https://doi.org/10.31107/2075-1990-2021-3-54-66

Киберпреступность как ключевой операционный риск платежно-расчетной инфраструктуры глобальной финансовой системы и подходы к его регулированию в ЕАЭС

Виктор Яковлевич Пищик
E-mail: vpiwik@fa.ru, ORCID: 0000-0002-9013-7670
Финансовый университет при Правительстве Российской Федерации, Москва 125993, Российская Федерация
Петр Викторович Алексеев
E-mail: palekseev@fa.ru, ORCID: 0000-0003-4479-890X
Финансовый университет при Правительстве Российской Федерации, Москва 125993, Российская Федерация

Аннотация
Одним из ключевых направлений формирования общего финансового рынка Евразийского экономического союза (далее также — ЕАЭС, Союз) является развитие общего платежного пространства (ОПП) Союза. В условиях роста и трансформации рисков платежно-расчетной инфраструктуры глобальной финансовой системы (ПРИ ГФС) (санкционного, системного, операционного и других) весьма актуальной является задача эффективной нейтрализации их влияния на платежно-расчетные инфраструктуры стран ЕАЭС. В статье уточнен понятийный аппарат, связанный с трансформацией рисков ПРИ ГФС, проведена их систематизация. Проанализированы источники операционного риска ПРИ ГФС, включая угрозы нарастания киберпреступности.
Авторы полагают, что основным видом операционного риска для ПРИ ГФС в перспективе будут кибератаки с использованием троянских программ, вирусов-шифровальщиков, фишинга, а также блокирование доступа пользователей к интернет-сайтам с помощью DDoS-атак. При этом число DDoS-атак в России уже несколько лет подряд имеет тенденцию роста, который в 2021 г., возможно, еще более усилится за счет ряда факторов, приведенных в статье. Показано, что в России и других странах ЕАЭС рост киберпреступности является одной из основных угроз стабильному функционированию национальных ПРИ и кредитно-финансовых систем в целом. В связи с этим обоснована необходимость развития регионального сотрудничества по вопросам кибербезопасности в рамках ЕАЭС с использованием опыта Европейского союза, где этой проблеме уделяется весьма серьезное внимание. Наряду с этим целесообразно наращивание международного сотрудничества стран мира на площадке ООН с целью повышения уровня кибербезопасности при использовании ПРИ ГФС всеми субъектами мировой экономики и обеспечения успешного развития ОПП ЕАЭС.

Ключевые слова: *Евразийский экономический союз, общее платежное пространство, платежно-расчетная инфраструктура, глобальная финансовая система, трансформация рисков, киберпреступность, кибербезопасность*

JEL: *F36, G15*

Благодарности: *статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансового университета при Правительстве Российской Федерации.*

Для цитирования: *Пищик В. Я., Алексеев П. В. Киберпреступность как ключевой операционный риск платежно-расчетной инфраструктуры глобальной финансовой системы и подходы к его регулированию в ЕАЭС // Финансовый журнал. 2021. Т. 13. № 3. С. 54–66. https://doi.org/10.31107/2075-1990-2021-3-54-66.*

https://doi.org/10.31107/2075-1990-2021-3-54-66

Cybercrime as a Key Operational Risk of the Payment and Settlement Infrastructure of the Global Financial System and Approaches to Its Regulation in the Eurasian Economic Union

Victor Ya. Pishchik[1], ***Peter V. Alekseev***[2]
[1,2] *Financial University under the Government of the Russian Federation, Moscow 125993, Russian Federation*
[1] *vpiwik@fa.ru, https://orcid.org/0000-0002-9013-7670*
[2] *palekseev@fa.ru, https://orcid.org/0000-0003-4479-890X*

Abstract
One of the key areas in the formation of a single financial market within the Eurasian Economic Union (hereinafter, EAEU or Union) is the development of a single payment space (SPS) of the Union. In the context of growth and transformation of the risks of the payment and settlement infrastructure (PSI) of the global financial system (GFS) (sanctions, systemic, operational and other risks), the problem of effectively neutralizing their impact on the PSI of the EAEU countries is highly topical. The article clarifies the conceptual apparatus associated with the transformation of risks for the PSI of the GFS, and carries out their systematization. Sources of operational risk of the GFS's PSI, including the threat of an increase in cybercrime, are analyzed. The authors assert that the main type of operational risk for the PSI of the GFS in the future will evidently be cyberattacks using trojans, ransomware viruses and phishing, as well as blocking user access to Internet sites using DDoS attacks. Nowadays, the number of DDoS attacks in Russia has been growing for several years in a row, and this growth may intensify in 2021 due to a number of factors set out in the article. It is indicated that, in Russia and other EAEU countries, growth in cybercrime is one of the main threats to the stable functioning of the national PSI as well as credit and financial systems in general. In this regard, the article substantiates the need to develop regional cooperation on cybersecurity issues within the EAEU using the experience of the European Union, where this issue is paid very serious attention. Besides, it is advisable to build up international cooperation between the countries of the world within the UN in order to enhance the cybersecurity of the GFS's PSI and ensure the successful development of the SPS in the EAEU.

Keywords: *Eurasian Economic Union, single payment space, payment and settlement infrastructure, global financial system, risk transformation, cybercrime, cybersecurity*

JEL: *F36, G15*

Acknowledgments: *The article was prepared based on the results of research carried out at the expense of budget funds within a state contract of the Financial University.*

For citation: *Pishchik V.Ya., Alekseev P.V. Cybercrime as a Key Operational Risk of the Payment and Settlement Infrastructure of the Global Financial System and Approaches to Its Regulation in the Eurasian Economic Union. Financial Journal, 2021, vol. 13, no. 3, pp. 54–66 (In Russ.). https://doi.org/10.31107/2075-1990-2021-3-54-66.*

ВВЕДЕНИЕ

Необходимым условием успешной финансово-экономической интеграции государств — членов ЕАЭС является развитие общего платежного пространства (ОПП) ЕАЭС, предусмотренное Концепцией формирования общего финансового рынка Евразийского экономического союза[1] и Стратегическими направлениями развития евразийской экономической интеграции на период до 2025 г.[2]

Теоретические, методологические и практические вопросы, связанные с созданием, развитием и интеграцией платежно-расчетных систем, рассмотрены в работах отечественных ученых: М. А. Абрамовой [Абрамова М. А. и др., 2016], А. А. Бердюгина [Бердюгин А. А., 2018], Е. А. Звоновой [Звонова Е. А., 2016], Л. Н. Красавиной [Красавина Л. Н., 2019], С. В. Криворучко и В. А. Лопатина [Криворучко С. В., 2004; Криворучко С. В., Лопатин В. А., 2013, 2017, 2018], Л. В. Лямина [Лямин Л. В., 2012], А. И. Смирнова [Смирнов А. И., 2014], П. А. Тамарова [Тамаров П. А., 2020], М. А. Эскиндарова [Эскиндаров М. А. и др., 2018], а также зарубежных исследователей С. Бауэра, Э. Бернройдера, К. Чудзиковского [Bauer S. et al., 2017], Т. Кокколы [Kokkola T., 2010], Х. Лейнонена [Leinonen H., 2005] и многих других. Тем не менее в целом данная проблематика исследована недостаточно.

Перспективы развития ОПП ЕАЭС будут во многом определяться последствиями происходящей в современных условиях трансформации рисков платежно-расчетной инфраструктуры глобальной финансовой системы. Для рассмотрения данной трансформации определим базовые понятия, связанные с ней.

Платежно-расчетная инфраструктура (ПРИ) страны, по нашему мнению, — это комплекс взаимосвязанных организаций страны (центральный (национальный) банк, кредитные и некредитные организации), обеспечивающих осуществление расчетов и платежей между экономическими субъектами. В число этих организаций входят операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры, операторы услуг информационного обмена и другие.

Платежно-расчетная инфраструктура глобальной финансовой системы (ПРИ ГФС) — это совокупность платежно-расчетных инфраструктур всех стран мира.

Риск ПРИ ГФС — это вероятность наступления убытков или иных нежелательных последствий для участников ПРИ ГФС.

Киберпространство — это сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов интернета и других телекоммуникационных сетей, технологической инфраструктурой, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства).

Кибербезопасность можно определить как совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

Киберпреступность, по нашему мнению, — это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Цель настоящей статьи — выявить основные риски платежно-расчетных инфраструктур государств — членов ЕАЭС на основе систематизации и анализа источников и видов

---

[1] *Концепция формирования общего финансового рынка Евразийского экономического союза (утв. решением Высшего Евразийского экономического совета от 1 октября 2019 г. № 20). URL: http://www.eurasiancommission.org.*

[2] *Стратегические направления развития евразийской экономической интеграции на период до 2025 г. (утв. решением Высшего Евразийского экономического совета от 11 декабря 2020 г. № 12). URL: http://www.eurasiancommission.org.*

рисков ПРИ ГФС и разработать подходы к их регулированию. Для достижения этой цели проведем систематизацию и определим основные направления трансформации рисков платежно-расчетной инфраструктуры, а также основные источники операционных рисков ПРИ ГФС.

СИСТЕМАТИЗАЦИЯ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ТРАНСФОРМАЦИИ РИСКОВ ПРИ ГФС

В условиях роста геополитических противоречий и напряженности происходит трансформация рисков ПРИ ГФС по линии роста санкционного, системного и операционного рисков, при этом сохраняется значительная роль кредитного риска, риска ликвидности, общего коммерческого, депозитарного, инвестиционного риска.

В табл. 1 систематизированы и определены риски ПРИ ГФС на основе международных стандартов («Основополагающих принципов для системно значимых платежных систем»[3], разработанных Комитетом по платежам и рыночным инфраструктурам (КПРИ) Банка международных расчетов, и «Принципов для инфраструктур финансового рынка»[4], разработанных КПРИ совместно с Техническим комитетом Международной организации комиссий по ценным бумагам).

Таблица 1

Риски платежно-расчетной инфраструктуры глобальной финансовой системы / Risks of the payment and settlement infrastructure in the global financial system

№	Риски	Определение риска
1	Правовой риск	Вероятность убытков участников ПРИ ГФС вследствие непредвиденного изменения законодательства, других нормативных правовых актов или их неправильного применения
2	Санкционный риск	Вероятность убытков участников ПРИ ГФС в результате международных ограничительных санкций (разновидность правового риска)
3	Системный риск	Вероятность нарушения функционирования ПРИ ГФС в результате невыполнения одним или несколькими ее участниками их денежных обязательств, что может вызвать цепную реакцию неплатежей
4	Операционный риск	Вероятность того, что недостатки информационных систем или внутренних процессов, человеческие ошибки, сбои или нарушения в управлении вследствие внешних событий, действия киберпреступников приведут к нарушению функционирования ПРИ ГФС
5	Кредитный риск	Вероятность невыполнения участниками ПРИ ГФС своих финансовых обязательств в полном объеме и в установленный срок
6	Риск ликвидности	Вероятность того, что участник ПРИ ГФС не будет иметь достаточных средств для выполнения своих финансовых обязательств в полном объеме и в установленный срок
7	Общий коммерческий риск	Вероятность ухудшения финансового положения ПРИ ГФС (как экономического субъекта) вследствие уменьшения ее доходов и/или увеличения расходов
8	Депозитарный риск	Вероятность потери депонированного актива в случае несостоятельности, халатности, мошенничества, неудовлетворительного управления или неадекватного учета актива депозитарием (субдепозитарием)
9	Инвестиционный риск	Вероятность потерь, которым подвергается ПРИ ГФС, когда инвестирует собственные ресурсы или ресурсы своих участников

Источник: составлено авторами на основе: Principles for financial market infrastructures / BIS, 2012 (https://www.bis.org/cpmi/publ/d101a.pdf); Core Principles for Systematically Important Payment Systems / BIS, 2001 (https://www.bis.org/cpmi/publ/d43.pdf) / Source: composed by the authors based on the international standards.

[3] *Core Principles for Systematically Important Payment Systems / Committee on Payment and Settlement Systems. BIS, 2001. URL: https://www.bis.org/cpmi/publ/d43.pdf.*

[4] *Principles for Financial Market Infrastructures / Committee on Payment and Settlement Systems; Technical Committee of the International Organization of Securities Commissions. BIS, IOSCO, 2012. URL: https://www.bis.org/cpmi/publ/d101a.pdf.*

Наибольшую опасность для стабильного функционирования современной ПРИ ГФС представляет усиление санкционного, системного и операционного рисков. Увеличение каждого из них обусловлено множеством факторов. Так, по мнению профессора С. В. Криворучко, рост системного риска обусловлен изменениями в информационных технологиях, деятельности участников ПРИ, рыночной среде и другими факторами [Криворучко С. В., 2004, с. 23]. В условиях нарастания геополитической напряженности в современном мире особую опасность для устойчивого функционирования ПРИ ГФС и ПРИ России как ее составной части представляет санкционный риск — вероятность убытков участников ПРИ в результате международных ограничительных санкций. Например, возможное отключение России и других подпавших под санкционный режим стран от международной системы передачи финансовых сообщений SWIFT может привести к платежному кризису на национальном и региональном уровнях и повлечь за собой обострение системного риска ПРИ ГФС. Реализация санкционных рисков наносит значительный ущерб национальной экономике. Как отметил Президент РФ В. В. Путин в интервью информационному агентству ТАСС 16 марта 2020 г., общий ущерб для российской экономики от западных санкций составил около 50 млрд долл. США, однако Россия смогла их компенсировать, в том числе благодаря импортозамещению[5].

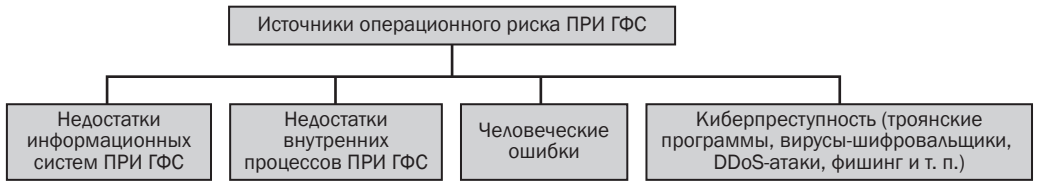
Сегодня актуальной проблемой глобальной финансовой системы является рост операционных рисков ПРИ ГФС, прежде всего за счет обострения угрозы киберпреступности. В связи с этим рассмотрим угрозу киберпреступности как ключевой операционный риск ПРИ ГФС.

КИБЕРПРЕСТУПНОСТЬ КАК КЛЮЧЕВОЙ ОПЕРАЦИОННЫЙ РИСК ПРИ ГФС

Сегодня киберпреступность является ключевым, но не единственным источником операционного риска ПРИ ГФС. Основные его источники представлены на рис. 1.

Рисунок 1

Основные источники операционного риска ПРИ ГФС /
Main sources of operational risk of the PRI GFS



Источник: составлено авторами / Source: composed by the authors.

По мнению Министра иностранных дел Российской Федерации С. В. Лаврова, увеличение масштабов киберпреступности является «киберпандемией», которая проявляется не только в виде посягательства на частную жизнь рядовых граждан, но и в «нападениях» на объекты здравоохранения, финансовые, образовательные структуры, международные организации. Преступная активность в онлайн-режиме, входящая согласно рейтингу Всемирного экономического форума в пятерку глобальных рисков, угрожает существованию и успешному функционированию целых отраслей. Как считает С. В. Лавров, «в отсутствие универсального международного “кодекса поведения” в киберсфере устойчивое

[5] *Интервью Президента РФ В. В. Путина информационному агентству ТАСС. 16.03.2020. URL: https://tass.ru/ekonomika/7987569.*

социально-экономическое и научно-техническое развитие всех без исключения стран становится уязвимым. Человечество рискует быть втянутым в опасную масштабную конфронтацию в онлайн-пространстве, которую невозможно будет удержать в локальных рамках в силу трансграничности современных средств коммуникаций и взаимозависимости национальных экономик» [Лавров С. В., 2020].

Как считают О. А. Юсупова и М. И. Горохова, риски киберпреступности реализуются в действиях, нарушающих конфиденциальность, доступность и целостность компьютерных данных. К этим действиям относятся: незаконный доступ, осуществленный с помощью взлома или обмана, получение компьютерных данных нелегальным путем, умышленное вмешательство в данные, подразумевающее их уничтожение, изменение, ухудшение или сокрытие, системные вмешательства, подразумевающие сознательное создание проблем в функционировании компьютерных систем, изготовление, приобретение и распространение инструментов совершения киберпреступлений и другое [Юсупова О. А., Горохова М. И., 2020, с. 3].

По мнению профессора Ю. Н. Жданова, кибератаки с кражей конфиденциальных данных людей стали одним из главных рисков для развития глобальной экономики, который представляет больше опасности, чем техногенные катастрофы и эпидемии. По его оценке, мировая экономика в 2022 г. может потерять от деятельности кибермошенников до 8 трлн долл. США, а в 2030-м — уже 90 трлн долл. [Авраменко Е., 2020].

В настоящее время подавляющее большинство киберпреступлений во всем мире совершается против кредитно-финансовых организаций, на которые, по нашим оценкам, приходится около 70 % всей хакерской активности. В целом киберпреступность сегодня является одним из ключевых операционных рисков ПРИ стран ЕАЭС.

В 2018 г. Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России (ФинЦЕРТ) получены сведения о 687 атаках, в том числе о 177 целевых[6] атаках, осуществленных на кредитно-финансовые организации России [Банк России, 2019а, с. 5].

В последнее время отмечается значительное увеличение количества DDoS-атак (*Distributed Denial of Service*, распределенная атака типа «отказ в обслуживании») на кредитно-финансовые организации. DDoS-атака является компьютерной атакой из одного источника, которая предполагает блокирование доступа пользователей к определенному интернет-сайту в результате намеренной «перегрузки» количества направляемых на него сообщений. В течение 2018 г. ФинЦЕРТом были получены сведения о 97 DDoS-атаках на кредитно-финансовые организации России [Банк России, 2019а, с. 5].

В отчете компании «Ростелеком-Солар», посвященном исследованию особенностей и масштабов DDoS-атак в период пандемии COVID-19, отмечается, что «... в целом DDoS с каждым годом становятся все популярнее у злоумышленников из-за простоты применения и низкой стоимости его организации» [Ростелеком-Солар, 2020, с. 4]. По данным «Лаборатории Касперского», с июля по сентябрь 2020 г. количество DDoS-атак по всем мире возросло в полтора раза по сравнению с соответствующим периодом 2019 г. Кроме того, в третьем квартале был установлен годовой рекорд по числу DDoS-атак в день (так, 2 июля 2020 г. программы компании зарегистрировали 323 атаки; предыдущий рекорд, 298 атак в день, был зарегистрирован 1 апреля 2020 г.)[7].

---

[6] *В контексте настоящей статистики под целевыми атаками специалистами ФинЦЕРТа подразумеваются атаки, направленные на получение финансовой выгоды и затрагивающие организации кредитно-финансовой сферы.*

[7] *«Лаборатория Касперского»: количество DDoS-атак в третьем квартале 2020 г. выросло в полтора раза. 29.10.2020. URL: https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-kolichestvo-ddos-atak-v-tretem-kvartale-2020-goda-viroslo-v-poltora-raza.*

По прогнозу компании StormWall, в 2021 г. количество DDoS-атак на онлайн-ресурсы компаний в России увеличится примерно на 20 % по сравнению с 2020 г. Число DDoS-атак уже несколько лет подряд имеет тенденцию роста, который в 2021 г. еще более усилится за счет ряда факторов:

— увеличение количества начинающих киберпреступников среди студентов и школьников в связи с организацией дистанционного обучения во время пандемии COVID-19;

— рост числа пользователей интернета во всем мире;

— активное развитие онлайн-бизнеса[8].

В последние годы в мире значительно обострились риски ПРИ, связанные с использованием злоумышленниками таких видов вредоносного программного обеспечения (ВПО), как троянские программы[9], вирусы-шифровальщики[10], фишинг. Эксперты ФинЦЕРТа отмечают стабильно высокий уровень использования данных программ в России с целью кражи данных с персональных компьютеров, а также средств со счетов в банках [Банк России, 2019b, с. 40].

Согласно отчету компании Check Point Research, работающей в сфере информационной безопасности, троянская программа Qbot в августе 2020 г. впервые вошла в мировой рейтинг самых распространенных видов ВПО, заняв в нем десятое место. Программа Qbot была впервые обнаружена специалистами в 2008 г., и с этого времени она эволюционировала из обычного трояна для кражи данных в универсальный инструмент, используемый киберпреступниками. В настоящее время Qbot способен, например, доставлять в зараженную систему другие виды ВПО, а также подключаться к целевой системе, чтобы осуществлять банковские транзакции, используя IP-адрес[11] жертвы. Как правило, Qbot распространяется классическим способом: посредством фишинговых писем, которые содержат опасные вложения или заманивают пользователей на подконтрольные киберпреступникам вредоносные сайты. При этом программа может похищать электронные письма своих жертв, а затем использовать их для рассылки спама, тем самым создавая более правдоподобные письма для введения в заблуждение пользователей. В период с марта по август 2020 г. исследователи Check Point обнаружили несколько кампаний с использованием Qbot.

По мнению руководителя компании Check Point Research В. В. Дягилева, «злоумышленники всегда ищут способы усовершенствовать ВПО. Сейчас они, по-видимому, вкладывают значительные средства в создание более продвинутых версий Qbot, которые можно будет использовать для массовых краж данных организаций и физических лиц». Согласно мировому рейтингу наиболее распространенных видов ВПО, в августе 2020 г. троян Emotet оставался самым распространенным ВПО в мире, за ним следуют трояны Agent Tesla и Formbook[12].

Согласно отчету Check Point, в январе 2021 г. одним из наиболее опасных видов ВПО был троян Fareit, впервые обнаруженный в 2012 г. Его разновидности похищают пароли

---

[8] *Число DDoS-атак на онлайн-ресурсы компаний в 2021 году увеличится минимум на 20 % / Tadviser, 30.03.2021. URL: https://www.tadviser.ru/index.php/Статья:DDoS-атаки_в_России.*

[9] *Троянские программы (англ. trojans) — вредоносные компьютерные программы, содержащие скрытый код. Обычно трояны маскируются под «здоровые» программы, необходимые для работы. Название произошло от древнегреческого мифа.*

[10] *Вирусы-шифровальщики (вирусы-вымогатели, англ. ransomware) — вредоносные компьютерные программы, осуществляющие скрытное шифрование компьютерной информации пользователя с целью вымогательства денежных средств за расшифровку, а также кибершпионаж и кражу данных с компьютеров.*

[11] *IP-адрес (от англ. Internet Protocol) — это уникальный числовой идентификатор устройства в компьютерной сети.*

[12] *August 2020's Most Wanted Malware: Evolved Qbot Trojan Ranks on Top Malware List for First Time. 09.09.2020. URL: https://blog.checkpoint.com/2020/09/09/august-2020s-most-wanted-malware-evolved-qbot-trojan-ranks-on-top-malware-list-for-first-time.*

и личные данные пользователей, хранящиеся в браузерах. Он способен устанавливать другие вредоносные программы на зараженные устройства[13].

По данным исследовательского центра Cybersecurity Ventures, в 2016 г. каждые 40 секунд предприятия в мире становились жертвой атаки с использованием вируса-шифровальщика. По прогнозу центра, в 2021 г. этот временной интервал сократится до 11 секунд [Herjavec Group, 2019]. По оценкам компании Group-IB, совокупный ущерб от вирусов-шифровальщиков в мире превысил в 2020 г. 1 млрд долл. США. При этом против компаний США в 2020 г. было направлено около 60 % всех атак, Европы — 20 %, Северной и Южной Америки — 10 %, Азии — 7 %, остальных стран — 3 %. В пятерку отраслей, которые чаще всего подвергаются атакам «шифровальщиков», входят: сферы производства и розничной торговли, государственные учреждения, здравоохранение, строительство[14].

Значительные масштабы имеет также такой вид киберпреступности, как фишинг (англ. *phishing*) — вид мошенничества в интернете, целью которого является получение каких-либо конфиденциальных данных пользователей. За 2018 г. компанией Group-IB было обнаружено и проанализировано более 1,9 млн уникальных фишинговых ссылок, что на 85 % больше, чем в 2017 г. Более 26 % из них приходится на финансовый сектор. При этом финансовый фишинг был направлен в основном против компаний США (48 % всех атак). Последующие места занимают Нидерланды (4,7 %), Германия (4,51 %) и Россия (4,46 %). Основной способ привлечения пользователей на фишинговые страницы — это перенаправление посетителей со взломанных сайтов, а также попадание мошеннических ресурсов в поисковую выдачу [Банк России, 2019, с. 5].

Проведенный анализ позволяет сделать вывод, что, по всей вероятности, наибольшую опасность для стабильного функционирования ПРИ стран ЕАЭС будут представлять риски киберпреступности, связанные с использованием троянских программ, вирусов-шифровальщиков, фишинга, а также блокирование доступа пользователей к интернет-сайтам кредитно-финансовых институтов с помощью DDoS-атак. Также большое значение сохранят другие риски функционирования ПРИ стран ЕАЭС. В связи с вышеизложенным рассмотрим подходы к регулированию рисков ПРИ в ЕАЭС, прежде всего рисков киберпреступности.

ПОДХОДЫ К РЕГУЛИРОВАНИЮ РИСКОВ КИБЕРПРЕСТУПНОСТИ В ЕАЭС

Очевидно, что эффективная нейтрализация рисков устойчивого функционирования платежно-расчетных инфраструктур имеет решающее значение для обеспечения стабильности всей глобальной финансовой системы. В условиях обострения рисков функционирования ПРИ, особенно рисков киберпреступности, необходимым условием поддержания финансовой стабильности является соответствие ПРИ ГФС международным стандартам. К ним относятся прежде всего «Основополагающие принципы для системно значимых платежных систем»[15], разработанные Комитетом по платежам и рыночным инфраструктурам Банка международных расчетов, «Принципы для инфраструктур финансового рынка»[16], разработанные КПРИ совместно с Техническим комитетом Международной организации комиссий по ценным бумагам, а также «Руководство по киберустойчивости для

---

[13] *Check Point: самое активное вредоносное ПО января 2021 года / Информационная безопасность, 18.02.2021. URL: http://www.itsec.ru/news/check-point-samoye-aktivnoye-vredonosnoye-po-yanvaria-2021.*

[14] *Ущерб от вирусов-вымогателей в мире превышает $1 млрд в год. 26.11.2020. URL: https://www.tadviser.ru.*

[15] *Core Principles for Systematically Important Payment Systems / Committee on Payment and Settlement Systems. BIS, 2001.*

[16] *Principles for Financial Market Infrastructures / Committee on Payment and Settlement Systems, Technical Committee of the International Organization of Securities Commissions. BIS, IOCSO, 2012.*

инфраструктур финансового рынка»[17], разработанное КПРИ совместно с Международной организацией комиссий по ценным бумагам.

В Российской Федерации, как и в других государствах — членах ЕАЭС, правовое регулирование национальной платежной системы (НПС) осуществляется с учетом международных стандартов. Так, ст. 22, 23, 24 Закона РФ от 27.06.2011 № 161-ФЗ «О национальной платежной системе» предусмотрено выявление системно и социально значимых платежных систем и следование стандартам наилучшей международной практики, подлежащее оценке со стороны Банка России в рамках функции наблюдения в НПС[18]. В качестве такого документа Банком России приняты стандарты «Принципы для инфраструктур финансового рынка», применяемые в отношении системно и социально значимых платежных систем.

Аналогичные изменения произошли и в других странах ЕАЭС, однако вопрос о соотношении и соответствии количественных и качественных критериев их значимости требует рассмотрения. Как считает П. А. Тамаров, в целом он связан с характеристиками субъектного состава НПС в различных странах и их гармонизацией в целях единообразного подхода национальных центральных банков к осуществлению контрольных функций в НПС (платежного оверсайта). В связи с этим необходима гармонизация национальных законодательств стран ЕАЭС в сфере платежных систем на основе международных стандартов в данной области [Тамаров П. А., 2020, с. 235].

Для успешного развития ОПП ЕАЭС необходимы разработка и развитие нормативного правового обеспечения данного процесса, в том числе в рамках формирования общего финансового рынка Союза. В связи с этим необходимо ускорить разработку и принятие конкретного плана мероприятий («дорожной карты») по реализации положений Концепции формирования общего финансового рынка ЕАЭС, утвержденной решением Высшего Евразийского экономического совета от 1 октября 2019 г. № 20. В данный план целесообразно включить конкретные меры и механизмы управления возникающими рисками платежно-расчетной инфраструктуры, в первую очередь угрозами киберпреступности.

Одной из важных проблем обеспечения кибербезопасности в ЕАЭС является отсутствие единого правового регулирования в данной области. Необходимо комплексное решение этой проблемы во всех сферах финансово-экономической деятельности государств — членов ЕАЭС, включая функционирование платежно-расчетных инфраструктур. В связи с этим необходимо тесное региональное сотрудничество по вопросам кибербезопасности. Важно при этом учитывать позитивный опыт обеспечения кибербезопасности в Европейском союзе. В 2004 г. в ЕС было создано Европейское агентство по сетевой и информационной безопасности (*European Union Agency for Cybersecurity*, ENISA) с целью достижения в нем высокого общего уровня кибербезопасности[19]. В 2016 г. Европарламент принял Директиву 2016/1148 «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза»[20], в которой закреплены вопросы обеспечения кибербезопасности критической информационной инфраструктуры ЕС (в том числе на рынке финансовых услуг).

---

[17] *Guidance on Cyber Resilience for Financial Market Infrastructures / Committee on Payment and Settlement Systems, Board of the International Organization of Securities Commissions. BIS, IOSCO, 2016.*

[18] *Закон РФ от 27.06.2011 № 161 «О национальной платежной системе» (с изменениями и дополнениями). URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102148779.*

[19] *URL: https://www.enisa.europa.eu/about-enisa.*

[20] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.*

Назрела необходимость принятия в рамках ЕАЭС согласованного концептуального документа по обеспечению кибербезопасности государств — членов Союза, в котором следует акцентировать внимание на следующих направлениях:

— разработка общего понятийного аппарата в области кибербезопасности, включающего единые определения терминов «киберугроза», «кибербезопасность», «киберпреступление» и связанных с ними понятий;

— формирование единых стандартизированных подходов к вопросам обеспечения кибербезопасности, киберустойчивости и к надзору за соответствующими рисками;

— согласование порядка обеспечения строгой идентификации клиентов при осуществлении транзакций и переводов денежных средств;

— координация политики и разработка коллективных механизмов обеспечения защиты прав потребителей в случае совершения несанкционированных транзакций и переводов денежных средств в результате кибератак.

В институциональном плане для развития регионального сотрудничества по предотвращению киберпреступности в рамках ЕАЭС целесообразно рассмотреть вопрос о создании Евразийского агентства по информационной безопасности как аналога Европейского агентства по сетевой и информационной безопасности.

Наряду с развитием регионального сотрудничества по вопросам кибербезопасности в рамках ЕАЭС необходимо наращивание международного сотрудничества стран мира на площадке Организации Объединенных Наций с целью разработки универсального международного кодекса поведения в киберсфере. Разработка и принятие такого кодекса в рамках ООН окажет содействие повышению уровня кибербезопасности при использовании ПРИ ГФС всеми субъектами мировой экономики и успешному развитию ОПП ЕАЭС.

ЗАКЛЮЧЕНИЕ

Резюмируя вышеизложенное, можно сделать следующие выводы.

1. В условиях роста геополитических противоречий и напряженности происходит трансформация рисков для ПРИ ГФС, связанная с обострением санкционного, системного и операционного рисков, при этом сохраняется значительная роль кредитного риска, риска ликвидности, общего коммерческого, депозитарного, инвестиционного риска.

2. Существенную угрозу для стабильного функционирования ПРИ ГФС представляет усиление операционных рисков, прежде всего вследствие увеличения масштабов киберпреступности в России, в рамках ЕАЭС и во всем мире.

3. Вероятнее всего, наибольшую опасность для стабильного функционирования ПРИ стран ЕАЭС будут представлять риски киберпреступности, связанные с использованием троянских программ, вирусов-шифровальщиков, фишинга, а также блокированием доступа пользователей к интернет-сайтам кредитно-финансовых институтов с помощью DDoS-атак.

4. При создании стабильной и эффективной ПРИ в рамках ЕАЭС важное значение имеет развитие регионального сотрудничества по вопросам обеспечения кибербезопасности. Для повышения его эффективности целесообразно использовать накопленный опыт Европейского союза в этой сфере межстранового взаимодействия. Предлагается в разрабатываемый в настоящее время в ЕАЭС план реализации положений Концепции формирования общего финансового рынка Евразийского экономического союза включить конкретные меры и механизмы управления возникающими рисками платежно-расчетной инфраструктуры, в первую очередь угрозами киберпреступности.

5. В институциональном плане для развития регионального сотрудничества по предотвращению киберпреступности в рамках ЕАЭС целесообразно рассмотреть вопрос о создании Евразийского агентства по информационной безопасности как аналога Европейского агентства по сетевой и информационной безопасности.

6. Необходимо наращивание международного сотрудничества стран мира на площадке ООН с целью разработки и принятия универсального международного кодекса поведения в киберсфере, что окажет содействие повышению уровня кибербезопасности при использовании ПРИ ГФС всеми субъектами мировой экономики и успешному развитию ОПП ЕАЭС.

Список источников

Абрамова М. А., Дубова С. Е., Криворучко С. В. и др. Гармонизация монетарной политики стран — членов ЕАЭС: возможности и перспективы: моногр. М.: Русайнс, 2016. 196 с.

Авраменко Е. Киберпреступность признали большей опасностью, чем эпидемии и техногенные катастрофы / Федеральное агентство новостей, 19.02.2020. URL: https://riafan.ru/1252056-kiberprestupnost-priznali-bolshei-opasnostyu-chem-epidemii-i-tekhnogennye-katastrofy.

Бердюгин А. А. Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. № 1. С. 28–38.

Звонова Е. А., Ершов М. В., Кузнецов А. В. и др. Реформирование мировой финансовой архитектуры и российский финансовый рынок: моногр. / Под ред. Е. А. Звоновой. М.: Русайнс, 2016. 430 с.

Криворучко С. В. Риски платежных систем: кредитный, ликвидности, правовой // Экономика, статистика и информатика. 2004. № 3. С. 17–27.

Криворучко С. В., Лопатин В. А. Национальная платежная система: структура, технологии, регулирование. Международный опыт, российская практика. М.: КноРус: ЦИПСиР, 2013. 456 с.

Криворучко С. В., Лопатин В. А. Особенности бизнес-моделей на рынке платежных услуг // Эффективное антикризисное управление. 2017. № 4. С. 35–40.

Криворучко С. В., Лопатин В. А. Влияние имплементации открытого банкинга на развитие национального сектора Финтех // Экономика. Налоги. Право. 2018. № 6. С. 80–86.

Лавров С. В. Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью // Внешнеэкономические связи. 2020. № 9. URL: https://eer.ru/sites/default/files/pdf/eer_1_2020.pdf.

Лямин Л. В. Принципы организации внутреннего аудита в условиях электронного банкинга // Банковское дело. 2012. № 5. С. 51–54.

Международные валютно-кредитные и финансовые отношения: учебник для академического бакалавриата / Отв. ред. Л. Н. Красавина. 5-е изд., перераб. и доп. М.: Юрайт, 2019. 534 с.

Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 г. / Банк России, 2019a. URL: https://cbr.ru/Collection/Collection/File/32085/DIB_2018_20190704.pdf.

Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности Банка России. 01.09.2018–31.08.2019 / Банк России, 2019b. URL: https://cbr.ru/Collection/Collection/File/32087/FINCERT_report_20191010.PDF.

DDoS-атаки в период COVID-19 / Ростелеком-Солар, 2020. URL: https://rt-solar.ru/upload/iblock/307/DDoSCOVID.PDF.

Смирнов А. И. Григорьев В. Р., Кохтюлина И. Н. и др. Глобальная безопасность в цифровую эпоху: стратагемы для России: моногр. / Под общ. ред. А. И. Смирнова. М.: ВНИИгеосистем, 2014. 394 с.

Тамаров П. А. Перспективы платежной системы ЕАЭС / Большая Евразия: развитие, безопасность, сотрудничество. Ежегодник. Вып. 3. Ч. 1. С. 231–236. М.: ИНИОН РАН, 2020.

Эскиндаров М. А., Абрамова М. А., Масленников В. В. и др. Направления развития финтеха в России: экспертное мнение Финансового университета // Мир новой экономики. 2018. № 2. С. 48–55. URL: https://doi.org/10.26794/2220-6469-2018-12-2-6-23.

Юсупова О. А., Горохова М. И. Киберпреступность в банковской сфере: современное состояние и способы защиты // Научный электронный журнал «Меридиан». 2020. № 9 (43). С. 1–4.

Bauer S., Bernroider E. W. N., Chudzikowski K. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks // Computer & Security. 2017. July. Vol. 68. P. 145–159. URL: https://doi.org/10.1016/j.cose.2017.04.009.

Kokkola T. Payment System / European Central Bank, 2010. 360 p.

Leinonen H. (ed.) Liquidity, risk and speed in payment and settlement systems — a simulation approach / Bank of Finland. Studies: E: 31. 2005. 350 p.

Official Annual Cybercrime Report / Herjavec Group, 2019. URL: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.

References

Abramova M.A., Dubova S.E., Krivoruchko S.V. et al. (2016). Harmonization of Monetary Policy of the EAEU Member States: Opportunities and Perspectives: Monograph. Moscow: Ru-Science Publ., 2016, 196 p. (In Russ.).

Avramenko E. (2020). Cybercrime Recognized as Greater Danger Than Epidemics and Technological Disasters. Federal News Agency, 19.02 (In Russ.). Available at: https://riafan.ru/1252056-kiberprestUnost-priznali-bolshei-epasnostyu-chem-epidemii-i-tekhnogennye-katastrofy.

Bank of Russia (2019a). Review of the Main Types of Computer Attacks in the Credit and Financial Sector in 2018 (In Russ.). URL: https://cbr.ru/Collection/Collection/File/32085/DIB_2018_20190704.pdf.

Bank of Russia (2029b). Report of the Center for Monitoring and Response to Computer Attacks in the Credit and Financial Sector of the Information Security Department of the Bank of Russia. 09.09.2018–31.08.2019 (In Russ.). URL: https://cbr.ru/nalytics/Ib/Fincert.

Bauer S., Bernroider E.W.N., Chudzikowski K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computer & Security*, vol. 68, pp. 145–159. Available at: https://doi.org/10.1016/j.cose.2017.04.009.

Berdyugin A.A. (2018). Information Security Risk Management in the Context of Electronic Banking. Risk Management of Information Security Violation in Conditions of Electronic Banking. *Voprosy kiberbezopasnosti — Cybersecurity Issue*, no. 1, pp. 28–38 (In Russ.).

DDoS Attacks in the Period of COVID-19. Rostelecom-Solar (In Russ.). URL: https://rt-solar.ru/analytics/Reports.

Eskindarov M.A., Abramova M.A., Maslennikov V.V. et al. (2018). Directions of Fintech Development in Russia: Expert Opinion of the Financial University. *Mir novoi ekonomiki — World of New Economy*, no. 2. pp. 48–55 (In Russ.). Available at: https://doi.org/10.26794/2220-6469-2018-12-2-6-23.

Herjavec Group (2019). Official Annual Cybercrime Report. URL: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.

Krasavina L.N. (ed.) (2019). International Monetary, Credit and Financial Relations: Textbook for Academic Bachelor's Degree, 5th ed. Moscow: Yurait, 534 p. (In Russ.).

Kokkola T. Payment System. European Central Bank, 2010, 360 p.

Krivoruchko S.V. (2004). Risks of Payment Systems: Credit, Liquidity, Legal. *Ekonomika, statistika i informatika — Economics, Statistics and Informatics*, no. 3, pp. 17–27 (In Russ.).

Krivoruchko S.V., Lopatin V.A. (2017). Features of Business Models in the Market of Payment Services. *Effektivnoe antikrizisnoe upravlenie — Strategic Decisions and Risk Management*, no. 4, pp. 35–40 (In Russ.).

Krivoruchko S.V., Lopatin V.A. (2013). National Payment System: Structure, Technology, Regulation. International experience, Russian practice. Moscow: KnoRus Publ., 456 p. (In Russ.).

Krivoruchko S.V., Lopatin V.A. (2018). The Impact of the Open Banking Implementation on the Development of the National FinTech Sector. *Ekonomika. Nalogi. Pravo — Economics. Taxes. Law*, no. 6, pp. 80–86 (In Russ.).

Lavrov S.V. (2020). Global Cyber Security Challenges and Russia's Initiatives to Fight Cyber Crime. *Vneshneekonomicheskie svyazi — External Economic Relations*, no. 9 (In Russ.). URL: https://eer.ru/article/gosudarstvo/u79/2020/09/28/2944.

Leinonen H. (ed.) Liquidity, risk and speed in payment and settlement systems — a simulation approach. Bank of Finland. Studies: E: 31, 2005, 350 p.

Lyamin L.V. (2012). The Principles of Organizing Internal Audit in the Context of Electronic Banking. *Bankovskoe delo — Banking*, no. 5, pp. 51–54 (In Russ.).

Smirnov A.I., Kuroedov B.V., Sandarov O.V. Global Security in the Digital Age: Stratagemes for Russia: monograph. Moscow: VNIIgeosystem Publ., 2014. 394 p. (In Russ.).

Tamarov P.A. (2020). Prospects for the EAEU Payment System. Greater Eurasia: Development, Security, Cooperation. Yearbook, iss. 3, part 1, pp. 231–236. Moscow: INION RAN Publ. (In Russ.).

Yusupova O.A., Gorokhova M.I. (2020). Cybercrime in the Banking Sector: the Current State and Methods of Protection. *Meridian*, no. 9 (43), pp. 1–4 (In Russ.).

Zvonova E.A., Ershov M.V., Kuznetsov A.V. et al. (2016). Reforming the World Financial Architecture and the Russian Financial Market: monograph. E.A. Zvonova (ed.). Moscow: Rusains Publ., 2016, 430 p. (In Russ.).

Информация об авторах

***Виктор Яковлевич Пищик**, доктор экономических наук, профессор Департамента мировых финансов Финансового университета при Правительстве Российской Федерации, г. Москва*
***Петр Викторович Алексеев**, кандидат экономических наук, ведущий научный сотрудник Института мировой экономики и международных финансов Финансового университета при Правительстве Российской Федерации, г. Москва*

Information about the authors

***Victor Ya. Pishchik**, Doctor of Economic Sciences, Professor at the Department of Global Finance, Financial University under the Government of Russian Federation, Moscow*
***Peter V. Alekseev**, Candidate of Economic Sciences, Leading Researcher at the Institute of Global Economy and International Finance, Financial University under the Government of Russian Federation, Moscow*

Статья поступила в редакцию 08.04.2021
Одобрена после рецензирования 17.05.2021
Принята к публикации 16.06.2021

Article submitted April 8, 2021
Approved after reviewing May 17, 2021
Accepted for publication June 16, 2021