Г. В. Федотова, Е. Р. Орлова, И. Е. Бочарова, Вопросы кибербезопасности цифровых финансовых сервисов, *ИТиВС*, 2022, выпуск 2, 37–45

DOI: 10.14357/20718632220205

Вопросы кибербезопасности цифровых финансовых сервисов

Г. В. Федотова, Е. Р. Орлова, И. Е. Бочарова

Федеральный исследовательский центр «Информатика и управление» РАН, Москва, Россия

Аннотация. В статье рассмотрены проблемы безопасности цифровых финансовых сервисов, функционирующих в настоящее время исключительно в онлайн-формате. Это привело к появлению дополнительных рисков, связанных с кибермошенничеством. Существующие системы кибербезопасности, как правило, реагируют лишь на факт хищений и на появления новых мошеннических схем, что недостаточно, т.к. низкий уровень возврата похищенных сумм со счетов клиентов позволяет кибермошенникам финансировать свою теневую деятельностьна перспективу. В связи с этим обозначилась потребность в прогнозировании возможных кибератак мошенников и противодействии им. Одним из способов такого противодействия может стать новый подход к построению системы кибербезопасности, в качестве которого предложено использовать метод онтологии (в терминах информатики). Такой подход позволит предметно представить весь механизм проведения сделки и заранее обнаружить уязвимости в существующей системе защиты.

Ключевые слова: финансовые сервисы, кибербезопасность, цифровизация, цифровая экономика, защита.

DOI 10.14357/20718632220205

Введение

Современное цифровое общество невозможно без цифрового финансового взаимодействия между субъектами бизнеса. Переход на цифровые сервисы и технологии с уверенностью можно признать основным трендом цифровизации. В условиях карантинных ограничений удаленные системы платежей и переводов позволили многим сферам бизнеса не растерять своих клиентов и сохранить необходимый уровень прибыли. Банковский сектор наиболее адекватно отреагировал на невозможность физического доступа клиентов к объектам системы платежей и существенно расширил свой цифровой функционал. Фактически в условиях пандемии банками были выстроены целые цифровые экосистемы, которые предоставили удаленный доступ к банковскому сервису по всему перечню услуг.

Финансовая экосистема - это единое онлайн-пространство, в котором взаимодействует множество сервисов, позволяющих удалённо работать со счетами клиентов. Сегодня практически любую денежно-финансовую операцию можно провести дистанционно, что позволяет строить целые бизнес-модели на технологиях удаленного доступа. Финансовые операции онлайн являются гарантом реализации многих сделок по покупке-продаже не только услуг, но и реальных товаров. Простота, скорость и удобство оплаты через платежные системы и онлайн сервисы привлекают все большее количество клиентов, желающих осуществлять такие переводы и платежи. Вынужденные карантинные меры показали, что будущее - за цифровыми финансовыми

сервисами. Благодаря возможности удаленной оплаты развиваются целые глобальные виртуальные корпоративные структуры.

Параллельно развитию цифровой реальности эволюционирует система преступлений в киберпространстве, растут объемы вызванных ими убытков [1]. Представленные на Рис. 1 данные характеризуют увеличение числа кибермошенников, постоянно ищущих новые схемы и технологии взломов счетов и баз данных.

Для сохранения своих конкурентных позиций цифровые сервисы и экосистемы должны постоянно контролировать ситуацию, учитывая уровень обеспечения цифровой безопасности, и изучать новые факты мошенничества [3-5]. В этой связи необходимо не просто изучать статистику кибератак, но и выявлять основные схемы работы мошенников, их методы и технологии. Нужен концептуальный подход к построению безопасного киберпространства, при котором будут учитываться многие факторы внешней и внутренней среды и особенности цифровых профилей клиентов.

Проблема обеспечения кибербезопасности в цифровом пространстве в последние годы рассматривалась многими авторами. Среди основных работ в области формирования теории и методологии обеспечения безопасности информационных сервисов можно отметить [6-8, 10, 13, 14, 23, 31]. Вопросам построения собственных систем кибербезопасности и обеспечения их функционирования посвящены работы [1, 5, 6, 15, 16, 21, 24]. Особенности функцтлнтрования цифровых финансовых сервисов и банкинга рассмотрены в работах [19, 25, 26, 30] и ряде других.

Приведенный нами перечень работ показывает, что данному направлению уделяется существенное внимание исследователей многих стран мира. В настоящее время осуществляются попытки сформулировать онтологические основы формирования безопасного цифрового финансового пространства.

1. Материалы исследования

Расширение спектра цифровых финансовых операций и фактически полный перевод некоторых сфер деятельности в онлайн-формат требует большего внимания к повышению безопасности платежных систем и аккумулированию баз персональных данных клиентов. Технологии сохранения конфиденциальности личной информации и денежных средств на счетах клиентов – это, прежде всего, вопрос репутации и будущего успеха онлайн бизнес-модели. Мошенники всегда ищут и используют слабые места в защите цифровых сервисов, поэтому необходимо тщательно проанализировать всю систему в разрезе ее структуры и сформировать комплекс защитных мер с учетом новых

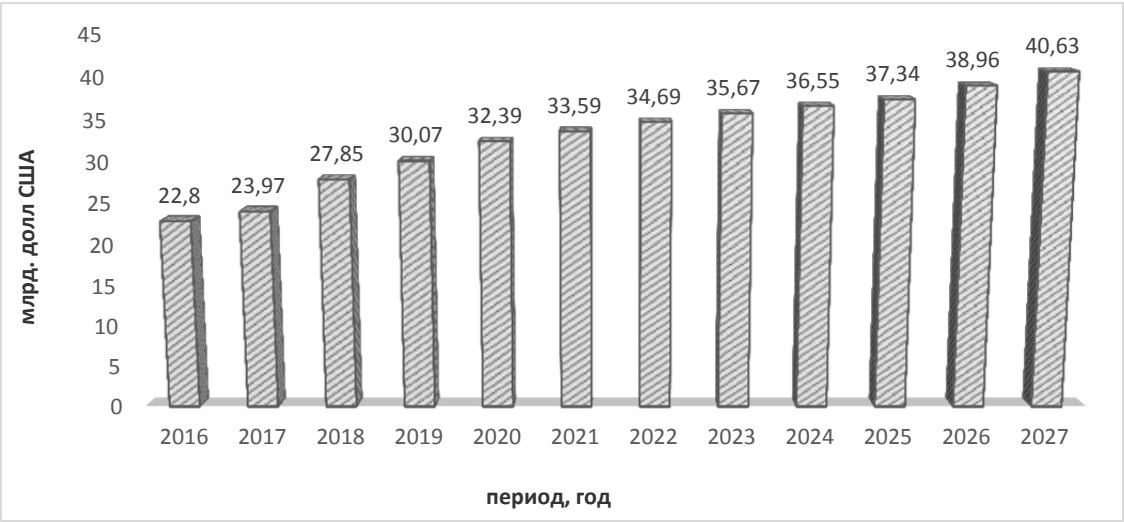

Рис.1. Уровень международных убытков от мошенничества с платежами в период с 2016 до 2027 года, млрд. долл. США [2]

схем мошенничества. Онтология, как наука о системных основах целого, позволит структурно представить кибербезопасность цифрового финансового сервиса и более качественно обосновать технологии защиты данных и счетов. Поэтому онтологический анализ выступил основной задачей данного исследования.

Для решения поставленной задачи были использования следующие методы научного исследования:

- обобщения и систематизации - для оценки происходящих процессов в системе цифрового финансирования сделок;
- статистического и графического анализа - для большей иллюстративности и понимания цифрового материала;
- логического анализа и аналогии - для сопоставления полученных результатов и формирования рекомендаций для будущего развития.

Информационную основу для анализа составили отчеты и методические материалы Банка России, аналитических компаний и данные тематических интернет-сайтов, находящиеся в открытом доступе. Полученные выводы были обоснованы и адаптированы под современные условия организации цифрового финансирования.

2. Результаты исследования

Банковская сфера постоянно расширяет ассортимент предоставляемых финансовых услуг и объединяется с крупными торговыми площадками для большего охвата клиентской базы. На примере Сбербанка России и Тинькофф Банка можно наблюдать принципиально новую бизнес-модель работы финансовой организации. Данные кредитные организации, по сути, являются мультикорпорациями нового поколения, включающими основные отраслевые направления. На основе собственных финансовых сервисов они формируют дополнительные и объединяют их. Благодаря широкому спектру предоставляемых услуг, эти банки аккумулируют большие клиентские базы с персональными данными и выстраивают индивидуальные профили клиентов.

Далее рассмотрим типичные характеристики финансовых экосистем, выстроенных различными организациями.

Представленные на Рис. 2 элементы экосистем известных компаний показывают, как происходит интеграция финансовых организаций и торговых компаний. На основе цифровых финансовых систем появляются новые виды

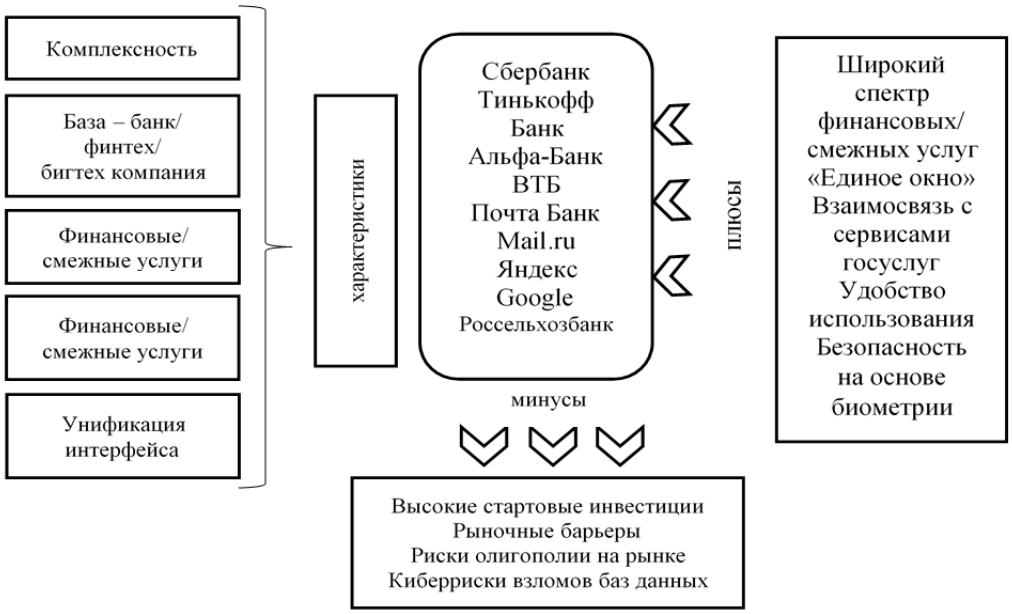

Рис. 2. Основные элементы цифровых сервисов в составе известных экосистем
Составлено авторами по [4, 5]

бизнес-моделей, предлагающих своим клиентам комплексные услуги. Возможности финансовых сервисов позволяют совершать многие операции дистанционно и экономить на содержании офиса.

К сожалению, рассматриваемая финансовая экосистема не является абсолютно безопасной. Основную угрозу для неё представляют кибермошенники, которые могут взломать системы защиты и выкрасть информацию персонального характера или получить доступ к счетам клиентов. Для нивелирования данного фактора цифровые сервисы ведут постоянную работу по совершенствованию системы защиты своих ресурсов [3-5]. Несмотря на все усилия собственников финансовых цифровых сервисов объемы кибермошенничества по данным Банка России на протяжении последних трех лет растут.

На Рис. 3 представлены данные по количеству и объемам операций клиентов различных банков, совершенных без их согласия. Из графика видно, что общее число незаконных онлайн сделок увеличивается год от года. Негативным фактом является низкий процент раскрытия таких краж. Так, по данным Банка России, в 2020 году удалось вернуть 11,3% похищенных средств, в 2019 году сумма возврата составила – 14,6%. До 85% похищенных средств остаются у мошенников, что дает им возможность разрабатывать и финансировать новые схемы и технологии взломов баз данных и счетов [2, 9].

Из анализа практики функционирования финансовых сервисов видно, что мошенниками разработано большое количество схем и технологий вывода ресурсов со счетов [10, 11]. Наиболее распространенные и эффективные сервисы и каналы хищения показаны на Рис. 4.

Как видно из рисунка, почти все случаи мошенничества были совершены через сеть Интернет и средства доступа к ней (до 95%). На втором месте - банковская система (25,9%), на третьем - банкоматы и терминалы (14,6%), на четвертом - электронные кошельки (13,1%). Основными объектами мошенничества являются безналичные денежные средства и переводы – 76,75%. Следовательно, самым незащищенным каналом является Интернет-оплата покупок и платежей, а также онлайн запросы персональных данных клиентов [11]. На Рис. 5 показаны наиболее часто применяемые злоумышленниками в сети Интернет схемы (по материалам Positive Technologies).

Из диаграммы видно, что мошенники постоянно используют сайты компаний и электронную почту пользователей (спам-рассылки, нигерийские письма, предупреждения об обновлении или о взломе, фальшивые клики на рекламу, предложения перейти на фальшивые страницы в интернете и т.д.). Практически все повседневные и текущие операции пользователей сети подвергаются атакам мошенников. Поэтому для успешной борьбы с кибермошенниками нужно хорошо понимать, какие последствия могут повлечь неосторожные действия в интернете, каким образом противостоять атакам и провокациям в онлайн пространстве и защитить свои данные и счета [13-15].

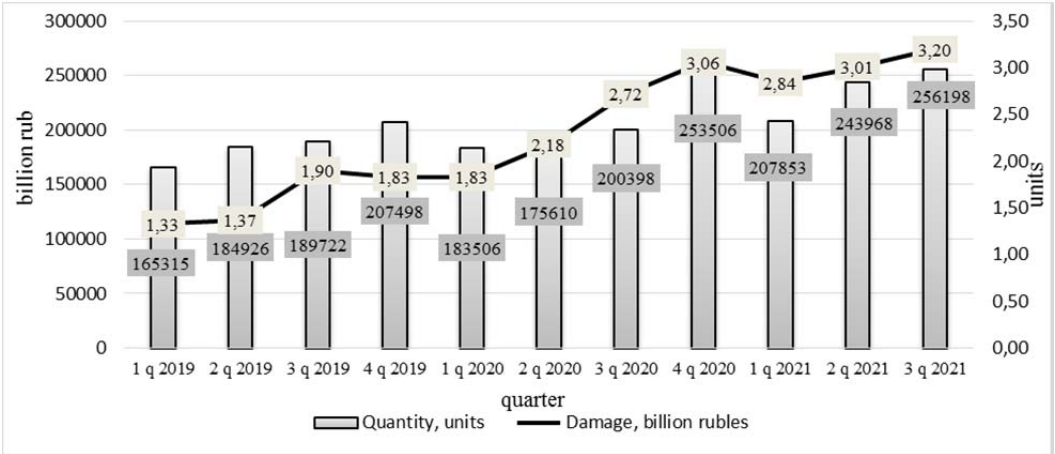

Рис. 3. Объемы и количество совершенных операций без согласий клиента в общем объеме операций [7]

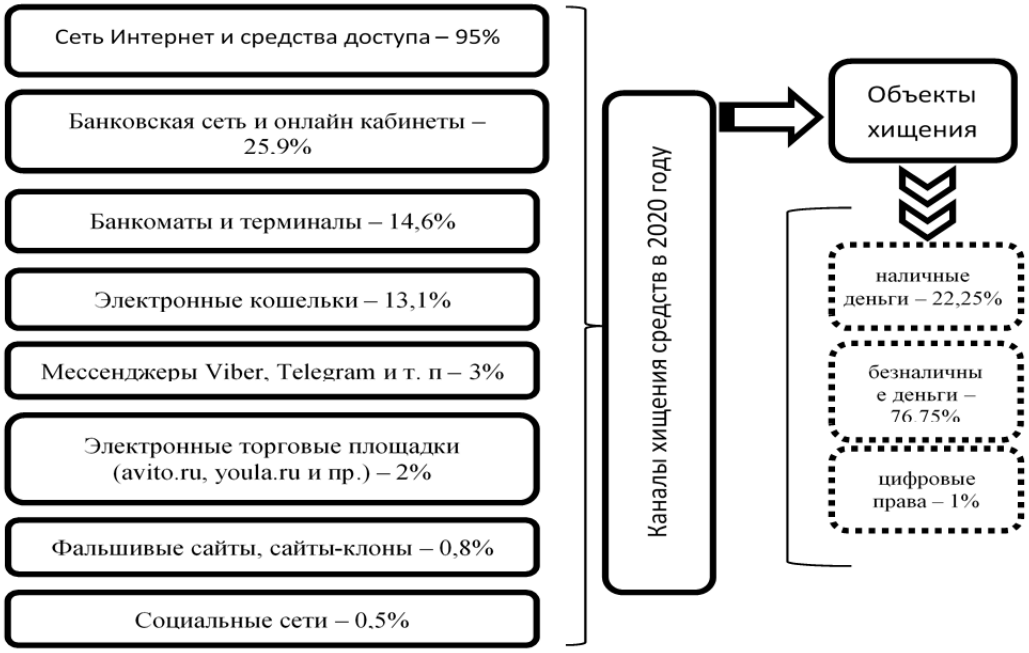

Рис. 4. Наиболее популярные каналы и объекты хищений по итогам 2020 года [7]

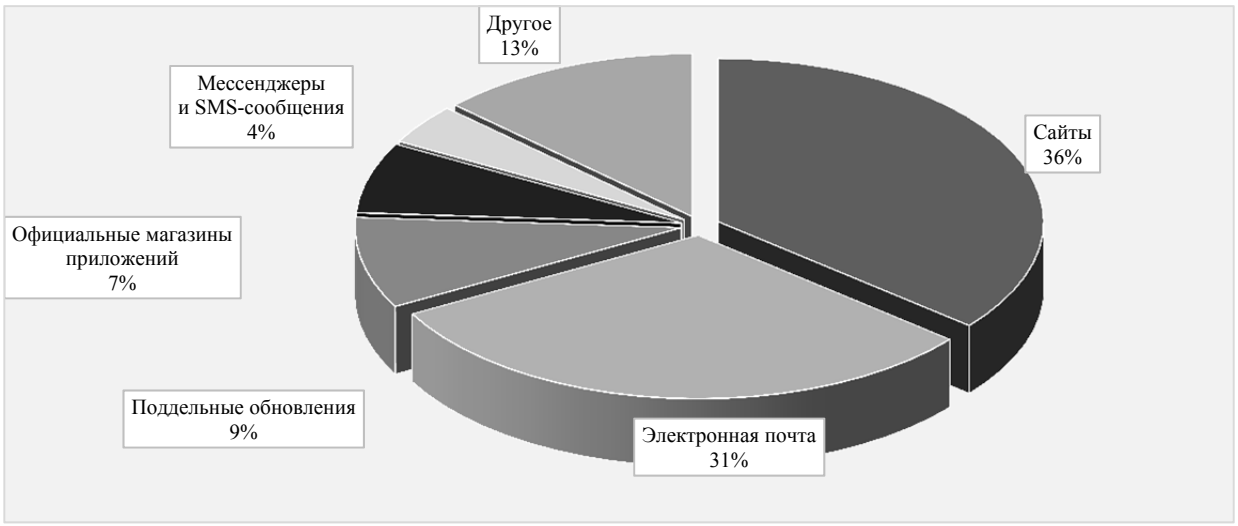

Рис. 5. Способы кибератак на частных лиц через сеть Интернет [12]

Все выше сказанное делает актуальным формирование новой концепции поведения в киберпространстве, позволяющей четко представлять факторы и взаимосвязи использования цифровых финансовых сервисов [16, 17]. Именно такой концепцией является онтология, которая, по своей сути, является философско-методическим подходом, дающим возможность разбивать целое на составные элементы и выявить взаимосвязи между этими элементами. В качестве примера использования данной концепции рассматривается применение онтологического подхода к реализации онлайн-сделки в финансовой экосистеме (Рис. 6).

Процесс заключения сделки раскладывается на отдельные этапы, выявляются основные субъекты этих этапов, их взаимоотношения и взаимосвязи, определяется характер связей и оценивается их безопасность. При таком разложении на элементы можно выяснить слабые/узкие места в сделках и определить наиболее вероятные точки атак мошенников.

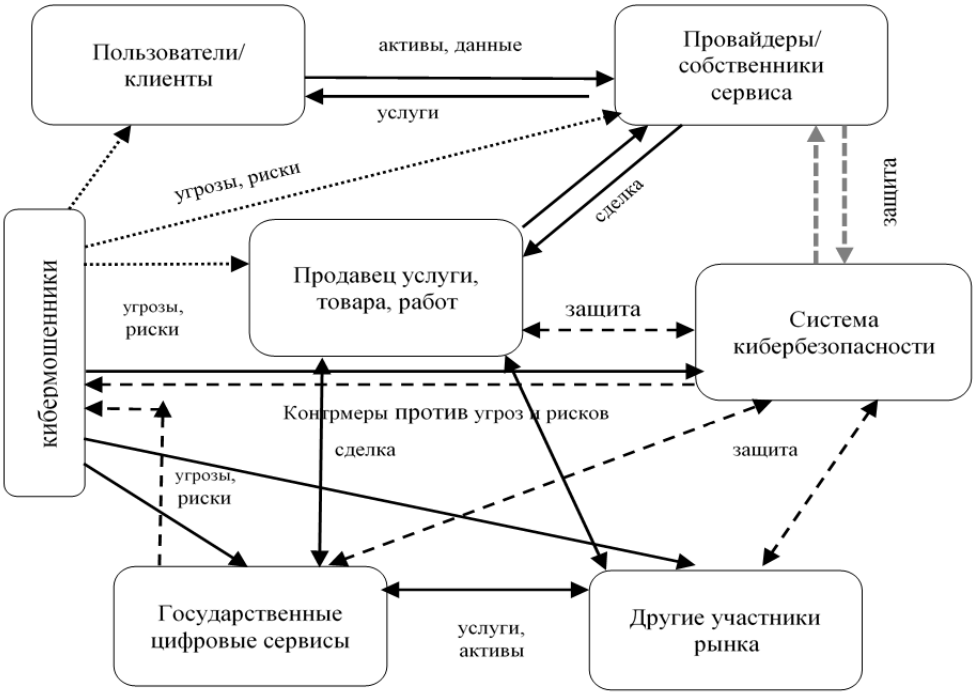

Рис. 6. Базовая онтология кибербезопасности при использовании цифровых финансовых сервисов в сделках
Источник: составлено авторами

Из представленной на Рис. 1 схемы видно, что наименее защищенным звеном здесь являются пользователи (клиенты) с их личными средствами доступа к сети Интернет, т.к. они не имеют собственных систем защиты. Остальные субъекты в ответ на кибератаки усиливают защиту своих сервисов и каналов передачи информации. Государство и специализированные технологические структуры формируют контрмеры против кибермошенников.

Современное киберпространство постоянно расширяется и усложняется, вовлекая все новых участников. Мир движется к виртуальной организации многих видов бизнеса и возникновению компаний, которые существуют только в онлайн среде. Финансовые ресурсы — это наиболее удобный вид актива, который наряду с информационными базами может действовать только в онлайн-пространстве в виде записей на счетах владельцев. Такая форма активов удобна и не требует дополнительных затрат на хранение и транспортировку. Сегодня уже есть валюты, не имеющие физического двойника, выступающие в виртуальном пространстве полноценным платежным средством в системах онлайн платежей [21, 24, 25].

Как уже ранее было сказано, цифровые финансовые сервисы являются весьма привлекательными для атак кибермошенников. Участившиеся факты кибермошенничества в период пандемии и карантинных ограничений доказывают слабую защищенность финансовых сервисов от несанкционированных действий. Системы кибербезопасности, выстраиваемые многими финансовыми организациями, не дают 100% гарантии защиты, так как часто реагируют только на факт хищения или появление новых мошеннических схем/ По прогнозам аналитической компании Positive Technologies, в 2022 году атаки будут только усиливаться. В фокусе внимания, помимо цифровых финансовых сервисов, окажутся государственные цифровые сервисы, поиск наиболее уязвимых мест в системах киберзащиты частных компаний и их веб-ресурсов, особенности работы онлайн-кабинетов кредитных учреждений и сделки с цифровыми активами (NFT) [23, 26].

С нашей точки зрения для формирования оптимальной системы кибербезопасности цифровых сервисов необходимо подходить к вопросам организации цифрового взаимодействия концептуально: формировать онтологический взгляд на

весь процесс. Онтология позволяет на примере отдельных элементов киберпространства оценить эффективность его работы и предугадать наиболее уязвимые моменты в системе, в сделках.

Заключение

Присутствие финансовых ресурсов в онлайн-пространстве год от года увеличивается, появляются новые виртуальные активы, требующие дополнительных механизмов защиты от кибермошенников. Обеспечение высокой степени защиты своих ресурсов – вопрос репутации цифрового бизнеса и его пребывания на рынке. В связи с этим затраты на развитие систем кибербезопасности продолжают расти, так как появление новых мошеннических схем не оставляет возможности для прекращения поиска новых контрмер против мошенников.

Цифровые финансовые сервисы всегда будут находиться в поле зрения мошенников, так как через них ежедневно проводится огромное количество онлайн-переводов. Виртуальные финансовые активы клиентов проще всего вывести через наименее защищённые каналы сети Интернет в момент совершения онлайн-операций. Для лучшего понимания процесса кибервзаимодействия необходимо комплексно представлять проблему кибербезопасности в каждом конкретном случае и применять онтологический подход для ее решения. Такой подход позволит предметно представить весь механизм проведения сделки и обнаружить уязвимости в существующей системе защиты.

Литература

1. Alotaibi F, Furnell S, Stengel I, Papadaki M (2016) A review of using gaming technology for cyber-security awareness Int. J. Inf. Secur. Res. (IJISR) 6(2): 660- 666.
2. European Commission “Commission recommendation of 26. 3.2019: Cybersecurity of 5G networks” (2019). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534&from=GA Accessed 12 Jan 2022.
3. Dimitrov P, Vasenska Iv, Koyundzhiyska-Davidkova Bl, Krastev Vl, Durana P, Poulaki I (2021) Financial Transactions Using FINTECH during the Covid-19 Crisis in Bulgaria Risks 9(3): 48.
4. Fraudulent Transfers Fall on the Bank Shoulders//https//www.rbc.ru/newspaper/2021/12/06/6/a8d14639a79476b808c4eee. Accessed 12 Jan 2022.
5. Computer Security Incident Handling Guide (2021). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP. 800-61r2.pdf. Accessed 12 Jan 2022.
6. Borodakij Y.V., Dobrodeev A.Y., Butuzov I.V. (2013) Cybersecurity as the Main Factor of National and International Security of the XXI Century (Part I) Problems of Cybersecurity 1 (1):2-9.
7. Bogdanov Y.M., Selivanov S.A., Ogarok A.P. et others (2016) Methodic Aspects of Computer Attacks Protection in Communication Networks of Increased Sustainability. Informatization and Communication 2:13-17.
8. Bezkorovaynij M.M., Losev S.A., Tatuzov A.L. (2011) Cybersecurity in the Present World. Terms and Content. Informatization and Communication 6: 27-32.
9. Интернет-мошенники в России заработали более 150 млрд рублей за 2020 год. https://3dnews.ru/1028667/internetmoshenniki-v-rossii-zarabotali-bolee-150-mlrd-rubley-za-2020-god. Accessed 12 Jan 2022.
10. Казарин ОВ, Тарасов АА (2013) Современные концепции кибербезопасности ведущих зарубежных государств Вестник Российского государственного гуманитарного университета 14: 58-74.
11. Кибербезопасность в секторе банковских и финансовых услуг – угрозы IoT, потенциальные решения и блокчейн (2019). https://www.stoodnt.com/ Accessed 12 Jan 2022.
12. Positive Technologies: итоги 2021 года в кибербезопасности и какие вызовы принесет 2022-й. https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-itogi-2021-goda-v-kiberbezopasnosti-i-kakie-vyzovy-prineset-2022-j/. Accessed 26 Jan 2022.
13. Li Y, Cao Y., Qiu H., Gao L, Du Z. and Chen S (2016) Big wave of the intelligent connected vehicles China Communications 13(2): 27-41.
14. Luo Q (2018) Wireless telematics systems in emerging intelligent and connected vehicles: threats and solutions IEEE Wirel. Commun. 25(6): 113-119.
15. Lonsdale MDS, Lonsdale D, Lim HW (2019) The impact of delivering online information neglecting user-centered information design principles. cyber security awareness websites as a case study Inf. Des. J. 24(2): 3-41.
16. Марков АС, Цирлов ВЛ (2007) Управление рисками - нормативный вакуум информационной безопасности Открытые системы. СУБД 8: 63-67.
17. Magomedov SG, Kolyasnikov PV, Nikulchev EV (2020) Development of technology for controlling access to digital portals and platforms based on estimates of user reaction time built into the interface Russian Technological Journal 8(6): 34-46. (In Russ.) https://doi.org/10.32362/2500-316X-2020-8-6-34-46.
18. Burlakov VV, Skubriy EV, Orlova LN, Fedotova GV, Sukhinin AV (2021) Cyber Security in the Era of COVID-19 // Threats to Digital Platforms Stability and Cyber Hygiene Rules Studies in Systems Decision and Controlthis link is disabled: 1565–1574.
19. Nenovsky N, Chobanov P (2021) Digital currency Vs the crypto Bloomberg Businessweek bg July: 44-53.
20. Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федера-

ции (2014). https://cbr.ru/statichtml/file/59420/rs-25-14.pdf. Accessed 28 Jan 2022.
21. Sadek A (2016) Special issue on cyber transportation systems and connected vehicle research J. Intell. Transp. Syst 20(1): 1-3.
22. Селиванов СА, Огарок АЛ (2020) Обеспечение кибербезопасности сложных информационных и управляющих систем Информатизация и связь 1: 28-33.
23. Sizov VA, Kirov AD (2021) The development of models of an analytical data processing system for monitoring information security of an informatization object using cloud infrastructure Russian Technological Journal 9(6): 16-25. (In Russ.) https://doi.org/10.32362/2500-316X-2021-9-6-16-25.
24. Старовойтов АВ (2011) Кибербезопасность как актуальная проблема современности Информатизация и связь 6: 4-7.
25. Thakor, Anjan V (2019) Fintech and banking: What do we know? Journal of Financial Intermediation 41: 100833.
26. Трунцевский ЮВ (2020) Современные вызовы банковского мошенничества финансовому обеспечению электронной коммерции Банковское право 6: 28-36.
27. Шеремет ИА Информационная и кибербезопасность: интервью (2013). http://echo.msk.ru/programs/arsenal/1208183-echo/. Accessed 22 Jan 2022.
28. Штитилис Д, Клишаускас В (2013) Особенности правового регулирования кибербезопасности в национальных законах Литвы, России и США: стратегии кибербезопасности Вопросы российского и международного права 7-8: 80-100.
29. Walls A, Perkins E, Weiss J Definition: Cybersecurity. Gartner. 2013. ID:G00252816. 4 p.
30. Zlateva D, Stavrova E, Vladov R (2017) Digital Bank Marketing in the Context of the Circular Economy International Journal for Science and Arts 1(1): 31-38.
31. Zaytsev A, Dmitriev N, Fayzullin R, Mihel E (2021) Formation of Investment Behavior Strategy using the Game-theoretic Method TEM Journal 10(2): 673-681.

Федотова Гилян Васильевна. Федеральный исследовательский центр «Информатика и управление» РАН, Москва, Россия, ведущий научный сотрудник, доктор экономических наук, доцент, Количество печатных работ: 360. Область научных интересов: проблемы социально-экономического развития региона, кибербезопасность. E-mail: g_evgeeva@mail.ru

Орлова Елена Роальдовна. Федеральный исследовательский центр «Информатика и управление» РАН, Москва, Россия, зав. отделом, доктор экономических наук, профессор, Количество печатных работ: 200. Область научных интересов: проблемы социально-экономического развития региона, инвестиционное развитие, цифровая трансформация. E-mail: orlova@isa.ru

Бочарова Ирина Евгеньевна. Федеральный исследовательский центр «Информатика и управление» РАН, Москва, Россия инженер-исследователь, Количество печатных работ: 60. Область научных интересов: проблемы инвестиционное развитие, цифровая трансформация. E-mail: irisha.maka@yandex.ru

Problems of Digital Financial Services Cybersecurity

G. V. Fedotova, E. R. Orlova, I. E. Bocharova

Federal Research Center "Computer Sciences and Control" RAS, Moscow, Russia

Abstract. Problems of digital financial services security are regarded in the article. As many digital financial services function exclusively in online-format, additional risks, connected with cyberbullies attacting security systems appeared. Pandemia and forced quarantine of the last three years made many users to realize transfers and payments remotely. At the same time, the number of thefts from customer's accounts of has grown as well. Existing cybersecurity systems react, as a rule, just to the fact of the thefts and appearance of new fraudulent schemes. Now it is not enough, it is necessary to predict possible attacts of the scammers, as low level of refund of stolen amounts let cyberbullies finance their shadow activity further. Therefore it is necessary to form a new approach to constructing security system. As such an approach the ontology method is proposed. It can present the entire mechanism of the transaction in detail and detect a vulnerability in the existing system in advance.

Keywords*:* financial services, cybersecurity, digitalization, digital economy, protection.

DOI 10.14357/20718632220205

References

1. Alotaibi F, Furnell S, Stengel I, Papadaki M (2016) A review of using gaming technology for cyber-security awareness Int. J. Inf. Secur. Res. (IJISR) 6(2): 660- 666.
2. European Commission "Commission recommendation of 26. 3.2019: Cybersecurity of 5G networks" (2019). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX: 32019H0534&from=GA Accessed 12 Jan 2022.
3. Dimitrov P, Vasenska Iv, Koyundzhiyska-Davidkova Bl, Krastev Vl, Durana P, Poulaki I (2021) Financial Transac-

tions Using FINTECH during the Covid-19 Crisis in Bulgaria Risks 9(3): 48.
4. Fraudulent Transfers Fall on the Bank Shoulders//https//www.rbc.ru/newspaper/2021/12/06/6/a8d14639a79476b808c4eee. Accessed 12 Jan 2022.
5. Computer Security Incident Handling Guide (2021). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP. 800-61r2.pdf. Accessed 12 Jan 2022.
6. Borodakij Y.V., Dobrodeev A.Y., Butuzov I.V. (2013) Cybersecurity as the Main Factor of National and International Security of the XXI Century (Part I) Problems of Cybersecurity 1 (1):2-9.
7. Bogdanov Y.M., Selivanov S.A., Ogarok A.P. et others (2016) Methodic Aspects of Computer Attacks Protection in Communication Networks of Increased Sustainability. Informatization and Communication 2:13-17.
8. Bezkorovaynij M.M., Losev S.A., Tatuzov A.L. (2011) Cybersecurity in the Present World. Terms and Content. Informatization and Communication 6: 27-32.
9. Internet Scanners Earned Over 150 milrd roubles in 2020 https://3dnews.ru/1028667/internetmoshenniki-v-rossii-zarabotali-bolee-150-mlrd-rubley-za-2020-god. Accessed 12 Jan 2020.
10. Kazarin O.V.,Tarasov A.A. (2013). Modern Concepts of Cybersecurity of the Leading Foreign Countries. Vestnik of the Russian State Humanitarian University 14: 58-74.
11. Cybersecurity in a Sector of Bank and Finance Services - Threats loT, Potential Decisions and Blockchain (2019). https://www.stoodnt.com/ Accessed 12 Jan 2022.
12. Positive Technologies: итоги 2021 года в кибербезопасности и какие вызовы принесет 2022-й. https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-itogi-2021-goda-v-kiberbezopasnosti-i-kakie-vyzovy-prineset-2022-j/. Accessed 26 Jan 2022.
13. Li Y, Cao Y., Qiu H., Gao L, Du Z. and Chen S (2016) Big wave of the intelligent connected vehicles China Communications 13(2): 27-41.
14. Luo Q (2018) Wireless telematics systems in emerging intelligent and connected vehicles: threats and solutions IEEE Wirel. Commun. 25(6): 113-119.
15. Lonsdale MDS, Lonsdale D, Lim HW (2019) The impact of delivering online information neglecting user-centered information design principles. cyber security awareness websites as a case study Inf. Des. J. 24(2): 3-41.
16. Markov AS, Tsirlov VL (2007) Risks Management - Regulatory Vacuum of Information Security. Open Systems. CUBD 8:63-67
17. Magomedov SG, Kolyasnikov PV, Nikulchev EV (2020) Development of technology for controlling access to digital portals and platforms based on estimates of user reaction time built into the interface Russian Technological Journal 8(6): 34-46. (In Russ.) https://doi.org/10.32362/2500-316X-2020-8-6-34-46.
18. Burlakov VV, Skubriy EV, Orlova LN, Fedotova GV, Sukhinin AV (2021) Cyber Security in the Era of COVID-19 // Threats to Digital Platforms Stability and Cyber Hygiene Rules Studies in Systems Decision and Controlthis link is disabled: 1565–1574.
19. Nenovsky N, Chobanov P (2021) Digital currency Vs the crypto Bloomberg Businessweek bg July: 44-53.
20. Recommendations in the Field of Standartization of the Bank of Russia. Ensuring Information Security of the Bank Shoulders//https System Organizations of the Russian Federation (2014). https://cbr.ru/statichtml/file/59420/rs-25-14.pdf. Accessed 28 Jan 2022.
21. Sadek A (2016) Special issue on cyber transportation systems and connected vehicle research J. Intell. Transp. Syst 20(1): 1-3.
22. Selivanov S.A., Ogarok A.L. (2020) Ensuring Cybersecurity of Complex Information and Management Systems. Informatization and Communication 1: 28-33.
23. Sizov VA, Kirov AD (2021) The development of models of an analytical data processing system for monitoring information security of an informatization object using cloud infrastructure Russian Technological Journal 9(6): 16-25. (In Russ.) https://doi.org/10.32362/2500-316X-2021-9-6-16-25.
24. Starovoiytov A.V. Cybersecurity as an Actual Problem of the Modernity. Informatization and Communication 6: 4-7.
25. Thakor, Anjan V (2019) Fintech and banking: What do we know? Journal of Financial Intermediation 41: 100833.
26. Truntsevskij Y.V. (2020). Modern Challenges of Bank Fraud to Financial Support for e-commerce. Banking Law 6:28-36.
27. Sheremet I.A. Information and Cybersecurity: Interview (2013). htto:// echo.msk.ru/programs/arsenal/1208183-echo/. Accessed 22 jan 2022.
28. Shtitilis D., Klishkauskas V. (2013). Specific Features of Cybersecurity Legal Regulation in National Laws of Lithuania, Russia and the Usa: Cybersecurity Strategies. Problems of Russian and International Law 7-8: 80-100.
29. Walls A, Perkins E, Weiss J Definition: Cybersecurity. Gartner. 2013. ID:G00252816. 4 p.
30. Zlateva D, Stavrova E, Vladov R (2017) Digital Bank Marketing in the Context of the Circular Economy International Journal for Science and Arts 1(1): 31-38.
31. Zaytsev A, Dmitriev N, Fayzullin R, Mihel E (2021) Formation of Investment Behavior Strategy using the Game-theoretic Method TEM Journal 10(2): 673-681.

Fedotova G. V. Doctor of Economics, Associate Professor, Federal Research Center, "Computer Sciences and Control" RAS, Russia (Moscow), 9 Prosp. 60—Letia Oktyabrya, Moscow, 117312, Russia, evgeeva@mail.rui

Orlova E. R. Doctor of Economics, Professor, Head of Department, Federal Research Center "Computer Sciences and Control" RAS, Russia (Moscow), 9 Prosp. 60—Letia Oktyabrya, Moscow, 117312, Russia, orlova@isa.ru

Bocharova I. E. Engineer-Researcher, Federal Research Center "Computer Sciences and Control" RAS, Russia (Moscow), 9 Prosp. 60—Letia Oktyabrya, Moscow, 117312, Russia, irisha.maka@yandex.ru