ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2587-5671-2022-26-6-52-71
УДК 338.242(045)
JEL G20, 21

Вызовы и угрозы цифровой экономики для устойчивости национальной банковской системы

М.Н. Дудин[a], С.В. Шкодинский[b]
[a, b] Институт проблем рынка Российской академии наук, Москва, Россия;
[b] Научно-исследовательский финансовый институт Минфина России, Москва, Россия

АННОТАЦИЯ

Цель исследования — выработка конкретных методически аргументированных предложений по совершенствованию механизма обеспечения устойчивого развития национальной банковской системы и ее защищенности перед внешними вызовами и угрозами киберпространства. **Новизна исследования** состоит в комплексном анализе процессов обеспечения киберустойчивости банковской системы России в условиях эскалации внешних вызовов и угроз цифровой экономики. Авторы использовали следующие **методы** исследования: общенаучные (наблюдение, сравнение, измерение, анализ и синтез, метод логического рассуждения), конкретно-научные (статический анализ, экспертные оценки, графический метод). Проведен критический обзор отечественной и зарубежной научной литературы и практических рекомендаций по обеспечению защиты банковского института от киберугроз в цифровой экономике; представлен компаративный анализ организации системы обеспечения кибербезопасности в российской и зарубежных банковских системах; сделан многоаспектный статистический анализ киберугроз для российских банков; обоснованы рекомендации и предложения по организационно-экономическому и правовому совершенствованию системы защиты российских банков от внутренних и внешних киберугроз. Показано, что основными проблемными точками (зонами) банковской системы, создающими предпосылки для возникновения киберрисков являются: 1) отсутствие рыночной саморегуляции и обмена информацией о кибератаках и механизмах их совершения; 2) низкая эффективность сотрудничества сегмента e-commerce с государственным регулятором сети Internet — Роскомнадзором; 3) недостаточная профессиональная подготовка и компетентность сотрудников банков в части выявления признаков кибератаки; 4) ограниченность бюджета малых и средних банков, не позволяющих им содержать самостоятельные подразделения киберзащиты; 5) популяризация и активный рост рыночного присутствия финтех-сервисов и компаний. Сделан **вывод**, что для организационно-экономического и правового совершенствования системы защиты российских банков от внутренних и внешних киберугроз необходимы следующие меры: интенсификация процессов развития бизнес-модели банковских экосистем; создание федерального межбанковского реестра счетов кибермошенников; формирование единого банковского «полигона» для тестирования уязвимостей программного обеспечения и др.

Ключевые слова: банки; киберустойчивость; цифровая экономика; вызовы и угрозы; уязвимости; хакерские атаки; финтех; персональные данные; мошенничество

Для цитирования: **Дудин М.Н., Шкодинский С.В. Вызовы и угрозы цифровой экономики для устойчивости национальной банковской системы. *Финансы: теория и практика*. 2022;26(6):52-71. DOI: 10.26794/2587-5671-2022-26-6-52-71**

ORIGINAL PAPER

Challenges and Threats of the Digital Economy to the Sustainability of the National Banking System

M.N. Dudin[a], S.V. Shkodinsky[b]
[a, b] Institute of Market Problems of the Russian Academy of Sciences, Moscow, Russia;
[b] Financial Research Institute, Ministry of Finance of Russia, Moscow, Russia

ABSTRACT

The **goal** of the study — development of specific methodical reasoned proposals on improvement of the mechanism for ensuring sustainable development of the national banking system and its security against external challenges and threats to cyberspace. The **scientific novelty** consists in a comprehensive analysis of the processes of ensuring the cyber stability of the Russian banking system in the context of escalation of external challenges and threats to the digital

economy. The authors used the following **methods**: general scientific (observation, comparison, measurement, analysis and synthesis, logical reasoning method), specific scientific (static analysis, peer review, graphical method). In the article conducted a critical review of domestic and foreign scientific literature and practical recommendations to ensure the protection of the banking institution from cyber threats in the digital economy; presented a comparative analysis of the organization of the cybersecurity system in the Russian and foreign banking systems; done multidimensional statistical analysis of cyber threats for Russian banks; substantiated recommendations and proposals on organizational, economic and legal improvement of the system of protection of Russian banks from internal and external cyber threats. As a **result**, it is shown that the main problem points (zones) of the banking system, creating the prerequisites for the occurrence of cyber-risks are: 1) there is no exchange of information on cyber-attacks and their mechanisms; 2) banks interact inefficiently with the state regulator of Internet — Roskomnadzor; 3) low level of competence of bank employees who are responsible for cybersecurity; 4) limited budget of small and medium-sized banks that wouldn't allow them to care independent cyber-protection units; 5) growing popularity of new fintech services and new fintech companies. The author draws a **conclusion** that the following measures are necessary for organizational, economic and legal improvement of the system of protection of Russian banks from internal and external cyber threats: the processes of development of banking ecosystems should be intensified; a federal interbank register of cyber fraudsters must be created; a single banking "polygon" for testing cyber threats needs to be developed.
Keywords: banks; cyber resilience; digital economy; challenges and threats; vulnerabilities; hacker attacks; fintech; personal data; fraud

***For citation*: Dudin M.N., Shkodinsky S.V. Challenges and threats of the digital economy to the sustainability of the national banking system. *Finance: Theory and Practice*. 2022;26(6):52-71. DOI: 10.26794/2587-5671-2021-26-6-52-71**

ВВЕДЕНИЕ

Банковская система является одной из наиболее восприимчивых сфер национальной экономики любой страны к инновациям и изменяющейся архитектуре устройства социально-экономической системы. Это объясняется дуализмом экономических интересов банковского института в условиях цифровизации. С одной стороны, формирование цифровой экономики — мощный драйвер к качественной эволюции продуктового портфеля с возможностью предложения персонифицированных продуктов и сервисов розничным и корпоративным клиентам. С другой стороны, банки стремятся к снижению издержек на оказание банковских услуг и реализацию продуктов для своих клиентов. Однако следует понимать, что на этих «весах интересов» еще необходимо разместить интересы национального государственного регулятора — Центрального банка — и его стратегические цели по обеспечению безопасного и устойчивого функционирования банковской системы страны в целом.

Переход человечества в новую фазу развития, именуемую Индустрией 4.0, несет в себе ряд системных противоречий и рисков для стабильного функционирования банковской системы. Одним из основополагающих из них является масштабная трансфигурация бизнес-процессов из физических аналогов в цифровые, появление виртуальных конструктов, что ослабляет возможности банков в обеспечении достаточного контроля всех этих звеньев, а значит, повышает их уязвимость перед внешними вызовами и угрозами цифрового окружения.

Данная научная статья является результатом структурированного обзора отечественной и зарубежной практики организации системы киберзащиты от вызовов и угроз устойчивого развития банковской системы, многоаспектного статистического анализа киберугроз для российских банков, а также обоснования конкретных методически аргументированных предложений по совершенствованию механизма обеспечения устойчивого развития российской банковской системы.

МАТЕРИАЛЫ И МЕТОДЫ

Теоретико-методологическая база исследования включает в себя научные труды отечественных (А.С. Яблочкин, А.П. Кошкин [1]; И.Н. Тимоничева, В.В. Яновский, А.С. Бережной [2]; П.В. Ревенков, А.А. Бердюгин [3]; Л.А. Чалдаева; А.А. Килячков, А.А. Якорев [4]; Н.И. Быканова, Д.В. Гордя, Д.В. Евдокимов [5]) и зарубежных (N.A.-D. Khalifa [6]; Aguayo F. Zabala, B. Ślusarczyk [7]; A.W. Dorn, S. Webb [8]) академических кругов, а также практические исследования и рекомендации ведущих консалтинговых агентств (PT Security; PWC; Deloitte; Kaspersky Security Laboratory) и специалистов (Н.Н. Федотов, И.С. Ашманов; П. Зингер, А. Фридман; В. Снайдер; Б. Тускан; М. Хюппонен) в области кибербезопасности.

При написании статьи использовались общенаучные методы научного исследования (наблюдение, сравнение, измерение, анализ и синтез, метод логического рассуждения) и конкретно-научные (статический анализ, экспертные оценки, графический метод). Обоснованность и достоверность

результатов научного исследования обеспечивается корректностью и строгостью построения логики и схемы исследования, а также использованием верифицированной статистической информации из авторитетных источников (аналитические отчеты Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, тематические отчеты «Кибербезопасность. Тренды и прогнозы» PT Security, тематические материалы консалтинговых агентств PWC, Deloitte, Kaspersky Security Laboratory).

ОБЗОР ЛИТЕРАТУРЫ И ИССЛЕДОВАНИЙ

Обеспечение безопасности функционирования любого бизнеса — стратегическая задача менеджмента, решение которой гарантирует его выживание в условиях рынка и обеспечение доверия клиентов (не пренебрегая другими факторами обеспечения конкурентоспособности). В отношении банков данный постулат особенно справедлив, так как клиенты предоставляют им свои денежные средства на хранение или доверительное управление, а также используют их инфраструктуру и сервисы для проведения различных транзакций.

Критический обзор отечественной и зарубежной научной литературы и практических рекомендаций по обеспечению защиты банковского сектора от киберугроз в цифровой экономике показал наличие существенных различий в понятийном аппарате кибербезопасности банковской системы.

В отечественных научных и практических кругах в понятийном аппарате делается акцент на раскрытие понятия «кибербезопасность» и стремление учесть как можно больше потенциальных точек (зон) в бизнес-процессах банков, которые могут подвергнуться атакам извне. Отметим, что отечественная практика банков носит именно оборонительный характер и характеризуется стремлением точно и максимально полно объяснить содержание таких понятий, как «безопасность банковских бизнес-процессов в цифровой экономике», «банковская кибербезопасность», «киберустойчивость».

Так, согласно ст. 2 Доктрины информационной безопасности Российской Федерации под *информационной безопасностью* понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства[1]. В данном определении, на наш взгляд, содержится достаточно общий подход, отражающий политическую ориентацию государственных регуляторов на недопущение и предотвращение проявления потенциальных вызовов и угроз цифровой экономики для экономической безопасности страны в целом.

По мнению С.И. Луценко, кибербезопасность банковского института следует рассматривать как комплексный механизм применения организационных, технологических, кадровых и административных инструментов противодействия влиянию внешних кибератак и профилактике правонарушений внутреннего информационного контура банковской системы с его адаптацией под изменяющийся информационно-технологический ландшафт цифровой экономики[2]. В данном определении существенное место имеет тот факт, что механизм должен быть адаптивным, т.е. динамичным и меняться (точнее сказать — подстраиваться) под эволюционирующие вызовы и угрозы цифровой экономики, тем самым обеспечивая безопасность финансовых активов и информации банковской системы.

Несколько иной подход представили в своих работах А.С. Алпееев, М.М. Безкоровайный и А.Л. Татузов. По их мнению, кибербезопасность банковского института — проактивная система реагирования на внутренние и внешние вызовы и угрозы киберпространства, которая базируется на гибкой методологии Agile, позволяющей в самые краткие сроки трансформировать банковские бизнес-процессы под новые источники киберугроз [9, 10]. Ценность данного определения лежит в обосновании возможности достижения синергии в случае применения гибких методик управления проектного менеджмента в сфере IT (методика Agile специализируется именно на проектах в сфере IT) и классических правилах информационной гигиены в банках. То есть это определение подводит нас к новому термину, который упоминался ранее, — «киберустойчивость».

Кроме того, в работе Р.И. Захарченко и И.Д. Королева под киберустойчивостью понимается способность системы управления бизнес-процессами

[1] Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646. URL: https://www.garant.ru/products/ipo/prime/doc/71456224/#0 (дата обращения: 20.01.2022).

[2] Луценко С.И. Политика Российской Федерации в области кибербезопасности. URL: http://digital-economy.ru/images/easyblog_articles/504/IB 777.pdf (дата обращения: 20.01.2022).

выполнять свои функции в сложной, резко меняющейся обстановке в условиях деструктивных информационных воздействий [11]. В данном определении речь идет о возможности банковской системы сохранять свою дееспособность даже при свершившейся кибератаке, что выводит вопрос обеспечения устойчивого развития уже на уровень всей банковской системы страны. Должен быть создан целостный механизм взаимострахования банков на случай кибератак извне и эффективный фильтр для предотвращения формирования агрессивной информационной среды внутри банковской системы.

В зарубежной практике, как в научных, так и в законодательных трудах, категориальный аппарат акцентирован на раскрытии сущности вызовов и угроз для банковской системы с позиции понятий «кибератака», «кибертерроризм» и «кибервойна». Это позволяет сделать предположение о стремлении зарубежных специалистов разграничить приведенные выше понятия, что связано с интересом государственных регуляторов (как финансовых, так и военных) к рассмотрению цифрового ландшафта и его инфраструктуры как «театра военных действий». Данное предположение может быть аргументировано проведенным содержательным анализом таких документов, как Национальная стратегия кибербезопасности»[3], «Таллинское руководство по применению международного права к кибероперациям»[4] (2017 г.) и «Акт о кибербезопасности» (Cybersecurity Act)[5] (2019 г.).

Выделим и подход, представленный Международным союзом электросвязи, в котором кибербезопасность представлена как «технологии, концепции, меры государственной политики, процедуры и практики, направленные на защиту активов (компьютеров, инфраструктуры, приложений, услуг, систем связи и информации) и киберпространства от атак, нанесения ущерба и неавторизованного доступа[6]». В приведенном определении достаточно четко прослеживается ориентация всех участников киберпространства на отражение кибератак и подразумевается (хотя прямо и не декларируется) принятие ответных мер в отношении агрессора.

В соответствии со ст. 1 Закона о кибербезопасности ЕС понятие «кибербезопасность» трактуется как «деятельность, необходимая для защиты сетей и информации, пользователей информационных сетей и иных сторон, которые могут быть затронуты киберугрозами»[7]. При этом в самом Законе есть уточнение (несколько размытое), что под деятельностью могут пониматься и активные действия со стороны уполномоченных органов ЕС, направленные на превентивную защиту от возможных кибератак[8]. Полагаем, что указанный Закон ЕС ориентирован на возможную активную наступательную политику.

Отсылку к восприятию киберпространства как объекта политических и экономических интересов ЕС можно найти в Директиве ЕС 2016/1148 о кибербезопасности: в частности ст. 9, 11, 13 указывают, что в случае необходимости уполномоченные государственные регуляторы и участники ГЧП-соглашений — владельцы критической инфраструктуры — могут участвовать в организации активных действий, направленных на нивелирование влияния источника киберугроз путем разрыва с ними дипломатических отношений, блокирования финансовых транзакций, исключения посреднических институтов из международных договоров обмена информацией или корреспондирующих отношений в финансовой (банковской) сферах.

В Национальной стратегии кибербезопасности США содержится отсылка к дополнению закона — Cloud Act, в котором содержится разрешение на участие американских IT-корпораций группы FAMGA и отдельных спецслужб в сборе информации о потенциальных источниках киберугроз и принятии решения о превентивном воздействии на них вплоть до уничтожения с целью нивелиро-

[3] Новая стратегия кибербезопасности США: краткий анализ новой редакции (16.10.2018). URL: http://csef.ru/ru/oborona-i-bezopasnost/272/novaya-strategiya-kiberbezopasnosti-ssha-kratkij-analiz-novoj-redakczii-8665 (дата обращения: 21.01.2022).

[4] Таллинское руководство 2.0 и захват киберпространства (06.02.2017). URL: https://www.geopolitica.ru/article/tallinskoe-rukovodstvo-20-i-zahvat-kiberprostranstva (дата обращения: 21.01.2022).

[5] Акт ЕС о Кибербезопасности (Cybersecurity Act) (17.12.2019). URL: https://medium.com/lawgeek-by-aurum/eu-cybersecurity-act-review-aurum-law-firm-d588db539e75 (дата обращения: 21.01.2022).

[6] International Telecommunications Union (ITU) (2008). Overview of Cybersecurity, Recommendation ITU– T X. 1205. URL: https://www.itu.int/rec/T-REC–X.1205–200804-I (дата обращения: 21.01.2022).

[7] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No. 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151/1. URL: http://data.europa.eu/eli/reg/2019/881/oj (дата обращения: 22.01.2022).

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148 (дата обращения: 22.01.2022).

вания рисков деструктивного влияния на объекты критической инфраструктуры.

Зарубежные академические круги придерживаются более мягкой точки зрения по вопросу раскрытия сущности вызовов и угроз для банковской системы, однако в целом сохраняют солидарность о допущении активных действий в отношении источника угрозы. Так, Н.А.-Д. Кхалифа считает, что в понятие киберустойчивости банковской системы обязательно следует включать «механизм возмездия», который может быть реализован как самим пострадавшим от атаки, так и по принципу солидарности, другими банками — участниками соглашений о киберзащите корпоративных интересов [6, с. 43–44]. Кроме того, А.В. Дорн и С. Вебб считают, что банковская кибербезопасность — это целостная система не только защиты финансовых активов и устойчивого функционирования национальной финансовой инфраструктуры, но и инструмент превентивного влияния на мировые очаги киберугроз и потенциальных кибератак [8, с. 24].

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Мы полагаем, что представленный критический обзор отечественной и зарубежной точек зрения на сущность вызовов и угроз для банковской системы характеризуется аппозитивным подходом. В этой связи считаем необходимым представить таблицу результатов компаративного анализа организации системы обеспечения кибербезопасности в российской и зарубежных банковских системах (*табл. 1*).

Как следует из приведенного компаративного анализа, в отечественной практике банки обладают достаточной самостоятельностью в вопросе организации системы кибербезопасности собственной деятельности. При этом важно отметить и факт отсутствия специальных программ развития секьюрити-инфраструктуры для банков, финансируемых за счет государственных источников (внебюджетные фонды, целевые бюджеты крупнейших участников рынка кибербезопасности государственной формы собственности, например ГК «Ростех»). Это делает банковскую систему более уязвимой, так как, за исключением группы системно значимых банков и входящих в топ-100, большинство банков не могут себе позволить такие расходы ввиду длительности их окупаемости и неявного коммерческого эффекта.

Изучение положения банковской системы России с позиции ее устойчивости перед киберугрозами цифровой экономики считаем целесообразным начать с количественного и качественного анализа кибератак, что позволяет понять их масштабность и целевую ориентацию (*рис. 1 и 2*).

Как следует из приведенных данных в *рис. 1*, наблюдается устойчивый рост кибератак на российскую банковскую систему, причем при анализе среза функциональных уровней видно, что основной интерес атакующих ориентирован на банки 2 уровня (в среднем за исследуемый период на них было совершено 738 атак) и значительно меньше — на НКФО (283 атаки). При анализе причин учащения атак на российский банковский сектор было установлено следующее:

- *во-первых*, Банком России отмечается устойчивый рост безналичных расчетов в розничном банкинге: так, за 2020 г. удельный вес безналичных платежей в розничном обороте составил 70,3% (64,7% — в 2019 г.)[9], что опережает темпы развития рынка дистанционного банковского обслуживания большинства стран Западной Европы и даже США и объективно привлекает хакерские группы;
- *во-вторых*, Россия входит в тройку стран с самой активной цифровой трансформацией банковских сервисов — по данным E&Y, в 2019 г. удельный вес активных пользователей digital-банкинга составил 82,0% (для сравнения — среднемировой уровень составляет 64%)[10]. Важно отметить, что digital-трансформация в российских банках идет снизу вверх, т.е. клиенты банков мотивируют их к внедрению новейших цифровых финансовых сервисов, причем банки зачастую не обладают достаточно надежными системами защиты от внешних киберугроз, что вкупе повышает интерес хакерских группировок к атакам;
- *в-третьих*, в российской банковской системе наиболее активно развиваются следующие сегменты: цифровой банкинг (онлайн-кредитование, открытие вкладов, обмен валют, реже — инвестиционные продукты) — данный сервис развивается у 78,7% всех банков и группа платежно-расчетных сервисов (денежные переводы, электронные деньги, P2P-займы), представляющие собой фактически расширенное продолжение цифрового банкинга для взаимодействия банков и, например, телеком-операторов, производителей гаджетов для связи и обмена финансовой информацией —

[9] Итоги работы Банка России: коротко о главном, 2020 год. URL: https://cbr.ru/about_br/publ/annrep2020short/platezhnaya-sistema/ (дата обращения: 26.01.2022).

[10] Global FinTech Adoption Index 2021. URL: https://www.ey.com/en_gl/ey-global-fintech-adoption-index (дата обращения: 26.01.2022).

более 18,0%[11]. Этот факт развития также вносит свой вклад в уязвимость российской банковской системы, так как стремительное развитие виртуальных платежных сервисов не гармонизировано с финансовой грамотностью и цифровой гигиеной клиентов при работе в сети Интернет, что многократно повышает уязвимость обеих сторон.

Исходя из особенностей развития российского рынка банковских сервисов, рассмотрим состав и структуру объектов, подверженных кибератакам за 2016–2021 гг. (I–III кварталы). При этом следует отметить, что в указанный период кибератаки на банковскую систему стали комплексными, т.е. их целями выступали более одного объекта, что свидетельствует о повышении рисков для киберустойчивости российской банковской системы (*рис. 2*).

Данные *рис. 2* свидетельствуют о том, что ключевым объектом криминальных интересов хакеров является банковская инфраструктура — в среднем на данный объект приходится 57,5% всех зафиксированных кибератак. На втором месте — розничные клиенты — немногим больше 31,0%, третье место со значительным отставанием занимает группа «банкоматы, POS-терминалы, мобильные устройства» — 18,5%. На первый взгляд может показаться, что хакеры умышленно выбирают самое защищенное звено — банковскую инфраструктуру, однако на самом деле большое количество клиентов не заявляют о том, что подверглись атаке, или их гаджеты были использованы как точка входа, в том числе, для нанесения ущерба банковской инфраструктуре.

С наступлением пандемии COVID-19 атаки на розничных клиентов, а также использование их гаджетов для хакерских атак значительно возросло ввиду объективных причин: введение карантинных мер, популяризация инструментов бесконтактной доставки и заказов продуктов и услуг через интернет-магазины, что вкупе с недостаточно высокой цифровой культурой населения привело к росту кибератак на данные группы объектов.

Отметим, что факт активного превалирования атак на банковскую инфраструктуру прямо свидетельствует об участии в этом профессиональных хакеров очень высокого уровня с использованием мощного оборудования (серверов, Data-центров). Это косвенно может свидетельствовать о проведении санкционированных государственными регуляторами кибератак с целью найти уязвимости в ее архитектуре для получения нового инструмента политического давления на Россию, а в худшем варианте — развязывании кибервойны[12].

Следующим шагом настоящего исследования является изучение инструментов совершения кибератак, что является информационной основой для разработки конкретных предложений по совершенствованию механизма защиты от кибератак и общего повышения киберустойчивости российской банковской системы (*рис. 3*).

Как следует из приведенной диаграммы на *рис. 3*, ключевым инструментом совершения кибератак на российскую банковскую систему выступило программное обеспечение, содержащее в себе вредоносный код — в среднем его применение в атаках составило 53,7%. В его составе следует отметить превалирование шпионского программного обеспечения (в 2020 г. его удельный вес составил более 40,0%) для сбора персональных данных о клиентах и их счетах.

На втором месте расположился инструмент социальной инженерии — 37,7%, который ввиду пандемии COVID-19 резко набрал популярность. Причем его проявление было как в «привычной» для специалистов кибербезопасности форме (телефонное мошенничество), так и новых, сложных форматах, интегрированных в кастомизированные процессы сервиса (например, партнерские программы банка и представителей ритейла, медицинских центров). По данным ФинЦЕРТ, в 2020 г., по сравнению с 2019 г., отмечен рост данного инструмента на 86,0%, что не только снижает работу служб безопасности банков, но и существенно подрывает доверие клиентов к банковской системе в целом[13].

Третье место занимает хакинг — 21,8%, и следует отметить, что его использование было системным и тщательно организованным: по данным ФинЦЕРТ, за 2019–2020 гг. было зафиксировано 225 атак хакерской группировки RTM[14] (сокращение от самоназвания Remote Transaction Manager), целью которого было удаленное управление транзакциями клиентов — владельцев валютных вкладов и инвестиционных депозитов.

---

[11] Исследование рынка технологического предпринимательства в России, 2020. (21.12.2020). URL: https://drive.google.com/file/d/1NsSN 3e_NkGS 1k2dfVb7cx6fXX8jHCNaA/view (дата обращения: 26.01.2022).

[12] Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах (2021). URL: https://cbr.ru/Collection/Collection/File/32122/Attack_2019–2020.pdf (дата обращения: 27.01.2022); Цифровая угроза: кто может стоять за кибератаками на Россию (13.05.2021). URL: https://russian.rt.com/world/article/861272-rossiya-kiberataki-ssha-bezopasnost (дата обращения: 27.01.2022).

[13] Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах (2021). URL: https://cbr.ru/Collection/Collection/File/32122/Attack_2019–2020.pdf (дата обращения: 27.01.2022).

[14] Там же.

Таблица 1 / Table 1

Организация системы обеспечения кибербезопасности в российской и зарубежных банковских системах: компаративный анализ / Organization of cyber security in Russian and foreign banking systems: a comparative analysis

Критерии сравнения / Criteria comparison	Российская банковская система / Russian banking system	Зарубежные банковские системы / Foreign banking systems
1. Источники мотивации/интереса к развитию кибербезопасности	– Учащение кибератак на банковскую систему из-за рубежа; – острое технологическое неравенство инструментов защиты банковских сервисов; – отсутствие единых национальных стандартов кибербезопасности банков; – повышение рисков использования кибертерроризма в политических интересах ЕС и США; – ужесточение международных требований стандартов кибербезопасности	– Политические интересы использования инструментов кибератак на банковские системы (США, Великобритания); – учащение случаев «утечки» персональной информации о клиентах банков (ЕС, США); – обострение технологического неравенства между банками-партнерами (ЕС); – формирование прецендентов санкционного давления на банковскую систему и ее отдельные банки (Китай) с целью ее ослабления на мировом рынке
2. Основные стейкхолдеры	– Президент РФ; – государственные регуляторы — Центральный банк РФ, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации; – системно значимые кредитные организации (13 банков)[a]	– Европейское управление банковского надзора; — Комитет по глобальным финансовым системам BIS; — Общество всемирных межбанковских финансовых телекоммуникаций (SWIFT); — Служба регулирования отрасли финансовых услуг[b]; – страновые регуляторы в лице центральных банков
3. Обобщенное описание механизма осуществления политики кибербезопасности	Банками разрабатываются индивидуальные риск-стратегии и карты киберугроз с учетом специфики клиентской базы, применяемых финансовых инструментов и действующих сервисов. Главная цель для банков — соответствие критериям требований безопасного функционирования, установленным Центральным банком РФ и международными регулятивными институтами (при ведении активной международной деятельности). Минимальные (пороговые) требования к технологическому обеспечению банковской деятельности закреплены в СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»[c] ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»[d]. Ключевым экспертным лицом, аккумулирующим информацию о киберинцидентах в банках, выступает созданный при Центробанке орган — Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Департамента информационной безопасности Банка России[e]	В *США* коммерческие банки разрабатывают коллективную политику в сфере кибербезопасности (проект Sheltered Harbor[f]) на основе корреспондентских отношений или состава финансовой группы и согласуют ее с Национальным управлением кибербезопасности[g] В *ЕС* страновые банки-регуляторы разрабатывают общегосударственные стратегии кибербезопасности и согласовывают их с Европейским центральным банком, что позволяет гармонизировать усилия отдельных стран в обеспечении устойчивого развития банковской системы ЕС [12, 13]. В *Великобритании* начиная с 2014 г. действует Центр оценки киберситуации, с которым связаны все банки королевства и который обладает полномочиями принятия антикризисных решений на случай проведения атаки и угрозы дестабилизации банковской системы[h] В *Китае* система киберзащиты банков строится по принципу мягкой силы: передача данных банковской системы происходит по выделенной автономной сети, к которой клиенты подключаются только на время совершения операций или получения услуг. Кроме этого, государство применяет модель «цифрового национализма» — введения специальных требований о локализации всех данных в пределах юрисдикции государства. Это позволяет собирать информацию о всех пользователях сети и идентифицировать их личности, что выступает дополнительной защитой от хакерских атак [14]

Окончание таблицы 1 / Table 1 (continued)

Критерии сравнения / Criteria comparison	Российская банковская система / Russian banking system	Зарубежные банковские системы / Foreign banking systems
4. Источники финансирования проектов и программ формирования киберзащиты	Банки индивидуально определяют в рамках стратегии развития сроком на 1, 3 или 5 лет (прогноз) создание специальных фондов финансирования проектов в сфере кибербезопасности или применяется метод регулярных отчислений в специальный фонд[i]	В *США* банки активно участвуют в финансируемых Google и Microsoft программах кибербезопасности, которые тестируют новые продукты защиты от кибератак, а затем продают лицензии на их использование[j] В *ЕС* банки и центробанки государств-членов получают финансовую поддержку от рамочных программ, утвержденных Парламентом ЕС для обеспечения киберустойчивости банковской сферы, а затем уже на уровне регуляторов отдельных стран происходит распределение финансирования между банками. В *Великобритании* банки активно взаимодействуют с венчурными компаниями в сфере кибербезопасности в форме партнерств, в том числе обеспечивая финансирование стартапов взамен на получение новейших решений в сфере информационной защиты (например, платформа национального технологического сотрудничества Tech Nation, городские платформы London Tech и North Tech для поддержки IT-сообщества, университетов и бизнес-школ, занимающихся исследованием и развитием кибербезопасности[k] В *Китае* в период с 2020 по 2023 г. планируется освоить государственное финансирование в размере 40 млрд долл. США на обеспечение кибербезопасности страны[l], в том числе на банковский сектор ожидается выделить почти половину. Финансирование будет направлено на оплату разработок IT-группы BAT, Huawei, ZTE

Источники / Sources: разработано авторами по данным [12–16] / compiled by the authors on the data [12–16]:

[a] Банк России утвердил перечень системно значимых кредитных организаций / Bank of Russia approved list of systemically significant credit organizations (11.10.2021). URL: https://cbr.ru/press/pr/?file=11102021_133500PR 2021–10–11T13_27_28.htm (дата обращения: 22.01.2022) / (accessed on 22.01.2022); [b] Обзор регулирования финансовых рынков / Regulatory overview of financial market (16.05.2016–15.07.2016). URL: https://cbr.ru/finmarkets/files/development/review_020916.pdf (дата обращения: 22.01.2022) / (accessed on 22.01.2022); [c] СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (01.06.2014) / STO BR IBBS-1.0 "Information Security of Organizations of the Banking System of the Russian Federation. General Regulations". URL: https://cbr.ru/statichtml/file/59420/st-10–14.pdf (дата обращения: 23.01.2022) / (accessed on 23.01.2022); [d] ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»: Приказ Федерального агентства по техническому регулированию и метрологии от 08.08.2017 № 822-ст. / GOST R 57580.1–2017 "Security of financial (banking) operations. Protection of information of financial organizations. Basic composition of organizational and technical measures": Order of the Federal Agency for Technical Regulation and Metrology No. 822 from 08.08.2017. URL: https://docs.cntd.ru/document/1200146534 (дата обращения: 23.01.2022) / (accessed on 23.01.2022); [e] Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Департамента информационной безопасности Банка России / Center for Monitoring and Response to Computer Attacks in the Financial Sphere (FinCERT) of the Information Security Department of the Bank of Russia. URL: https://cbr.ru/analytics/ib/fincert/ (дата обращения: 23.01.2022) / (accessed on 23.01.2022); [f] Банки США строят систему защиты от масштабных кибератак / US Banks build system of defense against large-scale cyber-attacks (06.12.2017). URL: https://www.securitylab.ru/news/490069.php (дата обращения: 23.01.2022) / (accessed on 23.01.2022); [g] Карасев П. Новые стратегии США в области кибербезопасности / Karasev P. New US cybersecurity strategies (15.11.2018). URL: https://russiancouncil.ru/analytics-and-comments/analytics/novye-strategii-ssha-v-oblasti-kiberbezopasnosti/ (дата обращения: 23.01.2022) / (accessed on 23.01.2022); [h] Киберготовность Соединенного Королевства: краткий обзор / United Kingdom cyberreadiness: a brief overview (октябрь 2016). URL: https://analytica.digital.report/wp-content/uploads/2017/05/CRI-UK-RU.pdf (дата обращения: 23.01.2022) / (accessed on 23.01.2022); [i] Кибербезопасность российской экономики и банковской индустрии в целом / Cyber security of the Russian economy and banking industry in general (17.02.2021). URL: https://plusworld.ru/professionals/kiberbezopasnost-rossijskoj-ekonomiki-i-bankovskoj-industrii-v-tselom/ (дата обращения: 23.01.2022) / (accessed on 23.01.2022); Кибербезопасность 2021. Кто виноват и что делать? / Cybersecurity 2021. Who is to blame and what to do? (12.11.2021). URL: https://plusworld.ru/journal/2021/plus-8–2021/kiberbezopasnost-2021-kto-vinovat-i-chto-delat/ (дата обращения: 23.01.2022) / (accessed on 23.01.2022); Ревенков П. Обеспечение кибербезопасности в кредитно-финансовой сфере / Revenkov P. Ensuring cyber security in the financial and credit sphere (06.11.2019). URL: https://www.secuteck.ru/articles/obespechenie-kiberbezopasnosti-v-kreditno-finansovoj-sfere (дата обращения: 23.01.2022) / (accessed on 23.01.2022); [j] Google и Microsoft взяли на себя обязательства вложиться в кибербезопасность / Google and Microsoft has committed to invest in cybersecurity (26.08.2021). URL: https://www.forbes.ru/newsroom/tehnologii/438209-google-i-microsoft-vzyali-na-sebya-obyazatelstva-vlozhitsya-v (дата обращения 24.01.2022) / (accessed on 24.01.2022); [k] Завтрашняя экономика Британии — план правительства / Britain's economy tomorrow — the government's plan. URL: https://d-russia.ru/zavtrashnyaya-ekonomika-britanii-plan-pravitelstva.html (дата обращения 24.01.2022); Цифровая экономика Британии — состояние и планы развития / Britain's digital economy — state and development plans. URL: https://d-russia.ru/tsifrovaya-ekonomika-britanii-sostoyanie-i-plany-razvitiya.html (дата обращения: 24.01.2022) / (accessed on 24.01.2022); [l] Киберпреступность и киберконфликты: Китай / Cybercrime and cyberconflict: China (14.07.2021). URL: https://www.tadviser.ru/index.php/Статья:_Киберпреступность_и_киберконфликты:_Китай#. (дата обращения: 24.01.2022) / (accessed on 24.01.2022).

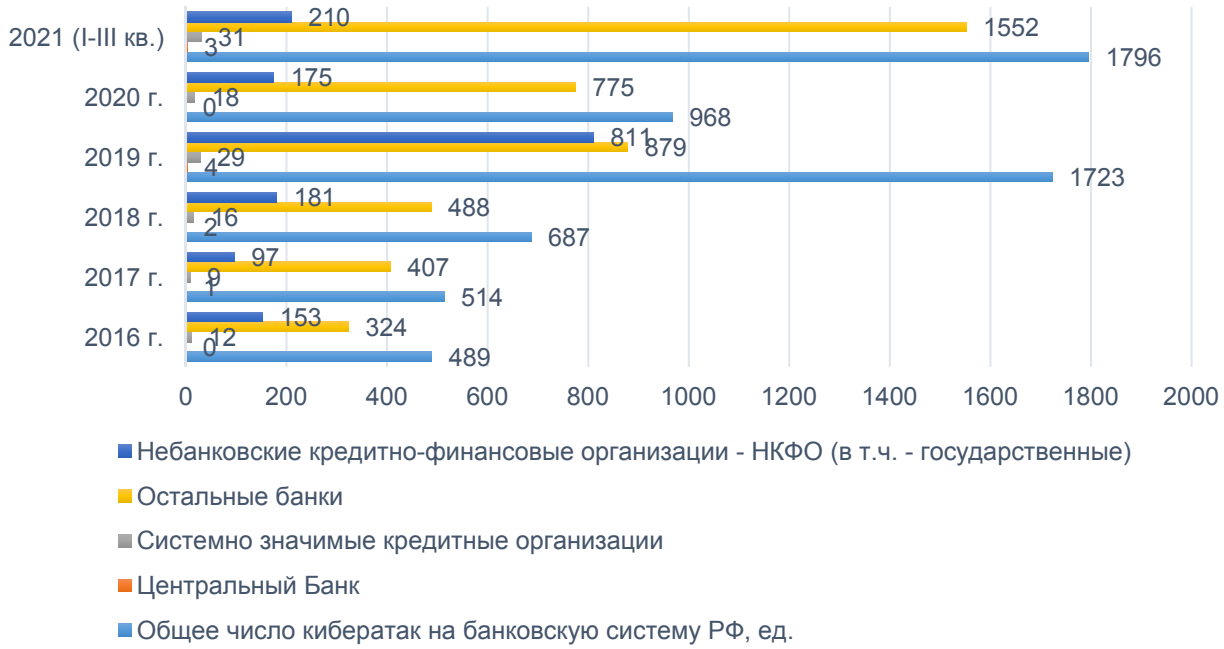

Рис. 1 / Fig. 1. **Количество кибератак на банковскую систему РФ в разрезе ее функциональных уровней за 2016–2021 гг. (I–III кв.), ед. / Number of Cyber Attacks on the Russian Banking System by Functional Level in 2016–2021 (Q1–Q3), units**

Источники / Sources: Обзор операций, совершенных без согласия клиентов финансовых организаций за 2016 год: аналитический отчет Департамента информационной безопасности Банка России / Overview of transactions made without the consent of clients of financial organizations in 2016: analytical report of the Information Security Department of the Bank of Russia (21.02.2017). URL: https://cbr.ru/Collection/Collection/File/32093/survey_transfers_16.pdf (дата обращения 25.01.2022)/ (accessed on 25.01.2022); Обзор операций, совершенных без согласия клиентов финансовых организаций за 2017 год: аналитический отчет Департамента информационной безопасности Банка России / Overview of transactions made without the consent of clients of financial organizations in 2017: analytical report of the Information Security Department of the Bank of Russia (15.10.2018) URL: https://cbr.ru/Collection/Collection/File/32094/survey_transfers_17.pdf (дата обращения: 25.01.2022) / (accessed on 25.01.2022); Обзор операций, совершенных без согласия клиентов финансовых организаций за 2018 год: аналитический отчет Департамента информационной безопасности Банка России / Overview of transactions made without the consent of clients of financial organizations for 2018: analytical report of the Information Security Department of the Bank of Russia (06.03.2019). URL: https://cbr.ru/Collection/Collection/File/32091/gubzi_18.pdf (дата обращения: 25.01.2022) / (accessed on 25.01.2022); Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год: аналитический отчет Департамента информационной безопасности Банка России / Overview of transactions made without the consent of clients of financial organizations for 2019: analytical report of the Information Security Department of the Bank of Russia (19.02.2020). URL: https://cbr.ru/Collection/Collection/File/32189/Review_of_transactions_2019.pdf (дата обращения: 26.01.2022) / (accessed on 26.01.2022); Обзор операций, совершенных без согласия клиентов финансовых организаций за 2020 год: аналитический отчет Департамента информационной безопасности Банка России / Overview of operations performed without the consent of clients of financial organizations for 2020: analytical report of the Information Security Department of the Bank of Russia (12.06.2021). URL: https://cbr.ru/Collection/Collection/File/32190/Review_of_transactions_2020.pdf (дата обращения: 26.01.2022) / (accessed on 26.01.2022); Актуальные киберугрозы: III квартал 2021 года / Current Cyber Threats: Q3, 2021 (08.12.2021). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q3/#id2 (дата обращения: 26.01.2022) / (accessed on 26.01.2022).

Рассмотрим основные мотивы совершения кибератак на банковскую систему РФ. Полученные результаты позволят определить основные точки (зоны) внимания банков при оценке киберустойчивости собственных бизнес-моделей (*рис. 4*).

Данные, приведенные на *рис. 4*, позволяют сделать вывод, что ключевым мотивом к совершению кибератак выступает получение финансовой выгоды от кражи денег и их эквивалентов с целью обогащения — в среднем на него пришлось 72,5%. Однако важно отметить, что его удельный вес в структуре мотивов постепенно снижается: это объясняется, с одной стороны, усилением работы банков над собственной защищенностью от внешних и вну-

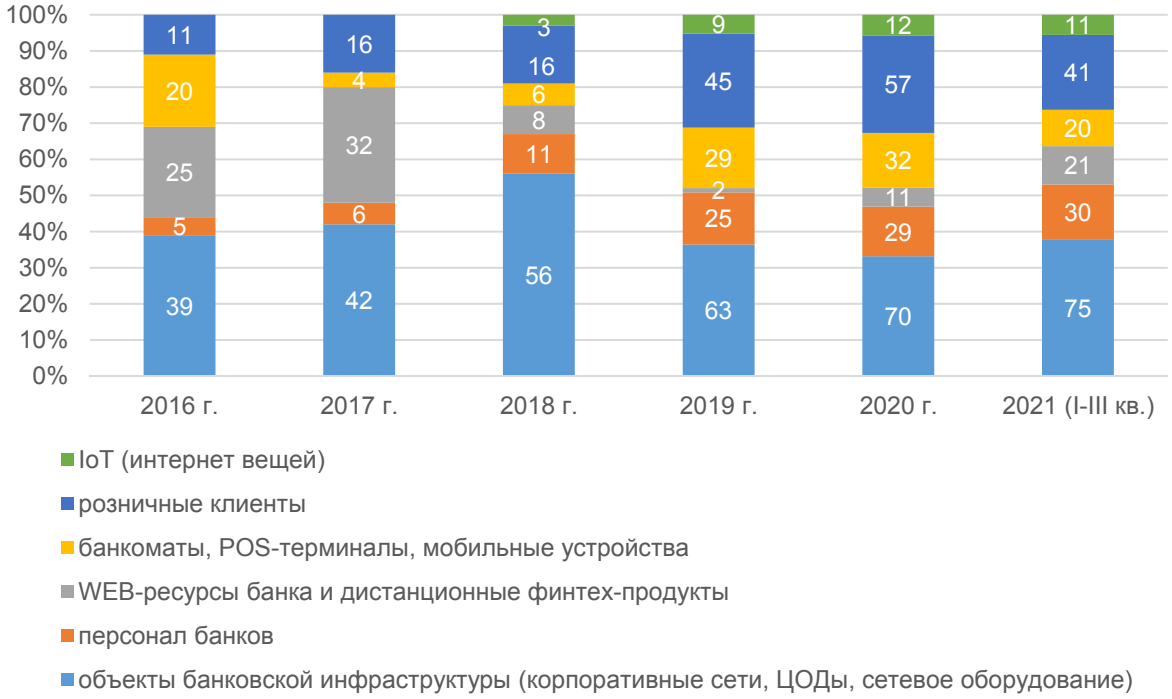

Рис. 2 / Fig. 2. **Состав и структура объектов банковской системы, подверженных кибератакам за 2016–2021 гг. (I–III кварталы), в % / Composition and structure of banking system facilities exposed to cyber-attacks for 2016–2021 (Q1–Q3), in %**

Источники / Sources: Кибербезопасность 2016–2017: от итогов к прогнозам / Cybersecurity 2016–2017: from totals to forecasts (26.01.2017). URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016–2017-rus.pdf (дата обращения: 27.01.2022) / (accessed on 27.01.2022); Актуальные киберугрозы — 2017. Тренды и прогнозы / Current cyber threats — 2017. Trends and forecasts (06.03.2017). URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf (дата обращения: 27.01.2022) / (accessed on 27.01.2022); Кибербезопасность 2017–2018: цифры, факты, прогнозы / Cybersecurity 2017–2018: figures, facts, forecasts (13.12.2017). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2017–2018/ (дата обращения: 27.01.2022) / (accessed on 27.01.2022); Кибербезопасность 2018–2019: цифры, факты, прогнозы / Cybersecurity 2018–2019: figures, facts, forecasts (18.12.2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2018–2019/ (дата обращения: 27.01.2022) / (accessed on 27.01.2022); Актуальные киберугрозы — 2018. Тренды и прогнозы / Current cyber threats — 2018. Trends and forecasts (12.03.2019). URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-rus.pdf (дата обращения: 27.01.2022) / (accessed on 27.01.2022); Кибербезопасность 2019–2020. Тренды и прогнозы / Cybersecurity 2019–2020. Trends and Forecasts (19.12.2019). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019–2020/ (дата обращения: 27.01.2022) / (accessed on 27.01.2022).

тренних киберрисков, а с другой — более активной работой Центробанка по информированию о киберинцидентах и проведению тестов банков на киберустойчивость[15].

В то же время вырос удельный вес такого мотивирующего фактора, как получение и последующая продажа персональных данных, шантаж и вымогательство — за I–III квартал 2021 г. его удельный вес составил 47,0%: активное развитие практик социальной инженерии и популяризация виртуальных сервисов обусловили развитие моделей хищения персональных данных с целью их продажи в DarkNet-сети или использовании для шантажа и вымогательств.

К концу 2021 г. также отмечается рост таких настораживающих факторов, как хактивизм (популяризация хакерской культуры и кибератак) — 20,0% и фиксация признаков организованных и санкционированных профильными государственными регуляторами программных кибератак (4,0%).

Эти две тенденции несут в себе опасный потенциал, так как на фоне пандемии и снижения реальных доходов населения возрастает социальная напряженность среди населения, а эскалация военно-политического противостояния России и блока

[15] Банк России подвел итоги первых антихакерских учений (10.02.2021). URL: https://www.mn.ru/smart/bank-rossii-podvel-itogi-pervyh-antihakerskih-uchenij-uchastie-v-nih-bylo-dobrovolnym (дата обращения: 28.01.2022).

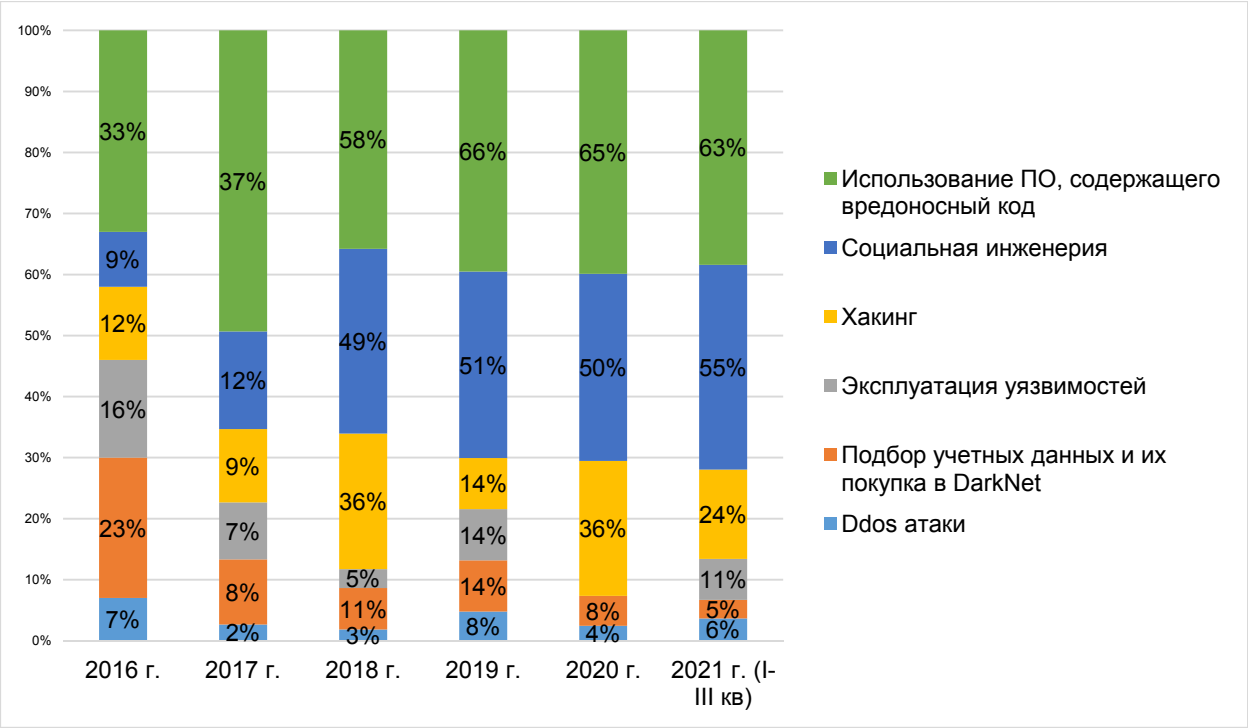

Рис. 3 / Fig. 3. **Инструменты реализации кибератак в отношении участников банковской системы Российской Федерации в 2016–2021 гг. (I–III кв.), в % / Cyberattack tools against members of the Russian banking system in 2016–2021 (Q1–Q3), %**

Источники / Sources: Тестирование на проникновение в организациях кредитно-финансового сектора / Penetration testing in credit sector organizations (20.02.2020). URL: https://www.ptsecurity.com/ru-ru/research/analytics/pentest-finance-2020/ (дата обращения: 28.01.2022) / (accessed on 28.01.2022); APT-атаки на кредитно-финансовую сферу в России: обзор тактик и техник/ ART-attacks on the credit and financial sphere in Russia: a review of tactics and techniques (10.10.2019). URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-finance-2019/ (дата обращения: 28.01.2022) / (accessed on 28.01.2022); Защищенность кредитно-финансовой сферы, итоги 2018 года. Оценка Positive Technologies / Credit and financial security, 2018 results. Positive Technologies Assessment (05.07.2020). URL: https://www.ptsecurity.com/ru-ru/research/analytics/credit-and-financial-security-2019/ (дата обращения: 28.01.2022) / (accessed on 28.01.2022); Уязвимости онлайн-банков: подводим итоги анализа / Vulnerabilities of online banks: summarizing the analysis (05.04.2019). URL: https://www.ptsecurity.com/ru-ru/research/analytics/vulnerabilities-rbo-2019/ (дата обращения: 28.01.2022) / (accessed on 28.01.2022); Векторы хакерских атак на банки / Vectors of hacker attacks on banks (05.06.2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/banks-attacks-2018/ (дата обращения: 28.01.2022) / (accessed on 28.01.2022); Статистика уязвимостей финансовых приложений / Financial application vulnerability statistics (24.04.2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-application-vulnerabilities-2018/ (дата обращения: 28.01.2022) / (accessed on 28.01.2022); Актуальные киберугрозы: III квартал 2021 года / Current cyber threats: Q3, 2021 (08.12.2021). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q3/#id2 (дата обращения: 27.01.2022) / (accessed on 27.01.2022).

НАТО вполне может быть дополнена проведением массированных кибератак на объекты банковской инфраструктуры.

Вместе с тем доказать факт наличия угрозы кибервойны непросто: следуя нормам международного гуманитарного права, это означает признание государства агрессором со всеми вытекающими отсюда политическими и экономическими последствиями для всех участников[16].

На заключительном этапе исследования был проведен анализ защищенности российских банков от кибератак за 2016–2021 гг. (I–III кв.) (*табл. 2*).

Как следует из приведенных данных в *табл. 2*, несмотря на повышение уровня успешно отражен-

[16] The right tool for the job: how does international law apply to cyber operations? (06.10.2020). URL: https://blogs.icrc.org/law-and-policy/2020/10/06/international-law-cyber-operations/ (дата обращения: 28.01.2022); Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts (март 2021). URL: https://international-review.icrc.org/articles/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913 (дата обращения: 28.01.2022).

Рис. 4 / Fig. 4. **Состав и структура мотивов совершения кибератак на банковскую систему за 2016–2021 гг. (I–III кв.), в % / Composition and structure of motives for cyberattacks on the banking system in 2016–2021 (Q1–Q3), in %**

Источники / Sources: Тестирование на проникновение в организациях кредитно-финансового сектора / Penetration testing in credit sector organizations (20.02.2020). URL: https://www.ptsecurity.com/ru-ru/research/analytics/pentest-finance-2020/ (дата обращения: 29.01.2022) / (accessed on 29.01.2022); APT-атаки на кредитно-финансовую сферу в России: обзор тактик и техник / ART-attacks on the credit and financial sphere in Russia: a review of tactics and techniques (10.10.2019). URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-finance-2019/ (дата обращения: 29.01.2022) / (accessed on 29.01.2022); Защищенность кредитно-финансовой сферы, итоги 2018 года. Оценка Positive Technologies / Credit and financial security, 2018 results. Positive Technologies Assessment (05.07.2020). URL: https://www.ptsecurity.com/ru-ru/research/analytics/credit-and-financial-security-2019/ (дата обращения: 29.01.2022) / (accessed on 29.01.2022); Уязвимости онлайн-банков: подводим итоги анализа / Vulnerabilities of online banks: summarizing the analysis (05.04.2019). URL: https://www.ptsecurity.com/ru-ru/research/analytics/vulnerabilities-rbo-2019/ (дата обращения: 29.01.2022) / (accessed on 29.01.2022); Векторы хакерских атак на банки / Vectors of hacker attacks on banks (05.06.2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/banks-attacks-2018/ (дата обращения: 29.01.2022) / (accessed on 29.01.2022); Статистика уязвимостей финансовых приложений / Financial application vulnerability statistics (24.04.2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-application-vulnerabilities-2018/ (дата обращения: 29.01.2022) / (accessed on 29.01.2022); Актуальные киберугрозы: III квартал 2021 года / Current cyber threats: Q3, 2021 (08.12.2021). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q3/#id2 (дата обращения: 29.01.2022) / (accessed on 29.01.2022).

ных кибератак на банки (52,7% в 2020 г. против 39,5% в 2016 г.), объем потерь для банковской системы постоянно возрастает. Кроме этого, констатируется снижение индекса устойчивости национальной банковской системы по категории коммерческих банков 2 группы — в 2020 г. он составил 3,4, тогда как в 2016 г. был 5,5.

Основываясь на изложенном выше аналитическом материале, авторы выявили основные проблемные точки (зоны), влияющие на киберустойчивость российской банковской системы в условиях продолжающихся цифровых трансформаций (*табл. 3*).

По итогу описания точек (зон) влияния на киберустойчивость российской банковской системы в заключительной части нашего исследования представляем рекомендации и предложения по организационно-экономическому и правовому совершенствованию системы защиты российских банков от внутренних и внешних киберугроз (*табл. 4*).

Полагаем, что обеспечение киберустойчивости банковской системы РФ требует применения системных мер, которые включают в себя как административные (совершенствование зако-

Таблица 2 / Table 2

Ключевые показатели защищенности российских банков от кибератак за 2016–2020 гг. / Key indicators of Russian banks' protection against cyberattacks for 2016–2020

Показатели / Indicators	2016	2017	2018	2019	2020
1. Показатель успешно отраженных кибератак, в % к итогу	39,5	42,4	44,7	49,5	52,7
2. Объем потерь банковской системы от кибератак, млн руб.	1080	961,3	1384,7	5723,5	8757,2
3. Уровень возмещения банками убытков от кибератак (сумма возвращенных банком средств / сумма похищенных средств * 100), в % к итогу	18,3	17,2	16,2	15	11,3
4. Индекс устойчивости национальной банковской системы (соотношение отраженных и успешно проведенных кибератак) по категориям банковских институтов:					
4.1. Центральный банк	–	1	2	4	–
4.2. Системно значимые кредитные учреждения	7,9	7,2	6,8	8	7,7
4.3. Коммерческие банки 2 группы	5,5	4,7	4,9	4,5	3,4
4.4. НКФО	6,2	5,8	5,5	4,9	4,1

Источники / Sources: Обзор операций, совершенных без согласия клиентов финансовых организаций за 2016 год: аналитический отчет Департамента информационной безопасности Банка России / Overview of transactions made without the consent of clients of financial organizations in 2016: analytical report of the Information Security Department of the Bank of Russia (21.02.2017). URL: https://cbr.ru/Collection/Collection/File/32093/survey_transfers_16.pdf (дата обращения: 17.05.2021) / (accessed on 17.05.2021); Обзор операций, совершенных без согласия клиентов финансовых организаций за 2017 год: аналитический отчет Департамента информационной безопасности Банка России / Overview of transactions made without the consent of clients of financial organizations in 2017: analytical report of the Information Security Department of the Bank of Russia (15.10.2018). URL: https://cbr.ru/Collection/Collection/File/32094/survey_transfers_17.pdf (дата обращения: 17.05.2021) / (accessed on 17.05.2021); Обзор операций, совершенных без согласия клиентов финансовых организаций за 2018 год: аналитический отчет Департамента информационной безопасности Банка России / Overview of transactions made without the consent of clients of financial organizations in 2018: analytical report of the Information Security Department of the Bank of Russia (06.03.2019). URL: https://cbr.ru/Collection/Collection/File/32091/gubzi_18.pdf (дата обращения: 17.05.2021)/ (accessed on 17.05.2021); Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год: аналитический отчет Департамента информационной безопасности Банка России/ Overview of transactions made without the consent of clients of financial organizations in 2019: analytical report of the Information Security Department of the Bank of Russia (19.02.2020). URL: https://cbr.ru/Collection/Collection/File/32189/Review_of_transactions_2019.pdf (дата обращения: 17.05.2021)/ (accessed on 17.05.2021); Обзор операций, совершенных без согласия клиентов финансовых организаций за 2020 год: аналитический отчет Департамента информационной безопасности Банка России / Overview of transactions made without the consent of clients of financial organizations in 2020: analytical report of the Information Security Department of the Bank of Russia (12.06.2021). URL: https://cbr.ru/Collection/Collection/File/32190/Review_of_transactions_2020.pdf (дата обращения: 17.05.2021)/ (accessed on 17.05.2021).

нодательства в вопросах оборота персональных данных, ужесточения ответственности за их сохранность и совершение киберпреступлений), экономические (формирование банками целевых бюджетов расходов на информационную безопасность) меры, так и общественно-просветительскую работу, направленную на формирование необходимых компетенций в сфере безопасного поведения клиентов в виртуальном пространстве.

ВЫВОДЫ

По итогам проведенного научного исследования было установлено, что, в целом, имеет место тенденция к увеличению угроз цифровой экономики для устойчивости национальной банковской системы и росту их качественной, профессиональной составляющей, что косвенно свидетельствует о вероятном присутствии политических интересов стран — участниц НАТО в части идентификации

Таблица 3 / Table 3

Основные проблемные точки (зоны) влияния на киберустойчивость российской банковской системы / Main problem points (zones) of influence on the cyber resilience of the Russian banking system

Проблемная точка (зона) / Problem Point (Zone)	Характеристика проблемной точки (зоны), оценка ее влияния / Characteristics of the problem point (zone), assessment of its impact
1. Отсутствие рыночной саморегуляции и обмена информацией о совершенных кибератаках и механизмах их совершения	*Характеристика проблемной точки (зоны):* в настоящее время в РФ отсутствует институт рыночной саморегуляции банков, НКФО и их клиентов (физических и юридических) в части обмена информацией о кибератаках и механизмах их совершения ввиду рисков потери деловой репутации, ослабления конкурентных позиций на рынке, корпоративного эгоизма менеджмента[a]. *Оценка влияния проблемной точки (зоны)*: информационный вакуум способствует масштабированию кибератак и их тиражированию, так как опыт противодействия им формируется индивидуально каждым банком, т.е. у инициаторов атак появляется временное и технологическое преимущество в совершении кибератак и максимизации ущерба
2. Низкая эффективность сотрудничества сегмента e-commerce с государственным регулятором сети Интернет Роскомнадзором	*Характеристика проблемной точки (зоны):* в настоящее время между сегментом e-commerce и Роскомнадзором превалируют меры административного воздействия на нарушение правил работы с персональными данными клиентов, необеспечение должной защиты при их обработке и т.д.[b] Вместе с тем вопрос превентивной защиты от кибератак, повышение киберграмотности менеджмента сферы e-commerce носит крайне локальный и точечный характер, что делает сегмент e-commerce точкой вторжения хакеров для получения последующего доступа к банковским продуктам (картам, мобильному банкингу и т.п.). *Оценка влияния проблемной точки (зоны)*: e-commerce сегмент является важнейшим источником для кражи персональных данных клиентов и их использования для получения доступа к банковским продуктам: по данным FreightWave, количество онлайн-преступлений в сфере e-commerce увеличилось на 50% в 2020 г.[c]
3. Недостаточная профессиональная подготовка и компетентность сотрудников банков в части выявления признаков кибератаки	*Характеристика проблемной точки (зоны):* по данным отчета PWC только 16% руководителей банков ведут системную работу по формированию в составе службы безопасности команды киберспециалистов и их интеграции в бизнес-процессы всех подразделений банка и 23% проводят регулярное повышение квалификации персонала банка на предмет идентификации киберугроз на рабочих местах[d]. *Оценка влияния проблемной точки (зоны)*: человеческий фактор рассматривается как важная уязвимость для проведения кибератак по мере совершенствования технических аспектов защиты периметра банка. С учетом развития практик социальной инженерии использование уязвимости за счет человеческого фактора становится очень эффективным средством: при высоком качестве схемы атаки ее идентификация в составе операционных бизнес-процессов становится крайне сложно идентифицируемой
4. Ограниченность бюджета малых и средних банков, не позволяющих им содержать самостоятельные подразделения киберзащиты	*Характеристика проблемной точки (зоны):* по данным отчета Positive Technologies, только у 29,0% банков формируется регулярный бюджет на финансирование программ киберзащиты, а у 32,0% — осуществляются однократные инвестиции в приобретение новых инструментов кибербезопасности[e]. *Оценка влияния проблемной точки (зоны)*: острая дифференциация расходов на кибербезопасность отражается на общей киберустойчивости банковской системы, так как попадание внутрь защищенного периметра вредоносного объекта не только свидетельствует о наличии уязвимости, но и с учетом экспоненциального роста корреспондентских счетов между банками мультиплицирует риски «заражения» даже самых защищенных банков

Окончание таблицы 3 / Table 3 (continued)

Проблемная точка (зона) / Problem Point (Zone)	Характеристика проблемной точки (зоны), оценка ее влияния / Characteristics of the problem point (zone), assessment of its impact
5. Популяризация и активный рост рыночного присутствия финтех-сервисов и компаний	*Характеристика проблемной точки (зоны):* финтех-компании в РФ преимущественно являются надстройками банков и подчиняются общей политике безопасности, однако имеется и группа самостоятельных НКФО (по данным за 2020 г. – 71 ед.[f]), целевое использование которой преимущественно заключается в организации денежных переводов в обход банка (анонимные кошельки, P2P-транзакции). Так, с января по май 2020 г. зафиксировано 165 тысяч мошеннических операций на общую сумму 1,6 млрд руб.)[g] *Оценка влияния проблемной точки (зоны)*: бизнес-модели финтех-компаний строятся по отличным от традиционных банков принципам и, что важно, не подчиняются большинству норм безопасного функционирования банков, установленных Центробанком. Кроме этого, нерегулируемое развитие финтех-сервисов ставит под угрозу соблюдение Россией стандартов ФАТФ (Группы разработки финансовых мер борьбы с отмыванием денег) [17]

Источники / Sources: разработано авторами на основании/ developed by authors based on:

[a] Результаты исследования мнения рынка по вопросам развития финансовых технологий на 2021–2023 гг./ The results of a study of the market opinions on the development of financial technologies for 2021–2023 (2020). URL: https://www.accenture.com/_acnmedia/PDF-163/Accenture-Result-Research-Market-Opinion-Russian.pdf (дата обращения: 28.01.2022) / (accessed on 28.01.2022); [b] Like war, shares of destruction. How Roskomnadzor fights social networks and what will happen next (06.12.2021). URL: https://skillbox.ru/media/business/kak-roskomnadzor-boretsya-s-sotssetyami/ (дата обращения: 29.01.2022) / (accessed on 29.01.2022); [c] E-commerce cybercrime jumped 50% in 2020. URL: https://www.freightwaves.com/news/e-commerce-cybercrime-jumped-50-in-2020 (дата обращения: 29.01.2022) / (accessed on 29.01.2022); [d] Глобальное исследование «Доверие к цифровым технологиям» 2021 / Global research "Trust in digital technologies" 2021. URL: https://www.pwc.ru/ru/publications/dti-2021/e-version-digital-trust-insights-2021-in-russian.pdf (дата обращения: 30.01.2022) / (accessed on 30.01.2022); [e] Сколько стоит безопасность. Анализ процессов обеспечения информационной безопасности в российских компаниях / How much is security. Analysis of information security processes in Russian companies (2017). URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/IS-Cost-rus.pdf (дата обращения: 30.01.2022) / (accessed on 30.01.2022); Онлайн-безопасность превыше всего для банков / Online security above all for banks (29.04.2021). URL: https://www.comnews.ru/content/214362/2021–04–29/2021-w17/onlayn-bezopasnost-prevyshe-vsego-dlya-bankov (дата обращения: 30.01.2022) / (accessed on 30.01.2022). [f] Fintech by the numbers Incumbents, startups, investors adapt to maturing ecosystem (2020). URL: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/financial-services/fintech-by-the-numbers.pdf (дата обращения: 30.01.2022) / (accessed on 30.01.2022); Развитие финтех-рынка в России: необанки и стартапы / Development of the fintech-market in Russia: neobanks and startups (11.12.2019). URL: https://www.finam.ru/analysis/forecasts/razvitie-fintex-rynka-v-rossii-neobanki-i-startapy-20191211–142048/ (дата обращения: 30.01.2022) / (accessed on 30.01.2022); [g] Финансовый регулятор раскрыл объем мошеннических операций в 2020 году/ Financial regulator disclosed volume of fraudulent transactions in 2020 (23.06.2020). URL: https://долг.рф/short_news/160461/?utm_source=yxnews&utm_medium=desktop (дата обращения: 22.07.2021) / (accessed on 22.07.2022).

потенциальных уязвимостей периметра банковской системы РФ.

При анализе киберустойчивости банковской системы России было установлено, что, несмотря на рост успешности отражения кибератак, потери национальной банковской системы увеличились. Это связано в первую очередь с возрастанием атак, направленных на подрыв доверия населения к банкам, а также учащением случаев использования «белых пятен» в национальном законодательстве со стороны финтех-компаний в собственных корыстных интересах.

Отметим, что государственный регулятор в лице Центрального банка России проводит активную и системную работу по снижению количества источников киберрисков и активно совершенствует законодательную базу по пресечению использования юридических коллизий и неурегулированности вопросов привлечения к ответственности за совершенные деяния в сфере преступлений с использованием ИКТ.

Статья вносит теоретический вклад в развитие проблематики обеспечения киберустойчивости банковской системы России и совершенствование практик организации системы киберзащиты в банках и НКФО. Полагаем, что материал статьи будет полезен для всех, кто интересуется вопро-

Таблица 4 / Table 4

Рекомендации и предложения по организационно-экономическому и правовому совершенствованию системы защиты российских банков от внутренних и внешних киберугроз / Recommendations and proposals for organizational, economic and legal improvements to the system of protection of Russian banks from internal and external cyberthreats

Рекомендации/ предложения / Recommendations/ suggestions	Содержание рекомендаций/предложений. Оценка возможного эффекта / Contents of the recommendations/suggestions. Assessment of the possible effect
1. Интенсификация процессов развития бизнес-модели банковских экосистем	*Содержание предложения.* Экосистема как бизнес-модель имеет в качестве ядра сильный и финансово устойчивый банк, который способен не только формировать зону притяжения для партнеров, но и заинтересован в обеспечении создания безопасного пространства для совершения транзакций для клиентов и партнеров, что, собственно, гарантирует устойчивость и экономическую ценность экосистемы для всех ее участников. *Оценка возможного эффекта:* 1) формирование рыночных центров аккумулирования информации о киберугрозах в рамках экосистемы и ее циркуляции между участниками; 2) накопление опыта противодействия кибератакам и снижение их влияния на участников банковской экосистемы; 3) масштабирование и тиражирование сложных ИКТ-решений обеспечения защиты банковской инфраструктуры и клиентских устройств доступа. *Примеры успешных практик применения:* в бизнес-модели экосистемы, возглавляемой ПАО «Сбербанк», реализуется методология CARTA (Continuous adaptive risk and trust assessment) — специальная банковская структура ведет постоянное наблюдение за всеми рисками, возникающими в экосистеме, а защитные меры должны быть продуманы и реализованы в каждом процессе, каждым участником, а информационное взаимодействие банка — главы экосистемы с партнерами реализуется через многоступенчатую фильтр-систему с реализацией спецификации OpenID Connect (фреймворк OAuth 2.0)[a]
2. Создание федерального межбанковского реестра счетов кибермошенников[b]	*Содержание предложения.* Начиная с 2018 г. обсуждается инициатива о создании межбанковского реестра счетов, с помощью которых мошенники выводят похищенные денежные средства, однако до сих пор его разработка остается на уровне частных решений крупнейших банков страны, что не позволяет системно подойти к решению данной проблемы. *Оценка возможного эффекта:* 1) сокращение вариантов выведения денежных средств за рубеж; 2) повышение прозрачности и контроля за сомнительными транзакциями; 3) привлечение к ответственности банков и финтех-компаний, уличенных в пособничестве хакерам и мошенникам. *Примеры успешных практик применения:* банковский регулятор Саудовской Аравии реализует инициативу SOC-центра, хранящего цифровой профиль каждого банка и финтех-компании, статистику кибератак, опыт их отражения и результаты расследований по сомнительным операциям или актам мошенничества банков и финтех-бизнесов
3. Формирование единого банковского «полигона» для тестирования уязвимостей программного обеспечения	*Содержание предложения.* Разработка при участии Банка России, ГК «Ростех» и Ассоциации банков России совместного инфраструктурного решения — «тестировочной песочницы» для проведения испытаний новых программных продуктов и решений в области киберзащиты, а также имитации атак на существующие архитектуры организации защиты бизнес-процессов банков так называемыми «белыми хакерами»[c]. *Оценка возможного эффекта:* 1) формирование национальной методологии проведения тестирования программного обеспечения на наличие уязвимостей; 2) выявление «черных входов» и шпионских кодов в иностранном программном обеспечении для банков и финтех-сервисов; 3) повышение квалификации специалистов в сфере кибербезопасности и популяризация безопасной работы; 4) проведение полноценных учений возможных кибератак различной масштабности. *Оценка возможного эффекта.* В РФ формирование платформы тестирования уязвимостей банковского ПО и архитектуры информационной модели регламентировано Федеральным проектом «Информационная безопасность» (программа «Цифровая экономика РФ»)[d]. *Примеры успешных практик применения:* в США в 2017 г. была принята концепция zero trust (нулевое доверие даже к пользователям внутри периметра ИКТ-архитектуры бизнеса) и на ее основе создана коммерческая платформа DataVisor Global Intelligence Network[e], позволяющая тестировать уязвимости ПО банков за плату, а также конструировать различные сценарии атак

Окончание таблицы 4 / Table 4 (continued)

Рекомендации/ предложения / Recommendations/ suggestions	Содержание рекомендаций/предложений. Оценка возможного эффекта / Contents of the recommendations/suggestions. Assessment of the possible effect
4. Развитие регулятивного надзора за операционной деятельностью финтех-сервисов	*Содержание предложения.* В настоящее время самостоятельные финтех-компании, действующие вне банковских лицензий, практически не урегулированы в своей операционной деятельности. В частности, следует рассмотреть введение регуляции по таким аспектам, как введение практики screen scrapping (мониторинг операционных рисков), ужесточение правил оборота и идентификации при использовании SIM-карт, номеров телефона, услуг провайдеров и хостеров при аренде серверов. *Оценка возможного эффекта:* 1) формирование открытой доверительной среды обмена информацией о неблагонадежных клиентах и объектах инфраструктуры; 2) формирование базы цифровых профилей юридических и физических лиц с оценкой рисков их финансового поведения на основе анализа финансовых транзакций и деловых операций. *Примеры успешных практик применения:* Банк Англии в 2015 г. инициировал обязательный переход банков на API (Application programming interface)[f], что позволит банкам и государственному регулятору идентифицировать на ранней стадии неблагонадежных клиентов и объекты телекоммуникационной инфраструктуры (например, телеком-провайдеры), обеспечивающие реализацию потенциально киберопасных транзакций
5. Развитие практики «киберпатронажа» со стороны банков — владельцев экосистем и администраторов суперсервисов	*Содержание предложения.* Альтернативным решением обеспечения достаточной кибербезопасности малых и средних банков по новым стандартам киберустойчивости является заключение партнерского соглашения с управляющими банками экосистем или администраторов суперсервисов для предоставления права пользования защищенной инфраструктурой за определенную плату. В таком случае риски проведения атак распределяются между сторонами и обе стороны получают синергетический эффект от взаимодействия: патроны — дополнительный доход, малые банки — доступ к защищенной инфраструктуре и возможность развивать новые сервисы и банковские продукты на ландшафте экосистемы
6. Повышение финансовой грамотности розничных и корпоративных клиентов банков и НКФО	*Содержание предложения.* Российский индекс финансовой грамотности (РИФГ) в 2020 г. составил 54 балла (в 2018 г.— 53, в 2017 г.— 52)[g], что объективно недостаточно для формирования безопасного поведения в условиях эскалации киберугроз. Исходя из этого, следует принять ряд мер по популяризации безопасного поведения в сети Интернет при совершении финансовых операций, а также по проведению консультационной и информационно-просветительской работы об актуальных киберугрозах в форме TV-передач, подкастов на радио и популярных форумах в социальных сетях, онлайн-встречах со специалистами в области кибербезопасности[h]

Источники / Sources: разработано авторами по данным [18–27] / developed by authors based on [18–27]:

[a] Сбербанк: экосистема — новые возможности, новые вызовы кибербезопасности / Sberbank: ecosystem — new opportunities, new challenges to cybersecurity (11.01.2019). URL: https://www.it-world.ru/cionews/security/158287.html (дата обращения: 30.01.2022) / (accessed on 30.01.2022); [b] Кибератаки на банки: тренды, уязвимости и роль регулятора / Cyberattacks on banks: trends, vulnerabilities and the role of regulator (27.07.2018). URL: https://plusworld.ru/professionals/kiberataki-na-banki-trendy-uyazvimosti-i-rol-regulyatora/ (дата обращения: 30.01.2022) / (accessed on 30.01.2022); [c] Результаты исследования мнения рынка по вопросам развития финансовых технологий на 2021–2023 гг./ The results of a study of the market opinions on the development of financial technologies for 2021–2023 URL: https://www.accenture.com/_acnmedia/PDF-163/Accenture-Result-Research-Market-Opinion-Russian.pdf (дата обращения: 30.01.2022) / (accessed on 30.01.2022); [d] Выполнение работ по созданию киберполигона для обучения и тренировки учащихся, специалистов и экспертов разного профиля, руководителей в области информационной безопасности и ИТ современным практикам обеспечения безопасности / Execution of works on the creation of Cyber Range to training students, specialists and experts of various disciplines, managers in the field of information security and IT to modern security practices. URL: https://digital.gov.ru/uploaded/files/03kiberpoligontz.pdf (дата обращения: 31.01.2022) / (accessed on 31.01.2022); [e] Список Gartner: какие технологии помогут бизнесу в 2022 году/ Gartner List: what technologies will help business in 2022 (18.11.2021). URL: https://habr.com/ru/company/netologyru/blog/590117/ (дата обращения: 31.01.2022) / (accessed on 31.01.2022); DataVisor. URL: https://www.weforum.org/organizations/datavisor (дата обращения: 31.01.2022) / (accessed on 31.01.2022); [f] Информационно-аналитическое обозрение «Российская банковская система сегодня» / Information and analytical review of "Russian Banking System Today" (сентябрь 2019). URL: https://asros.ru/upload/iblock/c30/20397_informatsionnoanaliticheskoeobozrenie sentyabr2019.pdf (дата обращения: 17.01.2021) / (accessed on 17.01.2022); [g] Измерение уровня финансовой грамотности: 3 этап / To measure the level of financial literacy: 3rd stage. URL: https://cbr.ru/analytics/szpp/fin_literacy/fin_ed_intro/ (дата обращения: 31.01.2022) / (accessed on 31.01.2022); [h] Стратегия повышения финансовой грамотности в Российской Федерации на 2017–2023 годы. Распоряжение Правительства РФ № 2039-р от 25.09.2017 / Strategy for improving financial literacy in the Russian Federation for 2017–2023. Order of the Government of the Russian Federation No. 2039 from 25.09.2017. URL: http://static.government.ru/media/files/uQZdLRrkPL AdEVdaBsQrk505szCcL4PA.pdf (дата обращения: 31.01.2022) / (accessed on 31.01.2022).

сами безопасного финансового поведения, а также ответственных за кибербезопасность в банках, а также небанковской сфере, имеющей тесную связь с банковской инфраструктурой (e-commerce сегмент, венчурные команды в сфере финансовых технологий и др.).

БЛАГОДАРНОСТИ

Статья подготовлена в рамках государственного задания Института проблем рынка РАН, тема НИР «Институциональная трансформация экономической безопасности при решении социально-экономических проблем устойчивого развития национального хозяйства России». Институт проблем рынка РАН, Москва, Россия.

ACKNOWLEDGEMENTS

The article was prepared within a state assignment of the Market Economy Institute of the Russian Academy of Sciences; the topic of research is "Institutional transformation of economic security in the solution of socioeconomic sustainable development problems of the national economy of Russia". Market Economy Institute, Russian Academy of Sciences, Moscow, Russia.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. Яблочкин А.С., Кошкин А.П. Современные направления исследований в области стратегий информационной безопасности. *Национальная безопасность / nota bene*. 2019;(5):34–47. DOI: 10.7256/24540668.2019.5.31224
   Yablochkin A.S., Koshkin A.P. Current vectors of research in the area of information security strategies. *Natsional'naya bezopasnost' / nota bene = National Security / nota bene*. 2019;(5):34–47. (In Russ.). DOI: 10.7256/24540668.2019.5.31224 (In Russ.)
2. Тимоничева И.Н., Яновский В.В., Бережной А.С. Уровень доверия к безопасности финансовых технологий: барьер или точка роста. *Научный результат. Экономические исследования*. 2021;7(3):81–88. DOI: 10.18413/2409–1634–2021–7–3–0–7
   Timonicheva I.N., Yanovskiy V.V., Berezhnoy A.S. The level of confidence in the safety of financial technologies: A barrier or a point of growth. *Nauchnyi rezul'tat. Ekonomicheskie issledovaniya = Research Result. Economic Research*. 2021;7(3):81–88. DOI: 10.18413/2409–1634–2021–7–3–0–7 (In Russ.)
3. Ревенков П.В., Бердюгин А.А. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания. *Национальные интересы: приоритеты и безопасность*. 2017;13(9):1747–1760. DOI: 10.24891/ni.13.9.1747
   Revenkov P.V., Berdyugin A.A. Social engineering as a source of risks in online banking services. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*. 2017;13(9):1747–1760. DOI: 10.24891/ni.13.9.1747 (In Russ.)
4. Чалдаева Л.А., Килячков А.А., Якорев А.А. К вопросу о формировании государственных функций по обеспечению безопасности в виртуальном пространстве России. *Власть*. 2020;28(3):37–46. DOI: 10.31171/vlast.v28i3.7293
   Chaldaeva L.A., Kilyachkov A.A., Yakorev A.A. On the formation of state functions to ensure security in the virtual space of Russia. *Vlast' = The Authority*. 2020;28(3):37–46. (In Russ.). DOI: 10.31171/vlast.v28i3.7293 (In Russ.)
5. Быканова Н.И., Гордя Д.В., Евдокимов Д.В. Тенденции и закономерности процесса цифровизации банковского сектора. *Научный результат. Экономические исследования*. 2020;6(2):42–51. DOI: 10.18413/2409–1634–2020–6–2–0–6
   Bykanova N.I., Gordya D.V., Evdokimov D.V. Trends and patterns of the banking sector digitalization process. *Nauchnyi rezul'tat. Ekonomicheskie issledovaniya = Research Result. Economic Research*. 2020;6(2):42–51. DOI: 10.18413/2409–1634–2020–6–2–0–6 (In Russ.)
6. Khalifa N.A.-D. Cybercrime: theoretical determinants, criminal policies, prevention & control mechanisms. *International Journal of Technology and Systems*. 2020;5(1):34–63. DOI: 10.47604/ijts.1133
7. Zabala Aguayo F., Ślusarczyk B. Risks of banking services' digitalization: The practice of diversification and sustainable development goals. *Sustainability*. 2020;12(10):4040. DOI: 10.3390/SU 12104040
8. Dorn A.W., Webb S. Cyberpeacekeeping: New ways to prevent and manage cyberattacks. *International Journal of Cyber Warfare and Terrorism*. 2019;9(1):19–30. DOI: 10.4018/IJCWT.2019010102

9. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. *Вопросы кибербезопасности*. 2014;(5):39–42.
   Alpeev A. Terminology of security: Cybersecurity, information security. *Voprosy kiberbezopasnosti = Cybersecurity Issues*. 2014;(5):39–42. (In Russ.).
10. Безкоровайный М.М., Татузов А.Л. Кибербезопасность — подходы к определению понятия. *Вопросы кибербезопасности*. 2014;(1):22–27.
    Bezkorovainy M., Tatuzov A. Cybersecurity — approaches to the definition. *Voprosy kiberbezopasnosti = Cybersecurity Issues*. 2014;(1):22–27. (In Russ.).
11. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве. *Наукоемкие технологии в космических исследованиях Земли*. 2018;10(2):52–61. DOI: 10.24411/2409–5419–2018–10041
    Zakharchenko R.I., Korolev I.D. Methods of estimation of stability of functioning of objects of critical information infrastructure operating in cyberspace. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli = High Tech in Earth Space Research*. 2018;10(2):52–61. DOI: 10.24411/2409–5419–2018–10041 (In Russ.).
12. Carrapico H., Barrinha A. European Union cyber security as an emerging research and policy field. *European Politics and Society*. 2018;19(3):299–303. DOI: 10.1080/23745118.2018.1430712
13. Christou G. Cybersecurity in the European Union: Resilience and adaptability in governance policy. London: Palgrave Macmillan; 2016. 222 p. DOI: 10.1057/9781137400529
14. Горян Э.В. Закон о кибербезопасности Китайской Народной Республики как ключевой инструмент обеспечения информационной безопасности финансово-банковской системы. *Административное и муниципальное право*. 2020;(3):47–55. DOI: 10.7256/2454–0595.2020.3.32677
    Gorian E. Cybersecurity law of the People's Republic of China as a key instrument for ensuring information security of the banking and finance system. *Administrativnoe i munitsipal'noe pravo = Administrative and Municipal Law*. 2020;(3):47–55. DOI: 10.7256/2454–0595.2020.3.32677 (In Russ.).
15. Najaf K., Mostafiz M.I., Najaf R. Fintech firms and banks sustainability: Why cybersecurity risk matters? *International Journal of Financial Engineering*. 2021;8(2):2150019. DOI: 10.1142/s2424786321500195
16. Uddin M.H., Mollah S., Ali M.H. Does cyber tech spending matter for bank stability? *International Review of Financial Analysis*. 2020;72:101587. DOI: 10.1016/j.irfa.2020.101587
17. Поветкина Н.А., Леднева Ю.В. «Финтех» и «регтех»: границы правового регулирования. *Право. Журнал Высшей школы экономики*. 2018;(2):46–67. DOI: 10.17323/2072–8166.2018.2.46.67
    Povetkina N.A., Ledneva Yu.V. Fintekh and redtekh: Boundaries of legal regulation. *Pravo. Zhurnal Vysshei shkoly ekonomiki = Law. Journal of the Higher School of Economics*. 2018;(2):46–67. (In Russ.). DOI: 10.17323/2072–8166.2018.2.46.67 (In Russ.).
18. Vakulyk O., Petrenko P., Kuzmenko I., Pochtovyi M., Orlovskyi R. Cybersecurity as a component of the national security of the state. *Journal of Security and Sustainability Issues*. 2020;9(3):775–784. DOI: 10.9770/JSSI.2020.9.3(4)
19. Cybersecurity capacity maturity model for nations (CMM). Revised edition. Oxford: Global Cyber Security Capacity Center; 2020. DOI: 10.2139/ssrn.3657116
20. Sutherland E. Cybersecurity: Governance of a new technology. In: Proc. PSA18 Political Studies Association Int. conf. (Cardiff, 26–28 March 2018). London: Political Studies Association; 2018. DOI: 10.2139/ssrn.3148970
21. Camillo M. Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions*. 2017;10(2):196–200. URL: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/jrmfi-mark-camillo-article-mar-2017.pdf
22. Wang F.F. Legislative developments in cybersecurity in the EU. *Amicus Curiae*. 2020;1(2):233–259. DOI: 10.14296/ac.v1i2.5131
23. Bakker T.G., Streff K. Accuracy of self disclosed cybersecurity risks of large U.S. banks. *The Journal of Applied Business and Economics*. 2016;18(3):39–51. URL: http://www.na-businesspress.com/JABE/BakkerTG_Web18_3_.pdf
24. De Fréminville M. Cybersecurity and decision makers: Data security and digital trust. Hoboken. NJ: John Wiley & Sons, Inc.; 2020. 224 p.
25. Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия. *Социальные новации и социальные науки.* 2020;(1):77–96. DOI: 10.31249/snsn/2020.01.06

Semeko G.V. Information security in the financial sector: Cybercrime and countermeasures strategy. *Sotsial'nye novatsii i sotsial'nye nauki = Social Novelties and Social Sciences.* 2020;(1):77–96. DOI: 10.31249/snsn/2020.01.06 (In Russ.)

26. Нестерова Д.А. Риски информационной безопасности коммерческих банков в условиях новой экономической и технологической реальности. *Инновации и инвестиции.* 2020;(5):144–150.
Nesterova D.A. Information security risks of commercial banks in the new economic and technological reality. *Innovatsii i investitsii = Innovation & Investment*. 2020;(5):144–151. (In Russ.).
27. Шкодинский С.В., Дудин М.Н., Усманов Д.И. Анализ и оценка киберугроз национальной финансовой системе России в цифровой экономике. *Финансовый журнал*. 2021;13(3):38–53. DOI: 10.31107/2075–1990–2021–3–38–53
Shkodinsky S.V., Dudin M.N., Usmanov D.I. Analysis and assessment of cyberthreats to the national financial system of Russia in the digital economy. *Finansovyi zhurnal = Financial Journal*. 2021;13(3):38–53. DOI: 10.31107/2075–1990–2021–3–38–53 (In Russ.)

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Михаил Николаевич Дудин — доктор экономических наук, профессор, заместитель директора по науке, Институт проблем рынка РАН, Москва, Россия
Mikhail N. Dudin — Dr. Sci. (Econ.), Prof., Deputy Director for Science, Market Economy Institute, Russian Academy of Sciences, Moscow, Russia
http://orcid.org/0000-0001-6317-2916
Автор для корреспонденции / Corresponding author
dudinmn@mail.ru

Сергей Всеволодович Шкодинский — доктор экономических наук, профессор, заведующий лабораторией промышленной политики и экономической безопасности, Институт проблем рынка РАН, Москва, Россия; главный научный сотрудник Центра отраслевой экономики, Научно-исследовательский финансовый институт Минфина России, Москва, Россия
Sergey V. Shkodinsky — Dr. Sci. (Econ.), Prof., Head of the Laboratory of Industrial Policy and Economic Security, Market Economy Institute, Russian Academy of Sciences, Moscow, Russia; Chief Researcher at the Center for Sectoral Economics, Financial Research Institute, Moscow, Russia
http://orcid.org/0000-0002-5853-3585
sh-serg@bk.ru

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.
Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Статья поступила в редакцию 13.02.2022; после рецензирования 28.02.2022; принята к публикации 27.03.2022.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 13.02.2022; revised on 28.02.2022 and accepted for publication on 27.03.2022.
The authors read and approved the final version of the manuscript.