https://doi.org/10.31107/2075-1990-2021-3-38-53

Анализ и оценка киберугроз национальной финансовой системе России в цифровой экономике

Сергей Всеволодович Шкодинский
E-mail: sh-serg@bk.ru, ORCID: 0000-0002-5853-3585
Научно-исследовательский финансовый институт Минфина России, Москва 127006, Российская Федерация;
Институт проблем рынка РАН, Москва 117418, Российская Федерация
Михаил Николаевич Дудин
E-mail: dudinmn@mail.ru, ORCID: 0000–0001–6317–2916
Институт проблем рынка РАН, Москва 117418, Российская Федерация
Далер Ирматович Усманов
E-mail: us.dali@mail.ru, ORCID: 0000-0002-0357-1584
Институт проблем рынка РАН, Москва 117418, Российская Федерация

Аннотация
Актуальность темы научной статьи заключается в необходимости теоретической и практической проработки проблемы эскалации количества и качества киберугроз и атак, совершаемых на институты финансовой системы России, с точки зрения обеспечения безопасного и устойчивого развития. Цель статьи — комплексный анализ киберугроз, возникающих для национальной финансовой системой РФ в условиях цифровизации экономики. Предметом научного исследования выступают процессы обеспечения национальной безопасности финансовой системы России в цифровой экономике. В качестве методологической и фундаментальной основы исследования были использованы научные и практические исследования российских и зарубежных ученых в сфере кибербезопасности, цифровой экономики и государственного управления. Авторы систематизировали различные подходы к ключевым категориям: «цифровой суверенитет» и «кибервойна»; установили, что наиболее актуальными финансовыми вызовами и угрозами для цифровой экономики Российской Федерации являются: хакерские атаки, финансовые диверсии на финансовом рынке, конструирование и запуск социоинженерийных троянов, инфраструктурные атаки на IoT-сети (интернет вещей), продажа хакерских инструментов с открытым кодом; проанализировали количество и качество кибератак на отечественные финансовые институты за 2016–2020 гг.; обобщили потери, нанесенные кибератаками финансовым институтам; определили основные сценарии развития киберугроз и кибератак для национальной финансовой системы. В заключение исследования сделан вывод о том, что дальнейшая проработка вопросов обеспечения кибербезопасности финансовых институтов в цифровой экономике требует обоснования конкретных программ и мероприятий, реализуемых как коммерческими банками в рамках индивидуальных стратегий обеспечения цифровой безопасности, так и органами власти и управления с позиции обеспечения цифрового суверенитета государства.

Ключевые слова: *кибертерроризм, финансовые институты, цифровая экономика, безопасность финансовых транзакций*

JEL: *G21, G28*

Финансирование: *статья подготовлена в рамках государственного задания ИПР РАН, тема НИР «Институциональная трансформация экономической безопасности при решении социально-экономических проблем устойчивого развития национального хозяйства России».*

Для цитирования: *Шкодинский С. В., Дудин М. Н., Усманов Д. И. Анализ и оценка киберугроз национальной финансовой системе России в цифровой экономике // Финансовый журнал. 2021. Т. 13. № 3. С. 38–53. https://doi.org/10.31107/2075-1990-2021-3-38-53.*

---

https://doi.org/10.31107/2075-1990-2021-3-38-53

Analysis and Assessment of Cyberthreats to the National Financial System of Russia in the Digital Economy

Sergey V. Shkodinsky[1], ***Mihail N. Dudin***[2], ***Daler I. Usmanov***[3]
[1] *Financial Research Institute, Moscow 127006, Russian Federation*
[1, 2, 3] *Market Economy Institute, Moscow 117418, Russian Federation*
[1] *sh-serg@bk.ru, https://orcid.org/0000-0002-5853-3585*
[2] *dudinmn@mail.ru, http://orcid.org/0000-0001-6317-2916*
[3] *us.dali@mail.ru, https://orcid.org/ 0000-0002-0357-1584*

Abstract
The relevance of the topic of this scientific article lies in the need for a theoretical and practical study of the problem of escalating numbers and quality of cyber threats and attacks committed against institutions of the Russian financial system, implying their safe and sustainable development being ensured in Industry 4.0. The purpose of the article is a comprehensive analysis of cyberthreats facing the national financial system of the Russian Federation in the context of economy digitalization. The subject of scientific research is the processes of ensuring national security of the Russian Federation's financial system in the digital economy. In the process of research, the authors relied on general scientific methods (observation, comparison, measurement, analysis and synthesis, as well as logical reasoning), specific scientific methods (static analysis, expert assessments, and graphical method), and the foresight method. The validity and reliability of the results of scientific research are ensured by the correctness and rigor of the logic and research scheme construction. Scientific and practical research of Russian and foreign scientists in the field of cybersecurity, digital economy and public administration was used as a methodological and fundamental basis of the study. Various approaches to key categories—digital sovereignty and cyberwar—have been systematized, and it has been established that the most pressing financial challenges and threats to the digital economy of the Russian Federation are as follows: hacker attacks, financial sabotage in the financial market, design and launch of social engineering trojans, infrastructure attacks on IoT (Internet of Things) networks, and sale of hacker tools with open source. The authors have analyzed the number and quality of cyberattacks on domestic financial institutions in 2016–2020; summarized the losses caused by cyberattacks to financial institutions; and identified the main scenarios for the development of cyberthreats and cyberattacks for the national financial system. As the main conclusion, the authors determine that further elaboration of the issues of ensuring financial institution cybersecurity in the digital economy requires justification and implementation of specific programs and activities carried out both by commercial banks within the framework of individual strategies for ensuring digital security, and by authorities and management with positions of ensuring the digital sovereignty of the state.

Keywords: *cyberterrorism, financial institutions, digital economy, security of financial transactions*

JEL: *G21, G28*

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

For citation: *Shkodinsky S.V., Dudin M.N., Usmanov D.I. Analysis and Assessment of Cyberthreats to the National Financial System of Russia in the Digital Economy. Financial Journal, 2021, vol. 13, no. 3, pp. 38–53 (In Russ.). https://doi.org/10.31107/2075-1990-2021-3-38-53.*

ВВЕДЕНИЕ

Соперничество и борьба являются неотъемлемыми компонентами жизненного цикла социально-экономической системы, созданной человечеством. На протяжении всей истории война как высшая форма осуществления борьбы сторон за свои интересы являлась стратегическим инструментом достижения поставленных целей / разрешения противоречий между отдельными государствами или коалициями. Но с наступлением эпохи Индустрии 4.0 ее механизм и формат протекания перестали быть явными, приобретя невидимый характер. Отметим, что новый тренд на широкое применение информационных технологий в производстве обусловил наступление так называемой четвертой промышленной революции (Индустрии 4.0), под которой мы понимаем новую ступень технологического развития на основе разработки и инкорпорации в широкий гражданский оборот новейших решений, созданных с применением цифровых технологий.

Сегодня цифровая инфраструктура становится не только важнейшим ресурсом обеспечения конкурентных преимуществ национальной экономики и инструментом реализации права государства на цифровой суверенитет в мировом digital-пространстве, но и настоящей площадкой для ведения кибервойн. Такая двойственность применения новейших информационных технологий является естественным стремлением как индивида, так и государства к превосходству над другими: с помощью достижений четвертой промышленной революции наиболее развитые страны, с одной стороны, создают технологические барьеры от интервенции развивающихся стран и новых экономических гигантов Азиатского региона, а с другой — получают право осуществлять невидимый контроль и вмешательство во внутренние дела других государств через элементы цифровой инфраструктуры. При этом лучшим объектом для искусственного ослабления потенциального или реального военно-политического противника или экономического конкурента является его финансовая система.

Важно подчеркнуть, что ключевыми признаками цифровой экономики являются: 1) информационная открытость и транспарентность социально-экономических систем; 2) стремление государств к цифровой интеграции. В то же время цифровизация экономики неоднозначно воспринимается специалистами, изучающими эту сферу: с одной стороны, при росте информационной транспарентности увеличиваются риски кибератак на национальную экономику, с другой — при углублении цифровой интеграции происходит медленная, но устойчивая потеря цифрового суверенитета одной из сторон-участниц. Указанные противоречия положены в основу настоящего научного исследования, целью которого является комплексный анализ киберугроз для национальной финансовой системы РФ в условиях цифровизации экономики с учетом эскалации военно-политической и экономической напряженности в международном диалоге России с ЕС и США и сложно прогнозируемыми сценариями дальнейшего развития событий.

Основные задачи исследования: систематизация различных подходов к ключевым категориям: «цифровой суверенитет» и «кибервойна»; выявление наиболее актуальных финансовых вызовов и угроз для цифровой экономики Российской Федерации; оценка потерь, нанесенных кибератаками финансовым институтам России; определение основных сценариев развития киберугроз и кибератак для национальной финансовой системы.

ОБЗОР ЛИТЕРАТУРЫ И ИССЛЕДОВАНИЙ

Принято считать, что генезис формирования цифровой экономики как новой модели устройства социально-экономических систем восходит к научным исследованиям американского информатика Н. Негропонте, который в 1995 г. обосновал идею о грядущем наступлении точки невозврата, обусловленной стремительным распространением

информационных технологий во всех сферах жизни человека и общества. Он ввел в оборот такие термины, как «цифровые телекоммуникации», «цифровая планета», «цифровые технологии» и др. [Negroponte N., 1995, p. 4, 5, 11]. Однако вплоть до 2011 г. его идеи считались менеджментом бизнеса и государственными институтами футуристичными.

Изучение цифровой экономики как инструмента военно-политического влияния относится к научным работам Дж. Вестермана и В. Дхара[1], которые развили классические работы специалистов в области кибербезопасности конца 90-х гг. XX в. — нач. XXI в.: Дж. Перритта [Perritt J., 1998], Дж. Раухофера, Ц. Бовдена [Rauhofer J., Bowden C., 2013] и ввели в научный оборот понятие «цифровой суверенитет» как меру самостоятельности выражения и осуществления интересов государства в мировом цифровом пространстве и как оценочный показатель устойчивости национальной цифровой инфраструктуры перед возможными внутренними и внешними киберугрозами и хакерскими атаками.

Систематизированное и глубокое исследование киберугроз и кибервойны как неотъемлемых частей новой реальности, сформированной результатами Индустрии 4.0, опубликовано американскими учеными П. Зингером и А. Фридманом в книге «Кибербезопасность и кибервойна: что каждый должен знать» [Singer P., Friedman A., 2014, p. 49].

В российской практике рассмотрение вопросов кибербезопасности применительно к цифровой экономике относят к профессиональным исследованиям экспертов в сфере корпоративной информационной защиты Н. Н. Федотова и И. С. Ашманова, чей вклад преимущественно носит практико-ориентированный характер и нацелен на обеспечение безопасности акторов в цифровом пространстве [Бухарин В. В., 2016, с. 87].

Обзор научно-теоретических и прикладных публикаций позволил установить, что ни в зарубежном, ни в отечественном научном обороте не содержится унифицированного определения таких ключевых понятий, как «цифровой суверенитет» и «кибервойна». Это, на наш взгляд, объясняется, с одной стороны, различием уровня цифровой зрелости государств, а с другой — дифференцированностью целей и задач ключевых акторов цифровой экономики: высокотехнологичных корпораций и государственных институтов национальной безопасности. Кроме этого, существуют противоречивые точки зрения о корректности использования понятия «кибервойна» в качестве научного термина. Так, по мнению Н. А. Чернышенко, это понятие отражает масштабное вмешательство представителей одного государства в интересы другого, причем стороны могут быть достаточно точно идентифицированы. Кроме того, должны присутствовать весомые основания для начала военных действий, поэтому более корректным считается применение термина «кибертерроризм» [Чернышенко Н. А., 2015, с. 38–39; Бегларян М. Е. и др., 2020] (табл. 1).

Таблица 1

Определение понятия «кибертерроризм» («кибервойна») в отечественной и зарубежной литературе / Definition of the cyberterrorism (cyberwar) concept in native and foreign literature

Авторы и источники	Содержание определения понятия
I. Зарубежные авторы	
R. A. Clarke, R. K. Knake [Clarke R. A.; Knake R. K., 2010, p. 55]	*Кибертерроризм* — анонимное несанкционированное проникновение в частную или публичную (государственную) информационную инфраструктуру с целью нанесения какого-либо ущерба или ее разрушения. *Кибервойна* — осуществление санкционированных государственным институтом управления действий по вмешательству в деятельность другого государства через инструменты цифровой инфраструктуры

[1] *Ведущие ученые в области цифровой экономики выступят с открытыми лекциями на FINOPOLIS 2018. URL: https://fomag.ru/news/vedushchie-uchenye-v-oblasti-tsifrovoy-ekonomiki-vystupyat-s-otkrytymi-lektsiyami-na-finopolis-2018/.*

Авторы и источники	Содержание определения понятия
P. Levinson [Levinson P., 2020, p. 171]	*Кибервойна* — форма реализации военного конфликта двух и более сторон в виртуальном пространстве путем деструктивного воздействия на физические объекты национальной экономики через каналы телекоммуникаций
F. Cristiano [Cristiano F., 2018, p. 25–26]	*Кибервойна* — эволюционно новый этап реализации военных интересов государства путем перевода традиционных военных операций в цифровое (виртуальное) пространство с привлечением частных высокотехнологичных бизнесов и специалистов в области несанкционированного доступа в информационные системы (хакеров)
R. J. Harknett, M. Smeets [Harknett R. J., Smeets M., 2020, p. 38]	*Кибервойна* — это санкционированное государством вторжение в информационное пространство другого политического субъекта с целью нанесения ему материального ущерба или установления контроля за подчиняющимися ему объектами инфраструктуры, а также отдельными институтами (например, банками, фондовыми биржами). Кибертерроризм — реализуемые частными лицами, или группами, или отдельными бизнесами анонимные атаки на объекты инфраструктуры, финансовые институты или гражданских лиц преимущественно с целью получения материальной выгоды
M. C. Libicki [Libicki M. C., 2020, p. 79]	*Кибертерроризм* — противоправная атака или угроза атаки на информационно-компьютерные системы частных или публичных лиц с целью получения материальной выгоды или принуждения атакуемых лиц к совершению определенных действий (бездействия)
II. Отечественные авторы	
М. Е. Бегларян и др. [Бегларян М. Е. и др., 2020, с. 14]	*Кибервойна* — применение специальными силами одного государства информационно-компьютерных технологий и сети Internet для нанесения ущерба объектам инфраструктуры в другом государстве без прямой физической интервенции
И. А. Кучерков [Кучерков И. А., 2019, с. 79]	*Кибервойна* — проведение военных действий (атак) на определенные объекты, расположенные на территории другого государства в виртуальном пространстве и без физического контакта вооруженных сил
Щетилов А. (см.: https://www.crime-research.org/library/chetilov.htm)	*Кибертерроризм* — совокупность преступных действий, совершаемых в виртуальном (цифровом) пространстве с целью оказания несанкционированного воздействия (влияния) на информационную инфраструктуру и собственно хранящуюся в ней информацию
С. И. Буз [Буз С. И., 2019, с. 79–80]	*Кибервойна* — разработанная и утвержденная профильными органами государственного управления программа действий в информационной сети для нанесения ущерба или получения контроля над значимыми объектами на территории государства-противника без прямого физического контакта с его территорией

Источник: составлено авторами на основе анализа и обобщения научных публикаций / Source: compiled by the authors based on the analysis and synthesis of scientific publications.

Как следует из данных табл. 1, в зарубежной практике активно используется термин «кибервойна», что обусловлено рядом причин.

Во-первых, в таких странах, как США, Великобритания, отдельных государствах ЕС (Франция, Германия), уровень развития цифровой экономики настолько высок, что их цифровая инфраструктура способна к реальному влиянию на социально-экономические системы других государств [Семеко Г. В., 2020, с. 80].

Во-вторых, ориентация сильнейших политических и военных лидеров на милитаризированный характер использования возможностей цифровой экономики. Так, в США в 2018 г. была принята новая «Стратегия национальной кибербезопасности Соединенных Штатов Америки» (*National Cyber Strategy of the United States of America*)[2], в которой

[2] *National Cyber Strategy of the United States of America (16.10.2018). URL: https://digital.library.unt.edu/ark:/67531/metadc1259394/.*

закреплены способы ведения кибервойны. Отдельно следует отметить принятый Cloud Act, дающий отдельным корпорациям США и американским спецслужбам право доступа к американским серверам, расположенным в других государствах, без уведомления последних о своем присутствии[3], что позволяет сделать вывод о силовых сценариях действий Администрации США с использованием цифровых технологий Индустрии 4.0. В ЕС также имеется пример милитаризации цифровых технологий — Таллинское руководство по применению международного права к кибероперациям[4].

В-третьих, для стран Восточной Европы (в том числе государств — членов СНГ) и Азиатского региона характерна острая технологическая зависимость от импорта информационных технологий из США и частично стран ЕС, что делает по умолчанию бесполезной ведение именно кибервойны. Для смягчения возможных последствий данной проблемы, например, в РФ были приняты специальные нормативно-правовые акты, запрещающие импорт информационных технологий для объектов критической инфраструктуры и объектов военно-промышленного комплекса[5].

АНАЛИЗ КИБЕРУГРОЗ ФИНАНСОВОЙ СИСТЕМЕ РОССИИ

Изучение вопроса обеспечения национальной безопасности финансовой системы РФ в цифровой экономике следует начать с идентификации самих вызовов и угроз цифрового пространства, а также их количественного и качественного анализа. Опираясь на публикации экспертов в области кибербезопасности И. Сачкова, Р. А. Граймса, Г. В. Семеко, К. Лагард, авторами была построена классификация наиболее актуальных финансовых вызовов и угроз цифровой экономике Российской Федерации (табл. 2).

Таблица 2

Классификация актуальных киберугроз для финансовой системы Российской Федерации / Actual financial cyberthreats classification for the Russian financial system

Наименование финансовой киберугрозы	Характеристика финансовой киберугрозы
1. Хакерские атаки, спонсируемые государством-противником	*Цели киберугрозы* — нарушение стабильного функционирования крупнейших финансовых институтов государства и (или) получение возможности контроля и манипулирования его деятельностью для нанесения экономического ущерба стране в целом. *Объекты киберугрозы*: центральные банки, фондовые биржи, финансовые Data-центры, майнинговые фермы; реже — VIP-клиенты, топ-менеджмент банка. *Особенности финансовой киберугрозы*: высочайшая квалификация хакеров, инфраструктурная поддержка атак с помощью военной инфраструктуры инициатора атаки, масштабность и системность характера атаки. *Примеры хакерских команд*: Equation Group, Lazarus

[3] *CLOUD Act / The Congress of the United States of America. URL: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.*

[4] *The Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013. URL: https://d-russia.ru/wp-content/uploads/2013/08/tallinnmanual.pdf.*

[5] *Постановление Правительства РФ от 14.07.2014 № 656 (ред. от 30.04.2020) «Об установлении запрета на допуск отдельных видов товаров машиностроения, происходящих из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд». URL: http://www.consultant.ru/document/cons_doc_LAW_165608/; Постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд». URL: https://base.garant.ru/71252170/.*

Наименование финансовой киберугрозы	Характеристика финансовой киберугрозы
2. Финансовые диверсии на финансовом рынке, инициируемые крупнейшими финансовыми корпорациями	*Цели киберугрозы* — формирование на фондовых биржах панических настроений, снижение стоимости или исключение из котировального листа отдельных бизнесов путем информационных вбросов (фейк-новостей, информации, порочащей деловую репутацию компании и ее топ-менеджеров), организация утечки инсайдерской информации, хакерских атак на активы компании (организация искусственных сбоев или аварий). *Объекты киберугрозы*: акции крупнейших бизнесов (голубые фишки), а также вмешательство в процессы участия отдельных бизнесов в международных инвестиционных программах и проектах (преимущественно — сфера военно-промышленного комплекса и энергетики). *Особенности финансовой киберугрозы*: искусственное ухудшение рейтинговых позиций крупнейших бизнесов государства, снижение их инвестиционной привлекательности, отстранение государства от международных инвестиционных проектов и программ. *Примеры хакерских команд*: Cobalt, BlackEnergy, Idustroyer, HAVEX
3. Конструирование и запуск социоинженерных троянов	*Цели киберугрозы* — получение через аккаунты частных и публичных лиц — клиентов банков доступа ко всей банковской инфраструктуре и осуществление операций по ее выведению из строя, а также хищению персональных данных клиентов и их денежных средств. *Объекты киберугрозы*: программные модули социальных сетей, аккаунты в интернет-банкинге, файловые менеджеры владельцев банковских карт и др. *Особенности финансовой киберугрозы*: доступ к критической банковской инфраструктуре хакеры получают через менее защищенные частные и публичные аккаунты, находящиеся за контуром основной банковской инфраструктуры, а следовательно, имеющие более высокую уязвимость. *Примеры хакерских команд*: APT10, WINNITI, Regin, REXAN
4. Инфраструктурные атаки на IoT-сети (интернет вещей)	*Цели киберугрозы* — получение контроля над бизнес-процессами финансово-промышленных экосистем, а также нанесение им прямого и косвенного ущерба вследствие нарушения стабильности их работы, а также хищения или манипулирования приватными данными пользователей таких экосистем. *Объекты киберугрозы*: системы дистанционной оплаты платных автодорог, сервисы дистанционной медицины, системы «умного дома» и «безлюдного офиса», интегрированные в банковскую бизнес-модель. *Особенности финансовой киберугрозы*: через взлом аккаунта или элементов финансовой инфраструктуры хакеры получают возможность влиять на физическую инфраструктуру, находящуюся за контурами банка, а также конструировать социальный хаос или техногенные происшествия. *Примеры хакерских команд*: Fancy Bears, Lizard Squad, Anonymous
5. Продажа хакерских инструментов с открытым кодом	*Цели киберугрозы* — вовлечение в орбиту хакеров граждан, которые склонны к нарушению законодательства или мотивированы к мести, и передача им инструментов для совершения хакерских атак. *Объекты киберугрозы*: как правило, атаки направлены на быстрый доступ к денежным средствам объектов атаки, например частные банковские карты, электронные кошельки, аккаунты интернет-банкинга. *Особенности финансовой киберугрозы*: ввиду передачи инструментов для совершения хакерских атак новым лицам идентификация источников таких атак часто может быть затруднена, кроме того, возможна т. н. флешмоб-атака с множества географически удаленных точек доступа, а значит, вероятность раскрытия участников атаки значительно усложняется. *Примеры хакерских команд*: Anonymous, LulzSec*

** См.: ForkLog (https://forklog.com/anatomiya-hakerskih-gruppirovok-kto-i-zachem-vzlamyvaet-tsifrovye-sistemy/).*
Источник: составлено авторами по данным [Сачков И., 2017; Семеко Г. В., 2020; Клауберг Р. 2020; Тарханова Е. А. и др., 2018] / Source: compiled by the authors based on data from [Sachkov I., 2017; Semeko G. V., 2020; Clauberg R., 2020; Tarkhanova E. A. et al., 2018].

По сравнению с указанными агрегированными формами киберугроз в Европейской конвенции по киберпреступности (ETS 185)[6] классификация финансовых киберугроз имеет несколько иной вид:

[6] *Конвенция о компьютерных преступлениях № 185 / Совет Европы, Будапешт, 23 ноября 2001 г. URL: https://rm.coe.int/1680081580.*

— незаконный доступ (несанкционированное вторжение в институты финансовой системы);

— незаконный перехват (получение приватных данных третьим лицом), вмешательство в данные (искажение, удаление или иные неправомерные действия с информацией, приводящей к ее качественной некорректности);

— вмешательство в систему или бизнес-процессы (установление несанкционированного контроля третьим лицом над бизнес-процессами или управленческими действиями).

Рассмотрим динамику кибератак, осуществленных на институты национальной финансовой системы РФ за 2016–2020 гг. (табл. 3).

Таблица 3

Ключевые показатели кибератак на институты национальной финансовой системы Российской Федерации за 2016–2020 гг. / Key indicators of financial cyberthreats for the Russian national financial system institutes in 2016–2020

Показатели	2016 г.	2017 г.	2018 г.	2019 г.	2020 г.
1. Совокупное количество совершенных кибератак на институты национальной финансовой системы, ед. В том числе:	489	514	687	1723	968
Центральный банк	-	1	2	4	-
системообразующие банки	12	9	16	29	18
остальные банки	324	407	488	879	775
небанковские кредитно-финансовые организации — НКФО (в т. ч. государственные)	153	97	181	811	175
2. География источников кибератак, в % к общему количеству	100	100	96,7	100	100
Резиденты РФ	49,7	42,8	40,5	48,5	48,4
Страны СНГ	16,8	25,5	22,8	16,4	13,9
Дальнее зарубежье	33,5	31,7	33,4	35,1	37,7
3. Совокупный объем нанесенного материального ущерба институтам национальной финансовой системы, млн руб., в том числе:	1942,4	1687,8	2539,6	10 494,7	16 749,6
убытки, причиненные клиентам банков и НКФО, млн руб.	1080	961,3	1384,7	5723,5	8757,2
расходы на восстановление дееспособности банковской инфраструктуры после кибератаки, млн руб.	862,4	726,5	1154,9	4771,2	7992,4
4. Показатели защищенности институтов национальной финансовой системы					
Удельный вес отраженных кибератак, %	39,5	42,4	44,7	49,5	52,7
Уровень возмещения банками убытков от кибератак (сумма возвращенных банком средств / сумма похищенных средств * 100), %	18,3	17,2	16,2	15,0	11,3
Индекс устойчивости институтов национальной финансовой системы (соотношение отраженных и успешно проведенных кибератак) по категориям финансовых институтов:					
— Центральный банк РФ	-	1,0	2,0	4,0	-
— системообразующие банки	7,9	7,2	6,8	8,0	7,7
— остальные банки	5,5	4,7	4,9	4,5	3,4
— небанковские кредитно-финансовые организации — НКФО (в т. ч. государственные)	6,2	5,8	5,5	4,9	4,1

Источник: составлено авторами по данным Банка России (Обзоры несанкционированных переводов денежных средств, ФинЦЕРТ, 2016–2020) / Source: compiled by the authors based on data of the Bank of Russia.

Как следует из данных табл. 3, финансовые институты в РФ за 2016–2020 гг. ощутили возрастающее количество кибератак. Так, в 2020 г. по сравнению с 2016 г. их количество

выросло на 479 ед., или на 98 %. При этом структурно в группе риска кибератак ключевое место занимают коммерческие банки не системообразующего уровня — на них пришлось в среднем 65,6 % всех кибератак. В части географического распределения источников проведения атак на финансовые институты следует отметить высокий удельный вес хакерских группировок дальнего зарубежья — в среднем их участие составило 34,2 % (хакеры-резиденты — 45,9 %).

Тревожным сигналом о наличии в национальной финансовой системе Российской Федерации серьезных технологических уязвимостей служит рост убытков, нанесенных кибератаками на финансовые институты (в 2020 г. по сравнению с 2016 г. произошел более чем 8-кратный рост совокупных потерь от хакерских атак), несмотря на устойчивый рост коэффициента отражения хакерских атак (в 2020 г. по сравнению с 2016 г. процент успешно отраженных атак вырос на 13,2 п. п. и составил 52,7 %).

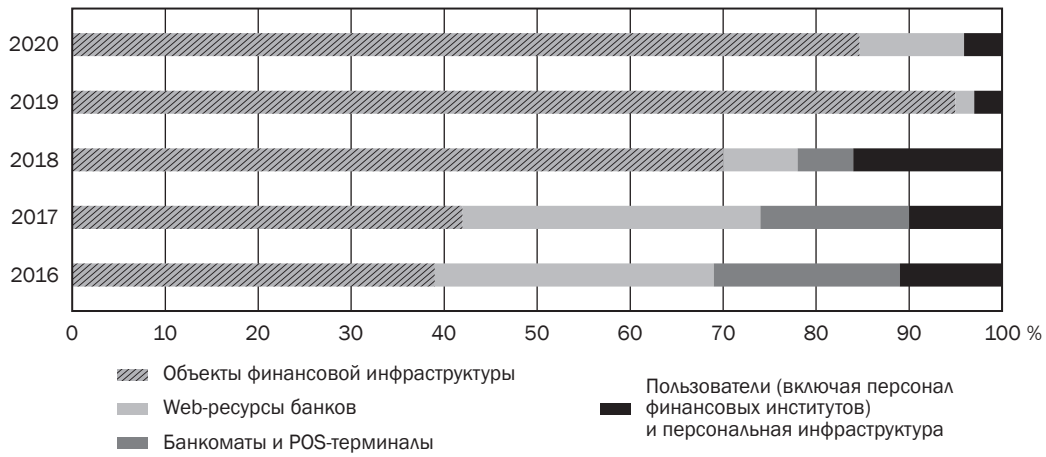
Это позволяет сделать вывод, что финансовые институты успешно справляются только с относительно простыми механизмами осуществления кибератак, по которым у них уже есть профессиональный опыт управления и защиты. В отношении же сложных и многоходовых механизмов атаки, построенных с применением социальной инженерии и вовлечением в процесс реализации атаки самих клиентов путем введения последних в добросовестное заблуждение о том, что у национальных финансовых институтов достаточная защищенность от хакерских атак. Данный тезис подтверждается и показателем динамики уровня возмещения банками убытков от кибератак: в 2020 г. по сравнению с 2016 г. он снизился на 7,0 п. п. и составил 11,3 %.

Важным штрихом является структурный анализ индекса устойчивости институтов национальной финансовой системы: наивысшие результаты принадлежат системообразующим банкам (среднее значение — 7,52), низший — коммерческим банкам несистемообразующего уровня (среднее значение — 4,6), причем в отношении последних имеет место негативная тенденция снижения общей устойчивости к финансовым кибератакам.

Представим структурный анализ объектов атак на институты национальной финансовой системы РФ за 2016–2020 гг. (рис. 1).

Рисунок 1

Структура объектов кибератак на институты национальной финансовой системы РФ за 2016–2020 гг. / Objects' structure of cyberattacks on national financial system institutes in 2016–2020



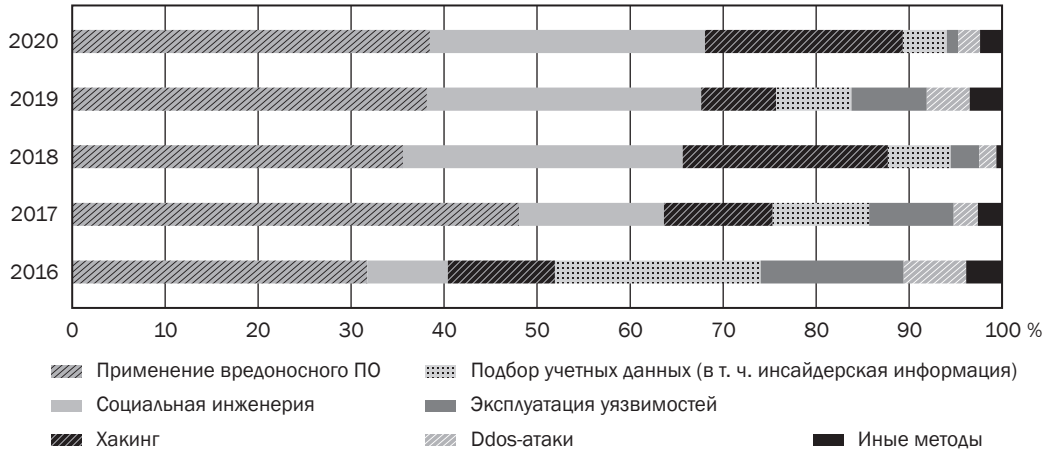
Источник: составлено авторами по данным аналитических материалов Positive Technologies за 2016–2020 гг. (https://www.ptsecurity.com/ru-ru/research/analytics/) / Source: compiled by the authors according to the analytical data of Positive Technologies in 2016–2020.

Как следует из данных, представленных на рис. 1, в 2016–2020 гг. ключевым направлением кибератак на финансовые институты стали объекты финансовой инфраструктуры: рост атак на них увеличился с 39 % в 2016 г. до 95 % в 2020 г. Второе по значимости направление — веб-ресурсы банка: в среднем на них пришлось 16,6 % кибератак. В отношении объектов пользовательского интерфейса наблюдается значительное сокращение атак: в 2020 г. их удельный вес составил только 4,0 % (для сравнения: в 2016 г. — 11,0 %), что говорит о росте уровня цифровой культуры пользователей при работе в виртуальном пространстве. В целом же ситуация свидетельствует о росте профессионализма кибератак с направленностью как на деструктивное воздействие на глобальные объекты финансовой инфраструктуры, так и на получение доступа к индивидуальным банковским аккаунтам клиентов.

Далее рассмотрим структуру методов совершения кибератак на институты национальной финансовой системы РФ за 2016–2020 гг., что позволит лучше понять проблемные зоны в архитектуре самой инфраструктуры финансовых институтов и регулятивных пробелов национального законодательства (рис. 2).

Рисунок 2

Структура инструментов совершения кибератак на институты национальной финансовой системы РФ за 2016–2020 гг., % /
Tools' structure of cyberattacks on national financial system institutes in 2016–2020, %



Источник: составлено авторами по данным аналитических материалов Positive Technologies за 2016–2020 гг. (https://www.ptsecurity.com/ru-ru/research/analytics/) / Source: compiled by the authors according to the analytical data of Positive Technologies in 2016–2020.

Данные рис. 2 свидетельствуют о том, что на протяжении 2016–2020 гг. основным методом совершения кибератак на финансовые институты стало применение вредоносного ПО (в среднем 51,8 %), причем в 2020 г. отмечен рост по сравнению с 2016 г. на 32,0 п. п. до отметки 65,0 %. Далее следует метод социальной инженерии (34,2 %), который, в свою очередь, включает многообразие частных инструментов (например, фишинг, под которым понимается вид интернет-мошенничества для кражи паролей, номеров карт, банковских счетов и другой конфиденциальной информации)[7].

Следует также отметить, что в 2018 и 2020 гг. зафиксирован всплеск хакинга (36,0 %), причем основными источниками атак было сетевое пространство США, ФРГ

[7] *Финансовые киберугрозы в 2020 году / Лаборатория Касперского, 2021. URL: https://securelist.ru/financial-cyberthreats-in-2020/101160/.*

и Нидерландов[8]. Если до 2019 г. отмечалось превалирование монетизированных целей применения вредоносного ПО (шифрование, угроза удаления данных, вирусы и т. п.), то после 2019 г. лидером стало применение шпионского ПО, которое собирает данные о финансовых транзакциях и клиентах банков. Наконец, начиная с 2018 г. отмечается адресность и комплексность проведения кибератак на финансовые институты, что также свидетельствует о росте качества и проработанности стратегии их совершения.

Как представляется, можно сделать следующие обобщения.

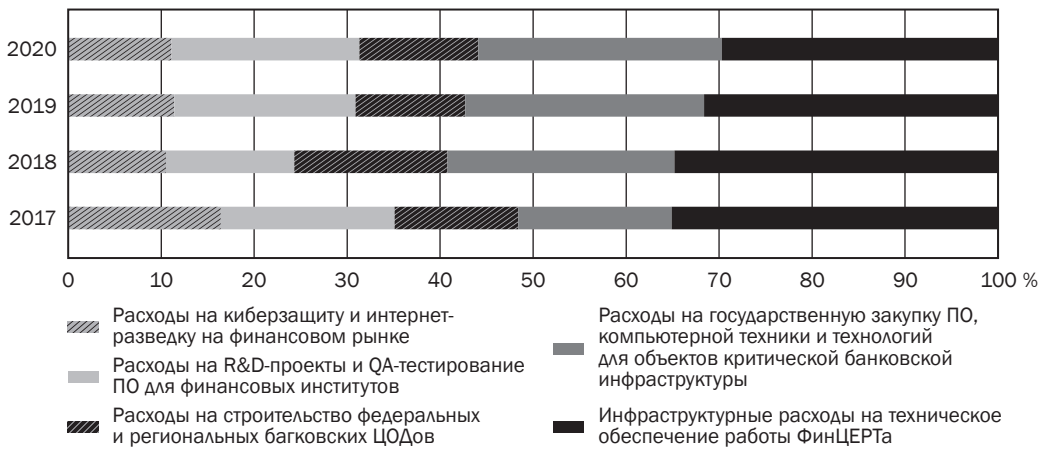
Во-первых, виртуальное пространство цифровой экономики постепенно становится реальной угрозой для национальной безопасности страны ввиду масштабного проникновения информационных и компьютерных технологий во все отрасли экономики и сферы жизни граждан.

Во-вторых, финансовая система и ее важнейшие элементы — банки — являются высоковосприимчивыми к цифровым инновациям, которые обеспечивают не только снижение транзакционных издержек при совершении финансовых операций, но и повышают лояльность клиента за счет персонализации банковских продуктов.

В-третьих, основой конкурентной стратегии современного банка и гарантом его «рыночного долголетия» является информация о клиенте и его предпочтениях, а также интеграция в информационное пространство как финансовой сферы, так и сферы физических нефинансовых бизнесов в формате экосистем, что одновременно дает конкурентные преимущества банку, но и повышает его ответственность за безопасность и приватность собираемой и анализируемой информации в рамках стратегии работы с большими данными (*Big Data Security Strategy*)[9].

Рисунок 3

Структура расходов финансовых институтов на обеспечение кибербезопасности в цифровой экономике в 2017–2020 гг. / Cybersecurity costs of financial institutes in digital economy in 2017–2020



Источник: составлено авторами по данным аналитических и отчетных материалов (https://iz.ru/687793/anastasiia-alekseevskikh/banki-uvelichili-na-15-raskhody-na-kiberbezopasnost; https://cbr.ru/Collection/Collection/File/32087/FINCERT_report_20191010.PDF; https://infraone.ru/sites/default/ files/analitika/2020/investicii_v_infrastrukturu_informacionnye_tekhnologii_infraone_research.pdf) / Source: compiled by the authors based on analytical and reporting materials.

---

[8] *В МИД РФ назвали страны, откуда Россию атаковали хакеры в 2020 году. URL: https://regnum.ru/news/polit/3266429.html; Кибервойна России и США. URL: https://www.tadviser.ru/index.php/Статья:Кибервойна_России_и_США#.*

[9] *7 Big Data Security Concerns (11.03.2021). URL: https://www.qubole.com/blog/big-data-security-concerns/.*

В завершение аналитической оценки киберугроз национальной финансовой системе РФ рассмотрим динамику расходов на обеспечение национальной безопасности и противодействие киберугрозам с учетом структуры расходов, регламентируемой Указом Президента РФ «О Стратегии национальной безопасности Российской Федерации» № 683 от 31.12.2015, Национальной программой «Цифровая экономика» и федеральным проектом «Цифровое государственное управление» (рис. 3). По данным рис. 3 основной статьей расходов финансовых институтов на обеспечение кибербезопасности в цифровой экономике выступили инфраструктурные расходы на техническое обеспечение работы Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) — в среднем удельный вес данного компонента составил 31,5 %, далее следуют расходы на государственные закупки ПО и технических средств для объектов критической банковской инфраструктуры (23,2 %) и расходы на R&D-проекты и QA-тестирование ПО для финансовых институтов (18,1 %).

Таким образом, в настоящее время вопрос обеспечения кибербезопасности функционирования институтов национальной финансовой системы РФ тесно связан с административными решениями государственного регулятора и повышением требований к уровню технологического обеспечения работы банков и НКФО [Zver'kova T. N., 2019, p. 18–19].

В заключение нашего исследования рассмотрим возможные сценарии развития киберугроз и кибератак на институты национальной финансовой системы России (табл. 4).

Таблица 4

Основные сценарии развития киберугроз и кибератак на институты национальной финансовой системы РФ / Main scenarios of cyberthreats and cyberattacks development for national financial system institutes of the Russian Federation

Наименование сценария	Описание сценария
1. Сценарий активной киберинтервенции в финансовую систему РФ	*Предпосылки сценария*: — обострение политического и экономического противостояния мировых лидеров — РФ и США (плюс союзники); — иммунитет национальной экономики против пакетных продуктовых и технологических санкций; — рост автономности национальной цифровой инфраструктуры (развитие Рунета, разработка собственного ПО, формирование национального файервола). *Механизм реализации сценария*: санкционированные военным руководством США и союзниками серии кибератак на крупнейшие банки РФ (Сбербанк, ВТБ, ВЭБ.РФ), отраслевые банки, финансирующие военно-промышленный комплекс (Промсвязьбанк) через их партнеров в других странах с целью нарушения нормальных режимов их функционирования, а также разрушения корреспондентских связей мегабанков РФ с заграничными партнерами
2. Сценарий использования мягкой силы технологического превосходства	*Предпосылки сценария*: — в настоящее время банковская система РФ имеет уровень импортозависимости в части технологий и инфраструктурного обеспечения международных банковских контактов от 60 до 82 %*; — инфраструктурная зависимость от распространения банковских продуктов дистанционного сервиса от ведущих технологических компаний (Apple Store, Play Market); — санкционное давление на банковскую систему РФ путем угроз и шантажа (например, угроза отключения от системы SWIFT). *Механизм реализации сценария*: предполагаемые противники могут воздействовать на банковскую систему через технологические инструменты, например ограничение или отключение доступа к элементам критический инфраструктуры, создание помех для работы мобильных приложений или шпионаж за клиентами через приложения

Наименование сценария	Описание сценария
3. Сценарий активной кибервойны между РФ и союзниками и США (включая силы НАТО)	*Предпосылки сценария*: — нарастание холодного противостояния РФ и ее политических противников; — обострение внутренних проблем в экономике (девальвация рубля, гражданские волнения); — необходимость США сохранить статус мирового военного лидера. *Механизм реализации сценария*: осуществление программы массированных кибератак на объекты финансовой инфраструктуры друг друга с государственной поддержкой хакеров и их материальным и технологическим обеспечением

** По данным PwC (https://www.pwc.ru/ru/publications/collection/issledovaniye-vnutrennego-audita-finansovykh-organizatsiy.pdf).*
Источник: разработано авторами по данным [Sukhodolov A. P., Beryozkin Y. M., 2018; Chernyakov M. K., Chernyakova E. C., 2018; Поветкина Н. А., Леднева Ю. В., 2018; Dhote T. et al., 2020; Дмитриева Г. С., 2020; Кох Л. В., Кох Ю. В., 2019; Нестерова Д. А., 2020] / Source: developed by the authors according to [Sukhodolov A. P., Beryozkin Y. M., 2018; Chernyakov M. K., Chernyakova E. S., 2018; Povetkina N. A., Ledneva Yu. V., 2018; Dhote T. et al., 2020; Dmitrieva G. S., 2020; Kokh L., Kokh Yu., 2019; Nesterova D. A., 2020].

ЗАКЛЮЧЕНИЕ

Как следует из представленного анализа, Российская Федерация в настоящее время находится под воздействием серьезных рисков, обусловленных киберугрозами, ориентированными на ее финансовые институты с целью ослабления экономики и усиления социально-экономических волнений и напряженности. Подчеркнем, что современная архитектура мировой финансовой системы очень чувствительна к любым манипуляциям и тем более шоковым воздействиям в виде разрушения или выведения из нормальной работы систем связи, фондовых бирж, Data-центров международных платежных систем, о последствиях которых эксперты могут судить крайне субъективно. Как представляется, рост давления на институты финансовой системы и увеличение количества провокационных атак инкогнито будут продолжаться и дальше. В связи с этим руководству страны и административным центрам управления финансовыми институтами следует продолжить развитие собственных программных и цифровых продуктов, банковской инфраструктуры, а также популяризацию сегмента Рунета среди граждан России и стран СНГ как безопасной и политически нейтральной площадки для формирования и развития цифровой экономики, построенной на фундаменте собственных высокотехнологичных решений и сервисов (например, масштабирование опыта лабораторий Сбербанка, цифровизации бизнес-процессов Тинькофф Банка и др.).

В заключение подчеркнем, что проведенный анализ не снимает необходимости дальнейшей проработки теоретических и практических вопросов обеспечения кибербезопасности финансовых институтов в цифровой экономике.

Список источников

Бегларян М. Е., Войтова-Долгих Я. Н., Одинцов С. А. Исторические аспекты понятий «киберпреступление» и «кибертерроризм» в законодательстве: проблемы трактования // Вестник Краснодарского университета МВД России. 2020. № 4 (50). С. 11–16.

Буз С. И. Киберпреступления: понятие, сущность и общая характеристика // Юристъ — Правоведъ. 2019. № 4 (91). С. 78–83.

Бухарин В. В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестник МГИМО-Университета. 2016. № 6 (51). С. 76–91. URL: https://doi.org/10.24833/2071-8160-2016-6-51-76-91.

Дмитриева Г. С. Цифровые технологии в банковском секторе экономики // Известия Санкт-Петербургского государственного экономического университета. 2020. № 1 (121). С. 49–54.

Клауберг Р. Проблемы цифровизации и искусственного интеллекта в сферах современной экономики, общества и управления // Вестник Российского университета дружбы народов. Серия: Экономика. 2020. Т. 28. № 3. С. 556–567. URL: https://doi.org/10.22363/2313-2329-2020-28-3-556-567.

Кох Л. В., Кох Ю. В. Банки и финтех-компании: конкуренты или партнеры // Вестник Забайкальского государственного университета. 2019. Т. 25. № 6. С. 111–121. URL: https://doi.org/10.21209/2227-9245-2019-25-6-111-121.

Кучерков И. А. О понятии «киберпреступление» в законодательстве и научной доктрине // Юридическая наука. 2019. № 10. С. 78–82.

Нестерова Д. А. Риски информационной безопасности коммерческих банков в условиях новой экономической и технологической реальности // Инновации и инвестиции. 2020. № 5. С. 144–151.

Поветкина Н. А., Леднева Ю. В. «Финтех» и «регтех»: границы правового регулирования // Право. Журнал Высшей школы экономики. 2018. № 3. С. 46–67. URL: https://doi.org/10.17323/2072-8166.2018.2.46.67.

Сачков И. 5 актуальных киберугроз, которые грозят финансовыми потерями / Гарант.Ру, 2017. URL: https://www.garant.ru/ia/opinion/author/sachkov/1119775/.

Семеко Г. В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. 2020. № 1 (1). С. 77–96. URL: https://doi.org/10.31249/snsn/2020.01.06.

Тарханова Е. А., Чижевская Е. К., Бабурина Н. Т. Институциональные изменения и цифровизация бизнес операций в финансовых учреждениях // Журнал институциональных исследований. 2018. Т. 10. № 4. С. 145–156. URL: https://doi.org/10.17835/2076-6297.2018.10.4.145-155.

Чернышенко Н. А. Кибервойна: теория и практика // Наукові праці. Політологія. 2015. Т. 260. Вып. 248. С. 37–41.

Chernyakov M. K., Chernyakova E. C. Technological Risks of the Digital Economy // Корпоративные финансы. 2018. Т. 12. № 4. С. 99–110. URL: https://doi.org/10.17323/j.jcfr.2073-0438.12.4.2018.99-109.

Clarke R. A., Knake R. K. Cyber War: The Next Threat to National Security and What to Do About It. Nova Iorque: HarperCollins, 2010. 290 p.

Cristiano F. From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises // Journal of War and Culture Studies. 2018. Vol. 11. Iss. 1. P. 22–37. URL: https://doi.org/10.1080/17526272.2017.1416761.

Dhote T., Pathak P., Kulkarni P. Coping with the challenges posed by GAFA and other digital disruptors: Can advanced technologies help the banking sector? // International Journal of Scientific and Technology Research. 2020. No. 9 (2). P. 2196–2199.

Harknett R. J., Smeets M. Cyber campaigns and strategic outcomes // Journal of Strategic Studies. 2020. No. 4. P. 36–42. URL: https://doi.org/10.1080/01402390.2020.1732354.

Levinson P. Micro-cyberwar vs. macro-cyberwar: towards the beginning of a taxonomy // Digital War. 2020. No. 1. P. 171–172. URL: https://doi.org/10.1057/s42984-020-00020-z.

Libicki M. C. Cyberwar is What States Make of It // The Cyber Defense Review. 2020. Vol. 5. No. 2. P. 77–87.

Negroponte N. Being Digital. NY: Knopf, 1995, 256 p.

Perritt J. The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance // Indiana Journal of Global Legal Studies. 1998. Vol. 5. Iss. 2. P. 423–442.

Rauhofer J., Bowden C. Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud // Edinburgh School of Law Research Paper. 2013. No. 28. URL: https://doi.org/http://dx.doi.org/10.2139/ssrn.2283175.

Singer P., Friedman A. Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford Univ. Press, 2014. 320 p.

Sukhodolov A. P., Beryozkin Y. M. From the Institutional to the Platform Economy // Управленец. 2018. Vol. 9. No. 3. P. 8–14. URL: https://doi.org/10.29141/2218-5003-2018-9-3-2.

Zver'kova T. N. Regional Banks & FinTech: a Standoff or Partnership? // Digest Finance. 2019. Т. 24. № 1 (249). С. 13–20. URL: https://doi.org/10.24891/df.24.1.13.

References

Beglaryan M.E., Vojtova-Dolgikh Ya.N., Odintsov S.A. (2020). Historical Aspects of the Concepts of "Cybercrime" and "Cyberterrorism" in Legislation: Problems of Interpretation. *Vestnik Krasnodarskogo universiteta MVD Rossii — Bulletin of Krasnodar University of the Ministry of Internal Affairs of Russia*, no. 4 (50), pp. 11–16 (In Russ.).

Buz S.I. (2019). Cyber Crimes: Concept, Essence and General Characteristic. *Jurist — Pravoved — Attorney*, no. 4 (91), pp. 78–83 (In Russ.).

Bukharin V.V. (2016). The Russian's Digital Sovereignty as a Technical Basis of Information SECurity. *Vestnik MGIMO Universiteta — Bulletin of MGIMO University*, no. 6, pp. 76–91 (In Russ.). Available at: https://doi.org/10.24833/2071-8160-2016-6-51-76-91.

Chernyshenko N.A. (2015). Cyberwar: Theory and Practice. *Nauchnye raboty. Politologija — Scientific Work. Political Science*, vol. 260, iss. 248, pp. 37–42 (In Russ.).

Chernyakov M.K., Chernyakova E.S. (2018). Technological Risks of the Digital Economy. *Korporativnye finansy — Journal of Corporate Finance*, vol. 12, no. 4, pp. 99–110. Available at: https://doi.org/10.17323/j.jcfr.2073-0438.12.4.2018.99-109.

Clarke R.A., Knake R.K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. Nova Iorque: HarperCollins, 290 p.

Cristiano F. (2018). From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises. *Journal of War and Culture Studies*, vol. 11, iss. 1, pp. 22–37. Available at: https://doi.org/1010.1080/17526272.2017.1416761.

Dmitrieva G.S. (2020). Digital Technologies in the Banking Sector of Economy. *Izvestia Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta — Bulletin of St. Petersburg State University of Economics*, no. 1, pp. 49–54 (In Russ.).

Dhote T., Pathak P., Kulkarni P. (2020). Coping with the challenges posed by GAFA and other digital disruptors: Can advanced technologies help the banking sector? *International Journal of Scientific and Technology Research*, no. 9 (2), pp. 2196–2199.

Harknett R.J., Smeets M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, no. 4, pp. 36–42. Available at: https://doi.org/10.1080/01402390.2020.1732354.

Klauberg R. (2020). Challenges of Digitalization and Artificial Intelligence for Modern Economies, Societies and Management. *Vestnik Rossiiskogo universiteta druzhby narodov — RUDN Journal of Economics*, vol. 28, no. 3, pp. 556–567 (In Russ.).

Kokh L., Kokh Yu. (2019). Banks and Fintech Companies: Competitors or Partners. *Vestnik Zabajkal'skogo gosudarstvennogo universiteta — Bulletin of Transbaikal State University*, vol. 25, no. 6, pp. 111–121 (In Russ.). Available at: https://doi.org/10.21209/2227-9245-2019-25-6-111-121.

Kucherkov I.A. (2019). On the Concept of Cybercrime in Legislation and Scientific Doctrine. *Yuridicheskaya nauka — Legal Science*, no. 10, pp. 78–82 (In Russ.).

Levinson P. (2020). Micro-cyberwar vs. macro-cyberwar: towards the beginning of a taxonomy. *Digital War*, no. 1, pp. 171–172. Available at: https://doi.org/10.1057/s42984-020-00020-z.

Libicki M.C. (2020). Cyberwar is What States Make of It. *The Cyber Defense Review*, vol. 5, no. 2, pp. 77–87.

Negroponte N. (1995). Being Digital. NY: Knopf, 256 p.

Nesterova D.A. (2020). Information Security Risks of Commercial Banks in the New Economic and Technological Reality. *Innovacii i investicii — Innovation and Investment*, no. 5, pp. 144–151 (In Russ.).

Perritt J. (1998). The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance. *Indiana Journal of Global Legal Studies*, vol. 5, iss. 2, pp. 423–442.

Povetkina N.A., Ledneva J.V. (2018). Fintekh and Redtekh: Boundaries of Legal Regulation. *Pravo. Zhurnal Vysshey shkoly ekonomiki — Law. Journal of the Higher School of Economics*, no. 3, pp. 46–67. Available at: https://doi.org/10.17323/2072-8166.2018.2.46.67 (In Russ.).

Semeko G.V. (2020). Information Security in the Financial Sector: Cybercrime and Countermeasures Strategy. *Sotsial'nye novatsii i social'nye nauki — Social Innovation and Social Sciences*, no. 1, pp. 77–96. Available at: https://doi.org/10.31249/snsn/2020.01.06. (In Russ.).

Tarkhanova E.A., Chizhevskaya E.K., Baburina N.T. (2018). Institutional Changes and Ditigalization of Business Operations in Financial Institutions. *Zhurnal institucional'nyh issledovanij — Journal of Institutional Studies*, vol. 10, no. 4, pp. 145–156 (In Russ.).

Rauhofer J., Bowden C. (2013). Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud. *Edinburgh School of Law Research Paper*, no. 28. Available at: https://doi.org/http://dx.doi.org/10.2139/ssrn.2283175.

Sachkov I. (2017). 5 Current Cyber Threats That can Cause Financial Losses. Garant.Ru, 2017 (In Russ.). Available at: https://www.garant.ru/ia/opinion/author/sachkov/1119775/.

Singer P., Friedman A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford: Oxford Univ. Press, 320 p.

Sukhodolov A.P., Beryozkin, Y.M. (2018). From the Institutional to the Platform Economy. *Upravlenets — The Manager*, vol. 9, no. 3, pp. 8–14. Available at: https://doi.org/10.29141/2218-5003-2018-9-3-2.

Zver'kova T.N. 2019. Regional Banks & FinTech: a Standoff or Partnership? *Daidzhest finansy — Digest Finance*, vol. 24, no. 1 (249), pp. 13–20. Available at: https://doi.org/10.24891/df.24.1.13.

Информация об авторах

***Сергей Всеволодович Шкодинский**, доктор экономических наук, профессор, главный научный сотрудник Центра отраслевой экономики Научно-исследовательского финансового института Минфина России, г. Москва; заведующий лаборатории промышленной политики и экономической безопасности Института проблем рынка РАН, г. Москва*

***Михаил Николаевич Дудин**, доктор экономических наук, профессор, заместитель директора по науке Института проблем рынка РАН, г. Москва*

***Далер Ирматович Усманов**, кандидат экономических наук, доцент, старший научный сотрудник лаборатории проблем пространственного развития Института проблем рынка РАН, г. Москва*

Information about the authors

***Sergey V. Shkodinsky**, Doctor of Economic Sciences, Professor, Chief Researcher at the Center for Sectoral Economics, Financial Research Institute, Moscow; Head of the Laboratory for Industrial Policy and Economic Security, Market Economy Institute, Russian Academy of Sciences, Moscow*

***Mihail N. Dudin**, Doctor of Economic Sciences, Professor, Deputy Director for Science, Market Economy Institute, Russian Academy of Sciences, Moscow*

***Daler I. Usmanov**, Candidate of Economic Sciences, Associate Professor, Senior Researcher at the Laboratory of Spatial Development Problems, Market Economy Institute, Russian Academy of Sciences, Moscow*

Статья поступила в редакцию 11.05.2021
Одобрена после рецензирования 11.06.2021
Принята к публикации 16.06.2021

Article submitted May 11, 2021
Approved after reviewing June 11, 2021
Accepted for publication June 16, 2021