Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2023, Том 15, № 3 / 2023, Vol. 15, Iss. 3 https://esj.today/issue-3-2023.html

URL статьи: https://esj.today/PDF/08ECVN323.pdf

Ссылка для цитирования этой статьи:
Шкодинский, С. В. Цифровая трансформация банковских бизнес-моделей и проблемы обеспечения кибербезопасности / С. В. Шкодинский, Ю. А. Крупнов, О. М. Толмачев // Вестник евразийской науки. — 2023. — Т. 15. — № 3. — URL: https://esj.today/PDF/08ECVN323.pdf

For citation:
Shkodinsky S.V., Krupnov Yu.A., Tolmachev O.M. Digital transformation of banking business models and cybersecurity issues. *The Eurasian Scientific Journal*. 2023; 15(3): 08ECVN323. Available at: https://esj.today/PDF/08ECVN323.pdf. (In Russ., abstract in Eng.)

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»

УДК 336.7

ГРНТИ 06.73.55

Шкодинский Сергей Всеволодович
ФГБУН «Институт проблем рынка Российской Академии наук», Москва, Россия
Заведующий лабораторией промышленной политики и экономической безопасности
ФГБОУ ВО «Государственный университет просвещения», Мытищи, Россия
Заведующий кафедрой «Экономического и финансового образования»
Доктор экономических наук, профессор
E-mail: sh-serg@bk.ru
ORCID: https://orcid.org/0000-0002-5853-3585
РИНЦ: https://www.elibrary.ru/author_profile.asp?id=248887
SCOPUS: https://www.scopus.com/authid/detail.url?authorId=57192955537

Крупнов Юрий Александрович
ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Институт экономической политики и проблем экономической безопасности
Ведущий научный сотрудник Центра мониторинга и оценки экономической безопасности
Доктор экономических наук, доцент
E-mail: yakrupnov@fa.ru
ORCID: https://orcid.org/0000-0002-9524-3747

Толмачев Олег Михайлович
ФГБОУ ВО «Государственный университет просвещения», Мытищи, Россия
Доцент кафедры «Экономического и финансового образования»
Кандидат экономических наук, доцент
E-mail: oltom@inbox.ru
ORCID: https://orcid.org/0000-0003-3385-2667

Цифровая трансформация банковских бизнес-моделей и проблемы обеспечения кибербезопасности

Аннотация. Актуальность темы исследования обусловлена необходимостью комплексного изучения проблем кибербезопасности и стабильности функционирования банковской системы России в условиях стремительного распространения цифровых банковских сервисов и услуг. Цифровизация банковского сектора предопределила появление

новых цифровых сервисов и продуктов, в том числе цифровых банков и экосистем. Вместе с тем цифровая трансформация актуализирует вопросы обеспечения национальной финансовой и кибербезопасности. Цель исследования — представить характеристику основных направлений цифровой трансформации бизнес-моделей банков в контексте обеспечения кибербезопасности банковской системы России. В статье систематизированы различные точки зрения на понятие «цифровая трансформация бизнес-модели банка», представлена компаративная характеристика подходов к цифровой трансформации банковских бизнес-моделей с учетом мирового опыта, проанализирована динамика киберугроз банковской системы РФ, описана структура объектов банковской системы России, подвергавшихся кибератакам, разработаны предложения по обеспечению кибербезопасности отечественной банковской системы. При подготовке теоретического раздела публикации, посвященного идентификации и описанию основных вызовов и угроз безопасности банковского сектора применялись общенаучные методы: наблюдение, сравнение, измерение, анализ и синтез, метод логического рассуждения, критический обзор научной литературы и профессиональных публикаций; при подготовке аналитического раздела, посвященного обработке статистических данных идентифицированных ранее вызовов и угроз использовались конкретно-научные методы: статический анализ, графический метод; в заключительной части научного исследования, посвященного формализации и аргументации конкретных рекомендаций и предложений, авторами использовался экспертный метод. Основные выводы исследования состоят в обобщении следующих ключевых особенностей стратегии безопасного функционирования банковского сектора: смещение акцента на мониторинг вызовов и угроз всего рынка сразу одним институциональным актором — Фин-ЦЕРТом Банка России; приоритет в закупке готовых цифровых продуктов Банком России для системообразующих банков и объектов критической инфраструктуры банковской системы; популяризация модели «держать врага снаружи», которая в современных реалиях цифровизации общества теряет свою эффективность. Результаты научного исследования могут быть полезны экспертам в сфере государственного регулирования банковского сектора, а также специалистам при формировании стратегий устойчивого развития в контексте эскалации международных санкций и попыток финансово-экономической изоляции страны.

Ключевые слова: цифровизация; цифровая трансформация; бизнес-модели; киберугрозы; банковская система; кибербезопасность

Введение

Объявление политической элитой России курса на цифровую трансформацию национальной экономики, закрепленного в Указе Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» № 203[1] и Программе цифровой экономики (распоряжение Правительства № 1632-р от 28.07.2017 г.)[2] ознаменовало начало новой вехи устройства и регуляции всех национальных институтов: осознание, принятие и переход к парадигме Индустрии 4.0, фундаментальным положением которой является сквозная цифровизация бизнес-процессов и создание бесшовного информационного пространства между всеми участниками социально-экономической системы.

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента № 203 от 09.05.2017 г. [Электронный ресурс] — Режим доступа: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 30.09.2022, свободный).

[2] Цифровая экономика Российской Федерации: Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р [Электронный ресурс] — Режим доступа: Название http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 30.09.2022, свободный).

Вместе с тем, процессы цифровизации получают неоднозначную оценку среди многочисленных агентов социально-экономической системы ввиду появления новых вызовов и угроз экономической и цифровой безопасности.

Цифровая трансформация экономики несет в себе как позитивные, так и негативные тенденции для устойчивого и безопасного функционирования национальной банковской системы.

Цель научного исследования — представить характеристику основных направлений цифровой трансформации бизнес-моделей банков в контексте обеспечения кибербезопасности банковской системы России.

Методология исследования базируется на использовании как общенаучных методов (наблюдение, сравнение, измерение, анализ и синтез, метод логического рассуждения, критический обзор научной литературы и профессиональных публикаций), так и конкретно-научных методов (статический анализ, графический метод, экспертный метод).

Обзор литературы и исследований.

Переход к цифровой экономике и ее влияние на банковскую сферу воспринимается как академическими, так и бизнес-кругами неоднозначно.

Ряд авторов выделяют незаметную, но очень существенную монополизацию роли создания и доставки экономической ценности банковского продукта клиенту на стороне IT-отрасли (фактически, они единолично отвечают за механизм функционирования оцифрованных продуктов, банк же выступает только заказчиком и его оператором).[3]

Некоторые специалисты подчеркивают, что сама возможность цифровой трансформации бизнес-модели банкинга с целью удержания своей позиции на рынке (тем более — для ее преумножения или усиления) требует перекраивания границ доступной информации для внешних агентов [1; 2], а это несет множество скрытых угроз и рисков безопасности всей архитектуре бизнес-модели банка.[4]

Отдельные эксперты отмечают, что сама стратегия цифрового перехода, являясь объективным требованием времени, требует учета значительного технологического разрыва между мировыми лидерами в сфере IT и Россией [3; 4], чей интеллектуальный капитал используется преимущественно в формате аутсорсинга отдельных задач, а также подвержен волнам релокации[5].

В таблице 1 представлен критический обзор суждений наиболее авторитетных отечественных и зарубежных специалистов, определяющих понятийный конструкт «цифровая трансформация бизнес-модели банка».

Можно сделать вывод о том, что в отечественной практике цифровая трансформация бизнес-модели банка понимается ожидаемо прагматично, но в отличие от мировой, в ней прослеживается сильный интерес государственных регуляторов и политических элит [10; 11].

---

[3] 6 трендов цифровизации банков в 2022 году (23.12.2021). URL: https://www.e-xecutive.ru/finance/novosti-ekonomiki/1994639-6-trendov-tsifrovizatsii-bankov-v-2022-godu (дата обращения: 20.12.2022).

[4] Цифровизация и будущее банков: три сценария (20.01.2022). URL: https://econs.online/articles/opinions/tsifrovizatsiya-i-budushchee-bankov-tri-stsenariya/ (дата обращения: 20.12.2022).

[5] Масштабы изменений при релокации и кого они коснулись (29.09.2022). URL: https://vc.ru/hr/510638-masshtaby-izmeneniy-pri-relokacii-i-kogo-oni-kosnulis (дата обращения: 25.12.2022).

Таблица 1

Сущность понятийного конструкта «цифровая трансформация бизнес-модели банка»

Авторы (Источник)	Содержание определения, описание возможностей и угроз
I. Отечественная литература	
1. Стратегия развития информационного общества РФ на 2017–2030 годы (ст. 4, п./п. р)[1]	<…> хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, а использование которых позволяет <…> существенно повысить эффективность различных видов продуктов и сервисов.
2. Гайсина Д.В.[6]	Процесс трансфигурации банковских продуктов и услуг в формат start-end цифровых цепочек, происходящий в пространстве Internet.
3. Лебедева И.А. [1]	Перевод архитектуры банковских процессов создания, управления, реализации и обслуживания банковских продуктов (услуг) в цифровое пространство-реплику физических контактов клиента и банка.
4. Дудин М.Н., Шкодинский С.В., Усманов Д.И. [5]	Формирование принципиально новой инфраструктуры осуществления банковского бизнеса с учетом смены функциональной парадигмы Internet с поиска информации на планетарную экосистему связи всех-со-всеми.
II. Зарубежная литература	
1. Uddin M.H. [6]	Стратегия интеграции потенциала цифровых технологий в финансовые продукты и сервисы банка для генерации экономической добавленной стоимости.
2. Ghauri F.A [7]	Фундаментальная реорганизация бизнес-модели банка с целью обеспечения его конкурентоспособности в новых условиях рыночного устройства и парадигмы делового поведения.
3. Tripathi S. [8]	Процесс формирования новой организационно-правовой и экономической конструкции, в которой частные и публичные коммерческие интересы реализуются в бесшовном информационном пространстве.
4. Jibril A.B. [9]	Некоторая «договоренность» субъектов рыночного пространства по поводу перевода бизнес-процессов в виртуальную среду, где продукты и сервисы конструируются под запросы конкретного клиента с учетом принципов smart manufacturing (умное производство).

Составлено авторами

Таблица 2

Компаративная характеристика подходов к цифровой трансформации банковских бизнес-моделей: мировой опыт

Подход	Характеристика подхода
1. Классический банк с цифровыми каналами	*Предпосылки применения*: ухудшение конкурентной позиции банков с традиционной физической БМ; возрастание запроса клиентов на новые персонализированные продукты и сервисы; снижение показателей рентабельности активов и деловой активности. *Цель*: внедрение в традиционную физическую БМ отдельных элементов цифрового банкинга для поддержания конкурентной позиции и деловой активности классических банков. *Механизм:* менеджмент банка выбирает критические зоны внимания, требующие неотложной модернизации, и ускоренно оцифровывает входящие в них продукты и сервисы, контуры БМ и ее физическая парадигма функционирования не меняются. *SWOT-характеристика подхода:* преимуществами является сравнительно низкие издержки на трансформацию, сохранение консервативных интересов менеджмента, краткосрочное удовлетворение ожиданий клиентов; недостатками считаются вероятные конфликты между традиционной и цифровой парадигмой управления бизнес-процессами, репликация банковских продуктов и как следствие, рост издержек на их администрирование и контроль, проблемность своевременного обновления цифровой инфраструктуры ввиду ее автономности нахождения в контуре физической БМ.

[6] Гайсина Д.В. Трансформация современных бизнес-моделей в сторону экосистем: доклад на конференции «Проектирование бизнес-структур». Бизнес-студио. (16.09.2017). — URL: https://www.businessstudio.ru/upload/iblock/7e6/Гайсина.pdf (дата обращения: 30.12.2022).

Подход	Характеристика подхода
2. Цифровой филиал классического банка	*Предпосылки применения:* растущие запросы клиентов на полный перевод сервисов в цифровую среду; готовность менеджмента к экспериментам в сфере цифровой трансформации; желание сохранить деловую активность в физической и цифровой среде. *Цель*: создание дочерней бизнес-единицы в составе физической БМ банка в формате «финансовой песочницы» для разработки, тестирования и интеграции цифровых инструментов реализации продуктов и сервисов в операционный банкинг, а также разведение потоков клиентов в соответствии с их предпочтениями. *Механизм:* менеджментом банка выбирается один или несколько инфраструктурных объектов, обладающих наиболее высоким инновационным потенциалом, затем руководство этих структур разрабатывает индивидуальные стратегии цифровой трансформации и реализует описанные работы, после чего на контрольной сессии оценивается эффективность их работы и определяется дальнейший порядок внедрения лучших практик в масштабы материнской БМ банка. *SWOT-характеристика подхода:* преимуществами является взвешенный и диверсифицированный подход к трансформации, создание собственной инфраструктуры отладки цифрового перехода и формирование профессионального опыта работы в цифровой парадигме; к недостаткам относятся высокие издержки на содержание такого филиала, вероятное возникновение конфликта подчиненности и сложности обмена данными вплоть до обратного поглощения дочерней структурой материнской организации; точечность применения цифровых практик банкинга и ограниченные возможности их масштабирования на всю материнскую БМ.
3. Цифровой банковский бренд	*Предпосылки применения*: декларирование менеджментом банка готовности к фундаментальной цифровой трансформации, принятие стратегии цифрового ребрендинга БМ, цели M&A сделки с полностью цифровым банком. *Цель*: позиционирование банка как стремящегося к переменам и инновациям через планомерную, пошаговую и системную работу над цифровизацией бизнес-процессов. *Механизм:* менеджментом банка формируется карта цифрового перехода и строится график работ с определением центров ответственности и точками сопряжения интересов и взаимодействий, и поэтапно проводится оцифровка контуров и уровней физической БМ банка. *SWOT-характеристика подхода:* преимуществами является взвешенный подход к технологическим и процессным инновациям, минимизирующий риски и ошибки выбора пути реформы; высокая согласованность интересов менеджмента и клиентов банка, рациональное использование финансовых ресурсов на реорганизацию операционной инфраструктуры; к недостаткам относятся длительность цифрового перехода (возникает угроза потери самого конкурентного преимущества); сложность прогнозирования длительности стадий жизненного цикла банковского бренда, реактивность реагирования менеджмента банка на новейшие технологические разработки, высокая киберуязвимость бизнес-модели.
4. Полностью цифровой банк	*Предпосылки применения*: продуктивная межотраслевая кооперация с IT-компаниями и финтех-рынком; агрессивная инвестиционная политика, ориентированная на достижение технологического лидерства; наличие долгосрочной стратегии поглощения банков-конкурентов с физической парадигмой управления. *Цель*: создание полностью оцифрованной бизнес-модели банковских продуктов и сервисов, которые персонализируются и дорабатываются с учетом запросов конкретного клиента в обмен на монетизированное использование персональных данных о клиенте. *Механизм:* менеджмент банка отказывается от физической парадигмы или формирует greenfield-проект полностью цифровых продуктов и сервисов (в случае открытия нового банка); вторым этапом формируется цифровой ландшафт для размещения самих продуктов — финансовый супермаркет; на третьем этапе происходит масштабирование БМ путем включения в ее состав новых продуктов, в т. ч. смежных или квазибанковских (например, управление системами умный дом с ID-ключом банковского клиента, цифровая подпись клиента и т. п.). *SWOT-характеристика подхода:* преимуществами является гармонизация интересов менеджмента с положениями цифровой парадигмы и трендами цифровой реформации экономики, банк как актор открыт к инновациям и активно развивает обратную связь с клиентами; достижение информационной прозрачности банкинга и раннее выявление проблем функционирования продукта (сервиса); возможность бесшовной межбанковской кооперации и развития кобрендинговых продуктов и услуг; к недостаткам относятся высокие издержки на обеспечение киберзащиты персональных данных и инфраструктуры проведения транзакций, возможное возникновение агентских конфликтов между банком и IT-партнером ввиду разности видений перспектив развития совместного бизнеса.

Подход	Характеристика подхода
5. Банковская цифровая экосистема / финансовая метавселенная	*Предпосылки применения:* опережающее технологическое развитие IT-сферы в стране, аккумулирование значительных финансовых фондов в небанковской среде, регуляторный либерализм и лоббирование интересов IT-бизнеса в части его инкорпорации в финансовый сектор; олигополистический рынок банков с центристскими интересами переформатирования рынка «под себя». *Цель*: создание киберпространства с нулевой конкуренций — финансовой экосистемы с формированием системы допуска бизнесов финансового и нефинансового секторов на основе партнёрств и лояльного отношения к владельцу экосистемы. *Механизм:* один или объединение нескольких суперкрупных банков производит масштабную инвестиционную интервенцию и формирует цифровую сетевую платформу, которая на основании запросов клиентов заполняется партнерами, предоставляющими финансовые (в т. ч. банковские) и нефинансовые услуги на эксклюзивных условиях. Правила поведения, стандарты обмена данными и взаимодействия регламентируются и контролируются владельцем экосистемы. Финансовая метавселенная представляет собой новый уровень развития экосистемы, основанный на бесшовной интеграции банка и IT-бизнеса в новообразование, представляющее цифровой слепок жизни конкретного клиента, в который переносится его поведение, интересы, деловая активность и т. д. для формирования и тестирования сценариев его поведения (сам субъект также может участвовать в его разработке и проигрывании). *SWOT-характеристика подхода:* преимуществами является полное проникновение банков в жизнь клиентов и по сути наблюдение за ней с целью проактивной оптимизации финансовых продуктов и сервисов; инновационное развитие всех партнеров экосистемы и инфраструктурная поддержка со стороны банка-инициатора; формирование нового цифрового мира, где можно в игровой форме «прогонять» сценарии поведения социума, анализировать макроэкономические пропорции и выявлять точки и зоны финансовых правонарушений и преступлений; к недостаткам относятся принятие клиентами отказа от минимальных границ личной неприкосновенности, возникновение негативных эффектов виртуальной репликации (участники метавселенной будут пробовать перенести события из виртуальной среды в реальную), возникновение финансового и делового двоемыслия, сопряженного со полной информационной прозрачностью транзакций; масштабирование киберугроз и стремительное, взрывное развитие сегмента Darknet в части торговли персональной информацией.

Разработано авторами по данным [5; 12–14]

В рамках теоретического раздела научного исследования также была подготовлена компаративная характеристика подходов к цифровой трансформации банковских бизнес-моделей (далее — БМ), применяемых в мировой практике, что позволяет лучше понять их сильные и слабые стороны в контексте обеспечения безопасности в цифровой среде (табл. 2).

Компаративная характеристика подходов к цифровой трансформации банковских бизнес-моделей позволяет заключить: чем более высокий уровень проникновения цифровых технологий в бизнес-процессы банка, тем большему количеству киберугроз он подвержен.

Конечно, обеспечение безопасного функционирования банков в условиях перехода к цифровой экономике *не сводится исключительно к проблеме защиты от хакерских атак или защите критической инфраструктуры*, напротив, такая задача предполагает анализ очень широкого круга факторов экономического, технологического, кадрового и регулятивного характера. Однако принимая во внимание ограниченность статистической информации о реальных и потенциальных вызовах и угрозах для банков нового времени (этому вопросу посвящен отдельный раздел стратегии развития банка, но он, по понятным причинам, составляет коммерческую тайну), акцент в научном исследовании будет сделан именно на анализе динамики, структуры и объектов киберугроз и проблемах регуляторного несовершенства банковской системы РФ.

Проблемы обеспечения кибербезопасности банковской системы России

Представим статистические данные по проблеме научного исследования. Основным источником верифицированной статистической информации явились ежегодные

аналитические отчеты Департамента информационной безопасности Банка России, а также обзорные публикации PT Security.com. В таблице 3 представлена динамика киберугроз (кибератак) банковской системы РФ за 2016–2021 гг.

Таблица 3

Динамика киберугроз (кибератак) банковской системы РФ за 2016–2021 гг.

Показатели	2016 г.	2017 г.	2018 г.	2019 г.	2020 г.	2021 г.
1. Общее количество реализованных киберугроз (кибератак) на субъекты банковской системы, ед. *В том числе*:	489	514	687	1723	968	1 154
1.1 Банк России	…	1	2	4	…	3
1.2 Системообразующие банки	12	9	16	29	18	139
1.3 Коммерческие банки II уровня	324	407	488	879	775	598
1.4 НКФО (включая финтех-компании)	153	97	181	811	175	414
2. Оценочная сумма от реализованных киберугроз (кибератак), млн руб. *В том числе*:	1 080	961,3	1 384,7	5 723,5	8 757,2	10 156,1
2.1 Убытки, причиненные клиентам банков	607	541	779	3219	5801	7 032
2.2 Расходы на восстановление нормального функционирования банков после атак	279	301	411	1 987	2 316	1 900
2.3 Иные (непрямые) потери и убытки	194	120	195	518	640	1 224
3. Индикаторы защищенности банковского сектора от киберугроз (атак)						
3.1 Удельный вес отраженных атак, в % к итогу	39,5	42,4	44,7	49,5	52,7	49,4
3.2 Уровень возмещения потерь средств клиентов[7]	18,3	17,2	16,2	15,0	11,3	6,8
3.3 Индекс киберустойчивости банковского сектора по категориям участников:						
3.5 Банк России	…	1,0	2,0	4,0	…	…
3.6 Системообразующие банки	7,9	7,2	6,8	8,0	7,7	6,4
3.7 Коммерческие банки II уровня	5,5	4,7	4,9	4,5	3,4	3,9
3.8 НКФО (включая финтех-компании)	6,2	5,8	5,5	4,9	4,1	3,5
4. Уровень интернет-культуры и цифровой гигиены клиентов банка, %	31,4	35,2	39,6	42,8	45,6	49,1

Источники: [8]

Как следует из приведенных выше данных, банковская система России в анализируемом периоде все чаще подвергалась кибератакам, причем начиная с 2019 г. отмечен рост их активности на системообразующие банки — это может расцениваться как «повышение ставок» самими авторами кибератак, так и санкционированными недружественными государствами с целью дестабилизации всей банковской системы и зарождения панических настроений в обществе вкупе с дискредитацией топ-менеджмента крупнейших банков.

Второй важной чертой является активный рост кибератак на представителей финтеха, что, в общем, является общемировым трендом смены клиентских предпочтений с классических банков на представителей НКФО, придерживающихся более гибких правил взаимодействия с

[7] Рассчитывается как сумма возвращенных банку средств / сумма похищенных средств×100 %.

[8] Обзоры операций, совершенных без согласия клиентов финансовых организаций за 2016–2021 гг.: аналитические отчеты Департамента информационной безопасности Банка России (21.02.2017, 15.10.2018, 06.03.2019, 19.02.2020, 12.06.2021, 11.04.2022). URL: https://cbr.ru/Collection/Collection/File/32093/survey_transfers_16.pdf; https://cbr.ru/Collection/Collection/File/32094/survey_transfers_17.pdf; https://cbr.ru/Collection/Collection/File/32091/gubzi_18.pdf; https://cbr.ru/Collection/Collection/File/32189/Review_of_transactions_2019.pdf; https://cbr.ru/Collection/Collection/File/32190/Review_of_transactions_2020.pdf; https://cbr.ru/analytics/ib/operations_survey/2021/ (дата обращения: 30.01.2023) / Reviews of transactions made without the consent of clients of financial organizations in 2016–2021: analytical reports of the Department of Information Security of the Bank of Russia (accessed on 30.01.2023).

клиентами и в меньшей степени подвержены регуляторным ограничениям, что, собственно, и приводит к такой «нежелательной» популярности у криминальных элементов.

С ростом количества атак отмечается рост сумм убытков, причиняемых банкам, при этом важно отметить практически пятикратный рост расходов на восстановление нормального функционирования банков после таких атак, начиная с 2019 г. и четырехкратный рост непрямых убытков, связанных с потерей имиджа и доверия со стороны клиентов, а также привлечение внимания банковского регулятора и проведение комплекса внеплановых проверок.

Для идентификации слабых мест в банковской системе России рассмотрим структуру объектов кибератак за 2016–2021 гг. (рис. 1).

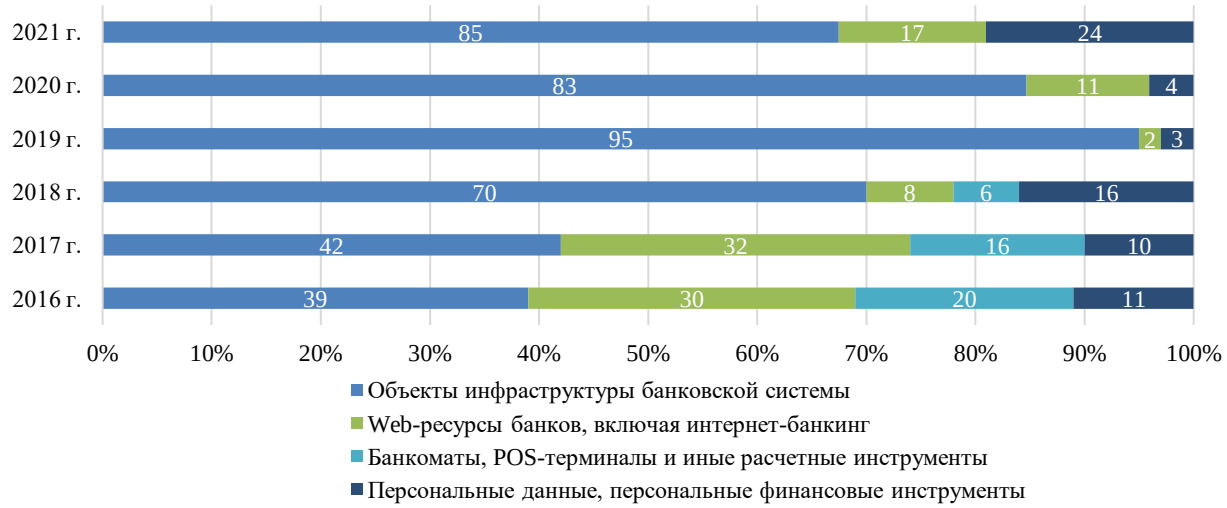

Рисунок 1. *Структура объектов банковской системы России, подвергавшихся кибератакам в 2016–2021 гг., в % (источники: [9])*

Согласно приведенным данным структура объектов кибератак в анализируемом периоде существенно изменилась: начиная с 2018 г. интерес хакерских групп сконцентрировался вокруг объектов инфраструктуры банков (прирост составил 28,0 п.п. и продолжил увеличиваться).

[9] Кибербезопасность 2016–2017: от итогов к прогнозам (26.01.2017). URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf (дата обращения: 03.02.2023);

Актуальные киберугрозы — 2017. Тренды и прогнозы (06.03.2017). URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf (дата обращения: 03.02.2023);

Кибербезопасность 2017–2018: цифры, факты, прогнозы (13.12.2017). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2017-2018/ (дата обращения: 03.02.2023);

Кибербезопасность 2018–2019: цифры, факты, прогнозы (18.12.2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2018-2019/ (дата обращения: 03.02.2023);

Актуальные киберугрозы — 2018. Тренды и прогнозы (12.03.2019). URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-rus.pdf (дата обращения: 03.02.2023);

Кибербезопасность 2019–2020. Тренды и прогнозы (19.12.2019). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020/ (дата обращения: 03.02.2023);

Актуальные киберугрозы: итоги 2020 года (28.04.2021). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (дата обращения: 03.02.2023);

Актуальные киберугрозы: итоги 2021 года (19.04.2022). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (дата обращения: 03.02.2023).

Несмотря на логичность предположения о слабости банковской инфраструктуры, оно является во многом ошибочным: хакеры используют банковскую инфраструктуру, чтобы максимизировать свои выгоды от атаки и, согласно своей идеологии, нанести больший ущерб банковской системе.

Вторым объектом внимания хакеров стали персональные данные и индивидуальные финансовые инструменты (банковские карты) — в анализируемом периоде отмечено два пика атак: 2018 г. — 16,0 % и 2021 г. — 24,0 %, что объясняется масштабным ростом популярности практик социальной инженерии и новых форм мошенничества с использованием телекоммуникационных технологий (телефонное мошенничество, фишинг, спам-рассылки с вредоносными программами): так, по данным за 2021 г., из зарегистрированных МВД 518 тыс. киберпреступлений, 249 тыс. ед. связано с телефонным мошенничеством[10].

На рисунке 2 представлена диаграмма, отражающая структуру наиболее часто применяемых инструментов совершения кибератак на банки, что позволяет идентифицировать основные точки (зоны) внимания менеджмента банков и регулятора.

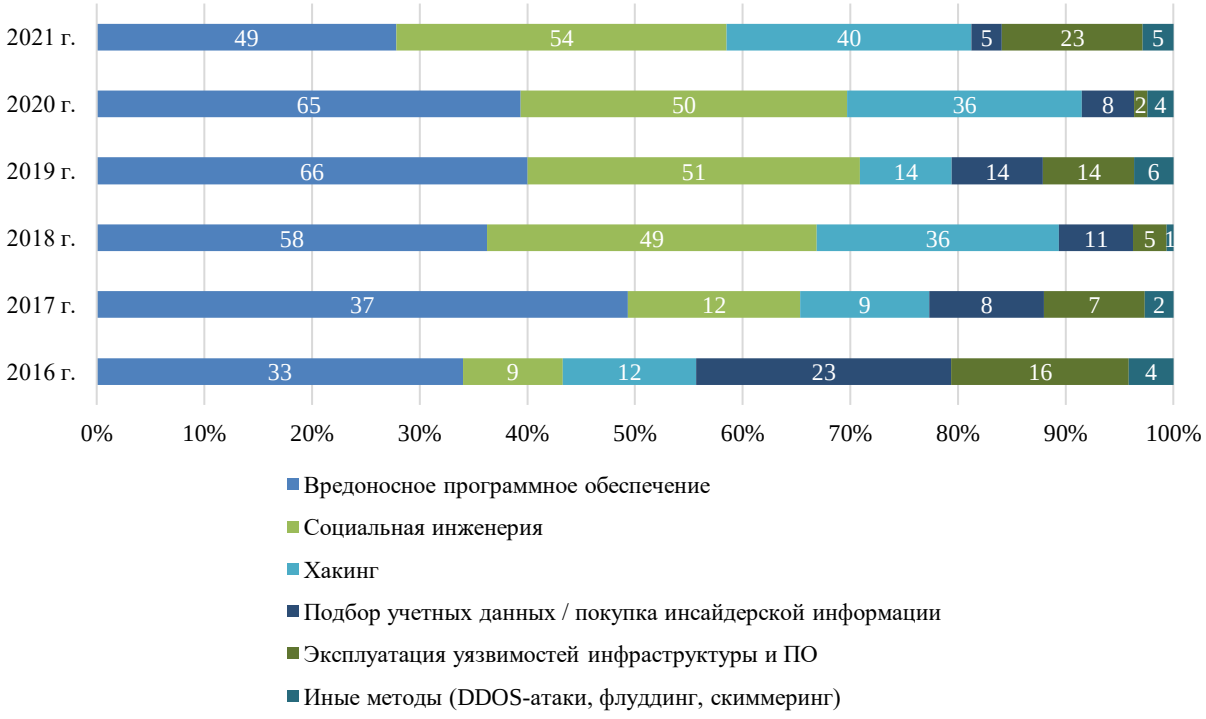

Рисунок 2. *Структура инструментов совершения кибератак на банки в 2016–2021 гг., % (источники: [11])*

Как следует из приведенной диаграммы, основным источником угроз для российских банков является применение вредоносного программного обеспечения — в среднем данный инструмент использовался в 51,3 % всех атак, на втором месте — социальная инженерия

[10] Число киберпреступлений в России выросло в 1,8 раза (18.02.2022). URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России# (дата обращения: 05.02.2023).

[11] Отчеты Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за 2015–2020 гг. (19.07.2016). URL: https://cbr.ru/Collection/Collection/File/32090/FinCERT_survey.pdf;

Актуальные киберугрозы: итоги 2021 года (19.03.2023). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (дата обращения: 03.04.2023).

(37,5 %), замыкает тройку лидеров хакинг — 24,5 % (превалирующими адресами атак было сетевое пространство США, ФРГ и Нидерландов [12, 13], что косвенно свидетельствует о возможной политической аффилиации руководства стран).

В анализируемом периоде Банком России предпринимались определенные шаги в направлении обеспечения кибербезопасности банковской системы. В частности, на регулярной основе проводился мониторинг вызовов и угроз всему финансовому рынку; осуществлялось техническое обеспечение Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России. Отметим, что Банком России популяризируется модель «держать врага снаружи», однако в современных реалиях цифровизации общества она теряет свою эффективность, т. к. благодаря достижениям социальной инженерии практически любой гаджет, подключенный к сети Internet, может стать инструментом совершения преступления [2; 15–17].

Вместе с тем, слабых мест еще достаточно. Исходя из этого, авторы считают целесообразным реализовать следующие предложения:

1. Банком России совместно с системообразующими банками реализовать инициативу по созданию национальной линии информационной безопасности функционирования банков — аналог Великого Китайского файрволла[14], к которому за определенную плату будут подключать все банки (это позволит последним экономить на частных системах информационной безопасности).

Главным преимуществом такой системы станет обмен в режиме реального времени о всех актуальных вызовах и угрозах информационного пространства, фиксация всех случаев атак (по мнению Г. Грефа, более 80,0 % компаний нефинансового сектора скрывают факты кибератак[15], которые затем могут распространиться на банки, которые, в свою очередь, также утаивают каждую пятую успешную атаку[16]).

2. Запустить практику аутсорсинга сервисов кибербезопасности путем членства в банковской экосистеме — на примере экосистемы ПАО «Сбер» может быть выстроен бесшовный комплекс киберзащиты для сторонних банков путем продажи им лицензий на инструменты обеспечения информационной безопасности.

3. Обеспечить финансовую поддержку отечественным финтех-проектам в сфере кибербезопасности — в рамках программы импортозамещения в сфере ИКТ. Данная мера позволит максимизировать продуктивность стартапов в данном направлении, тем самым снизить риски эксплуатации узявимостей, содержащихся в иностранных инструментах информационной безопасности. Практическая реализация такого предложения требует консолидации усилий ведущих участников венчурного рынка: АО «Российская венчурная компания», «Фонд Сколково», РФПИ с инновационной инфраструктурой для формирования

[12] В МИД РФ назвали страны, откуда Россию атаковали хакеры в 2020 году (12.05.2021) [Электронный ресурс] — Режим доступа: https://regnum.ru/news/polit/3266429.html (дата обращения: 03.10.2022, режим доступа: свободный).

[13] Кибервойна России и США (06.04.2021) [Электронный ресурс] — Режим доступа: https://www.tadviser.ru/index.php/Статья:Кибервойна_России_и_США#... (дата обращения: 03.10.2022, режим доступа: свободный).

[14] Краткая история ИБ в Китае: как возводили Великий китайский файрвол (30.04.2018). URL: https://habr.com/ru/company/vasexperts/blog/354698/ (дата обращения: 19.02.2023).

[15] Г. Греф: более 80% компаний скрывают факты кибератак (21.06.2019). URL: https://traders-union.ru/iaftnews/finance/news/335016/ (дата обращения: 10.02.2023).

[16] Банки утаивают каждую пятую успешную кибератаку (23.11.2017). URL: https://www.securitylab.ru/news/489810.php (дата обращения: 11.02.2023).

портфеля стартап-проектов и отбора наиболее перспективных из них для последующего финансирования и включения в состав госзаказа.

4. Разработать стандарт минимальных требований к кибербезопасности участников банковского сектора и установить контрольные индикаторы оценки их исполнения. Для многих банков (особенно малых) расходы на кибербезопасность не является первостепенными при формировании стратегии развития, что приводит к повышенной уязвимости их бизнес-модели.

5. Провести тестирование практики применения цифрового рубля (в настоящее время пилотирование операций с реальными цифровыми рублями проводится ЦБ РФ) как инструмента мониторинга и обеспечения безопасности трансграничных переводов для компаний стратегического значения — для повышения защищенности банковских переводов с участием важнейших для национальной экономики компаний рекомендуется ввести практику расчетов цифровым рублем, построенным на механизме блокчейн, что повышает прозрачность и отслеживаемость операций [14; 17; 18].

Заключение

Вопрос обеспечения безопасности банковского сектора России в условиях цифровой трансформации экономики носит сложный и многоаспектный характер, и в рамках исследования был рассмотрен только один из фундаментальных блоков — кибербезопасность банков, которая в современных условиях приобретает все более масштабный характер.

Переход к цифровой экономике и ее влияние на банковскую сферу воспринимается неоднозначно ввиду незаметной, но очень существенной монополизации роли эффективной трансформации на стороне IT-отрасли.

К ключевым особенностям стратегии безопасного функционирования банковского сектора относятся: смещение акцента на мониторинг вызовов и угроз всего рынка сразу одним институциональным актором — ФинЦЕРТом Банка России; приоритет в закупке готовых продуктов информационной безопасности для системообразующих банков и объектов критической инфраструктуры банковской системы.

Реализация представленных в статье предложений во многом может способствовать устранению слабых сторон действующей практики обеспечения безопасности банков от вызовов и угроз цифровизации.

ЛИТЕРАТУРА

1. Лебедева И.А. Цифровая трансформация банковского сектора России: возможности и риски для банков и их клиентов. Социальные новации и социальные науки. — 2022. — № 1. — С. 74–85. URL: https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-bankovskogo-sektora-rossii-vozmozhnosti-i-riski-dlya-bankov-i-ih-klientov.
2. Дмитриева Г.С. Цифровые технологии в банковском секторе экономики. Известия Санкт-Петербургского государственного экономического университета. — 2020. — № 7. — С. 49–54.
3. Андреева О.В. Технологический и финансовый суверенитет Российской Федерации: проблемы, противоречия, механизмы обеспечения. Journal of Economic Regulation (Вопросы регулирования экономики). — 2014. — № 4(5). — С. 126–135.

4. Омелехина Н.В. Финансовый суверенитет государства: к постановке проблемы исследования правовой идентификации. Финансовое право. — 2017. — № 4. — С. 12–21.
5. Дудин М.Н., Шкодинский С.В., Усманов Д.И. Ключевые тенденции и закономерности развития цифровых бизнес-моделей банковских сервисов в Индустрии 4.0. Финансы: теория и практика. — 2021. — № 25(5). — С. 59–78. DOI: 10.26794/2587-5671-2021-25-5-59-78. URL: https://elibrary.ru/item.asp?id=46956330.
6. Uddin, M.H., Mollah, S., & Ali, M.H. Does cyber tech spending matter for bank stability? International Review of Financial Analysis. — 2020. — № 72. — DOI: 10.1016/j.irfa.2020.101587. URL: https://www.sciencedirect.com/science/article/abs/pii/S1057521920302313.
7. Ghauri, F.A. Why Financial Sectors Must Strengthen Cybersecurity. International Journal of Computer Science and Information Security (IJCSIS). — 2021. — № 19(7). — URL: https://zenodo.org/record/5163796#.ZGCZLSPP2Uk (дата обращения 12.01.2023).
8. Tripathi, S., & Gupta, M. A holistic model for Global Industry 4.0 readiness assessment. Benchmarking. — 2021. — № 28(10). — P. 3006–3039. DOI: 10.1108/BIJ-07-2020-0354.
9. Jibril, A.B., Kwarteng, M.A., Chovancova, M., & Denanyoh, R. Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. In Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS. — 2020. — P. 270–276. Academic Conferences and Publishing International Limited. DOI: 10.34190/ICCWS.20.020.
10. Алонцева В.Р. Оценка состояния цифрового банкинга в РФ. Международный журнал гуманитарных и естественных наук. — 2018. — № 5(2). — С. 88–91. URL: https://cyberleninka.ru/article/n/otsenka-sostoyaniya-tsifrovogo-bankinga-v-rossii/viewer.
11. Гонтарь Л.О. Смарт-подходы в цифро-финансовой экосистеме: финтех в условиях применения цифровых платформ и умного контроля. E-Management. — 2021. — № 4(2). — С. 44–50.
12. Косарев В.Е. О цифровой эволюции банков в направлении необанков. Финансовые рынки и банки. — 2020. — № 3. — С. 56–61.
13. Уразова С.А. Цифровая трансформация банковских систем как основа перехода к новому периоду их эволюции. Финансовые исследования. — 2021. — № 2(71). — С. 55–66.
14. 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). — С. 38–53. DOI: 10.31107/2075-1990-2021-3-38-53.
15. Рябичева О.И. Цифровизация розничных банковских услуг в российской федерации на современном этапе. Журнал прикладных исследований. — 2021. — № 6-9. — С. 896–905.
16. Соколинская Н.Э., Зиновьева Е.А. Анализ готовности российских коммерческих банков к цифровизации экономики в условиях трансформации мирового рынка. Финансовые рынки и банки. — 2020. — № 4. — С. 50–57.

17. Зверькова Т.Н. Региональные банки и FinTech: противостояние или партнерство. Финансы и кредит. — 2018. — № 24(12). — С. 2771–2782. DOI: 10.24891/fc.24.12.2771.

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). — P. 775–784. DOI: 10.9770/JSSI.2020.9.3(4).

Shkodinsky Sergey Vsevolodovich
Market Economy Institute of Russian Academy of Sciences, Moscow, Russia
State University of Education, Mytishchi, Russia
E-mail: sh-serg@bk.ru
ORCID: https://orcid.org/0000-0002-5853-3585
RSCI: https://www.elibrary.ru/author_profile.asp?id=248887
SCOPUS: https://www.scopus.com/authid/detail.url?authorId=57192955537

Krupnov Yuriy Aleksandrovich
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: yakrupnov@fa.ru
ORCID: https://orcid.org/0000-0002-9524-3747

Tolmachev Oleg Mikhailovich
State University of Education, Mytishchi, Russia
E-mail: oltom@inbox.ru
ORCID: https://orcid.org/0000-0003-3385-2667

Digital transformation of banking business models and cybersecurity issues

Abstract. The relevance of the research topic is due to the need for a comprehensive study of cybersecurity issues and the stability of the Russian banking system in the context of the rapid spread of digital banking services and services. The digitalization of the banking sector has predetermined the emergence of new digital services and products, including digital banks and ecosystems. At the same time, the digital transformation makes the issues of national financial and cyber security more relevant. The purpose of the research is to describe the main areas of digital transformation of banks' business models in the context of cybersecurity of the Russian banking system. The article systematizes different points of view to the concept of "digital transformation of bank business models", presents a comparative characterization of approaches to digital transformation of banking business models with regard to global experience, analyzes the dynamics of cyber threats to the Russian banking system, describes the structure of the Russian banking system objects that have been subject to cyber attacks, develops proposals to ensure the cyber security of the domestic banking system. When preparing the theoretical section of the publication, dedicated to the identification and description of the main challenges and threats to the security of the banking sector, general scientific methods were used: observation, comparison, measurement, analysis and synthesis, method of logical reasoning, critical review of scientific literature and professional publications; when preparing the analytical section, dedicated to the processing of statistical data of previously identified challenges and threats, specific scientific methods were used: static analysis, graphic method; in the final The main conclusions of the research consist in summarizing the following key features of the strategy of secure functioning of the banking sector: shift of emphasis on monitoring of challenges and threats to the entire market at once by one institutional actor — Fin-CERT of the Bank of Russia; priority in procurement of ready-made digital products by the Bank of Russia for systemically important banks and critical infrastructure facilities of the banking system; popularization of the "keep the enemy outside" model, which loses its effectiveness in the current reality of digitalization of society. The results of the research may be useful to experts in state regulation of the banking sector, as well as to specialists in the formation of sustainable development strategies in the context of escalating international sanctions and attempts to isolate the country financially and economically.

Keywords: digitalization; digital transformation; business models; cyber threats; banking system; cybersecurity