Часть 1

ТЕНДЕНЦИИ ЭКОНОМИЧЕСКОГО РАЗВИТИЯ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

УДК 330.14

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ФИНАНСОВОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

И. Н. Александров[1)], А. Е. Паршуков[2)], В. Н. Дорошко[3)]

[1)] *кандидат экономических наук, доцент, Санкт-Петербургский политехнический университет Петра Великого, г. Санкт-Петербург, Российская Федерация, e-mail: a7830298@gmail.com*
[2)] *кандидат экономических наук, доцент, Санкт-Петербургский политехнический университет Петра Великого, г. Санкт-Петербург, Российская Федерация, e-mail: a7830298@gmail.com*
[3)] *кандидат экономических наук, доцент, Белорусский торгово-экономический университет потребительской кооперации г. Гомель, Республика Беларусь, e-mail: vetaldoroshko@gmail.com*

Четвертая промышленная революция – один из самых неоднозначных этапов эволюции мировой экономики: основой ее непредсказуемости является вовлечение в экономические отношения всех государств мира, независимо от уровня их экономического и технологического развития. Информационная открытость, без которой Индустрия 4.0 не может функционировать, несет огромные риски для российской экономики. Прозрачность экономических систем стала источником появления новой концепции не только управленческого, но и военно-политического мышления элит.

Ключевые слова: риски; цифровая инфраструктура; банковская система; санкции.

SECURITY PROBLEMS OF THE FINANCIAL INFRASTRUCTURE OF THE RUSSIAN FEDERATION

I. N. Aleksandrov[1)], A. E. Parshukov[2)], V. N. Daroshka[3)]

[1)] *PhD in Economics, Associate* Professor, *Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russian Federation, e-mail: a7830298@gmail.com*
[2)] *PhD in Economics, Associate* Professor, *Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russian Federation, e-mail: a7830298@gmail.com*
[3)] *PhD in Economics, Associate Professor, Belarusian Trade and Economic University of Consumer Cooperatives, Gomel, Republic of Belarus, e-mail: vetaldoroshko@gmail.com*

The Fourth Industrial Revolution is one of the most ambiguous stages in the evolution of the world economy: the basis of its unpredictability is the involvement in economic

relations of all countries of the world, regardless of their level of economic and technological development. Information openness, without which Industry 4.0 cannot function, carries huge risks for the Russian economy. The transparency of economic systems has become the source of a new concept of not only managerial, but also military-political thinking of the elites.

Keywords: risks; digital infrastructure; banking system; sanctions.

Идея о том, что цифровая экономика может стать генератором изменений в военном и политическом мышлении государственных элит, восходит к исследованиям американского ученого Н. Негропонте, который в 2000 году высказал идею о наступлении точки невозврата из-за формирования «Индустрии 4.0», которая приведет к фундаментальным изменениям в структуре социально-экономических отношений, но до 2011 года его идеи считались футуристическими и маловероятными [1].

Изучение научной литературы показало, что оценка цифровой экономики как инструмента военно-политического влияния отсылает к научным работам Перритт Дж., Раухофер Дж., Боуден К [2; 3]. Авторы ввели понятие «цифровой суверенитет» как мера независимости выражения и реализации частных, государственных и общественных интересов в глобальном цифровом пространстве.

В настоящее время в отечественной и зарубежной литературе нет единого мнения о правильности использования понятий «кибертерроризм», «кибервойна», «хакерство».

На основе сравнительного анализа определения понятий в отечественной и зарубежной практике были сделаны следующие выводы: 1) в зарубежной практике под кибертерроризмом понимаются любые несанкционированные действия государства по нарушению стабильности социально-экономической системы другого государства; кибервойна рассматривается как программный продукт, уполномоченных специализированными органами государственного управления влиять на другое государство или его интересы; 2) в отечественной практике, напротив, более «популярным» определением кибервойны, которое обусловлено политическими интересами элиты и возможностью более широкого применения мер кибертерроризма, с другой стороны, рассматривается как инициатива частных лиц, которые действуют от своего имени и не имеют системного характера; 3) ориентация мировых лидеров на военизированное использование возможностей цифровой экономики: например, в США в 2018 году была принята новая версия документа «Национальная стратегия кибербезопасности». В ЕС, например, действуют Таллиннские руководящие принципы по применению международного права к кибероперациям и Закон о кибербезопасности.

В целом, можно сказать, что в научной литературе эти концепции рассматриваются как новый политико-экономический фактор гибридной войны в виртуальном пространстве всемирной сети Интернет.

Далее рассмотрим динамику кибератак на учреждения национальной финансовой системы Российской Федерации с 2016 по 2020 год.

В 2020 году, по сравнению с 2016 годом, количество кибератак увеличилось на 479 единиц, или на 198,0 %, при этом коммерческие банки 2-го уровня являются основной инфраструктурной целью атак (в среднем 65,6 % всех кибератак). Географически основной поток атак на финансовые учреждения исходил от хакерских групп, проживающих в России (45,9 %), на втором месте – иностранные хакерские группы (34,2 %). Опасной тенденцией является увеличение совокупных потерь от кибератак: в 2020 году по сравнению с 2016 годом произошло более чем 8-кратное увеличение потерь, несмотря на устойчивый рост показателя отражения хакерских атак (в 2020 году по сравнению с 2016 годом процент успешно отраженных атак увеличился на 13,2 п. Это позволяет сделать следующий вывод: финансовые учреждения, имеющие опыт противодействия атакам или разрабатывающие собственные бизнес-практики кибербезопасности, входят в число успешных борцов с кибертеррористами. Это подтверждается динамикой уровня возмещения банками убытков от кибератак: в 2020 году по сравнению с 2016 годом он снизился на 7,0 п.п. и составил 11,3 % – незащищенным банкам просто нечем было компенсировать потери.

Анализ структуры атакованных объектов указывает на рост класса и профессионализма хакеров: в 2016–2020 годах наблюдается рост интереса к деструктивному воздействию на инфраструктуру финансового рынка России с последующим ослаблением национальной экономики в целом. В 2020 году на объекты финансовой инфраструктуры пришлось 95,0 % всех атак, тогда как в 2016 году они не превышали 39,0 %; атаки на банковские вебресурсы заняли второе место (в среднем 16,6 %), т. е. хакеры все чаще нацеливаются на хост-объекты, а не на отдельные банковские счета клиентов.

Чтобы лучше понять проблемные области рассмотрим таблицу.

Структура методов кибератак для институтов национальной финансовой системы на 2016–2020 годы, % [4]

Показатели	2016	2017	2018	2019	2020
1. Использование вредоносных	программ 33	37	58	66	65
2. Социальная инженерия	9	12	49	51	50
3. Взлом	12	9	36	14	36
4. Сбор учетных данных (включая инсайдерскую информацию)	23	8	11	14	8
5. Эксплуатация уязвимостей	16	7	5	14	2
6. Ddos-атаки	7	2	3	8	4
7. Другие методы	4	2	1	6	4

По мере развития инфраструктуры финансового рынка в Российской Федерации растет и качественно меняется состав инструментов кибератак: в 2016 году основными инструментами были вредоносные программы (33,0 %) и сбор учетных данных пользователей (23,0 %), тогда как в 2020 году вредоносное ПО (65,0 %) и социальная инженерия (50,0 %) стали абсолютные лидеры, на долю ранее популярного инструмента эксплуатации уязвимостей приходится всего 2,0 %.

В качестве заключения следует отметить, что в настоящее время в России рассматривается вопрос о будущих кибератаках с учетом требований Указа Президента «О Стратегии национальной безопасности Российской Федерации» № 683 от 31.12.2015. Эксперты по прогнозированию сформулировали основные сценарии кибератак на национальную финансовую систему.

Военно-политические амбиции использования цифровых технологий для влияния на международный порядок не рассматриваются в качестве основных целей, а скорее наоборот, для России это имеет более выраженный оборонительный характер, а также инструмент снижения импортозависимости от внешнего мира.

Библиографические ссылки

1. *Негропонте Н.* Быть цифровым Нью-Йорк : Кнопф, 1995. 256 с.

2. *Перритт Дж.* Интернет как угроза суверенитету? Размышления о роли Интернета в укреплении национального и глобального управления // Indiana Journal of Global Legal Studies. 1998. V. 5, 2.

3. *Раухофер Дж., Боуден С.* Защита своих собственных: последствия для фундаментальных прав для суверенитета данных ЕС в облаке. Исследовательская работа Эдинбургской школы права, 2013 год.

4. Кибербезопасность 2019–2020. Тенденции и прогнозы (19.12.2019) [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020 / (дата обращения 21.07.2021).