Доверие и безопасность в информационном обществе

ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ РОССИИ

Статья рекомендована к публикации членом редакционного совета А. А. Стрельцовым 27.03.2025.

Пищик Виктор Яковлевич

Доктор экономических наук, профессор
Финансовый университет при Правительстве Российской Федерации, Кафедра мировой экономики и мировых финансов, профессор
Москва, Российская Федерация
vpiwik@fa.ru

Алексеев Пётр Викторович

Кандидат экономических наук
Финансовый университет при Правительстве Российской Федерации, Институт глобальных исследований, ведущий научный сотрудник
Москва, Российская Федерация
palekseev@fa.ru

Аннотация

Одной из актуальных проблем мирового сообщества в настоящее время является быстрый масштабный рост глобальной киберпреступности, наблюдаемый в течение последних тридцати лет. Особую опасность для субъектов российской экономики сегодня представляют: атаки на критические информационные инфраструктуры; криптоджекинг; рост числа DDoS-атак на интернет-сайты российских организаций; угрозы, связанные с функционированием дарквеба. В России создана и успешно функционирует полноценная национальная система обеспечения кибербезопасности. Однако для эффективного противодействия растущей киберпреступности, носящей во многом трансграничный характер, необходимы её дальнейшее развитие и совершенствование с учётом новых вызовов и угроз в глобальном информационном пространстве. Актуальной задачей является укрепление сотрудничества Российской Федерации с иностранными партнерами в области обеспечения информационной безопасности, в том числе в целях установления эффективно действующего международно-правового режима обеспечения безопасности в сфере использования информационно-коммуникационных технологий (ИКТ). В связи с этим предлагается дополнить Конвенцию против киберпреступности, принятую ООН 24 декабря 2024 г., протоколом по дополнительным составам преступлений, включая использование ИКТ в террористических и экстремистских целях, в мошенничестве в банковской сфере, а также торговлю наркотиками, оружием, поддельными документами, вредоносными программами, технологиями фишинга, DDoS-атак, прочими запрещёнными товарами и услугами. Это окажет содействие устойчивому развитию мирового сообщества.

Ключевые слова

цифровизация; информационно-коммуникационные технологии; ИКТ; критические информационные инфраструктуры; международная информационная безопасность; МИБ; информационная безопасность; кибербезопасность; киберпреступность; кибератаки; киберугрозы; кибернетические риски; глобальные проблемы; профилактика глобальных экономических кризисов

https://doi.org/10.52605/16059921_2026_01_85

Введение

Лавинообразное нарастание угроз от вредоносного применения информационно-коммуникационных технологий привело к глубокому осознанию опасностей, которые новые технологии могут нести для устойчивого развития мирового сообщества. Целью статьи является выявление тенденций и перспектив обеспечения кибербезопасности России. Задачи статьи: анализ основных киберугроз для российской экономики; исследование развития нормативного правового обеспечения кибербезопасности субъектов российской экономики; рассмотрение международных аспектов обеспечения кибербезопасности нашей страны. Методология исследования включает структурирование, сравнение, обобщение, системный, экономический, институциональный, логический анализ, индукцию, дедукцию, синтез.

1 Основные киберугрозы для российской экономики

Кибербезопасность можно определить как совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. В Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 2 июля 2021 г. № 400, отмечено, что «быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства. Расширяется использование информационно-коммуникационных технологий для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности, что представляет угрозу международному миру и безопасности. Увеличивается количество компьютерных атак на российские информационные ресурсы. Большая часть таких атак осуществляется с территорий иностранных государств. Инициативы Российской Федерации в области обеспечения международной информационной безопасности встречают противодействие со стороны иностранных государств, стремящихся доминировать в глобальном информационном пространстве» [2]. По данным главы Сбербанка Г.О. Грефа, общий ущерб субъектов мировой экономики от кибератак в 2019 г. составил 2,5 трлн. долл., в 2024 г. – 8,5 трлн. долл. По его прогнозу, в 2026 г. общий ущерб для глобальной экономики от кибератак может составить 10 трлн. долл. [3]. В современных условиях наибольшую опасность для России представляют следующие киберугрозы.

1. Кибератаки на критические информационные инфраструктуры (КИИ) – несанкционированное воздействие на информационные системы, которые используются для управления важными процессами в стране с целью нарушения их работы. К таким процессам относятся: здравоохранение, транспорт, энергетика, связь, банковская сфера, наука, оборона и т.п. Это воздействие может осуществляться с помощью вредоносного программного обеспечения, DDoS-атак, фишинга, социальной инженерии и других методов. Кибератака вирусом Stuxnet в 2010 г., приведшая к остановке сотен центрифуг по обогащению урана в г. Натанзе и на АЭС в г. Бушере в Иране, показала высокую опасность кибератак для экономики и экологии стран и регионов. Начиная с 2010 г., во всём мире участились кибератаки на КИИ с целью как шпионажа, так и диверсий. Анализ кибератак на КИИ доказывает рост их количества и масштабов в геометрической прогрессии из года в год, что напрямую угрожает безопасности мирового сообщества [4]. По мнению Группы правительственных экспертов ООН[1], «опасность вредоносных нападений с использованием ИКТ на критически важную инфраструктуру является реальной и серьезной» [5].

2. Криптоджекинг (англ. cryptojacking) — это киберпреступление, при котором злоумышленники используют компьютеры других пользователей без их ведома для майнинга криптовалют с помощью специального вредоносного программного обеспечения. В последние годы криптоджекинг стал распространенным видом киберпреступности во многих странах мира, в том числе в России. Для заражения компьютеров жертв вредоносным программным обеспечением криптоджекеры используют социальную инженерию, фишинг и другие методы [6].

Приведём наиболее известные инциденты криптоджекинга.

- Coinhive был запущен в 2017 г. как легальный сервис, позволяющий его клиентам получать доход, осуществляя майнинг криптовалюты Monero с использованием их

[1]В состав группы вошли представители Белоруссии, Бразилии, Ганы, Германии, Египта, Израиля, Испании, Кении, Китая, Колумбии, Малайзии, Мексики, Пакистана, Республики Корея, Российской Федерации, Соединенного Королевства Великобритании и Северной Ирландии, Соединенных Штатов Америки, Франции, Эстонии и Японии.

компьютеров. Однако киберпреступники впоследствии захватили сервис Coinhive и через него внедрили вредоносное программное обеспечение на компьютеры миллионов пользователей в разных странах мира. С помощью этого вредоносного программного обеспечения осуществлялся нелегальный майнинг криптовалют. В 2019 г. сервис Coinhive был ликвидирован по решению регулирующих органов.

- В 2018 г. во многих странах мира был распространен компьютерный вирус FacexWorm, который осуществлял нелегальный майнинг криптовалют.
- В 2018 году криптоджекеры проникли в облачную платформу Amazon Web Services, принадлежащую крупнейшему американскому интернет-магазину Amazon. Они осуществляли нелегальный майнинг криптовалют с помощью данной облачной платформы.
- В 2020 году злоумышленники использовали облачную платформу GitHub, принадлежащую американской компании Microsoft, для нелегального майнинга криптовалют [6].

3. Рост числа атак типа «Отказ в обслуживании» (Distributed Denial of Service, DDoS-атаки), под которыми понимаются попытки ограничить доступ пользователей к интернет-сайту путём его намеренной перегрузки направляемыми сообщениями. Общее число DDoS-атак против интернет-сайтов России увеличилось с 147176 в 2021 г. до 2465041 в 2024 г. (в 17 раз) (рисунок 1).

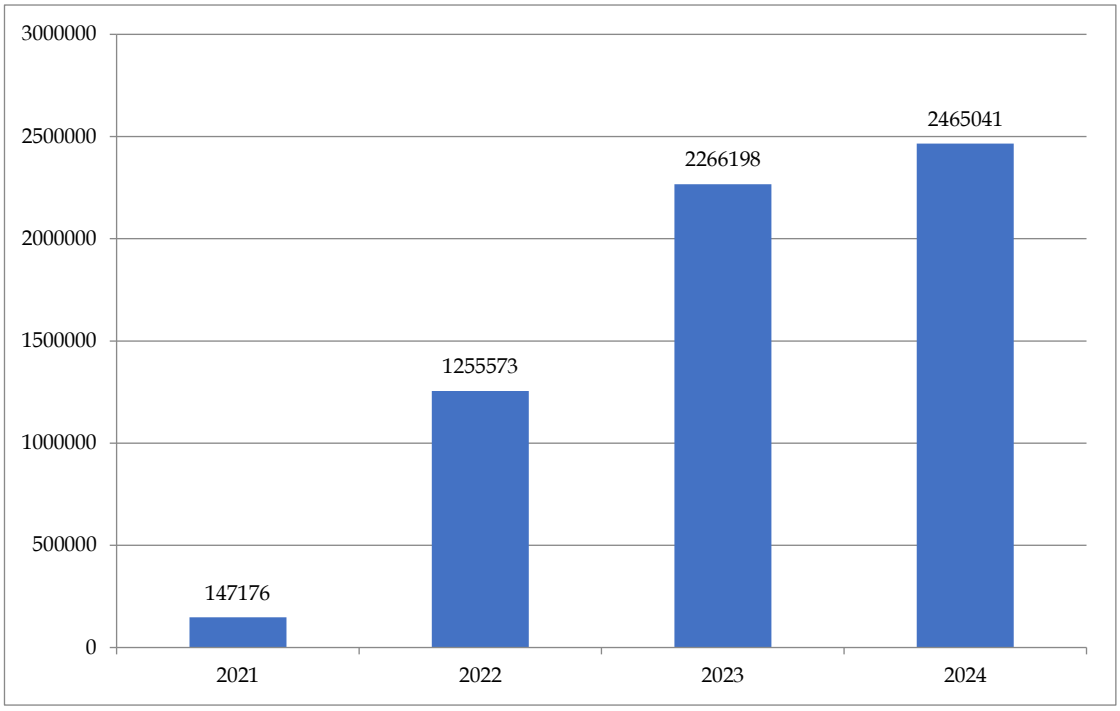

Рис. 1. Динамика общего количества DDoS-атак в России в 2021–2024 гг.
Источник: Отчет по атакам за 2024 год.
URL: https://ddos-guard.net/otchet-ddos-guard-2024.pdf
(дата обращения: 27.03.2025)

В 2024 году источниками 32,4% общего количества DDoS-атак были российские IP-адреса, IP-адреса США – 20,6%, Сингапура – 5,2%, Китая – 5,1%, Индии – 4,7%, Германии – 4,4%, Великобритании – 4,2%, Нидерландов – 3,6%, Индонезии – 2,9%, других стран – 16,9% [7].

4. Угрозы, связанные с функционированием дарквеба.

Особую опасность для России представляет дарквеб (Dark Web, темная паутина) – теневой сегмент Интернета, который зашифрован и поэтому «невидим» для традиционных браузеров (таких как Yandex Browser, Google Chrome). Для доступа к нему необходимо задействование специального программного обеспечения (например, Tor Browser). По состоянию на конец 2019 г. в дарквебе действовали около 8400 сайтов. При этом порядка 57% контента темной паутины носили криминальный характер и были связаны с распространением вредоносных программ, технологий фишинга, DDoS-атак, незаконной торговлей оружием, наркотиками, поддельными документами, украденными персональными данными и т.п. [8]. В настоящее время дарквеб используется во

многих странах мира [8]. В силу своего трансграничного характера, наличия в нём большого количества криминальных сайтов, присущих дарквебу анонимности пользователей, конфиденциальности обмена информацией он представляет собой существенную опасность для всех субъектов мировой экономики.

2 Развитие нормативного правового обеспечения кибербезопасности субъектов российской экономики

В настоящее время в Российской Федерации сформирована и развивается системная нормативная правовая база обеспечения кибербезопасности государства. Базовым документом стратегического планирования, на основе которого сформировано и развивается нормативное правовое обеспечение кибербезопасности субъектов российской экономики, является Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 2 июля 2021 г. №400 «Об утверждении Стратегии национальной безопасности Российской Федерации», которая определяет национальные интересы и стратегические национальные приоритеты Российской Федерации, цели и задачи государственной политики в области обеспечения национальной безопасности и устойчивого развития Российской Федерации на долгосрочную перспективу. Важное значение имеет также Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации», которая представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. В настоящее время в Российской Федерации применяются следующие основные федеральные законы в сфере обеспечения кибербезопасности.

1. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» – регулирует отношения, возникающие при: 1) осуществлении права на поиск, получение, передачу, производство и распространение информации; 2) применении информационных технологий; 3) обеспечении защиты информации.
2. Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры» – регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях её устойчивого функционирования при проведении в отношении неё компьютерных атак. В соответствии со ст. 5 данного Федерального закона в Российской Федерации создана и функционирует Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).
3. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» – регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации.
4. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» – устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

В целом в России на основе принятых нормативных правовых документов создана и успешно функционирует полноценная национальная система обеспечения кибербезопасности [9]. Однако для эффективного противодействия растущей киберпреступности, носящей во многом трансграничный характер, необходимы её дальнейшее развитие и совершенствование с учётом новых вызовов и угроз в глобальном информационном пространстве. Особо важное значение для противодействия растущей киберпреступности имеет сотрудничество России с иностранными партнерами [9]. В связи с этим рассмотрим международные аспекты обеспечения кибербезопасности России.

3 Международные аспекты обеспечения кибербезопасности России

В современных условиях особенно важно развивать международное сотрудничество по вопросам обеспечения информационной безопасности, прежде всего на площадке Организации Объединенных Наций. В противном случае обостряется проблема быстрого неконтролируемого роста информационных рисков, способных вызвать новый беспрецедентный по глубине и силе глобальный финансово-экономический кризис. В Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 2 июля 2021 г. № 400, отмечается необходимость укрепления сотрудничества Российской Федерации с иностранными партнерами в области обеспечения информационной безопасности, в том числе в целях установления международно-правового режима обеспечения безопасности в сфере использования информационно-коммуникационных технологий [2].

В настоящее время работа по решению глобальной проблемы кибербезопасности ведется главным образом на площадке ООН, и в этой сфере достигнут существенный прогресс. 5 декабря 2018 г. Генеральная Ассамблея ООН приняла резолюцию №73/27, в которой зафиксирован свод международных правил, норм и принципов ответственного поведения государств в глобальном информационном пространстве [10]. Эти правила, нормы и принципы не имеют обязательного характера, однако они могут быть полезными для разработки и установления международно-правового режима обеспечения безопасности в сфере использования информационно-коммуникационных технологий. По мнению Министра иностранных дел Российской Федерации С. В. Лаврова, важнейшее значение для противодействия глобальной киберпреступности в настоящее время имеют разработка и принятие универсального кодекса поведения в киберсфере, признанного всем мировым сообществом [11]. Данная инициатива С.В. Лаврова получила развитие в подготовленной Россией и США совместной Резолюции под названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере использования информационно-коммуникационных технологий», которая представляет собой рамочную концепцию правил ответственного поведения государств в киберпространстве. В этой Резолюции, принятой Генеральной Ассамблеей ООН 6 декабря 2021 г. под номером 76/19, отмечается, что все государства заинтересованы в поощрении использования информационно-коммуникационных технологий в мирных целях, а также в предотвращении конфликтов, возникающих в результате их использования. Особое внимание в документе обращено на необходимость «предотвратить использование информационных ресурсов или технологий в преступных или террористических целях» [12]. Важной вехой в борьбе с киберпреступностью стало принятие 24 декабря 2024 г. 193 государствами-членами ООН юридически обязывающей Конвенции ООН против киберпреступности [13]. Конвенция призвана стать прочной основой для налаживания правоохранительного сотрудничества в противодействии использованию информационно-коммуникационных технологий в преступных целях. Документ нацелен на борьбу с несанкционированным доступом к электронным данным и их незаконным перехватом; подлогом, хищением или мошенничеством; отмыванием доходов от противоправных деяний; другими киберпреступлениями. Закрепляется цифровой суверенитет государств над своим информационным пространством, в том числе посредством наращивания международного взаимодействия между компетентными ведомствами. В перспективе сфера охвата соглашения может быть расширена за счет разработки протокола по дополнительным составам преступлений с целью эффективного противодействия использованию ИКТ в террористических и экстремистских целях, а также торговле наркотиками и оружием [14].

Заключение

Резюмируя вышесказанное, следует отметить, что в России создана и успешно функционирует полноценная национальная система обеспечения кибербезопасности. Однако для эффективного противодействия растущей киберпреступности, носящей во многом трансграничный характер, необходимы её дальнейшее развитие и совершенствование с учётом новых вызовов и угроз в глобальном информационном пространстве. Актуальной задачей является укрепление сотрудничества Российской Федерации с иностранными партнерами в области обеспечения информационной безопасности, в том числе в целях установления эффективно действующего международно-правового режима обеспечения безопасности в сфере использования информационно-коммуникационных технологий. Шагом вперёд в сфере обеспечения глобальной кибербезопасности стало принятие Резолюции Генеральной Ассамблеи ООН от 24 декабря 2024 г.

№79/243, которой была утверждена Конвенция ООН против киберпреступности. Данную Конвенцию целесообразно дополнить протоколом по дополнительным составам преступлений, включая использование ИКТ в террористических и экстремистских целях, в мошенничестве в банковской сфере, а также в торговле наркотиками, оружием, поддельными документами, вредоносными программами, технологиями фишинга, DDoS-атак, прочими запрещёнными товарами и услугами. Это окажет содействие устойчивому развитию мирового сообщества.

Благодарности

Исследование выполнено за счет гранта Российского научного фонда №24-18-00443, https://rscf.ru/project/24-18-00443

Литература

1. Кондратьев Н.Д. Большие циклы конъюнктуры и теория предвидения. М.: Экономика, 2002.
2. Стратегия национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 2 июля 2021 г. №400). URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=602263723 (дата обращения: 27.03.2025).
3. Греф оценил ожидаемый ущерб мировой экономике от кибератак к 2026 году. 13.11.2024. URL: https://1prime.ru/20241113/gref-852788594.html (дата обращения: 27.03.2025).
4. Ромашкина Н.П. Проблема международной информационной безопасности в ООН (история, спорные вопросы, перспективы)//Мировая экономика и международные отношения. 2020. Т. 64. №12. С. 25-32.
5. Доклад Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности от 22 июля 2015 г. A/70/174. URL: https://documents.un.org/doc/undoc/gen/n15/228/37/pdf/n1522837.pdf (дата обращения: 27.03.2025).
6. Miah S. Cryptomining malware. 06.08.2024. URL: https://www.webopedia.com/definitions/cryptomining-malware (дата обращения: 27.03.2025).
7. DDoS-атаки в России. 24.12.2024. URL: https://www.tadviser.ru/index.php/Статья:DDoS-атаки_в_России (дата обращения: 27.03.2025).
8. Juan H. Dark web statistics & trends for 2024. 12.02.2024. URL: https://preyproject.com/blog/dark-web-statistics-trends (дата обращения: 27.03.2025).
9. Лопатин В.Н. Информационное право: учебник. – 3-е изд., изм. и доп. – М.: Проспект, 2023. 656 с.
10. 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 27.03.2025).
11. 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 (дата обращения: 27.03.2025).
12. Резолюция Генеральной Ассамблеи ООН от 6 декабря 2021 г. №76/19 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере использования информационно-коммуникационных технологий». URL: https://documents.un.org/doc/undoc/gen/n21/377/51/pdf/n2137751.pdf (дата обращения: 27.03.2025).
13. Резолюция Генеральной Ассамблеи ООН от 24 декабря 2024 г. №79/243 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». URL: https://docs.un.org/ru/A/RES/79/243 (дата обращения: 27.03.2025).
14. О принятии Конвенции ООН против киберпреступности. 26.12.2024. URL: https://www.mid.ru/print/?id=1989289&lang=ru (дата обращения: 27.03.2025).
15. Годовой отчет Банка России за 2023 год. URL: https://cbr.ru/Collection/Collection/File/49041/ar_2023.pdf (дата обращения: 27.03.2025).

16. Декларация Генеральной Ассамблеи ООН от 25 сентября 2015 г. «Преобразование нашего мира: Повестка для в области устойчивого развития на период до 2023 года». URL: https://docs.cntd.ru/document/420355765 (дата обращения: 27.03.2025).
17. Декларация тысячелетия Организации Объединенных Наций. Утверждена Резолюцией Генеральной Ассамблеи ООН от 08 сентября 2000 г. №55/2. URL: https://docs.cntd.ru/document/901784387 (дата обращения: 27.03.2025).
18. Богданов А.А. Тектология (Всеобщая организационная наука): в 2 кн. М.: Экономика, 1989.
19. Международная информационная безопасность: Теория и практика : учебник для вузов: в 3 т. / под общ. ред. А.В. Крутских. М.: Издательство «Аспект Пресс», 2021.
20. Арбатов А.Г., Богданов К.В., Стефанович Д.В. и др. Международная безопасность: новый миропорядок и технологическая революция. М.: Издательство «Весь Мир», 2023. 432 с.
21. Белоус А.И., Солодуха В.А. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. М.: Техносфера, 2021. 482 с.
22. Ашманов И.С., Касперская Н.И. Цифровая гигиена. СПб.: Издательство «Питер», 2022. 398 с.
23. Криворучко С.В., Медведева М.Б., Шуст П.М. Новые риски цифровых финансовых сервисов//Банковские услуги. 2024. №10. С. 30-37.
24. Шеремет И.А. Обеспечение кибербезопасности в условиях развития цифровой экономики//Вестник Московского университета. Серия 25: Международные отношения и мировая политика. 2019. №1. С. 3-19.
25. Никитин А.И. Потенциал кризисного реагирования и военно-техническое сотрудничество стран ЕС//Современная Европа. 2020. № 5. С. 142-154.
26. Аккаева Х.А. Кибератаки на критическую информационную инфраструктуру//Право и управление. 2023. №9. С. 347-351.
27. Wang H., Lau N., Gerdes R. Examining Cybersecurity of Cyberphysical Systems for Critical Infrastructures Through Work Domain Analysis//Human Factors. 2018. Vol. 60. №5. P. 699-718.
28. Абрамов Е.С. Построение адаптивной системы информационной безопасности//Известия ЮФУ. Технические науки. 2009. №11. С. 99-109.

TRENDS AND PERSPECTIVES OF PROVISION OF CYBERSECURITY IN RUSSIA

Pishchik, Victor Yakovlevich

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

Alekseev, Petr Victorovich

Candidate of economic sciences, leading researcher
Financial University under the Government of the Russian Federation, institute for global research
Moscow, Russian Federation
palekseev@fa.ru

Abstract

One of the topical problems of the world community at present is the rapid large-scale growth of global cybercrime observed over the past thirty years. Nowadays particularly dangerous for subjects of the Russian economy today are: attacks on critical information infrastructures; cryptojacking; the growing number of DDoS attacks on websites of Russian organizations; threats associated with the functioning of the dark web. In Russia an effective national cybersecurity system has been created and is successfully functioning. However, in order to effectively counter the growing cybercrime, which is largely transborder in nature, its further development and improvement are necessary, taking into account new challenges and threats in the global information space. It is expedient to strengthen cooperation between the Russian Federation and foreign partners in the field of information security, including for the purpose of establishing an effectively functioning international legal regime for ensuring security in the field of using information and communication technologies (ICT). In this regard, it is proposed to supplement the Convention against Cybercrime, adopted by the United Nations on December 24, 2024, with a protocol on additional crimes, including the use of ICT for terrorist and extremist purposes, banking fraud, as well as trafficking in drugs, weapons, counterfeit documents, malware, technologies of phishing, DDoS attacks, and other prohibited goods and services. This will contribute to the sustainable development of the global community.

Keywords

digitalization; information and communication technologies; ICT; critical information infrastructures; international information security; IIS; information security; cybersecurity; cybercrime; cyberattacks; cyber threats; cyber risks; global problems; prevention of global economic crises

References

1. Kondratiev N.D. Bol'shie tsikly konyunktury i teoriya predvideniya. M.: Ekonomika, 2002.
2. Strategiya natsional'noi bezopasnosti Rossiiskoi Federatsii (utverzhdena Ukazom Prezidenta RF ot 2 iyulya 2021 g. №400). URL: http://pravo.gov.ru/proxy/ips/?docbody= &firstDoc=1&lastDoc=1&nd=602263723 (data obrashcheniya: 27.03.2025).
3. Gref otsenil ozhidaemyi ushcherb mirovoi ekonomike ot kiberatak k 2026 godu. 13.11.2024. URL: https://1prime.ru/20241113/gref-852788594.html (data obrashcheniya: 27.03.2025).
4. Romashkina N.P. Problema mezhdunarodnoi informatsionnoi bezopasnosti v OON (istoriya, spornye voprosy, perspektivy)//Mirovaya ekonomika i mezhdunarodnye otnosheniya. 2020. T. 64. №12. S. 25-32.
5. Doklad Gruppy pravitel'stvennykh ekspertov OON po dostizheniyam v sfere informatizatsii i telekommunikatsii v kontekste mezhdunarodnoi bezopasnosti ot 22 iyulya 2015 g. A/70/174. URL: https://documents.un.org/doc/undoc/gen/n15/228/37/ pdf/n1522837.pdf (data obrashcheniya: 27.03.2025).
6. Miah S. Cryptomining malware. 06.08.2024. URL: https://www.webopedia.com/definitions/cryptomining-malware (data obrashcheniya: 27.03.2025).

7. DDoS-ataki v Rossii. 24.12.2024. URL: https://www.tadviser.ru/index.php/Stat'ya:DDoS-ataki_v_Rossii (data obrashcheniya: 27.03.2025).
8. Juan H. Dark web statistics & trends for 2024. 12.02.2024. URL: https://preyproject.com/blog/dark-web-statistics-trends (data obrashcheniya: 27.03.2025).
9. Lopatin V.N. Informatsionnoe pravo: uchebnik. – 3-e izd., izm. i dop. – M.: Prospekt, 2023. 656 c.
10. 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 (data obrashcheniya 27.03.2025).
11. Lavrov S.V. Global'nye problemy kiberbezopasnosti i mezhdunarodnye initsiativy Rossii po bor'be s kiberprestupnost'yu//Vneshneekonomicheskie svyazi. 2020. №9. URL: https://eer.ru/sites/default/files/pdf/eer_1_2020.pdf (data obrashcheniya: 27.03.2025).
12. Rezolyutsiya General'noi Assamblei OON ot 6 dekabrya 2021 g. №76/19 «Dostizheniya v sfere informatizatsii i telekommunikatsii v kontekste mezhdunarodnoi bezopasnosti i pooshchrenie otvetstvennogo povedeniya gosudarstv v sfere ispol'zovaniya informatsionno-kommunikatsionnykh tekhnologii». URL: https://documents.un.org/doc/undoc/gen/n21/377/51/pdf/n2137751.pdf (data obrashcheniya: 27.03.2025).
13. Rezolyutsiya General'noi Assamblei OON ot 24 dekabrya 2024 g. №79/243 «Protivodeistvie ispol'zovaniyu informatsionno-kommunikatsionnykh tekhnologii v prestupnykh tselyakh». URL: https://docs.un.org/ru/A/RES/79/243 (data obrashcheniya: 27.03.2025).
14. O prinyatii Konventsii OON protiv kiberprestupnosti. 26.12.2024. URL: https://www.mid.ru/print/?id=1989289&lang=ru (data obrashcheniya: 27.03.2025).
15. Godovoi otchet Banka Rossii za 2023 god. URL: https://cbr.ru/Collection/Collection/File/49041/ar_2023.pdf (data obrashcheniya: 27.03.2025).
16. Deklaratsiya General'noi Assamblei OON ot 25 sentyabrya 2015 g. «Preobrazovanie nashego mira: Povestka dlya v oblasti ustoichivogo razvitiya na period do 2023 goda». URL: https://docs.cntd.ru/document/420355765 (data obrashcheniya: 27.03.2025).
17. Deklaratsiya tysyacheletiya Organizatsii Ob"edinennykh Natsii. Utverzhdena Rezolyutsiei General'noi Assamblei OON ot 08 sentyabrya 2000 g. №55/2. URL: https://docs.cntd.ru/document/901784387 (data obrashcheniya: 27.03.2025).
18. Bogdanov A.A. Tektologiya (Vseobshchaya organizatsionnaya nauka): v 2 kn. M.: Ekonomika, 1989.
19. Mezhdunarodnaya informatsionnaya bezopasnost': Teoriya i praktika : uchebnik dlya vuzov: v 3 t. / pod obshch. red. A.V. Krutskikh. M.: Izdatel'stvo «Aspekt Press», 2021.
20. Arbatov A.G., Bogdanov K.V., Stefanovich D.V. i dr. Mezhdunarodnaya bezopasnost': novyi miroporyadok i tekhnologicheskaya revolyutsiya. M.: Izdatel'stvo «Ves' Mir», 2023. 432 s.
21. Belous A.I., Solodukha V.A. Osnovy kiberbezopasnosti. Standarty, kontseptsii, metody i sredstva obespecheniya. M.: Tekhnosfera, 2021. 482 s.
22. Ashmanov I.S., Kasperskaya N.I. Tsifrovaya gigiena. SPb.: Izdatel'stvo «Piter», 2022. 398 s.
23. Krivoruchko S.V., Medvedeva M.B., Shust P.M. Novye riski tsifrovykh finansovykh servisov//Bankovskie uslugi. 2024. №10. S. 30-37.
24. Sheremet I.A. Obespechenie kiberbezopasnosti v usloviyakh razvitiya tsifrovoi ekonomiki//Vestnik Moskovskogo universiteta. Seriya 25: Mezhdunarodnye otnosheniya i mirovaya politika. 2019. №1. S. 3-19.
25. Nikitin A.I. Potentsial krizisnogo reagirovaniya i voenno-tekhnicheskoe sotrudnichestvo stran ES//Sovremennaya Evropa. 2020. № 5. S. 142-154.
26. Akkaeva Kh.A. Kiberataki na kriticheskuyu informatsionnuyu infrastrukturu//Pravo i upravlenie. 2023. №9. S. 347-351.
27. Wang H., Lau N., Gerdes R. Examining Cybersecurity of Cyberphysical Systems for Critical Infrastructures Through Work Domain Analysis//Human Factors. 2018. Vol. 60. №5. P. 699-718.
28. Abramov E.S. Postroenie adaptivnoi sistemy informatsionnoi bezopasnosti//Izvestiya YuFU. Tekhnicheskie nauki. 2009. №11. S. 99-109.