УДК 338.2 JEL O38 DOI: https://doi.org/10.26425/2309-3633-2025-13-3-52-63
Получено: 05.05.2025 Статья доработана после рецензирования: 11.07.2025 Принято: 20.07.2025

Цифровизация розничных платежей и развитие системы риск-менеджмента

Ларина Ольга Игоревна[1]
Канд. экон. наук, доц. каф. маркетинга
ORCID: 0000-0002-9841-8194, e-mail: oilarina@mail.ru

Кузнецова Валентина Вильевна[2]
Канд. ист. наук, доц. каф. мировой экономики и управления внешнеэкономической деятельностью
ORCID: 0000-0002-8698-4295, e-mail: vkuz_55@mail.ru

[1]Государственный университет управления, 109542, Рязанский пр-т, 99, г. Москва, Россия

[2]Московский государственный университет имени М.В. Ломоносова, 119991, Ленинские горы, 1, г. Москва, Россия

Аннотация

Цель – развитие подходов к риск-менеджменту в платежной сфере. Стремительная цифровизация платежей изменила структуру и качество платежных рисков. В ближайшее время сектор расчетно-платежных услуг будет сталкиваться с ростом уровней различных факторов риска, усилением регуляторного контроля и со значительными изменениями в мировых стандартах риск-менеджмента. Управление платежными рисками – современная и непростая задача, решение которой постоянно и динамично эволюционирует в силу трансформаций среды, инструментов платежей и поведения пользователей. Актуальным направлением развития риск-менеджмента в платежной сфере выступает построение системы упреждающего выявления мошенничеств. Использование передовых цифровых технологий и инструментов может позволить участникам платежных цепочек опережать возникающие угрозы. Анализируются системы быстрых платежей (далее – СБП) и сопутствующие им риски мошеннических действий. Применялись методы анализа, синтеза, обобщения, а также логический метод. Использованы опубликованные регуляторами данные о зафиксированных способах мошенничеств за последние 5 лет. Авторы приводят классификацию мошеннических действий в платежной сфере и отмечают применяемые методы выявления мошенничеств. На основе практического опыта использования российской СБП и системного анализа кейсов СБП других стран авторы предлагают направления совершенствования платежного риск-менеджмента. Результаты могут применяться в практике функционирования как платежных систем в целом, так и их отдельных участников.

Ключевые слова: цифровизация платежей, управление рисками, платежная система, мошенничества, риск-менеджмент, системы быстрых платежей, платежные риски, безопасность платежей

Для цитирования: Ларина О.И., Кузнецова В.В. Цифровизация розничных платежей и развитие системы риск-менеджмента// Управление. 2025. Т. 13. № 3. С. 52–63. DOI: 10.26425/2309-3633-2025-13-3-52-63

Received: 05.05.2025 Revised: 11.07.2025 Accepted: 20.07.2025

Digitalisation of retail payments and development of a risk management system

Olga I. Larina[1]
Cand. Sci. (Econ.), Assoc. Prof. at the Marketing Department
ORCID: 0000-0002-9841-8194, e-mail: oilarina@mail.ru

Valentina V. Kuznetsova[2]
Cand. Sci. (Hist.), Assoc. Prof. at the World Economy and Management of Foreign Economic Activity Department
ORCID: 0000-0002-8698-4295, e-mail: vkuz_55@mail.ru

[1]State University of Management, 99, Ryazansky prospekt, Moscow 109542, Russia

[2]Lomonosov Moscow State University, 1, Leninskie gory, Moscow 119991, Russia

Abstract

The purpose of the article is to develop approaches to risk management in the payment sector. The rapid digitalisation of payments has changed the structure and quality of payment risks. In the near future, the settlement and payment services sector will face increasing levels of various risk factors, enhanced regulatory control, and significant changes in global risk management standards. Payment risk management is a modern and challenging task, the solution of which is constantly and dynamically evolving due to transformations in the environment, payment instruments, and user behaviour. An urgent area of risk management development in the payment sector is the construction of a system for proactive fraud detection. The use of advanced digital technologies and tools can allow participants in payment chains to stay ahead of emerging threats. The article analyses fast payment systems (hereinafter referred to as FPS) and associated risks of fraudulent actions. Methods of analysis, synthesis, generalisation as well as the logical method are applied. The data published by regulators on recorded fraud ways over the past 5 years are used. The authors provide a classification of fraudulent activities in the payment sector and note the methods used to detect fraud. Based on the practical experience of using Russian FPS and system analysis of FPS cases from other countries, the authors propose ways to improve payment risk management. The results of the article can be applied in the practice of functioning of both payment systems as a whole and their individual participants.

Keywords: digitalisation of payments, management of risks, payment system, frauds, risk management, fast payment systems, payment risks, payment security

For citation: Larina O.I., Kuznetsova V.V. (2025). Digitalisation of retail payments and development of a risk management system. *Upravlenie / Management (Russia)*, 13 (3), pp. 52–63. DOI: 10.26425/2309-3633-2025-13-3-52-63

Введение / Introduction

В последние несколько лет розничные платежи стали важным направлением бизнеса для банков и финтех-компаний (финтех – финансовые технологии). Технологические инновации и усиление конкуренции среди поставщиков платежных услуг привели к увеличению количества вариантов доступа розничных клиентов к платежным услугам и улучшению качества их обслуживания. Однако обратной стороной данной тенденции стал рост рисков розничных платежей как для поставщиков, так и для пользователей.

Даже в том случае, если поставщики услуг розничных платежей точно соблюдают установленные стандарты безопасности и применяют необходимые технологии и техники (на уровнях оборудования и программного обеспечения (далее – ПО), все еще остаются разрывы между пользовательскими запросами на безопасность и теми условиями безопасности, которые предлагают поставщики услуг розничных платежей [Reichenbach, Grzebiela, Költzsch, Pippow, 2022]. Быстрые темпы обновления платежных продуктов, услуг, правил и технологий сопровождаются не менее быстрыми темпами изменений в методах мошенничеств, незаконного использования и нарушения безопасности конфиденциальных данных. Более того, поставщики инновационных способов платежа сталкиваются с теми же, а в ряде случаев и с бóльшими, рисками, что и провайдеры традиционных платежных методов. Мошенников особенно привлекают инновационные технологии (далее – ИТ), они их применяют, выявляя любые слабые места. Неспособность поставщиков инновационных и традиционных платежных услуг контролировать растущие риски может приводить к отказу пользователей от платежных инноваций [Merz, 2021].

Так, все платежные процессы сопряжены с рисками, которые клиентам и поставщикам услуг необходимо контролировать. Ограничивая доступ к платежным сетям, отслеживая соблюдение регуляторных стандартов снижения рисков и применяя штрафы за их несоблюдение, поставщики платежных услуг способны свести большую часть тех из них, что связаны с мошенничеством, незаконным использованием и нарушениями безопасности данных, к минимуму, но далеко не все. Для розничных платежей эти операционные риски являются преобладающими. Поставщики услуг розничных платежей в последнее время стали объектом разнообразных компьютерных атак, наносящих существенный ущерб всем участникам платежных цепочек. По данным Juniper Research, из-за финансовых мошенничеств в 2020–2023 гг. только поставщики онлайновых услуг электронной торговли, продаж авиабилетов, денежных переводов и банковских услуг в общем ежегодно теряли более 200 млрд долл. США [Vanini, Rossi, Zvizdic, Domenig, 2023].

В российской научной литературе анализ рисков платежных инноваций и применения соответствующих мер риск-менеджмента не получил должного освещения, в публикациях основное внимание уделяется анализу рисков цифровой трансформации экономики и центрального банка [Городнова, 2021; Хетагуров, Гаглоева, 2023; Криворучко, Ризванова, Бердышев, 2024]. В то же время в средствах массовой информации растет число сообщений, посвященных рискам мошенничеств, присущим системам быстрых платежей (далее – СБП)[1], а также соответствующих разъяснений банков, размещенных на их сайтах, о потенциальных угрозах, с которыми могут сталкиваться пользователи.

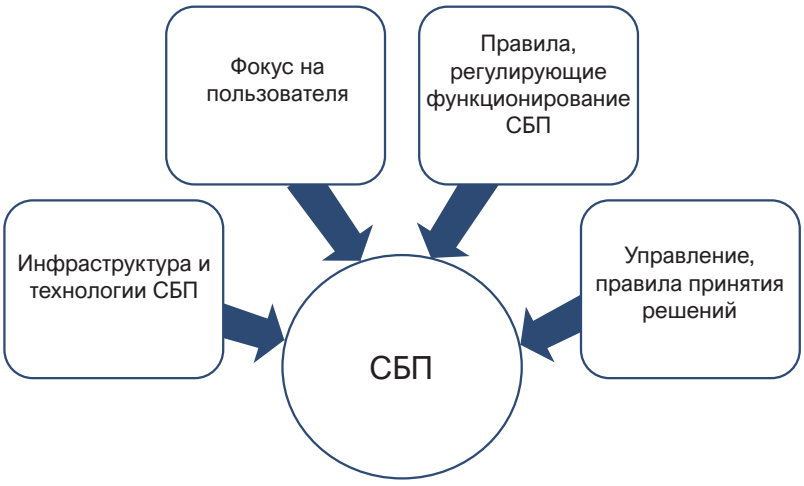
Целью статьи выступает развитие подходов к риск-менеджменту в платежной сфере, в связи с чем в настоящей работе исследуются новые риски, возникшие из-за цифровой трансформации платежных систем (анализируются СБП и розничные системы онлайн-оплаты), проводится их классификация, а также предлагаются способы их минимизации и перспективные направления риск-менеджмента.

Отличительные характеристики СБП / Distinctive characteristics of FPS

Платеж считается быстрым, если перевод сообщения и доступность средств для получателя происходят в режиме реального времени на круглосуточной основе (см. рисунок). Первая СБП была создана в Республике Корея в 2001 г. В настоящее время такие системы функционируют более чем в 100 юрисдикциях [Frost, Wilkens, Kosse, Shreeti, Velásquez, 2024].

В Российской Федерации (далее – РФ, Россия) благодаря развертыванию СБП в 2019 г. стало возможным осуществлять практически моментальный перевод денег (осуществлять платежи и переводить деньги со счетов в кредитных организациях на любые счета и банковские карты) получателю по номеру его мобильного телефона или QR-коду (англ. quick response – быстрый отклик). Косвенный доступ пользователей к СБП является персонифицированным, его предоставляют кредитные организации только клиентам-держателям карточного счета. СБП – это платежная система Центрального банка РФ (далее – ЦБ РФ),

[1] РИА Новости. Названа главная опасность быстрых платежей через СБП. Режим доступа: https://ria.ru/20240130/sbp-1924252885.html (дата обращения: 01.05.2025).



Составлено авторами по материалам исследования / *Compiled by the authors on the materials of the study*

Рисунок. Основные компоненты СБП
Figure. Main components of FPS

который выступает ее собственником, оператором и конечным расчетным центром [Кузнецова, Ларина, 2024].

По данным Национальной системы платежных карт, в 2024 г. россияне совершили 3,7 млрд оплат товаров и услуг на 6,5 трлн руб. через СБП[2]. Стремительный рост популярности СБП в России сопровождается также высокими темпами роста мошеннических операций и соответствующих убытков пользователей и поставщиков услуг быстрых платежей (по авторским оценкам, за 2024 г. число жалоб клиентов на мошеннические атаки увеличилось в 1,6 раза).

Риски, присущие СБП / Risks inherent in FPS

По статистике, около 60 % операционных сбоев в платежных системах приводят к общим потерям не менее 1 млн долл. США[3]. СБП, как и другим платежным системам, присущи несколько основных рисков: правовой, кредитный, операционный и риск утраты ликвидности. При этом особую значимость в последнее время обретают отдельные подвиды операционного риска – риски безопасности, в частности риск мошенничества (и связанный с ними репутационный риск), поскольку они воздействуют на доверие пользователей к розничным платежным услугам. Имеющаяся общая типология рисков мошенничества разграничивает их на два типа: неавторизированные и авторизованные («дружеские»), которые могут быть направлены на физические лица (далее – физлица), торговые компании, поставщиков платежных услуг и операторов платежных систем. Среди неавторизированных мошенничеств преобладают различные формы кибератак. Под кибератакам понимаются ситуации, когда мошенники пытаются украсть, изменить, отключить или уничтожить данные, приложения или другие активы посредством несанкционированного доступа к сети, компьютерной системе или устройству[4]. Они обычно направлены на утечку конфиденциальных данных (информации), необходимых для начала несанкционированного платежа либо инициирования своих операций, или на получение доступа к ним. Кибератаки могут принимать различные формы:

• целевые и непрерывные атаки на ИТ-инфраструктуру, в ходе которых мошенники неоднократно и в течение длительного периода времени пытаются получить доступ к ИТ-инфраструктуре. Их цели – использовать или получить данные, нанести ущерб системам процессинга, проникнуть в процессинговые системы для подмены параметров. Их объектами являются все участники платежной экосистемы: кредитные организации, операторы систем процессинга, платежных и любых иных систем (например, информационных) и поставщики технологических услуг;

• вредоносное ПО (троянские, шпионские, рекламные программы, троянские программы удаленного доступа, программы-вымогатели и др.). В рамках цепочек платежей цель мошенничества – получить коды, пароли, логины и т.п., чтобы присвоить учетные данные

[2] РИА Новости. В работе СБП произошел сбой. Режим доступа: https://ria.ru/20250214/sbp-1999506319.html (дата обращения: 01.05.2025).

[3] Stripe. Payments risk management 101: key components and best practices. Режим доступа: https://stripe.com/resources/more/payments-risk-management-101-key-components-and-best-practices (дата обращения: 01.05.2025).

[4] NIST Computer Security Resource Center. Cyber attack. Режим доступа: https://csrc.nist.gov/glossary/term/cyber_attack (дата обращения: 01.05.2025).

онлайн-банкинга и/или платежных приложений для доступа к информации, которую можно монетизировать;

• атаки «человек посередине». В этом случае мошенники тайно перехватывают сообщения и информацию и обмениваются ими с двумя сторонами, которые полагают, что общаются друг с другом напрямую. Так, получив контроль за устройством клиента, мошенники могут перенаправлять платеж. Данный вид может сочетаться с вредоносным ПО и иными угрозами;

• фишинг – это форма социальной инженерии, применение которой позволяет получить личную информацию пользователя посредством разных способов (например, через электронную почту или СМС (англ. short message service – служба коротких сообщений, далее – SMS). Фишинговые атаки становятся все более изощренными, переходя от заражения электронной почты и рассылки текстовых сообщений к другим каналам связи, а также таргетированными на конкретные группы пользователей, компаний;

• социальная инженерия. Мошенники используют данные технологии после получения доступа к личной информации пользователей платежных сетей, стремясь добиться их доверия и принудить клиента провести мошенническую операцию или раскрыть информацию для заключения подобной сделки. Цель технологий социальной инженерии – манипулирование поведением плательщиков;

• техники подмены личности. Мошенники могут выдавать себя за официальных лиц, работников банков или кредитных организаций, кадровых агентств, родственников и др. для получения нужной им информации и/или проведения операций;

• мошенничества, использующие QR-код. Мошенники могут манипулировать QR-кодами для получения информации пользователей (так называемый квишинг), перенаправлять людей на поддельные веб-сайты, заставлять их загружать файлы и/или приложения, зараженные вредоносными программами, или заменять исходную платежную информацию на платежные данные мошенника. В пункте продаж это может происходить при замене существующего QR-кода фальшивым, похожим на QR-код продавца. Несколько платежей могут быть инициированы до того, как продавец и/или клиент понимает, что QR-код является мошенническим. Эти методы становятся все более распространенным, поскольку такой способ оплаты получает большую популярность.

Внедрение и быстрое распространение СБП сопряжено, с одной стороны, со значительными выгодами для пользователей (прежде всего для физлиц и малого бизнеса), а с другой – с ростом и трансформацией различных рисков. Отдельные взаимосвязи между потенциальными выгодами СБП и порождаемыми ими рисками приведены в табл. 1.

Таблица 1

Ключевые особенности СБП и факторы, связанные с мошенничеством

Table. 1. Key features of SBP and fraud-related factors

Ключевые черты	Потенциальные выгоды	Возможности для мошенничества
Скорость	Средства доступны для бенефициара в течение нескольких секунд. Средства сразу зачисляются на банковский счет	Строгие правила СБП означают, что у провайдера платежных услуг и оператора СБП мало времени для проверки на случай мошенничества и комплаенса. Даже если преступление выявлено, крайне мало времени для реализации контрмер, так как деньги почти мгновенно зачисляются на счет получателя и он может распределить их по многим другим счетам
Постоянная доступность	Непрерывная доступность системы напоминает черты наличных денег. Увеличивает полезность для плательщика и получателя	Мошенники могут работать круглые сутки, особенно когда банки закрыты, то есть когда жертвы не в состоянии проверить свои счета
Конечность платежа	Придает большую безопасность платежу, так как он не может быть отозван. Позволяет улучшить денежный поток для компаний-получателей. Отсутствие комиссий делает быстрые платежи более привлекательными по сравнению с картами для электронной торговли / пунктов продаж	Деньги, украденные мошенниками со счета, трудно вернуть. К тому моменту, когда транзакция будет признана мошеннической, незаконно полученные средства могут уже исчезнуть со счета. Это затрудняет возврат утраченных средств
Высокие лимиты сделок	У многих СБП относительно высокие лимиты сделок, что может быть выгодно для их использования бизнесом. Чем выше лимит сделок, тем больше возможный круг пользователей СБП	Возможность отправки больших объемов средств по одной сделке делает СБП очень привлекательными для мошенников. Высокие лимиты сделок могут нести риски для национальной платежной системы

Составлено авторами по материалам источника[5] / *Compiled by the authors on the materials of the source*[5]

Разработка классификации мошенничеств важна для понимания их разных типов, поскольку конкретные типы требуют реализации различных мер противодействия. Например, методы многофакторной аутентификации помогают эффективно бороть-

[5] World Bank Group. Fraud risks in fast payments. Режим доступа: https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud%20in%20Fast%20Payments_Final.pdf (дата обращения: 01.05.2025).

ся с несанкционированным мошенничеством, но они не позволяют предотвратить санкционированное мошенничество. В табл. 2 представлены обзор и виды разных методов, обычно используемых для внедрения мошенничества.

Таблица 2

Классификация методов, применяемых для внедрения мошенничества

Table. 2. Classification of methods commonly used to introduce fraud

Методы мошенничества		
Кибератаки (вредоносные программы, атаки «человек посередине», фишинг и т.д.)		
Социальная инженерия		
Техники подмены личности		
Инсайдерские угрозы		
Методы, основанные на QR-кодах		
Мошеннические действия	**Примеры мошенничеств**	**Субъекты, в отношении которых направлена атака**
Неавторизированные	Кража личных данных и захват счета. Подмена SIM-карты. Разнообразные типы киберпреступлений	● ■ ● ● ■ ► ♦
Приложения авторизованного платежа в одно касание	Подмена личности. Мошенничество с текстовыми СМС-сообщениями. «Романтические» мошенничества. Мошенничества с расширенными комиссиями. Мошенничества с покупками. Мошенничества со счетами	● ■ ● ■ ● ■ ● ■ ● ■ ● ■
Санкционированные мошенничества		■

Составлено авторами по материалам источника[6] / *Compiled by the authors on the materials of the source*[6]

Примечание: преступники часто сочетают одновременное использование нескольких методов мошенничеств; SIM – subscriber identity module (англ. модуль идентификации абонента); ● – физлица; ■ – торговые и деловые компании; ►– финансовые институты и операторы процессинга; ♦ – операторы платежных систем

Постоянное совершенствование способов мошенничеств, использование злоумышленниками узких мест и/или «провалов» в ПО, применяемом поставщиками платежных услуг, равно как и в ИТ, значительно усложняют противодействия мошенничествам.

Текущие меры безопасности в платежных услугах / Current security measures in payment services

Управление платежными рисками включает комплекс методов и мер, применяемых провайдерами для выявления, оценки и снижения потенциальных рисков, связанных с обработкой и проведением платежей. Основная цель управления платежными рисками – защитить финансовые интересы и репутацию бизнеса, сохраняя при этом безопасный и удобный процесс оплаты для пользователей СБП.

Предотвращение мошенничеств в СБП часто рассматривается как бесконечная игра кошки с мышкой: мошенники используют новые методы, чтобы избежать своего выявления или обмануть жертв, в то время как участники платежных систем постоянно обновляют ПО, проводят образовательные кампании или вводят дополнительные правила для предотвращения мошеннической деятельности. Недопущение мошенничеств – сложная задача из-за большого числа потенциальных уязвимостей на каждом этапе платежной цепочки, требующих постоянного обновления методов их снижения и/или избегания, тогда как преступникам, как правило, нужен лишь один пункт подсоединения к платежной цепочке. Для предотвращения и снижения потенциальных убытков, вызванных мошенничествами, может использоваться комплекс различных мер, которые наиболее результативны при скоординированном применении.

Правила платежных схем СБП – необходимый инструмент для предотвращения мошенничеств и возврата украденных фондов. Установленные транзакционные лимиты (на величину и число сделок) позволяют оператору и поставщику услуг СБП проводить дальнейший анализ сделок, составлять отчет о мошенничествах для инфраструктурного оператора, реализовывать обязательное разрешение спорных ситуаций, при которых возникает подозрение о мошенничестве.

Лимиты сделок. Операторы СБП вправе устанавливать:

• лимиты на число сделок, которые может осуществить плательщик в течение определенного периода времени (дня, недели, месяца и т.п.). Они могут быть зафиксированы в правилах платежной системы либо установлены операторами платежных схем;

• лимиты на объем каждой сделки или на общий объем набора сделок, инициированных плательщиком в течение определенного периода времени. Когда ограничен объем индивидуальной транзакции или нескольких платежей, то ограничен и объем средств, которые могут быть украдены. В СБП разных стран, как правило, действуют свои лимиты на объем индивидуальной сделки. Так, в Соединенных Штатах Америки система Real-Time Payments ограничивает объем сделки в 1 млн долл. США, а европейская система SEPA Instant Credit Transfer – в 100 тыс. евро[7].

[6] World Bank Group. Fraud risks in fast payments. Режим доступа: https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud%20in%20Fast%20Payments_Final.pdf (дата обращения: 01.05.2025).

[7] World Bank Group. The future of fast payments. Режим доступа: https://fastpayments.worldbank.org/sites/default/files/2023-10/Future%20of%20Fast%20Payments_Final.pdf (дата обращения: 01.05.2025).

Хотя установка подобных лимитов позволяет снизить риски мошенничеств, она существенно уменьшает ценность СБП для пользователей, главным образом для малого бизнеса. В России лимиты на переводы существуют, но носят несколько иной характер[8]. Они связаны с бизнес-стратегией оператора СБП (ЦБ РФ). В настоящее время они составляют месячные лимиты переводов по СБП: ежемесячная сумма бесплатных переводов физлицам – 100 тыс. руб.; ежемесячная сумма переводов с комиссией – от 150 тыс. руб. Комиссия за перечисление сумм свыше 100 тыс. руб. – до 0,5 %. Подключенные к СБП банки вправе устанавливать ее самостоятельно, но итоговая сумма платы за один перевод не может быть более 1 500 руб. Действует также лимит на переводы самому себе, с одного счета на другой, максимальная необлагаемая комиссией сумма – до 30 млн руб. в месяц. Ограничения на перечисления в пользу юридических лиц, самозанятым и индивидуальным предпринимателям не установлены;

• требование получения согласия финансового института на проведение платежа. Оно может содержаться в договоре между финансовым институтом и оператором СБП. Если установленные требования не были соблюдены при отправке или получении платежной инструкции, то для финансового института и оператора платежной системы это служит сигналом возможного мошенничества. Однако введение подобного требования противоречит самой сути СБП.

Функционирование СБП не предполагает проведения проверок легитимности платежа, поэтому перед поставщиками платежных услуг стоят задачи автоматизации таких процессов, как проверка соблюдения требований законодательства и санкционных ограничений [Dobler, Garrido, Grolleman, Khiaonarong, Nolte, 2021]. Однако их решение осложнено отсутствием необходимых структурированных данных, без наличия которых возможны ложные сигналы о потенциальных мошенничествах. Для преодоления данного противоречия предлагается введение в правила СБП задержки исполнения платежной инструкции, если у поставщика есть подозрения о возможном мошенничестве, в целях, например, изучения характера платежа. В частности, в Мексике правила СБП SPEI устанавливают, чтобы поставщики услуг быстрых платежей автоматизировали такие процессы. В СБП Бразилии Pix уведомляет отправителей, когда их транзакции приостановлены[9].

Отчеты о мошенничестве оператору СБП. Для эффективного функционирования защитного ПО требуется значительный объем данных. Хотя операторы СБП имеют доступ к данным уровня платежной инструкции, они не знают, какие сделки являются легитимными, а какие – мошенническими. Введение в соглашение между оператором СБП и поставщиком платежных услуг требования об обязательном уведомлении обо всех выявленных случаях мошенничеств позволяет несколько смягчить указанное противоречие. Более того, оператор СБП может взять на себя разработку и поддержание ПО по борьбе с мошенничеством для участников платежной системы.

Обязательные механизмы разрешения споров. Важны для предотвращения и разрешения случаев мошенничества. Они содержат четкие руководящие принципы в отношении ответственности потребителей, обеспечивая общие механизмы отчетности, и помогают стандартизировать механизмы восстановления списанных преступниками средств. Большинство норм состоит из трех компонентов: структурированный канал сообщений, позволяющий потребителям начать процесс разрешения конфликта как можно раньше; установленный набор руководящих принципов относительно ответственности и механизм компенсации ущерба. Каждый из них важен и помогает предотвращать формирование порочных стимулов для обеих сторон, например, в случае санкционированного («дружеского») мошенничества и отсутствия компенсации от финансового института за легитимное мошенничество [Mallekoote, Balraadjsing, 2022].

Централизованные решения предотвращения мошенничеств. В последние годы операторы СБП стали чаще применять централизованные решения предотвращения мошенничеств. В отдельных случаях такие системы оценивают транзакции и оповещают отправителя и получателя. В других случаях операторы обмениваются информацией, сочетающей требования об уведомлении пользователей о мошеннических транзакциях и предложения о дополнительной защите. Хотя системы, отслеживающие денежных мулов (денежный мул – это лицо, получающее и перемещающее деньги жертв мошенничества; одни знают, что помогают преступной деятельности, другие же не знают, что их действия играют на руку преступникам) [10], не могут остановить мошеннические транзакции, они помогают вернуть средства и выявить более крупные сети, занимающиеся кражей и отмыванием денег.

[8] Система быстрых платежей. Лимиты переводов по СБП. Режим доступа: https://sbp.nspk.ru/blog/limity-perevodov-po-sbp?utm_source=google.ru&utm_medium=organic&utm_campaign=google.ru&utm_referrer=google.ru (дата обращения: 01.05.2025).

[9] World Bank Group. The future of fast payments. Режим доступа: https://fastpayments.worldbank.org/sites/default/files/2023-10/Future%20of%20Fast%20Payments_Final.pdf (дата обращения: 01.05.2025).

[10] Consumer Financial Protection Bureau. What is a money mule? Режим доступа: https://www.consumerfinance.gov/ask-cfpb/what-is-a-money-mule-en-2108/ (дата обращения: 01.05.2025).

Мошенничество и скоринг риска. Операторы СБП «видят» все входящие и исходящие платежи, и, следовательно, имеют более полное представление о каждой конкретной транзакции, чем отправляющая или принимающая стороны. Интеллектуальная система оценки, управляемая оператором СБП, может оповестить отправителя и получателя платежа о мошенничестве. Например, операторы СБП Индии и Южной Африки централизовали возможности по выявлению мошенничеств.

Обмен информацией. Помимо предложения решений по оценке мошенничества, ряд операторов СБП поддерживают платформы обмена информацией. Такие платформы предлагают широкий спектр различных услуг, включая возможность сообщать о подозреваемых преступниках и потенциально мошеннических транзакциях. Хотя два типа решений теоретически различны, они совместимы и часто предлагаются одновременно. Новая платежная платформа Австралии включает контур службы обмена данными, как и система Iberpay в Испании. Другим примером является система FPAD (англ. freight payable at destination – фрахт оплачивается в пункте назначения), созданная EBA Clearing (англ. European Banking Authority Clearing System – система клиринга Европейского банковского управления) в Еврозоне и запущенная в марте 2024 г. (в настоящее время к системе присоединилось 50 участников)[11].

Выявление счетов денежных мулов. Они используются мошенниками для отправки и получения платежей. В Великобритании VocaLink/Mastercard было разработано решение Mule Insights (далее – MITS) для выявления счетов денежных мулов[12]. Система оценивает и использует данные локальной системы и СБП для отслеживания перемещения средств между счетами. MITS использует алгоритмы нейронных сетей для выявления подозрительных денежных мулов, поставщиков услуг и отслеживает средства по мере их поступления.

Аутентификация на основе рисков. Базируется на применении транзакционных данных (например, местоположения, устройства, профиля пользователя, шаблонов входа в систему и др.) для аутентификации клиента. Информация служит входными данными для оценки уровня риска, которую можно использовать для выявления рискованных транзакций или сделок с низким уровнем риска и при необходимости запуска дополнительных мер безопасности. В Мексике регулятор обязал провайдеров учитывать геолокацию пользователя для разрешения доступа к услугам онлайн-банкинга.

Подтверждение платежа. Рост мошенничеств с приложениями заставил регуляторов вмешиваться, требуя предоставления отправителями платежей дополнительных данных при одновременном сохранении их конфиденциальности. Великобритания первой ввела требование подтверждения получателем платежа для крупных банков, и в настоящее время оно становится все более популярным. В последние несколько лет различные платежные сервисы на основе зашифрованных личных данных (номер телефона и/или электронная почта, так называемый псевдоним) начали делиться определенной информацией о получателе с отправителями.

Помимо выгод для плательщиков, подобная система нуждается в защите от преступлений. Например, преступник может попытаться добыть каталоги псевдонимов, чтобы получить личную информацию, а затем использовать ее для совершения других видов мошенничества. В CoDi в Мексике существует обязательный период охлаждения, в течение которого недавно добавленные псевдонимы, привязанные к банковскому счету, не могут быть оплачены.

Цифровые ID. Услуги цифровых ID (англ. identifier – идентификатор) также все больше используются для аутентификации отправителей быстрых платежей. Использование цифрового ID с биометрической информацией (сканирование лица, отпечатка большого пальца, сканирование радужной оболочки глаза и т.д.) применяется часто, но не всегда. Такие системы (BankID в Швеции и Норвегии, It's Me в Бельгии, SAVI в Мексике, iDIN в Нидерландах, Aadhaar в Индии) следят за тем, чтобы лицо, инициирующее платеж, было лицом уполномоченного совершить его. Эти услуги безопасности опираются на тесное межотраслевое сотрудничество, но сложны в применении[13].

Новые направления риск-менеджмента в СБП / New directions of risk management in FPS

Государственное регулирование. Устанавливает обязательные стандарты для финансовых организаций и правила СБП, что обеспечивает дополнительную защиту конечных пользователей и создает возможности для тестирования новых технологий. Технологии и правила СБП имеют большое значение для предотвращения, обнаружения и отслеживания мошенничества

[11] EBA Clearing. Why FPAD? Режим доступа: https://www.ebaclearing.eu/services-fraud-fighting/fpad/why-fpad/ (дата обращения: 01.05.2025).

[12] QuadCorps. Mule insights. Режим доступа: https://quadcorps.co.uk/mule-insights/ (дата обращения: 01.05.2025).

[13] World Bank Group. The future of fast payments. Режим доступа: https://fastpayments.worldbank.org/sites/default/files/2023-10/Future%20of%20Fast%20Payments_Final.pdf (дата обращения: 01.05.2025).

по мере его распространения по платежной системе. В ряде случаев регуляторы требуют от финансовых организаций наличия механизмов борьбы с мошенничеством, интегрированных в их системы обработки платежей (например, Pix в Бразилии), обязательного использования таких инструментов, как IBAN (англ. International Bank Account Number – международный номер банковского счета), Name Check (Европейский союз (далее – ЕС), или применения периодов охлаждения при добавлении новых получателей (CoDi в Мексике).

Во многих странах регуляторы стали требовать от кредитных организаций предоставления информации (отчетности) о выявленных мошенничествах. Централизованное накопление данных позволяет сопоставлять, анализировать и распространять информацию о преступных схемах среди всех участников СБП. В других странах потери от мошенничества побудили регуляторов и/или платежные сообщества ввести распределение убытков между кредитными организациями и потребителями СБП. В Великобритании любые убытки, связанные с платежными мошенничествами, должны быть разделены напополам между отправляющим и получающим поставщиком платежных услуг (схема возмещения убытков в Великобритании стала действовать с октября 2024 г.)[14]. Целью этого является создание стимула для всех игроков делать все возможное для предотвращения мошенничеств, как санкционированных, так и несанкционированных.

Во всех юрисдикциях растущей тенденцией становится развитие общих систем отчетности о мошенничествах. Например, орган денежного регулирования Сингапура сообщил о разработке COSMIC[15], безопасной цифровой платформе (поддерживающей регуляторные требования), позволяющей финансовым институтам обмениваться информацией о клиентах, демонстрирующих несколько «красных флажков» при выполнении определенных условий. COSMIC – централизованная платформа, позволяющая обмениваться данными в структурированном формате и определяющая, как и когда следует делиться конкретной информацией.

Рост фишинга и кибератак сделали небезопасными логины, основанные только на имени и паспорте. Поставщики услуг СБП озабочены поиском наилучших вариантов аутентификации пользователей до начала платежа. Это может быть реализовано с помощью разных компонентов и принимать множество форм. В EC Revised Payment Services Directive (PSD2) обязывает поставщиков платежных услуг при платеже на сумму сверх 30 евро использовать два из трех возможных вариантов аутентификации:

- данные паспорта или PIN-код (англ. personal identification number – персональный идентификационный номер);
- устройство, привязанное к пользователю;
- биометрические данные (отпечаток большого пальца, сканирование лица и т.п.).

Однако такой подход не является надежным, как показывают мошеннические практики подмены SIM-карт (например, перенос телефонного номера на новую SIM-карту, контролируемую мошенниками для перехвата одноразовых паролей, отправленных для аутентификации пользователя). В Мексике, Пакистане, Великобритании поставщики услуг обязаны применять многофакторный подход к аутентификации для разных типов сделок.

Использование новых технологий сопряжено с необходимостью поддержания непрерывности функционирования и может оказаться затруднительным при рассмотрении таких вопросов, как конфиденциальность данных, соблюдение строгих правил платежных соглашений и разработка программируемых приложений интерфейсов. В Индии, например, правительство создало регуляторную песочницу, которая позволяет поставщикам платежных услуг P2P (англ. peer-to-peer – от персоны к персоне) тестировать новые технологии [Shabsigh, Khiaonarong, Leinonen, 2020]. Она предназначена для разработки мер противодействия кибератакам. Использование песочниц помогает поставщикам платежных услуг тестировать разработки, выявлять недостатки, вводить исправления и пробовать новые технологии. Подобные меры гораздо сложнее реализовывать без среды тестирования.

Межотраслевые инициативы. Правила, технологии и регулирование платежных схем не являются единственными в противодействии мошенникам: также применяются базы данных преступников, межотраслевое сотрудничество и кампании по повышению осведомленности о мошенничестве, обучение конечных пользователей. Операторы СБП могут участвовать в обмене информацией между участниками платежных цепочек. Это реализуется в форме оповещений и обеспечивает обмен информацией в режиме реального времени или в форме вызываемой базы данных, в которой хранятся и обновляются данные о мошенниках. Ею могут управлять оператор СБП или регулирующий орган, банковская ассоциация, платежная

[14] A&O Shearman. The UK's authorised push payment (APP) fraud reimbursement scheme. Режим доступа: https://www.aoshearman.com/en/insights/ao-shearman-on-fintech-and-digital-assets/the-uks-authorised-push-payment-app-fraud-reimbursement-scheme (дата обращения: 02.05.2025).

[15] Monetary Authority of Singapore. COSMIC. Режим доступа: https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic (дата обращения: 02.05.2025).

ассоциация и т.д. Например, в Бразилии участники обязаны предоставлять отзывы о мошеннических транзакциях в Pix. Это также относится к мошенническим подменам псевдонимов, которые включены в списки наблюдения, или черные списки. В Нидерландах, Нигерии и Японии есть формы баз данных преступников, что помогает противодействию мошенничествам. Какова фактическая форма базы данных, кто имеет доступ к ней, как получаются данные базы – важные вопросы, определяющие ее полезность.

В ряде стран проводятся образовательные кампании, повышающие осведомленность пользователей о конкретном типе мошенничества (например, в Нидерландах). В Великобритании кампания «Получите 5, чтобы остановить мошенничество» нацелена на информирование общества о различных мошенничествах, включая те из них, что связаны с платежными приложениями. Образование должно носит постоянный характер. Мошенничество – это проблема не только финансовой отрасли: бизнес и физлица ежедневно страдают от фишинга и кибератак. В некоторых случаях, таких как мошенничество с подменой SIM-карт, используются уязвимости, имеющие последствия для конечных пользователей финансовых услуг. Когда люди звонят в компании со своего телефона, им часто задают ряд вопросов для подтверждения их личности. На такие вопросы часто относительно легко ответить, используя информацию, полученную при сканировании аккаунтов в социальных сетях или посредством взлома чьей-то электронной почты. Это означает, что, за исключением какого-либо цифрового удостоверения личности или персонального общения, взаимодействия, сотрудникам телекоммуникационных компаний сложно быть на 100 % уверенным, с кем они говорят. Использование цифрового ID для проверки личности звонящего помогает решить эти проблемы. Другой вариант (Нигерия) – пометить маркером данный номер в каталоге, если номер телефона, привязанный к банковскому счету, перенесен на новую SIM-карту. Третий вариант (Великобритания) заключается в том, чтобы телекоммуникационные компании блокировали мошеннические SMS-идентификаторы.

Ключевые компоненты эффективной стратегии управления платежными рисками. Управление платежным риском требует одновременного использования нескольких взаимосвязанных методов. Наиболее часто применяются следующие.

1. Передовые цифровые технологии для раннего выявления мошенничеств (использование машинного обучения и искусственного интеллекта для анализа данных транзакций). Эти системы должны быть обучены на больших наборах данных для обнаружения тонких и сложных моделей мошеннической деятельности, которые более простые системы, основанные на правилах, могут не заметить, и спроектированы так, чтобы адаптироваться и развиваться по мере того, как преступники меняют свои методы.

2. Поведенческая аналитика позволяет отслеживать, как пользователи обычно взаимодействуют с платежными системами. Любое отклонение от этих закономерностей может быть отмечено для дальнейшего расследования. Это включает время транзакций, частоту, отпечатки пальцев, устройства, а также скорость или шаблоны набора текста.

3. Анализ данных в реальном времени оценивает уровень риска каждой транзакции на основе текущих и исторических данных. Такие системы должны включать статические правила (например, запрет транзакции выше определенной суммы) и динамические модели, которые адаптируются к меняющимся закономерностям в данных.

4. Безопасная токенизация и шифрование. Передовые методы шифрования и токенизации защищают данные при хранении и передаче. Токенизация заменяет конфиденциальные элементы данных неконфиденциальными эквивалентами, которые можно безопасно хранить и использовать, не раскрывая значения данных.

5. Провайдеры должны управлять доступом к платежным системам с помощью надежных протоколов аутентификации, чтобы только авторизованный персонал имел доступ к конфиденциальным информации и системам.

6. Проведение углубленного анализа платежных связей. Такой анализ изучает связи между транзакциями в различных системах и сетях для выявления цепочек подозрительной активности. Это помогает раскрыть сложные схемы мошенничества, в которых участвуют несколько сторон или в которых атака осуществляется из нескольких локаций.

7. Использование регуляторных технологий для управления и автоматизации контроля за соблюдением финансовых требований, действующих в различных юрисдикциях. Такие решения помогают вести мониторинг и составлять отчеты в режиме реального времени, снижая риски и затраты на соблюдение требований.

8. Передовые меры кибербезопасности. Современные инструменты прогнозного моделирования и количественной оценки киберрисков демонстрируют потенциальные финансовые последствия различных киберсобытий и могут служить ориентиром для упреждающих инвестиций в кибербезопасность.

9. Сетевое взаимодействие – общеотраслевые сети для совместной работы, обмена информацией о тенденциях развития мошеннических методов и защитных тактиках, а также создание общей

аналитической платформы, обеспечивающей доступ к более широкому набору данных.

10. Прогнозное моделирование. Такие модели позволяют оценивать вероятность будущего мошенничества на основе исторических данных, моделей поведения и информации о внешних угрозах, а также заранее отмечать транзакции с высоким уровнем риска для дальнейшего расследования.

11. Платформы интегрированного управления рисками обеспечивают целостное представление о рисках в платежной системе, сопоставляя различные типы и оценивая их взаимозависимости.

12. Присвоение числовых значений различным факторам риска на основе их вероятности и потенциального воздействия на базе данных стресс-тестирования и количественного анализа. Это помогает расставить приоритеты в распределении ресурсов и сосредоточить внимание на наиболее вероятных из них.

13. Качественный анализ рисков учитывает такие факторы, как репутационный ущерб, связанный с конкретным риском, возможность проверки со стороны регулирующих органов и влияние на доверие клиентов.

14. Сканирование и аудит комплаенса гарантируют, что участники платежной системы соблюдают соответствующие правила и стандарты, положения внутренней политики и процедуры.

Таким образом, следование четкой и последовательной тактике риск-менеджмента позволяет выявлять и оценивать многие риски.

Заключение / Conclusion

Выделим наиболее актуальные и перспективные направления и компоненты платежного риск-менеджмента:

• внутренний анализ данных: изучение исторических данных транзакций с точки зрения закономерностей, указывающих на мошенничество (необычные объемы транзакций, резкие скачки возвратных платежей или аномалии в поведении клиентов). Использование алгоритмов машинного обучения помогает выявлять корреляции и тенденции, которые могут быть неочевидны при проверке вручную;

• использование данных об угрозах из надежных источников позволяет учитывать новые тенденции мошенничества, новые векторы атак и уязвимостей в платежной системе. Такая информация нужна для превентивной корректировки моделей риска и мер безопасности;

• регулярная оценка/переоценка рисков с учетом изменений в бизнес-среде, новых технологий и возникающих угроз;

• мониторинг ключевых индикаторов, таких как уровень мошенничества, коэффициенты возвратных платежей и уровень ложных срабатываний, чтобы измерить эффективность стратегий управления рисками и разработать необходимые корректирующие меры;

• применение комплексных систем, классифицирующих различные типы платежных рисков: мошеннические, операционные, системные и риски комплаенса; их систематическое изучение для выявления потенциальных уязвимостей;

• использование сетевого анализа для понимания взаимосвязей между различными участниками платежного процесса в целях выявления сложных схем мошенничества, в которых участвуют несколько взаимосвязанных сторон, например сговор или отмывание денег;

• проведение моделирования и стресс-тестов для оценки возможности функционирования платежной системы в экстремальных условиях – в условиях технических сбоев и сложных кибератак. Это позволяет выявлять потенциальные точки сбоя в аппаратных и программных системах;

• сценарный анализ и анализ последствий для понимания влияния различных рисковых событий. Разработка подробных сценариев эволюции потенциальных рисков и моделирование их финансовых последствий позволит ранжировать риски по вероятности материализации и степени возможного воздействия на платежную систему;

• внедрение сложных инструментов оценки кибербезопасности, способных анализировать состояние безопасности платежной системы в режиме реального времени. Подобные инструменты способны оценивать уязвимости, тестировать на вероятность проникновений и выявлять уязвимости нулевого дня.

Последствия плохого риск-менеджмента в платежных системах могут быть серьезными, поэтому важно учитывать риск на каждом этапе – от регистрации клиента в СБП до завершения платежной транзакции.

СПИСОК ЛИТЕРАТУРЫ

Городнова Н.В. Анализ рисков и безопасности системы электронных средств платежа. Экономическая безопасность. 2021;2(4):401–420. https://doi.org/10.18334/ecsec.4.2.111691

Криворучко С.В., Ризванова И.А., Бердышев А.В. Развитие системы быстрых платежей Банка России в современных условиях. Вестник университета. 2024;8:163–174. https://doi.org/10.26425/1816-4277-2024-8-163-174

Кузнецова В.В., Ларина О.И. Управление рисками расчетных и платежных систем. М.: КноРус; 2024. 272 с.

Хетагуров Г.В., Гаглоева Э.Н. Система быстрых платежей: возможности, факторы роста и риски. Вестник Томского государственного университета. Экономика. 2023;62:72–84. https://doi.org/10.17223/19988648/62/6

Dobler M.C., Garrido J.M., Grolleman D.J., Khiaonarong T., Nolte J. E-money. Prudential supervision, oversight, and user protection. Washington: International Monetary Fund; 2021. 34 p.

Frost J., Wilkens P.K., Kosse A., Shreeti V., Velásquez C. Fast payments: design and adoption. BIS Quarterly Review. 2024.

Mallekoote P.M., Balraadjsing S.K. Oversight and risk management of payments schemes. Journal of Risk Management in Financial Institutions. 2022;4(15):418–428.

Merz M. Contemporaneous financial intermediation. How DLT changes the cross-border payment landscape. Digital Finance. 2021;3:25–44. https://doi.org/10.1007/s42521-021-00029-3

Reichenbach M., Grzebiela T., Költzsch T., Pippow I. Individual risk management for digital payment systems. Computational Economics. 2022.

Shabsigh G., Khiaonarong T., Leinonen H. Distributed ledger technology experiments in payments and settlements. Washington: International Monetary Fund; 2020. 22 p.

Vanini P., Rossi S., Zvizdic E., Domenig Th. Online payment fraud: from anomaly detection to risk management. Financial Innovation. 2023;66(9). https://doi.org/10.1186/s40854-023-00470-w

REFERENCES

Gorodnova N.V. Risk and security analysis of the electronic payment system. Economic Security, 2021;2(4):401–420. (In Russian). https://doi.org/10.18334/ecsec.4.2.111691

Dobler M.C., Garrido J.M., Grolleman D.J., Khiaonarong T., Nolte J. E-money. Prudential supervision, oversight, and user protection. Washington: International Monetary Fund; 2021. 34 p.

Frost J., Wilkens P.K., Kosse A., Shreeti V., Velásquez C. Fast payments: design and adoption. BIS Quarterly Review. 2024.

Khetagurov G.V., Gagloeva E.N. Fast payment system: opportunities, growth factors and risks. Tomsk State University Journal of Economics. 2023;62:72–84. (In Russian). https://doi.org/10.17223/19988648/62/6

Krivoruchko S.V., Rizvanova I.A., Berdyshev A.V. Development of the Bank of Russia's fast payment system in modern conditions. Vestnik universiteta. 2024;8:163–174. (In Russian). https://doi.org/10.26425/1816-4277-2024-8-163-174

Kuznetsova V.V., Larina O.I. Risk management of settlement and payment systems. Moscow: KnoRus; 2024. 272 p. (In Russian).

Mallekoote P.M., Balraadjsing S.K. Oversight and risk management of payments schemes. Journal of Risk Management in Financial Institutions. 2022;4(15):418–428.

Merz M. Contemporaneous financial intermediation. How DLT changes the cross-border payment landscape. Digital Finance. 2021;3:25–44. https://doi.org/10.1007/s42521-021-00029-3

Reichenbach M., Grzebiela T., Költzsch T., Pippow I. Individual risk management for digital payment systems. Computational Economics. 2022.

Shabsigh G., Khiaonarong T., Leinonen H. Distributed ledger technology experiments in payments and settlements. Washington: International Monetary Fund; 2020. 22 p.

Vanini P., Rossi S., Zvizdic E., Domenig Th. Online payment fraud: from anomaly detection to risk management. Financial Innovation. 2023;66(9). https://doi.org/10.1186/s40854-023-00470-w