European Journal of Interdisciplinary Research and Development
Volume- 52 June- 2026
Website: www.ejird.journalspark.org ISSN (E): 2720-5746

ГРАЖДАНСКО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИМУЩЕСТВЕННЫХ ПРАВ ГРАЖДАН В ЦИФРОВОЙ ЭКОСИСТЕМЕ БАНКОВ

Рамазонов Исмоилбек Абдирашидович
Академия правоохранительных органов Республики Узбекистан
Свободный Соискатель по специальности
12.00.03 — Гражданское право, предпринимательское право,
семейное право, международное частное право

Аннотация:
В данной статье исследуются актуальные вопросы трансформации и совершенствования институтов частного права, направленных на защиту имущественных интересов граждан в условиях масштабного внедрения цифровых банковских экосистем. Опираясь на контент-анализ современных доктринальных подходов к регулированию киберпространства, автор выявляет глубокую информационную и технологическую асимметрию в отношениях между кредитными организациями и потребителями финансовых услуг. Особое внимание уделено гражданско-правовой квалификации хищений, совершаемых методами «социальной инженерии», перераспределению бремени доказывания (onus probandi) в судебных спорах и переходу от классической концепции вины к принципу профессионального риска банка (strict liability). Сформулирован комплекс научно обоснованных предложений по модернизации гражданского и банковского законодательства, включая внедрение обязательного киберстрахования и законодательное закрепление динамического антифрод-мониторинга.

Ключевые слова: имущественные права граждан, цифровая экосистема банков, гражданско-правовое обеспечение, социальная инженерия, профессиональный риск, strict liability, бремя доказывания, антифрод, киберстрахование.

Introduction

Стремительная цифровизация финансового сектора и повсеместное внедрение дистанционного банковского обслуживания (ДБО) кардинально изменили ландшафт современной экономики. Масштабная реализация государственных стратегий развития цифрового пространства, таких как концепция «Цифровой Узбекистан – 2030», открыла перед финансовыми институтами колоссальные технологические возможности. В то же время данный процесс повлек за собой беспрецедентный рост деструктивных явлений в сфере информационно-коммуникационных технологий. Банковский сектор, будучи ключевым элементом критической информационной инфраструктуры, стал основным объектом транснациональных кибератак и таргетированных мошеннических схем.

Традиционная парадигма борьбы с киберпреступностью исторически опирается на публично-правовые инструменты преимущественно на нормы уголовного и уголовно-процессуального права. Однако правоприменительная практика наглядно демонстрирует ограниченность такого подхода. Высокая степень анонимности злоумышленников, использование децентрализованных криптоактивов и трансграничный характер преступлений приводят к тому, что подавляющее большинство уголовных дел приостанавливается в связи с невозможностью установления лица, подлежащего привлечению в качестве обвиняемого. В этих условиях частный интерес добросовестного гражданина (клиента банка), лишившегося своих сбережений, остается незащищенным. Публичное наказание преступника, даже в случае его поимки, далеко не всегда гарантирует оперативное и полное восстановление имущественного положения потерпевшего. Таким образом, возникает острая научно-практическая необходимость смещения исследовательского фокуса в плоскость частного права и модернизации гражданско-правовых механизмов защиты прав потребителей финансовых услуг.

Для выработки комплексной стратегии защиты прав граждан в финансовом киберпространстве необходимо интегрировать современные теоретические разработки в области информационной безопасности и правового обеспечения цифровых систем. Как справедливо отмечает А.В. Остроушко, правовое регулирование общественных отношений в киберпространстве требует междисциплинарного и комплексного подхода, гармонично сочетающего актуализацию внутреннего законодательства с повышением цифровой грамотности населения [1]. Применительно к банковской сфере это означает, чтотрадиционные гражданско-правовые институты (такие как договор банковского счета, деликтная ответственность, неосновательное обогащение) не могут применяться в отрыве от технико- технологических реалий функционирования банковских платформ.

Более того, М.Н. Степанова обосновывает, что информационная безопасность национального масштаба напрямую зависит от гибкости правовых рамок, адаптированных к вызовам современных технологий [2]. В банковском секторе эта гибкость должна проявляться в способности гражданского права оперативно реагировать на появление новых способов хищения активов, распределяя имущественные риски справедливым образом. В свою очередь, Т.В. Кокорева указывает на неизбежную трансформацию гражданско-правовых механизмов под воздействием меняющихся социально-экономических парадигм и внешних факторов [3]. Если ранее банковское право адаптировалось преимущественно под новые финансовые инструменты (например, «зеленое» кредитование), то сегодня ключевым вектором его трансформации становится обеспечение тотальной технологической безопасности транзакций и минимизация рисков «цифрового отчуждения» клиентов.

Центральной проблемой действующего механизма гражданско-правового регулирования отношений «банк – клиент» в условиях кибер-угроз является глубокая информационная, технологическая и экономическая асимметрия сторон. В силу ст. 771 Гражданского кодекса Республики Узбекистан, банк обязуется принимать и зачислять

поступающие на счет, открытый клиенту, денежные средства, выполнять распоряжения клиента о перечислении и выдаче соответствующих сумм. При этом на практике правоотношения сторон оформляются договорами присоединения (ст. 360 ГК РУз), условия которых разрабатываются банками в одностороннем порядке.

Анализ типовых договоров ДБО показывает, что кредитные организации включают в них дискриминационные оговорки (disclaimers), полностью освобождающие банк от ответственности в случае, если транзакция была совершена с использованием аутентификационных данных клиента (SMS-коды, CVV/CVC-коды, push-уведомления). Судебные инстанции при рассмотрении подобных споров зачастую занимают формальную позицию: поскольку кодовое подтверждение было введено, распоряжение считается исходящим от самого клиента, а передача кода третьим лицам квалифицируется как «грубая неосторожность» самого гражданина, что согласно ст. 1000 ГК РУз является основанием для уменьшения размера возмещения вреда или отказа в нем.

Такой подход игнорирует природу современных киберпреступлений, совершаемых с использованием методов «социальной инженерии» (vishing, phishing). Преступники используют глубокие психоэмоциональные манипуляции, методы подмены номеров (spoofing) и фальшивые цифровые интерфейсы, визуально неотличимые от легитимных приложений банков. В таких условиях традиционная цивилистическая концепция вины, основанная на модели поведения «разумного и осмотрительного участника оборота», превращается в фикцию. Профессиональный банк обладает штатом ИТ-специалистов, алгоритмами искусственного интеллекта и системами мониторинга транзакций, в то время как рядовой гражданин лишен возможности технически распознать высокотехнологичную атаку. Возложение всего бремени убытков на слабую сторону договора противоречит базовым принципам справедливости и добросовестности, закрепленным в ст. 8 ГК РУз.

Дополнительную сложность представляет процессуальный аспект. Согласно общему правилу доказывания, каждая сторона должна доказать те обстоятельства, на которые она ссылается (ст. 72 Гражданского процессуального кодекса). В кибер-спорах клиент физически не имеет доступа к программно-аппаратным комплексам банка, серверам и лог-файлам, чтобы доказать наличие уязвимости в системе безопасности банка или факт несанкционированного перехвата трафика.

Для преодоления системного кризиса в правоприменительной практике предлагается кардинальное реформирование гражданско-правовых механизмов защиты по трем ключевым направлениям:

1. Внедрение принципа профессионального (предпринимательского) риска банка (Strict Liability). Необходимо на законодательном уровне закрепить, что банк, как субъект, извлекающий прибыль из функционирования высокорисковой цифровой среды, несет ответственность за убытки от несанкционированных транзакций независимо от своей вины. В Гражданский кодекс следует имплементировать норму, аналогичную европейской Директиве PSD2 (Payment Services Directive 2) [7].

Если клиент заявляет, что он не давал поручения на списание средств, банк обязан незамедлительно восстановить баланс счета (в течение 24 часов), за исключением случаев, когда банк сможет неопровержимо доказать умысел или прямой сговор со стороны самого клиента. Риск совершения операции под влиянием обмана третьих лиц должен ложиться на банк как на профессионального оператора системы.

2. Законодательное перераспределение бремени доказывания (Reversal of Burden of Proof). В рамках споров по киберхищениям должна действовать законная презумпция вины банка в необеспечении безопасности конфиденциальных данных и каналов связи. Именно на финансовый институт должна быть возложена процессуальная обязанность доказать, что его информационная система в момент совершения спорной транзакции функционировала в абсолютно штатном режиме, не имела внутренних сбоев, а архитектура безопасности ДБО исключала возможность перехвата одноразовых паролей.

3. Нормативное закрепление динамического антифрод-мониторинга. В закон «О банках и банковской деятельности» необходимо ввести императивное требование о внедрении интеллектуальных систем предотвращения мошенничества. Юридическим критерием «ложной транзакции» должно стать несоответствие операции поведенческому профилю клиента (динамический маркер: резкая смена геолокации, нетипичный объем и скорость переводов, оформление моментального онлайн-кредита с последующим транзитным выводом средств). Если антифрод-система банка не заблокировала операцию, обладающую явными признаками аномальности, банк признается не проявившим должной осмотрительности (due diligence) и обязан в полном объеме возместить клиенту причиненный реальный ущерб.

4. Развитие института обязательного киберстрахования. По аналогии с выводами цивилистической доктрины о трансформации механизмов обеспечения стабильности оборота [3, 6], целесообразно внедрить обязательное страхование гражданской ответственности коммерческих банков за риски, связанные с нарушением информационной безопасности. Создание специализированных страховых пулов позволит абсорбировать имущественные потери граждан в наиболее сложных случаях «социальной инженерии», сохраняя при этом ликвидность и финансовую устойчивость банковской системы в целом.

В заключении нашего исследования стоит отметить что модернизация гражданско-правовых механизмов борьбы с киберпреступностью в банковском секторе требует решительного отказа от устаревших формальных подходов. Защита имущественных интересов граждан в цифровом пространстве может быть эффективной только тогда, когда право распределяет риски в пользу экономически и технологически более слабой стороны. Возложение на банки строгой имущественной ответственности за несанкционированные транзакции и перенос бремени доказывания станут мощным катализатором для самих кредитных организаций в части совершенствования их внутренних систем кибербезопасности. Предложенные меры позволят создать сбалансированную частноправовую экосистему, гарантирующую реальную защиту конституционных прав граждан на собственность в эпоху тотальной цифровизации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Остроушко А. В. О совершенствовании механизма правового обеспечения прав граждан в киберпространстве // Пробелы в российском законодательстве. 2023. Т. 16. No 3. С. 37-45.
2. Степанова М. Н. Информационная безопасность в правовом поле: стратегии правового регулирования и защиты киберпространства // Правопорядок: история, теория, практика. 2024. No 1 (40). С. 48-52.
3. Кокорева Т. В. Трансформация гражданско-правового регулирования банковского кредитования экологического предпринимательства в Российской Федерации и Европейском Союзе // Правовая парадигма. 2021. Т. 20. No 4. С. 136-142.
4. Рустамбеков И. Р. Цифровое право: Теория и практика. Монография. – Ташкент: ТГЮУ, 2023. – 240 с.
5. Гулямов С. С. Гражданско-правовое регулирование цифровых финансов. – Ташкент: Юстиция, 2022. – 310 с.
6. Наливайченко Е. В. Развитие цифровой экономики в условиях глобализации. – Симферополь: Ариал, 2019. – 276 с.
7. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2) // Official Journal of the European Union. L 337/35.
8. Smith G. Internet Law and Regulation. 5th Edition. – London: Bird & Bird, 2020. – 850 p. Постановление Пленума Верховного суда Республики Узбекистан «О некоторых вопросах судебной практики по делам, связанным с мошенничеством в сфере ИКТ» от 15.12.2024 г.
9. World Bank Report. Cybersecurity in Financial Sector: Regulatory Approaches. – Washington DC, 2024. – 188 p.