УДК 336.71:346.548(470+571)
DOI: 10.34020/1993-4386-2024-3-28-33

УГРОЗЫ БЕЗОПАСНОСТИ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ В СОВРЕМЕННОЙ РОССИЙСКОЙ ПРАКТИКЕ

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

Среди прочих отраслей российской экономики банковский сектор является одним из наиболее динамично развивающихся. Следовательно, его устойчивость к различным потрясениям и возможным угрозам будет являться одной из центральных точек опоры экономической безопасности государства. Современная статистика свидетельствует о росте различного рода инцидентов в финансовой сфере. Регулярный мониторинг и детальный анализ мошеннических схем позволят минимизировать возможности преступных манипуляций, тем самым значительно снизить число рисков и объем финансовых потерь.

В представленной статье проведен структурный и географический анализ инцидентов в финансовой сфере, зафиксированных в 2023 году, и составлен эскиз современного ландшафта возможных угроз. Оптимальный подход к формированию информационной и экономической безопасности личных и финансовых данных в частности, и банковской деятельности в целом, предполагает комплексные меры защиты, как с точки зрения индивидуального пользователя, так и с позиции представителей банковского сообщества и регулятора.

Ключевые слова: кибермошенничество, угрозы безопасности, DDoS-атаки, фишинг атаки.

Введение

Экономическая безопасность национальной экономики формируется исходя из реалий функционирования всех ее отраслей. Следовательно, экономическая безопасность одного из наиболее динамично развивающихся секторов – банковского – становится одной из центральных точек ее опоры. Значимость банковского сектора для экономики подчеркивается и в Стратегии национальной безопасности Российской Федерации[1], а его дальнейшее технологическое и функциональное развитие трактуется как ключевой показатель не только экономической, но национальной безопасности государства.

В современных условиях наиболее острыми и актуальными являются вопросы обеспечения безопасности банковских платежей, переводов, сохранности клиентских денежных средств на счетах, что обусловлено ростом преступности в этой сфере. Различные манипуляции мошенников в финансовом секторе, включая кибератаки, составляют около 20 % от всего объема мошеннических действий в мире [1]. В начале 2024 года Всемирный экономический форум опубликовал очередной отчет о глобальных рисках «The Global Risks Report 2024»[2], в котором мошенничество в сфере денежного обращения, включая кибермошенничество, было признано составной частью глобального технологического риска. Задачи подобных «нападений» сводятся к нарушению целостности и непрерывности работы банковского сектора (потеря денежных средств участниками банковского рынка, нарушение непрерывности цикла оказания услуг банками, неустойчивость и банкротство, системный кризис), а также к нанесению финансового ущерба экономике и обществу в целом (подрыв доверия к финансовой системе, к государству как к регулятору, социальное напряжение).

Вопросами экономической и информационной безопасности национальной экономики в целом и банковского сектора в частности в разные годы занимались отечественные ученые Л. И. Абалкин [2], В. К Сенчагов [3], М. А. Гуреева [4], А. Е. Городецкий [5], И. В. Караваева [6] и другие. Значимость вопросов выявления новых угроз и необходимость усиления мер безопасности банковской деятельности отмечается в научных работах А. С. Виноградовой [7], С. В. Мамонтовой [8], Е. А. Ягуповой [9], В. О. Одинцова [10] и др. Над поиском эффективных мер по выявлению и минимизации последствий новых угроз в работе банков в условиях цифровизации российской экономики работают И. А. Зарипов [11], Г. Я. Казакова [12], Н. В. Тарасова [13], О. И. Тимофеева [14], Н. В. Фадейкина [15] и другие.

[1] Указ Президента РФ от 2 июля 2021 г. № 400 «Стратегии национальной безопасности Российской Федерации».

[2] The Global Risks Report 2024. URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (дата обращения: 19.07.2024).

«Новый этап развития информационной безопасности в кредитно-финансовой сфере наступил после одобрения Советом директоров Банка России 22 мая 2023 г. обновленных "*Основных направлений развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов*" (одобрены Советом директоров Банка России 22.05.2023), где были подведены итоги реализации Основных направлений 2019–2021 и определено содержание таких новых направлений развития информационной безопасности в КФС на период 2023–2025, как:

1) "защита прав потребителей финансовых услуг и повышение уровня доверия к цифровым технологиям (в том числе: а) противодействие совершению операций без согласия клиентов, социальной инженерии; б) противодействие компьютерным атакам; в) финансовая киберграмотность)";

2) "создание условий для безопасного внедрения цифровых и платежных технологий и обеспечения технологического суверенитета (в том числе: а) развитие регулирования; б) развитие национальной платежной инфраструктуры и цифровой рубль; в) экспериментальные правовые режимы и регулятивная «песочница»; г) технологический суверенитет)";

3) "обеспечение контроля рисков ИБ, операционной надежности для непрерывности оказания банковских и финансовых услуг (в том числе: а) RegTech- и SupTech-проекты[3]; б) киберучения; в) риск-профилирование (Банк России продолжит практику формирования риск-профиля поднадзорных организаций для оценки фактических рисков информационной безопасности и операционной надежности); г) аутсорсинг информационных технологий и использование облачных сервисов)"» [15].

Современная статистика свидетельствует о неумолимом росте различного рода инцидентов в финансовой сфере. Так, в течение 2023 года через Автоматизированную систему обработки инцидентов (АСОИ ФинЦЕРТ) было зафиксировано более тысячи актов мошенничества[4], что вдвое больше, чем было выявлено годом ранее. Это говорит о пристальном внимании преступников к данной отрасли, внедрении инновационных тактик, техник и инструментов кражи не принадлежащих им денежных средств, личной (персональные и учетные данные), в том числе и финансовой информации (данные банковских карт, состояние счетов).

Постоянный мониторинг и детальный анализ мошеннических схем в финансовой сфере со стороны всех заинтересованных лиц (владельцев счетов, финансово-кредитных институтов, регулятора, представителей научной общественности), а также открытость и публичность такого рода информации, позволят «выбить почву из-под ног» мошенников, минимизировать возможности для их манипуляций, тем самым значительно снизить число рисков и объем финансовых потерь.

Результаты исследования

Итак, обратимся к статистике инцидентов в финансовой сфере, зафиксированных ФинЦЕРТ[5] в 2023 году, что позволит составить эскиз современного ландшафта возможных угроз. Наибольший удельный вес приходится на так называемые DDoS-атаки (компьютерные атаки типа «распределенный отказ в обслуживании», основной целью которых является нарушение доступности финансовых услуг и сервисов) – 41,2 %. Столь высокое значение данного типа угрозы объясняется простотой ее реализации (злоумышленникам не требуется глубокой технической подготовки) и доступностью данных (доступы к ботнетам продаются, а иногда и безвозмездно раздаются на хакерских форумах). Хакеры активно применяли комплексные атаки, а также ботнеты, состоящие из нескольких вредоносных программ. На глобальном уровне произошел всплеск DDoS-атак на DNS-сервера, что создало большие проблемы для организаций. Однако, стоит отметить, что число DDoS-атак в 2023 году в России сократилось по сравнению с предыдущим периодом на беспрецедентные 68 %. Эксперты-оптимисты считают, что такое сокращение может быть объяснено снижением активности политически мотивированных хактивистов в последнее время, а также развитием навыков предотвращения базовых видов DDoS-атак путем оснащения инфраструктуры адекватными средствами защиты (к примеру, при приобретении услуги anti-DDoS). Пессимистическая экспертная позиция основывается на том, что на смену более простым инструментам DDoS-атак пришли новые, усовершенствованные (с внедрением нейросетей, способных имитировать поведение человека, его голос и даже внешность); активность хактивистов перетекла в более сложные, утонченные и, самое главное, скрытые формы атак (такие как внедрение троянов, шифровальщиков). Злоумышленники все чаще прибегают к методам социальной инженерии, позволяющей значительно нарушить защищенность конфиденциальной информации, а в некоторых случаях – полностью остановить деятельность организации на какое-то время.

Как уже говорилось ранее, в целях минимизации последствий такого рода атак в банковском

[3] В ходе мероприятий по развитию RegTech- и SupTech- проектов планируется реализовать совершенствование системы внешнего аудита информационной безопасности. Обеспечение качества оценки соответствия защиты информации в организациях кредитно-финансовой сферы определено в составе инициативы в рамках *Основных направлений развития технологий SupTech и RegTech на период 2021–2023 годов.*

[4] Обзор основных типов компьютерных атак в финансовой сфере в 2023 году // Банк России : офиц. сайт. URL: https://sdlinfo.ru/wp-content/uploads/2024/05/Attack_2023.pdf (дата обращения: 22.07.2024).

[5] Там же.

секторе ФинЦЕРТ осуществляет постоянный мониторинг доступности услуг и операционной надежности финансовых организаций. Так, за прошлый год было выявлено 719 сбоев, 77 % из которых привели к инцидентам. Среднее время простоя при этом зафиксировано в районе 7 часов 35 минут, что значительно превышает обозначенные регулятором нормы (доступность банковских сервисов после сбоя должна быть обеспечена в течение двух часов[6]). Львиная доля (85 %) зафиксированных сбоев была обусловлена ошибками в работе ИТ-систем и сервисов, остальные 17 % пришлись на DDoS-атаки. Этот факт свидетельствует о необходимости продолжения начатой работы по технологическому и кадровому совершенствованию банковской деятельности. Однако, следует обратить внимание и на то, что несмотря на технические сбои, усилия злоумышленников, средний показатель доступности услуг и сервисов у финансовых организаций составил 99,5 % от общего времени работы.

На долю атак с использованием вредоносного программного обеспечения (ВПО) в 2023 году приходилось 34,34 %, на фишинговые рассылки – 15,26 %. Практика свидетельствует, что технологии таких «нападений» не изменились и представляют собой отправку электронного письма, содержащего ссылку на загрузку файла. При открытии файла либо компрометируется учетная запись пользователя, а его данные отправляются на сервер злоумышленников (фишинговая атака), либо автоматически на компьютер пользователя устанавливается ВПО. Часто кибермошенники используют такие приложения для внедрения шифровальщиков, кодирующих данные на мобильном устройстве и предлагающих раскодировать их за выкуп. В последние годы крупнейшие финансовые организации внедряют в систему «Клиент-Банк» фрод-модули, но риск несанкционированных трансакций в полной мере пока не снят[7].

Также представляет интерес анализ географии угроз-рассылок. Было выявлено, что абсолютное большинство почтовых серверов для рассылки ВПО находились в США (41 % от всех рассылок ВПО) и Нидерландах (35 %). Этот факт позволяет сделать вывод об их абузоустойчивости (игнорирование жалоб со стороны пользователей, отказ в доступе). Далее в порядке убывания веса участников следуют Россия (13 %), Вьетнам (6 %) и Венгрия (4 %). Почтовые сервисы, с которых осуществлялись фишинговые рассылки (на них же хранятся украденные у пользователей личные и финансовые данные), были размещены преимущественно в странах Юго-Восточной Азии (Индия – 31 %, КНР – 17 %, Вьетнам – 16 %), далее следуют Россия (14 %), США (12 %) и Нидерланды (10 %). Данные географического анализа дополняют эскиз ландшафта возможных угроз в работе банка и способствуют эффективности предпринимаемых мер по их ликвидации (повышается оперативность принятия решений, понятна траектория их направленности).

Помимо компьютерных атак мошенники активно используют в качестве инструмента телефонные звонки с применением сетей операторов связи, а также мессенджеров. Благодаря усиленной целенаправленной совместной работе регулятора, институтов кредитно-финансовой сферы, операторов связи, число звонков с городских телефонных номеров значительно снизилось (более чем на 75 %). Решить проблему мошенничества с применением мобильных номеров сложнее. Более того, число звонков с номером 8-800 за 2023 год увеличилось вдвое по сравнению с предыдущим периодом, хотя в целом в общей массе их доля почти незаметна (не более 1 %).

Заключение

В целом все выявленные угрозы безопасности банковской деятельности в современной российской практике наглядно демонстрируют необходимость постоянного совершенствования тактик, техник и инструментов борьбы как на уровне пользователей банковскими услугами, так и на уровне банковского сообщества и регулятора.

Оптимальный подход к защите своих собственных личных и финансовых данных с точки зрения индивидуального пользователя включает комплексные меры защиты: использование надежных паролей, отличающихся друг от друга в различных сервисах, отказ от использования сторонних приложений для хранения аутентификационных данных, применение настроек приватности, обязательное прохождение двухфакторной аутентификации.

В условиях роста мошенничества в финансовой сфере банкам также целесообразно использовать все возможные способы обеспечения безопасности в банковском секторе: как традиционные (идентификация клиента при помощи паролей и ПИН-кодов; аутентификация по SMS-коду; физическая защита банковских данных), так и более современные, продвинутые технологии (к примеру, биометрическая аутентификация по отпечаткам пальцев, голосовым командам, сканирование сетчатки глаза). В решении вопросов обеспечения

[6] Положение Банка России от 12 января 2022 г. № 787-П (ред. от 06.10.2023) «Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг» // СПС «Гарант». URL: https://ivo.garant.ru/#/document/404495544 /paragraph/14:0 (дата обращения: 20.07.2024).

[7] Информационная безопасность в финансовых системах // Searchinform : сайт компании ООО «СёрчИнформ». URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/bezopasnost-informatsionnykh-sistem/informatsionnaya-bezopasnost-v-finansovykh-sistem/ (дата обращения: 20.07.2024).

безопасности банковской деятельности ключевое место принадлежит именно инновационным методам обнаружения и предотвращения угроз. Значительную помощь в этом оказывает внедрение в работу кредитно-финансовых организаций искусственного интеллекта (к примеру, системы фрод-мониторинга) и технологий машинного обучения [16]. Их применение позволяет своевременно выявлять и анализировать те активности, которые могут спровоцировать появление возможных угроз. Например, если система замечает признаки необычного поведения клиента (перевод денег в ночное время, перевод значительной суммы средств), то, посчитав эту ситуацию подозрительной, она может заблокировать счет. Также с их помощью становится возможной реализация предсказательных моделей, эффективно предотвращающих попытки киберпреступлений.

Не менее результативным в борьбе против мошенников становится использование для хранения личной и финансовой информации клиентов технологии блокчейн [17]. Благодаря тому, что внесение любых изменений возможно только при наличии согласия всех участников, данная технология характеризуется как предельно защищенная, а, следовательно, и безопасная.

Не допустить возникновение угрозы информационной безопасности «изнутри», банкам позволит обеспечение кадровой (профессиональной) защищенности: четкие, детализированные условия приема сотрудников на работу, тщательный и систематический контроль за соблюдением рекомендаций и правил информационной безопасности, регулярное повышение квалификации персонала, разработка эффективных программ повышения лояльности.

Не менее значительная роль в решении вопросов обеспечения безопасности банковской деятельности принадлежит регулятору. С целью повышения уровня финансовой грамотности Банк России регулярно обновляет раздел на официальном сайте «Противодействие мошенническим практикам». Как уже отмечалось выше, такой подход с приданием гласности мошеннических схем позволяет воспрепятствовать дальнейшему их использованию. Представители регулятора активно общаются с гражданами на тему финансового мошенничества в чатах в Telegram. Листовки, брошюры, буклеты, социальная реклама на телевидении, размещение информации о мерах противодействия мошенникам на объектах транспортной и социальной инфраструктуры – все эти и другие инструменты использует регулятор в целях защиты граждан от преступников.

В контексте работы с представителями банковского сообщества с целью отработки навыков отражения киберугроз и реагирования на различные типы инцидентов, Банк России проводит так называемые киберучения.

В нормотворческом ракурсе Банк России за последние несколько лет выпустил стандарты СТО БР БФБО-1.5-2018 об управлении инцидентами информационной безопасности и СТО БР ИББС-1.0-2014, освещающий общие вопросы информационной безопасности в финансовой и кредитной сферах, одобрил «Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов»[8], установил более жесткие требования к программным модулям (Единой биометрической системе, системе быстрых платежей, платформам, обслуживающим маркетплейсы, цифровому профилю клиента). Это привело к заметному снижению числа инцидентов, а также к повышению уровня доверия населения: в 2023 году он составил 73,32 % (против целевого ориентира в 60 %)[9].

В дальнейшем Банк России планирует доработать требования, связанные с использованием Интернета вещей как новой угрозы с применением искусственного интеллекта и BigData, а также технологии распределенных ресурсов и изменением архитектуры информационных систем [18].

Эффективность мер по предотвращению возникновения угроз безопасности в финансовой сфере доказывается фактом отсутствия серьезных, глубоких, длительных нарушений в работе банковского сектора. Однако регулярные сбои в работе банкоматов и онлайн-приложений создают определенную напряженность в обществе, что побуждает уделять еще большее внимание информационной безопасности в финансовых системах.

Литература

1. *Ашмика А.* Киберпреступления, связанные с электронными картами, и банковское мошенничество // Право и цифровая экономика. 2023. № 1 (19). С. 60-71. DOI:10.17803/2618-8198.2023.19.1.060-071

2. *Абалкин Л. И.* Экономическая безопасность России: угрозы и их отражение // Вопросы экономики. 1994. № 12. С. 4-15.

3. *Сенчагов В. К.* Экономическая безопасность России // ЭКО. 2007. № 5 (395). С. 16–23.

4. *Гуреева М. А., Зиядуллаев Н. С., Ларионов И. К.* Экономическая безопасность государства: противодействие спектру угроз – от материально-вещественных до информационно-цифровых: монография. 2-е издание. – М.: Изд-во «Дашков и К», 2021. –478 с.

5. *Городецкий А. Е.* Экономическая безопасность России: новая стратегия в новых реалиях // Проблемы теории и практики управления. 2018. № 1. С. 8–23.

[8] Одобрены Советом директоров Банка России 22 мая 2023 г.

[9] Основные направления развития информационной безопасности кредитно-финансовой сферы // Банк России : офиц. сайт. URL: https://cbr.ru/Content/Document/File/148351/onrib_2025.pdf.

6. *Караваева И. В., Иванов Е. А.* Стабильность или развитие: что сегодня может обеспечить экономическую безопасность России? // Федерализм. 2019. № 1. С. 118–134.

7. *Виноградова А. С., Молчанов И. Н.* Подходы к обеспечению информационной безопасности банковского сектора // Теория и практика проектного образования. 2020. № 2 (14). С. 40–42.

8. *Мамонтова С. В.* Экономическая и информационная безопасность в условиях цифровой экономики // Регион: системы, экономика, управление. 2022.№ 4 (59). С. 145–153. DOI: 10.22394/1997-4469-2022-59-4-145-153

9. *Ягупова Е. А., Черникова Л. Ф., Гасанова В. Т.* Банковская безопасность в условиях цифровой экономики Российской Федерации // Экономика и предпринимательство. 2021. № 10 (135). С. 308–313. DOI:10.34925/EIP.2021.135.10.057

10. *Одинцов В. О.* Экономическая безопасность кредитных организаций в условиях роста цифровых рисков // Вестник евразийской науки. 2023. Т. 15, № 6. С. 18–30

11. *Зарипов И. А.* Цифровой банкинг: смена парадигмы современных финансов // Мир новой экономики. 2022. Т. 16, № 2. С. 51-63. DOI:10.12737/2306-627X-2022-11-1-13-22

12. *Казакова Г. Я, Очир-Гаряева Т .Б., Наминова К. А.* и др. Автоматизированная информационная система (АИС) для банков: составляющие и их функционал // Экономика и предпринимательство. 2024. № 1 (162). С. 1418–1423. DOI:10.34925/EIP.2024.162.1.276

13. *Тарасова Н. В., Акиншина И. И.* Тенденции цифровой трансформации банковского сектора и проблемы обеспечения кибербезопасности // Первый экономический журнал. 2023. № 11 (341). С. 159–166. DOI:10.58551/20728115_2023_11_159

14. *Тимофеева О. И.* Цифровая трансформация российской банковской сферы в условиях современных вызовов и угроз // Управленческий учет. 2023. № 7. С. 145–152. DOI: 10.25806/uu72023145-152

15. *Фадейкина Н.В.* Информационная и экономическая безопасность кредитной организации как факторы обеспечения ее устойчивости // Сибирская финансовая школа. 2024. № 2 (154). С. 50–60. DOI: 10/34020/1993-4386-2024-2-50-60

16. *Сну Б., Демьянова О. В., Хуан Х. Я.* Цифровые финансы и искусственный интеллект в построении современной цифровой среды //Дискуссия. 2023. № 4 (119). С. 18–32. DOI: 10.46320/2077-7639-2023-4-119-18-32

17. *Забелышенская У. Д., Николова К., Питухина Д. Д., Смирнов В. В.* Инновации в финансовой сфере: исследование влияния блокчейна на развитие онлайн банкинга и будущее электронных денег // Финансовая экономика. 2023. № 12. С. 304–307.

18. *Магомадов М. В., Ибрагимов Ю. М., Зарипова Р. С.* Финтех инновации и будущее финансовых услуг // Экономика и управление: проблемы, решения. 2023. Т. 5, № 11 (140). С. 95–102. DOI: 10.36871/ek.up.p.r.2023.11.05.011

Сведения об авторе

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

THREATS TO THE SECURITY OF BANKING ACTIVITIES IN MODERN RUSSIAN PRACTICE

D. Panina
Orenburg State University,
Orenburg, Russia

Among other sectors of the Russian economy, the banking sector is one of the most dynamically developing. Consequently, its resistance to various shocks and possible threats will be one of the central points of support for the economic security of the state. Modern statistics show an increase in various types of incidents in the financial sector. Regular monitoring and detailed analysis of fraudulent schemes will minimize the possibility of criminal manipulation, thereby significantly reducing the number of risks and the amount of financial losses.

The presented article provides a structural and geographical analysis of incidents in the financial sector recorded in 2023, and a sketch of the modern landscape of possible threats is compiled. The optimal approach to the formation of information and economic security of personal and financial data, in particular, and banking activities in general, involves comprehensive protection measures both from the point of view of the individual user and from the position of representatives of the banking community and the regulator.

Keywords: cyber fraud, security threats, DDoS attacks, phishing attacks.

Referencis

1. Ashmika A. Cybercrimes related to electronic cards and bank fraud, *Pravo i tsifrovaya ekonomika*, 2023, No. 1 (19), pp. 60–71. (In Russ.). DOI: 10.17803/2618-8198.2023.19.1.060-071

2. Abalkin L. I. Economic security of Russia: threats and their reflection, Voprosy ekonomiki, 1994, No. 12, pp. 4-15. (In Russ.).

3. Senchagov V. K. Economic security of Russia, *EKO*, 2007, No. 5 (395), pp. 16–23. (In Russ.).

4. Gureeva M. A., Ziyadullaev N. S., Larionov I. K. *Ekonomicheskaya bezopasnost' gosudarstva: protivodeistvie spektru ugroz – ot material'no-veshchestvennykh do informatsionno-tsifrovykh: monografiya* [Economic security of the state: countering a range of threats – from material to information and digital: monograph], Moscow: Izd-vo «Dashkov i K», 2021, 478 p. (In Russ.).

5. Gorodetskii A. E. Economic security of Russia: a new strategy in new realities, *Problemy teorii i praktiki upravleniya*, 2018, No 1, pp. 8–23. (In Russ.).

6. Karavaeva I. V., Ivanov E. A. Stability or development: what can ensure Russia's economic security today? *Federalizm*, 2019, No. 1, pp. 118-134. (In Russ.).

7. Vinogradova A. S., Molchanov I. N. Approaches to ensuring information security of the banking sector, *Teoriya i praktika proektnogo obrazovaniya*, 2020, No. 2 (14), pp. 40–42. (In Russ.).

8. Mamontova S. V. Economic and information security in the digital economy, *Region: sistemy, ekonomika, upravlenie*, 2022, No. 4 (59), pp. 145–153. (In Russ.). DOI: 10.22394/1997-4469-2022-59-4-145-153

9. Yagupova E. A., Chernikova L. F., Gasanova V. T. Banking security in the digital economy of the Russian Federation, *Ekonomika i predprinimatel'stvo*, 2021, No. 10 (135), pp. 308–313. (In Russ.). DOI: 10.34925/EIP.2021.135.10.057

10. Odintsov V. O. Economic security of credit institutions in the context of growing digital risks, *Vestnik evraziiskoi nauki*, 2023, Vol. 15, No. 6, pp. 18–30. (In Russ.).

11. Zaripov I. A. Digital banking: a paradigm shift in modern finance, *Mir novoi ekonomiki*, 2022, Vol. 16, No. 2, pp. 51–63. (In Russ.). DOI: 10.12737/2306-627X-2022-11-1-13-22

12. Kazakova G. Ya., Ochir-Garyaeva T. B., Naminova K. A., Kegdeeva E. M., Badlaeva O. A., Tumudov E. N. Automated Information System (AIS) for banks: components and their functionality, *Ekonomika i predprinimatel'stvo*, 2024, No. 1 (162), pp. 1418–1423. (In Russ.). DOI:10.34925/EIP.2024.162.1.276

13. Tarasova N. V., Akinshina I. I. Trends in the digital transformation of the banking sector and cybersecurity issues, *Pervyi ekonomicheskii zhurnal*, 2023, No. 11 (341), pp. 159–166. (In Russ.). DOI: 10.58551/20728115_2023_11_159

14. Timofeeva O. I. Digital transformation of the Russian banking sector in the context of modern challenges and threats, *Upravlencheskii uchet*, 2023, No. 7, pp. 145–152. (In Russ.). DOI: 10.25806/uu72023145-152

15. Fadeikina N. V., Zyryanov V. S. Information and economic security of a credit institution as factors of ensuring its sustainable development, *Sibirskaya finansovaya shkola*, 2024, No. 2 (154), pp. 50–60. (In Russ.). DOI: 10.34020/1993-4386-2024-2-50-60

16. Snu B., Dem'yanova O. V., Khuan Kh. Ya. Digital finance and artificial intelligence in building a modern digital environment, *Diskussiya*, 2023, No. 4 (119), pp. 18–32. (In Russ.). DOI: 10.46320/2077-7639-2023-4-119-18-32

17. Zabelyshenskaya U. D., Nikolova K., Pitukhina D. D., Smirnov V. V. Innovations in the financial sector: a study of the impact of blockchain on the development of online banking and the future of electronic money, *Finansovaya ekonomika*, 2023, No. 12, pp. 304–307. (In Russ.).

18. Magomadov M. V., Ibragimov Yu. M., Zaripova R. S. Fintech innovation and the future of financial services, *Ekonomika i upravlenie: problemy, resheniya*, 2023, Vol. 5, No. 11 (140), pp. 95–102. (In Russ.). DOI: 10.36871/ek.up.p.r.2023.11.05.011

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.
ORCID: 0000-0001-9035-7860, ResearcherID: XTO-8544-2023, AuthorID: 781328.
E-mail: darpanina2015@yandex.ru