Секция «10.5 Компьютерное право и информационная безопасность»

Реализация положений Конвенции ООН против киберпреступности в законодательстве Российской Федерации как фактор обеспечения финансовой безопасности

Научный руководитель – Морозов Андрей Витальевич

Наумов Иван Иванович

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия

E-mail: god.real.god@mail.ru

Актуальность темы. В современном мире интернет проник во все сферы жизни, что привело к резкому росту числа кибернетических преступлений. Преступники совершенствуют тактики, используя сложные IT-технологии, требующие специальных знаний. Бурное развитие информационных технологий ускорило обмен информацией, но послужило причиной возникновения нового типа криминальной активности. Проблема приобрела глобальный характер, а финансовые потери достигают сотен миллиардов долларов. Противодействие киберпреступности является критически важным элементом для обеспечения финансовой стабильности России, так как хищение средств и атаки на финансовые институты наносят прямой вред экономике и ослабляют доверие к финансовой системе [3].

Цель работы — анализ реализации положений Конвенции ООН против киберпреступности в законодательстве РФ в контексте обеспечения финансовой безопасности.

Международно-правовое регулирование. В целях борьбы с негативной тенденцией 24 декабря 2024 года Генеральной Ассамблеей ООН была принята Конвенция ООН по противодействию киберпреступности. Документ, предложенный Российской Федерацией, призван укрепить международное сотрудничество и обеспечить защиту общества от опасностей в цифровой среде [5]. Конвенция охватывает широкий спектр незаконных действий: несанкционированный доступ к информационным системам, перехват данных, нанесение ущерба информации, нарушение работы ИКТ, неправомерное использование устройств, подделку документов и мошенничество. Особое внимание уделяется противодействию детской порнографии и легализации доходов. Конвенция вступит в силу после ратификации 40 государствами. Правительство России планирует завершить внутренние процедуры присоединения к концу 2027 года.

Статистика и угрозы. Согласно данным ежегодного анализа Центробанка России, в 2024 году 9% опрошенных стали жертвами финансовых афер, а с различными видами мошенничества столкнулись 30% респондентов. Телефонное мошенничество и СМС-рассылки остаются наиболее распространенными. Впервые в число лидеров вошло завладение аккаунтами на портале Госуслуг [6]. Угроза имеет множество аспектов: рост преступлений внутри страны и вовлечение российских хакеров в международные кибератаки. Высокая общественная опасность связана с транснациональным характером: преступник, жертва и объект атаки могут находиться в разных странах [1].

Законодательные и организационные меры. Эффективное противодействие требует комплексного подхода и модернизации правовой базы. Правительство Российской Федерации одобрило план реализации Концепции государственной политики в области борьбы с преступлениями в сфере ИКТ [2]. Ключевыми направлениями являются:

1. Совершенствование законодательства.
2. Усиление профилактических мер.

3. Реализация организационно-технических мер.
4. Обеспечение правоохранительных структур кадрами.
5. Расширение международного сотрудничества.
6. Развитие научно-исследовательской базы.

В рамках реализации Конвенции правоохранительные органы получат полномочия запрашивать у операторов связи и провайдеров сведения о подозрительных действиях. Координировать взаимодействие будут МВД, Минцифры, ФСБ и Роскомнадзор. Для гарантии безопасности граждан вступил в силу закон, устанавливающий уголовную ответственность для владельцев банковских карт, передающих их мошенникам [4].

Технологические решения. Важная роль отводится технологическим средствам защиты. Планируется формирование базы фишинговых ресурсов, создание алгоритмов обнаружения преступлений и внедрение надежных методов шифрования. К концу сентября 2026 года планируется создание единого реестра официальных веб-сайтов крупных интернет-магазинов. Особое значение придается искусственному интеллекту: к марту 2028 года будет разработан алгоритм для выявления случаев применения нейросетей в киберпреступных целях. Информация об угрозах будет интегрирована в мобильные приложения госорганов и банков.

Проблемы международного сотрудничества. Вероятным препятствием станет нынешний политический климат. Эффективность Конвенции обусловлена уровнем доверия между государствами. Примером сложностей служит уголовное преследование лиц, связанных с группировкой REvil, задержанных в 2022 году на основе данных США. Сложности возникли из-за того, что Минюст США не ответил на запросы РФ о правовой помощи. Проблема заключается в напряженных отношениях между Россией и западными державами. Проект соглашения предусматривает основания для отклонения запросов. Тем не менее, практические мотивы могут подтолкнуть государства к сотрудничеству даже в условиях конфронтации.

Заключение. Реализация положений Конвенции ООН против киберпреступности в законодательстве РФ является значимым фактором обеспечения финансовой безопасности. Успешная борьба с киберпреступностью укрепляет устойчивость финансовой системы, оберегает интересы граждан и предприятий, формирует условия для прогресса цифровой экономики. Необходима дальнейшая модернизация правовой базы, наращивание кадровых ресурсов и развитие технологий защиты с учетом организованного и международного характера угроз.

Источники и литература

1) Батюкова В. Е. Состояние киберпреступности в банковской сфере / В.Е. Батюкова // Государственная служба и кадры. 2021. № 3. — URL: https://cyberleninka.ru/article/n/sostoyanie-kiberprestupnosti-v-bankovskoy-sfere (дата обращения: 21.09.2025).

2) Распоряжение Правительства РФ от 14.08.2025 N 2207-р «Об утверждении Плана мероприятий по реализации Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» // https://www.consultant.ru/document/cons_doc_LAW_512576 (дата обращения: 21.09.2025).

3) Тарханова Е.А. Кибермошенничество как ключевая угроза процесса цифровизации банковской деятельности / Е А. Тарханова, А.В. Фрицлер // Экономическая безопасность страны, регионов, организаций различных видов деятельности. Тюмень,: ТюмГУ-Press, 2022— 303 с.

4) Федеральный закон от 24.06.2025 N 176-ФЗ "О внесении изменений в статью 187 Уголовного кодекса Российской Федерации" // https://www.consultant.ru/document/cons_doc_LAW_508353 (дата обращения: 21.09.2025).
5) Конвенция ООН против киберпреступности // https://www.un.org/ru/documents/treaty/A-RES-79-243 (дата обращения: 21.09.2025).
6) Центральный банк России. Киберпортрет 2024 // https://cbr.ru/statistics/information_security/cyber_portrait/2024 (дата обращения: 21.09.2025).