Ученые записки Крымского федерального университета имени В. И. Вернадского.
Экономика и управление. 2018. Т. 4 (70). № 2. С. 22–33.

УДК 330.131.7:004.946.5

ДЕТЕРМИНАНТЫ ВОЗНИКНОВЕНИЯ И ПРОЯВЛЕНИЯ КИБЕРРИСКОВ В МЕЖДУНАРОДНОМ БИЗНЕСЕ

Горда А. С., Горда О. С.

Крымский федеральный университет имени В. И. Вернадского, Симферополь, Российская Федерация
E-mail: alx7777@mail.ru

Исследованы сущность, особенности и условия возникновения и реализации киберрисков в международном бизнесе. Выделены причинно-следственный, секторальный и инструментальный подходы к определению дефиниции киберрисков. Предложено рассматривать кибериски в широком и узком понимании. Систематизированы криминальные и некриминальные источники киберрисков. Изучены явления кибератаки и киберинцидента как основные инструменты реализации киберриска. Выявлены киберугрозы для развития внешней торговли. Проанализированы основные киберинциденты глобального уровня.
Ключевые слова: киберриск, кибератака, киберугроза, киберинцидент.

ВВЕДЕНИЕ

На протяжении последних десятилетий развитие Интернета обусловило революционные изменения в сфере связи и коммуникации, что стало существенным фактором мирового экономического роста. С одной стороны, это дало возможность субъектам хозяйствования и населению во всем мире получить выгоды от эффективности, скорости и удобства цифровых операций и мгновенного обмена информацией, а с другой стороны, обусловило для субъектов международного бизнеса рост вероятности получения финансовых убытков, потери данных и ухудшения репутации из-за киберпреступных действий конкурентов и хакеров.

Начиная с 2012 г. проблема киберрисков на мировом уровне была официально названа одной из пяти ключевых угроз человечеству. В материалах Мирового экономического форума 2012 г. кибератаки заняли четвертое место в рейтинге угроз. Через пять лет в подобном рапорте были отмечены новые типы киберугроз – кража и мошенничество с данными [1]. Активизация данных процессов обуславливает актуальность проведенного исследования детерминант формирования и проявления киберрисков в международном бизнесе.

В современной научной литературе экономическим аспектам киберрисков и методам управления ими посвящено относительно незначительное количество работ. Следует отметить, что темпы исследований данной проблематики в развитых странах несколько опережают отечественные разработки. Такой разрыв, с одной стороны, объясняется уровнем развития финансовой системы и ее зависимостью от информационных технологий. А с другой стороны – проблема киберрисков объединяет в себе две различные сферы: финансовую и информационную, что требует междисциплинарного подхода к их исследованию.

Существенную роль в исследовании сущности, факторов и последствий киберрисков в международной экономической деятельности играют частные учреждения: консалтинговые, страховые компании и компании по разработке

информационно-программного обеспечения, в частности такие, как AON, Pricewaterhouse-Coopers, Deloitte, Ernstand Young, Society of Actuaries, International Association, Allianz, Geneva Association и др. С ростом киберрисков и негативных финансовых последствий их проявления все большее внимание этой угрозе уделяют государственные и коммерческое учреждения, в частности Федеральное бюро расследований США, Банк международных расчетов и др.

В различных источниках кибериски рассматриваются в таких аспектах, как:

– систематические риски в деятельности финансовых учреждений и финансовых рынков [2];

– составляющая операционных рисков компаний [3; 4];

– вероятность наступления событий в сфере информационных активов, компьютерных и коммуникационных ресурсов [5];

– вероятные преступления, совершенные с помощью сети Интернет [6].

Одной из наиболее полных теоретических разработок считается работа Eling M. [7], где рассмотрено 209 позиций по тематике киберрисков. При этом автор выделил 7 сфер исследований киберрисков.

Среди отечественных исследователей следует выделить работы Бочковой А. А. [8], Безкоровайного М. М., Татузова А. Л. [9], Талиповой Л. Р. [10], Булай Ю. Г., Булай Р. И. [11], Карповой Д. Н. [12], Бураевой Л. А. [13], Згоба А. И., Маркелова Д. В., Смирнова П. И. [14], которые уделили внимание проблемам киберугроз, вопросам обеспечения кибербезопасности, изучению киберпреступлений и киберпреступности и др. Несмотря на то, что в указанных исследованиях отражены отдельные аспекты проявления киберрисков, в отечественной научной литературе пока недостаточно внимания было уделено комплексным исследованиям экономических проблем киберрисков.

Целью статьи является исследование детерминант возникновения киберрисков и их негативного влияния на мировую и национальные экономики.

ОСНОВНОЙ МАТЕРИАЛ

На основе изучения существующих наработок в научной литературе и нормативно-правовых актов представляется возможным выделить три подхода относительно понимания сущности категории киберриска в международном бизнесе: причинно-следственный, секторальный и инструментальный.

Причинно-следственный подход связывает последствия проявления киберрисков и источников их возникновения. Согласно данному подходу, кибериск – это любой риск финансовых потерь, сбоев или нанесения вреда репутации предприятия или организации вследствие отказов систем информационных технологий [15]. Рабочая группа Комитета по выплатам и рыночной инфраструктуре и Международная организация комиссий по ценным бумагам Банка международных расчетов рассматривают кибериск как объединение вероятности события, которое происходит в сфере информационных активов организации, компьютерных и коммуникационных ресурсов и последствий этого события для организации [5].

В секторальном подходе акцент делается на сферах реализации киберрисков. Киберриск может быть определен как угроза, связанная с онлайн-активностью, интернет-торговлей, электронными системами и технологическими сетями, а также хранением персональных данных [16].

В основе инструментального подхода – инструменты, с помощью которых происходит реализация киберрисков. Форум Chief Risk Officers (CRO) определил кибериски как любые риски, возникающие при использовании электронных данных и их передаче, включая технологические инструменты, такие как Интернет и телекоммуникационные сети. Сюда же включаются физические убытки, обусловленные нарушениями кибербезопасности, мошенничеством, злоупотреблениями данными, любой ответственностью, которая возникает вследствие хранения данных, а также доступности, целостности и конфиденциальности электронной информации относительно частных лиц, компаний или правительств [17].

Анализ вышеперечисленных подходов дает возможность утверждать, что кибериску присущи признаки операционного риска. Следует заметить, что средой возникновения киберрисков является киберпространство. Несмотря на существование множества подходов к определению киберпространства, можно выделить его признаки, присутствующие во всех подходах. Так, киберриск не может существовать без материальных элементов киберпространства, он содержит информацию и является виртуальным [18]. Подобного подхода придерживается Федеральная служба расследований США и трактует кибериски как вероятные преступления, осуществленные при посредничестве сети Интернет [6].

Понятие киберрисков можно рассматривать в узком и широком значении. В узком значении кибериски связаны с операционными угрозами информационным и технологическим активам, которые отрицательно влияют на конфиденциальность, доступность и целостность информации или информационной системы. Киберриск – это операционный риск, который заключается в получении прямых или косвенных убытков экономическими субъектами вследствие их функционирования в киберпространстве. В широком значении кибериски – это вероятность угрозы интерактивным цифровым сетям, которые используются для передачи, модификации и хранения информации.

В большинстве случаев кибериски возникают вследствие совершения киберпреступлений. Киберпреступления представляется возможным разделить на две группы: киберзависимые преступления и кибервозможные преступления. Под киберзависимыми преступлениями понимают преступления, осуществляемые лишь с использованием устройств информационно-коммуникационных технологий, которые является одновременно инструментом и целью преступления. Например, разработка и распространение вредоносного программного обеспечения для получения финансовой выгоды, осуществления взлома для кражи, повреждения или уничтожения данных и/или сетевой активности.

Кибервозможные преступления – это традиционные преступления, которые могут быть увеличены в масштабе с помощью компьютеров, компьютерных сетей или других форм информационно-компьютерной техники. Например,

мошенничество с использованием кибертехнологий и кража данных [19].

Учитывая проблему быстрой диффузии киберугроз и практически полное отсутствие контроля за их распространением, необходимо выделить уровни проявления киберпреступлений:

- микроуровень (уровень отдельных домохозяйств и предприятий);
- макроуровень (уровень отдельных отраслей);
- мезоуровень (уровень отдельных стран или их объединений).

Источники возникновения операционных киберрисков систематизировали Cebula J. J. и Young L. R., выделив четыре класса: действия людей, бездеятельность систем и технологий, ошибки во внутренних процессах и внешние события [4]. Каждый класс делится на подклассы, которые в своем составе имеют различные элементы-факторы. С точки зрения управления рисками подчеркивается, что самое большое значение для субъектов бизнеса имеют перебои (бездеятельность) в системах и технологиях (табл. 1).

Таблица 1.

Систематизация источников киберрисков

Источники киберрисков			
Некриминальные		Криминальные (киберпреступные)	
Форс-мажорные	Отключения электроэнергии, природные катастрофы, уничтожение серверов, компьютерной техники вследствие пожаров, наводнений т. д.	Физические атаки	Осуществление кражи физических данных, в частности кража конфиденциальных банковских данных клиентов сотрудниками банков
Технические недостатки	Сбои в работе оборудования, в частности потеря данных вследствие поломок жестких дисков или других компонентов компьютера; ошибки в программном обеспечении	Хакерские атаки	Шпионаж за данными клиентов или саботаж процессов функционирования компаний, в частности DDos-атаки, использование вирусов, «червей», «троянских коней» и т. п.
Человеческий фактор	Неумышленное раскрытие информации на веб-страницах, ошибочные уведомления и т. д.	Шантаж и вымогательство	Действия преступных группировок, нацеленные на шантаж и угрозы, в частности похищение конфиденциальных, секретных данных с требованием выплаты выкупа, зачастую в криптовалюте

Источник: составлено авторами на основе [19]

Одним из инструментов реализации киберрисков является кибератака. Федеральный совет экспертизы финансовых учреждений США (Federal Financial Institutions Examination Council, FFIEC) разграничивает понятие кибератаки и

киберинцидента. Под кибератакой понимается попытка повредить, нарушить или получить несанкционированный доступ через киберпространство к компьютеру, компьютерной системе или электронной сети связи с целью нарушения, выключения, уничтожения или злонамеренного контроля над вычислительным механизмом или инфраструктурой; или уничтожение целостности данных, или похищение информации [20]. Киберинцидент рассматривается FFIEC как действия с использованием компьютерных сетей, которые приводят к фактическому или потенциально неблагоприятному влиянию на информационную систему или информацию.

В докладе британской специализированной страховой компании «Hiscox» за 2016 г. отмечено, что киберпреступления принесли убытки мировой экономике на сумму в 450 млрд долл. США. Было похищено свыше 2 млрд записей персональных данных [21]. В том же 2016 г. вредоносная интернет-активность нанесла экономике США убытков на сумму от 57 до 109 млрд долл. США. Следует отметить, что 43 % кибератак в США направлено на малый бизнес [22]. Согласно данным правительства Великобритании, обработанных совместно с фирмой Pricewaterhausecooper, убытки от кибератак для малого и среднего бизнеса страны в 2015 г. составили от 75 тыс. до 310 тыс. фунтов и от 1,46 млн до 3,41 млн фунтов – для субъектов крупного бизнеса [23].

К перечню форм реализации киберриска следует добавить и третью категорию – кибер-терроризм. Особенностью кибер-терроризма является мотивация, которая заключается в деструктивном влиянии на социально важную инфраструктуру (систему электроснабжения, водоснабжения, железнодорожного сообщения и т. д.) [24]. Четвертой категорией, которую следует рассматривать как наиболее тяжелую форму проявления киберрисков, является кибервойна, характерной особенностью которой является использование информационных технологий одной страной с целью разрушения и создания нестабильности в другой стране или группе стран. Ключевой критерий деления на такие формы реализации киберрисков – это мотивация кибервмешательства и механизм его влияния на информационные системы. На практике провести такое четкое разделение – довольно сложная задача, поскольку зачастую тяжело определить основную мотивацию преступного кибердействия.

Консалтинговая компания Phenomenon провела опрос среди 2168 фирм в странах Европы, Южной Америки, Азии и Африки, которые ввели управление киберрисками как составляющую системы управления рисками. Ответ респондентов показал, что 46 % имели опыт с кибератаками, причем они носили различный характер: 46 % – были связаны с попытками разрушения бизнеса и IT-процессов, 34 % – были направлены на повреждение или кражу конфиденциальных данных фирмы (например, интеллектуальной собственности), 26 % – направлялись на кражу конфиденциальной информации частных лиц [25]. Согласно исследованиям страховой компании Allianz, к киберрискам, которые в максимальной степени влияли на деятельность компаний, принадлежат прерывание бизнес-процессов, кража интеллектуальной собственности и кибервымогательство [26].

По данным Центра стратегических и международных исследований (CSIS),

количество значительных киберинцидентов возрастает практически каждый год. При этом наблюдается четкая тенденция рост их количества в течение 2014–2017 гг. (рис. 1).

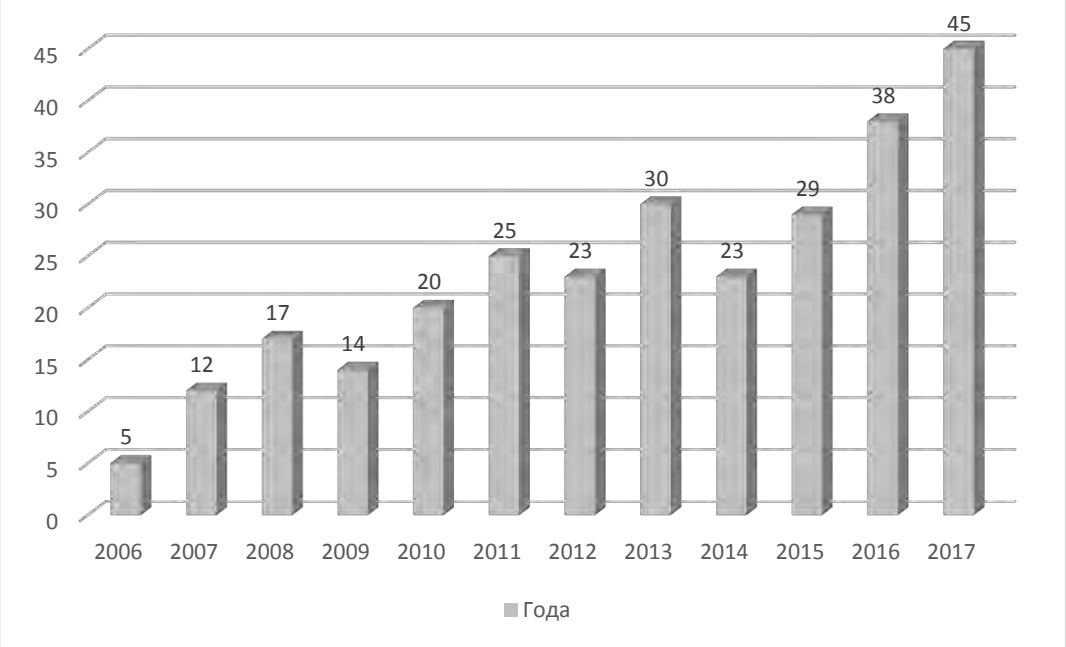

Рис. 1. Динамика роста количества киберинцидентов в мире.
Источник: составлено авторами на основе [27].

Совместные исследования CSIS и компании McAfee свидетельствуют, что ежегодная стоимость ущерба от киберпреступлений в глобальном масштабе составляет 445–600 млрд долл. США. Это составляет приблизительно 1 % мирового ВВП [28]. В структуре мотиваций кибератак по состоянию на январь 2018 г. наибольшую долю занимают киберпреступления – 81,7 %. Доля кибершпионажа составила 12,2 %, кибервойн – 4,3 %, хактивизма – 1,7 % [29]. По векторам воздействия кибератак по состоянию на январь 2018 г. преобладали вредоносные программы – 43,5 %. При этом доля похищения учетных записей составила 14,8 %, неизвестных атак – 13 %, целевых атак – 9,6 %, DDos-атак – 6,1 % [29]. Наиболее мощными киберинцидентами в 2017 г. стали Wannacry, Petya, Dragonfly 2.0, Equifax, Deloitte LLP (табл. 2).

В настоящее время наблюдается активизация влияния рынка криптовалют на реализацию кибератак. Национальное криминалистическое агентство Великобритании (NCA) отмечает, что криптовалюты помогают киберпреступникам получать платежи от жертв, содействуют росту киберпреступности как услуги, облегчают проведение финансовых операций в киберпреступном мире [35].

Таблица 2.

Краткая характеристика крупнейших киберинцидентов в 2017 году

Название	Период	Программное обеспечение	Масштабы распространения	Размер убытков
Wannacry	Май 2017 г., четыре дня	*Ransomware.* Использовалась уязвимость *Eternal Blue в Windows XP* и *Windows Server 2003*	Количество стран охвата – 150. Количество жертв – около 200 тыс.	Около 4 млрд долл. США
NotPetya	Впервые появился как *Petya* в 2016 г. *NotPetya – в* июне 2017 г.	*Malware.* Использовались уязвимости *Eternal Blue* и *Eternal Romancey в Windows XP* и *Windows Server* 2003	Количество стран охвата – свыше 60. Нидерланды: судоходная компания *TNT Express*, дочерняя компания *FedEx.* Дания: конгломерат по транспорту и логистики Maersk. Испания: транснациональные компании. Австралия: юридическая фирма *DLA Piper*, авиалинии *«Qantas».* Украина: правительственные организации, банки, государственные энергетические учреждения и железнодорожные компании, аэропорты «Борисполь» и «Жуляны», автозаправки, организации водоснабжения, телефонные компании и др.	Неизвестен
Dragonfly 2.0	Первая половина 2017 г.	Троянские программы удаленного доступа, замаскированные под обновления *Flash: Backdoor.Goodor*, *Backdoor.Dorshel* и *Trojan.Karagany.B*	Ориентирован на критические отрасли энергетики США, Турции и Швейцарии	Неизвестен
Equifax	Сентябрь 2017 г.	Нарушение данных (*data breaches)*	Британское отделение американского кредитно-рейтингового агентства *Equifax* признало, что почти 700 тысяч британских потребителей имели доступ к личным данным других клиентов после кибератаки, что намного больше, чем считалось ранее	27,3 млн долл. США
Deloitte LLP	Март 2017 г.	Нарушение данных (*data breaches)*	*Deloitte* – одна из крупнейших частных фирм Нью-Йорка, зарегистрированная в Лондоне. Предоставляет консультации по аудиту, налогообложению, кибербезопасности для крупнейших банков мира, международных компаний, медиа предприятий, фармацевтических фирм и государственных учреждений. Гипотетически могли быть похищенные данные с 5 млн писем в облаке. Однако официально было заявлено, что лишь 350 клиентов могут оказаться под угрозой	Неизвестен

Источник: составлено авторами на основе [30–34]

Во время опроса риск-менеджеров финансовых услуг, проведенного компанией Depository Trust&Clearing Corporation (DTCC), 70 % респондентов заметили, что киберриск имеет наиболее существенное влияние на функционирование глобальной финансовой системы. Вместе с тем к пяти наиболее значимым рискам, которые угрожают функционированию глобальной финансовой системы, также принадлежат: географический риск (50 %), влияние новых регуляторных требований (41 %), экономический спад (33 %), монетарная политика (31 %) [36]. Однако сфера финансовых услуг и глобальная финансовая система не являются исключениями для киберугроз. Их мощное влияние также испытают сферы коммунальных услуг, транспорта, здравоохранения, нефтегазовая индустрия, правительственные органы и др. В декабре 2015 г. в Турции произошли кибератаки на сети, используемые банками, правительством и средствами массовой информации. Среди сфер международного бизнеса наиболее чувствительными к киберугрозам являются телекоммуникации, логистика и производство.

Не является исключением для влияния киберрисков и сфера международной торговли, основой расширения которой в настоящее время становится Интернет, информационные и коммуникационные технологии. Прежде всего, это касается трансграничной е-коммерции, доля которой уже составляет около 7 % общего объема е-коммерции [37]. Использование современных технологий обусловило не только значительный рост е-коммерции, но и активизацию киберугроз в виде несанкционированного доступа к персональным данным потребителей, их использования или модификации. Это касается заражения компьютеров вредоносными программами, в частности вирусами, «червями», «троянскими конями»; хактивизма, кибершпионажа путем доступа к незащищенной информации через Wi-Fi, подделки IP-адресов и сканирования портов. Кибершпионаж становится одним из значимых инструментов получения конкурентных преимуществ на международном рынке. При этом зачастую финансирование кибер-шпионажа осуществляются правительствами. Ярким примером является взаимное обвинение Китая и США в кибершпионаже и применение на этой почве взаимных санкций.

Значительное влияние кибератаки оказывают на объекты глобального снабжения. Примером является кибератака на гигант судоходства «Maersk» летом 2017 г., осуществляющего международные перевозки товаров, в частности нефти. Она послужила причиной значительную перерыва в работе компании во время отключения компьютеров с помощью вредоносного программного обеспечения и принесла убытки в размере около 300 млн долл. США [28]. Хотя подобные инциденты могут обусловить и гораздо более серьезные последствия для глобальной экономики.

Следует заметить, что последствия (в экономическом контексте – потери) от реализации киберрисков делятся на прямые и косвенные [2]. Прямые потери связаны с экспертизой, расследованием, правовой защитой, информированием клиентов, укреплением систем защиты данных клиентов и компании. Косвенные расходы менее заметны, но долгосрочны и более сложны в оценке. В табл. 3 отражены основные негативные последствия реализации киберриска в международном бизнесе.

Таблица 3.

Последствия реализации киберрисков в международном бизнесе

Прямые	Опосредованные
Потеря собственных данных компании (коммерческих тайн, конфиденциальной информации)	Отзыв продукта(ов) с рынка
Потеря клиентов	Расторжение контрактов
Санкции от государственных органов	Кадровые изменения
Активизация технических и технологических исследований	Рост страховых премий
Усиление общественных связей	Рост расходов на обслуживание займов
Повышение уровня кибербезопасности	Обесценивание торговой марки
Информирование о взломе и/или краже данных клиентов	Потеря интеллектуальной собственности
Формирование систем защиты клиентов от взлома	Потери доходов по контрактам
Затраты на адвокатские гонорары и судебные разбирательства	Потеря ценности связи с клиентом
Расходы, связанные с выплатой компенсаций клиентам	Потеря репутации и значительные финансовые и временные затраты на ее восстановление

Источник: составлено авторами на основе [37]

В 2016 г. вредоносная активность в Интернете была по масштабам вторым в мире типом экономической преступности и затронула 32 % организаций. В Индии за период с 2004 г. по 2014 г. уровень преступности в Интернете увеличился в 19 раз. Одновременно с этим она сейчас занимает третье место после США и Китая по количеству источников вредоносной онлайн-деятельности. В Великобритании за 2016 г. каждое пятое предприятие подвергалось кибератакам, и лишь 24 % британских компаний утверждает, что они в состоянии обеспечить безопасность и защиту от кибервзломов [39]. В США в 2017 г. кибератакам также подвергалась каждая пятая компания. При этом две трети предприятий страны считают киберриск фундаментальным вызовом для своего бизнеса [40]. Последствия от кибератак становятся все более ощутимыми из-за применения киберпреступниками все более совершенных технологий, которые содействуют этому виду преступной деятельности.

ВЫВОДЫ

Киберриск является динамичным риском, в основе которого лежит вмешательство и нарушение целостности информационного обеспечения. Киберриск чаще всего проявляется через кибератаки, последствия которых могут быть как прямыми, так и опосредствованными, что значительно усложняет процесс оценки финансовых и экономических потерь. Кроме того, финансовые потери от реализации киберрисков не ограничены во времени, то есть могут проявиться намного позднее, после непосредственно кибератаки.

Ежегодно фиксируется стремительный рост количества киберинцидентов и их стоимости. Объектами кибератак могут быть физическое и юридическое лица, являющиеся субъектами внешнеэкономической деятельности, отдельные отрасли экономики, страны или даже группы стран. Наиболее угрожающей формой проявления киберриска является кибервойна, которая может охватывать целую страну.

Основными инструментами обеспечения кибербезопасности участников трансграничной е-коммерции являются аутентификация клиентов, антивирусное программное обеспечение, шифрование, цифровая подпись. Такие технологии, как биометрия и искусственный интеллект способствуют идентификации клиентов, обеспечению безопасности транзакций и минимизации убытков от кибермошенничества.

Кроме того, для предупреждения реализации киберрисков киберпространство должно регулироваться определенными правилами и нормами поведения. Национальные органы кибербезопасности должны получать от субъектов национальной экономики своевременные и точные отчеты о киберсобытиях. Национальные и наднациональные инструменты и механизмы минимизации киберрисков должны предусматривать предоставление внутренних данных компаний финансовым учреждениям и их автоматическую обработку. На первом этапе это может осуществляться на периодической основе, а в дальнейшем – в режиме реального времени. При этом должна осуществляться проверка надежности данных.

Учитывая криминальную природу кибератак, органы надзора за рынками финансовых услуг должны взаимодействовать с соответствующими правоохранительными органами на основе двустороннего предоставления информации. Для быстрой адаптации к постоянно модифицируемым киберугрозам регуляторные правила для финансовых учреждений должны быть максимально гибкими. В данном направлении во многих странах уже сделаны первые шаги, но основная работа по формированию действенных и эффективных механизмов предотвращения и минимизации последствий киберрисков еще впереди, в том числе и на уровне международных организаций и наднациональных органов ведущих интеграционных объединений.

Список литературы

1. Global Economic Forum. The Global Risks Report 2017. 12th Edition [Электронный ресурс]. URL: http://wef.ch/risks2017.
2. Kopp E., Kaffenberger L., Wilson C. Cyber Risk, Market Failures, and Financial Stability. Working Paper, 2017. International Monetary Fund. [Электронный ресурс]. URL: https://www.imf.org/~/media/Files/Publications/WP/2017/wp17185.ashx.
3. Peters Gereth W., Shevchenko P. V., Cohen D. R., Maurice D. Understanding Cyber Risk and Cyber Insurance, FinTech: Growth and Deregulation. [Электронный ресурс]. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3065635.
4. Cebula J. J., Young L. R. A Taxonomy of Operational Cyber Security Risks, Carnegie Mellon University. [Электронный ресурс]. URL: https://www.sei.cmu.edu/reports/10tn028.pdf.
5. Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, Guidance on Cyber Resilience for Financial Market Infrastructures. June 2016. [Электронный ресурс]. URL: https://www.bis.org/cpmi/publ/d146.htm.

6. Federal Bureau of Investigation, Internet Crime Report. 2016. [Электронный ресурс]. URL: https://pdf.ic3.gov/2016_IC3Report.pdf.

7. Eling M. What do we know about cyber risk and cyber risk insurance? // The Journal of Risk Finance. 2017. Iss. 5. P. 474–491.

8. Бочкова А. А. Киберугрозы на фондовых рынках: критерии анализа // Скиф. 2017. № 11. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/kiber-ugrozy-na-fondovyh-rynkah-kriterii-analiza.

9. Безкоровайный М. М., Татузов А. Л. Кибербезопасность подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya.

10. Талипова Л. Р. Международно-правовая регламентация киберпреступности // Гуманитарные, социально-экономические и общественные науки. 2016. № 4. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovaya-reglamentatsiya-kiberprestupnosti.

11. Булай Ю. Г., Булай Р. И. Профилактика и противодействие киберпреступности, а также международным киберугрозам // Академическая мысль. 2017. № 1. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/profilaktika-i-protivodeystvie-kiberprestupnosti-a-takzhe-mezhdunarodnym-kiberugrozam.

12. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/kiberprestupnost-globalnaya-problema-i-ee-reshenie.

13. Бураева Л. А. О некоторых вопросах обеспечения кибербезопасности в современных условиях // Теория и практика общественного развития. 2015. № 13. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/o-nekotoryh-voprosah-obespecheniya-kiberbezopasnosti-v-sovremennyh-usloviyah.

14. Згоба А. И., Маркелов Д. В., Смирнов П. И. Кибербезопасность: угрозы, вызовы, решения // Вопросы кибербезопасности. 2014. № 5 (8). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-ugrozy-vyzovy-resheniya.

15. Institute of Risk Management. [Электронный ресурс]. URL: https://www.theirm.org/knowledge-andresources/thought-leadership/cyber-risk.

16. Olsen T. Cyber risk insurance. 18.06.2013. [Электронный ресурс]. URL: https://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf.

17. CRO Forum. The Cyber Risk Challenge and the Role of Insurance. December 2014. [Электронный ресурс]. URL: http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance.

18. Rajnovic D. Cyberspace – What is it? Cisco Blogs. July 2012. [Электронный ресурс]. URL: https://blogs.cisco.com/security/cyberspace-what-is-it.

19. Eling M., Wirfs J. H. Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class Institute of Insurance Economics Universitat St. Gallen. 2016, 174 p. [Электронный ресурс]. URL: www.ivw.unisg.ch.

20. FFIEC. Cybersecurity Assessment Tool Glossary. June 2015. [Электронный ресурс]. URL: http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_C_Glossary_June_2015_PDF5.pdf.

21. Киберпреступления обошлись мировой экономике в $450 миллиардов в 2016 году. [Электронный ресурс]. URL: http://biz.censor.net.ua/news/3020281/kiberprestupleniya_oboshlis_mirovoyi_ekonomike_v_450_milliardov_v_2016_godu.

22. CEA Report: The Cost of Malicious Cyber Activity to the U.S. Economy. February 16, 2018. [Электронный ресурс]. URL: https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyberactivity-u-s-economy.

23. PricewaterhouseCooper. 2015 Information Security Breaches Survey. Department for Business, Innovation and Skills. [Электронный ресурс]. URL: www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html.

24. Hua J., Bapna S. The economic impact of cyber terrorism. The Journal of Strategic Information Systems. 2013. № 22 (2). P. 175–186.

25. Ponemon Institute LLC. Global Cyber Risk TransferComparison Report. 2017. [Электронный ресурс]. URL: http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-

transfercomparison-report.jsp.

26. Allianz Global Corporate and Speciality. A Guide to Cyber Risks. [Электронный ресурс]. URL: https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.

27. Significant Cyber Incidents Since 2006: Center for Strategic&International Studies. [Электронный ресурс]. URL: https://csis-prod.s3.amazonaws.com/s3fs-public/180308_Significant_Cyber_Events_List.pdf?Szs5ZuZShJAIfgcUXRsvB5T8C76PJR0y.

28. Lewis J. Economic Impact of Cybercrime No Slowing Down. [Электронный ресурс]. URL: https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-b9303ae70.

29. Passeri P. Cyber Attacks Statistics. January 2018. Nextgen Network Monitor. [Электронный ресурс]. URL: https://www.hackmageddon.com/2018/02/22/january-2018-cyber-attacks-statistics.

30. WannaCry Ransomware – A Wake-Up Call for Cybersecurity and Data Management. [Электронный ресурс]. URL: http://en.finance.sia-partners.com/20170609/wannacry-ransomware-wake-callcybersecurity-and-data-management.

31. Personal details of almost 700,000 Britons hacked in cyber-attack. [Электронный ресурс]. URL: https://www.theguardian.com/technology/2017/oct/11/personal-details-of-almost-700000-britons-hacked-in-cyber-attack.

32. Surane J. Equifax Is Haunted By Its Costly Cyber Attack. [Электронный ресурс]. URL: https://www.bloomberg.com/news/articles/2017-11-09/equifax-haunted-by-cyberattack-as-costs-jump-lawsuits-abound.

33. Deloitte hit by cyber-attack revealing clients' secret email. [Электронный ресурс]. URL: https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attackrevealing-clients-secret-emails.

34. The Biggest Cybersecurity Threats of 2017: The Need to Prepare. 24.10.2017. [Электронный ресурс]. URL: http://en.finance.sia-partners.com/20171024/biggest-cybersecurity-threats-2017-need-prepare.

35. UK national risk assessment of money laundering and terrorist financing. [Электронный ресурс]. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.

36. Reagan J., Raghavan A., Thomas A. Quantifying risk: What can cyber risk management learn from the financial services industry? Deloitte Review. Iss. 19. July 25, 2016. [Электронный ресурс]. URL: https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/quantifying-risk-lessons-from-financial-services-industry.html.

37. 5 ways to make global e-commerce easier for everyone. December, 2017. [Электронный ресурс]. URL: https://www.weforum.org/agenda/2017/12/ecommerce-trade-wto-growth-opportunity.

38. Bahar M., Satnick T. Cyber Kinks in the Global Supply Chain. [Электронный ресурс]. URL: http://www.globaltrademag.com/global-trade-daily/commentary/cyber-kinks-global-supply-chain.

39. Payment cybersecurity: Be prepared. Be protected. London: Worldpay 2017. [Электронный ресурс]. URL: http://offers.worldpayglobal.com/rs/850-JOA-856/images/Worldpay_Security_Whitepaper_v10.1.pdf?mkt_tok=eyJpIjoiTXpsa05EZ3hOR1F3TlRRNSIsInQiOiJGWlVjTDVDZjdGOUVTa1BwNHlWYXExNUl4WXJQVTlpM2NHRmtNOU5vZDJJcGlTWWlTRDZGcFBibUkwakxpNVpTZ2VScFF0MllEclV0b2FBOUtMQ21qdHhacU1MXC9VYVMyQ01zdWQrUm9PWlFzT0k3T21YUXQ0R01OWlIyQ2todDAifQ%3D%3D.

40. Willis Towers Watson. Cyber Risk Survey Report 2017. [Электронный ресурс]. URL: https://www.willistowerswatson.com/en/insights/2017/06/2017-cyber-risk-survey-report.

Статья поступила в редакцию 26.04.2018