Гурулева Анжелика Андреевна
преподаватель
Никифорова Ярослава Олеговна
студентка
Красноярский филиал ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Красноярск, Красноярский край

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ПРОГРЕССИРУЮЩИХ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация: *статья посвящена вопросу анализа современного состояния киберпреступности в Российской Федерации, характеризующегося устойчивым ростом информационных атак (в среднем 20% ежегодно), активным использованием технологий искусственного интеллекта злоумышленниками, а также участившимися случаями утечек данных и действий программ-вымогателей. В работе рассматриваются основные виды киберугроз, включая фишинговые и DDoS-атаки, вирусы-шифровальщики, а также новые вызовы, связанные с применением дипфейков. Особое внимание уделяется факторам роста киберпреступности, среди которых выделяются доступность технологий, недостаточная осведомленность населения и отставание законодательной базы от темпов развития угроз. В статье анализируются меры противодействия киберпреступности, включая законодательные инициативы (Федеральный закон №187-ФЗ), технические средства защиты, образовательные программы для пользователей и механизмы международного сотрудничества правоохранительных органов. Делается вывод о необходимости комплексного подхода к обеспечению цифровой безопасности, объединяющего усилия государства, бизнеса и гражданского общества.*

Ключевые слова: *киберпреступность, информационная безопасность, фишинг, DDoS-атаки, программы-вымогатели, искусственный интеллект, дипфейки, защита персональных данных, цифровая грамотность, противодействие киберугрозам.*

На сегодняшний день на территории Российской Федерации информационные атаки характеризуются резким ростом, в среднем около 20% ежегодно по данным официальной статистики, смещением фокуса на использование искусственного интеллекта (ИИ) для атак, масштабными утечками данных и действиями программ-вымогателей.

Развитие цифровых технологий значительно расширило возможности взаимодействия между людьми и организациями, однако вместе с этим возросли риски киберугроз. Киберпреступления стали серьезной проблемой для многих стран мира, включая Россию.

По данным статистики, количество случаев мошенничества в сфере высоких технологий постоянно растет, ставя перед правоохранительными органами новые задачи и вызовы.

Основные виды киберпреступлений.

Фишинговые атаки.

Фишинг является одним из наиболее распространенных видов кибератак. Преступники создают поддельные веб-сайты, имитирующие известные бренды и организации, чтобы обмануть пользователей и заставить их раскрыть конфиденциальную информацию, такую как пароли, номера кредитных карт и личные данные. Особенно уязвимы становятся пожилые граждане, менее знакомые с современными технологиями.

Пример. В Москве зафиксирован случай, когда злоумышленники рассылали письма якобы от Сбербанка, предлагая обновить учетные записи клиентов. Получив доступ к персональным данным, преступники похитили крупную сумму денег с банковских счетов жертвы.

Атаки типа DDoS.

DDoS-атаки представляют собой целенаправленные попытки перегрузить серверы путем отправки большого количества запросов одновременно, вызывая отказ системы. Такие атаки часто используются против государственных учреждений, крупных компаний и финансовых организаций, что приводит к значительным финансовым потерям и нарушению нормальной работы сервисов.

Пример: Один из банков федерального уровня подвергся мощному DDoS-нападению, которое привело к временной остановке обслуживания онлайн-клиентов на несколько часов.

Вирусы-шифровальщики.

Злоумышленники активно используют вредоносное ПО для кражи информации и вымогательства. Например, троянские программы позволяют удаленно контролировать зараженные устройства, собирая ценную информацию и передавая её третьим лицам. Шифровальщики же шифруют файлы на компьютере жертвы, запрашивая выкуп за восстановление доступа.

Пример: Российский университет столкнулся с атакой вируса-шифровальщика, заблокировавшего всю систему электронной документации и учебных материалов. Администрация вынуждена была заплатить значительный штраф, чтобы вернуть контроль над файлами.

Причины роста киберпреступности.

Рост числа киберпреступлений обусловлен несколькими факторами:

Облегчение доступа к технологиям: Современные инструменты и технологии сделали создание сложных схем мошенничества доступным даже для новичков.

Недостаточная осведомленность населения: многие россияне недостаточно информированы о методах защиты личной информации и легко попадают в ловушки преступников.

Отсутствие строгого контроля: несмотря на усилия правоохранительных органов, законодательная база и меры профилактики пока отстают от темпов развития угроз.

Развитие нейросетей на территории России серьезно повлияло на развитие IT-отрасли, например, на осуществление анализа информации или ее поиск и создание текстов, что делает атаки с использованием ИИ более целенаправленными и масштабируемыми.

Кроме того, мошенники используют искусственный интеллект для генерации дипфейков. Согласно данным Центрального банка Российской Федерации с января по сентябрь 2024 года число правонарушений, в которых задействована система «deepfake», увеличилось в 30 раз.

Одним из способов противодействия утечкам данных является формирование четкой государственной политики в сфере кибербезопасности, включающей разработку нормативных актов, направленных на защиту данных и инфраструктуры.

Государство предлагает применение методов защиты персональных данных и предотвращения киберпреступлений.

Цифровая безопасность в эпоху прогрессирующих киберпреступлений требует непрерывного и сложного подхода. Приоритизация критичных активов, быстрое обнаружение и отработка инцидентов, а также постоянное обучение персонала – ключевые элементы устойчивости к современным угрозам.

Борьба с киберпреступностью включает комплекс мер, направленных на предотвращение, выявление и пресечение преступлений, совершаемых с использованием компьютерных технологий и сети Интернет. Основные направления борьбы включают:

Законодательные меры.

Разработка и принятие законов, регулирующих использование киберпространства и устанавливающих ответственность за совершение киберпреступлений. Например, в России действует Федеральный закон №187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств».

Технические средства защиты.

Использование антивирусных программ, межсетевых экранов, систем обнаружения вторжений и шифрования данных для предотвращения несанкционированного доступа и кражи информации.

Обучение пользователей.

Проведение образовательных кампаний и тренингов для повышения осведомленности пользователей о методах кибератак и способах защиты от них. Это помогает снизить риск стать жертвой мошенничества или фишинга.

Сотрудничество правоохранительных органов.

Создание специализированных подразделений, занимающихся расследованием киберпреступлений. Международное сотрудничество также играет важную роль, поскольку многие преступления совершаются трансгранично.

Проблема киберпреступности требует комплексного подхода. Необходимо повысить уровень цифровой грамотности среди населения, усилить профилактику и мониторинг рисков, совершенствовать законодательство и внедрять современные методы защиты данных. Только совместными усилиями государства, бизнеса и гражданского общества возможно эффективно противостоять новым вызовам в области информационной безопасности.

Список литературы

1. Журнал РБК: сайт. – URL: https://www.rbc.ru/ (дата обращения: 10.02.2026).

2. Информационный портал Банки.ру: сайт. – URL: https://www.banki.ru/ (дата обращения: 12.02.2026).

3. Портал актуальных новостей и аналитики – Рамблер/финансы: сайт. – URL: https://finance.rambler.ru/ (дата обращения: 11.02.2026).