

ФЕДИНА Любовь Михайловна,
к.ю.н., преподаватель кафедры информационных
технологий и специальной техники ОВД
Северо-Кавказского института повышения квалификации
(филиал) Краснодарского университета МВД России,
e-mail: mail@law-books.ru

ТАМБИЕВ Сергей Арсенович,
старший преподаватель кафедры информационных
технологий и специальной техники ОВД
Северо-Кавказского института повышения квалификации
(филиал) Краснодарского университета МВД России,
e-mail: mail@law-books.ru

КРАТКАЯ ХАРАКТЕРИСТИКА И ТЕНДЕНЦИИ РАЗВИТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В РОССИИ

Аннотация. Настоящее исследование посвящено развитию информационных технологий в России, и способам их незаконного использования злоумышленниками. Авторами раскрываются приоритетные направления инновационных решений и цифровой инфраструктуры, а также выделяются их уязвимые места для возможных кибератак. Кроме того, даётся краткая характеристика состава преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Для масштабного понимания проблематики приводятся статистические данные о киберпреступлениях, совершенных в Российской Федерации за последние пять лет, на основании которых авторы спрогнозировали тенденции развития криминогенной обстановки в ближайшее время.

Ключевые слова: киберпреступления, информационные технологии, искусственный интеллект, фишинг, кибербезопасность, кибератаки, цифровизация.

FEDINA Lyubov Mikhailovna,
candidate of Law associate professor
of special and technical training department
of the North-Caucasian Advanced Training Institute
(branch) of the Krasnodar University
of the Ministry of Internal Affairs of Russia

TAMBIEV Sergey Arsenovich,
Senior Lecturer at the Department
of Information Technologies and Special Equipment
of the North Caucasus Advanced Training Institute
(branch) of the Krasnodar University
of the Ministry of Internal Affairs of Russia

A BRIEF DESCRIPTION AND TRENDS IN THE DEVELOPMENT OF CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES IN RUSSIA

Annotation. *This study focuses on the development of information technology in Russia and the ways in which it is illegally used by malicious actors. The authors explore the priority areas of innovative solutions and digital infrastructure, as well as their vulnerabilities to potential cyberattacks. Additionally, they provide a brief overview of the types of crimes committed using information and telecommunication technologies or in the field of computer information. To gain a comprehensive understanding of the issue, the study presents statistical data on cybercrimes committed in the Russian Federation over the past five years, which are used to predict future trends in the criminal environment.*

Key words: *cybercrimes, information technology, artificial intelligence, phishing, cybersecurity, cyberattacks, and digitalization.*

Информационно-телекоммуникационные технологии (далее – ИКТ) на сегодняшний день играют ключевую роль в социально-экономическом развитии России, обеспечивая инновационные решения и повышение эффективности во всех сферах жизнедеятельности. Для оценки масштабов данного повсеместного внедрения ИКТ, выделим следующие основные направления развития, характерные для нашей страны:

Прежде всего, это цифровая экономика, которая является приоритетным направлением стратегии развития России. Ключевые цели включают создание современной цифровой инфраструктуры, развитие инновационных решений и обеспечение доступности цифровых услуг населению.

Кроме того, так называемый «интернет вещей» (далее – IoT) позволяет объединить устройства в единую систему управления, способствуя автоматизации процессов в промышленности, транспорте, здравоохранении и быту. Различные технические принадлежности и устройства «умного дома» с каждым днем всё плотнее входят в жизнь рядовых граждан, при этом представляя собой латентную угрозу перехвата, прослушки и иных способов утечки информации.

Развитие «Электронного правительства» и внедрение искусственного интеллекта (далее – ИИ) стало одним из приоритетных направлений перспектив информационных технологий в России. Комплекс государственных услуг и сервисов, предоставляемых гражданам и бизнесу в электронном виде, повышают прозрачность административных процедур, улучшают качество обслуживания населения, снижают уровень коррупции.

Основными видами преступлений в сфере компьютерной информации являются:

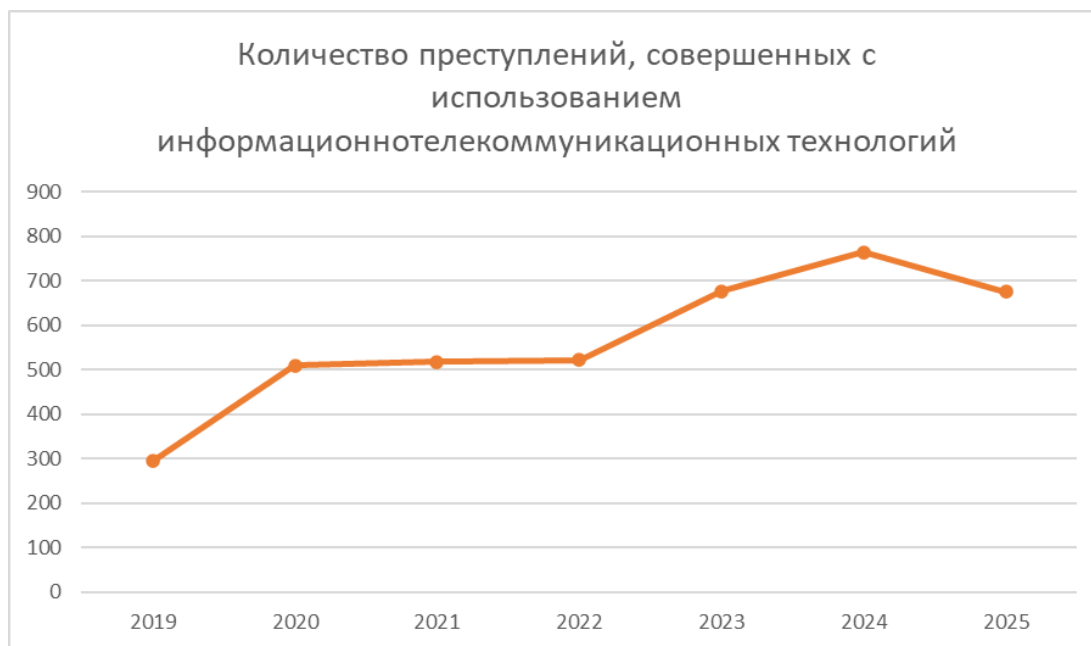
1. Неправомерный доступ к охраняемой законом компьютерной информации (статья 272 УК РФ), то есть преступления, предполагающие несанкционированный доступ к данным, хранящимся на компьютерах, серверах или иных устройствах обработки инфор-

мации. Преступление считается тяжким, если оно совершено группой лиц по предварительному сговору либо лицом с использованием своего служебного положения. Например, взлом корпоративной базы данных с целью хищения персональных сведений сотрудников.

2. Создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ). Этот состав включает разработку программного обеспечения, предназначенного для нарушения нормального функционирования компьютеров, серверов или сетей. Такие программы часто используются для кражи данных, вымогательства или саботажа инфраструктуры. В качестве примера можно указать разработку вируса-шифровальщика, который блокирует работу организации до выплаты выкупа.
3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274 УК РФ). Данный состав охватывает случаи умышленного или халатного несоблюдения установленных норм защиты информации, повлекших утрату важных данных или нарушение работоспособности системы. Иллюстрацией данного состава можно обозначить игнорирование требований безопасности, приведшее к заражению вирусом корпоративной сети предприятия.

Важно помнить, что использование любых инструментов для несанкционированного доступа к данным или нарушения конфиденциальности является незаконным и влечет ответственность согласно законодательству большинства стран, включая Россию.

Переходя к рассмотрению отдельных видов преступных деяний, совершенных с использованием ИКТ нельзя не отметить их ошеломляющие тенденции роста в нашей стране в период с 2020 по 2024 годы. В количественном выражении это выглядит следующим образом:



Приведенные данные представляются более значительными в спектре всероссийской криминальной обстановки, поскольку их удельный вес в общем числе зарегистрированных преступлений к концу декабря 2025 года составил 38,1%. При этом четыре из пяти подобных деяний (84,8%) совершаются с использованием сети «Интернет» и больше половины (52,2%) относится к категориям тяжких и особо тяжких [3].

Причина подобного значительного роста киберпреступности именно с 2020 года очевидна, поскольку наступившая пандемия, изоляционные меры трансформировали общественные отношения в другую плоскость и противоправные деяния перешли в сторону глобальной цифровизации.

Продолжая анализировать общую динамику российской киберпреступности в 2025 году, необходимо отметить снижение показателей как в целом зарегистрированных преступлений (-11,8%), так и по отдельным направлениям, например: дистанционные кражи сокращены на 23,6%, дистанционное мошенничество уменьшилось на 9%, преступления в области компьютерных данных сократились на 42,2%, что свидетельствует о положительных результатах усилий правоохранительных органов и регуляторов в области информационной безопасности.

Также среди причин сокращения случаев кибермошенничества можно выделить принятие законодательных инициатив, включая концепцию государственной системы противодействия преступлениям в ИКТ-сфере [4], формирование специальных подразделений и служб мониторинга, направленных на выявление и пресечение нарушений, повышение осведомленности среди

граждан о рисках и методах предотвращения преступлений и развитие технологических решений для обнаружения и блокировки попыток хищения средств.

Однако, здесь необходимо отметить один принципиально важный нюанс, заключающийся в том, что официальная статистика отражает только зарегистрированные и подтвержденные случаи киберпреступлений, а, следовательно, реальные цифры могут быть значительно выше. Прежде всего многие компании предпочитают не сообщать о нарушениях, чтобы сохранить репутацию, да и среди граждан отмечается высокая латентность данных противоправных деяний и их последствий, нежелание обращаться в правоохранительные органы. Кроме того, информация о некоторых инцидентах поступает значительно позже фактического времени кибератаки, что искажает текущую картину.

В связи с этим, представляется необходимым проанализировать текущую ситуацию по направлениям преступного воздействия, и тенденции их возможного роста в наступившем году.

Но всё же, основное внимание злоумышленников сосредоточено на сферах, обеспечивающих наибольшую финансовую выгоду или политический эффект. Государственные учреждения, финансовая сфера, промышленные объекты, телекоммуникации и энергетика остаются самыми привлекательными мишенями. Специализированные атаки типа шифровальщиков и вайперов ведут к значительным экономическим и репутационным убыткам.

При этом, нельзя исключать и человеческий фактор, который остается одним из важнейших составляющих успешных атак. Многие инциденты

начинаются с элементарных ошибок сотрудников, которые переходят по сомнительным ссылкам, открывают подозрительные файлы или раскрывают важную информацию. Недостаточное информирование и отсутствие регулярных тренировок приводят к существенному увеличению числа успешных атак. Растущая сложность цифровых экосистем и зависимость от технологий только повышают риски человеческого фактора. Сотрудники становятся основным каналом проникновения в корпоративные сети, и необходимость укрепления образовательных программ возрастает.

При этом, цифровая среда стремительно развивается, охватывая всё большее количество устройств и сервисов. Это создает новую поверхность для атак. Особенно опасно то, что многие устройства IoT (интернет вещей) выпускаются с низкой степенью защиты, становясь удобной отправной точкой для злоумышленников.

Логичным представляется то, что преступная среда увеличивает интенсивность атак с целью получения финансовых выгод. Тенденция вымогательства и шантажа усиливается, причем злоумышленники адаптируются к новым условиям, используя не только традиционные схемы шифрования, но и более тонкие способы влияния на бизнес-процессы и репутацию компаний.

Учитывая вышесказанное, можно спрогнозировать рост киберпреступности в России в ближайшее время, что обусловлено комбинацией факторов: развитием технологий, увеличением числа потенциальных объектов атаки, ухудшением качества цифровой гигиены и отсутствием должного уровня осведомленности сотрудников. Перед бизнесом и государственными структурами встает острая необходимость адаптироваться к новым угрозам, наращивая усилия по обучению персонала, улучшению внутренней культуры безопасности и применению новейших технологий защиты. Реакция должна быть быстрой и эффективной, чтобы предотвратить серьезные последствия для экономики и безопасности страны.

Список литературы:

- [1] Рухлова М. А. Криминологические и уголовно-правовые меры борьбы с преступлениями в сфере компьютерной информации // Вестник науки. 2025. №6 (87). С.589-598
- [2] Уголовный кодекс Российской Федерации: федеральный закон текст с изменениями и дополнениями на 29.12.2025 № 63-ФЗ [принят Государственной думой 13 июня 1996 г. (в ред. от 20.01.2026)] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) (дата обращения: 01.02.2026)
- [3] Характеристика состояния преступности в Российской Федерации за январь – декабрь

2025-2019 годов // МВД России: офиц. сайт. URL: <https://мвд.рф/reports/item>(дата обращения: 01.02.2026)

[4] Распоряжение Правительства Российской Федерации от 30 декабря 2024 г. №4154-р «Об утверждении Концепции государственной системы противодействия противоправным действиям, совершаемым с использованием информационно-коммуникационных технологий» // Официальный интернет-портал правовой информации (www.pravo.gov.ru) (дата обращения: 01.02.2026)

[5] Кочесок Р.Х. Киберпреступность в России: тенденции и методы борьбы // Пробелы в российском законодательстве. 2023. №5. с/242-246

[6] Сыч Д.А., Аминов И.Р. Криминологическая характеристика киберпреступности // Международный журнал гуманитарных и естественных наук. 2024. №11-3 (98). С.162-164

[7] Шевко Н. Р., Лукина М. А. Киберпреступность: современное состояние и меры противодействия // Правопорядок: история, теория, практика. 2024. №2 (41). с.130-133

References:

- [1] Rukhlova M. A. Criminological and criminal legal measures to combat crimes in the field of computer information//Bulletin of Science. 2025. №6 (87). P.589-598
- [2] Criminal Code of the Russian Federation: federal law text with amendments and additions to 29.12.2025 No. 63-FZ [adopted by the State Duma on June 13, 1996 (as amended by 20.01.2026)] // Official Internet portal of legal information (www.pravo.gov.ru) (date of appeal: 01.02.2026)
- [3] Characteristics of the state of crime in the Russian Federation for January - December 2025-2019//Ministry of Internal Affairs of Russia: Office. site. URL: <https://мвд.рф/reports/item> (accessed on: 01.02.2026)
- [4] Order of the Government of the Russian Federation of December 30, 2024 No. 4154-r "On approval of the Concept of the state system for countering illegal acts committed using information and communication technologies" //Official Internet portal of legal information (www.pravo.gov.ru) (date of appeal: 01.02.2026)
- [5] Kochesokov R.H. Cybercrime in Russia: trends and methods of struggle//Gaps in Russian legislation. 2023. №5. с/242-246
- [6] Sych D.A., Aminov I.R. Criminological characterization of cybercrime//International Journal of Humanities and Natural Sciences. 2024. №11-3 (98). С.162-164
- [7] Shevko N.R., Lukina M.A. Cybercrime: the current state and countermeasures//Law and order: history, theory, practice. 2024. №2 (41). p.130-133.