Published in the Russian Federation
Sochi Journal of Economy
Has been issued since 2007.
ISSN: 2541-8114
2018, 12(1): 68-78

www.vestnik.sutr.ru

UDC 33 + 004.056

Cybersecurity Issues in the Implementation of the Digital Economy

Vladlena S. Oladko [a, *]

[a] Financial university under the Government of the Russian Federation, Russian Federation

Abstract

The article discusses the important branch of development of economic system as the digital economy. The digital economy is a future step of global economic system development due to the transformation of all human activities under the influence of information and telecommunication technologies. The division of the digital economy into economic hubs is presented. Each hub is described. The objects and subjects of the digital economy's information infrastructure are analyzed, conclusion about the problems of its cybersecurity are made. The statistics of cybersecurity events are studied and classified into three groups – normal events, abnormal events and threat events. On the basis of the information infrastructure and events provides a list of potential cybersecurity incidents and their consequences to the digital economy's subjects and objects. The risk factors for cybersecurity and their management strategies are defined. It draws conclusions about the need to ensure the security of the information infrastructure on the side of consumer subjects, subjects of manufacturers, kernel objects, and remote services, networks and communication channels, data stores. The author in the conclusion suggests the scheme of realization of protection mechanisms from cybersecurity threats on two levels: organizational-administrative and technical.

Keywords: digital production, information infrastructure, risk, damage, e-commerce, Internet market, information security.

1. Введение

Современный уровень развития инфокоммуникационных технологий, массовый охват практически всех отраслей мировой экономики глобальными сетями и наличие сетевого общества постепенно привели к необходимости модернизации классической экономической системы и сферы услуг. Решением данной проблемы стало внедрение цифровой экономики, задачей которой является стимулирование цифрового производства, создание универсальных маркетплейсов для эффективного предоставления данных, продуктов и услуг во всех сферах жизни общества, повышение качества товаров и услуг, произведённых с использованием современных цифровых технологий. О переходе на цифровую экономику в конце 2016 г. объявил Президент России Владимир Путин. В послании к Федеральному Собранию глава государства предположил, что в ближайшее десятилетие ИТ-индустрия станет одной из ключевых экспортных отраслей страны, в связи с чем была рабочая группа Экономического совета при президенте РФ по направлению «Цифровая экономика».

Программа «Цифровая экономика» была утверждена распоряжением Правительства РФ №1632-р от 28 июля 2017 года [1] и создается в целях ускорения цифровой трансформации Российской Федерации. Основная задача программы — создание основы

* Corresponding author
E-mail addresses: oladko.vs@yandex.ru (V.S. Oladko)

для развития технологий в России. Эта основа должна складываться из правового регулирования, образования, инфраструктуры, стимулирования разработок и исследований, информационной безопасности как информационной инфраструктуры, так и страны в целом.

2. Материалы и методы

Для написания статьи были использованы материалы научной, учебной литературы, законодательство Российской Федерации, постановления Правительства, статистические данные, собранные из печатных и электронных источников информации. Основными методами исследования при выполнении работы были: метод описания, системного анализа, аналогии и обобщения, а также элементы теории управления рисками.

3. Обсуждение

Информационная инфраструктура цифровой экономики

Цифровая экономика — это система экономических, социальных и культурных отношений, основанных на использовании цифровых технологий [2]. На сегодняшний момент цифровая экономика в России — это те сегменты рынка, где добавленная стоимость создается с помощью цифровых (информационных) технологий.

По данным российского интернет форума РИФ+КИБ 2017 [3] вклад цифровой экономики в ВВП России оценивается в 2,8 %, при этом 19 % от ВВП формируют интернет-зависимые рынки. Эффективное развитие рынков в цифровой экономике возможно только при наличии развитых технологий, поэтому разработанная программа развития сфокусирована на двух базовых направлениях:

–институты, создающие условия для развития цифровой экономики: нормативное регулирование, кадры и образование;

–основные инфраструктурные элементы цифровой экономики: информационная инфраструктура и информационная безопасность.

Сегодня кадровая индустрия Рунета насчитывает 2,5 млн сотрудников, инфраструктура и программное обеспечение оцениваются в 2 000 млрд рублей, Маркетинг и реклама – 171 млрд рублей, цифровой контент – 63 млрд рублей, электронная коммерция – 1238 млрд рублей.

Анализ источников [4-7] показывает, что цифровая экономика строится на базе веб-приложений, сетей передачи данных и современных информационных технологий к которым можно отнести большие данные, нейротехнологии, искусственный интеллект, системы распределённого реестра, квантовые технологии, интернет-вещей и промышленный интернет, робототехнику, сенсорику, виртуальная и дополненная реальности. Основным продуктом цифровой экономики является цифровое производство, удаленная продажа и обмен товара, предоставление электронных платежных сервисов, информации и услуг.

В 2017 году аналитики Российской ассоциации электронных коммуникаций (РАЭК) впервые поделили экономическую систему цифровой экономики на хабы [8]:

1) Государство и общество;
2) Маркетинг и реклама;
3) Финансы и торговля;
4) Инфраструктура и связь;
5) Медиа и развлечения;
6) Кибербезопасность;
7) Образование и кадры;
8) Стартапы.

Каждый хаб занимает свою нишу и вносит вклад в развитие всей экономической системы РФ. Для обеспечения существования и выполнения целевых бизнес-процессов каждого хаба системы цифровой экономики используется информационная инфраструктура (см. рис. 1).

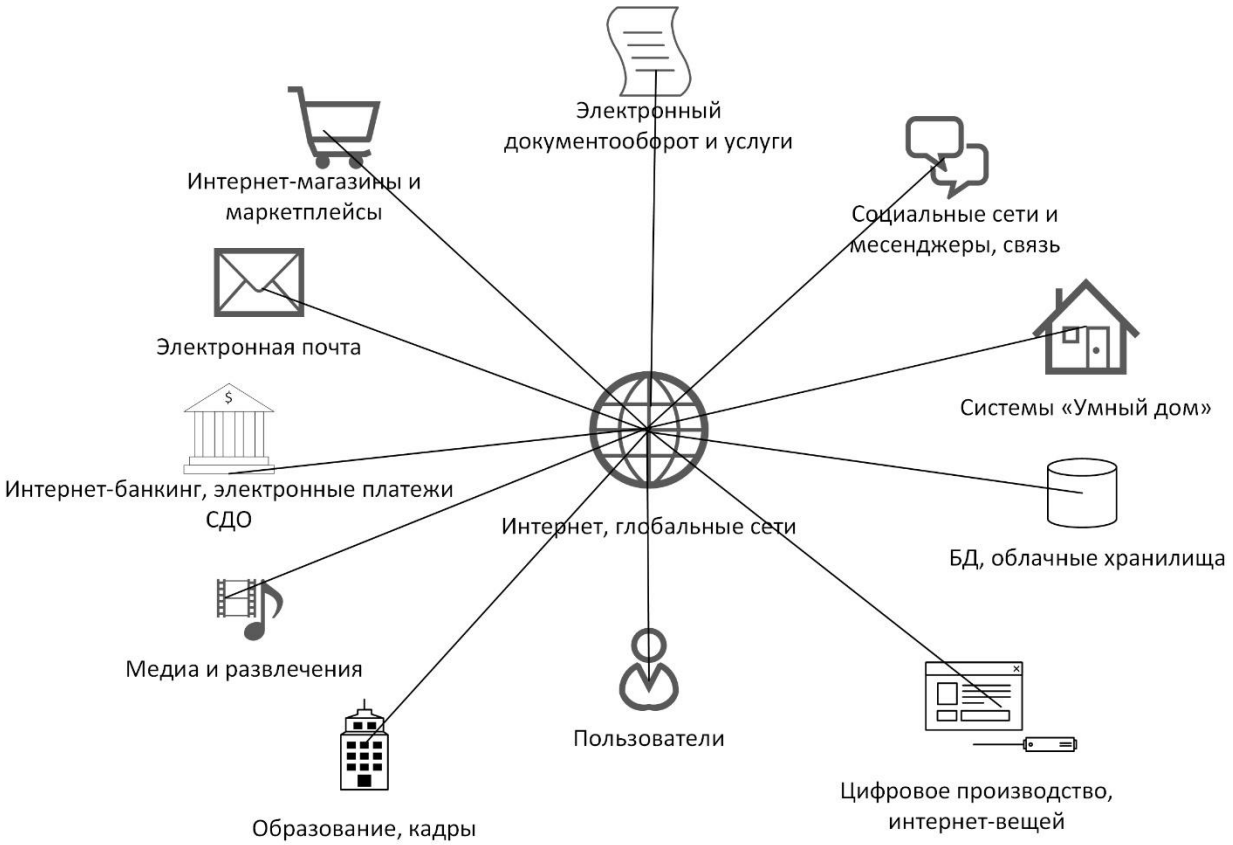

Рис. 1. Информационная инфраструктура цифровой экономики

Информационная инфраструктура цифровой экономики имеет распределённую архитектуру и представляет собой гетерогенную интегрированную систему с полным жизненным циклом, которая окружена существенной средой [9] порождающей угрозы безопасности случайного или умышленного характера. Каждая угроза несет потенциальные риски обусловленные:

– наличием круглосуточно доступных удаленных сервисов и каналов обслуживания;

– использованием открытых или слабозащищенных протоколов передачи данных;

– регулярным доступом к услугам и сервисам множества лиц;

– наличием доступных из внешних сетей интерфейсов удаленного доступа и управления сетевым оборудованием и серверами, которые должны быть доступны только ограниченному числу администраторов;

– привязкой счетов платежных карт и вкладов к интернет-банку и платежным сервисам;

– низкой информационной грамотностью некоторых категорий пользователей;

– навязыванием дополнительных информационных сервисов;

– ростом числа уязвимостей и использованием компонентов с известными уязвимостями;

– редким обновлением программного-аппаратного обеспечения;

– незащищенным хранением личных данных пользователей;

– небезопасной конфигурацией и ошибками в конфигурации объектов информационной инфраструктуры;

– слабыми паролями и утерей аутентификаторов;

– некорректной аутентификацией и управлением сессией пользователей;

– небезопасной десериализацией данных и ошибками в коде сервисов услуг и веб-приложений;

– отсутствием подсистем регистрации событий и мониторинга.

Результатом реализации угроз являются деструктивные информационные и физические воздействия на циркулирующие данные, бизнес-процессы, инфраструктурные

технические, программные и экономические компоненты, пользователей системы. Последствиями воздействий является нарушение устойчивого функционирования подсистем информационной инфраструктуры цифровой экономики, внедрение вредоносного кода и XML-сущностей, межсайтовый скриптинг, мошенничество, хищение денежных средств, компрометация платежных транзакций, утечка персональных данных пользователей, кража «цифровой личности», а также финансовый ущерб и снижение репутации участников цифрового взаимодействия.

События и инциденты кибербезопасности

Каждое действие пользователей и процедуры реализации технологического процесса порождают множество событий, характеризующих процессы функционирования информационной инфраструктуры систему цифровой экономики.

Все события с точки зрения информационной безопасности можно разделить на три группы – нормальные события, аномальные события, опасные события [10]. Описание каждой группы событий представлено в таблице 1.

Таблица 1. Группы событий кибербезопасности цифровой экономики

№	Группа событий	Описание
1	Нормальные события	Описывают процесс штатного функционирования объектов информационной инфраструктуры системы цифровой экономики в соответствии с их задачами и согласно документам, регламентирующим работу. Составляют большую часть от всех событий происходящих в системе.
2	Аномальные события	Подозрительная активность, которая характеризуется временным изменением штатного режима функционирования объектов информационной инфраструктуры системы цифровой экономики, неполным исполнением услуг, прерыванием бизнес-процесса. Может быть вызвана резким увеличением спроса на некоторый цифровой товар или услугу, временным ростом нагрузки на сеть, появлением новых пользователей, обновлением программно-аппаратного обеспечения, деятельностью злоумышленника, сбоями в работе обеспечивающих подсистем и объектов информационной инфраструктуры. При регистрации данного типа событий необходим их дальнейший анализ и последующий контроль до выяснения причин и источников аномалии.
2	Опасные события	Описывают процессы связанные с прерыванием бизнес-процессов, нарушением безопасности данных, кражей финансовых средств ошибками, сбоями и отказами объектов информационной инфраструктуры цифровой экономики. Связаны с атаками злоумышленника и деструктивными воздействиями техногенного и природного характера. Требует немедленного применения специализированных средств и мер, направленных на обнаружение источника и причин нарушения, быстрого блокирования и устранения последствий.

Согласно представленной выше классификации к событиям информационной безопасности в первую очередь можно отнести аномальные события и опасные события. Событие информационной безопасности - какое-либо событие информационной безопасности, идентифицируемое появлением определенного состояния системы, сервиса или сети, указывающее на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности [11]. Как было показано Волковым А.Н. в своем докладе «Кибербезопасность в цифровом мире» на прошедшей в ноябре 2017 года в рамках IV Международного форума Финансового университета «Что день грядущий нам готовит?» конференции «Информационная безопасность надежный щит цифровой экономики» [12] число событий безопасности напрямую связано со сложностью информационной инфраструктуры, количеством субъектов и объектов взаимодействия в системе цифровой экономики и при наращивании сложности возрастает в геометрической прогрессии. Каждое событие не существует по отдельности, а является частью процесса реализации инцидента информационной безопасности (см. рис. 2).

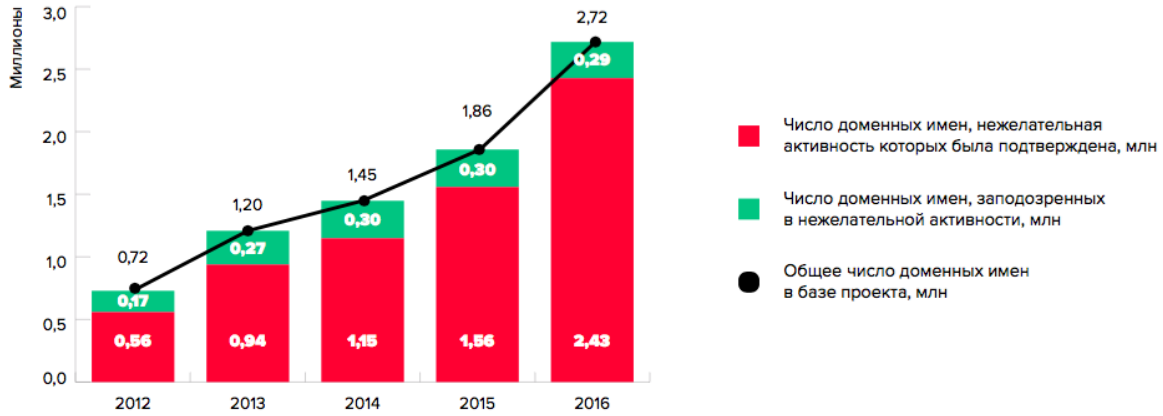

Рис.2. Тенденция роста числа событий безопасности за 2012 – 2016 гг.

Поскольку информационная инфраструктура цифровой экономики построена на использовании удаленных рабочих мест и сетевых сервисов, веб-приложений, маркетплейсов, платежных систем и систем электронной коммерции различного типа, то ей будут присуще все типы инцидентов безопасности характерные для составляющих ее систем [5; 13; 14]:

– утечка чувствительных данных и конфиденциальной информации;
– утечка персональных и личных данных пользователей;
– компрометация данных и транзакций;
– мошенничество;
– отказ одной из сторон взаимодействия от обязательств;
– атаки на пользователей;
– атаки на системы защиты информационной инфраструктуры;
– атаки на реализацию объектов информационной инфраструктуры;
– перехват управления объектами информационной инфраструктуры;
– отказ в обслуживании;
– кража финансовых средств и их электронных заместителей;
– деструктивные действия вредоносного ПО;
– прерывание ключевых бизнес-процессов.

Таким образом, существование и развитие цифровой экономики невозможно без развитой распределенной информационной архитектуры с безопасными технологиями удаленного доступа, обмена данными и защиты личности участников взаимодействия. Поэтому чтобы создать цифровое производство и обеспечить устойчивое существование и развитие цифровой экономики, необходимо уметь эффективно противодействовать киберугрозам и управлять рисками кибербезопасности.

Управление рисками кибербезопасности цифровой экономики

Процессы управления рисками кибербезопасности цифровой экономики должны учитывать требования к безопасности ключевой информационной инфраструктуры РФ и охватывать все субъекты и объекты информационной инфраструктуры цифровой экономики. Процессы управления рисками реализуются двумя взаимосвязанными и чередующимися видами деятельности (см. рис. 3):

– регламентной оценкой рисков;
– нейтрализацией рисков за счет выбора эффективных и экономичных защитных механизмов и средств.

Рис. 3. Схема управления рисками кибербезопасности информационной инфраструктуры системы цифровой экономики

Регламентная оценка рисков, описывается этапами:

–инвентаризация анализируемых объектов информационной инфраструктуры цифровой экономики;

–выбор методики оценки рисков, может быть количественной, качественной или гибридной;

–идентификация активов;

–анализ угроз и их последствий для отдельных объектов информационной инфраструктуры, бизнес-процессов, субъектов цифрового взаимодействия и все системы в целом;

–определение уязвимостей в защите объектов и субъектов;

–оценка рисков и интерпретация полученных результатов.

Действия по нейтрализации рисков включают:

–выбор стратегии по управлению выявленными рисками;

–принятие допустимых рисков;

–выбор механизмов и дополнительных средств обеспечения безопасности, направленных на устранение выявленных уязвимостей, ликвидацию и уменьшение риска;

–реализация и проверка выбранных мер;

–оценка остаточного риска.

4. Результаты

Поскольку информационная инфраструктура цифровой экономики представляет собой сложную многоуровневую систему, использующую технологии клиент-серверного взаимодействия, распределенного доступа к данным посредством глобальных сетей, то при реализации стратегии управления рисками кибербезопасности необходимо использовать защиту на каждом уровне. При этом необходимо учитывать, что система цифровой экономики является критически важным объектом информационной инфраструктуры, следовательно, при планировании стратегии защиты информации необходимо учитывать требования безопасности к данным объектам.

Защита строится на организационно-административном уровне и техническом (см. рис. 4), соотношение между которыми распределяется в соотношении 70 % и 30 % соответственно.

Задачами организационно-административного уровня являются:

–планирование стратегии и мер обеспечения безопасности;

–разработка и оформление документов, инструкций и политики безопасности для объектов информационной инфраструктуры цифровой экономики;

–внедрение административных мер по защите и контрою действий персонала, уровня защищенности объектов;

–оценка благонадежности и рисков деструктивного поведения субъектов (персонала, пользователей, потребителей услуг) цифровой экономики;

–повышение уровня осведомленности персонала, проведение тренингов;

–контроль качества подготовки и профессиональных компетенций ответственных за защиту информации;

–внедрение технических мер для обеспечения информационной безопасности.

Рис. 4. Уровни обеспечения кибербезопасности информационной инфраструктуры цифровой экономики

Технический уровень защиты объектов информационной-инфраструктуры цифровой экономики подразумевает использование специализированных программных, программно-аппаратных и технических средств защиты. Защита охватывает сетевую безопасность, безопасность программных средств и автоматизированных рабочих мест пользователей, вопросы управления доступом, обеспечения конфиденциальности, целостности данных и транзакций, а также управление непрерывностью бизнеса. Средства образуют интегрированную систему, включающую [15]:

–средства защиты от атак на прикладном уровне (WAF);

–средства однократной и многофакторной аутентификации;

–средства управления идентификационными данными и доступом (IAM);

–средства управления доступом к информации (IRM);

–механизмы контроля доступа к периферийным устройствам и приложениям;

–системы защиты от утечки конфиденциальной информации (DLP)

–инфраструктуры открытых ключей (PKI);

– средства антивирусной защиты;
– механизмы защиты электронной почты от спама, вирусов и других угроз;
– механизмы контентной фильтрации web-трафика;
– средства контроля целостности программных сред;
– средства криптографической защиты при хранении информации;
– системы управления инцидентами и событиями ИБ (SIEM);
– системы управления соответствием требованиям ИБ (Compliance Management);

Целью планирования, проектирования, внедрения, эксплуатации и совершенствования интегрированной системы защиты объектов информационной инфраструктуры цифровой экономики является выполнение требований безопасности регуляторов, минимизация рисков и обеспечение приемлемого уровня защищенности при допустимых затратах (см. рис. 5).

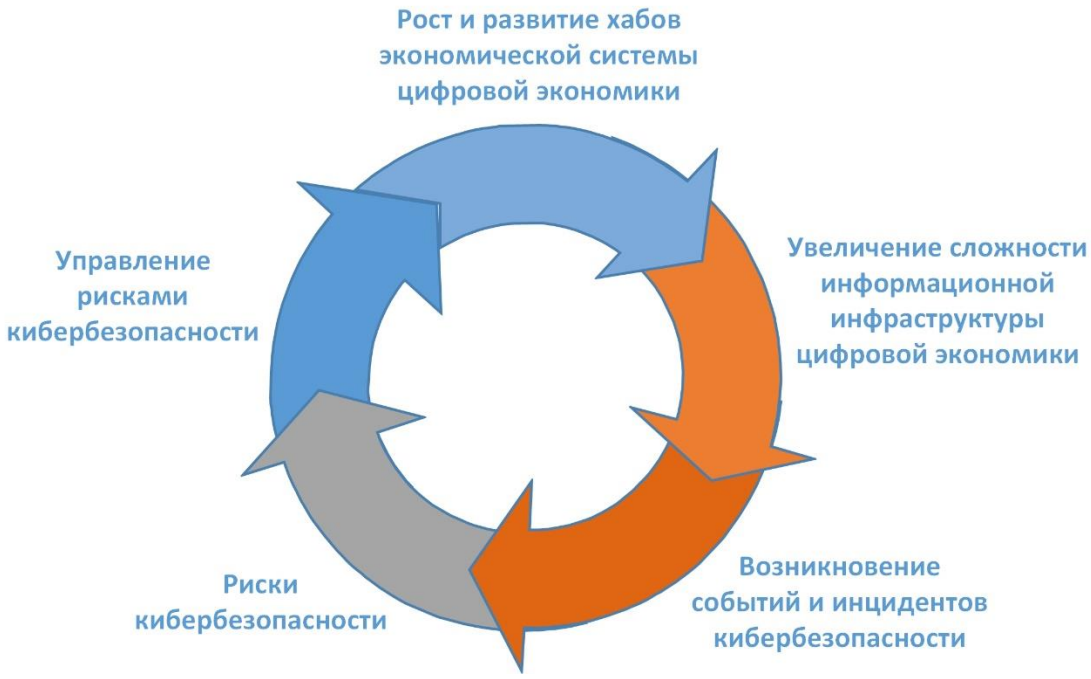

Рис.5. Влияние процессов кибербезопасности на цифровую экономику

Адекватность решения задач, необходимых для достижения поставленной цели будет оказывать непосредственное влияние на экономическую эффективность объектов системы цифровой экономики, развитие отдельных хабов экономической системы цифровой экономики и успешность реализации всей программы «Цифровая экономика» в целом.

5. Заключение

Цифровая экономика представляет собой сложную гетерогенную систему, включающую множество субъектов, объектов информационной инфраструктуры, бизнес-процессов, взаимодействующих между собой и разделенных на хабы. Успешность и рост этой экономической системы невозможны без применения и совершенствования сетей, информационных технологий, систем искусственного интеллекта, что в свою очередь приводит к росту числа событий и инцидентов безопасности. Для противодействия рискам и ущербу от инцидентов необходимо проводить ряд мероприятий, направленных на управление рисками. Для повышения эффективности данных мероприятий предлагается использовать интегрированную систему защиты объектов информационной инфраструктуры, реализованную на организационно-административном и техническом уровнях.

Литература

1. Распоряжение Правительства от 28 июля 2017 года №1632-р. Об утверждении программы «Цифровая экономика Российской Федерации» [Электронный ресурс]. URL: http://m.government.ru/all/28653/

2. Беркана А. Зачем России цифровая экономика//Rusbase [Электронный ресурс].URL: https://rb.ru/longread/digital-economy-in-russia/

3. Материалы конференции Российский Интернет Форум РИФ+КИБ 2017 [Электронный ресурс].URL: http://2017.russianinternetforum.ru/itogi/

4. Шмырова В. «Цифровая экономика» обойдется в 520 миллиардов//Издание о высоких технологиях C-news [Электронный ресурс]. URL: http://www.cnews.ru /news/top/2017-12-18_zapusk_tsifrovoj_ekonomiki_obojdetsya_v_520_milliardov

5. Введение в «Цифровую» экономику / А.В. Кешелава В.Г. Буданов, В.Ю. Румянцев и др.; под общ. ред. А.В. Кешелава; гл. «цифр.» конс. И.А. Зимненко. – ВНИИГеосистем, 2017. –28 с.

6. Сударушкина И.В., Стефанов Н.А. Цифровая экономика // Азимут научных исследований: экономика и управление. 2017. Т.6. №1. С. 182-184.

7. Бабкин А.В., Буркальцева Д.Д., Костень Д.Г., Воробьев Е.Н. Формирование цифровой экономики в России: сущность, особенности, техническая нормализация, проблемы развития // Научно-технические ведомости СПбГПУ. Экономические науки.2017. Т.10. №3. С. 9-25.

8. Цифровая экономика 2016 / Итоговая брошюра исследования Экономика Рунета 2015–2016. [Электронный ресурс]. URL: http://raec.ru/live/analytics/9863/

9. Аткина В.С. Разработка методов, алгоритмов и программы для анализа катастрофоустойчивости информационных систем / Диссертация на соискание ученой степени кандидата технических наук. Южный федеральный университет. Волгоград, 2013.

10. Виттенбург Е.А., Оладько В.С., Пушкарская А.И. Модель оценки безопасности на основе данных мониторинга информационной системы // Информационные системы и технологии. 2017. № 4 (102). С. 87-93.

11. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности // Система ГАРАНТ. URL: http://base.garant.ru/70795320/#ixzz4MOF779bo

12. Волков А.Н. Кибербезопасность в цифровом мире // Материалы конференции Информационная безопасность в цифровом мире 29 ноября 2017, Финуниверситет г. Москва.

13. Oladko V.S. The model of information security audit in the information system of e-commerce type of B2E // Sochi Journal of Economy. 2016. № 2 (40). С. 117-126.

14. Борзунов А.А. Развитие человеческих ресурсов как ключевой фактор обеспечения экономической безопасности компании в условиях цифровой экономики [Текст] // Проблемы современной экономики: материалы VI Междунар. науч. конф. (г. Самара, август 2017 г.). Самара: ООО "Издательство АСГАРД", 2017. С. 94-97. URL https://moluch.ru/conf/econ/archive/261/12799

15. План мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации». Утвержден Правительственной комиссией по использованию информационных технологий улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18 декабря 2017 г. № 2) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_287575/

References

1. Rasporyazhenie Pravitel'stva ot 28 iyulya 2017 goda №1632-r. Ob utverzhdenii programmy «Tsifrovaya ekonomika Rossiiskoi Federatsii» [Elektronnyi resurs]. URL: http://m.government.ru/all/28653/

2. Berkana A. Zachem Rossii tsifrovaya ekonomika//Rusbase [Elektronnyi resurs].URL: https://rb.ru/longread/digital-economy-in-russia/

3. Materialy konferentsii Rossiiskii Internet Forum RIF+KIB 2017 [Elektronnyi resurs].URL: http://2017.russianinternetforum.ru/itogi/

4. Shmyrova V. «Tsifrovaya ekonomika» oboidetsya v 520 milliardov//Izdanie o vysokikh tekhnologiyakh C-news [Elektronnyi resurs].URL: http://www.cnews.ru/news/top/2017-12-18_zapusk_tsifrovoj_ekonomiki_obojdetsya_v_520_milliardov

5. Vvedenie v «Tsifrovuyu» ekonomiku / A.V. Keshelava V.G. Budanov, V.Yu. Rumyantsev i dr.; pod obshch. red. A.V. Keshelava; gl. «tsifr.» kons. I.A. Zimnenko. VNIIGeosistem, 2017. 28 p.
6. Sudarushkina I.V., Stefanov N.A. Tsifrovaya ekonomika // Azimut nauchnykh issledovanii: ekonomika i upravlenie. 2017. T.6. №1. pp. 182-184.
7. Babkin A.V., Burkal'tseva D.D., Kosten' D.G., Vorob'ev E.N. Formirovanie tsifrovoi ekonomiki v Rossii: sushchnost', osobennosti, tekhnicheskaya normalizatsiya, problemy razvitiya // Nauchno-tekhnicheskie vedomosti SPbGPU. Ekonomicheskie nauki.2017. T.10, №3. pp. 9-25.
8. Tsifrovaya ekonomika 2016 / Itogovaya broshyura issledovaniya Ekonomika Runeta 2015–2016 [Elektronnyi resurs].URL: http://raec.ru/live/analytics/9863/
9. Atkina V.S. Razrabotka metodov, algoritmov i programmy dlya analiza katastrofoustoichivosti informatsionnykh sistem// dissertatsiya na soiskanie uchenoi stepeni kandidata tekhnicheskikh nauk / Yuzhnyi federal'nyi universitet. Volgograd, 2013.
10. Vittenburg E.A., Olad'ko V.S., Pushkarskaya A.I. Model' otsenki bezopasnosti na osnove dannykh monitoringa informatsionnoi sistemy // Informatsionnye sistemy i tekhnologii. 2017. № 4 (102). pp. 87-93.
11. GOST R ISO/MEK 27002-2012 Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil menedzhmenta informatsionnoi bezopasnosti// Sistema GARANT. URL: http://base.garant.ru/70795320/#ixzz4MOF779bo
12. Volkov A.N. Kiberbezopasnost' v tsifrovom mire//Materialy konferentsii Informatsionnaya bezopasnost' v tsifrovom mire 29 noyabrya 2017, Finuniversitet g. Moskva.
13. Oladko V.S. The model of information security audit in the information system of e-commerce type of B2E // Sochi Journal of Economy. 2016. № 2 (40). pp. 117-126.
14. Borzunov A. A. Razvitie chelovecheskikh resursov kak klyuchevoi faktor obespecheniya ekonomicheskoi bezopasnosti kompanii v usloviyakh tsifrovoi ekonomiki [Tekst] // Problemy sovremennoi ekonomiki: materialy VI Mezhdunar. nauch. konf. (g. Samara, avgust 2017 g.). Samara: OOO "Izdatel'stvo ASGARD", 2017. pp. 94-97. URL https://moluch.ru/conf /econ/archive/261/12799
15. Plan meropriyatii po napravleniyu «Informatsionnaya bezopasnost'» programmy «Tsifrovaya ekonomika Rossiiskoi Federatsii». Utverzhden Pravitel'stvennoi komissiei po ispol'zovaniyu informatsionnykh tekhnologii uluchsheniya kachestva zhizni i uslovii vedeniya predprinimatel'skoi deyatel'nosti (protokol ot 18 dekabrya 2017 g. № 2) [Elektronnyi resurs]. URL: http://www.consultant.ru/document/cons_doc_LAW_287575/

УДК 33 + 004.056

Проблемы кибербезопасности в условиях внедрения цифровой экономики

Владлена Сергеевна Оладько [a, *]

[a] Финансовый университет при Правительстве Российской Федерации,
Российская Федерация

Аннотация. В статье рассматривается такая отрасль развития экономической системы как цифровая экономика. Цифровая экономика является будущей ступенью развития глобальной экономической системы за счет трансформации всех сфер человеческой деятельности под влиянием информационных и телекоммуникационных технологий. Описываются составляющие цифровую экономику хабы. Проводится анализ объектов и субъектов информационной инфраструктуры цифровой экономики, делается вывод о существовании проблем кибербезопасности. Исследуется статистика событий кибербезопасности и проводится их классификация на три группы – нормальные события, аномальные события и опасные события. На основе информационной инфраструктуры и данных о событиях приводиться список потенциальных инцидентов кибербезопасности и их последствий для субъектов и объектов цифровой экономики. Раскрываются факторы риска кибербезопасности и стратегии по управлению ими. Формулируется вывод о необходимости

* Корреспондирующий автор
Адреса электронной почты: oladko.vs@yandex.ru (В.С. Оладько)

обеспечения безопасности информационной инфраструктуры на стороне субъектов-потребителей, субъектов-производителей, ядра объектов и удаленных сервисов, сети и каналов связи, хранилищ данных. В заключении автором предлагается схема реализации механизмов защиты от угроз кибербезопасности на двух уровнях: организационно-административном и техническом.

Ключевые слова: цифровое производство, информационная инфраструктура, риск, ущерб, ВВП, электронная коммерция, интернет-рынок.