

ПОВЫШЕНИЕ КИБЕРУСТОЙЧИВОСТИ КРЕДИТНОЙ ОРГАНИЗАЦИИ В УСЛОВИЯХ «ИНДУСТРИИ 4.0»*

Гилян Васильевна ФЕДОТОВА ^{a,*}, Денис Дмитриевич ТКАЧЕНКО ^b

^a доктор экономических наук, профессор кафедры менеджмента
и финансов производственных систем,
Волгоградский государственный технический университет (ВолгГТУ),
Волгоград, Российская Федерация
g_evgeeva@mail.ru
<https://orcid.org/0000-0002-2066-8628>
SPIN-код: 2353-5794

^b доктор экономических наук, профессор кафедры финансов и бухгалтерского учета,
Волжский институт экономики, педагогики и права (ВИЭПП),
Волжский, Российская Федерация
TkachenkoDD@rambler.ru
<https://orcid.org/0000-0002-2865-4220>
SPIN-код: 9262-1950

* Ответственный автор

История статьи:

Рег. № 208/2020
Получена 13.04.2020
Получена в доработанном
виде 30.04.2020
Одобрена 16.05.2020
Доступна онлайн
16.06.2020

УДК 336.71

JEL: G21, G24, G28, O32

Ключевые слова:

кредитные организации,
киберустойчивость,
умные технологии,
цифровизация,
Индустрия 4.0

Аннотация

Предмет. Моделирование инструментов превентивной защиты информационных систем и оценка их киберустойчивости.

Цели. Оценка сложившихся угроз и определение направлений развития процессов информатизации в кредитной сфере.

Методология. В работе использованы методы нормативно-правового анализа и оценки современной ситуации в сфере государственного управления кибербезопасностью в финансово-кредитном секторе экономики. Для оценки сложившейся ситуации и подведения итогов работы отрасли за последние годы был проведен контент-анализ статистики взломов и утечек различного рода информации. Цифровые данные получены из открытых источников в Интернете, обработаны методами финансового, графического, трендового анализа, формализованы и систематизированы.

Результаты. Определены новые тренды развития финансово-кредитной сферы и усложнения систем повышения информационной безопасности. Показано, что предлагаемая Банком России процедура внедрения умных технологий в операционные процессы кредитных организаций позволит усилить кибербезопасность банковских систем.

Область применения. Результаты исследования могут быть использованы для определения стратегических ориентиров для развития банковской сферы в условиях информационного общества.

Выводы. Информатизация всех банковских операционных систем, усложнение процедур и протоколов работы требуют внедрения новых мощных ресурсов в финансовые технологии. Усиление кибербезопасности должно стать одним из основных трендов развития финансово-кредитной сферы на ближайшее будущее.

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2020

Для цитирования: Федотова Г.В., Ткаченко Д.Д. Повышение киберустойчивости кредитной организации в условиях «Индустрии 4.0» // Национальные интересы: приоритеты и безопасность. – 2020. – Т. 16, № 6. – С. 998 – 1012.
<https://doi.org/10.24891/ni.16.6.998>

Цифровой переход на онлайн-обслуживание и фактически полную автоматизацию многих транзакций повлек за собой появление ряда новых угроз, связанных с необходимостью усиления защиты информационных ресурсов банков, в том числе сведений о клиентах, о клиентских счетах и доступа к ним.

Актуальность настоящего исследования заключается в важности оценки происходящих сегодня трансформационных изменений в системе финансового обслуживания клиентов кредитных организаций. Участвовавшие кибератаки мошенников на информационные банковские системы и онлайн платежные сервисы заставляют искать новые решения для защиты данных и клиентских счетов. Возрастающая роль и популярность «умных» технологий позволяет на их основе моделировать инструменты превентивной защиты информационных систем и отслеживать их киберустойчивость.

Впервые термин «киберустойчивость» был использован в 2014 г. в отчете Bank for International Settlements (BIS) *CPMI – Cyber Resilience in Financial Market Infrastructures*. В данном документе было дано определение киберустойчивости как возможности предчувствовать кибератаки, адаптироваться к ним и быстро восстанавливаться после вызванных ими нарушений [1].

Киберустойчивость кредитной организации – это не только способность противостоять атакам злоумышленников, но и возможность просчитывать и прогнозировать возможные взломы систем, после чего быстро восстанавливать их работоспособность. Высокая киберустойчивость банка позволяет ему максимально эффективно и без перебоев работать с ресурсами, обеспечивать полную защиту личной информации своих клиентов и контрагентов, поддерживать высокую ликвидность и мобильность ответов на кредитные запросы. Статистика утечек информации за последние 10 лет демонстрирует рост зарегистрированных случаев (рис. 1).

Представленная на рис. 1 динамика утечки данных имеет устойчивую тенденцию к росту числа взломов систем. Так, только за I полугодие 2019 г. было зарегистрировано 1 276 ед. утечек информации, что на 22,8% выше, чем за весь 2018 г. Данные факты заставляют пересмотреть концепцию обеспечения информационной защиты собственных систем, искать новые инструменты и механизмы на смену неэффективным способам защиты [2, 3]. Под утечками информации мы понимаем незаконное завладение не только финансовой информацией, но и любой информацией личного характера, способной нанести вред репутации и личности гражданина.

Проанализируем статистику наиболее проблемных отраслей экономики, в которых происходит утечка.

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-010-00103 А.

Согласно данным, представленным на *рис. 2*, в 2019 г. больше всего фактов утечки данных наблюдалось в отраслях «Высокие технологии» (65%) и «Банки и финансы» (58,1%). Видно, что основными целями атак мошенников являются три отрасли: 1) высокие технологии; 2) торговля и HoReCa (гостинично-ресторанный бизнес); 3) банки и финансы. Повторяющиеся хакерские атаки и взломы, факты утечки различного рода информации заставляют кредитные организации усиливать меры по обеспечению сохранности внутренней информации. Государство также старается отслеживать и контролировать ситуацию.

В практике многих стран сложились и давно применяются два основных подхода к обеспечению кибербезопасности экономических систем:

- 1) *планируемая киберустойчивость*, основанная на формировании запасов и резервов ресурсов для быстрого реагирования, и исправления последствий кибератак;
- 2) *адаптивная киберустойчивость*, когда компания осуществляет инвестирование в человеческие ресурсы, которые в любой момент опасности позволят быстро среагировать и найти решение.

Россия в настоящее время не придерживается преимущественно какого-либо определенного подхода, на практике используются их комбинации. Так, осуществляется инвестирование в повышение информационной грамотности персонала, формируются резервы для финансирования последствий кибератак. Тем не менее регулирующие структуры стараются предотвратить возможные атаки хакеров, поэтому регулярно проводят проверки состояния систем кибербезопасности кредитных организаций [4, 5].

Так, в 2019 г. Банк России провел 109 проверок кредитных организаций на предмет их киберустойчивости, вследствие которых было установлено 730 нарушений безопасности банковских систем. По результатам проверок были применены санкции по отношению к нарушителям, а также составлен доклад «Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 гг.». Основная цель доклада – актуализация «умных технологий» (AI, Big Data, IoT) в кредитно-финансовой сфере.

Умные технологии сегодня выступают основой информационных коммуникаций в развитых странах. Их широкое применение во всех сферах экономики и управления позволяет интенсифицировать и максимизировать процессы производства и технологического прорыва. Переход на информационные платформы влечет за собой ряд глобальных угроз, которые могут внести дисбаланс в работу цифровых платформ, так как нарушают их целостность и не дают полной защиты пользователям. В связи с этим возникает потребность усиления традиционных инструментов защиты баз данных посредством внедрения умных технологий.

К настоящему времени уже накоплен определенный опыт исследований умных технологий в различных отраслях народного хозяйства, определены горизонты их возможностей, выявлен огромный потенциал применения в процессе противодействия угрозам.

В свою очередь, киберустойчивость кредитной организации представляет собой комплексную защиту всей информационной архитектуры финансово-кредитной сферы, и прежде всего – регулирующих эту сферу структур. Противостояние кибератакам и успешное их прогнозирование, оперативное возобновление деятельности в течении 1–2 часов после взломов – все это будет характеризовать кредитное учреждение как устойчивое и надежное звено финансовой инфраструктуры [6].

Финансовый сектор постоянно испытывает давление мошенников в результате массовых рассылок электронных писем с вредоносными программами, мошеннических SMS-сообщений. В последнее время злоумышленники стараются использовать так называемые «умные вещи» в качестве криминальных инструментов, что заставляет усиливать взаимодействия финансовых организаций и соответствующих служб Минкомсвязи России.

В последние годы рост количества кибератак, прежде всего в финансовом секторе, вызывает обеспокоенность международного сообщества. Так, в отчете Всемирного экономического форума 2018 г. кибератаки названы глобальным технологическим риском. Наиболее популярные виды и суммы хищений за последние два года представлены в *табл. 1*.

Из данных *табл. 1* можно заключить, что кибермошенничества направлены в первую очередь на хищения небольших сумм со счетов физических лиц с использованием так называемых «троянов» – целевых вредоносных программ (более 109,5 млн руб.). В мире существуют целые группы преступных сообществ, специализирующихся на определенных видах кибермошенничества. К ним можно отнести «русскаяязычную тройку» – Cobalt, Silence и MoneyTaker, а также северо-корейскую Lazarus и группу SilentCards из Кении. При этом помимо указанных групп постоянно появляются все новые организации, специализирующиеся на кибермошенничестве. В последние годы выросло количество преступлений с применением социальной инженерии и телефонного мошенничества [7].

Мировое сообщество отмечает, что рост потерь прибыли от кибератак, периодически повторяющиеся сбои в функционировании мировых финансовых рынков, массовые утечки информации из засекреченных баз данных – все это становится мировым трендом на фоне развития цифровых технологий. Появление новых видов преступлений и новых инструментов требует от финансового регулятора постоянного мониторинга и гибкости в предотвращении взломов систем, оперативного внедрения превентивных технологий в работу систем защиты.

Банк России регулярно отслеживает объемы несанкционированных операций со счетов юридических лиц в кредитных организациях, объемы несанкционированных операций с использованием платежных карт, выпущенных российскими банками (*рис. 3*).

Статистика, представленная Департаментом информационной безопасности Банка России, демонстрирует снижение объемов несанкционированных операций по счетам юридических лиц, в то время как суммы незаконных операций с

платежными картами российских банков в 2018 г. выросли. Необходимо обратить внимание на данную тенденцию и принять соответствующие меры.

Согласно докладу Банка России о направлениях развития кредитно-финансовой сферы до 2021 г., были выделены следующие направления обеспечения киберустойчивости отрасли:

- контроль и мониторинг показателей информационных угроз и рисков;
- контроль уровня несанкционированных банковских финансовых операций;
- оперативная реакция на компьютерные атаки;
- максимальная защита потребительских прав;
- стандартизация в области обеспечения информационной безопасности и киберустойчивости;
- осуществление межведомственного взаимодействия по вопросам безопасности;
- отслеживание деятельности нелегальных участников финансового рынка;
- формирование культуры информационной безопасности в обществе.

Остановимся более подробно на некоторых мерах. Сегодня большое внимание уделяется превентивным мерам обеспечения киберустойчивости. Таким инструментом предупреждения несанкционированных операций со счетами клиентов служит прототип автоматизированной системы (АС) «Фид-Антифрод», направленный на сбор данных и быстрый обмен протоколами о правомерности операций без согласия клиента (*рис. 4*).

На *рис. 5* представлена информация о количестве сообщений о несанкционированных операциях, переданных Антифродом в ФинЦЕРТ. Автоматизированная система аккумулирует следующие данные: номера паспортов клиентов и других получателей средств в хешированном виде по всем проведенным банковским операциям, которые проводились без согласия владельца счета; данные в виде хэша по номерам СНИЛС всех, кто получал средства без согласия владельцев счетов; список номеров ИНН получателей денег со счетов без согласия владельцев; список счетов получателей и БИКов кредитных организаций; списки номеров банковских карт, номеров телефонов, номеров электронных кошельков, участвовавших в банковских операциях без согласия владельца счета [8].

Согласно определению Всемирного банка, экономика знаний базируется на четырех основных блоках, определяющих платформу данной модели: институциональная структура, инновационная система, образование, информационная инфраструктура.

В основу работы антифрода заложен принцип машинного обучения, а человеческий фактор в его функционале практически отсутствует. В данном случае использование элементов AI поддерживает взаимодействие операционного центра со всеми счетами клиентов, что позволяет мгновенно производить анализ и информирование соответствующих служб. Можно сказать, что работа антифродов

основана на методологии BigData. Алгоритм работы антифрода в кредитных учреждениях достаточно сложен – он мгновенно запускается и срабатывает при малейших случаях нетипичных банковских операций. Причем это не просто защита банковских операционных и дистанционных систем обслуживания, а самый сложный процесс обработки огромного массива данных и принятия решений по ним [9–11].

Информационная безопасность связана с обменом данными между всеми участниками, формирующими уровень киберустойчивости организаций финансового сектора. В рамках финансово-кредитной сферы работает автоматизированная система обработки инцидентов Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (АСОИ ФинЦЕРТ), специальное структурное подразделение Банка России, к которой в настоящий момент подключены все банки Российской Федерации, а также другие финансовые структуры и органы управления. Состав участников АСОИ ФинЦЕРТ представлен на рис. 6.

Система обмена данными АСОИ ФинЦЕРТ включает в себя около 826 участников – компаний различной сферы деятельности. Основную долю участников составляют кредитные организации (415 ед.) и субъекты страхового рынка (81 ед.). Также в состав участников входят IT-компании, операторы связи, государственные органы и т.п.

Помимо внутривостранового обмена данными необходимо налаживать международное сотрудничество с кредитными организациями иностранных государств. Фактически к АСОИ ФинЦЕРТ уже подключены четыре национальных банка стран – членов ЕАЭС. Заключенные соглашения позволят сформировать единое киберустойчивое информационное пространство в финансовой сфере, которое, в свою очередь, потребует поиска механизмов для прогноза и минимизации рисков последствий кибератак [12, 13].

В заключение отметим, что набирающая размах цифровизация уже не может остановиться, поэтому процессы формирования огромных баз данных требуют внимательного отношения к их безопасности. Созданные информационные платформы, сервисы, программы должны не просто работать, но будут постоянно усложняться, модернизироваться, повышать свою киберустойчивость. Постоянные и все учащающиеся кибератаки на ресурсы финансово-кредитного сектора заставляют искать новые подходы и инструменты для укрепления киберустойчивости кредитных организаций. Появившиеся тенденции использовать «умные вещи» в криминальном бизнесе требуют внедрения не менее умных технологий для разработки решений по укреплению безопасности информационных систем и защиты информации о клиентах в кредитных организациях. Именно поэтому Банк России обязывает кредитные организации неуклонно повышать свою киберустойчивость, инвестируя в разработку новых технологий в условиях Индустрии 4.0.

Таблица 1

Статистика наиболее популярных кибератак на финансово-кредитный сектор за 2-е полугодие 2018 г. – 1-е полугодие 2019 г.

Table 1

Statistics on the most popular cyberattacks against the financial and credit sector from H2 2018 through H1 2019

Вид мошенничества	Кол-во групп	Число успешных атак	Средняя сумма одного хищения, руб.	Средняя сумма хищений за год, руб.	Общая сумма хищений за указанный период, руб.
Хищения у юридических лиц с «троянами» для ПК	2	1	500 000	250 000	62 250 000
Хищения у физических лиц с «троянами» для ОС Android	5	40	11 000	440 000	109 560 000
Целевые атаки на банки	3	...	31 000 000	...	93 000 000
Фишинг (подмена страниц сайтов)	11	435	800	348 000	86 652 000
Обналичивание похищенных средств	...	...	...	467 100	158 157 900

Источник: Вся статистика Интернета на 2019 г. в мире и в России.

URL: <https://web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/>

Source: All Internet statistics for 2019 in the world and in Russia.

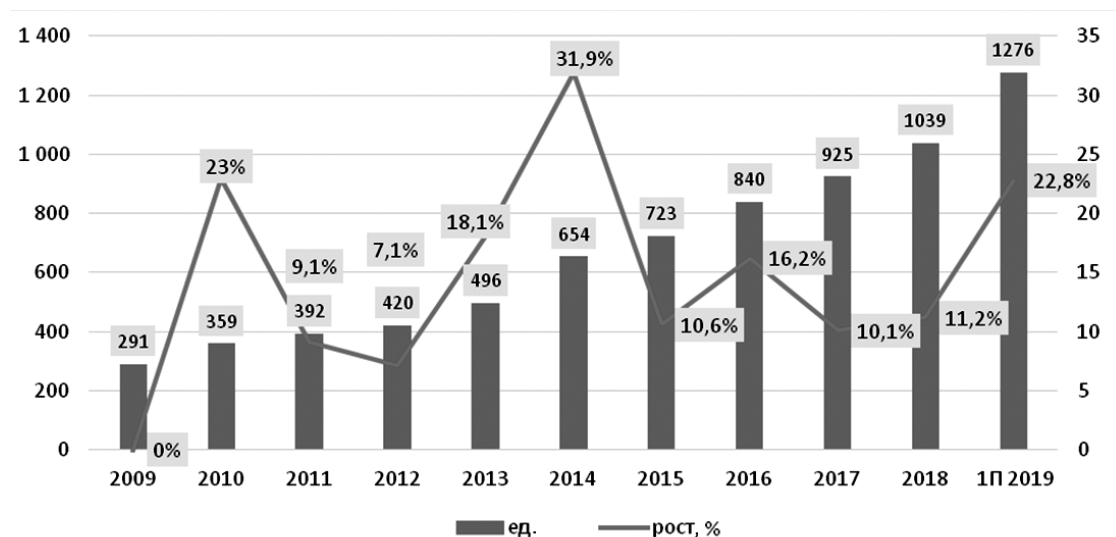
URL: <https://web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/> (In Russ.)

Рисунок 1

Количество утечек информации в 2009–2019 гг.

Figure 1

The number of instances of data leakage, 2009–2019

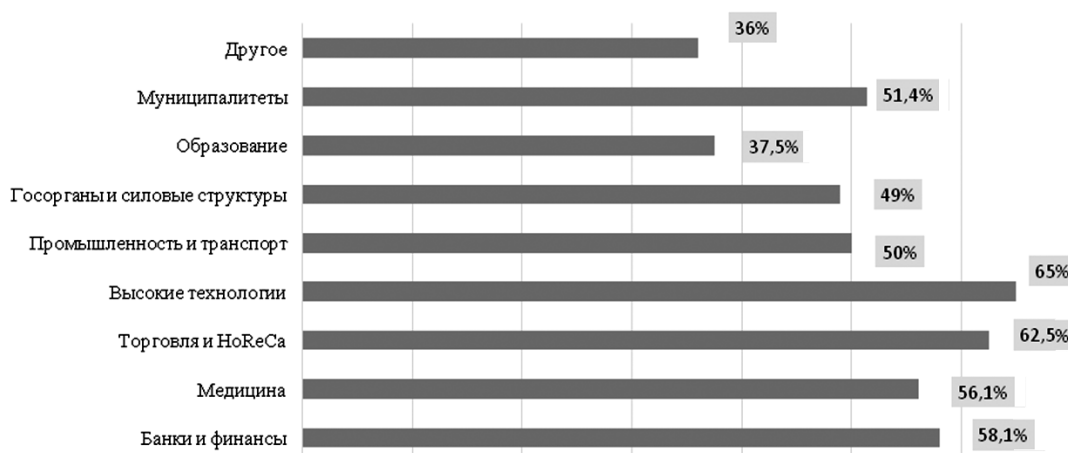


Источник: Аналитический центр InfoWatch.

URL: https://infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf

Source: The Analytics Center of InfoWatch.

URL: https://infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf (In Russ.)

Рисунок 2**Отраслевая статистика утечек информации, %****Figure 2****Data leakage statistics by industry, percentage***Источник:* Аналитический центр InfoWatch.URL: [https://infowatch.ru/sites/default/files/report/analytics/russ/](https://infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf)

Global_Data_Leaks_Report_2019_half_year.pdf

Source: The Analytics Center of InfoWatch.URL: [https://infowatch.ru/sites/default/files/report/analytics/russ/](https://infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf)

Global_Data_Leaks_Report_2019_half_year.pdf (In Russ.)

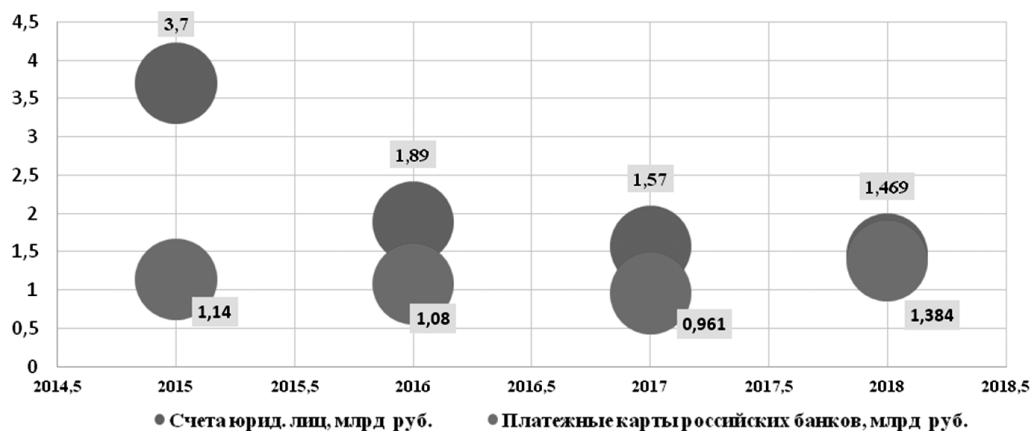
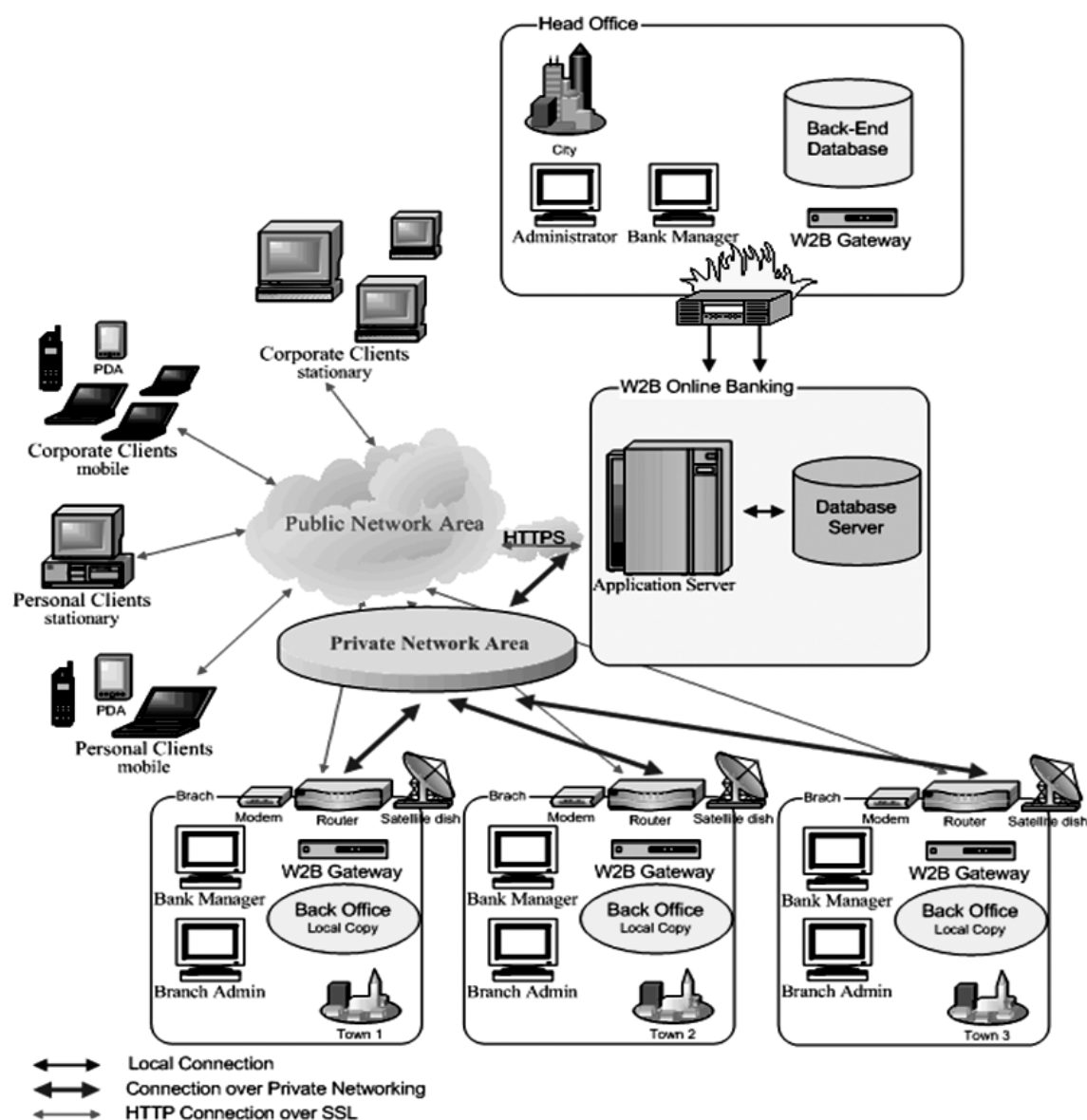
Рисунок 3**Объемы несанкционированных операций, зарегистрированных ЦБ РФ в 2014–2018 гг., млрд руб.****Figure 3****Volumes of unauthorized operations recorded by the Central Bank of the Russian Federation, 2014–2018, billion RUB***Источник:* ЦБ РФ усилит надзор над киберустойчивостью банков.URL: <https://ren.tv/news/ekonomika/475891-tsb-rf-usilit-nadzor-nad-kiberustoichivostiu-bankov>*Source:* The Central Bank of the Russian Federation will strengthen supervision over the cyber resilience of banks. URL: <https://ren.tv/news/ekonomika/475891-tsb-rf-usilit-nadzor-nad-kiberustoichivostiu-bankov> (In Russ.)

Рисунок 4

Схема работы антифрода в кредитных организациях

Figure 4

The fraud detection scheme in credit institutions



Источник: Как выбрать антифрод-систему для банка? URL: <http://tadviser.ru/index.php>

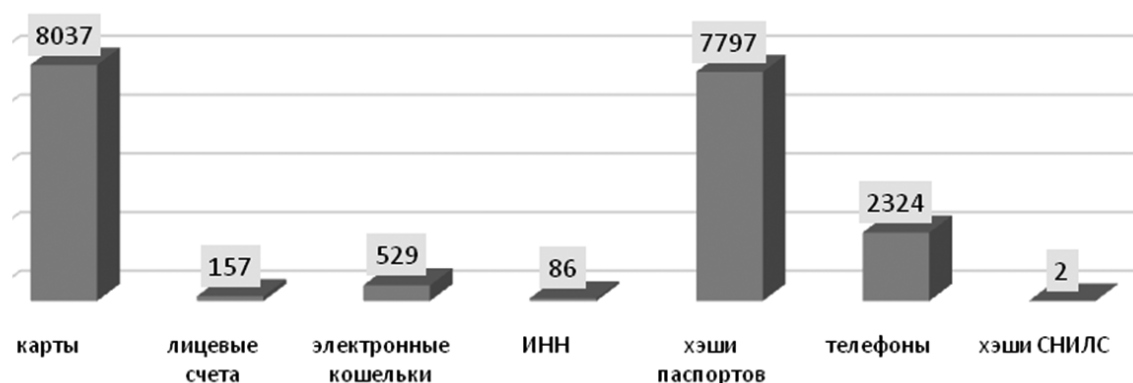
Source: How to choose an antifraud system for a bank? URL: <http://tadviser.ru/index.php> (In Russ.)

Рисунок 5

Количество сообщений о признаках несанкционированных операций, переданных на 31.08.2019

Figure 5

The number of reports on attributes of unauthorized operations delivered as of August 31, 2019



Источник: ЦБ РФ усилит надзор над киберустойчивостью банков.

URL: <https://ren.tv/news/ekonomika/475891-tsb-rf-usilit-nadzor-nad-kiberustoichivostiu-bankov>

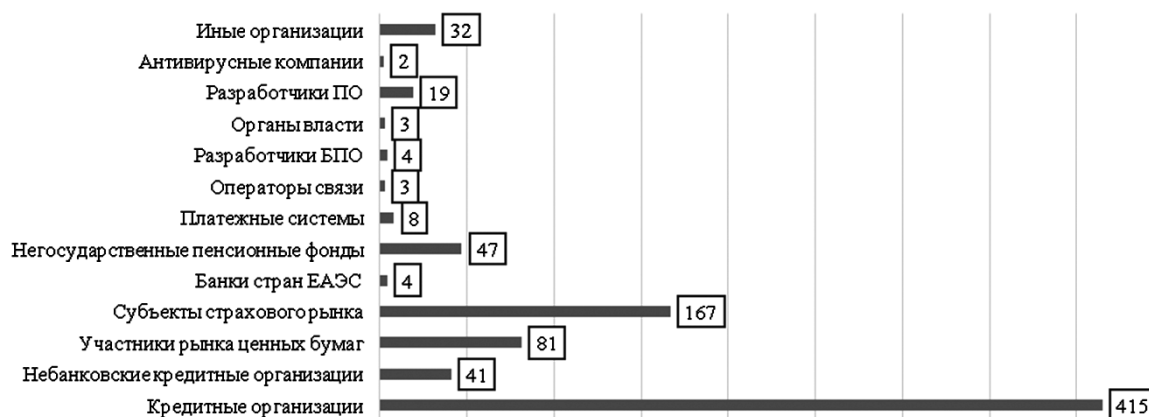
Source: The Central Bank of the Russian Federation will strengthen supervision over the cyber resistance of banks. URL: <https://ren.tv/news/ekonomika/475891-tsb-rf-usilit-nadzor-nad-kiberustoichivostiu-bankov> (In Russ.)

Рисунок 6

Состав участников АСОИ ФинЦЕРТ

Figure 6

The composition of parties to the Automated System for Incident Processing FinTsERT



Источник: Аналитический центр InfoWatch.

URL: https://infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf

Source: The Analytics Center of InfoWatch.

URL: https://infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf (In Russ.)

Список литературы

1. Dudin M.N., Lyasnikov N.V., Reshetov K.Yu. et al. Economic Profit as Indicator of Food Retailing Enterprises Performance. *European Research Studies Journal*, 2018, vol. 21, no. 1, pp. 468–479.
2. Gordin M.D. Scientific Babel: The Language of Science from the Fall of Latin to the Rise of English. London, Profile Books, 2015.
3. Fedotova G.V., Chugumbaev R.R., Chugumbaeva N.N. et al. Increase of Economic Security of Internet Systems of Credit Organizations. In: Popkova E. (ed.) *The Future of the Global Financial System: Downfall or Harmony*. ISC 2018. Lecture Notes in Networks and Systems. Vol. 57. Springer, 2018, pp. 922–931.
URL: https://doi.org/10.1007/978-3-030-00102-5_98
4. Kharitonov A.S. The Evolution of the Administrative-Legal Mechanism of Management of National Projects and State Programs. *State Administration*, 2011, no. 26.
5. Korolev L.N. Evolutional Computations, Neuronet, Genetic Algorithms – Formal Statements. *Journal of Mathematical Sciences*, 2010, vol. 168, iss. 1, pp. 80–88.
URL: <https://doi.org/10.1007/s10958-010-9976-z>
6. Мизюн В.А. Интеллектуальные методы управления предприятием. СПб.: Изд-во Санкт-Петербургской академии управления и экономики, 2008. 288 с.
7. Marsden T., Sonnino R. Rural Development and the Regional State: Denying Multifunctional Agriculture in the UK. *Journal of Rural Studies*, 2008, vol. 24, iss. 4, pp. 422–431. URL: <https://doi.org/10.1016/j.jrurstud.2008.04.001>
8. Cheyns E., Daviron B., Djama M. et al. The Standardization of Sustainable Development Through the Insertion of Agricultural Global Value Chains into International Markets. In: *Sustainable Development and Tropical Agri-chains*. Dordrecht, Springer, 2017, pp. 283–303.
9. Giannakis E., Bruggeman A. The Highly Variable Economic Performance of European Agriculture. *Land Use Policy*, 2015, vol. 45, pp. 26–35.
URL: <https://doi.org/10.1016/j.landusepol.2014.12.009>
10. Визильтер Ю.В., Желтов С.Ю., Князев В.А. и др. Обработка и анализ цифровых изображений с примерами на LabVIEW и IMAQ Vision. М.: ДМК Пресс, 2016. 464 с.
11. Шапиро Л., Стокман Дж. Компьютерное зрение. М.: Бином. Лаборатория знаний, 2006. 752 с.
12. Popkova E.G., Popova E.V., Sergi B.S. Clusters and Innovational Networks Toward Sustainable Growth. In: Sergi B.S. (Ed.) *Exploring the Future of Russia's Economy*

and Markets: Towards Sustainable Economic Development. Bingley, UK, Emerald Publishing, 2018, pp. 107–124.

13. *Sukhodolov A.P., Popkova E.G., Kuzlaeva I.M.* Methodological Aspects of Study of Internet Economy. In: *Internet Economy vs Classic Economy: Struggle of Contradictions*. Studies in Computational Intelligence, vol. 714, Springer, Cham, 2018, pp. 53–61. URL: https://doi.org/10.1007/978-3-319-60273-8_5

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

pISSN 2073-2872
eISSN 2311-875X

National Interests

REINFORCING THE CYBER RESILIENCE OF A CREDIT INSTITUTION IN INDUSTRY 4.0

Gilyan V. FEDOTOVA ^{a,*}, Denis D. TKACHENKO ^b

^a Volgograd State Technical University (VSTU),
Volgograd, Russian Federation
g_evgeeva@mail.ru
<https://orcid.org/0000-0002-2066-8628>

^b Volzhsky Institute of Economics, Pedagogics and Law,
Volzhsky, Volgograd Oblast, Russian Federation
TkachenkoDD@rambler.ru
<https://orcid.org/0000-0002-2865-4220>

* Corresponding author

Article history:

Article No. 208/2020
Received 13 April 2020
Received in revised form
30 April 2020
Accepted 16 May 2020
Available online
16 June 2020

JEL classification: G21,
G24, G28, O32

Keywords:

credit
institution, cyber resilience,
smart technology,
digitalization, Industry 4.0

Abstract

Subject. The article discusses the modeling of preventive protection of IT systems and evaluates their cyber resilience.

Objectives. The study evaluates the existing threats and determines how informatization processes may unfold in the credit segment.

Methods. Research is based on methods of regulatory and legislative analysis. We evaluate today's public administration of cybersecurity in the financial and credit sector. To give a view of the existing situation and sum up the sector's performance for the recent years, we performed the content analysis of statistics on data hacking and leakages.

Results. The article highlights new trends in the financial and credit sector and the growing complexity of data security systems. As proposed by the Bank of Russia, the integration of smart technologies is showed to reinforce the cybersecurity of banking systems.

Conclusions and Relevance. The informatization of all banking operation systems, growing complexity of procedures and work logs require new robust resources to be integrated into financial technologies. Stronger cybersecurity should lay a trend in the financial and credit sector in the nearest future. The findings can be used to flag strategic milestones of the banking development in the information-driven society.

© Publishing house FINANCE and CREDIT, 2020

Please cite this article as: Fedotova G.V., Tkachenko D.D. Reinforcing the Cyber Resilience of a Credit Institution in Industry 4.0. *National Interests: Priorities and Security*, 2020, vol. 16, iss. 6, pp. 998–1012. <https://doi.org/10.24891/ni.16.6.998>

Acknowledgments

The study was supported by the Russian Foundation for Basic Research (RFBR) as part of scientific project № 18-010-00103 A.

References

1. Dudin M.N., Lyasnikov N.V., Reshetov K.Yu. et al. Economic Profit as Indicator of Food Retailing Enterprises Performance. *European Research Studies Journal*, 2018, vol. 21, no. 1, pp. 468–479.
2. Gordin M.D. *Scientific Babel: The Language of Science from the Fall of Latin to the Rise of English*. London, Profile Books, 2015.
3. Fedotova G.V., Chugumbaev R.R., Chugumbaeva N.N. et al. Increase of Economic Security of Internet Systems of Credit Organizations. In: Popkova E. (ed.) *The Future of the Global Financial System: Downfall or Harmony*. ISC 2018. *Lecture Notes in Networks and Systems*, vol 57. Springer, 2018, pp. 922–931.
URL: https://doi.org/10.1007/978-3-030-00102-5_98
4. Kharitonov A.S. The Evolution of the Administrative-Legal Mechanism of Management of National Projects and State Programs. *State Administration*, 2011, no. 26.
5. Korolev L.N. Evolutional Computations and Neuronet and Genetic Algorithms – Formal Statements. *Journal of Mathematical Sciences*, 2010, vol. 168, iss. 1, pp. 80–88. URL: <https://doi.org/10.1007/s10958-010-9976-z>
6. Mizyun V.A. *Intellectual'nye metody upravleniya predpriyatiem* [Intellectual methods of corporate governance]. St. Petersburg, St. Petersburg Academy of Management and Economics Publ., 2008, 228 p.
7. Marsden T., Sonnino R. Rural Development and the Regional State: Denying Multifunctional Agriculture in the UK. *Journal of Rural Studies*, 2008, vol. 24, iss. 4, pp. 422–431. URL: <https://doi.org/10.1016/j.jrurstud.2008.04.001>
8. Cheyns E., Daviron B., Djama M. et al. The Standardization of Sustainable Development through the Insertion of Agricultural Global Value Chains into International Markets. In: *Sustainable Development and Tropical Agri-Chains*. Dordrecht, Springer, 2017, pp. 283–303.
9. Giannakis E., Bruggeman A. The Highly Variable Economic Performance of European Agriculture. *Land Use Policy*, 2015, vol. 45, pp. 26–35.
URL: <https://doi.org/10.1016/j.landusepol.2014.12.009>
10. Vizil'ter Yu.V., Zheltov S.Yu., Knyazev V.A. et al. *Obrabotka i analiz tsifrovyykh izobrazhenii s primerami na LabVIEW i IMAQ Vision* [Digital image processing and analysis and cases in LabVIEW and IMAQ Vision]. Moscow, DMK Press Publ., 2016, 464 p.
11. Shapiro L., Stockman G. *Komp'yuternoe zrenie* [Computer Vision]. Moscow, Binom.Laboratoriya znaniy Publ., 2006, 752 p.

12. Popkova E.G., Popova E.V., Sergi B.S. Clusters and Innovational Networks Toward Sustainable Growth. In: Sergi B.S. (Ed.) *Exploring the Future of Russia's Economy and Markets: Towards Sustainable Economic Development*. Bingley, UK, Emerald Publishing, 2018, pp. 107–124.
13. Sukhodolov A.P., Popkova E.G., Kuzlaeva I.M. Methodological Aspects of Study of Internet Economy. In: *Internet Economy vs Classic Economy: Struggle of Contradictions*. Studies in Computational Intelligence, vol. 714, Springer, Cham, 2018, pp. 53–61. URL: https://doi.org/10.1007/978-3-319-60273-8_5

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.