следователей. Вносится предложение о корректировке УПК РФ для упрощения изъятия облачных данных и криптоактивов.

В условиях санкционных ограничений ускоряется импортозамещение ПО для криминалистического анализа, например, разрабатывается аналог UFED на базе отечественных алгоритмов. Осознавая скорость эволюции угроз, ведомство создает «лабораторию будущего» в ЭКЦ СКР для тестирования методов противодействия ИИ-атакам и потенциальным квантовым угрозам.

В перспективе до 2028 года СК РФ планирует внедрение единой цифровой платформы для автоматизации сбора и анализа цифровых доказательств, развитие сети киберполигонов для тренировки следователей в условиях, имитирующих реальные атаки, а также создание специализированного подразделения по расследованию преступлений в метавселенных и с использованием нейроинтерфейсов.

Таким образом, система противодействия киберпреступности эволюционирует от реактивных мер к проактивной модели, основанной на прогнозировании угроз, междисциплинарном взаимодействии и технологическом суверенитете. Ее эффективность будет определяться гибкостью правовых механизмов, уровнем подготовки кадров и способностью интегрировать передовые научные разработки в практическую деятельность.

2.3. Методы противодействия и расследования киберпреступлений Российской Федерации

В Российской Федерации в 2025–2026 годах формируется развернутый механизм противодействия киберпреступности и ее расследования. Его содержание не сводится к одному направлению: одновременно развиваются

законодательные решения, межведомственная координация, техническое переоснащение соответствующих процедур и профилактика, рассчитанная на системное снижение цифровых рисков. Конфигурация этой работы складывается не сразу, а через совмещение нескольких линий регулирования, что для рассматриваемой сферы, впрочем, вполне характерно.

Особое значение в данном контексте имеет Федеральный закон Российской Федерации от 01.04.2025 № 41-ФЗ. Именно этот акт закрепил правовую основу для развертывания государственной информационной системы, предназначенной для противодействия правонарушениям, совершаемым с использованием интернет-технологий. Тем самым была задана институциональная рамка, в пределах которой последующие меры — организационные, технические и процессуальные — получили более связанный, хотя и не полностью однородный, характер. С 1 марта 2026 года эта система начнет функционировать в полном объеме, обеспечивая оперативный обмен данными между правоохранительными органами, операторами связи, кредитными организациями, мессенджерами, провайдерами хостинга и иными участниками. В ГИС будут аккумулироваться сведения о лицах, причастных к противоправным действиям, а также об абонентских номерах, использованных для мошеннических операций. Предшествующим этапом стал пилотный проект (12 мая 2025 года - 1 марта 2026 года) по налаживанию взаимодействия госорганов, банков и операторов связи. В нем участвовали Минцифры, МВД России, ФСБ России, Роскомнадзор, Росфинмониторинг, ФСТЭК, Генпрокуратура РФ, СК РФ и представители финансового сектора.

Цель проекта - отработать механизмы информационного обмена для своевременного предотвращения преступлений с использованием информационно-коммуникационных технологий. По итогам пилотного этапа до 2 марта 2026 года Минцифры, МВД России, ФСБ России и Роскомнадзор должны сформировать единую платформу сбора и анализа данных на базе ГИС «Антифрод», что позволит консолидировать информацию о цифровых преступлениях и ускорить реагирование на угрозы.

Законодательные изменения 2025 года существенно расширили инструменты защиты. Введен запрет на использование иностранных мессенджеров для коммуникаций с гражданами со стороны госорганов, банков и операторов связи. Банки обязаны проверять факт добровольного согласия клиента на снятие наличных в банкоматах. Граждане получили возможность устанавливать самозапрет на онлайн-оформление сим-карт через «Госуслуги», а также введен запрет на передачу сим-карт третьим лицам (с исключениями для близких родственников). Дополнительно введена маркировка звонков от ИП и ООО, что повышает прозрачность коммуникаций и затрудняет действия мошенников. На техническом уровне внедряются алгоритмы машинного обучения для выявления аномалий в поведении пользователей - например, массового копирования файлов или подозрительных транзакций.

До 3 августа 2026 года предполагается подготовить проект документа стратегического планирования, посвященного противодействию правонарушениям, совершаемым с применением ИКТ. В этом документе намечено нормативно зафиксировать базовые понятия и систему целевых индикаторов, относящихся к борьбе с кибермошенничеством; такая рамка нужна не только для терминологической определенности, но и для согласования практики различных ведомств. В целом формируемая на 2025–2026 годы модель противодействия киберпреступности складывается как многокомпонентная: в ней соединяются правовые решения, технические инструменты, организационные механизмы и образовательные меры, направленные на устойчивую защиту цифровой среды.

Отдельный блок связан с ограничением доступа к противоправным интернет-ресурсам во внесудебном порядке. Речь идет о фишинговых сайтах, площадках, распространяющих вредоносное программное обеспечение, а также ресурсах, реализующих несертифицированные средства связи. Параллельно формируется единый реестр электронных ссылок, ведущих на официальные сайты востребованных интернет-магазинов; его введение ориентировано на снижение риска использования сайтов-имитаторов.

Специальная работа ведется и в отношении преступлений, где применяются инструменты искусственного интеллекта: разрабатывается алгоритм, предназначенный для выявления такого использования, в том числе при распознавании дипфейков и синтезированной речи. В основные мобильные приложения государственных органов, банков и иных социально значимых сервисов планируется встроить модуль обязательного уведомления граждан о вероятных преступных посягательствах¹.

Профилактика в этой сфере выстраивается не как совокупность разрозненных акций, а в более регулярном режиме. Предусмотрены меры по повышению цифровой и финансовой грамотности населения, включая размещение социальной рекламы в средствах массовой информации. Особо выделено направление, связанное с предупреждением вовлечения несовершеннолетних в киберпреступную деятельность: ко II кварталу 2026 года должен быть создан депозитарий профилактических материалов. Реализация обозначенных инициатив возложена на Минцифры России, МВД России, Минэкономразвития, Роскомнадзор, Банк России и иные государственные структуры. Одновременно разрабатываются программы подготовки специалистов для правоохранительных органов; они охватывают современные подходы к анализу цифровых следов, восстановлению данных, а также экспертизе вредоносного программного обеспечения.

Сохраняет значение и международное взаимодействие, без которого противодействие транснациональным киберугрозам в практическом плане оказывается существенно затруднено. В продолжение рассмотрения мер противодействия и расследования киберпреступлений в РФ в 2025–2026 годах важно отметить усиление ответственности операторов связи и финансовых организаций. Рассматривается вопрос об установлении обязанности операторов связи, интернет-провайдеров, организаторов распространения

¹ Киберпреступность в 2026 году: новые схемы утечек данных. URL: <https://falcongaze.com/ru/pressroom/publications/informacionnaya-bezopasnost/> (дата обращения 27.01.2026).

информации и иных структур оперативно уведомлять правоохранительные органы о выявленных признаках преступлений, совершаемых с использованием цифровых технологий. Эта инициатива будет реализована при участии МВД России, Минцифры, ФСБ и Роскомнадзора во взаимодействии с Генпрокуратурой РФ и СК РФ. По итогам работы в III квартале 2027 года правительство планирует выйти с законодательными инициативами по изменению действующего регулирования. Одновременно ведется работа по повышению ответственности за нарушение законодательства в области персональных данных.

К тому же сроку (III квартал 2027 года) МВД России, Минцифры, Минэкономразвития, ФСБ России и Роскомнадзор при содействии Генпрокуратуры РФ представят предложения по увеличению срока давности привлечения к административной ответственности за такие правонарушения. Это позволит эффективнее пресекать утечки данных и наказывать виновных¹. В сфере технической защиты продолжается развитие единого реестра адресов электронных ссылок на официальные сайты популярных интернет-магазинов. Его создание запланировано на III квартал 2026 года при участии Минцифры, МВД России, Минфина, ФНС России и Роскомнадзора. Реестр призван минимизировать риски, связанные с электронными двойниками интернет-магазинов, которые используются для кражи персональных данных и финансовых махинаций.

Особое внимание уделяется противодействию использованию искусственного интеллекта в преступных целях. Минцифры, МВД России и Роскомнадзор ведут разработку специализированного алгоритма, способного выявлять признаки применения ИИ при совершении киберпреступлений - например, генерацию дипфейков, синтезированной речи или автоматизированных фишинговых атак. Завершение этой работы

¹ СК РФ. Официальный сайт. URL: <https://tass.ru/obschestvo/24573429?ysclid=mkzh42p83834667093>. (дата обращения 27.01.2026)

запланировано на I квартал 2028 года. В рамках профилактической работы расширяется интеграция модуля обязательного информирования граждан о возможных преступлениях в мобильные приложения госорганов, банков и социально значимых сервисов. Проработать этот вопрос поручено Минцифры и МВД России к I кварталу 2027 года. Параллельно продолжается размещение социальной рекламы в СМИ, направленной на повышение цифровой и финансовой грамотности населения. Для координации усилий государства и бизнеса формируется оперативный штаб по противодействию интернет-мошенничеству. В его состав войдут представители ключевых федеральных ведомств, Центробанка РФ, кредитных организаций, операторов связи и цифровых платформ.

Основные задачи штаба включают выявление новых мошеннических схем; сбор и систематизация эффективных мер противодействия; ведение единой базы профилактических и оперативных мероприятий; подготовка предложений по изменению законодательства. В числе новых законодательных инициатив - усиление ответственности операторов связи за нарушение правил продажи сим-карт, в том числе иностранным гражданам. Также вводится механизм детских сим-карт, позволяющий родителям контролировать доступ ребенка к нежелательному контенту и снижать риски вовлечения в мошеннические схемы. Для борьбы с дропперами (лицами, предоставляющими мошенникам доступ к банковским счетам) предлагается ограничить количество банковских карт на одного человека до 20, что затруднит создание сетей для обналичивания преступных средств.

Закрепляется право гражданина сообщать о кибермошенничестве через «Госуслуги», что упростит фиксацию инцидентов и ускорит оповещение банков, операторов связи и цифровых платформ. Для защиты учетных записей на «Госуслугах» вводится требование о восстановлении доступа только доверенными способами: через МФЦ, банковские приложения или биометрию. Важным направлением остается международное сотрудничество в сфере кибербезопасности. Россия участвует в разработке универсальных стандартов

и механизмов взаимодействия с зарубежными правоохранительными органами, что особенно актуально в условиях транснационального характера современных киберугроз¹. Таким образом, система противодействия киберпреступлениям в РФ на 2025–2026 годы и перспективу до 2028 года выстраивается как многоуровневая и адаптивная, сочетающая совершенствование нормативной базы; внедрение передовых технических решений; усиление межведомственной координации; профилактику и просвещение; международное взаимодействие.

Цель - не только оперативное реагирование на киберпреступления, но и предотвращение киберпреступлений за счет создания устойчивой цифровой среды, где риски для граждан и бизнеса минимизированы, а злоумышленники сталкиваются с системным и скоординированным противодействием.

Вывод по второй главе исследования.

Анализ статистических данных о киберпреступлениях в РФ за 2023–2025 годы демонстрирует существенные расхождения между информацией, предоставляемой МВД России и СК РФ. Эти различия не свидетельствуют о противоречиях в работе ведомств, а отражают объективную специфику их компетенций, методик учета и целевых задач. МВД РФ ведет учет всех зарегистрированных киберпреступлений, включая сообщения о неправомерном доступе к данным, распространении вредоносного ПО, нарушениях правил эксплуатации ИКТ-сетей и иных противоправных действиях в цифровой среде.

В структуре министерства действует специализированное управление (УБК МВД России), которое занимается выявлением, предупреждением и раскрытием таких правонарушений. Статистика МВД России показывает общий объем зафиксированных инцидентов, их распределение по способам совершения (например, через мессенджеры, соцсети) и каналам

¹ СК РФ. Официальный сайт. URL: <https://tass.ru/obschestvo/24573429?ysclid=mkzh42p83834667093>. (дата обращения 27.01.2026)

распространения угроз. Так, за 11 месяцев 2025 года было зарегистрировано 627 тысяч киберпреступлений - на 10,8% меньше, чем за аналогичный период 2024 года. При этом почти две трети (63,4%) составили хищения и мошенничества (397,4 тысячи случаев), а число преступлений, связанных с незаконным оборотом наркотиков в интернете, выросло на 28,5% (до 109,2 тысячи). СК РФ, напротив, фокусируется на расследовании тяжких и особо тяжких преступлений, где информационно-коммуникационные технологии выступают инструментом для достижения преступной цели. В сферу внимания комитета попадают дела о хищениях крупных сумм, преступлениях против половой неприкосновенности несовершеннолетних, террористической и экстремистской деятельности, а также атаках на критическую информационную инфраструктуру.

Отчетность СК РФ отражает не общее количество зарегистрированных случаев, а число завершенных расследований и направленных в суд уголовных дел. Например, в 2024 году было расследовано свыше 21 тысячи киберпреступлений - на 12% больше, чем в 2023 году. При этом акцент делается на детализации специфических аспектов: использовании искусственного интеллекта для подделки голоса и изображения, вовлечении несовершеннолетних в противоправные действия, атаках на стратегические отрасли.

Причины расхождений в данных обусловлены несколькими факторами:

- различаются критерии учета: МВД России фиксирует все поступившие сообщения, включая те, что еще находятся на стадии проверки, тогда как СК РФ отчитывается только о делах, по которым собрана доказательная база и принято процессуальное решение;

- временные рамки учета не всегда совпадают: статистика МВД России охватывает календарный период, а расследования СК РФ могут длиться дольше года;

- методология классификации преступлений отличается: МВД России группирует случаи по техническим признакам (тип вредоносного ПО, канал

атаки), а СК РФ по уголовно-правовой квалификации (ст. 159 УК РФ, ст. 272 УК РФ и др.). Кроме того, сложность атрибуции преступлений (например, определение юрисдикции или личности злоумышленника) нередко приводит к передаче дел между ведомствами, что создает временные лаги в отчетности.

Прикладной аспект указанного расхождения связан прежде всего с различием аналитических задач. Сведения, публикуемые МВД России, используются для фиксации актуальной динамики и, в более практическом плане, для быстрой перенастройки профилактической работы. Рост числа преступлений в 2025 году на 17,5% потребовал, в частности, усиления контроля за коммуникацией через мессенджеры; именно такого рода массивы позволяют реагировать без существенной временной задержки, хотя сама управленческая корректировка обычно не исчерпывается одной мерой.

Иной ракурс задаёт статистика Следственного комитета РФ. Она в большей степени характеризует не общую текущую ситуацию, а результаты раскрытия и расследования наиболее сложных и общественно опасных схем. Через эти данные оценивается и то, насколько продуктивно выстроено межведомственное взаимодействие, поскольку его качество проявляется не в декларациях, а в итоговой результативности расследований.

Для законодателя наибольшую ценность представляет не изолированное использование ведомственной статистики, а ее сопоставление. Именно в таком сопоставлении становятся заметны регулятивные лакуны, включая случаи, где ответственность за применение технологий искусственного интеллекта в преступных целях разработана недостаточно или описана фрагментарно.

В этом отношении расхождения между данными МВД России и Следственного комитета Российской Федерации следует рассматривать не как признак системного дефекта, а как результат различия их функций, задач и уровня аналитической детализации.

Материалы МВД России позволяют оценивать общий масштаб распространения киберпреступности, тогда как отчетность СК РФ

концентрирует внимание на наиболее опасных формах таких деяний и на последствиях, которые они влекут. При совместном анализе возникает более объемное представление о ситуации: одна группа данных показывает широту явления, другая — его криминологически значимые акценты. Отсюда, хотя и не только отсюда, появляется возможность точнее определять направления корректировки законодательства и выстраивать межведомственное взаимодействие там, где разобщенность подходов пока сохраняется.

Перспективным остается унификация критериев учета, развитие совместных информационных систем (например, ГИС «Антифрод») и укрепление международного сотрудничества при расследовании трансграничных преступлений. Такой комплексный подход позволяет не только реагировать на текущие угрозы, но и выстраивать долгосрочную стратегию противодействия киберпреступности в цифровой среде.

ЗАКЛЮЧЕНИЕ

Итоговые выводы по задачам исследования

1. В результате исследования уточнено и конкретизировано понятие киберпреступления как уголовно наказуемого деяния, совершаемого в цифровой среде с обязательным использованием информационно-коммуникационных технологий в качестве ключевого инструмента реализации преступного умысла.

Выделены признаки: опосредованность взаимодействия преступника и жертвы (отсутствие физического контакта), трансграничный характер деяний (возможность совершения из любой точки мира), высокая латентность (сложность обнаружения и фиксации следов), активное применение методов цифровой конспирации (шифрование, VPN, криптовалюты, анонимные мессенджеры), а также динамичность - непрерывная эволюция схем и инструментов противоправной деятельности.

К особенностям отнесены: мультивекторность угроз (одновременное воздействие на разные объекты правоохраны), прямая зависимость от уровня цифровизации общества (рост числа преступлений параллельно с распространением цифровых сервисов), необходимость специализированных технических компетенций у правоохранителей (знание принципов работы сетей, криптографии, блокчейна) и высокая скорость совершения деяний (мошеннические операции могут занимать секунды).

2. Рассмотрена классификация киберпреступлений по объекту посягательства и способу совершения. К преступлениям против собственности отнесены: мошенничество с использованием фишинга и социальной инженерии, хищения через банковские приложения и платежные системы, дропперские схемы (использование подставных лиц для вывода средств). Классификация демонстрирует необходимость дифференцированного подхода: для каждого типа требуются специфические методы выявления, фиксации доказательств и профилактики.

3. Анализ нормативно- правовой базы показал, что регулирование строится на комплексе нормативных актов. В последние годы внедрены новые механизмы защиты, а именно самозапреты на кредиты, «период охлаждения» для подозрительных операций, маркировка звонков, ограничения на использование иностранных мессенджеров в госсекторе. Однако выявлены существенные пробелы: фрагментарность регулирования (отсутствие единого кодифицированного акта по киберпреступлениям), отставание норм от технологических реалий (не определены понятия «дипфейк», «криптовалютный миксер»), недостаточная гармонизация с международным правом (не ратифицирована Будапештская конвенция о киберпреступности). Это снижает эффективность противодействия трансграничным угрозам и затрудняет экстрадицию преступников.

4. Статистический анализ за 2023–2025 годы выявил противоречивую динамику. Хищения и мошенничество занимают особенное положение, а преступления, связанные с незаконным оборотом наркотиков в интернете.

Отмечен рост атак через мессенджеры. МВД фиксирует все зарегистрированные сообщения (включая находящиеся на проверке), а СК отчитывается только о завершенных расследованиях и направленных в суд делах. Это создает противоречивость в данных.

5. Приоритетом являются тяжкие и особо тяжкие преступления, где ИКТ выступают инструментом: хищения в крупном размере с применением ИИ (подделка голоса, дипфейки), вовлечение несовершеннолетних в противоправные сообщества (суицидальные группы, экстремистские организации), атаки на критическую информационную инфраструктуру (энергетика, транспорт, госуслуги), а также террористическая деятельность (координация, сбор средств). Особенностью расследований является необходимость междисциплинарной экспертизы: компьютерно-техническая, лингвистическая (анализ контента), финансовая (отслеживание криптовалютных транзакций). Это требует от следователей не только юридических знаний, но и понимания цифровых технологий, что актуализирует вопрос подготовки кадров.

6. Выявлены следующие группы методов противодействия: технологические: компьютерно-техническая экспертиза, анализ цифровых следов, ГИС «Антифрод» для обмена данными между банками и правоохранителями; правовые: актуализация УК РФ (дополнение составов преступлений), ФЗ 187-ФЗ (регулирование КИИ), введение самозапретов и «периода охлаждения»; организационные: межведомственные штабы (МВД, СК, ФСБ, Минцифры), взаимодействие с ИТ-компаниями и банками; международные: участие в разработке конвенции ООН против киберпреступности, запросы о правовой помощи; профилактические: повышение цифровой грамотности, социальная реклама, модули информирования в мобильных приложениях.

Оценка эффективности показала положительные результаты: снижение общего числа зарегистрированных преступлений (–10,8% в 2025 г.), рост раскрываемости тяжких дел (+12% в 2024 г.), внедрение ГИС «Антифрод»

ускорило блокировку мошеннических операций; проблемы: дефицит ИТ-следователей (нехватка специалистов с компетенциями в криптографии и блокчейн-анализе), временные лаги между регистрацией и расследованием (до 6–12 месяцев), сложность экстрадиции трансграничных преступников, отсутствие норм об ответственности за ИИ-преступления; перспективы: автоматизация анализа цифровых следов с помощью ИИ, расширение программ подготовки следователей, унификация критериев учета между ведомствами, усиление международного сотрудничества. Автор исследования считает, что противодействие киберпреступлениям требует системного подхода: совершенствования законодательства (ликвидация пробелов, гармонизация с международными нормами), внедрения передовых технологий (ИИ для анализа данных, блокчейн-трекинг), укрепления межведомственной и международной координации, а также последовательной профилактики.

Предложения по совершенствованию противодействия киберпреступлениям:

- создать единый кодифицированный акт по киберпреступлениям, который систематизирует все составы преступлений в цифровой среде; вводит чёткие определения новых технологических терминов («дипфейк», «криптовалютный миксер», «ИИ-преступление» и т. д.); устанавливает единые критерии учёта и отчётности для всех правоохранительных органов, устраняя расхождения в данных МВД и СК РФ;

- усилить подготовку ИТ-следователей и экспертов: разработать специализированные образовательные программы в вузах МВД и СК с углублённым изучением криптографии, блокчейн-анализа, методов цифровой криминалистики; организовать регулярные курсы повышения квалификации для действующих следователей с привлечением специалистов из ИТ-компаний; создать систему стажировок в профильных подразделениях ФСБ и Минцифры для обмена опытом;

- развивать технологические инструменты противодействия: масштабировать ГИС «Антифрод» на все регионы, интегрировав её с системами банков, операторов связи и платформ электронной коммерции; внедрить алгоритмы ИИ для автоматизированного анализа цифровых следов и выявления подозрительных транзакций в режиме реального времени; разработать национальную систему блокчейн-трекинга для отслеживания криптовалютных операций, связанных с преступной деятельностью;

- углубить международное сотрудничество: ускорить процесс ратификации Будапештской конвенции о киберпреступности для упрощения экстрадиции и обмена данными с зарубежными партнёрами; инициировать создание региональной платформы обмена информацией по киберпреступлениям в рамках СНГ и БРИКС; наладить прямое взаимодействие между российскими правоохранительными органами и международными организациями (Интерпол, Европол) для оперативного реагирования на трансграничные угрозы.

Реализация данных предложений позволит создать комплексную систему противодействия киберпреступлениям, сочетающую совершенствование законодательства, развитие технологий, укрепление межведомственной координации и повышение квалификации специалистов. Это обеспечит баланс между оперативным реагированием на текущие угрозы и стратегическим планированием долгосрочной защиты цифровой среды.

Предложения автора исследования представлены в Приложении 2 (таблица 1).

Эти предложения требуют детальной проработки с учетом баланса между безопасностью и правами граждан, а также международного опыта в сфере регулирования киберпространства.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аккаева Х.А. Киберпреступления: криминологический анализ / Х.А. Аккаева // Право и управление. 2025. № 1. С. 317–322.
2. Апухтина А.О. Киберпреступность: понятийно-содержательный аспект / А. О. Апухтина // Молодой ученый. 2024. № 45 (544). С. 229-231.
3. Арипшев А.М. О некоторых вопросах обеспечения эффективного противодействия киберпреступлениям / А.М. Арипшев // Право и управление. 2025. № 1. С. 329–331.
4. Астахова Е.А. Перспективы противодействия использованию ИКТ в преступных целях / Е.А. Астахова // Правовая политика и правовая жизнь. 2025. № 1. С. 56–64.
5. Баишев Д.А. Проблемы противодействия киберпреступности / Д.А. Баишев // Молодой ученый. 2025. № 20 (571). С. 378-380.
6. Бондарь Е.О. Киберпреступность как новая криминальная угроза / Е.О. Бондарь // Вестник Московского университета МВД России. 2020. № 1. С. 155–158.
7. Бормотова Т.М., Ильин А.Е., Белянский Е.Б., Макаров В.В. Киберпреступность в России: состояние и методология анализа / Т.М. Бормотова и [др.] // Этносоциум и межнациональная культура. 2023. № 10 (184). С. 60–73.
8. Булохов И.И. Понятие и признаки киберпреступления / И.И. Булохов. - Текст: непосредственный // Молодой ученый. - 2022. - № 46 (441). - С. 182-183.
9. Взять цифровой след. Как раскрываются преступления в МВД. URL: <https://secpost.ru/vzyat-czifrovoj-sled-kak-raskryvayut-kiberprestupleniya-v-rossii-v-2025-godu?ysclid=mkzbfmvvdj486492345> (дата обращения 28.01.2026).
10. Гекк Б.В. Борьба с киберпреступностью в РФ: анализ явления и законодательные меры противодействия / Б. В. Гекк // Молодой ученый. 2024. № 8 (507). С. 149-151.

11. Гильмутдинова Ю.Ю. Проблемы уголовно-правовой квалификации киберпреступлений по законодательству РФ / Ю.Ю. Гильмутдинова // *Lex criminalis scientiarum*. 2025. № 1 (3). С. 51–55.
12. Кобец П.Н. Правовые основы предупреждения киберпреступлений: отечественный и зарубежный опыт / П.Н. Кобец // *Научный вестник Омской академии МВД России*. 2022. № 2. С. 101-105.
13. Конвенция Организации Объединенных Наций против киберпреступности: резолюция Генеральной Ассамблеи. 2024. № 79/243.
14. Кочесоков Р.Х. Киберпреступность в России: тенденции и методы борьбы / Р.Х. Кочесоков// *Пробелы в российском законодательстве*. 2023. Т. 16. №5. С. 242-246.
15. Киберпреступность в 2026 году: новые схемы утечек данных. URL:<https://falcongaze.com/ru/pressroom/publications/informacionnaya-bezopasnost/> (дата обращения 27.01.2026).
16. Клишков В.Б., Стебенева Е.В., Яковлева М.А. Киберпреступность: понятие, признаки, основные направления противодействия/ В.Б Клишков, Е.В. Стебенева, М.А. Яковлева // *Вестник Нижегородского университета им. Н. И. Лобачевского*. 2022. № 4. С. 106–114.
17. Мозжерина Е.С. Кибератаки и киберпреступления: современные тренды и методы предотвращения / Е.С. Мозжерина// *Молодой ученый*. 2024. № 48 (547). С. 5-7.
18. Михайлюк В.А. Киберполиция - современный правоохранительный орган в борьбе с интернет-преступностью / В.А. Михайлюк // *Вестник Уфимского юридического института МВД России*. 2023. № 1(99). С. 74-79.
19. Новые тенденции в борьбе с киберпреступностью: уголовно-правовые меры. URL: <https://companies.rbc.ru/news/bFD5SBdC24/novyie-tendentsii-v-borbe-s-kiberprestupnostyu-ugolovno-pravovyye-meryi/?ysclid=mkbbp5r8g1941400558> (дата обращения 15.01.2026).

20. Никиташенко В.В. Понятие и признаки киберпреступности / В.В. Никиташенко// Молодой ученый. 2021. № 14 (356). С. 250-252.

21. Никульченкова Е.В. О необходимости введения дефиниции «киберпреступление» в уголовный закон Российской Федерации/ Е.В. Никульченкова // Вестник Омского университета. Серия. Право. 2022. Т. 19. № 3. С. 98–107.

22. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 г. № 149-ФЗ (в ред. от 29.12.2025)// Собрание законодательства РФ. 2006. № 31 (часть I). Ст. 3448.

23. О персональных данных: федеральный закон от 27.07.2006 г. № 152-ФЗ (в ред. от 01.09.2025)// Собрание законодательства РФ. 2006. № 31 (часть I). Ст. 3451.

24. О защите детей от информации, причиняющей вред их здоровью и развитию: федеральный закон от 29.12.2010 г. № 436-ФЗ (в ред. от 01.03.2024)// Собрание законодательства РФ. 2011. № 1. Ст. 48.

25. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26.07.2017 г. № 187-ФЗ (в ред. от 01.09.2025)// Собрание законодательства РФ. 2017. № 31 (часть I). Ст. 4736

26. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37. URL: <https://normativ.kontur.ru/document?moduleId=7&documentId=439211&ysclid=mkz0c4b54590851850> (дата обращения 27.01.2026).

27. О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации»: федеральный закон от 01.04.2025 № 41-ФЗ // принят Государственной Думой 25.03.2025,

одобрен Советом Федерации 27.03.2025 (за исключением положений ст. 1 ФЗ № 41-ФЗ (вступит с 01.03.2026).

28. О внесении изменений в отдельные законодательные акты РФ: федеральный закон РФ от 31.07.2025 № 282-ФЗ// принят Государственной Думой 22.07.2025, одобрен Советом Федерации 22.07.2025.

29. Проблемы противодействия киберпреступности: материалы II Международной научно-практической конференции (Москва, 26 апреля 2024 года) / Под общ. ред. О.Ю. Антонова, Э.Б. Хатова. - М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2024. – 146 с.

30. Проблемы противодействия киберпреступности: материалы III Международной научно-практической конференции (Москва, 4 июня 2025 г.). М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2025. – 279 с.

31. Ройхка А.А. Зарождение киберпреступности и этапы ее последующего генезиса: российский и зарубежный опыт / А.А. Ройхка // Молодой ученый. 2025. № 13 (564). С. 130-131.

32. Сомов Р.Н. Киберпреступность: основные проявления и особенности противодействия / Р. Н. Сомов// Молодой ученый. 2024. № 42 (541). С. 185-187.

33. Сычева Е.А. История развития киберпреступности в России / Е.А. Сычева// Проблемы совершенствования российского законодательства: Сборник тезисов Всероссийской (с международным участием) научной конференции курсантов, слушателей и студентов, Барнаул, 12–13 апреля 2021 года. Барнаул: Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Барнаульский юридический институт Министерства внутренних дел Российской Федерации», 2022. С. 282–283.

34. Статистика киберпреступности по данным МВД России. URL: <https://www.ec-rs.ru/blog/novosti/statistika-kiberprestupnosti-v-rossiyskikh->

regionakh-dannye-mvd-za-2024-god/?ysclid=mkzazhqlux584169377 (дата обращения 27.01.2026).

35. СК РФ. Официальный сайт. URL: <https://tass.ru/obschestvo/24573429?ysclid=mkzh42p83834667093>. (дата обращения 27.01.2026)

36. Степанов Е.А. Пути совершенствования расследования и раскрытия компьютерных преступлений / Е.А. Степанов // Вестник науки. 2025. № 1 (82). С. 454–462.

37. Трофимова А.Ю. История развития уголовного законодательства в части регламентации оснований ответственности за преступления в сфере компьютерной информации / А.Ю. Трофимова// Молодой ученый. 2021. № 53 (395). С. 128-129.

38. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 20.01.2026) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

39. Черенцова Р.С. Проблемы правового регулирования киберпреступности в современной России / Р.С. Черенцова// Актуальные исследования. 2025. №21 (256). ч. III. С. 54–56.

40. Шевко Н.Р., Лукина М.А. Киберпреступность: современное состояние и меры противодействия/ Н.Р. Шевко, М.А. Лукина // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 130–133.

41. Шикула И.Р., Куркин Е.Н. 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.

42. Швыряев П.С. Проблема киберпреступности в России: актуальное состояние и перспективы решения/ П.С. Швыряев // Уровень жизни населения регионов России. 2023. Том 19. № 4. С. 616–629.

43. Шляхтова О.Г. Компьютерные преступления: историко-правовой аспект / О.Г. Шляхтова// Известия Гомельского государственного университета им. Ф. Скорины. 2023. № 2 (137).

44. Шляхтова О.Г. О подходах к пониманию и классификации преступлений в сфере компьютерной безопасности / О.Г. Шляхтова// Молодой ученый. 2024. № 10 (509). С. 240-243.

ПРИЛОЖЕНИЕ 1



Рисунок 1 – Киберпреступления в России (2024)

Источник: составлено автором исследования на основании официальных данных МВД России



Рисунок 2 - Структура и раскрываемость киберпреступлений в России (2023-2026, прогноз)

Источник: составлено автором исследования на основании официальных данных МВД
России



Рисунок 3 - Статистика киберпреступлений, расследованных СК РФ в 2023–2025 гг.
Источник: составлено автором исследования на основании официальных статистических
данных Следственного комитета Российской Федерации за 2023–2025 гг.

ПРИЛОЖЕНИЕ 2

Таблица 1 - Предложения по корректировке нормативной базы в сфере противодействия киберпреступности

Нормативный акт / статья	Предлагаемое изменение	Обоснование
Ст. 272 УК РФ (неправомерный доступ к компьютерной информации)	Уточнить понятие «компьютерная информация», включив в него данные, обрабатываемые и хранимые в облачных сервисах, распределенных системах и на устройствах Интернета вещей (IoT).	Расширение использования облачных технологий и IoT-устройств приводит к появлению новых объектов преступного посягательства, что требует актуализации уголовно-правового определения.
Ст. 273 УК РФ (создание, использование и распространение вредоносных программ)	Дополнить статью новой частью, устанавливающей ответственность за разработку и распространение инструментов, предназначенных для облегчения создания вредоносного программного обеспечения (в том числе фишинговых конструкторов и автоматизированных скриптов).	Криминализация вспомогательных инструментов позволит пресекать киберпреступную деятельность на ранних стадиях и снизить уровень латентной киберпреступности.
Ст. 274.1 УК РФ (неправомерное воздействие на критическую информационную инфраструктуру)	Расширить перечень объектов критической информационной инфраструктуры, включив в него системы здравоохранения, образования и транспорта, а также уточнить критерии их значимости.	Активная цифровизация социально значимых сфер повышает их уязвимость перед киберугрозами и требует усиленной уголовно-правовой защиты.
Ст. 274.3 УК РФ (незаконное использование)	Увеличить размер максимального штрафа за деяния, совершенные группой	Повышение санкций усилит превентивный эффект нормы и повысит риски для

абонентского терминала пропуска трафика)	лиц по предварительному сговору, до 1,5 млн рублей.	организаторов мошеннических схем.
Федеральный закон «О связи»	Установить обязанность операторов связи по автоматической блокировке вызовов с иностранных номеров, не прошедших обязательную верификацию в российской системе нумерации.	Мера направлена на снижение количества трансграничных мошеннических звонков и повышение защищенности абонентов.
Федеральный закон «О персональных данных»	Ввести обязанность операторов персональных данных обеспечивать хранение журналов доступа к персональным данным в течение не менее трех лет.	Хранение логов доступа упростит расследование утечек персональных данных и установление виновных лиц.
ФЗ № 41-ФЗ (ГИС противодействия правонарушениям)	Дополнить функционал системы сведениями о так называемых «дропперах» и связанных с ними банковских счетах с возможностью их оперативной блокировки.	Обеспечит более эффективное противодействие выводу похищенных денежных средств и финансовым аспектам киберпреступности.
Ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации)	Дополнить статью квалифицирующим признаком, предусматривающим повышенную ответственность за совершение мошенничества с использованием технологий искусственного интеллекта.	Рост применения ИИ в преступных схемах требует специального уголовно-правового регулирования.
Ст. 63 УК РФ (обстоятельства, отягчающие наказание)	Включить в перечень отягчающих обстоятельств использование методов социальной инженерии при совершении преступлений.	Признание социальной инженерии отягчающим обстоятельством повысит ответственность за

		манипулятивные способы обмана потерпевших.
--	--	---