УДК 336.77.067.22
DOI: 10.34020/1993-4386-2024-2-61-66

К ВОПРОСУ О БЕЗОПАСНОСТИ БАНКОВСКИХ ПЛАТЕЖЕЙ В СОВРЕМЕННОЙ РОССИЙСКОЙ ПРАКТИКЕ

Д. С. Панина
Оренбургский государственный университет,
Оренбург, Россия

Взаимодействие банковского сектора с внешней средой (не всегда благоприятной) определяет возможность появления новых угроз, финансовых потерь и, как следствие, необходимость применения инструментария для обеспечения безопасности банковских платежей. Его развитие является приоритетной задачей для банковского сообщества и входит в сферу интересов каждого участника расчетно-платежного сегмента.

В данной публикации проведен динамический и факторный анализ числа и объема мошеннических операций с денежными средствами клиентов банков. Снизить их число представляется возможным благодаря совместным действиям IT-специалистов и сотрудников служб безопасности банков, операторов связи, правоохранительных органов, регулятора. Для достижения большей эффективности в вопросе защиты клиентских средств следует применять весь арсенал имеющихся в распоряжении способов, начиная от самых простых, таких как обучение навыкам обеспечения собственной безопасности, и заканчивая сложными научно-методическими и технологическими способами.

Ключевые слова: кибермошенничество, безопасность платежей, социальная инженерия, фишинговые атаки.

Введение

Одним из наиболее значимых и ценных ресурсов в современном мире является информация. Именно она привлекает сегодня разного рода злоумышленников, вызывая их преступный интерес. Огромный массив конфиденциальной личной и финансовой информации содержится в информационных системах банков. Нарушение безопасности такой информации может привести к невосполнимым потерям – от массового несанкционированного списания денежных средств со счетов банковских клиентов до серьезных сбоев в работе всей банковской системы. Поэтому обеспечение защиты банковской информации и конфиденциальности клиентской базы – один из ключевых вопросов, стоящих перед всем банковским сообществом.

Статистика последних лет подтверждает неумолимый рост популярности безналичных платежей (общемировой прирост в течение последних 10 лет – около 14,2 % [1]). В Российской Федерации их доля также продолжила уверенный рост и по итогам 2023 г. достигла уровня 83,4 %[1]. Столь стремительное расширение зоны безналичных платежей определяет закономерный рост рисков информационной безопасности. Они могут быть спровоцированы как самим владельцем счета (осознанная или неосознанная передача данных по счетам третьим лицам), так и быть независимыми от его действий или бездействий (хакерские атаки, перехват трафика и прочее). Поэтому крайне важной задачей является их своевременное выявление с целью дальнейшего совершенствования способов и технологий обеспечения безопасности платежей.

Необходимость детального исследования и постоянного мониторинга рисков, возникающих в сфере банковских платежей, отмечают в научных трудах такие российские исследователи, как: С. К. Абрамян [2], Е. В. Бочкарева [3], Ю. А. Васильева [4], М. Е. Горчакова [5] и другие. Поиском новых методов и способов минимизации новых угроз и их возможных последствий в национальной экономике занимаются С. Ф. Джалилова [6], В. С. Канхва [7], А. В. Карагодин [8], А. С. Обухова [9] и другие. Серьезность вопросов обеспечения реальной защищенности платежей отмечается и органами государственного регулирования отечественного банковского сектора (Положения Банка России № № 762-П[2],

[1] Цифровизация платежей и внедрение инноваций на платежном рынке. Аналитический доклад. – М.: Центральный банк Российской Федерации, 2024. – 46 с. URL: https://cbr.ru/Content/Document/File/161600/analytical_report_20240605.pdf (дата обращения: 28.06.2024).

[2] Положение Банка России от 29 июня 2021 г. № 762-П (ред. от 03.08.2023) «О правилах осуществления перевода денежных средств».

802-П[3], 821-П[4], 719-П[5], ГОСТ Р 57580.1-2017[6], Основные направления развития информационной безопасности кредитно-финансовой сферы[7] и др.).

Эта проблема актуальна не только для российской практики, она не осталась незамеченной и в зарубежной литературе. Необходимость тщательного анализа всех банковских переводных операций и выявления возможных рисков (как в контексте мошеннических операций, кибератак, так и с целью предотвращения легализации денежных средств или иного имущества, приобретенных другими лицами преступным путем) отмечают такие зарубежные исследователи, как Пьер-Лоран Шатен, Джон Макдауэл, Седрик Муссе, Пол Аллан Шотт, Эмиль ван дер Дус де Вильбуа [10], Питер Вайл, Стефани Ворнер [11] и другие. Трансформация систем риск-менеджмента, динамичное развитие платежной инфраструктуры, постоянно увеличивающийся поток переводных банковских операций, появление новых видов угроз на рынке платежей обусловливают необходимость продолжения аналитической работы на данном сегменте.

Результаты исследования

Вопросы безопасности банковских платежей волнуют не только кредитно-финансовые организации и их клиентов, они являются одними из наиболее острых и значимых для мегарегулятора – Банка России. В контексте этого вопроса особое внимание уделяется, во-первых, возможности существенного снижения вероятности несанкционированного списания средств со счетов банковских клиентов [12] и, во-вторых, обеспечению сохранности денежных средств в процессе перевода их по счетам [13]. В первом случае ответственность за потерю денежных средств может нести как сам владелец счета (если платеж прошел по его волеизъявлению, даже если речь идет о злонамеренном введении его в заблуждение со стороны третьих лиц или получении от него реквизитов счета любым мошенническим способом), так и банк (в случае, если потеря денежных средств со счета связана с хакерской атакой, которую кредитной организации не удалось нейтрализовать, или с перехватом злоумышленниками трафика). Во втором случае при несоблюдении сохранности платежей ответственность будут нести банки и операторы платежной системы, которые обязаны отслеживать и устранять любые уязвимости системы, реализовывать технологии защиты клиентских средств от несанкционированных списаний, обеспечивать защиту трафика. Обе эти проблемы чаще всего связаны с действиями (попытками) третьих лиц, заинтересованных в краже не принадлежащих им средств.

За период 2020–2023 гг. в сегменте платежей очевиден рост числа мошеннических операций с денежными средствами, совершенных без согласия клиентов (ОБС) – в 1,6 раза и пропорциональное их увеличение по объему (табл. 1).

Таблица 1

Динамика операций без согласия клиентов в сегменте платежей за период 2020–2023 гг.*

Показатели	2020 г.	2021 г.	2022 г.	2023 г.	Изменения за 2020–2023 гг., %
Количество ОБС, *тыс. ед.*	180,3	256,2	288,8	291,5	61,6
Объем ОБС, *млн руб.*	2 506,6	3 206,5	3 591,1	3 947,9	57,5
Доля социальной инженерии, %	64	41	54,1	31,6	49,3
Доля возмещенных (возвращенных) средств (от объема), %	13,1	7,7	3,4	5,5	41,9
Количество предотвращенных ОБС, *тыс. ед.*	10 266	10 654	10 701	10 788	5,1
Объем предотвращенных ОБС, *трлн руб.*	0,98	1,23	1,48	1,68	71,4

* Составлено автором на основе статистических данных Банка России[8].

[3] Положение Банка России от 25 июля 2022 г. № 802-П (ред. от 25.07.2022) «О требованиях к защите информации в платежной системе Банка России» (вместе с «Правилами материально-технического обеспечения формирования электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре участника обмена при осуществлении переводов денежных средств в платежной системе Банка России с использованием сервиса срочного перевода и сервиса несрочного перевода, а также правила материально-технического обеспечения обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре операционного центра, платежного клирингового центра другой платежной системы при предоставлении операционных услуг и услуг платежного клиринга при переводе денежных средств с использованием сервиса быстрых платежей»).

[4] Положение Банка России от 17 августа 2023 г. № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

[5] Положение Банка России от 4 июня 2020 г. № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

[6] ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (утв. и введен в действие Приказом Росстандарта от 08.08.2017 г. № 822-ст).

[7] Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов (одобрены Советом директоров Банка России 22.05.2023).

[8] Подробнее см. «Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств» за первый квартал 2023 г., размещенный Банком России 31 мая 2023 г. URL: https://cbr.ru/statistics/ib/review_1q_2023/ (дата обращения: 28.06.2024).

При этом к 2022 г. заметно постепенное снижение темпов роста мошеннических действий в сегменте банковских платежей как по объему, так и по числу. Этот факт может быть объяснен тем, что на фоне резкого ухудшения геополитической обстановки, усиления санкционного давления со стороны стран Европы и США, с российского рынка «ушли» основные операторы международных платежных систем. Это привело к общему снижению числа расчетов, а следовательно, и к сокращению возможностей преступных действий в их отношении. Помимо этого, причастным к снижению темпов роста киберпреступлений в сегменте платежей является и мегарегулятор.

Статистика свидетельствует о том, что наибольшее число операций без согласия клиентов до недавнего времени приходилось на оплату товаров и услуг в Интернете (48 % в 2021 г.). Однако постепенно активность киберпреступников в этом сегменте снизилась и устремилась в сектор дистанционных банковских сервисов (так, если на долю ОБС при оплате товаров и услуг в Интернете в 2023 г. приходилось 34,5 %, то на долю ОБС в ходе дистанционного банковского обслуживания – уже 46 %). Доступ к этим операциям позволяет мошенникам не только распорядиться не принадлежащими им средствами с банковских счетов по своему усмотрению, но и оформить на клиентов банка кредит и получить его. Поэтому больше всего угроз в 2023 г. было в дистанционном банковском обслуживании, а потери составили 9,3 млрд рублей [13].

Также стоит отметить, что если рассматривать количество фактов мошеннических действий третьих лиц при выполнении физическими лицами всех остальных типов операций, то самыми значительными в 2023 г. стали мошеннические действия с платежными картами: их доля по числу приблизилась к отметке 85 %, а по объему – к отметке 47 %. При этом доля возмещенных (возвращенных) клиентам денежных средств в этом случае оказалась чрезмерно низкой и составила около 4 %, в то время как возврат средств, списанных в результате мошеннических действий третьих лиц в результате оплаты товаров и услуг в Интернете, составила порядка 28 %.

В сфере расчетов и платежей юридических лиц львиная доля ОБС также, как и в случае с расчетами физических лиц, приходится на дистанционное банковское обслуживание и переводы (91 % – по числу и 96 % – по объему). Однако стоит отметить растущий интерес бизнеса за последние 2 года и к расчетам через систему быстрых платежей (СБП), что связано с подключением к ней все большего числа банков (на начало 2024 года в нее вошли все 13 системно значимых банков, а также еще 194 из 324 банков). С учетом значимых преимуществ СБП, – эта тенденция, безусловно, будет развиваться и дальше.

Нельзя обойти вниманием и тенденцию к методичному сокращению доли возмещенных средств (с 11,9 % в 2020 г. до 4,3 % в 2023 г.). Столь незначительный уровень возмещения объясняется сохранением достаточно высокой доли применения мошенниками социальной инженерии (31,6 % в 2023 г.)[9]. В этом случае владельцы счетов самостоятельно (сознательно или неосознанно) раскрывают киберпреступникам личную финансовую информацию или переводят им денежные средства, при этом последующее возмещение (возвращение) средств банком становится невозможным. К аналогичным уловкам с применением возможностей социальной инженерии мошенники прибегают в социальных сетях и мобильных приложениях.

При этом следует обратить внимание на тот факт, что доля социальной инженерии постепенно сокращается – за исследуемый период она сократилась в 2 раза. Это происходит благодаря росту информированности населения о возможных киберпреступлениях и повышению уровня киберграмотности граждан, а также совместной работе Банка России, финансовых организаций, операторов связи и правоохранительных органов.

Также благодаря их совместным усилиям удается удерживать количество предотвращенных операций без согласия клиентов примерно на одном уровне – за период 2020–2023 гг. наблюдается небольшой рост (на 5 %) по числу и значительный (на 71,4 %) – по объему. Так, в результате сотрудничества Банка России с операторами связи в 2023 г. была инициирована блокировка более 900 тысяч телефонных номеров мошенников, что в 4,5 раза больше, чем годом ранее. Этот показатель является максимальным с начала такой работы в 2019 г. Аналогичная работа ведется и по социальным сетям – в том же 2023 г. было заблокировано более 1900 фейковых страниц и 122 тысячи фишинговых ресурсов.

Итак, очевидно, что разработка технологий обеспечения безопасности является приоритетной задачей для всего банковского сообщества и входит в сферу интересов каждого участника расчетно-платежного сегмента. При этом, как было сказано выше, угрозы могут быть как спровоцированными самим владельцем счета (осознанная или неосознанная передача данных по счетам третьим лицам), так и независимыми от его действий или бездействий (хакерские атаки, перехват трафика и проч.). Следовательно, способы и технологии защиты денежных средств могут отличаться в зависимости от видов возникающих угроз.

Самым простым способом защиты от мошенничества является обучение владельцев платежных средств и инструментов простым, но эффективным навыкам обеспечения собственной безопасности: контроль за сохранностью банковской карты и сим-карты, привязанной к номеру банковского счета (в случае их потери – немедленная блокировка); неразглашение личной финансовой информации (особенно в социальных сетях); осуществление заказов и их оплата только на проверенных Интернет-ресурсах; установка на компьютер и телефон сервисов защиты от спама и нежелательных вызовов.

Кроме таких простых методов, безусловно, используются и технологические средства. Банки (так же, как и операторы платежных систем) обязаны обеспечить защиту денежных средства клиентов, находящихся на счетах или в процессе перевода, от незаконных, мошеннических списаний или автоматического изменения адресата платежа. К мерам

[9] Там же.

по обеспечению безопасности функционирования платежных систем относят:

– применение специальных программных комплексов для предотвращения мошеннических транзакций (так называемые антифрод-системы) [14];

– использование электронно-цифровой подписи с несколькими уровнями защищенности, а также детализированной процедуры авторизации и идентификации участников переводной операции;

– использование различных, усложненных криптографических алгоритмов для надежного шифрования потоков информации, а также обеспечение безопасной передачи данных по защищенным каналам;

– безопасное, защищенное от несанкционированного доступа третьих лиц оборудование и программное обеспечение;

– безопасная, охраняемая территория, охраняемые помещения, арсенал документов;

– резервное копирование и возможность восстановления информации.

При этом следует помнить и об обеспечении внутренней информационной безопасности, что также является крайне необходимой мерой для того, чтобы защитить конфиденциальность данных от обычной халатности. Эта работа включает в себя проведение инструктажей сотрудников, имеющих доступ к банковским данным клиентов, контроль за выполнением соответствующих регламентов.

В целях обеспечения сохранности средств на карточных счетах, а также безопасности совершаемых платежей с использованием банковских карт активно внедряются технологии типа SmartVista и 3D Secure. Они способны нейтрализовать усилия мошенников, намеревающихся осуществить перехват номера платежной карты и последующее списание денежных средств. Также банки реализуют новейшую технологию использования биометрических данных клиентов (на сегодняшний день они уже доступны в онлайн-банкинге ПАО Сбербанк, АО «Т-Банк» (до 5 июня 2024 г. – АО «Тинькофф Банк»), ПАО «МТС-Банк» и других банков) и предлагают клиентам использовать виртуальные банковские карты вместо пластиковых. Массовое и повсеместное внедрение подобных технологий существенно расширит возможности безопасного приобретение товаров и услуг в режиме онлайн, позволит максимально снизить риски возникновения мошенничества. Кроме того, банки совместно с финтех-компаниями продолжают работу по усовершенствованию технологий контактной и бесконтактной оплаты [15].

В решении вопроса обеспечения безопасности банковских платежей значимое место принадлежит регулятору и его нормативно-правовым инициативам, которые способствуют усилению мер противодействия мошенникам.

Так, например, с 1 апреля 2024 года были представлены обновленные требования к обеспечению защиты информации при осуществлении денежных переводов. В частности, в новом Положении № 821-П установлены требования к защите информации для такого субъекта национальной платежной системы, как оператор электронной платформы (ему вменяется проведение ежегодного тестирования на предмет наличия возможности проникновения в инфраструктуру и анализ уязвимостей; проведение оценки соответствия защиты информации; применение программного обеспечения, прошедшего сертификацию и др.)[10].

Цель противодействия мошенникам реализуется и посредством внесения поправок в Федеральный закон от 27 июня 2011 г. № 161-ФЗ (ред. от 24.07.2023) «О национальной платежной системе». Они призваны решить проблему добровольной передачи владельцем счета личной финансовой информации злоумышленникам. Так, с 1 июля 2024 г. банки могут приостанавливать мошеннические операции сроком на 2 дня даже в случае их подтверждения клиентом. Также они обязаны будут отключить дистанционное обслуживание подозреваемого мошенника. При этом признаки мошенничества одновременно будут выявлять как банк отправителя платежа, так и банк его получателя. Все случаи реализации мошеннических схем будут передаваться в единую базу, и в случае подтверждения банком перевода в пользу субъекта, состоящего в данной базе, он будет обязан возместить клиенту всю сумму в течение 30 дней.

В целом за последние годы отмечается тенденция к ужесточению политики Банка России в контексте вопроса обеспечения безопасности различных систем, включая систему платежей. И если ранее предлагаемые им меры по защите финансовых и информационных потоков носили рекомендательный характер, то сейчас он требует от организаций финансового сектора обязательного их исполнения, вплоть до внесения изменений в нормативно-правовые документы. Например, в настоящее время банки обязаны в первые три часа после зафиксированной хакерской атаки сообщить о ней в Центр взаимодействия и реагирования Департамента информационной безопасности Банка России (ФинЦЕРТ). Ранее такой обязанности не существовало, более того, банки опасались «обнародования» такого рода информации из-за страха репутационных рисков и нежелания уплаты штрафов за несоблюдение требований безопасности и правил корпоративного поведения. Кроме того, значительно ужесточились меры воздействия на банки за несоблюдение требований мегарегулятора: от значительных по сумме штрафов (он может составить до 1 % от уставного капитала банка) вплоть до полного отключение финансовой организации-нарушителя от системы банковских платежей[11].

Уже на протяжении 10 лет действуют закрепленные в Стандарте Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС-1.0–2014) обязательные требования технического характера: подключенный к системе компьютер должен быть отключен от локальной сети банка, а компьютер, отправляющий платежи на корреспондентский счет Банка России на обработку должен постоянно мониториться для выявления несанкционированного вмешательства в программное обеспечение или подключения к сторонним серверам. Соблюдение этих требований позволило пресечь преступные

[10] Система денежных переводов. URL: https://www.banki.ru/wikibank/sistema_denejnyih_perevodov/ (дата обращения: 28.06.2024).

[11] Статистика национальной платежной системы. URL: https://cbr.ru/statistics/nps/psrf/ (дата обращения: 25.06.2024).

замыслы третьих лиц, усилить как внутреннюю, так и внешнюю информационную безопасность.

Также Банк России разработал механизм борьбы с угрозой использования мошенниками номеров телефонов банковских клиентов: Национальная система платежных карт регулярно мониторит поток осуществляемых платежей и запускает процесс блокировки в системе телефонных номеров, с которых осуществляются подозрительные поручения или массовая рассылка СМС, информируя при этом и банки.

Заключение

Благодаря имеющемуся опыту, сформированным навыкам гибкого регулирования и реагирования на новые вызовы и угрозы со стороны киберпреступников, у Банка России, тесно сотрудничающего с ведущей в сфере IT российской компанией АО «ФИНТЕХ», есть уникальная возможность в кратчайшие сроки осваивать новые технологии обеспечения безопасности платежей, применять передовые и эффективные инструменты борьбы с мошенничеством [15]. Очевидно, что ключевыми факторами развития в ближайшем будущем станут дальнейшее продвижение искусственного интеллекта, внедрение инструментов для быстрой и безопасной передачи данных между разными финансовыми и другими организациями – так называемый открытый банкинг, или OpenAPI, развитие гибких, надежных и в то же время открытых биллинговых систем, использование возможностей технологии блокчейн, продолжение совершенствования технологий кибербезопасности и др. Таким образом, можно сказать, что на современном этапе экономического развития России совершенствование технологий обеспечения безопасности банковских платежей является одной из первоочередных задач. Эффективность, безопасность и привлекательность внедряемых сервисов вкупе с высокой рентабельностью бизнеса позволяют сегменту банковских платежей успешно развиваться, привлекая новых клиентов. За счет успешного внедрения новаций российский рынок в ближайшее время сможет составить конкуренцию лидерам мирового рынка по обеспечению безопасности банковских платежей.

Литература

1. *Wei H., Grigor'ev V. N.* Problems and ways to optimize the use of payment cards in the banking system to increase profits // Economics: Yesterday, Today and Tomorrow. 2023. Т. 13, № 2-1. С. 153–166. DOI: 10.34670/AR.2023.70.47.012

2. *Абрамян С. К., Газизулина И. А.* Развитие современных форм и технологий банковского обслуживания // Идеи и идеалы. 2022. Т. 14, № 1–2. С. 247-260. DOI: 10.17212/2075-0862-2022-14.1.2-247-260

3. *Бочкарева Е. В.* К вопросу о кибербезопасности интернет-банкинга // Вестник Волжского университета им. В. Н. Татищева. 2023. Т. 2, № 1 (51). С. 196–203. DOI: 10.51965/2076-7919_2023_2_1_196

4. *Васильева Ю. А.* Драйверы роста качества банковских продуктов и услуг // Банковские услуги. 2020. № 3. С. 15–28. DOI:10.36992/2075-1915_2020_3_15

5. *Горчакова М. Е.* Цифровизация банковской системы России: современные тенденции // Экономика: вчера, сегодня, завтра. 2022. Т. 12, № 4-1. С. 386–392. DOI: 10.34670/AR.2022.48.84.002

6. *Джалилова С. Ф., Абдулмуслимова Д. Т.* Информационные технологии в сфере банковских услуг // Вестник Московского гуманитарно-экономического института. 2020. № 3. С. 93–102. DOI: 10.37691/2311-5351-2020-0-3-93-102

7. *Канхва В. С., Ниязбекова Ш. У., Галеев К. Ф.* Цифровые платежи и цифровизация банковского сектора на рынке финтех // Управленческий учет. 2022. № 7-1. С. 60–67. DOI: 10.25806/uu7-1202260-67

8. *Карагодин А. В.* Некоторые аспекты цифровизации банковской сферы // Финансовая экономика. 2020. № 7. С. 56–62

9. *Обухова А. С., Казаренкова Н. П.* Перспективы развития платежных услуг российских банков в условиях цифровизации экономики // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2023. Т. 11, № 3. С. 147–158.

10. *Шатен П.-Л., Макдауэл Дж., Муссе С., Шотт П. А., ван дер Дус де Вильбуа Э.* Предотвращение отмывания денег и финансирования терроризма. Практическое руководство для банковских специалистов. – М.: Альпина Паблишер, 2021. – 316 с.

11. *Вайл П., Ворнер С.* Цифровая трансформация бизнеса: изменение бизнес-модели для организации нового поколения. – М.: Альпина Паблишер, 2019. – 264 с.

12. *Цвырко А. А., Сухорукова Н. В., Иващенко Т. Н.* Адаптация банковского бизнеса к современным цифровым трендам // Естественно-гуманитарные исследования. 2022. № 41 (3). С. 372–381.

13. *Зубов С. А.* Обзор платежных систем в первой половине 2023 года // Экономическое развитие России. Т. 30, № 9. С. 33–37.

14. *Копнин А. А., Соколова Е. В., Долгополов А. А.* Методика обеспечения безопасности банковских интернет-транзакций на основе антифрод системы // International Journal of Professional Science. 2022. № 10. С. 149–157. DOI: 10.54092/25421085_2022_10_149

15. *Мансурова А. Ч.* Основные тенденции развития банковских инноваций и новые тренды в сфере банковских технологий // Известия ВУЗов Кыргызстана. 2021. № 1. С. 76–82. DOI: 10.26104/IVK.2019.45.557

Сведения об авторе

Панина Дарья Сергеевна – кандидат экономических наук, доцент, доцент кафедры банковского дела и страхования, Оренбургский государственный университет, Оренбург, Россия.
ResearcherID: XTO-8544-2023;
AuthorID: 781328;
ORCID: 0000-0001-9035-7860;
E-mail: darpanina2015@yandex.ru

ON THE ISSUE OF THE SECURITY OF BANK PAYMENTS IN MODERN RUSSIAN PRACTICE

D. Panina
Orenburg State University,
Orenburg, Russia

The interaction of the banking sector with the external environment (which is not always favorable) determines the possibility of new threats, financial losses and, as a result, the need to use tools to ensure the security of bank payments. Its development is a priority task for the banking community and falls within the sphere of interests of each participant in the settlement and payment segment. In this publication, a dynamic and factor analysis of the number and volume of fraudulent transactions with bank customers' funds is carried out. It is possible to reduce their number thanks to the joint actions of IT specialists and employees of the security services of banks, telecom operators, law enforcement agencies, and the regulator. To achieve greater efficiency in protecting client funds, the entire arsenal of available methods should be used, starting from the simplest, such as training in self-security skills, and ending with complex scientific, methodological and technological methods.

Keywords: cyber fraud, payment security, social engineering, phishing attacks.

References

1. Wei H., Grigor'ev V. N. Problems and ways to optimize the use of payment cards in the banking system to increase profits, Economics: Yesterday, Today and Tomorrow. 2023, Vol. 13, No. 2-1, pp. 153–166. DOI: 10.34670/AR.2023.70.47.012

2. Abramyan S. K., Gazizulina I. A. Development of modern forms and technologies of banking services, *Idei i idealy*, 2022, Vol. 14, No 1-2, pp. 247–260. (In Russ.).

3. Bochkareva E. V. On the issue of cybersecurity of Internet banking, *Vestnik Volzhskogo universiteta im. V. N. Tatishcheva*, 2023, Vol. 2, No. 1 (51), pp. 196-203. DOI: 10.51965/2076-7919_2023_2_1_196 (In Russ.).

4. Vasil'eva Yu. A. Drivers of growth in the quality of banking products and services, *Bankovskie uslugi*, 2020, No. 3, pp. 15-28. (In Russ.). DOI: 10.36992/2075-1915_2020_3_15

5. Gorchakova M. E. Digitalization of the Russian banking system: current trends, *Ekonomika: vchera, segodnya, zavtra*, 2022, Vol. 12, No. 4-1, pp. 386-392. (In Russ.). DOI: 10.34670/AR.2022.48.84.002

6. Dzhalilova S. F., Abdulmuslimova D. T. Information technologies in the field of banking services, *Vestnik Moskovskogo gumanitarno-ekonomicheskogo instituta*, 2020, No. 3, pp. 93-102. (In Russ.). DOI: 10.37691/2311-5351-2020-0-3-93-102

7. Kankhva V. S. Niyazbekova Sh. U., Galeev K. F. Digital payments and digitalization of the banking sector in the fintech market, *Upravlencheskii uchet*, 2022, No 7-1, pp. 60-67. (In Russ.). DOI: 10.25806/uu7-1202260-67

8. Karagodin A. V. Some aspects of digitalization of the banking sector, *Finansovaya ekonomika*, 2020, No. 7, pp. 56-62. (In Russ.).

9. Obukhova A. S., Kazarenkova N. P. Prospects for the development of payment services of Russian banks in the context of digitalization of the economy, *Izvestiya Yugo-Zapadnogo gosudarstvennogo* universiteta, Seriya: Ekonomika. Sotsiologiya. Menedzhment, 2023, Vol. 11, No. 3, pp. 147-158. (In Russ.).

10. Shaten P.-L., Makdauel Dzh., Musse S., Shott P. A., van der Dus de Vil'bua E. *Predotvrashchenie otmyvaniya deneg i finansirovaniya terrorizma. Prakticheskoe rukovodstvo dlya bankovskikh spetsialistov* [Prevention of money laundering and terrorist financing. A practical guide for banking professionals], Moscow: Al'pina Pablisher, 2021, 316 p. (In Russ.).

11. Vail P., Vorner S. Tsifrovaya transformatsiya biznesa: izmenenie biznes-modeli dlya organizatsii novogo pokoleniya [Digital business transformation: changing the business model for a new generation of organizations], Moscow: Al'pina Pablisher, 2019, 264 p. (In Russ.).

12. Tsvyrko A. A., Sukhorukova N. V., Ivashchenko T. N. Adapting the banking business to modern digital trends, *Estestvenno-gumanitarnye issledovaniya*, 2022, No. 41 (3), pp. 372-381 (In Russ.).

13. Zubov S. A. Overview of payment systems in the first half of 2023, *Ekonomicheskoe razvitie Rossii*, Vol. 30, No. 9, pp. 33-37 (In Russ.).

14. Kopnin A. A., Sokolova E. V., Dolgopolov A. A. A methodology for ensuring the security of online banking transactions based on an anti-fraud system, *International Journal of Professional Science*, 2022, No. 10, pp. 149-157. (In Russ.).

15. Mansurova A. Ch. The main trends in the development of banking innovations and new trends in the field of banking technologies, *Izvestiya VUZov Kyrgyzstana*, 2021, No. 1, pp. 76-82. (In Russ.).

About the author

Darya S. Panina – Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Banking and Insurance, Orenburg State University, Orenburg, Russia.
ResearcherID: XTO-8544-2023;
AuthorID: 781328;
ORCID: 0000-0001-9035-7860;
E-mail: darpanina2015@yandex.ru