ГОСУДАРСТВО, ГРАЖДАНСКОЕ ОБЩЕСТВО И СТАБИЛЬНОСТЬ

STATE, CIVIL SOCIETY AND STABILITY

УДК 338.2

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

А.А. Кайгородцев

https://orcid.org/0000-0002-7410-7383

Восточно-Казахстанский государственный университет им. С. Аманжолова, Усть-Каменогорск, Казахстан, e-mail: kay-alex@mail.ru

Т.Ф. Кайгородцева

Ярославский колледж индустрии питания, Ярославль, Россия, e-mail: tanya19651@mail.ru

DOI:10.14258/ssi(2020)3-06

Рассматриваются вопросы обеспечения информационной безопасности экономических систем в условиях цифровой экономики. Переход к цифровой экономике, сопряженный с новым витком развития информационных систем и базирующихся на них технологических решений, является причиной возникновения новых вызовов в сфере обеспечения информационной безопасности. Цель статьи — исследование проблемы обеспечения информацион-

ной безопасности России в условиях перехода страны к цифровой экономике. Дана характеристика вызовов и угроз, препятствующих развитию цифровой экономики. Определены основные направления обеспечения информационной безопасности. Одним из инструментов защиты информации является криптография, технологии которой дают возможность идентифицировать и аутентифицировать объекты и субъектов информационных систем, а также ограничивать несанкционированный доступ к информационным ресурсам. Дано обоснование использования технологий Блокчейн в качестве инструмента обеспечения информационной безопасности хозяйствующих субъектов и национальной экономики в целом. На основе технологий Блокчейн можно создать систему программно-информационных и аналитических средств, позволяющих с высокой степенью адаптивности, надежности и окупаемости решать различные задачи, предусмотренные Стратегией национальной безопасности Российской Федерации. Однако для расширения применения этих технологий требуется устранение присущих им недостатков и создание правовой основы для их использования.

Ключевые слова: *цифровая экономика, информационная безопасность, высокие технологии, угрозы безопасности, обеспечение безопасности*

PROBLEMS OF ENSURING INFORMATION SECURITY IN RUSSIA IN THE CONDITIONS OF DIGITALIZATION

A.A. Kaigorodtsev

https://orcid.org/0000-0002-7410-7383

S. Amanzholov East Kazakhstan state University, Ust-Kamenogorsk, Kazakhstan, e-mail: kay-alex@mail.ru

T.F. Kaigorodtseva

Yaroslavl College of food industry, Yaroslavl, Russia, e-mail: tanya19651@mail.ru

The article deals with the issues of ensuring information security of economic systems in the digital economy. The transition to the digital economy, coupled with a new round of development of information systems and technological solutions based on them, is the cause of new challenges in the field of information security. The purpose of the article is to study the problem of ensuring information security in Russia in the context of the country's transition to a digital economy. The article describes the challenges and threats that hinder the development of the digital economy. The directions of ensuring information security in the digital economy are defined. One of the tools for information protection is cryptography, which technologies allow you to: identify and authenticate objects and subjects of information networks; control / differentiate access to local network resources and off-network

services; ensure data integrity. The use of Blockchain technologies is a promising direction for ensuring information security of economic entities and the national economy as a whole. Based on Blockchain technologies, it is possible to create a system of software, information and analytical tools that allow for a high degree of adaptability, reliability and payback to solve various tasks provided for by the national security Strategy of the Russian Federation. However, expanding the use of these technologies requires addressing their inherent shortcomings and creating a legal framework for their use.

Keywords: *digital economy, information security, high technology, security threats, security maintenance*

Введение

В настоящее время в развитых странах мира происходит трансформация парадигмы обеспечения конкурентоспособности хозяйствующих субъектов, осуществляется переход к развитию инновационного процесса на основе глобальных сетей научно-исследовательских и опытно-конструкторских работ, формирование инновационной инфраструктуры сетевого типа, включающей виртуальные сетевые информационные альянсы, стратегические технологические платформы, инновационные кластеры и т.п. Для промышленной революции XXI в. характерны конвергенция технологий, стирание границ между физическими, биологическими и цифровыми сферами, возникновение аддитивного производства, развитие систем облачных вычислений и кибернетической безопасности (Филин & Якушев, 2018).

Это свидетельствует о переходе к цифровой экономике, которая, с одной стороны, способствует повышению эффективности общественного производства, уровня и качества жизни населения, но, с другой стороны, сопряжена с новыми вызовами и угрозами в информационной сфере. Государства, преступные сообщества, террористические и экстремистские организации, юридические и физические лица все чаще используют возможности трансграничного оборота информации и современных информационных технологий для достижения своих геополитических, военных, террористических, экстремистских, криминальных и иных противоправных целей, нанося тем самым ущерб интересам государств, организаций и населения в информационной сфере.

В связи с этим необходимо постоянно совершенствовать деятельность по обеспечению *национальной информационной безопасности*, под ней следует понимать состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие страны, оборона и безопасность государства[1].

[1] Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г., № 646. URL: https://www.garant.ru/products/ipo/prime/doc/71456224/

В Доктрине информационной безопасности РФ приведен перечень угроз информационной безопасности страны в различных сферах жизни и деятельности:

1. Внешние угрозы:
- применение странами Запада информационных технологий для ослабления национального суверенитета России, нарушения ее экономической и социально-политической стабильности и территориальной целостности;
- компьютерные атаки зарубежных спецслужб и террористических организаций на объекты критической информационной инфраструктуры;
- использование развитыми странами технологического превосходства для доминирования в информационном пространстве;
- усиление международной конкуренции в сфере информационных технологий и ресурсов;
- компьютерные преступления, в том числе транснациональные, в кредитно-финансовой сфере;
- возможность отключения в условиях применения странами Запада антироссийских экономических санкций финансовых институтов РФ от международных платежных систем и зарубежных автоматизированных информационных систем оформления воздушных перевозок.

2. Внутренние угрозы:
- зависимость экономики РФ от импорта электронных компонентов информационных технологий;
- недостаточно высокий уровень внедрения в производство отечественных результатов научных исследований в области информационных технологий;
- разглашение персональных данных граждан в процессе их обработки с использованием информационных технологий и др.

По мере развития цифровой экономики существенно возрастает вероятность реализации перечисленных угроз. Это свидетельствует об актуальности темы настоящей статьи, *целью* которой является исследование проблемы обеспечения информационной безопасности России в условиях перехода страны к цифровой экономике.

Теоретической и методологической основой исследования послужили государственные программные документы и работы российских ученых по проблемам формирования цифровой экономики и обеспечения национальной информационной безопасности. В процессе исследования применялись методы экономической логики, анализа и синтеза, индукции и дедукции, абстрактно-логический и монографический методы изучения социально-экономических явлений и процессов.

Результаты исследования

Цифровая экономика — это экономическая система, в которой ключевым фактором производства являются оцифрованные данные, обработка больших объемов и использование результатов анализа которых позволяют существенно повысить эффективность общественного производства.

В условиях цифровой экономики ключевым фактором производства во всех сферах социально-экономической деятельности являются данные в цифровой форме.

Программа перехода РФ к цифровой экономике предусматривает широкое использование: больших данных; нейротехнологий и искусственного интеллекта; системы распределенного реестра; квантовых технологий; новых производственных технологий; промышленного интернета; робототехники и сенсорики; беспроводной связи; технологий виртуальной и дополненной реальностей[1].

В случае успешной реализации программы перехода России к цифровой экономике возможен существенный рост эффективности общественного производства:

- повышение производительности труда на 40–45%;
- сокращение времени простоя оборудования на 30–50%;
- уменьшение складских расходов на 20–50%;
- сокращение сроков вывода новых товаров на рынок на 20–50%;
- повышение точности прогнозирования объемов продаж до 85% и более.

Вместе с тем массовое внедрение высоких технологий в течение ближайших пяти лет может привести к сокращению 7 млн рабочих мест, которые будут замещены 2 млн вакансий в новых сферах экономической деятельности (Бабкин и др., 2017).

По удельному весу цифровой экономики в ВВП, равному 3,9%, Россия значительно уступает США (10,9%), КНР (10,0%) и странам ЕС (8,2%) (Капранова, 2018).

В России развитию цифровой экономики препятствуют следующие вызовы и угрозы:

- возможность нарушения прав человека в информационной сфере, в том числе при идентификации[2] и обеспечении сохранности цифровых данных пользователя;
- угрозы личности, хозяйствующим субъектам и государству, связанные с тенденциями к построению сложных иерархических информационно-телекоммуникационных систем, широко использующих виртуализацию, облачные хранилища данных, а также разнородные технологии связи;
- наращивание возможностей внешнего информационно-технического воздействия на информационную инфраструктуру, в том числе на критическую информационную инфраструктуру;
- значительное увеличение масштабов киберпреступности;
- отставание от ведущих зарубежных стран в развитии информационных технологий;
- зависимость уровня развития экономики и социальной сферы от экспортной политики зарубежных стран;
- неэффективность научных исследований, связанных с разработкой перспективных информационных технологий, низкий уровень внедрения в производство

[1] Программа «Цифровая экономика Российской Федерации». Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 года № 1632-р. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

[2] Идентификация установление тождественности неизвестного объекта известному на основании совпадения признаков; соотнесение человека с его цифровым образом, опознание.

разработок российских ученых, нехватка квалифицированных специалистов в сфере обеспечения информационной безопасности[1].

Цифровизация экономики сопряжена с ростом угроз безопасности личности, общества и государства в информационной сфере, так как использование современных компьютерных технологий делает возможным:

- ограничение прав граждан на тайну переписки и телефонных переговоров;
- сбор информации о пользователях сети Интернет для использования ее как в коммерческих, так и в политических (например, манипулирование общественным мнением для того, чтобы вызвать массовые беспорядки, «цветные революции») целях;
- промышленный шпионаж. Так, в 1994 г. благодаря информации, полученной системой глобального контроля телекоммуникаций «Эшелон», управление которой осуществляет Агентство национальной безопасности США, был сорван контракт на покупку Саудовской Аравией французских самолетов, в результате чего выгодоприобретателем стала американская компания (Лопатин, 2008: 56–57);
- существенный рост киберпреступности. За 3 года, предшествующих принятию программы цифровизации российской экономики, количество преступлений в цифровой среде возросло на 75%2. В 2018 г. В России было выявлено 4,3 млрд компьютерных воздействий на критически важную инфраструктуру, что на 79% превышает уровень предыдущего года (2,4 млрд). При этом затраты предприятий среднего бизнеса, связанные с ликвидацией отрицательных последствий одного инцидента, составили около 1,6 млн руб., а на предприятиях крупного бизнеса — 16,1 млн руб. (Махалина & Махалин, 2020: 134);
- отключение российских банков от глобальной системы электронных платежей SWIFT, приводящее к затруднениям при осуществлении экспортно-импортных операций (Лесных, 2015).

Несмотря на то что информационная безопасность является существенным фактором обеспечения конкурентоспособности хозяйствующих субъектов, результаты обследования в 2017 г. 248 российских компаний свидетельствуют о том, что 40% из них не имеют стратегии обеспечения информационной безопасности, в 50% организаций отсутствуют планы реагирования на угрозы информационной безопасности, у 48% предприятий отсутствуют программы обучения сотрудников, направленные на повышение уровня информационной безопасности бизнеса (Удалов, 2018).

Одним из перспективных способов защиты информации является криптография, технологии которой позволяют:

- проводить идентификацию и аутентификацию[3] объектов и субъектов информационных сетей;
- осуществлять контроль/разграничение доступа к информационным ресурсам;

[1] Программа «Цифровая экономика Российской Федерации». Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 года № 1632-р. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

[2] Там же. С. 7.

[3] Аутентификация — процедура установления подлинности или соответствия.

- гарантировать целостность баз данных (Хочуева и др., 2018).

В настоящее время шифрование данных осуществляется по американским сертификатам безопасности. В случае отзыва сертификатов их владельцами произойдет рассекречивание информации, хранящейся на различных сайтах.

Российские криптографические алгоритмы достаточно надежны. Они одобрены специальным комитетом Международной организации по стандартизации. Однако крупнейшие мировые IT-корпорации отказываются от использования этих алгоритмов (Хочуева и др., 2018). В связи с этим компетентным государственным органам необходимо принимать решительные меры по переходу российских организаций на отечественное шифровальное программное обеспечение.

По мнению ряда экспертов (Бауэр, 2017; Горулев, 2018), в условиях цифровой экономики использование технологий Блокчейн (blockchain) является одним из перспективных инструментов решения различных задач обеспечения национальной безопасности.

Результаты исследований В.П. Бауэра свидетельствуют о том, что на основе трех сетевых технологий — криптовалют (Блокчейн 1.0), смарт-контрактов (Блокчейн 2.0) и приложений (Блокчейн 3.0) — можно создать систему программно-информационных и аналитических средств, позволяющих с высокой степенью адаптивности, надежности и окупаемости решать такие задачи Стратегии национальной безопасности РФ1, как:

- укрепление обороноспособности страны;
- обеспечение государственной и общественной безопасности;
- повышение уровня и качества жизни населения;
- обеспечение устойчивого экономического роста;
- развитие образования, науки, технологий, здравоохранения и культуры;
- рациональное природопользование и др. (Бауэр, 2017: 155).

Данные технологии, в частности, могут применяться при обеспечении информационной безопасности хозяйствующих субъектов. Это объясняется тем, что она обладает следующими характеристиками:

- неизменность предыдущих записей является гарантией невозможности их фальсификации;
- децентрализованность, обеспечивающая простоту и надежность хранения информации;
- криптографичность, обусловливающая надежность защиты информации от несанкционированного доступа;
- возможность существенного сокращения стоимости трансакций вследствие замены традиционного хозяйственного договора смарт-контрактом (Горулев, 2018: 82–83).

Вместе с тем технологии Блокчейн позволяют участникам трансакций:

- сохранять конфиденциальность при проведении операций с криптовалютами, что делает возможным мошенничество, финансирование терроризма, отмывание доходов, полученных преступным путем, и т. п.;

[1] Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента РФ от 31 декабря 2015 года № 683. URL: http://www.consultant.ru/document/cons_doc_LAW_191669

- получать дополнительную доходность в результате проведения регулятивного арбитража;
- получать спекулятивный доход.

Кроме того, пользователи технологии Блокчейн в настоящее время сталкиваются с существенными технологическими ограничениями (например, длительность подтверждения трансакций, высокий уровень энергетических затрат и т.п.) (Горулев, 2018: 84).

Для обеспечения информационной безопасности необходимо активизировать подготовку кадров по информационной безопасности, а также обучать население способам защиты информации. Для этого планируется открытие массовых онлайн-курсов, развитие системы сертификации специалистов в области информационной безопасности, включение дисциплины «Информационная безопасность» в World Skills Russia (Старостина & Хохлов, 2018).

В условиях цифровой трансформации обеспечение информационной безопасности России предполагает решение следующих задач:

- выявление угроз информационной безопасности, причин и условий, способствующих их реализации;
- предотвращение утечки информации путем исключения несанкционированного доступа или воздействия на нее;
- мониторинг и анализ информационного пространства в целях выявления уязвимости информационных активов;
- комплексное использование методов и средств защиты компьютерных систем в целях нейтрализации угроз информационной безопасности;
- обеспечение единства, устойчивости и безопасности информационно-телекоммуникационной инфраструктуры РФ на всех уровнях информационного пространства;
- юридическая и организационная защита интересов личности, предпринимательских структур и государства;
- создание условий для увеличения объемов экспорта российских технологий информационной безопасности, а также учет национальных интересов в международных документах по вопросам информационной безопасности;
- применение отечественных технологий обеспечения целостности, конфиденциальности, аутентичности и доступности передаваемой информации и процессов ее обработки;
- преимущественное использование российского программного обеспечения и оборудования;
- государственная поддержка российских товаропроизводителей продуктов и услуг информационно-компьютерных технологий, осуществляющих патентование за рубежом;
- расширение использования технологий защиты информации на основе российских криптографических стандартов;
- предотвращение специальных воздействий, приводящих к разрушению, уничтожению, искажению информации либо к сбоям в работе информационных систем;

- минимизация и локализация ущерба от реализации угроз информационной безопасности (Хочуева и др., 2018).

Реализация мероприятий по обеспечению информационной безопасности хозяйствующих субъектов сопряжена с существенными затратами. Однако в настоящее время отсутствует научное обоснование уровня этих затрат. Одни эксперты считают, что крупные коммерческие организации должны расходовать на обеспечение своей информационной безопасности 1% совокупной годовой выручки от реализации продукции (работ, услуг), в то время как, по мнению специалистов IDC[1], инвестиции в информационную безопасность должны составлять 9,8-13,7% от общего бюджета IT-компаний (Махалина & Махалин, 2020: 137).

Заключение

В результате исследования были сделаны следующие выводы:

1. Осуществляемый в России переход к цифровой экономике, целью которого является существенное повышение эффективности общественного производства, сопряжен с усилением угроз национальной информационной безопасности.
2. Обеспечение информационной безопасности России предполагает решение следующих задач: выявление угроз информационной безопасности; предотвращение утечки конфиденциальной информации и действий конкурентов, криминальных структур и т.п., приводящих к уничтожению или искажению информации либо к сбоям в работе информационных систем; систематический мониторинг и анализ информационного пространства; комплексное использование методов и средств защиты компьютерных систем; обеспечение единства, устойчивости и безопасности информационно-телекоммуникационной инфраструктуры; занятие Россией лидирующих позиций в мировом информационном пространстве; преимущественное применение отечественных информационных технологий и программного обеспечения и оборудования; использование технологий защиты информации с использованием отечественных криптографических стандартов; минимизация и локализация ущерба от реализации угроз информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Бабкин А.В., Буркальцева Д.Д., Костень Д.Г., Воробьев Ю.Н. Формирование цифровой экономики в России: сущность, особенности, техническая нормализация, проблемы развития. Научно-технические ведомости СПбГПУ. Экономические науки, 2017, 10 (3), 9–25.

Бауэр В.П. Применение Блокчейн-технологии в разработке информационно-аналитической системы обеспечения национальной безопасности. В кн.: Стратегия экономической безопасности России: новые ориентиры развития. Сборник научных трудов I научно-практической конференции «Сенчаговские чтения». М.: Институт экономики РАН, 2017. С. 152–155.

[1] IDC — ведущий поставщик информации и консультационных услуг, организатор мероприятий на рынках информационных технологий, телекоммуникаций и потребительской техники.

Горулев Д.А. Экономическая безопасность в условиях цифровой экономики // Технико-технологические проблемы сервиса, 2018, 1 (43), 77–84.

Капранова Л.Д. Цифровая экономика в России: состояние и перспективы развития. Экономика. Налоги. Право, 2018, No. 2, 58–69.

Лесных Ю.Г., Повойко И.В. Риски и угрозы экономической безопасности России со стороны мирового финансового рынка в новых геоэкономических условиях. Вестник КубГАУ, 2015, 112 (08), 1462–1474.

Лопатин Ю.Н. Информационная безопасность в России. Проблемы, поиски решений. Гуманитарные исследования в Восточной Сибири, 2008, No. 2, 51–57.

Махалина О.М., Махалин В.Н. Цифровизация бизнеса увеличивает затраты на информационную безопасность. Информационные технологии в управлении, 2020, No. 1, 134–140.

Старостина Е., Хохлов А. Взгляд в будущее: система образования и воспитания кадров, успешно отвечающая на вызовы цифровой экономики. Информационная безопасность, 2018, No. 5. URL: https://lib.itsec.ru/articles2/job/vzglyad-v-buduscheesistema-obrazovaniya-i-vospitaniya-kadrov--uspeshno-otvechayuschaya-na-vyzovy-tsifrovoy-ekonomiki (дата обращения: 28.07.2020).

Удалов Д.В. Угрозы и вызовы цифровой экономики. Экономическая безопасность и качество, 2018, 1 (30), 12–18.

Филин С.А., Якушев А.Ж. Организационно-управленческие инновации как основа цифровой экономики. Национальные интересы: приоритеты и безопасность, 2018, 14 (7), 1319–1332.

Хочуева Ф.А., Шугунов Т.Л., Жуков А.З., Ингушев Ч.Х. Информационная безопасность сквозь призму цифровой экономики. Современные наукоемкие технологии, 2018, 11 (1), 65–71.

REFERENCES

Babkin, A.V., Burkal'ceva, D.D., Kosten', D.G., Vorob'ev, Yu.N. (2017). Formirovanie cifrovoj ekonomiki v Rossii: sushchnost', osobennosti, tehnicheskaya normalizaciya, problemy razvitiya [Formation of digital economy in Russia: nature, peculiarities, technical formalization, problems of development]. Nauchno-tehnicheskie vedomosti SPbGPU. *Ekonomicheskie nauki* [Scientific and technical statements of SPbSPU. Economic Sciences], vol. 10, no. 3, 9–25.

Bauer, V.P. (2017). Primenenie Blokchejn-tehnologii v razrabotke informacionno-analiticheskoj sistemy obespecheniya nacional'noj bezopasnosti [Blockchain technologies in the elaboration of the informational and analytical system of the national security]. In: *Strategiya ekonomicheskoj bezopasnosti Rossii: novye orientiry razvitiya: Sbornik nauchnyh trudov I nauchno-prakticheskoj konferencii «Senchagovskie chteniya»* [Strategy of economic security of Russia: new development thrusts: collection of scientific works of the I scientific and practical conference «Senchagov readings»] (pp. 152–155). Moscow: Institut ekonomiki RAN.

Gorulev, D.A. (2018). Ekonomicheskaya bezopasnost' v usloviyah cifrovoj ekonomiki

[Economic security in a digital economy] *Tehniko-tehnologicheskie problemy servisa* [Technical and technological issues of service], 1 (43), 77–84.

Kapranova, L.D. (2018). Cifrovaya ekonomika v Rossii: sostoyanie i perspektivy razvitiya [Digital economy in Russia: state of the art and perspectives of development]. *Ekonomika. Nalogi. Pravo* [Economy. Taxes. Law], no. 2, 58-69.

Lesnyh, Yu.G., Povojko, I.V. (2015). Riski i ugrozy ekonomicheskoj bezopasnosti Rossii so storony mirovogo finansovogo rynka v novyh geoekonomicheskih usloviyah [Risks and threats of economic security of Russia from global financial market in the contemporary geo-economic conditions]. *Vestnik KubGAU* [Scientific journal of KubSAU], 112 (08), 1462–1474.

Lopatin, Yu.N. (2008). Informacionnaya bezopasnost' v Rossii. Problemy, poiski reshenij [Information security in Russia: problems and search for solutions]. *Gumanitarnye issledovaniya v Vostochnoj Sibiri* [Humanities Research in the Russian Far East], no. 2, 51–57.

Mahalina, O.M., Mahalin, V.N. (2020). Cifrovizaciya biznesa uvelichivaet zatraty na informacionnuyu bezopasnost' [Digitalization of business increases expenditure on information security]. *Informacionnye tehnologii v upravlenii* [Information technologies in management], no. 1, 134–140.

Starostina, E., Hohlov, A. (2018). Vzglyad v budushchee: sistema obrazovaniya i vospitaniya kadrov, uspeshno otvechayushchaya na vyzovy cifrovoj ekonomiki [Future outlook: system of education and human resources development responding to the challenges of digital economy]. *Informacionnaya bezopasnost'* [Information security], no. 5. URL: https://lib.itsec.ru/articles2/job/vzglyad-v-buduschee-sistema-obrazovaniya-i-vospitaniya-kadrov--uspeshno-otvechayuschaya-na-vyzovy-tsifrovoy-ekonomiki (accessed 28 July 2020).

Udalov, D.V. (2018). Ugrozy i vyzovy cifrovoj ekonomiki [Treats and challenges of digital economy]. *Ekonomicheskaya bezopasnost' i kachestvo* [Economic security and quality], 1(30), 12–18.

Filin, S.A., Yakushev, A.Zh. (2018). Organizacionno-upravlencheskie innovacii kak osnova cifrovoj ekonomiki [Organizational and management innovations as a basis for digital economy]. *Nacional'nye interesy: prioritety i bezopasnost'* [National interests: priorities and secueity], 2018, vol. 14, no. 7, 1319–1332.

Hochueva, F.A., Shugunov, T.L., Zhukov, A.Z., Ingushev, Ch.H. (2018). Informacionnaya bezopasnost' skvoz' prizmu cifrovoj ekonomiki [Information security through the prism of the digital economy]. *Sovremennye naukoemkie tehnologii* [Advanced science-intensive technologies], 11 (1), 65–71.