**Анна Павловна АЛЕКСЕЕВА,**
доктор юридических наук, профессор, ORCID 0000-0002-4569-7564
Санкт-Петербургский университет МВД России (г. Калининград)
профессор кафедры уголовного права, криминологии
и уголовно-исполнительного права Калининградского филиала
Заслуженный юрист Российской Федерации
*alexeeva.klg-mvd@yandex.ru*

**Наталья Николаевна БУГЕРА,**
кандидат юридических наук, доцент, ORCID 0000-0002-2459-7855
Волгоградская академия МВД России (г. Волгоград)
начальник кафедры уголовного права учебно-научного комплекса
по предварительному следствию в органах внутренних дел
*knn.76@mail.ru*

Научная статья
УДК 343.97:343.85

# ФИНАНСОВАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРЕСТУПНОСТИ: ВЫЗОВЫ И МЕХАНИЗМЫ СИСТЕМНОЙ ЗАЩИТЫ

**КЛЮЧЕВЫЕ СЛОВА. Корпоративное дропперство, финансовое мошенничество, система быстрых платежей, QR-эквайринг, противодействие.**

**АННОТАЦИЯ.** ***Введение.*** *Ускоренная цифровая трансформация финансового сектора России стимулирует появление новых способов совершения преступлений, угрожающих экономической безопасности государства. Особое внимание в ходе исследования, результаты которого представлены в статье, было уделено феномену современного дропперства (использования счетов и платежных инструментов третьих лиц для легализации преступных доходов посредством системы быстрых платежей и QR-эквайринга). Эволюция дропперства демонстрирует переход от взаимодействия с физическими лицами к вовлечению в него юридических лиц, формально занятых розничной торговлей, что существенно увеличило объемы транзакций и продлило жизненный цикл мошеннических схем.* ***Методы.*** *При проведении исследования оказался востребован интегративный междисциплинарный подход, предусматривающий использование системного метода, институционального, социологического, сценарного и прогностического анализа данных, контент-анализа судебной практики.* ***Результаты.*** *В последнее время произошла кардинальная трансформация природы дропперства: оно превратилось в корпоративную, высокотехнологичную мошенническую практику с применением QR-эквайринга и маскировкой под легальный бизнес. Его главные характеристики – масштабируемость, устойчивость и легитимность – формируют новую криминальную реальность. Сегодня общество столкнулось с феноменами виртуализации преступного пространства и административной мимикрии, обеспечивающими высокую прибыльность дропперства и его устойчивость к традиционным мерам противодействия. Современное законодательство нуждается в глубоком реформировании, а система защиты от преступных посягательств – в адаптации к условиям воздействия новых «цифровых» вызовов. Есть основания прогнозировать дальнейшее усложнение способов совершения мошенничества с применением высоких технологий, что требует разработки и реализации проактивных стратегий организации противодействия данному виду преступности и международного сотрудничества в этой сфере для обеспечения безопасности цифровой экономики.*

**ВВЕДЕНИЕ**

Цифровая трансформация финансового сектора Российской Федерации сопровождается возникновением качественно новых форм преступности, представляющих системную угрозу экономической безопасности государства. Современное дропперство – использование банковских счетов и платежных инструментов третьих лиц для легализации преступных доходов – претерпело кардинальные изменения с внедрением системы быстрых платежей (далее – СБП) и QR-эквайринга.

Научная новизна исследования, результаты которого представлены в настоящей статье, обусловлена несколькими факторами. Во-первых, масштабное внедрение QR-технологий в российскую платежную инфраструктуру создало качественно новые возможности для преступной деятельности. Во-вторых, существующая нормативная база оказалась неспособной эффективно противодействовать новым формам финансовых преступлений. В-третьих, отсутствие комплексного криминологического анализа современных дропперских схем затрудняет разработку адекватных мер противодействия.

Цель исследования заключалась в выявлении специфики трансформации дропперских схем в условиях цифровизации платежных систем и разработке научно обоснованных рекомендаций по совершенствованию противодействия новым формам финансовых преступлений.

Перед исследованием ставились следующие задачи: проанализировать эволюцию дропперских схем от традиционных форм к корпоративным; исследовать технологические особенности использования QR-кодов в преступных целях; оценить эффективность существующих регуляторных мер противодействия; раскрыть правовые и криминологические проблемы выявления новых форм преступлений; проанализировать уровень цифровой грамотности населения как фактора уязвимости к киберугрозам.

Актуальность проведенного нами исследования определяется стремительным ростом финансового мошенничества, осуществляемого посредством СБП. По данным Центрального банка Российской Федерации (далее – ЦБ РФ), в 2024 году объем операций, совершенных без согласия клиентов, достиг 27,5 млрд рублей, что на 74,4% больше показателя 2023 года. Количество мошеннических транзакций составило 1,196 млн, в 2,5 раза чаще стали совершаться хищения с использованием СБП, причиненный ими ущерб вырос до 8,25 млрд рублей. Прогнозы указывают на возможность увеличения объема ущерба в 2025-2026 годах до 40-52 млрд рублей[1].

Результаты исследования показывают, что дропперство претерпело качественную трансформацию. Если ранее в нем участвовали преимущественно физические лица – так называемые «невежественные дропперы» (drop-in-ignorance), а срок жизни мошеннических схем был весьма ограничен, то сегодня наблюдается иной феномен – корпоративное дропперство. Оно представляет собой не эволюцию старых методов, а принципиально новый формат организованной преступности, реализуемый в цифровой среде. В данном случае используются юридические лица, являющиеся псевдокоммерческими структурами, формально занимающимися розничной торговлей. Это создает многослойную систему маскировки, эксплуатирующую презумпцию добросовестности предпринимательской деятельности. Можно выделить три ключевые характеристики произошедшей трансформации: масштабируемость – лимиты увеличиваются до десятков миллионов рублей; устойчивость – схемы дольше сохраняют работоспособность (до двух недель); легитимность – эффективная маскировка под обычную хозяйственную деятельность. Совокупность этих факторов формирует новый тип криминальных отношений. Использование в дропперстве юридических лиц значительно увеличивает объем транзитных потоков по сравнению со схемами, в которых задействованы расчетные карты физических лиц, ограниченные по лимитам и быстро блокируемые после выявления подозрительной активности. Корпоративная оболочка обеспечивает устойчивость мошеннических схем и расширяет возможности по совершению финансовых операций.

По данным ЦБ РФ, только одним из крупных российских банков с начала 2025 года было выявлено 319 компаний-дропов с оборотом свыше 50 млн рублей в месяц[2]. При относительно небольшой стоимости услуг по подключению точки приема платежей через СБП (15-30 тысяч рублей) злоумышленники получают чрезвычайно выгодную модель с позиции соотношения затрат и прибыли. QR-эквайринг не просто стал новым инструментом мошенничества, а изменил саму природу дропперства. Внедрение удаленного режима совершения финансовых операций устраняет пространственные ограничения, позволяя размещать QR-коды на любых цифровых носителях без наличия физической инфраструктуры. Такое явление можно назвать «виртуализацией преступного пространства».

Значимый элемент преступных схем рассматриваемого нами вида представляет собой административная мимикрия – использование MCC-кодов розничных магазинов для легализации деятельности. MCC-коды, применяемые банками и платежными системами для классификации операций, создают легитимный профиль юридических лиц - мошенников. Регистрация таких лиц в «розничной» сфере (например торговля продуктами питания) способствует формированию представления об их надежности у банков и минимизирует риск блокировки денежных переводов. Такая подмена эксплуатирует доверие

[1] Чернышова Е. ЦБ зафиксировал рекордную сумму хищений у банковских клиентов в 2024 году // РБК: сайт. 18.02.2025 // URL: https://www.rbc.ru/finances/18/02/2025/67b489749a794780d1527516 (дата обращения: 28.09.2025).
[2] 319 компаний-дропов выявили банки России в 2025 году // ПрессАфф: сайт // URL: https://pressaff.com/tg-news/319-kompanij-dropov-vyyavili-banki-rossii-v-2025-godu-nelegalnye-onlajn-kazino-prinimali/ (дата обращения: 28.09.2025).

**Anna P. ALEKSEEVA,**
Doctor of Law, Professor, ORCID 0000-0002-4569-7564
Saint Petersburg University of the Ministry
of the Interior of Russia (Kaliningrad, Russia)
Professor of the Department of Criminal Law, Criminology
and Criminal Executive Law of the Kaliningrad Branch
Honored Lawyer of the Russian Federation
*alexeeva.klg-mvd@yandex.ru*

**Natalia N. BUGERA,**
Cand. Sci. (Jurisprudence), Associate Professor, ORCID 0000-0002-2459-7855
Volgograd Academy of the Ministry of the Interior of Russia (Volgograd, Russia)
Head of the Criminal Law Department of the Educational and Scientific
Complex on Preliminary Investigation in Internal Affairs Bodies
*knn.76@mail.ru*

**FINANCIAL SECURITY IN THE CONTEXT OF THE DIGITAL TRANSFORMATION OF CRIME: CHALLENGES AND SYSTEMIC PROTECTION MECHANISMS**

**KEYWORDS. Corporate droppery, financial fraud, fast payment system, QR acquiring, counteraction.**

**ANNOTATION.** ***Introduction.*** *The accelerated digital transformation of Russia's financial sector is stimulating the emergence of new methods of committing crimes that threaten the economic security of the state. The study, the results of which are presented in this article, focused on the phenomenon of modern droppering (the use of third-party accounts and payment instruments to launder criminal proceeds through the fast payment system and QR acquiring). The evolution of droppering demonstrates a shift from interactions with individuals to the involvement of legal entities formally engaged in retail trade, which has significantly increased transaction volumes and extended the life cycle of fraudulent schemes.* ***Methods.*** *The study utilized an integrative interdisciplinary approach, involving a systems method, institutional, sociological, scenario, and predictive data analysis, and a content analysis of judicial practice.* ***Results.*** *Recently, the nature of dropshipping has undergone a radical transformation: it has evolved into a corporate, high-tech fraudulent practice using QR acquiring and masquerading as a legitimate business. Its key characteristics – scalability, sustainability, and legitimacy – are creating a new criminal reality. Today, society is confronted with the virtualization of criminal space and administrative mimicry, which ensures the high profitability of dropshipping and its resilience to traditional countermeasures. Current legislation requires thorough reform, and the system of protection against criminal attacks must be adapted to the impact of new digital challenges. There is reason to predict a further increase in the sophistication of high-tech fraud methods, which requires the development and implementation of proactive strategies to combat this type of crime and international cooperation in this area to ensure the security of the digital economy.*

государства и финансовой системы к унифицированным классификаторам, которые не учитывают сложные криминальные сценарии. Автоматизированный контроль, ориентирующийся на MCC-коды, с трудом различает легальные и преступные транзакции. В результате массовый поток операций под легальными шифрами снижает эффективность финансового мониторинга и затрудняет выявление незаконных переводов.

Приняв во внимание эти обстоятельства, ЦБ РФ в октябре 2023 года выпустил методические рекомендации № 13-МР, обязав банки усиливать мониторинг QR-эквайринга, поскольку «всплески» по операциям в СБП зачастую свидетельствуют о нелегальной деятельности.

## МЕТОДЫ

В ходе исследования был использован комплекс междисциплинарных методов, обеспечивающих всесторонний анализ трансформации дропперских схем в условиях цифровизации финансового сектора. Криминологический анализ позволил выявить новые формы и характеристики корпоративного дропперства, рассмотреть механизмы виртуализации преступного пространства и административной мимикрии. Правовой анализ применялся для оценки соответствия действующего уголовного законодательства современным цифровым реалиям и выявления нормативных пробелов.

Использование эмпирического метода опиралось на статистические данные ЦБ РФ о масштабах мошенничества, осуществляемого посредством СБП, а также на результаты социологических исследований уровня цифровой грамотности населения, что позволило учесть социальные факторы уязвимости к киберугрозам. Прогностический и сценарный анализ потребовался для моделирования возможных направлений развития финансовой преступности и совершенствования технологических мер противодействия ей, в том числе концепции «предиктивного иммунитета» антифрод-систем.

Системный метод обеспечил интеграцию криминологических, правовых, социальных и технологических аспектов, анализ взаимосвязей между ними и выявление комплексных стратегий противодействия дропперству. Институциональный и социологический анализ позволил исследовать поведенческие факторы и роль межведомственного взаимодействия в формировании эффективной системы защиты.

Таким образом, использование вышеназванных методов создало основание для разработки науч-

но обоснованных рекомендаций по совершенствованию правового регулирования и технологий в сфере борьбы с новыми формами финансовых преступлений в условиях цифровой экономики.

**РЕЗУЛЬТАТЫ**

Проблема привлечения предпринимателей к ответственности за участие в нелегальных операциях с использованием QR-кодов во многом связана с трудностями доказывания их осведомленности об участии в реализации преступных схем: зачастую они утверждают, что ничего не знали об истинном назначении переводов, что усложняет сбор доказательственной базы [1, с. 465].

Анализ правовых механизмов противодействия дропперству обнаруживает системный кризис традиционного подхода к квалификации финансовых преступлений. Действующее законодательство, включая ст. 174 УК РФ, устанавливающую ответственность за легализацию (отмывание) преступных доходов, демонстрирует концептуальную неадекватность «аналогового» права цифровым реалиям.

Во-первых, ст. 174 УК РФ не учитывает современные механизмы электронных платежей и инновационные способы маскировки преступных финансовых схем, такие как использование корпоративных дропперских структур, QR-кодов и СБП. Законодательство ориентировано на классические механизмы преступлений и не способствует эффективной квалификации многоуровневых, распределенных и виртуализированных схем отмывания денег.

Во-вторых, законодательные нормы недостаточно гибки для реагирования на быстро меняющиеся технологические условия. Они не учитывают особенности цифровых финансовых активов, криптовалют, а также возможности использования технологий искусственного интеллекта (далее – ИИ) и автоматизированных систем, что позволяет преступникам эксплуатировать правовые пробелы и избегать наступления ответственности.

В-третьих, доказывание факта совершения преступления, предусмотренного ст. 174 УК РФ, усложняется из-за увеличения дистанции между лицами, непосредственно осуществляющими преступную деятельность, и теми, кто номинально выступает субъектом преступления. Это затрудняет идентификацию преступников и сбор доказательств, что может приводить к формальной констатации невиновности или смягчению наказания.

Наконец, законодатель реагирует на новые криминальные вызовы избирательно и частичными поправками, которые носят фрагментарный характер, не создавая комплексной системы противодействия цифровой финансовой преступности. Так, например, внесенные в ст. 187 УК РФ изменения, вступившие в силу 5 июля 2025 года, сводятся к введению уголовной ответственности за участие в мошеннических схемах по обналичиванию и передаче электронных средств платежа без признаков непосредственного хищения. Это своеобразная попытка закрыть «правовой пробел», который ранее позволял дропперам избегать уголовного преследования [2, с. 20]. Однако она не устраняет глубинных несовершенств, существующих в механизмах профилактики, межведомственного взаимодействия, цифровой идентификации и отслеживания цепочек транзакций.

Основываясь на результатах исследования, мы приходим к выводу о необходимости системной реконцептуализации подходов к противодействию дропперству. Предлагаемые в науке законодательные меры – введение в ст. 174 УК РФ квалифицирующих признаков для QR-эквайринга [3, с. 99], создание специальных диспозиций для корпоративного дропперства [4, с. 53] – должны рассматриваться как элементы более широкой стратегии адаптации правовой системы к цифровой реальности.

Примечательно, что на этом фоне с сентября 2024 года банки начали активно внедрять технологии ИИ для пересылки средств по СБП. В ответ на подобные вызовы Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Минцифры России) инициировало внесение поправок в ряд статей УК РФ (ст.ст. 158, 159, 163, 272 и 274), предложив закрепить новый квалифицирующий признак – «совершение преступления с применением искусственного интеллекта»[1]. Однако, как замечают эксперты, новое определение ИИ, представленное авторами поправок (комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека), вызывает серьезные дискуссии среди специалистов. К тому же дефиниция представляется в весьма абстрактной форме и отчасти противоречит действующим положениям Национальной стратегии развития искусственного интеллекта[2] (далее – Стратегия), содержащей более конкретное и детализированное определение (п. 5 разд. I). Оно учитывает разнообразие технологий, уровней и типов ИИ, а также их функциональное назначение в разных сферах применения: «искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека или превосходящие их». Соответственно, комплекс технологических решений здесь включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе с методами машинного обучения), процессы и сервисы по обработке дан-

[1] Минцифры предложило наказывать тюрьмой за использование ИИ в преступных целях // Вести.Ру: сайт. 10.06.2025 // URL: https://www.vesti.ru/article/4542269 (дата обращения: 01.09.2025).

[2] Национальная стратегия развития искусственного интеллекта на период до 2030 года утверждена Указом Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации».

ных и поиску решений. Дополнительно Стратегией введены четыре уточняющих понятия, что делает подход дифференцированным по уровням и типам ИИ:

- технологии ИИ – конкретные прикладные технологии (компьютерное зрение, обработка естественного языка, распознавание и синтез речи, интеллектуальная поддержка принятия решений и др.);

- перспективные методы ИИ – методы, направленные на создание принципиально новой научно-технической продукции, в том числе в целях разработки универсального (сильного) ИИ (автономное решение различных задач, автоматический дизайн физических объектов, автоматическое машинное обучение, обработка информации на основе новых типов вычислительных систем, интерпретируемая обработка данных и др.);

- смежные области применения ИИ – робототехника, беспилотный транспорт и иные комплексы, где ИИ является обязательным элементом;

- набор и разметка данных – регулируемые правовые объекты, необходимые для разработки ИИ-систем.

Таким образом, в отличие от «узких» уголовно-правовых формулировок Стратегия задает многоуровневую модель: уровень технологий (слабый, ограниченный, уже существующий ИИ), уровень перспективных методов (сильный ИИ), уровень инфраструктуры и данных, уровень функционального назначения (применение в экономике и социальной сфере). Стратегия ориентирована на практическое использование ИИ, его развитие и внедрение с учетом технологических особенностей и этических норм.

А вот абстрактность инициативы Минцифры России порождает ряд проблем. Во-первых, она затрудняет однозначное и предсказуемое правоприменение, поскольку пространный и неопределенный термин «ИИ» может быть интерпретирован слишком свободно, что приведет к избыточному расширению круга потенциальных преступлений и отягчающих обстоятельств. Во-вторых, существует опасность того, что реализация сформулированного Минцифры России предложения негативно скажется на инновационной деятельности, произведя «охлаждающий» эффект, так как разработчики и компании могут столкнуться с излишними юридическими рисками и неопределенностью при внедрении ИИ-технологий. В условиях, когда такие технологии широко применяются в многочисленных интернет-приложениях и пользовательских устройствах, в совершении практически любого преступления можно будет усмотреть отягчающее обстоятельство – использование ИИ. Это, в свою очередь, будет ослаблять мотивацию разработчиков программного обеспечения и тормозить технологический прогресс.

Кроме того, отметим, что на мотивацию IT-специалистов существенное влияние оказало введение в конце 2024 года в Уголовный кодекс Российской Федерации ст. 272.1[1]. В опубликованном 18 июня 2025 года обзоре подчеркнуты серьезные риски, связанные с применением этой нормы к профессиональной деятельности специалистов в области информационной безопасности и компаний, занимающихся защитой информации[2]. Данная правовая новелла криминализирует широкий спектр действий, осуществляемых с компьютерной информацией, включая незаконное использование, передачу, сбор и хранение персональных данных, а также создание и эксплуатацию ресурсов, предназначенных для таких операций. Ключевой проблемой является расширительное толкование деяний, составляющих объективную сторону состава преступления. Им потенциально охватываются типичные профессиональные сценарии работы специалистов в области информационной безопасности: выгрузка данных и анализ утечек из даркнета, скачивание баз данных при расследовании инцидентов, развертывание тестовых сред (honeypot, песочниц) с реальными персональными данными без согласия владельцев, мониторинг публичных и закрытых источников для выявления фишинг-ресурсов и других угроз, а также пентестинг (тестирование на проникновение), предусматривающий работу с чужими персональными данными без прямого согласия [5, с. 61]. Проблема усугубляется так называемым «порочным» согласием на обработку персональных данных, при котором формальное согласие их владельца может быть признано регулятором или судом недействительным, что оборачивается криминализацией даже добросовестной деятельности по защите информации.

Исходя из этого, можно сделать вывод о высоком риске применения ст. 272.1 УК РФ в отношении добросовестных специалистов и компаний, работающих в области информационной безопасности. Это обстоятельство требует либо развития «сужающей» судебной практики, либо внесения в законодательство специальных исключений, декриминализирующих действия, совершаемые в целях обеспечения информационной безопасности согласно внутреннему регламенту или по заказу клиента. Необходимо достичь баланса между потребностями кибербезопасности и избеганием чрезмерной криминализации профессиональной деятельности, что имеет ключевое значение для формирования эффективной правовой политики в сфере информационной безопасности и защиты персональных данных.

В рамках борьбы с новыми мошенническими схемами активно разрабатывается централизованная платформа противодействия дропперам. Концепция платформы будет представлена для общественного обсуждения в первом полугодии 2026 года, а запуск ее эксплуатации в целях оперативного обмена информацией и конструирования типологий для выявления подозрительных

[1] Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» вступил в силу 11 декабря 2024 г.

[2] Афанасьев С. Борьбу с утечкой персональных данных усилили // АГ-эксперт: сайт. 18.06.2025 // URL: https://www.advgazeta.ru/ag-expert/advices/borbu-s-utechkoy-personalnykh-dannykh-usilili/ (дата обращения: 02.09.2025).

операций на ранних стадиях намечен на 2027 год[1]. Реализация данного инициативного проекта призвана способствовать повышению эффективности финансового мониторинга и сужению пространства для злоупотреблений в платежной сфере благодаря организации взаимодействия между регуляторами, банками и экспертами на единой технологической и операционной основе [6]. Подготовка данной платформы отражает системность подхода к решению проблемы цифрового мошенничества и демонстрирует стремление к внедрению современных цифровых инструментов противодействия финансовым преступлениям в развивающейся экономической и технологической среде России [7, с. 371]. В настоящее время формируется комплекс решений, включающий в себя информационно-коммуникационную структуру, программное обеспечение, а также процессы и сервисы, направленные на обработку данных и поиск оптимальных решений в области цифровой безопасности [8, с. 687]. Технологическая архитектура новой платформы должна объединить сервисы информационной безопасности и аналитику, а также учитывать человеческий фактор. Многие пользователи, даже хорошо знающие базовые правила безопасного поведения в цифровой среде, не могут распознать контент-ориентированные угрозы [9, с. 53]. Поэтому предполагается, что платформа будет обладать образовательным потенциалом и станет ресурсом, формирующим поведенческие модели. В противном случае ее защитные функции будут ограничены техническим периметром, а криминальный риск останется в зоне «цифрового невежества».

Наши выводы подтверждаются результатами социологических исследований. Согласно данным аналитического отчета АНО «Цифровая экономика» и ВЦИОМ, подготовленного в 2025 году по итогам опроса 1626 граждан, уровень цифровой грамотности населения в России остается недостаточным для эффективного противодействия киберугрозам[2]. Большинство респондентов отметили, что основными источниками информации об опасностях такого рода для них служат новостные интернет-ресурсы (51%) и социальные контакты (45%), что указывает на фрагментарность и несистемность распространения критически важных знаний о цифровой безопасности. Несмотря на оптимистичные данные о применении гражданами базовых мер защиты – отказ от пересылки паролей (72%), от хранения банковских данных на электронных устройствах (71%), использование двухфакторной аутентификации (59%), – статистически значимая доля населения (20-25%) испытывает затруднения в распознавании современных контентно-ориентированных угроз, таких как дипфейк. Сложившаяся ситуация свидетельствует о наличии системного пробела («структурного провала знания») в функциональной цифровой безопасности населения, обусловленного доминированием неофициальных и неструктурированных каналов получения информации, что снижает уровень коллективной защищенности от высокотехнологичных атак [10, с. 18]. В результате формируется «нишевая уязвимость», охватывающая минимум 20-25% населения. Это люди, неспособные противостоять социально-инженерным воздействиям, что позволяет киберпреступникам эффективно обходить даже технически защищенные сервисы [11, с. 48].

Таким образом, возникает поведенческий парадокс: достигается формирование базовых рефлексов безопасности, однако недостаточная компьютерная грамотность существенно снижает порог устойчивости пользователя цифровых устройств к кибератакам. Усугубляет ситуацию асимметрия в темпах обновления технологий: образовательные программы совершенствуются с запаздыванием, в то время как технологии обхода средств защиты меняются значительно быстрее, что создает пространство для успешного осуществления кибератак [12, с. 238]. Следовательно, необходимы меры цифрового просвещения, ориентированные на обучение критическому мышлению, верификации информационных источников и навыкам определения цифровых следов поддельного контента [13, с. 92]. Требуется внедрение системных образовательных инициатив, предусматривающих использование симуляционных тренажеров, интегрированных в мобильные банковские приложения, включение в школьные программы обязательных учебных модулей по кибербезопасности, реализация проектов с изолированной средой для тестирования и развития средств распознавания дипфейков [14, с. 11]. Без системной и комплексной подготовленности пользователей технические средства информационной безопасности смогут компенсировать лишь часть ущерба, а цифровая преступность приобретет устойчивый и масштабируемый социальный канал распространения угроз, что потребует междисциплинарных и институциональных подходов для обеспечения кибербезопасности в масштабах всей страны.

Итак, анализ развития систем защиты от мошенничества в банковской сфере выявляет классическую динамику, сходную с функционированием иммунной системы человека. Повышение уровня защиты инициирует появление более изощренных и адаптивных методов ее обхода, используемых злоумышленниками. Однако в отличие от биологического иммунитета, где выработка антител происходит с высокой скоростью, финансовые системы вынуждены действовать в рамках регуляторных процедур, предусматривающих аудит, согласование и контроль соблюдения законов, нормативных актов и лицензионных условий. Это замедляет реакцию на новые угрозы и создает

[1] Кошкина Ю. ЦБ разработает новую платформу по контролю за переводами россиян. Как будет работать механизм по борьбе с сомнительными операциями // РБК: сайт. 25.12.2024 // URL: https://www.rbc.ru/finances/25/12/2024/676a90f29a794720bb4bc2b3 (дата обращения: 03.09.2025).

[2] Латун И. АЦ ВЦИОМ: Большинство пользователей не знают способов защиты от киберугроз // Российская газета: сайт. 17.09.2025 // URL: https://rg.ru/2025/09/17/ac-vciom-bolshinstvo-polzovatelej-ne-znaiut-sposobov-zashchity-ot-kiberugroz.html (дата обращения: 04.09.2025).

структурное несоответствие между временем, необходимым преступникам на адаптацию к новым условиям, и временем, требующимся для совершенствования защитных механизмов.

В связи с этим эффективность антифрод-систем[1] предопределяется не только способностью выявлять уже осуществляемые мошеннические действия, но и реализовывать прогностические функции, опережая развитие реальных угроз во времени. Современные практики компьютерного мошенничества, включая использование криптовалют, автоматизированных механизмов смешивания исходящих транзакций и дипфейк-технологий, формируют полиуровневые площадки для организации кибератак, существенно усложняя требования к системам безопасности.

В современных условиях развития цифровой экономики и постоянного совершенствования методов киберпреступности финансовые организации разрабатывают и внедряют современные технологические решения, основанные на применении ИИ. Главной их целью является моделирование различных сценариев кибератак в виртуальной среде, что позволяет предвосхищать угрозы, определять уязвимые точки и вырабатывать оптимальные стратегии защиты. ИИ обучается на больших данных, полученных от различных банковских учреждений, что повышает точность распознавания мошеннических схем и эффективность предотвращения преступных действий. Такая методология способствует глубокому пониманию тактики преступников и увеличивает адаптивные возможности систем безопасности.

Следующим этапом развития технологий защиты является формирование концепции «предиктивного иммунитета», при котором системы безопасности не только своевременно реагируют на выявленные угрозы, но и прогнозируют потенциальные атаки. Эта проактивная модель предусматривает генерацию сценариев возможных кибератак, защиту пользовательских операций и маршрутов передачи данных, а также оперативный обмен информацией об инцидентах и обнаруженных нарушениях.

Вместе с тем следует иметь в виду, что сегодня в условиях, когда киберугрозы и мошеннические схемы обладают транснациональным характером, локальные и национальные меры защиты нередко оказываются недостаточными [15, с. 125]. Необходимым становится развитие международного сотрудничества, формирование единых стандартов и протоколов обмена информацией и доказательствами, а также создание платформ совместного мониторинга и анализа киберугроз. Важным институтом такого сотрудничества является взаимное признание странами результатов аудитов безопасности, электронных подписей и сертификатов.

Можно говорить о том, что интеграция передовых ИИ-технологий в банковском секторе с системой международного нормативного и технического взаимодействия обеспечивает снижение асимметрии между быстрым развитием методов осуществления кибератак и сравнительно медленной реакцией систем защиты. Такая комплексная стратегия является залогом обеспечения устойчивого равновесия и безопасности финансовой экосистемы в условиях постоянного обновления вызовов со стороны цифровой преступности.

**ЗАКЛЮЧЕНИЕ**

Современное дропперство прошло значительную трансформацию, перейдя от примитивных схем с участием физических лиц к использованию сложных корпоративных структур, эффективно эксплуатирующих цифровые технологии, такие как QR-эквайринг и СБП. Эта эволюция создала новую криминальную реальность, характеризующуюся масштабируемостью, устойчивостью и высокой степенью маскировки под легитимную предпринимательскую деятельность. Критические риски связаны с низкой цифровой грамотностью населения, что увеличивает уровень его уязвимости к социально-инженерным атакам.

Одновременно с активизацией технологического прогресса проявились серьезные пробелы в нормативно-правовом регулировании, что затрудняет эффективное противодействие новым формам финансовых преступлений. Так, например, до середины 2025 года уголовной ответственности непосредственно за дропперство вовсе не существовало, дела возбуждались по смежным статьям кодекса, что осложняло преследование участников мошеннических схем. В то же время имеющееся законодательство, созданное для «аналогового» мира, не в полной мере учитывает современные технологические реалии. Оно плохо приспособлено к новым схемам виртуализации преступного пространства, QR-эквайрингу и деятельности компаний-дропов, не учитывает сложные сценарии легализации доходов и маскировки финансовых операций под легальный бизнес, что требует системного переосмысления и адаптации норм уголовного права к условиям цифровой эпохи. В частности, было бы правильно предусмотреть уголовную ответственность не только для исполнителей (дропперов), но и для организаторов мошеннических действий, владельцев компаний-дропов и финансовых посредников; признать в рамках УК РФ и УПК РФ цифровую валюту имуществом для усиления ответственности за реализацию схем незаконного обналичивания и кибервымогательства; существенно конкретизировать и разделить квалифицирующие признаки преступлений, совершаемых с применением ИИ, чтобы не осложнять работу законопослушных IT-специалистов и не создавать ситуаций правовой неопределенности. Вместе с тем стоило бы ввести прямую ответственность для банков и платежных агентов, не реагирующих на признаки незаконного обналичивания или игнорирующих уведомления регуляторов о подозрительных финансовых операциях; возложить на банки обязанности применять усиленные механизмы мониторинга и приостанавливать подозрительные операции, осуществляемые с использованием счетов физических лиц и корпоративных счетов.

[1] Антифрод-система – программно-аппаратный комплекс, предназначенный для выявления и блокировки мошеннических финансовых транзакций и защиты от кибератак.

Важными векторами совершенствования деятельности по обеспечению безопасности в рассматриваемой нами сфере являются разработка и внедрение инновационных банковских технологий, включая применение ИИ, биометрических и блокчейн-систем, а также расширение международного сотрудничества для борьбы с транснациональными криминальными схемами. В связи с этим необходимо институционализировать централизованные платформы совместного мониторинга и обмена информацией между банками, операторами платежных систем и государственными органами; усилить полномочия Росфинмониторинга и ЦБ РФ по временной блокировке подозрительных счетов и операций, обеспечить автоматическую реакцию на цифровые мошеннические схемы; ужесточить требования к идентификации клиентов при открытии счетов, особенно корпоративных: запретить их открытие без согласия представителей, ввести дополнительные проверки по MCC-кодам и типу бизнеса; реализовывать образовательные программы, ориентированные на повышение цифровой и финансовой грамотности населения, обучать правилам кибербезопасности в школах.

Эти меры позволят создать более устойчивую правовую основу для борьбы с современным дропперством, цифровым мошенничеством и финансовыми преступлениями, совершаемыми в новых технологических условиях. Ключевым же инструментом обеспечения безопасности финансовой системы становится проактивный подход, основанный на предиктивном анализе и превентивной защите.

Таким образом, комплексный междисциплинарный подход, предусматривающий и реформы законодательства, и технологические инновации, и международные договоренности, является необходимым условием для эффективного противодействия современному дропперству и поддержания экономической безопасности в условиях цифровизации финансового сектора. Только такая стратегия позволит минимизировать криминальные риски и обеспечить устойчивость легальной экономической деятельности. ■

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Пинкевич Т.В. Трансформация организованной преступности в условиях цифровизации // Право и управление. 2023. № 10. С. 464-469.

2. Иванов В.И. Темная сторона цифровизации российского общества: киберпреступность и ее вызовы // Вопросы безопасности. 2025. № 2. С. 14-26.

3. Михайлова Е.А. О необходимости уголовно-правового противодействия преступлениям в сфере незаконного оборота цифровых финансовых активов и цифровой валюты // Полицейская и следственная деятельность. 2025. № 1. С. 96-109.

4. Кисленко С.Л., Фокин А.Д. Мошенничество с использованием информационно-телекоммуникационных технологий как угроза национальной безопасности Российской Федерации // European and Asian Law Review. 2025. Т. 8. № 1. С. 41-54.

5. Попова А.В. Кибербезопасность банковской системы и этические правила взаимодействия человека с ИИ: к вопросу о необходимости сосуществования // Банковское право. 2021. № 1. С. 47-63.

6. Бабаев Э.А., Капустина Н.В. Современные риски использования новых финансовых технологий в схемах отмывания доходов и финансирования терроризма // Вестник евразийской науки. 2025. Т. 17. № s2.

7. Ущекин С.Н. Криминологическое предупреждение хищений, совершаемых с использованием электронных средств платежа: современное состояние и перспективы развития // Юридическая наука. 2025. № 4. С. 368-372.

8. Осипенко А.Л., Соловьев В.С. Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества // Всероссийский криминологический журнал. 2021. Т. 15. № 6. С. 681-691.

9. Орехова Е.А., Покровская В.Л. Риски применения цифровых технологий в экономике современной России // Вестник ВИЭПП. 2023. № 2. С. 49-62.

10. Петров А.А. Цифровизация экономики: проблемы, вызовы, риски // Торговая политика. 2018. № 3 (15). С. 9-31.

11. Петров А.А. Возможности и направления развития цифровой экономики в России и блокирующие факторы ее развития // Актуальные проблемы российского права. 2019. № 3 (100). С. 45-66.

12. Воскресенская Л.Н., Балашев Н.Б. Информационная безопасность в банковской сфере: тенденции развития и стратегия противодействия // Самоуправление. 2021. № 3 (125). С. 236-239.

13. Оганесян А.Г. Россия и глобальные вызовы в области информационной безопасности // Международная жизнь. 2018. № 14. С. 1-144.

14. Былевский П.Г. Эволюционная модель культуры информационной безопасности российских граждан // Журнал высоких гуманитарных технологий. 2025. № 2 (9). С. 6-14.

15. Катков С.В., Семененко Г.М., Костенко Н.С., Алексеева А.П. О мерах совершенствования организации работы оперативных и следственных подразделений МВД России по выявлению, раскрытию и расследованию хищений денежных средств с использованием банковских карт на территории Российской Федерации // Вестник Волгоградской академии МВД России. 2020. № 4 (55). С. 123-128.

**REFERENCES**

1. Pinkevich T.V. Transformatsiya organizovannoy prestupnosti v usloviyakh tsifrovizatsii // Pravo i upravleniye. 2023. № 10. S. 464-469.

2. Ivanov V.I. Temnaya storona tsifrovizatsii rossiyskogo obshchestva: kiberprestupnost' i yeye vyzovy // Voprosy bezopasnosti. 2025. № 2. S. 14-26.
3. Mikhaylova Ye.A. O neobkhodimosti ugolovno-pravovogo protivodeystviya prestupleniyam v sfere nezakonnogo oborota tsifrovykh finansovykh aktivov i tsifrovoy valyuty // Politseyskaya i sledstvennaya deyatel'nost'. 2025. № 1. S. 96-109.
4. Kislenko S.L., Fokin A.D. Moshennichestvo s ispol'zovaniyem informatsionno-telekommunikatsionnykh tekhnologiy kak ugroza natsional'noy bezopasnosti Rossiyskoy Federatsii // European and Asian Law Review. 2025. T. 8. № 1. S. 41-54.
5. Popova A.V. Kiberbezopasnost' bankovskoy sistemy i eticheskiye pravila vzaimodeystviya cheloveka s II: k voprosu o neobkhodimosti sosushchestvovaniya // Bankovskoye pravo. 2021. № 1. S. 47-63.
6. Babayev E.A., Kapustina N.V. Sovremennyye riski ispol'zovaniya novykh finansovykh tekhnologiy v skhemakh otmyvaniya dokhodov i finansirovaniya terrorizma // Vestnik yevraziyskoy nauki. 2025. T. 17. № s2.
7. Ushchekin S.N. Kriminologicheskoye preduprezhdeniye khishcheniy, sovershayemykh s ispol'zovaniyem elektronnykh sredstv platezha: sovremennoye sostoyaniye i perspektivy razvitiya // Yuridicheskaya nauka. 2025. № 4. S. 368-372.
8. Osipenko A.L., Solov'yev V.S. Osnovnyye napravleniya razvitiya kriminologicheskoy nauki i praktiki preduprezhdeniya prestupleniy v usloviyakh tsifrovizatsii obshchestva // Vserossiyskiy kriminologicheskiy zhurnal. 2021. T. 15. № 6. S. 681-691.
9. Orekhova Ye.A., Pokrovskaya V.L. Riski primeneniya tsifrovykh tekhnologiy v ekonomike sovremennoy Rossii // Vestnik VIEPP. 2023. № 2. S. 49-62.
10. Petrov A.A. Tsifrovizatsiya ekonomiki: problemy, vyzovy, riski // Torgovaya politika. 2018. № 3 (15). S. 9-31.
11. Petrov A.A. Vozmozhnosti i napravleniya razvitiya tsifrovoy ekonomiki v Rossii i blokiruyushchiye faktory yeye razvitiya // Aktual'nyye problemy rossiyskogo prava. 2019. № 3 (100). S. 45-66.
12. Voskresenskaya L.N., Balashev N.B. Informatsionnaya bezopasnost' v bankovskoy sfere: tendentsii razvitiya i strategiya protivodeystviya // Samoupravleniye. 2021. № 3 (125). S. 236-239.
13. Oganesyan A.G. Rossiya i global'nyye vyzovy v oblasti informatsionnoy bezopasnosti // Mezhdunarodnaya zhizn'. 2018. № 14. S. 1-144.
14. Bylevskiy P.G. Evolyutsionnaya model' kul'tury informatsionnoy bezopasnosti rossiyskikh grazhdan // Zhurnal vysokikh gumanitarnykh tekhnologiy. 2025. № 2 (9). S. 6-14.
15. Katkov S.V., Semenenko G.M., Kostenko N.S., Alekseyeva A.P. O merakh sovershenstvovaniya organizatsii raboty operativnykh i sledstvennykh podrazdeleniy MVD Rossii po vyyavleniyu, raskrytiyu i rassledovaniyu khishcheniy denezhnykh sredstv s ispol'zovaniyem bankovskikh kart na territorii Rossiyskoy Federatsii // Vestnik Volgogradskoy akademii MVD Rossii. 2020. № 4 (55). S. 123-128.

*Авторы заявляют об отсутствии конфликта интересов.*
*Авторами внесён равный вклад в написание статьи.*
*The authors declare no conflicts of interests.*
*The authors have made an equal contribution to the writing of the article.*


**ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ**
Алексеева А.П., Бугера Н.Н. Финансовая безопасность в условиях цифровой трансформации преступности: вызовы и механизмы системной защиты // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2025. № 4 (82). С. 9-17.