Доверие и безопасность в информационном обществе

ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья рекомендована к публикации членом редакционного совета А.А. Стрельцовым 21.09.2022.

Пищик Виктор Яковлевич
Доктор экономических наук, профессор
Финансовый университет при Правительстве Российской Федерации, департамент мировых финансов, профессор
Москва, Российская Федерация
vpiwik@fa.ru

Алексеев Петр Викторович
Кандидат экономических наук
Финансовый университет при Правительстве Российской Федерации, Институт мировой экономики и международных финансов, Департамент мировой экономики и международного бизнеса, ведущий научный сотрудник
Москва, Российская Федерация
palekseev@fa.ru

Аннотация

Актуальность темы исследования обусловлена необходимостью формирования глобальной системы международной информационной безопасности (МИБ) в условиях обострения информационных угроз. Создание такой системы позволит существенно повысить уровень информационной безопасности всех субъектов мировой экономики, обеспечить устойчивое социально-экономическое и научно-техническое развитие мирового сообщества.

Ключевые слова

Евразийский экономический союз; информационно-коммуникационные технологии; цифровизация; кибербезопасность; киберпреступность; информационные угрозы; международная информационная безопасность

Введение

Цифровизация мировой экономики вызывает глубокие изменения во всех сферах жизни общества. Возникают как большие ожидания (экономического роста, улучшения качества услуг и др.), так и опасения (сокращения рабочих мест, усиления неравенства, роста угроз информационной безопасности) [1]. В частности, серьёзную угрозу устойчивому развитию мирового сообщества представляет рост числа кибератак на промышленные и инфраструктурные объекты ряда стран мира. Первая масштабная трансграничная кибератака была зарегистрирована в Иране в 2010 г., когда компьютерным вирусом «Stuxnet» были выведены из строя сотни центрифуг по обогащению урана в г. Натанзе и на АЭС в г. Бушере [2]. Данный пример свидельствует о высокой опасности кибератак на компьютерные системы управления промышленными и инфраструктурными объектами для населения, экономики и экологии стран и регионов.

Со второй половины 2010-х годов угрозы кибербезопасности субъектов мировой экономики стали приобретать глобальные масштабы. 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 оценкам российских ученых, мировая экономика в 2022 г. может потерять от деятельности кибермошенников до 8 трлн долл., а в 2030-м – уже 90 трлн долл. [3]. В этой связи одним из важнейших приоритетов межгосударственного сотрудничества становится создание глобальной системы МИБ [4].

https://doi.org/10.52605/16059921_2023_02_89

1 Основные угрозы МИБ в современном мире

Согласно официальному определению Министерства иностранных дел Российской Федерации, международная информационная безопасность – это состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве [5].

В последние годы одной из основных угроз для МИБ является рост числа кибератак с использованием таких видов вредоносного программного обеспечения (ВПО) как троянские программы[1], вирусы-шифровальщики[2], фишинг[3]. Рост числа кибератак с использованием ВПО вызывает не только обострение рисков глобальных техногенных катастроф, но также приводит к снижению производительности и конкурентоспособности компаний, убыткам юридических и физических лиц [4].

Троянские вирусы являются в настоящее время одним из наиболее опасных видов ВПО. По данным компании Check Point, в феврале 2022 г. троянский вирус Emotet занимал первое место в мировом рейтинге ВПО: он атаковал 5% всех организаций в мире. За ним следуют троянские вирусы Formbook и Trickbot, которые затронули по 3 и 2% организаций в мире соответственно [6]. По оценкам экспертов, в настоящее время растут масштабы использования вирусов-шифровальщиков против юридических и физических лиц. Так, в 2021 г. от атак шифровальщиков в мире пострадали 80% организаций. Начиная с 2018 г., количество атак шифровальщиков против организаций во всём мире постоянно растет, при этом рекордный темп прироста количества атак был зарегистрирован в 2021 г. (68,5%) [7]. В последние годы серьёзной угрозой стала кража личных данных пользователей в сети Интернет. Так, в марте 2020 г. британская компания Comparitech сообщила об утечке данных более 267 млн. пользователей социальной сети Facebook (в основном, граждан США). Возможно, эти данные были использованы для рассылки фишинговых ссылок. Федеральная торговая комиссия США обязала Facebook выплатить рекордные $5 млрд. штрафа, что в 20 раз превышает самые крупные штрафы, которые применялись за утечки данных. В результате репутация самой компании, а также её позиции на фондовой бирже значительно ухудшились [8].

В последнее десятилетие отмечается значительное увеличение количества DDoS-атак (Distributed Denial of Service, распределенная атака типа «отказ в обслуживании») на предприятия и кредитно-финансовые организации. DDoS-атака является компьютерной атакой из одного источника, которая предполагает блокирование доступа пользователей к определенному интернет-сайту в результате его намеренной «перегрузки» направляемыми сообщениями. В настоящее время в мире ежедневно фиксируются около 5000 DDoS-атак и их число продолжает расти [9].

2 Тенденции обеспечения МИБ

В настоящее время в условиях беспрецедентного обострения угроз и рисков для международной информационной безопасности актуальной задачей является разработка и принятие единого международного нормативного правового акта, эффективно регулирующего вопросы обеспечения МИБ на глобальном уровне. Конвенция Совета Европы о киберпреступности от 23 ноября 2001 г. (Convention on Cybercrime of the Council of Europe) [10][4] содержит перечень киберпреступлений и предполагает создание механизмов международного сотрудничества по предотвращению, раскрытию и преследованию киберпреступлений. Однако страны БРИКС и подавляющее большинство развивающихся стран не присоединились к данной Конвенции ввиду того, что отдельные её положения, согласно официальной позиции, нарушают государственный суверенитет, а также могут нанести ущерб национальной безопасности государств-участников, правам и законным интересам их граждан и юридических лиц [4]. Кроме того, согласно официальной позиции России и ряда других государств положения Конвенции, разработанной в 2001 г., уже устарели. В частности, она криминализирует всего 9 видов незаконного использования

[1]Троянские программы (англ. *trojans*) – вредоносные компьютерные программы, осуществляющие кражу информации с заражённых компьютеров и кибершпионаж. Название произошло от древнегреческого мифа.

[2]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 информации с компьютеров.

[3]Фишинг (англ. *phishing*) – вид мошенничества в сети Интернет, целью которого является получение каких-либо конфиденциальных данных пользователей.

[4] По состоянию на 25 августа 2022 г. 65 государств ратифицировали конвенцию, а ещё четыре государства подписали конвенцию, но не ратифицировали её (URL: https://ru.xcv.wiki/wiki (дата обращения 26.08.2022)).

ИКТ, а сейчас их уже более 30. Кроме того, в Конвенции ни разу не упоминается Интернет, а также угроза пропаганды идеологии терроризма и экстремизма с использованием средств массовой информации и другие информационные угрозы [4]. В связи с этим Россия выступает за создание под эгидой ООН универсальной конвенции по противодействию преступлениям в информационной сфере, которая должна носить глобальный характер и основываться на фундаментальных принципах международного права [4].

Взаимодействие государств в области информационной безопасности реализуется в форме межгосударственного сотрудничества, прежде всего в рамках международных организаций. В современном мироустройстве принципиальное значение имеет взаимодействие в системе ООН [4].

Заинтересованность в обеспечении МИБ подтверждается принятием подавляющим большинством стран Резолюции Генеральной Ассамблеи ООН от 5 декабря 2018 г. №73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», которая не только сформулировала перечень правил поведения государств в информационном пространстве, но и создала под эгидой ООН эффективный переговорный механизм в формате профильной Рабочей группы открытого состава (РГОС ООН) для практического решения проблемы обеспечения МИБ [11]. В июне 2021 г. была запущена очередная РГОС ООН по вопросам безопасности в сфере использования ИКТ и самих ИКТ на период 2021–2025 гг., включающая представителей всех 193 государств-членов ООН [12].

На региональном уровне, в частности, в рамках Евразийского экономического союза (ЕАЭС), нормативное правовое регулирование вопросов обеспечения кибербезопасности находится в стадии становления. Общие подходы к обеспечению кибербезопасности в части определения задач, принципов и направлений обеспечения кибербезопасности в финансовом секторе государств-членов ЕАЭС сформулированы в утвержденной в 2019 г. Концепции формирования общего финансового рынка ЕАЭС [13]. Однако право ЕАЭС в сфере обеспечения кибербезопасности не охватывает другие сектора экономики, которые также уязвимы перед различными киберугрозами. Необходимо комплексное решение проблемы кибербезопасности во всех сферах финансово-экономической деятельности государств-членов ЕАЭС (включая безопасность государственного, производственного и финансового секторов экономики, юридических и физических лиц).

3 Перспективы обеспечения МИБ

Работа ООН в сфере обеспечения МИБ, как и в любой другой, зависит от воли и возможностей её государств-членов. Аргументированность мнения о том, что ООН недостаточно активно действует в области обеспечения МИБ, основывается на том факте, что до сих пор на её площадке не выработан международный консенсус по ряду принципиальных теоретических, политических и правовых вопросов, а именно:

1. Каково содержательное определение понятий «кибербезопасность», «киберпреступность», «информационное пространство», «информационная угроза», «информационная безопасность», «международная информационная безопасность» и связанных с ними понятий?
2. Может ли информация распространяться свободно или должны существовать правительственные ограничения?
3. Каким образом можно эффективно противодействовать киберпреступности?
4. На чем фокусировать правовое регулирование – на предотвращении уголовно наказуемых деяний или на противодействии использованию киберпространства для совершения «нападений» на государства?
5. Должно ли в данной области применяться действующее международное право или необходимы новые нормы и правила, возможно, в виде межгосударственного соглашения?

Необходимыми условиями для создания полноценной глобальной системы МИБ являются разработка качественного теоретического и методологического обоснования этого процесса, достижение международного консенсуса по вышеперечисленным принципиальным вопросам обеспечения МИБ, определение единых концептуальных подходов к созданию глобальной системы МИБ.

В современных условиях, с учетом сложившейся геополитической ситуации и растущего полицентризма в мире, следует активизировать также усилия по обеспечению международной информационной безопасности на региональном уровне. Актуальной задачей является разработка и принятие общего концептуального документа по обеспечению кибербезопасности государств-

членов ЕАЭС, учитывающего особенности ЕАЭС и опыт Европейского союза в данной области. Данный концептуальный документ должен содержать концептуальные подходы к обеспечению кибербезопасности всех экономических субъектов государств-членов ЕАЭС.

Заключение

В настоящее время назрела необходимость формирования полноценной глобальной системы международной информационной безопасности. Работа по теоретическому и методологическому обоснованию формирования глобальной системы МИБ начата, но ещё далека до завершения. Необходимо объединить усилия экспертов мирового сообщества, правительственных структур, международных организаций в интересах эффективного противодействия современным вызовам и угрозам в глобальном информационном пространстве.

На региональном уровне перед государствами-членами ЕАЭС стоит задача разработки, принятия и внедрения в собственное правовое поле согласованных нормативных правовых актов, направленных на эффективное противодействие киберпреступности во всех её проявлениях, и предусматривающих ответственность за киберпреступления. На современном этапе целесообразны разработка и принятие логически выстроенной концепции обеспечения региональной кибербезопасности государств-членов ЕАЭС, учитывающей особенности Союза и опыт Европейского союза в данной области.

Благодарности

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситету.

Литература

1. Ершова Т.В., Хохлов Ю.Е., Шапошник С.Б. Методология мониторинга развития и использования технологий работы с большими данными // Информационное общество. 2021. № 4-5. С. 2-32. https://doi.org/10.52605/16059921_2021_04_02.
2. Вирус Stuxnet нанес сокрушительный удар по ядерной программе Ирана. 16.12.2010. URL: https://www.securitylab.ru/news/402905.php (дата обращения 25.08.2022).
3. 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 (дата обращения 25.08.2022).
4. Крутских А.В. Международная информационная безопасность: теория и практика. Учебник для вузов в двух томах. М.: Издательство «Аспект Пресс», 2021.
5. Конвенция об обеспечении международной информационной безопасности (концепция) от 22 сентября 2011 г. URL: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/ CptICkB6BZ29/content/id/191666 (дата обращения 25.08.2022).
6. Самое опасное ПО февраля 2022 года: Emotet лидирует в рейтинге Check Point. 18.03.2022. URL: https://www.itsec.ru/news/samoye-opasnoye-vredonosnoye-po-fevralia-2022-emotet-lidiruyet-v-reitinge-check-point (дата обращения 25.08.2022).
7. 72 статистических факта о шифровальщиках, важных для безопасности в 2022 г. 09.03.2022. URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/351920.php (дата обращения 25.08.2022).
8. Десять самых громких кибератак XXI века. 20.02.2021. URL: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e (дата обращения 25.08.2022).
9. Kesavamoorthy R., Alaguvathana P., Suganya R., Vigneshwaran P. Classification of DDoS-attack – A Survey // TEST. Engineering and Management, Volume 83, March-April 2020, p. 12926-12932.
10. Convention on Cybercrime of the Council of Europe of 23.11.2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?module=treaty-detail&treatynum=185 (дата обращения 25.08.2022).
11. Резолюция Генеральной Ассамблеи ООН от 5 декабря 2018 г. №73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://undocs.org/ru/A/RES/73/27 (дата обращения 25.08.2022).

12. Глобальная киберповестка: дипломатическая победа. Интервью директора Департамента международной информационной безопасности МИД России А.В.Крутских. 07.06.2021. https://interaffairs.ru/news/show/30374 (дата обращения 25.08.2022).
13. Концепция формирования общего финансового рынка Евразийского экономического союза (утверждена Решением Высшего Евразийского экономического совета от 1 октября 2019 г. №20). URL: http://www.eurasiancommission.org/ru/act/finpol/dofp/Pages/conception.aspx (дата обращения: 25.08.2022).

TRENDS AND PERSPECTIVES OF THE PROVISION OF THE INTERNATIONAL INFORMATION SECURITY

Pishchik, Victor Yakovlevich

Doctor of economic sciences, professor
Financial University under the Government of the Russian Federation, Department of global finance, professor
Moscow, Russian Federation
vpiwik@fa.ru

Alekseev, Petr Viktorovich

Candidate of economic sciences
Financial University under the Government of the Russian Federation, Institute for global economy and international finance, Department of global economy and international business, leading researcher
Moscow, Russian Federation
palekseev@fa.ru

Abstract

The relevance of the research issue is due to the need to form a global system of international information security (IIS) in the context of exacerbation of information threats. The creation of such a system will significantly increase the level of information security of all subjects of the world economy, provide sustainable socio-economic, scientific and technological development of the world community.

Keywords

Eurasian economic union; information and communication technology; digitalization; cybersecurity; cybercrime; information threats; international information security

References

1. Ershova T.V., Hohlov Yu.E., Shaposhnik S.B. Metodologiya monitoringa razvitiya i ispol'zovaniya tekhnologii raboty s bol'shimi dannymi // Informatsionnoe obshchestvo. 2021. №4-5. S. 2-32. https://doi.org/10.52605/16059921_2021_04_02.
2. Virus Stuxnet nanes sokrushitel'nyi udar po yadernoi programme Irana. 16.12.2010. URL: https://www.securitylab.ru/news/402905.php (accessed on 25.08.2022).
3. Avramenko E. Kiberprestupnost' priznali bol'shei opasnost'yu, chem epidemii i tekhnogennye katastrofy. Federal'noe agentstvo novostei, 19.02.2020. URL: https://riafan.ru/1252056-kiberprestupnost-priznali-bolshei-opasnostyu-chem-epidemii-i-tekhnogennye-katastrofy (accessed on 25.08.2022).
4. Krutskikh A.V. Mezhdunarodnaya informatsionnaya bezopasnost': teoriya i praktika. Uchebnik dlya vuzov v dvukh tomakh. M.: Izdatel'stvo «Aspekt Press», 2021.
5. Konventsiya ob obespechenii mezhdunarodnoi informatsionnoi bezopasnosti (kontseptsiya) ot 22 sentyabrya 2011 g. URL: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/ CptICkB6BZ29/content/id/191666 (accessed on 25.08.2022).
6. Samoe opasnoe PO fevralya 2022 goda: Emotet lidiruet v reitinge Check Point. 18.03.2022. URL: https://www.itsec.ru/news/samoye-opasnoye-vredonosnoye-po-fevralia-2022-emotet-lidiruyet-v-reitinge-check-point (accessed on 25.08.2022).
7. 72 statisticheskikh fakta o shifroval'shchikakh, vazhnykh dlya bezopasnosti v 2022 godu. 09.03.2022. URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/351920.php (accessed on 25.08.2022).
8. Desyat' samykh gromkikh kiberatak XXI veka. 20.02.2021. URL: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e (accessed on 25.08.2022).
9. Kesavamoorthy R., Alaguvathana P., Suganya R., Vigneshwaran P. Classification of DDoS-attack – A Survey // TEST. Engineering and Management, Volume 83, March-April 2020, p. 12926-12932.
10. Convention on Cybercrime of the Council of Europe of 23.11.2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185? module=treaty-detail&treatynum=185 (accessed on 25.08.2022).

11. Rezolyutsiya General'noi Assamblei OON ot 5 dekabrya 2018 g. №73/27 «Dostizheniya v sfere informatizatsii i telekommunikatsii v kontekste mezhdunarodnoi bezopasnosti». URL: https://undocs.org/ru/A/RES/73/27 (accessed on 25.08.2022).
12. Global'naya kiberpovestka: diplomaticheskaya pobeda. Interv'yu direktora Departamenta mezhdunarodnoi informatsionnoi bezopasnosti MID Rossii A.V.Krutckikh. 07.06.2021. https://interaffairs.ru/news/show/30374 (accessed on 25.08.2022).
13. Kontseptsiya formirovaniya obshchego finansovogo rynka Evraziiskogo ekonomicheskogo soyuza (utverzhdena Resheniem Vysshego Evraziiskogo ekonomicheskogo soveta ot 1 oktyabrya 2019 g. №20). URL: http://www.eurasiancommission.org/ru/act/finpol/dofp/Pages/ conception.aspx (accessed on 25.08.2022).