ПРАВОВОЕ РЕГУЛИРОВАНИЕ БОРЬБЫ С КИБЕРПРЕСТУПЛЕНИЯМИ В СФЕРЕ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ УЗБЕКИСТАН И МЕЖДУНАРОДНОГО ОПЫТА

Еркинбаева Нуржахан Полатовна
Ташкентский Государственный Юридический Университет
nurjakhanerkinbaeva@gmail.com

Аннотация

В данной статье проводится комплексный анализ правового регулирования борьбы с киберпреступлениями в сфере электронных платежных систем в Республике Узбекистан в сравнении с международной практикой. Рассматриваются актуальные проблемы уголовно-правовой квалификации и расследования преступлений, связанных с незаконными операциями в платежных системах, включая фишинг, скимминг, компьютерное мошенничество и атаки на банковскую инфраструктуру. Автор анализирует действующее законодательство Узбекистана, выявляет его сильные стороны и существующие пробелы в сфере защиты электронных платежей от киберугроз. Особое внимание уделяется проблемам транснационального характера данных преступлений, что обуславливает необходимость международного сотрудничества правоохранительных органов. На основе анализа передового зарубежного опыта и рекомендаций международных организаций предлагаются конкретные направления совершенствования национального законодательства и правоприменительной практики. Исследование представляет интерес для юристов, специалистов правоохранительных органов и сотрудников служб безопасности финансовых учреждений.

Ключевые слова: киберпреступность, электронные платежные системы, информационная безопасность, компьютерное мошенничество, фишинг, скимминг, международное сотрудничество, уголовное законодательство, финансовая безопасность, платежные карты, электронные деньги.

1. Введение

Стремительное развитие информационно-коммуникационных технологий и цифровизация экономики привели к значительному росту электронных платежных

систем во всем мире, включая Республику Узбекистан. Появление разнообразных форм электронных платежей – от банковских карт до мобильных приложений и цифровых кошельков – существенно изменило финансовый ландшафт, сделав денежные операции более доступными, быстрыми и

удобными для населения и бизнеса. По данным Центрального банка Республики Узбекистан, за последние пять лет объем электронных платежей в стране увеличился более чем в десять раз, что свидетельствует о масштабной трансформации платежного поведения граждан.

Однако вместе с развитием электронных платежных систем неизбежно возникают и новые угрозы безопасности, связанные с киберпреступлениями. Хищения денежных средств со счетов граждан и организаций, фишинговые атаки, скимминг, компрометация данных платежных карт, атаки на банковскую инфраструктуру – все эти преступления приобретают новые формы и характеристики в цифровую эпоху. По мировой статистике, ежегодные потери от киберпреступлений в финансовой сфере превышают 1 триллион долларов США, и эта цифра продолжает расти.

Особую сложность для правовой системы представляет транснациональный характер киберпреступлений в сфере электронных платежей. Преступник, находящийся в одной стране, может без труда атаковать финансовые системы и похищать средства пользователей в другой стране, что создает серьезные проблемы юрисдикции, расследования и международного сотрудничества правоохранительных органов.

В Республике Узбекистан в последние годы предприняты значительные шаги по совершенствованию законодательства в сфере информационной безопасности и противодействия киберпреступности. Принят ряд нормативно-правовых актов, направленных на регулирование электронных платежных систем и обеспечение их безопасности. В частности, внесены изменения в Уголовный кодекс, предусматривающие ответственность за различные формы компьютерных преступлений, включая неправомерный доступ к компьютерной информации и мошенничество с использованием электронных средств платежа.[1]

Тем не менее, динамичное развитие информационных технологий и появление новых форм киберпреступлений требуют постоянного совершенствования правовой базы и правоприменительной практики. В этом контексте особую ценность представляет изучение международного опыта правового регулирования борьбы с киберпреступлениями в сфере электронных платежных систем.

Целью настоящего исследования является комплексный анализ правового регулирования борьбы с киберпреступлениями в сфере электронных платежных систем в Республике Узбекистан в сравнении с международной практикой, выявление существующих проблем и определение перспективных направлений совершенствования законодательства и правоприменительной деятельности.

Для достижения поставленной цели необходимо решить следующие задачи:

исследовать современное состояние электронных платежных систем в Узбекистане и нормативно-правовую базу их регулирования;

проанализировать типологию киберпреступлений в сфере электронных платежных систем;

изучить особенности уголовно-правовой квалификации и расследования данных преступлений в Узбекистане;

рассмотреть международный опыт правового регулирования и практики противодействия киберпреступлениям в платежной сфере;

определить проблемы и перспективы совершенствования законодательства Республики Узбекистан в данной области.

2. Методы

Методологическую основу исследования составляют общенаучные методы познания (анализ, синтез, индукция, дедукция), а также специальные юридические методы (формально-юридический, сравнительно-правовой, системный анализ нормативно-правовых актов).

В исследовании использованы следующие методы сбора и анализа информации:

Нормативно-правовой анализ - изучение законодательных актов Республики Узбекистан, регламентирующих функционирование электронных платежных систем и борьбу с киберпреступлениями, включая:

Уголовный кодекс Республики Узбекистан;

Закон Республики Узбекистан «О платежах и платежных системах»;

Закон Республики Узбекистан «Об электронной коммерции»; Закон Республики Узбекистан «Об информатизации»;

Подзаконные нормативные акты в данной сфере.

Сравнительно-правовой метод - изучение и сопоставление законодательства и практики противодействия киберпреступлениям в сфере электронных платежей в различных странах (США, ЕС, Сингапур, Южная Корея, Российская Федерация) и международных правовых актов:

Конвенция Совета Европы о киберпреступности (Будапештская конвенция); Директивы ЕС в области информационной безопасности;

Рекомендации ФАТФ по противодействию отмыванию денег с использованием виртуальных активов.

Статистический метод - анализ официальных статистических данных о состоянии киберпреступности в финансовой сфере, полученных от:

Министерства внутренних дел Республики Узбекистан; Центрального банка Республики Узбекистан;

Международных организаций (ООН, Интерпол).

Метод экспертного опроса - проведение интервью с 25 экспертами в области информационной безопасности и правоохранительной деятельности, включая:

Сотрудников специализированных подразделений МВД по борьбе с киберпреступностью;

Специалистов служб безопасности коммерческих банков; Независимых экспертов в области кибербезопасности.

Метод кейс-анализа - изучение и анализ 50 уголовных дел о киберпреступлениях в сфере электронных платежных систем, рассмотренных судами Республики Узбекистан в период 2020-2024 гг.

Научная новизна исследования заключается в комплексном анализе правового регулирования борьбы с киберпреступлениями в сфере электронных платежных систем в Узбекистане с учетом последних изменений законодательства и тенденций развития информационных технологий, а также в разработке конкретных предложений по совершенствованию нормативно-правовой базы на основе передового международного опыта.

Практическая значимость исследования определяется возможностью использования его результатов в законотворческой деятельности, правоприменительной практике, а также в образовательном процессе при подготовке специалистов в области информационного права и кибербезопасности.

3. Результаты

Анализ современного состояния электронных платежных систем в Республике Узбекистан показал значительный рост их использования за последние годы. По данным Центрального банка Республики Узбекистан, количество банковских карт в обращении превысило 25 миллионов единиц к началу 2025 года, а объем транзакций через мобильные платежные приложения увеличился на 78% по сравнению с предыдущим годом.

Исследование типологии киберпреступлений в сфере электронных платежных систем позволило выделить следующие наиболее распространенные виды противоправных деяний на территории Узбекистана:

Фишинговые атаки, направленные на получение конфиденциальных данных пользователей (логины, пароли, данные банковских карт) путем создания поддельных сайтов финансовых учреждений и рассылки мошеннических сообщений. Согласно статистике Министерства внутренних дел, в 2024 году зарегистрировано более 3000 случаев фишинга.

Скимминг – установка на банкоматы специальных устройств для считывания данных платежных карт. За последние два года выявлено 127 случаев установки скимминговых устройств, что привело к хищению средств с

более чем 1500 банковских карт граждан.

Компьютерное мошенничество, включающее несанкционированный доступ к электронным кошелькам и банковским аккаунтам пользователей. В 2024 году зарегистрировано 2145 случаев такого мошенничества.

DDoS-атаки на инфраструктуру банков и платежных систем с целью нарушения их работы и последующего хищения средств или вымогательства. За отчетный период зафиксировано 78 крупных атак на финансовые учреждения страны.

Анализ нормативно-правовой базы Республики Узбекистан показал, что основными законодательными актами, регулирующими вопросы борьбы с киберпреступлениями в сфере электронных платежных систем, являются:

Уголовный кодекс Республики Узбекистан, в частности статьи 168 (Мошенничество), 278-1 (Неправомерный доступ к компьютерной информации), 278-2 (Создание, использование или распространение вредоносных программ), 278-3 (Нарушение правил эксплуатации компьютерной системы);

Закон Республики Узбекистан «О платежах и платежных системах» от 1 ноября 2019 года;[2]

Закон Республики Узбекистан «Об электронной коммерции» от 22 мая 2015 года (в редакции от 2023 года);[3]

Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 года (с последующими изменениями);[4]

Постановление Кабинета Министров Республики Узбекистан «О мерах по совершенствованию системы информационной безопасности в сфере электронных платежей» от 17 марта 2023 года.[5]

Сравнительный анализ законодательства Республики Узбекистан с международными правовыми актами и законодательством передовых стран выявил как положительные стороны, так и определенные пробелы. К положительным аспектам можно отнести:

Принятие специализированного законодательства в сфере информационной безопасности и электронных платежей;

Внесение в Уголовный кодекс специальных составов преступлений, связанных с неправомерным использованием компьютерной информации;

Создание специализированных подразделений по борьбе с киберпреступностью в структуре правоохранительных органов.

Однако выявлен ряд проблемных аспектов:

Недостаточная детализация составов киберпреступлений в Уголовном кодексе, что затрудняет квалификацию новых форм противоправных деяний;

Отсутствие четких механизмов международного сотрудничества по расследованию трансграничных киберпреступлений;

Недостаточная регламентация ответственности финансовых учреждений за несоблюдение требований информационной безопасности;

Отсутствие специализированных процессуальных норм, регламентирующих особенности сбора и оценки электронных доказательств по делам о киберпреступлениях.

Исследование международного опыта показало, что наиболее эффективные правовые механизмы борьбы с киберпреступлениями в сфере электронных платежных систем сформированы в странах Европейского Союза, США, Сингапуре и Южной Корее. Анализ законодательства этих стран позволил выделить следующие передовые практики:

Детальная криминализация всех форм киберпреступлений в финансовой сфере с учетом их технологической специфики;

Установление повышенной ответственности за киберпреступления, повлекшие значительный материальный ущерб или нарушение работы критической инфраструктуры;

Наличие эффективных механизмов международного сотрудничества, включая совместные следственные группы и упрощенные процедуры обмена информацией;

Обязательное внедрение финансовыми учреждениями многоуровневых систем защиты и строгой аутентификации пользователей;

Создание национальных центров кибербезопасности с функциями оперативного реагирования на инциденты в финансовом секторе.

4. Обсуждение

Результаты проведенного исследования свидетельствуют о том, что правовое регулирование борьбы с киберпреступлениями в сфере электронных платежных систем в Республике Узбекистан находится в стадии активного развития, но при этом существует ряд проблем, требующих законодательного решения.

I. Проблемы уголовно-правовой квалификации киберпреступлений.

Одной из ключевых проблем является несовершенство уголовно-правовых норм, регламентирующих ответственность за киберпреступления в финансовой сфере. В отличие от законодательства развитых стран, в Уголовном кодексе Республики Узбекистан отсутствуют специальные составы преступлений,

охватывающие все современные формы посягательств на электронные платежные системы. Так, фишинговые атаки часто квалифицируются по общей статье о мошенничестве (ст. 168 УК), что не позволяет учесть специфику данного деяния и назначить адекватное наказание.

Эксперты, участвовавшие в опросе, отмечают необходимость введения в УК

специальных норм об ответственности за фишинг, кардинг (использование данных платежных карт без согласия владельца), а также за атаки на инфраструктуру электронных платежных систем. Примером эффективного подхода может служить законодательство США, где действует Computer Fraud and Abuse Act, предусматривающий ответственность за широкий спектр киберпреступлений, включая мошенничество с использованием компьютерных технологий и неправомерный доступ к защищенным компьютерным системам финансовых учреждений.[8]

II. Транснациональный характер киберпреступлений и проблемы юрисдикции.

Анализ судебной практики показывает, что значительная часть киберпреступлений в финансовой сфере совершается лицами, находящимися за пределами Узбекистана. Это создает серьезные проблемы юрисдикции и международного сотрудничества в расследовании таких дел.

В ходе исследования выявлено, что Узбекистан не является участником Будапештской конвенции о киберпреступности, что ограничивает возможности взаимодействия с правоохранительными органами других стран. Опыт стран-участниц Конвенции демонстрирует высокую эффективность механизмов международного сотрудничества, предусмотренных этим документом, включая процедуры сохранения компьютерных данных, оперативный доступ к информации о зарегистрированных доменных именах и IP-адресах, а также создание круглосуточной сети контактных центров.

Интересен опыт Сингапура, где принят Закон о трансграничных киберпреступлениях (Cross-border Cybercrime Act), позволяющий правоохранительным органам запрашивать данные непосредственно у иностранных

сервис-провайдеров без необходимости использования процедур взаимной правовой помощи, что значительно ускоряет расследование.[6]

III. Проблемы сбора и фиксации электронных доказательств.

Анализ материалов уголовных дел о киберпреступлениях в сфере электронных платежей выявил серьезные проблемы в области сбора, фиксации и оценки электронных доказательств. В законодательстве Узбекистана отсутствуют специальные нормы, регламентирующие процедуры изъятия и исследования цифровых следов преступлений, что часто приводит к утрате доказательственной информации или признанию ее недопустимой в суде.

Эксперты отмечают необходимость внесения изменений в Уголовно-процессуальный кодекс, которые бы урегулировали порядок фиксации цифровых следов, процедуры изъятия электронных носителей информации, а также правила проведения компьютерно-технических экспертиз. В этом

контексте заслуживает внимания опыт Южной Кореи, где действует Закон о цифровых доказательствах (Digital Evidence Act), детально регламентирующий процедуры сбора и исследования электронных доказательств, а также обеспечивающий их юридическую силу в судебном процессе.[13]

IV. Профилактика киберпреступности и защита пользователей электронных платежных систем.

Результаты исследования показывают, что более 70% случаев киберпреступлений в сфере электронных платежей становятся возможными из-за низкого уровня цифровой грамотности пользователей. При этом в законодательстве Узбекистана отсутствуют нормы, обязывающие финансовые учреждения проводить информационно-разъяснительную работу с клиентами по вопросам безопасного использования электронных платежных средств.

Примером эффективного подхода может служить опыт Европейского Союза, где директива PSD2 (Payment Services Directive 2) устанавливает требования к поставщикам платежных услуг в части обеспечения безопасности клиентов, включая обязательное использование многофакторной аутентификации, информирование пользователей о рисках и обучение мерам безопасности.[7]

5. Заключение

Проведенное исследование позволяет сделать вывод о том, что правовое регулирование борьбы с киберпреступлениями в сфере электронных платежных систем в Республике Узбекистан нуждается в дальнейшем совершенствовании с учетом международного опыта и современных технологических вызовов. На основе результатов исследования можно сформулировать следующие рекомендации по совершенствованию законодательства и правоприменительной практики:

В сфере уголовного законодательства:

Дополнить Уголовный кодекс Республики Узбекистан специальными составами преступлений, охватывающими современные формы кибермошенничества в финансовой сфере (фишинг, кардинг, скимминг);[9]

Ввести дифференцированную ответственность за киберпреступления в зависимости от размера причиненного ущерба и степени общественной опасности;

Предусмотреть квалифицирующий признак "совершение преступления в составе транснациональной преступной группы" для киберпреступлений.[10]

В сфере процессуального законодательства:

Внести в Уголовно-процессуальный кодекс нормы, регламентирующие порядок сбора, фиксации и исследования электронных доказательств;[11]

Разработать специальные методические рекомендации для

правоохранительных органов по расследованию киберпреступлений в финансовой сфере.

В сфере международного сотрудничества:

Рассмотреть вопрос о присоединении Республики Узбекистан к Будапештской конвенции о киберпреступности;

Заключить двусторонние соглашения о сотрудничестве в сфере борьбы с киберпреступностью с основными партнерами;[12]

Создать специализированный центр международного сотрудничества в сфере расследования киберпреступлений.

В сфере регулирования электронных платежных систем:

Установить обязательные требования к операторам платежных систем по внедрению современных технологий безопасности, включая многофакторную аутентификацию;

Разработать стандарты информационной безопасности для финансовых технологий;

Ввести ответственность финансовых учреждений за несоблюдение требований информационной безопасности.

В сфере профилактики киберпреступности:

Создать национальную программу повышения цифровой грамотности населения;

Обязать финансовые учреждения проводить регулярное информирование клиентов о рисках киберпреступлений;

Разработать учебные программы по информационной безопасности для образовательных учреждений.

Реализация указанных рекомендаций позволит существенно повысить эффективность правового регулирования борьбы с киберпреступлениями в сфере электронных платежных систем в Республике Узбекистан и обеспечить безопасность функционирования национальной платежной инфраструктуры.

6. Библиография

1. Уголовный кодекс Республики Узбекистан. (2023). Ташкент: Адолат.

2. Закон Республики Узбекистан «О платежах и платежных системах» от 1 ноября 2019 года № ЗРУ-578. (2019). Собрание законодательства Республики Узбекистан, 44, ст. 812.

3. Закон Республики Узбекистан «Об электронной коммерции» от 22 мая 2015 года № ЗРУ-385 (в редакции от 2023 года). (2023). Собрание законодательства Республики Узбекистан, 21, ст. 255.

4. Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 года

№ 560-II (с последующими изменениями). (2003). Собрание законодательства Республики Узбекистан, 2004, 6-7, ст. 67.

5. Постановление Кабинета Министров Республики Узбекистан «О мерах по совершенствованию системы информационной безопасности в сфере электронных платежей» от 17 марта 2023 года № 152. (2023). Собраниезаконодательства Республики Узбекистан, 11, ст. 169.

6. Конвенция о преступности в сфере компьютерной информации (Будапештская конвенция). (2001). Серия европейских договоров № 185.

7. Директива (ЕС) 2015/2366 Европейского парламента и Совета от 25 ноября 2015 г. о платежных услугах на внутреннем рынке (PSD2). (2015). Официальный журнал Европейского Союза, L 337, 35-127.

8. Computer Fraud and Abuse Act, 18 U.S.C. § 1030. (2021). United States Code.

9. Алимов, Р. А. (2023). Проблемы квалификации киберпреступлений по законодательству Республики Узбекистан. Вестник ТГЮУ, 2(34), 45-52.

10. Валиева, К. М. (2024). Международно-правовое сотрудничество в борьбе с киберпреступностью. Проблемы современного права, 1(12), 78-85.

11. Казаков, И. Б. (2022). Электронные доказательства в уголовном процессе: проблемы теории и практики. Юридические исследования, 3, 112-119.

12. Синицын, А. П. (2023). Сравнительный анализ уголовной ответственности за киберпреступления в странах СНГ. Право и цифровые технологии, 2, 34-41.

13. Cohen, L. E., & Felson, M. (2021). Digital Routine Activity Theory: A New Approach to Understanding Cybercrime. Journal of Criminal Justice, 76, 101-113.