Управление рисками и безопасностью

Deception-решения в системе экономической безопасности банка

Г.В. Федотова[I], Ю.А. Капустина[II], Р.Х. Ильясов[III], Цицигэ[IV]

[I] Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия
[II] Уральский государственный лесотехнический университет, г. Екатеринбург, Россия
[III] Чеченский государственный университет им. А.А. Кадырова, г. Грозный, Россия
[IV] Российский экономический университет им. Г.В. Плеханова, г. Москва, Россия

Аннотация. Работа посвящена обзору современных тенденций развития банковского онлайн-обслуживания клиентов с применением технологий дистанционного обслуживания. Усложнение банковских цифровых платформ привело к формированию информационных экосистем, позволяющих удовлетворять самые различные потребности клиентов. На примере экосистемы СБЕР показано, что сегодня банки не просто управляют счетами клиентов, но и интегрируются с маркетплейсами для оказания различных нефинансовых услуг. Процесс накопления колоссальных массивов персональной и конфиденциальной информации, финансовых активов привлекает интерес мошенников, работающих в сети Интернет. Статистика киберкраж и несанкционированных доступов в цифровые сервисы доказывает, что кибермошенничество постоянно расширяется и ищет новые инструменты для взломов систем. Поэтому цель работы заключается в обосновании нового подхода к выстраиванию защиты на основе детектирования кибератак – deception. Поставленная цель обусловила решение следующий задач: рассмотрены общие тенденции усложнения банковских цифровых платформ до целых экосистем, изучена статистика кибермошенничества в сети Интернет и особенности проведения целевых кибератак, предложен новый подход к выстраиванию системы защиты цифровых сервисов банков.

Ключевые слова: *безопасность, интернет-банкинг, персональные данные, кибермошенничество, кражи.*

DOI: 10.14357/20790279230212

Введение

Интернет-банкинг сегодня достаточно повседневная услуга, которая набирает из года в год все большее количество пользователей. Огромные возможности для экономии времени и издержек для кредитных учреждений будут способствовать расширению и дальнейшему усложнению услуг, оказываемых посредством Интернета. Повсеместно доказано, что финансовый сектор выступает лидером и катализатором последующей глобализации и цифровизации всей социально-экономической системы. Развивая онлайн-сервис финансовых услуг, государство способствует росту финансовой и информационной грамотности населения. Ежедневное или периоди-

ческое использование Интернета в осуществлении текущих платежей повышает доверие граждан к системам дистанционного доступа к своим счетам [1].

Современный коммерческий банк – это больше виртуальный мультибанк, который контактирует с клиентами через Интернет, что дает возможность построить финансовую систему информационной экономики, а в некоторых случаях отдельную экосистему. Кредитные организации постоянно расширяют свои возможности в онлайн пространстве – предлагают новые сервисы, оформление документов без посещения офиса, проводят огромные объемы электронных платежей и транзакций ежедневно [2]. Сегодня банки ищут новые точки роста и рыночные ниши, в том числе посредством перевода основных операций бизнеса в онлайн-пространство. И как новое веяние 2022 года – интеграция и расширение сотрудничества банков с маркетплейсами. (рис. 1).

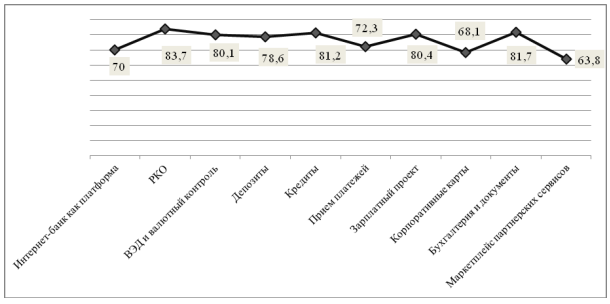

Рис. 1. Объемы банковских операций по итогам 2022 года, %.
Источник: составлено авторами по материалам [3]

По данным рис. 1 видим, что максимальный объем операций приходился на кредиты и зарплатные проекты от 81,2 до 80,4% соответственно. Объемы банковских услуг по интернет-банкингу достигли 70%, по обслуживанию маркетплейсов – 63,8%. Фактически эти доли рынка еще не достигли своего насыщения и имеют хороший потенциал к росту.

Расширение Интернета и переход целых секторов бизнеса в онлайн-пространство формируют прочную платформу для перевода и обслуживания финансовых потоков в цифровом виде. Поэтому вопросы обеспечения максимальной безопасности операций и сохранности информации, счетов клиентов представляют собой задачу первостепенной важности в системах безопасности кредитных организаций.

1. Результаты и обсуждения

Современный мир – мир цифровых и компьютерных технологий, посредством которых многие пользователи все чаще совершают финансовые операции через системы интернет-банкинга [4, 5]. Клиенты сегодня хотят от банка не только получать финансовые услуги и обслуживание счетов, но и другие нефинансовые услуги по самым различным вопросам. Банки готовы их предоставлять, поэтому они формируют целые экосистемы. Наиболее ярким примером выступает Сбербанк, который официально в сентябре 2020 года провел ребрендинг и приобрел новый фирменный знак СБЕР (рис. 2).

Рис. 2. Пример Digital-трансформации Сбербанка в экосистему СБЕР в 2022 году.
Источник: составлено авторами по материалам [3]

Произошедшие изменения в спектре банковских услуг Сбербанка – это следование современным требованиям клиентов, которые предъявляют новые запросы к банковскому обслуживанию [6, 7, 8]. Принципы работы современного банка строятся по вектору «скорость-качество-удобство», при этом усилившаяся конкуренция между банковскими и небанковскими организациями приводит к расширению перечня нефинансовых услуг банков. С целью сохранения клиентской базы банки выходят за пределы своих финансовых полномочий и формируют целые вселенные (экосистемы) по обслуживанию клиентов по самым разным вопросам. Лидерами в этой сфера выступают Сбербанк, Тинькофф, ВТБ и Газпром, которые предлагают максимально широкую линейку продуктов и услуг, при этом некоторые сервисы выделяются в отдельные подразделения банков.

Широкая линейка предоставляемых услуг, максимально привязывает клиента к банку, что экономит его время и усиливает лояльность к банку. Каждый клиент в банке становится персонализирован, к нему применяется индивидуальный подход и отслеживаются его действия в онлайн-системе [9, 10]. С этой целью сформированы цифровые фабрики данных, в которых аккумулируется полная информация по клиенту (его поисковые за-

просы, геолокация, время поиска, активность в сетях) и формируется его профиль, в соответствии с которым будут предложены определенные услуги и продукты как финансовые, так и нефинансовые. На основе массива данных работают фабрики продуктов и предложений от банка. При этом все поиски сопровождаются чат-ботами и виртуальными помощниками (рис. 3).

Рис. 3. Элементы цифровой платформы СБЕР. Источник: составлено авторами по материалам [3,11]

Цифровые платформы на примере Сбербанка представляют собой целые фабрики по хранению данных, последующей их обработкой и формированием новых фабрик предложений услуг и продуктов для клиентов с учетом их потребностей. Банки стали позиционировать себя в тесном взаимодействии с IT-технологиями, стали уделять внимание клиентскому опыту, формировать индивидуальные цифровые портреты клиентов. Поэтому рост популярности онлайн-сервисов растет с каждым годом, но с ростом их популярности растет уровень банковского мошенничества, которое перешло в онлайн-среду. Сегодня основной проблемой банков является обеспечение безопасности финансовых операций, совершаемых клиентами дистанционно, а также сохранение персональной информации и данных клиентов.

Появился и развивается на протяжении длительного периода новый вид мошенничества – киберпреступность, то есть преступления в цифровом пространстве [12, 13]. Как правило, объектами кибератак становятся в первую очередь интернет-сайты кредитных организаций, интернет-магазинов, платежных операторов, то есть цифровые хранилища денег и ценных активов юридических и физических лиц. В 2022 году увеличилось количество атак на приложения с пакетом Microsoft Office, наиболее популярным в России. Но, помимо данных целевых атак на офис, другие приложения тоже подвергаются регулярным массированным атакам. (рис. 4).

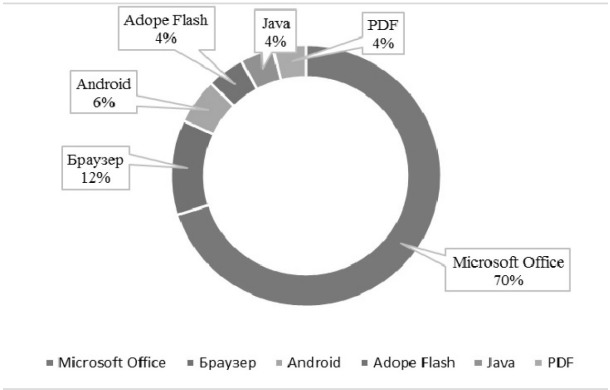

Рис. 4. Статистика распределения кибератак по эксплойтам в 2022 году. Источник: составлено авторами по материалам [14,20]

Согласно представленной статистике основными целями атак в 2022 году стали офисные приложения, браузеры и приложения для Android. Все перечисленные эксплойты используются банками для предоставления финансовых и нефинансовых услуг через свои цифровые платформы. Из года в год количество новых вредоносных программ растет и появляются новые методы и технологии взломов онлайн-сервисов банков и клиентских счетов. Теневая экономика сформировала новый сектор Интернета – Dark Net, в котором работают хакеры и создают свои продукты для реализации мошенничества и дестабилизации работы легальных цифровых систем. [15–17].

Статистика 2022 года показала с какой эффективностью и производительностью могут работать хакеры. Согласно отчетным данным Лаборатории Касперского 2022 год можно назвать рекордным по количеству атак и новых вредоносных программ. В 2022 году по сравнению с 2021 годом наблюдался рост ежедневных обнаруженных атак на 5%, при этом количество вирусных файлов достигало 400000 штук ежедневно. Кроме того, целевые атаки проводились под видом файлов Microsoft Office, которые фактически блокировали работу сервисов, систем, цифровых платформ. Цифры производительности сектора DarkNet свидетельствуют о масштабном и целенаправленном финансировании хакерства в сети Интернет (рис. 5).

Несмотря на впечатляющие цифры кибератак платформы продолжали работать в 2022 году. Банковское обслуживание проводилось фактически без перебоев, банки максимально быстро адаптировались к смене вендоров (после ухода иностранных компаний), к замене платежных систем, выдерживали массированные атаки хакеров и оперативно устраняли свои уязвимости.

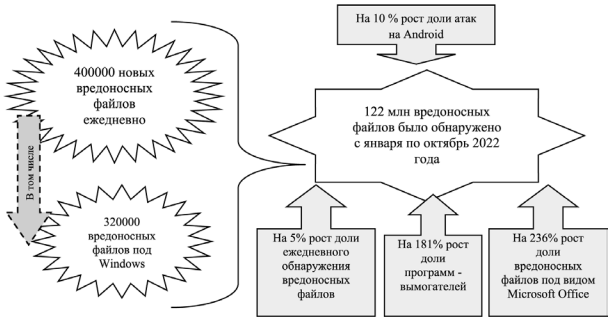

Рис. 5. Статистика ежедневных атак файлами-вирусами в 2022 году.
Источник: составлено авторами по материалам [18–20]

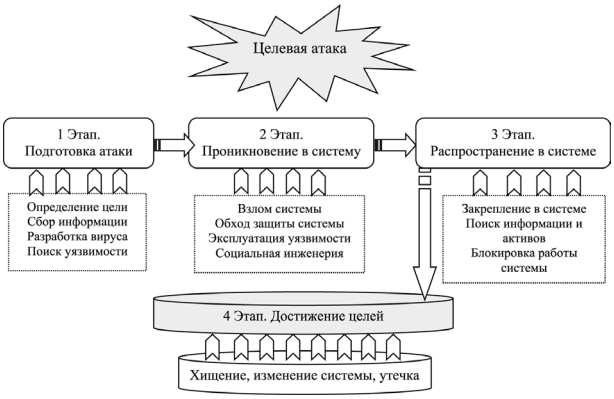

Рис. 6. Основные этапы реализации целевых кибератак на банки.
Источник: составлено авторами по материалам [20,22]

В 2023 году интернет-банкинг продолжит свое развитие и появятся следующие направления:
– система быстрых платежей (СБП);
– банки создают и углубляют свои цифровые платформы, выстраивая целые экосистемы на их основе;
– усложняется работа банков с Big Data с помощью которой формируется сегментированный оффер для клиентов;
– онлайн-финансовое планирование бюджетов клиентов;
– полная цифровизация данных, архивов и досье по клиентам;
– полный переход на безбумажный документооборот и применение электронной цифровой подписи;
– развитие корпоративных IoT на основе умных устройств от банков (ТВ-приставка SberBox, смарт-дисплей SberPortal);
– ESG-банкинг – концепция банковской деятельности, в основе которой лежит экологическая, социальная и корпоративная ответственность [3, 19, 21].

Банки всегда будут в центре внимания хакеров, так как атаки на банковский сектор имеют мошеннический характер, поскольку важным для злоумышленников является не информация, а средства на счетах клиентов. Можно заметить, что атаки на цифровые системы банков носят целевой таргетированный характер.

Целевые атаки готовятся определенное время, направлены на результативность (кражу), под них специально разрабатывается вредоносная программа с учетом штатных средств защиты. К сожалению, результативность подобных атак достаточно высокая, что обеспечивает достижение поставленной цели. Для лучшего понимания природы целевой атаки предлагаем изучить ее основные фазы (рис. 6).

Фактически целевые атаки APT (Advanced Persistent Threat) очень сложно предотвратить, так как хакеры действуют осторожно, хорошо маскируются и постоянно совершенствуют свой инструментарий и методику. Все существующие средства защиты сервисов от целевых атак в основном строятся на идентификации и детектировании известных атак. При появлении новых видов вредоносных файлов система не всегда может сработать на нее как на вирус. В этом заключается основная проблема всех систем обеспечения безопасности – они работают постфактум, после реализации атаки и перевода ее в массовый характер. Неизбежны при таком подходе ошибки системы защиты 1 и 2 уровней, что приводит к успеху целевых атак. Злоумышленники пользуются тем фактом, что не всегда система защиты реагирует однозначно на появление аномалии как на целевую атаку и поэтому не реагирует на нее. В такой ситуации необходимо усиливать работу по детектированию аномалий и однозначной идентификации их как атаки, после чего будет срабатывать система защиты согласно утвержденному протоколу.

Атаки APT требуют комплексного подхода к выстраиванию системы защиты цифровых платформ. Ежедневное обновление пакета вредоносных программ, атакующих сервисы, впечатляет своей масштабностью и заставляют искать новые специализированные решения по их предотвращению [22]. С усложнением цифровых платформ кредитных организаций должна модернизироваться и система безопасности, которая не просто должна блокировать работу всего сервиса, но и быстро уничтожать вирусы и вредоносные файлы. Высокие требования клиентов к скорости и бесперебойности совершений операций в онлайн-среде в режиме 24/7 наряду с растущей конкуренцией между финансовыми организациями исключают полную блокировку работы платформы. Поэто-

Рис. 7. Элементы системы безопасности (СБ) коммерческого банка.
Источник: составлено авторами по материалам [23,24]

му необходимы решения, которые автоматически будут отражать атаки, не нарушая темпов работы экосистемы и ее качества. Рассмотрим основные ключевые элементы выстраивания системы безопасности (рис. 7).

2. Deception-решения

Представленные элементы СБ необходимо постоянно модернизировать, буквально ежедневно, так как появление каждый день тысячи новых вредоносных программных обеспечений не оставляют вариантов для статичной работы. Поэтому новые решения для обеспечения безопасности продолжают появляться.

Одним из примеров нового подхода к выстраиванию защиты цифровой платформы выступают – Deception-ловушки, обеспечивающие обнаружение в режиме реального времени атаки APT, реальную защиту ценных активов за счет переключения целей хакеров на фейковые сайты и ложные активы, исключение ложных срабатываний и т.п. Помимо прочего в процессе детектирования атак данная технология также собирает и генерирует информацию о мошенниках – составляет их профиль, проводит анализ применяемых методов и инструментов, составляет хронологию взлома, определяет источники происхождения хакеров по IP-адресам и данным DNS [24, 25].

Представим схематично алгоритм работы Deception в системе безопасности коммерческого банка. Как видим из рис/ 8 фактически сеть Deception DDP создает внутри системы имитационную модель функционирования настоящих сервисов и узлов для отвлечения внимания злоумышленников. Сеть-ловушка работает во всей системе, зациклена на каждый входящий узел из внешней среды Интернет. С нашей точки зрения, необходимо таким образом настраивать DDP, чтобы любой входящий сигнал из вне поступал сначала в сеть-ловушку, где автоматически идентифицировался и детектировался, а затем по результатам оценки либо блокировался, либо дальше перенаправлялся в реальную сеть [26–28]. При этом на выходе из имитационной сети должна стоять штатная система антивирусного программного обеспечения, то есть будет осуществляться система двухуровневого контроля входных запросов: 1 уровень – детектирование входящих запросов, 2 уровень – антивирусная защита и оценка. Затем запросы поступают в реальную сеть (экосистему), где обрабатываются и направляются ответные запросы, оказываются финансовые услуги клиентам. В узле «Защита» не просто проходит штатная проверка на антивирусные уязвимости, но и должна генерироваться оперативная информация по новым обнаруженным вредоносным входящим запросам и файлам.

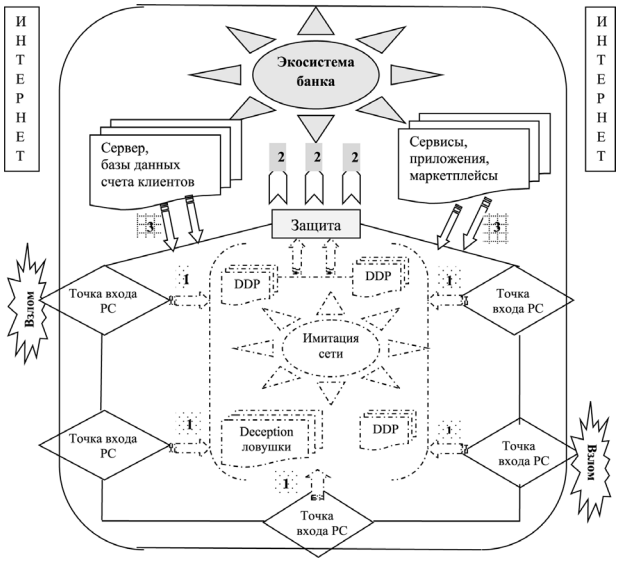

Рис. 8. Цифровая банковская сеть с раскинутой системой защиты Deception DDP (Distributed Deception Platform).
Источник: составлено авторами

В зависимости от скорости передачи накопленной информации по всей сети и ее применении будет зависеть эффективность всей системы защиты цифровой платформы. Очень важно, чтобы выстроенная система информационной безопасности банка быстро обменивалась информацией и быстро самообучалась. Только в таком случае система экономической безопасности будет результативно противостоять кибератакам и мошенническим провокациям. В данной ситуации очень перспективно выстраивать саму имитационную сеть на основе нейросетей, которые динамично трансформируются в процессе применения и быстро самообучаются [29, 30].

Технологии и решения Deception сегодня сравнительно новые и продолжают развиваться в соответствии с запросами клиентов. Отметим, что это решение не заменяет существующих стандартных систем антивирусного поиска, а только дополняет их новым подходом к обнаружению несанкционированных входов, взломов, целевых кибератак. Основная ценность данной технологии – это возможность обнаружить целевые атаки на систему, которые штатные ПО не в состоянии идентифицировать. Кроме того, при прохождении такой хакерской атаки через сеть DDP считывается сам профиль взломщика и его местоположение через IP-адрес компьютера. Основная задача сводится в правильной ее настройке и механизмах ее применения. Это превентивный подход к выстраиванию защиты, при котором на моменте входа отражаются хакерские атаки, что снижает их результативность и эффективность, сокращает долю несанкционированных операций со счетами клиентов и в итоге подрывает финансовую основу DarkNet.

Заключение

Резюмируя наше исследование, отметим, что проблемы обеспечения экономической безопасности в цифровой экономике трансформируются в проблему кибербезопасности, так как успех мошенников будет зависеть прежде всего от их технической возможности взломать систему. Поэтому сегодня в эпоху Digital системы защиты платежных и финансовых сервисов банков зависят от качества команды IT-специалистов. Кибератаки будут продолжаться и их методы будут модернизироваться, так как DarkNet – это цифровой теневой сектор со своими инвесторами и заказчиками, которые готовы финансировать нелегальные пути вывода денежных средств и ценной информации. Эксперты по безопасности банков должны тщательно детектировать и анализировать информацию, поступающую вместе с вредоносными ПО, чтобы формировать и выстраивать эффективную систему экономической безопасности.

Литература

1. *Melnik A., Ermolaev K., Kuzmin M.* Mechanism for Adjustment of the Companies Innovative Activity Control Indicators to Their Strategic Development Goals Global // Journal of Flexible Systems Management. 2019, № 20(4). P. 189-218. DOI:10.1007/s40171-019-00210-z.
2. *Sushil P.* Managing Lifetime Wastivity // Global Journal of Flexible Systems Management. 2018, № 19(3). P. 187-189. DOI:10.1007/s40171-018-0194-8.
3. Аналитический отчет «Business Internet Banking Rank 2022». Электронный ресурс. Режим доступа: https://www.markswebb.ru/report/business-internet-banking-rank-2022/#anchor-about.
4. *Burbach D.T. Watts C.* Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News // Naval War College Review. 2020, Vol. 73: No. 1, Article 17. Available at: https://digital-commons.usnwc.edu/nwc-review/vol73/iss1/17.
5. Global trends of the digital economy development / A. V. Kolesnikov, L. E. Zernova, V. V. Degtyareva Yu. I. Sigidov // Opcion. 2020. Vol. 36. No S26. P. 523-540.
6. *Федотова Г.В., Куразова Д.А.* Угрозы кибербезопасности устойчивости цифровых платформ // В сборнике: BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики. Материалы IX Международной научно-практической очно-заочной конференции. Отв. за выпуск: А.Ю. Коковихин, Н.М. Сурнина, отв. редактор В.В. Городничев. Екатеринбург. 2022. С. 118-120.
7. *Буряк В.В.* Хакеры, хактивизм и проблема обеспечения кибербезопасности в условиях цифровой экономики / В.В. Буряк // Бенефициар. Кемерово, 2018. С.12-18. Режим доступа: http://beneficiaridp.ru/wp-content/uploads/v27.pdf
8. *Буряк В.В.* Цифровая экономика, хактивизм и кибербезопасность: Монография / В. В. Буряк. Симферополь: ИП Зуева Т.В. 2019. 140 с.
9. *Клочкова Е. Н., Леднева О. В.* Оценка эффективности развития информационного общества в России и некоторых странах мира. Режим доступа: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/f73457f75b45591b44257d63004afbf9 (дата обращения: 15.01.2023).
10. *Бухт Р., Хикс Р.* Определение, концепция и измерение цифровой экономики // Вестник международных организаций. Т. 13. № 2. С. 143–172. DOI: 10.17323/1996.
11. *Гудкова О.В.* Риски и угрозы экономической безопасности России в условиях цифровизации экономики // Известия высших учебных заведений. Серия «Экономика, финансы и управление производством» [Ивэкофин]. 2022. № 01(51). С.73-80. DOI: 10.6060/ivecofin.2022511.587.
12. *Ермакова Л.В., Гудкова О.В., Дворецкая Ю.А.* Инновационные технологии на рынке банковских услуг. Бюллетень науки и практи-

ки. 2018. Т. 4. № 5. С. 424-429. DOI:10.5281/zenodo.1246290.
13. *Силаева В.В., Назарова О.Г.* Система управления рисками в таможенной деятельности как направление обеспечения национальной безопасности в сфере внешней торговли. Финансовая жизнь. 2021. № 2. С. 28-31.
14. *Махутов Н.А.* Безопасность и риски: системные исследования и разработки / Н.А. Махутов. Новосибирск: Наука. 2017. 724 с.
15. *Елисеев А.В., Кузнецов Н.К., Миронов А.С.* Системный подход в оценке динамических состояний технических объектов на основе методов структурного математического моделирования // Труды ИСА РАН. 2022. Том 72. Вып.1. С. 93-104. DOI: 10.14357/20790279220109.
16. *Лившиц В.Н., Шаталова О.М., Дмитриева О.В.* Управляемая экономика: актуальные вопросы государственного управления в условиях цифровой трансформации // Труды ИСА РАН. 2021. Том 71. Вып.4. С. 11-22. DOI: 10.14357/20790279210402
17. *Моденов А.К., Власов М.П.* Особенности экономической безопасности в цифровой экономике // Петербургский экономический журнал. 2020. №2. С. 121-134.
18. *Федотова Г.В., Орлова Е.Р., Бочарова И.Е*. Вопросы кибербезопасности цифровых финансовых сервисов // Информационные технологии и вычислительные системы. 2022. №2. С. 37-45. DOI 10.14357/20718632220205
19. *Капустина Ю. А., Ильясов Р. Х., Цицигэ.* Экономика хактивизма – новый вектор развития теневого бизнеса // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2022. 12(5). С. 56-67.
20. Аналитические отчеты об угрозах и уязвимостях АСУ ТП на портале Kaspersky Threat Intelligence. Электронный ресурс. Режим доступа: https://ics-cert.kaspersky.ru/services/
21. Тренды digital-трансформации банков 2021–2024. Электронный ресурс. Режим доступа: https://vc.ru/future/338072-trendy-digital-transformacii-bankov-2021-2024.
22. 2022-й стал «антирекордным» по количеству вирусов для ПК. Электронный ресурс. Режим доступа: https://4pda.to/2022/12/06/407105/2022_j_stal_antirekordnym_po_ kolichestvu_virusov_dlya_pk/
23. Цифровая повестка Евразийского экономического союза до 2025 года: перспективы и рекомендации Обзор. URL: http://documents.vsemirnyjbank.org/curated/ru/413921522436739705/pdf/EAEU-Overview-Full-RUS-Final.pdf
24. *Жиленков А.А., Черный С.Г.* Извлечение информации из BigData с помощью нейросетевых архитектур как сетей ассоциаций информационных гранул // Труды ИСА РАН. 2022. Том 72. Вып. 3. С. 81-90. DOI: 10.14357/20790279220308
25. *George B., Sahar V., Samir D., Grigoris A.* Supply Chain Risk Management and Artificial Intelligence: State of the Art and Future Research Directions // International Journal of Production Research. 2018, № 7. P. 2179-2202. DOI:10.1080/00207543.2018.1530476.
26. *Сиротюк В.О.* Методы построения и анализа онтологической модели и эталонной базы данных цифрового фонда интеллектуальной собственности // Информационные технологии и вычислительные системы. 2022. №3. С. 58-66. DOI 10.14357/20718632220306
27. *Швецов А.Н.* Новейшие информационные технологии «цифровизации экономики»: содержание, перспективы, затраты // Труды ИСА РАН. 2021. Том 71. Вып. 1. С. 27-35.
28. *Jankowicz D.* Limits to Knowledge Transfer: What They Already Know in the Post-Command Economies // Journal of East-West Business. 2001, № 7(2). P. 37-59. DOI:10.1300/J097v07n02_03.
29. *Clarence W. de Silva.* Vibration. Fundamentals and Practice. Boca Raton, London, New York, Washington, D.C.: CRC Press. 2000. 957 p.
30. *Tapscott, D.* The Digital Economy: Promise and Peril In The Age of Networked Intelligence, McGrawHill. 1995. 342 p.

Федотова Гилян Васильевна. Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Россия. Ведущий научный сотрудник. Доктор экономических наук, доцент. Количество печатных работ: более 400 (в т.ч. 20 монографий). Область научных интересов: управление социально-экономическими процессами, региональная экономика, экономика АПК. E-mail: g_evgeeva@mail.ru (ответственный за переписку)

Капустина Юлия Александровна. Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный лесотехнический университет», г. Екатеринбург, Россия. Директор Социально-экономического института. Кандидат экономических наук, доцент. Количество печатных работ: более 50 (в т.ч. 5 монографий). Область научных интересов: экономическая безопасность, управленческий учет, региональная и отраслевая экономика. E-mail: kapustina_bu@mail.ru

Ильясов Руслан Хизраилевич. Федеральное государственное бюджетное образовательное учреждение высшего образования «Чеченский государственный университет им. А.А. Кадырова», г. Грозный, Россия. Заведующий кафедрой. Кандидат экономических наук, доцент. Количество печатных работ: более 80 (в т.ч. 5 монографий). Область научных интересов: экономическая безопасность, кибербезопасность, цифровая экономика, математические методы в экономике. E-mail: ilyasov_95@mail.ru

Цицигэ. Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский экономический университет им. Г.В. Плеханова», г. Москва, Россия. Кандидат сельскохозяйственных наук, доцент. Количество печатных работ: более 30 (в т.ч. 3 монографии). Область научных интересов: региональная экономика и отраслевая экономика, цифровизация экономических процессов, информационные цифровые технологии. E-mail: nutug123@gmail.com

Deception solutions in the system of economic security of the bank

G.V. Fedotova[I], Yu.A. Kapustina[II], R.Kh. Ilyasov [III], Qiqige [IV]

[I] Federal State Institution "Federal Research Center "Computer Science and Management" of the Russian Academy of Sciences», Moscow, Russia

[II] Ural State Forest Engineering University, Yekaterinburg, Russia

[III] Kadyrov Chechen State University, Grozny, Russia

[IV] Plekhanov Russian University of Economics, Moscow, Russia

Abstract. The work is devoted to an overview of current trends in the development of online banking customer service using remote service technologies. The complication of banking digital platforms has led to the formation of information ecosystems that can satisfy a variety of customer needs. Using the SBER ecosystem as an example, it is shown that today banks not only manage customer accounts, but also integrate with marketplaces to provide various non-financial services. The process of accumulation of colossal arrays of personal and confidential information, financial assets attracts the interest of fraudsters working on the Internet. The statistics of cyber theft and unauthorized access to digital services proves that cyber fraud is constantly expanding and is looking for new tools to hack systems. Therefore, the purpose of the work was to substantiate a new approach to building protection based on the detection of cyber-attacks – deception. The goal set led to the solution of the following tasks: the general trends in the complication of banking digital platforms to entire ecosystems were considered, the statistics of cyber fraud on the Internet and the features of targeted cyber-attacks were studied, a new approach to building a system for protecting digital banking services was proposed.

Keywords: *security, internet banking, personal data, cyber fraud, theft.*

DOI: 10.14357/20790279230212

References

1. *Melnik A., Ermolaev K., Kuzmin M.* Mechanism for Adjustment of the Companies Innovative Activity Control Indicators to Their Strategic Development Goals Global // Journal of Flexible Systems Management. 2019, № 20(4). P. 189-218. DOI:10.1007/s40171-019-00210-z.
2. *Sushil P.* Managing Lifetime Wastivity // Global Journal of Flexible Systems Management. 2018, № 19(3). P. 187-189. DOI:10.1007/s40171-018-0194-8.
3. Analytical report "Business Internet Banking Rank 2022". Electronic resource. Access mode: https://www.markswebb.ru/report/business-internet-banking-rank-2022/#anchor-about
4. *Burbach D.T. Watts C.* Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News // Naval War College Review. 2020, Vol. 73: No. 1, Article 17. Available at: https://digital-commons.usnwc.edu/nwc-review/vol73/iss1/17
5. Global trends of the digital economy development / A. V. Kolesnikov, L. E. Zernova, V. V. Degtyareva Yu. I. Sigidov // Opcion. 2020. Vol. 36. No S26. P. 523-540.
6. *Fedotova G.V., Kurazova D.A.* Cybersecurity threats to the stability of digital platforms // In the collection: BI-technologies and corporate

information systems in optimizing business processes in the digital economy. Materials of the IX International scientific and practical part-time conference. Rep. for the issue: A.Yu. Kokovikhin, N.M. Surnina, responsible editor V.V. Gorodnichev. Yekaterinburg. 202., P. 118-120.
7. *Buryak V.V.* Hackers, hacktivism and the problem of ensuring cybersecurity in a digital economy / V.V. Buryak // Beneficiary. Kemerovo, 2018. P. 12-18. Access mode: http:// beneficiaridp.ru/wp-content/uploads/v27.pdf
8. *Buryak V.V.* Digital economy, hacktivism and cybersecurity: Monograph / V. V. Buryak. Simferopol: IP Zueva T.V., 2019. 140 p.
9. *Klochkova E. N., Ledneva O. V.* Evaluation of the effectiveness of the development of the information society in Russia and some countries of the world. Access mode: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/f73457f75b45591b44257d63004afbf9 (date of access: 01.15.2023).
10. *Bukht R., Hicks R.* Definition, concept and measurement of the digital economy // Vestnik mezhdunarodnykh organizatsii. T. 13. No. 2. P. 143–172. DOI: 10.17323/1996.
11. *Gudkova O.V.* Risks and threats to the economic security of Russia in the context of the digitalization of the economy // Izvestia of higher educational institutions. Series "Economics, Finance and Production Management" [Ivekofin]. 2022. No. 01(51). P. 73-80. DOI: 10.6060/ivecofin.2022511.587.
12. *Ermakova L.V., Gudkova O.V., Dvoretskaya Yu.A.* Innovative technologies in the banking services market // Bulletin of science and practice. 2018. V. 4. No. 5. P. 424-429. DOI:10.5281/zenodo.1246290.
13. *Silaeva V.V., Nazarova O.G.* The risk management system in customs activities as a direction for ensuring national security in the field of foreign trade // Fnancial life. 2021. No. 2. P. 28-31.
14. *Makhutov N.A.* Security and risks: system research and development / N.A. Makhutov. – Novosibirsk: Nauka, 2017. 724 p.
15. *Eliseev A.V., Kuznetsov N.K., Mironov A.S.* A systematic approach to assessing the dynamic states of technical objects based on methods of structural mathematical modeling // Proceedings of the ISA RAS. 2022. Volume 72. Issue 1. P. 93-104. DOI: 10.14357/20790279220109.
16. *Livshits V.N., Shatalova O.M., Dmitrieva O.V.* Managed economy: topical issues of public administration in the context of digital transformation // Proceedings of the ISA RAS. 2021. Volume 71. Issue 4. P. 11-22. DOI: 10.14357/20790279210402
17. *Modenov A.K., Vlasov M.P.* Features of economic security in the digital economy // Petersburg Economic Journal. 2020. №2. _. 121-134.
18. *Fedotova G.V., Orlova E.R., Bocharova I.E.* Issues of cybersecurity of digital financial services // Information technologies and computing systems. 2022. №2. pp. 37-45. DOI 10.14357/20718632220205
19. *Kapustina Yu. A., Ilyasov R. Kh., Tsitsige.* The economy of hacktivism is a new vector for the development of shadow business // Bulletin of the South-Western State University. Series: Economy. Sociology. Management. 2022.12(5). P. 56-67.
20. Analytical reports on ICS threats and vulnerabilities on the Kaspersky Threat Intelligence portal. Electronic resource. Access mode: https://ics-cert.kaspersky.com/services/
21. Trends in digital transformation of banks 2021–2024. Electronic resource. Access mode: https://vc.ru/future/338072-trendy-digital-transformacii-bankov-2021-2024
22. 2022 has become an "anti-record" in terms of the number of viruses for PCs. Electronic resource. Access mode: https://4pda.to/2022/12/06/407105/2022_j_stal_antirekordnym_po_kolichestvu_virusov_dlya_pk/
23. Digital Agenda of the Eurasian Economic Union until 2025: Perspectives and Recommendations Overview. URL: http://documents.vsemirnyjbank.org/curated/ru/413921522436739705/pdf/EAEU-Overview-Full-RUS-Final.pdf
24. *Zhilenkov A.A., Cherny S.G.* Extracting information from BigData using neural network architectures as networks of information granule associations // Proceedings of the ISA RAS. 2022. Volume 72. Issue. 3. P. 81-90. DOI: 10.14357/20790279220308
25. *George B., Sahar V., Samir D., Grigoris A.* Supply Chain Risk Management and Artificial Intelligence: State of the Art and Future Research Directions // International Journal of Production Research. 2018. No. 7. P. 2179-2202. DOI:10.1080/00207543.2018.1530476.
26. *Sirotyuk V.O.* Methods for constructing and analyzing an ontological model and a reference database for a digital intellectual property fund // Information technologies and computing systems. 2022. No3. P. 58-66. DOI 10.14357/20718632220306
27. *Shvetsov A.N.* The latest information technologies of "digitalization of the economy": content,

prospects, costs // Proceedings of the ISA RAS. 2021. Volume 71. Issue. 1. P. 27-35.
28. *Jankowicz D.* Limits to Knowledge Transfer: What They Already Know in the Post-Command Economies // Journal of East-West Business. 2001, № 7(2). P. 37-59. DOI:10.1300/J097v07n02_03.
29. *Clarence W. de Silva.* Vibration. Fundamentals and Practice. Boca Raton, London, New York, Washington, D.C.: CRC Press. 2000. 957 p.
30. *Tapscott, D.* The Digital Economy: Promise and Peril In The Age of Networked Intelligence, McGrawHill. 1995. 342 p.

Fedotova Gilyan Vasilievna. Federal State Institution "Federal Research Center "Computer Science and Management" of the Russian Academy of Sciences", Moscow, Russia. Leading Researcher. Doctor of Economics, associate professor. Number of printed works: more than 400 (including 20 monographs). Research interests: management of socio-economic processes, regional economics, economics of the agro-industrial complex. E-mail: g_evgeeva@mail.ru (responsible for correspondence)

Kapustina Yulia Alexandrovna. Federal State Budgetary Educational Institution of Higher Education "Ural State Forest Engineering University", Yekaterinburg, Russia. Director of the Socio-Economic Institute. Candidate of Economic Sciences, Associate Professor. The number of printed works is more than 50 (including 5 monographs). Research interests: economic security, management accounting, regional and sectoral economics. E-mail: kapustina_bu@mail.ru

Ilyasov Ruslan Khizrailevich. Federal State Budgetary Educational Institution of Higher Education "Chechen State University named after A.A. Kadyrov, Grozny, Russia. Head of the Department "Accounting, analysis, audit in the digital economy". Candidate of Economic Sciences, Associate Professor. The number of printed works is more than 80 (including 5 monographs). Research interests: economic security, cybersecurity, digital economy, mathematical methods in economics. E-mail: ilyasov_95@mail.ru

Qiqige. Federal State Budgetary Educational Institution of Higher Education "Russian University of Economics named after G.V. Plekhanov, Moscow, Russia. Candidate of Agricultural Sciences, Associate Professor of Management Theory and Business Technologies. Number of publications: more than 30 (including 3 monographs). Research interests: regional economy and branch economy, digitalization of economic processes, digital information technologies. E-mail: nutug123@gmail.com