УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СКВОЗЬ ПРИЗМУ ЦИФРОВОЙ ЭКОНОМИКИ

[1]Хочуева Ф.А., [1]Шугунов Т.Л., [2]Жуков А.З., [1]Ингушев Ч.Х.

[1]ФГБОУ ВО «Кабардино-Балкарский государственный университет им. Х.М. Бербекова», Нальчик, e-mail: fah11061987@mail.ru;

[2]Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России, Нальчик

В статье рассмотрены проблемы обеспечения защиты информации в условиях цифровой экономики. Цифровая экономика оказывает положительное влияние на все сферы жизни общества, но данные процессы сопровождаются и негативными последствиями, которые связаны с угрозами потери конфиденциальной информации. Потеря экономической информации в условиях функционирования цифровой экономики становится все более реальной ситуацией. Особенно в условиях активной информатизации экономики наибольшие потери наблюдаются в банковском секторе, за последние три года количество экономических преступлений именно в банковском секторе возросло. В статье представлен анализ современного состояния цифровой экономики и выявлены проблемы с обеспечением информационной безопасности в данной сфере. Так же проведен анализ количества утечек информации за 10 лет и сравнительный анализ причин нарушения информационной безопасности по итогам 2016–2017 гг. Необходимо создание эффективной системы информационной безопасности, это возможно при использовании и разработке дополнительных информационных ресурсов, обеспечивающих безопасность данных. Одним из условий выступает и формирование кадрового потенциала в сфере информационной безопасности, что будет включать реализацию программ повышения квалификации в сфере информационной безопасности. Переход к цифровой модели экономики – это объективное требование в современных условиях развития общества, но одним из ключевых вопросов при реализации данного перехода является обеспечение высокого уровня информационной безопасности.

Ключевые слова: информационная безопасность, цифровая экономика, конфиденциальная информация, блокчейн, информационные системы, киберустойчивость

INFORMATION SECURITY THROUGH THE PRISM OF THE DIGITAL ECONOMY

[1]Khochueva F.A., [1]Shugunov T.L., [2]Zhukov A.Z., [1]Ingushev Ch.Kh.

[1]The Federal State Budget Educational Institution of Higher Education «Kabardino-Balkaria State University Kh.M. Berbekov», Nalchik, e-mail: fah11061987@mail.ru;

[2]North-Caucasian Institute for enhancing qualifications (branch)University of the Ministry of Internal Affairs of Russia, Nalchik

The article considers the problems of ensuring information security in the area of the emerging digital economy in the Russian Federation. The digital economy has a positive impact on all spheres of society, but these processes are accompanied by negative consequences, which are associated with threats of loss of confidential information. The loss of economic information in the conditions of the functioning of the digital economy is becoming an increasingly real situation. Especially in conditions of active informatization of the economy, the largest losses are observed in the banking sector, over the past three years the number of economic crimes in the banking sector has increased. The article presents an analysis of the current state of the digital economy and identifies problems with ensuring information security in the economic sphere. Also, an analysis of the number of data leaks for 10 years and a comparative analysis of the reasons for the violation of information security in 2016-2017. It is necessary to create an effective information security system, this is possible with the use and development of additional information resources that ensure the security of information. One of the conditions is the formation of personnel potential in the field of information security, which will include the implementation of programs to improve skills in the field of information security. The transition to a digital economy model is an objective requirement in the current conditions of the development of society, but one of the key issues in implementing this transition is to ensure a high level of information security.

Keywords: information security, digital economy, confidential information, blocking, information systems, cyber-resistance

Старый уклад экономической сферы общества на данном этапе активно вытесняется таким новым направлением, как цифровая экономика. Цифровая экономика охватывает все сферы общества и активно вовлекает как физических, так и юридических лиц. Происходящие изменения в сфере экономики способствуют трансформации и других сфер жизни общества. Появляются новые профессии и рабочие места, которые требуют приобретения соответствующих знаний и навыков.

Построение модели цифровой экономики в Российской Федерации имеет ряд трудностей, которые связаны с тем, что сама экономическая система не является рыночной, а переход к цифровой экономике реализовали в основном в странах с рыночным типом экономики.

Одной из ключевых проблем в процессе формирования цифровой экономики является обеспечение информационной безопасности. Экономика выступает одной из сфер, где информация является важным ресурсом. Цифровая модель экономики повышает степень уязвимости информации.

Цель исследования: анализ эффективности функционирования системы информационной безопасности в условиях цифровой экономики на территории Российской Федерации.

Материалы и методы исследования

В рамках данного исследования применялись теоретические методы: аналитический обзор теоретических источников, анализ статистической информации, обобщение и представление результатов исследования в графическом виде.

Одна из проблем связана непосредственно с процессом цифровизации экономики, в первую очередь это отсутствие законодательной базы, что приводит к возникновению спорных моментов.

Существующие нормативно-правовые акты не в полной мере соответствуют реальной ситуации и остро встает вопрос защиты экономической информации, а, как известно, именно потеря экономической информации может нанести существенный вред государственной безопасности. Использование информационных технологий происходит благодаря развитию цифровой экономики, что качественно и количественно увеличивает возможности реализации всех операций посредством использования компьютера.

Следует отметить, что кроме положительных моментов подобная цифровая трансформация сопровождается и определенными рисками.

Связано это с тем, что часть информации, которая принадлежит потребителям данных информационных услуг, как физическим, так и юридическим лицам носит конфиденциальный характер, подвержена таким угрозам, как ее потеря или доступ к ней иных физических и юридических лиц [1].

В данных условиях глобальные масштабы обретает вопрос защиты персональных данных. Личная информация становится одним из ценнейших активов. Наблюдается рост случаев утечки информации. В первом полугодии 2017 г. аналитический центр InfoWatch зарегистрировал 925 случаев утечек конфиденциальной информации – на 10% больше, чем за аналогичный период 2016 г. (рис. 1).

В целях решения проблемы утечки информации необходимо выявить факторы, которые способствуют потере информации. Внешние атаки обусловили 10 из 20 зафиксированных «мегаутечек» (свыше 10 млн ПДн на каждую), на которые пришлись 7,68 млрд скомпрометированных записей (98% общего числа). В 43 случаях объем скомпрометированных данных превысил 1 млн записей. В 53% случаев виновными в утечках оказались сотрудники компаний, в 2% случаев высшие руководители и иные привилегированные пользователи (рис. 2, 3).

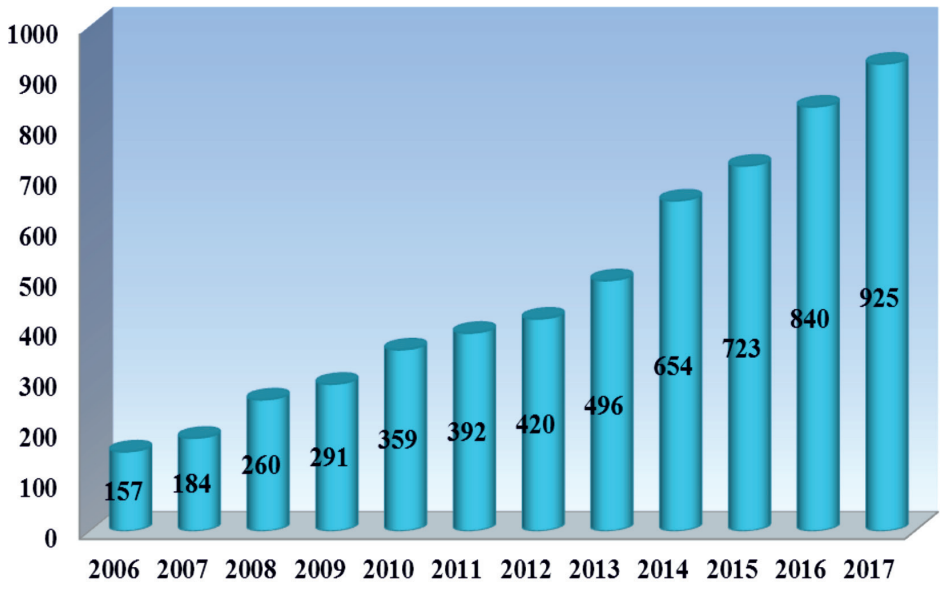

Рис. 1. Число утечек информации в первых полугодиях 2006–2017 гг.

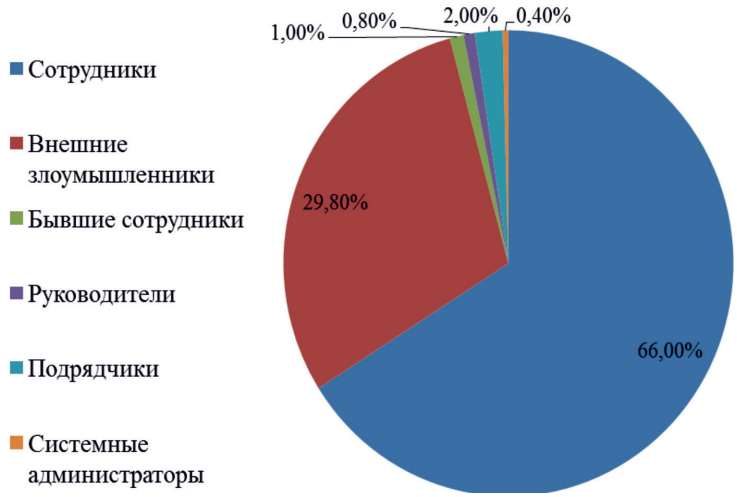

Рис. 2. Причины утечек информации в 2016 г.

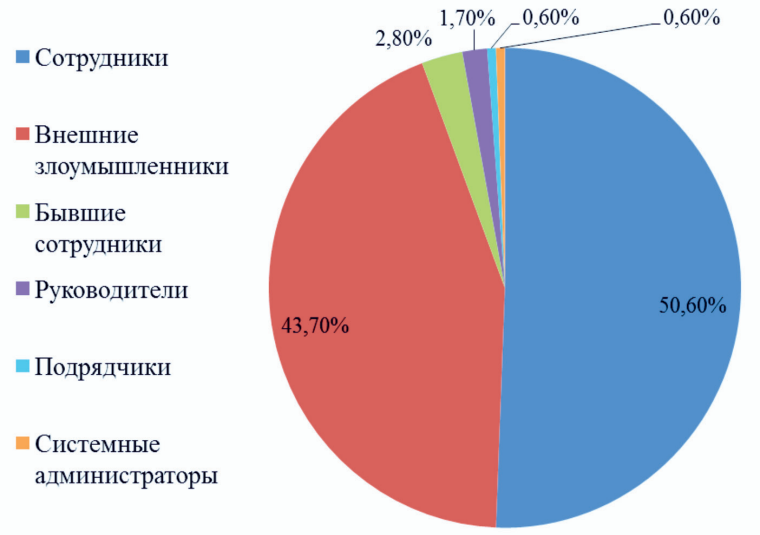

Рис. 3. Причины утечек информации в 2017 г.

Известно, что недостоверность или замена некоторой информации может нанести серьезный материальный и моральный вред. В данных условиях крайне актуален вопрос обеспечения информационной безопасности государственных структур, персональных данных и информации, принадлежащей коммерческим структурам.

Прежде всего, информационная безопасность в России является зрелой и вполне успешной отраслью экономики, понимающей не только свои задачи, но и методы их решения.

Многие экономисты, аналитики и специалисты в сфере информационных технологий утверждают, что Российская Федерация должна стать в данной ситуации лидером в сфере развития цифровой экономики. Модель цифровой экономики, на основе которой строится цифровая экономика в большинстве стран, является преимущественно американской. В Российской Федерации разрабатывается и предлагается свой вариант цифровой экономики [2].

Следует отметить, что на сегодняшний день Российская Федерация является мировым лидером по объему торгов, совершенных в формате B2B и B2G. По данным статистики за 2016 г. в денежном эквиваленте он составил более 650 млрд долларов США. Это приблизительно 1,2 млн поставщиков и заказчиков. Почти все сделки осуществляются в электронном виде. Наряду с этим Россия поступательно наращивает

обороты трансграничной электронной торговли, особенно после подключения к данному процессу Белоруссии и Казахстана. В частности, в рамках Таможенного союза в прошлом году объем торгов, совершенных в электронной форме в денежном эквиваленте достиг 900 млрд долл. США. В ближайшей перспективе будет преодолена планка в один триллион долларов США [3].

Следует сказать, что многие ведущие эксперты сходятся во мнении, что именно электронная торговля может стать главным драйвером для развития цифровой экономики. Более того, данная позиция отмечена в опубликованной в феврале 2017 г. программе развития экономики под названием «Стратегия Роста», которая была разработана Столыпинским клубом.

Одной из ключевых проблем в системе обеспечения информационной безопасности в условиях цифровой экономики является и низкий уровень культуры информационной безопасности. Работники не всегда осознают риски потери экономической информации, кроме того следует отметить, что наибольший процент утечки приходится именно на внутренних сотрудников, именно внутренние сотрудники в большинстве случаев причастны к потере информации.

В целях формирования культуры информационной безопасности в современных компаниях нужно регулярно проводить тренинги и семинары по повышению осведомленности работников, а корпоративные службы информационной безопасности (ИБ) должны быть максимально открыты для взаимодействия с коллегами из других подразделений при возникновении вопросов и проблемных ситуаций.

Информационная безопасность «становится сегодня важнейшим фактором развития цифровой экономики, расширения электронного взаимодействия участников рынка, внедрение элементов блокчейна, масштабное использование новых технологий выводит на первый план вопросы повышения конкурентоспособности отечественной финансовой системы, обеспечение ее безопасности как объекта критической информационной инфраструктуры» [4].

Защищенность информационных систем имеет для страны стратегическое значение. Вместе с тем ситуация явно обостряется ростом уровня угроз в информационном пространстве, при этом методы, способы и средства таких преступлений закономерно становятся все изощрённее, что требует адекватных мер по повышению киберустойчивости субъектов финансового рынка [5].

В качестве одного из инструментов защиты экономической информации выступает криптография.

Технологии криптографии позволяют реализовать следующие процессы информационной защиты:

- идентификацию объекта или субъекта сети или информационной системы;
- аутентификацию объекта или субъекта сети;
- контроль/разграничение доступа к ресурсам локальной сети или внесетевым сервисам;
- обеспечение и контроль целостности данных.

Общая схема простой криптосистемы показана на рис. 4.

Переход на российское шифровальное программное обеспечение является одним из ключевых инструментов защиты информации в современном экономическом пространстве России.

Межведомственная комиссия Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации разработала проект государственной программы «Цифровая экономика», в рамках которой предусмотрен переход на отечественное шифровальное программное обеспечение.

Осуществить полный переход участников процесса обмена цифровой информацией в рамках системы «Цифровая экономика» на российские системы шифрования данных разработчики планируют к 2021 г. В рамках данного проекта необходимо встроить российские программы шифрования в программное обеспечение.

В мире на данный момент функционируют две школы шифрования: Россия и США. Китай также начал активно заниматься данным вопросом.

Российские алгоритмы очень надежны. Российские алгоритмы одобрены специальным комитетом Международной организации по стандартизации (ISO). Со стороны крупнейших мировых IT-корпораций наблюдается настороженность и отказ от их использования, несмотря на признание их Международной организацией по стандартизации.

На данный момент шифрование данных осуществляется по американским сертификатам безопасности, в этой ситуации российские пользователи оказываются под угрозой рассекречивания своих данных, которые хранятся на различных сайтах в случае отзыва этих сертификатов их владельцами.

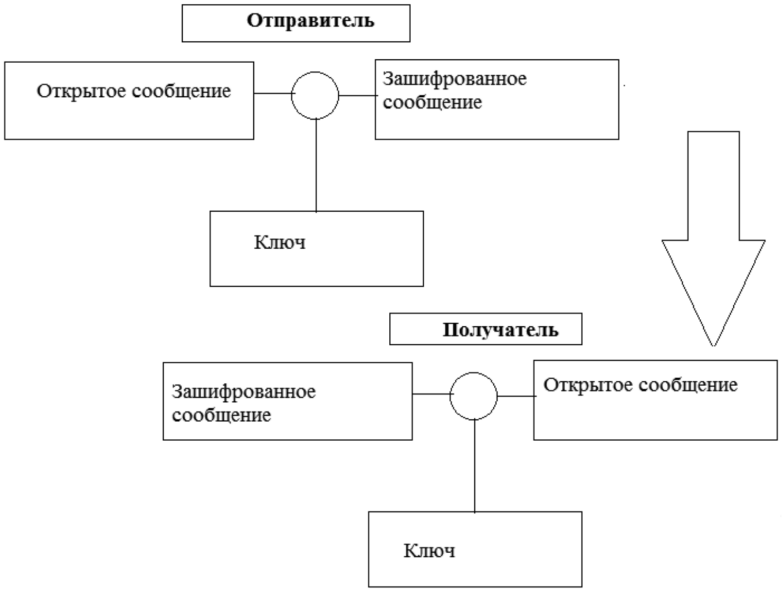

Рис. 4. Общая схема простой криптосистемы

В свете существующей ситуации в сфере информационной безопасности отмечается также еще один факт, представляющий опасность для российских пользователей сети и указанный в проекте программы. Свыше 60% информации, передающейся как бы внутри российского информационного пространства, проходит, тем не менее, через серверы других государств, что повышает возможность доступности ее для чтения сторонними лицами [6].

Для поддержания режима информационной безопасности особенно важны программно-технические меры и средства, поскольку основная угроза компьютерным системам находится в них: сбои оборудования, ошибки программного обеспечения, промахи пользователей и администраторов и т.п.

Необходимо формирование правового фундамента для обеспечения информационной безопасности в кредитно-финансовой сфере», первым делом сославшись на программу «Цифровая экономика Российской Федерации», утвержденную распоряжением правительства России 28 июля 2017 г., одним из направлений которой определена необходимость нейтрализация рисков, связанных с киберустойчивостью финансовых организаций. Важным документом является положение Доктрины информационной безопасности России, принятой указом президента в декабре 2016 г.

Значимым событием для отрасли в 2017 г. стало вступление в силу закона «О безопасности критической информационной инфраструктуры РФ».

Показатели критериев значимости для них будут установлены постановлением правительства. Предполагается, что в их основу ляжет среднедневное количество операций, осуществляемых субъектом отечественной информационной инфраструктуры. В соответствии с данным показателем к значимым объектам критической информационной инфраструктуры третьей категории в кредитно-финансовой сфере могут быть отнесены информационные и автоматизированные системы Банка России, Сбербанка, Национальной системы платежных карт, других значимых кредитных и финансовых организаций. Важной функцией регулятора становится содействие в предоставлении данных в государственную систему обнаружения, предупреждение и ликвидация последствий компьютерных атак на информационные ресурсы России [7].

Банком России создан специализированный Департамент информационной безопасности. На 2018 г. основная задача центра компетенций регулятора по обеспечению киберустойчивости организаций кредитно-финансовой сферы – это активизация информационного обмена о прецедентах с финансовыми организациями.

Кроме того, новый департамент будет определять потребности рынка в совершенствовании системы киберустойчивости, заниматься нормативным регулированием, предполагается, что спектр его функций будет достаточно широк. Информационный обмен с субъектами финансового рынка будет организован по определенной техноло-

гии в установленном формате электронных сообщений.

По заключению аналитиков, почти 99% всех киберпреступлений в мире связаны с воровством денег. Наибольшую опасность для банков сейчас представляют целевые атаки, ущерб от которых в прошлом году вырос почти на 300%. Одна из атак стоила российскому банку 140 млн руб., а общая сумма хищений выросла, по оценкам экспертов, до 2,5 млрд руб. [8].

Всего за 2017 г. было зарегистрировано не менее 21 атак «Кобальт Страйк». Атакам подверглись более 240 кредитных организаций, из них успешных атак было 11, сумма ущерба превысила 1 млрд. руб. При этом 8 из 11 пострадавших организаций не являлись участниками информационного обмена с ФинЦЕРТом, на базе которого и образуют новый департамент [9].

Проблемы безопасности и цифровизации тесно взаимосвязаны, на это следует обращать внимание.

Следует принимать во внимание и взаимосвязь цифровизации и проблем безопасности. С одной стороны, использование цифровых технологий создает благоприятные информационные возможности повышения безопасности на разных уровнях.

Бездумное вхождение в мировую цифровую экономику, включение в мировые цифровые цепочки создаст особые возможности для стран, более продвинувшихся в цифровом направлении, и сделает объектом манипулирования менее развитые страны, включая Россию. Особенно остро стоит проблема кибербезопасности [10].

Россия обязана сохранить суверенность экономики, общественно-политической жизни и национального развития, тем более исходя из существующих ныне геополитических сложностей. Имеется и внешнеэкономическая опасность, связанная с выросшими возможностями вывоза капитала за рубеж.

18 декабря 2017 г. Правительственная комиссия по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности утвердила две программы «Цифровая экономика Российской Федерации» на 2018–2024 гг.

План предусматривает финансирование из федерального бюджета в размере 22 333 млн руб. и внебюджетное финансирование – 11 710 млн руб.

Результаты исследования и их обсуждение

Количество утечек информации возрастает с каждым годом, особенно в условиях формирования цифровой экономики, так с 2006 по 2017 г. количество утечек конфиденциальной информации возросло в 8 раз. Основной причиной потери конфиденциальной информации по-прежнему остаются внутренние факторы, так основной процент приходится на сотрудников, более половины утечек происходит именно по вине сотрудников, но следует отметить снижение данного показателя в 2017 г. по сравнению с 2016 г.

По итогам реализации плана должны быть достигнуты целевые значения информационной безопасности на сетях связи и в российском сегменте интернета. Должна быть создана система стимулов для приобретения и использования компьютерного, серверного и телекоммуникационного оборудования российского производства. Созданы механизмы стимулирования использования отечественного программного обеспечения всеми участниками информационного взаимодействия.

Помимо этого, должны быть приняты национальные стандарты киберфизических систем. Необходимо обеспечить контроль обработки и доступа к персональным данным, большим пользовательским данным, в том числе в социальных сетях и прочих средствах социальной коммуникации. Создание национального и региональных центров реагирования на компьютерные инциденты обеспечит также высокий уровень информационной безопасности.

Также ожидается, что по итогам выполнения программы будет разработана система мер поддержки российских производителей продуктов и услуг информационно-компьютерных технологий, осуществляющих патентование продуктов за рубежом.

Утвержденный план содержит перечень целевых показателей и индикаторов.

С 10% в 2018 до 90% в 2024 г. должна увеличиться доля субъектов информационного взаимодействия, использующих стандарты безопасности в киберфизических системах и в части интернета вещей.

Доля граждан, повысивших грамотность в сфере информационной безопасности, медиапотребления и использования интернет-сервисов, к 2024 г. должна составить 50%.

Выводы

Резюмируя, отметим, что «картина получается в результате довольно безрадостная», имея в виду ситуацию в банковском секторе, который сталкивается сейчас с давлением со стороны финансовых технологий, вынуждающих к новым инструментам, с другой стороны, операторы связи

«поджимают», не столько сами операторы, сколько глобальные корпорации, которые «высасывают» большие данные и на их основе пытаются «монетизировать наших же пользователей».

В российской экономике цифровая трансформация будет оказывать возрастающее влияние на разные отрасли. ВВП до 2025 г. согласно всем расчетам должен увеличиться от 0,4 % до 0,9 % в связи с внедрением цифровой экономики. Сравнение этого роста с темпами роста прогнозов российской экономики позволяет сделать вывод, что цифровизация приведёт к росту ВВП с 2015–2025 гг. от 19 % до 34 %.

В наше время это самая актуальная тема для развития любой страны. Цифровая экономика может приводить к возникновению «умных» городов, транспорта и сельского хозяйства, отсутствию цифрового неравенства отдельных регионов, повышению цифровой грамотности у населения. Так же человечество может столкнуться и с отрицательными сторонами данной сферы: нарушение безопасности конфиденциальности личных данных населения, засорение информационного пространства, дефицит высокообразованных кадров и, наоборот, появление большого количества безработных людей, которые появились в результате внедрения цифровой экономики. В данном случае преимуществ будет больше, чем недостатков, поэтому необходимо развивать данную сторону экономики и внедрять её во всех регионах.

Список литературы

1. Введение в «Цифровую» экономику / под общ. ред. А.В. Кешелава; гл. «цифр.» конс. И.А. Зимненко. М.: ВНИИГеосистем, 2017. 28 с.

2. Аверьянов М.А., Евтушенко С.Н., Кочеткова Е.Ю. Цифровое общество: Новые вызовы // Экономические стратегии. 2016. № 7 (141). С. 90–91.

3. Экономика [Электронный ресурс]. URL: https://data-economy.ru/security (дата обращения: 15.09.2018).

4. Андреева Г.Н., Бадальянц С.В., Богатырева Т.Г., Бородай В.А., Дудкина О.В., Зубарев А.Е., Казьмина Л.Н., Минасян Л.А., Миронов Л.В., Стрижов С.А., Шер М.Л. Развитие цифровой экономики в России как ключевой фактор экономического роста и повышения качества жизни населения: монография. Нижний Новгород: Изд-во «Профессиональная наука», 2018. 131 с.

5. Об утверждении программы «Цифровая экономика Российской Федерации: Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р. [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_221756/ (дата обращения: 16.09.2018).

6. Дошина А.Д., Михайлова А.Е., Карлова В.В. Криптография. Основные методы и проблемы. Современные тенденции криптографии // Современные тенденции технических наук: материалы IV Междунар. науч. конф. (г. Казань, октябрь 2015 г.). Казань: Бук, 2015. С. 10–13.

7. Тарчоков Б.А. Анализ преступных деяний, совершенных в банковской сфере с использованием интернет технологий // Пробелы в российском законодательстве. 2017. № 5. С. 211–212.

8. Программа развития цифровой экономики в Российской Федерации до 2035 года [Электронный ресурс]. URL: http://spkurdyumov.ru/uploads/2017/05/strategy.pdf (дата обращения: 15.09.2018).

9. Кузнецов И.Н. Бизнес-безопасность. М.: Издательско-торговая корпорация «Дашков и К°», 2016. 416 с.

10. Удалов Д.В. Угрозы и вызовы цифровой экономики // Экономическая безопасность и качество. 2018. № 1. С. 12–18.