DOI: 10.34680/BENEFICIUM.2021.2(39).21-26
УДК 338.1:004.94:004.056
JEL D8, G14, L2, M15, O3

CC BY NC

ОРИГИНАЛЬНАЯ СТАТЬЯ

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЭКОНОМИКИ: УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.Г. Мустафаев, Дагестанский государственный университет народного хозяйства, Махачкала, Республика Дагестан, Россия
Д.Н. Кобзаренко, Дагестанский государственный университет народного хозяйства, Махачкала, Республика Дагестан, Россия
А.Я. Бучаев, Дагестанский государственный университет народного хозяйства, Махачкала, Республика Дагестан, Россия

Аннотация. Цифровая экономика представляет собой совокупность разнообразных экономических процессов, осуществляемых с помощью информационных технологий. Процессы цифровой трансформации, связанные, в том числе, с четвертой промышленной революцией (Индустрия 4.0), открывают потребителям новые парадигмы использования информационных технологий. Все больше компаний строят бизнес-процессы на основе сквозной интеграции информационных потоков и их непрерывной аналитике, принимая управленческие решения на основе Big Data. Одновременно эти процессы создают новые поверхности угроз для значительного числа экономических субъектов. Участники цифрового взаимодействия заинтересованы в конфиденциальности критической информации или персональных данных. Таким образом, остро стоит вопрос обеспечения информационной безопасности технологических процессов обработки данных в организациях. Целью представленного в статье исследования является определение и изучение вызовов и угроз, с которыми сопряжен процесс цифровой трансформации в экономической сфере. Риски цифровой безопасности по своей природе являются динамическими, что обусловлено физическими законами и спецификой цифрового окружения, а также участием в данных процессах человека. Аналитики фиксируют рост числа и тяжести последствий инцидентов информационной безопасности в критической цифровой инфраструктуре, приводящих к крупномасштабным бедствиям. Подобные тенденции стимулируют работу экономических субъектов и правительств по обеспечению информационной безопасности критически важной информационной инфраструктуры, например, сферы здравоохранения или финансов. Решение задачи обеспечения информационной безопасности цифровой экономики, ее защиты от киберугроз должно учитывать, что основное отличие социально-экономических систем от традиционных систем обработки информации состоит в том, что функционирование первых напрямую связано бизнес-процессами, которые в большинстве случаев являются необратимыми. Для преодоления описанных проблем следует рассматривать риски информационной безопасности в киберфизических системах на основе методов, используемых в управлении экономическими и социальными рисками.
Ключевые слова: анализ данных, защита информации, информационная безопасность, киберугроза, персональные данные, уязвимость, цифровая трансформация, цифровая экономика, digital economy.

Для цитирования: Мустафаев А.Г., Кобзаренко Д.Н., Бучаев А.Я. Цифровая трансформация экономики: угрозы информационной безопасности // BENEFICIUM. 2021. № 2(39). С. 21-26. DOI: 10.34680/BENEFICIUM.2021.2(39).21-26

ORIGINAL PAPER

DIGITAL TRANSFORMATION OF THE ECONOMY: THREATS TO INFORMATION SECURITY

A.G. Mustafaev, Dagestan State University of National Economy, Makhachkala, Republic of Dagestan, Russia
D.N. Kobzarenko, Dagestan State University of National Economy, Makhachkala, Republic of Dagestan, Russia
A.Y. Buchaev, Dagestan State University of National Economy, Makhachkala, Republic of Dagestan, Russia

Abstract. The digital economy includes a variety of economic processes carried out using information technology. Digital transformation processes, including those associated with the fourth industrial revolution, open up new paradigms for the use of information technologies for users. More and more companies are building business processes based on end-to-end integration of information flows and their continuous analytics, making management decisions based on data. At the same time, these processes create new threat surfaces for a large number of economic agents. Participants in digital interactions are interested in the confidentiality of critical information or personal data. Thus, there is an acute issue of ensuring information security of technological data processing processes in

organizations. The aim of the work is to consider the challenges and threats that are associated with the process of digital transformation in the economic sphere. Digital security risks are dynamic in nature, which is due to physical laws and the specifics of the digital environment, as well as human participation in these processes. Analysts have noted an increase in the number and severity of the impact of information security incidents on critical digital infrastructure, leading to large-scale disasters. These trends are driving the work of organizations and governments to ensure the information security of critical information infrastructure, such as healthcare or finance. The solution to the problem of ensuring information security of the digital economy from cyber threats should take into account that the main difference between socio-economic systems and traditional information processing systems is that the functioning of the former is directly related to business processes, which in most cases are irreversible. To overcome the described problems, information security risks in cyber-physical systems should be considered based on the methods used in the management of economic and social risks.

Keywords: data analysis, information protection, information security, cyber threat, personal data, vulnerability, digital transformation, digital economy.

For citation: Mustafaev A.G., Kobzarenko D.N., and Buchaev A.Y. Digital Transformation of the Economy: Threats to Information Security // BENEFICIUM. 2021. Vol. 2(39). Pp. 21-26. (In Russ.). DOI: 10.34680/BENEFICIUM.2021.2(39).21-26

Под цифровой экономикой понимается широкий спектр экономической деятельности и коммерческих транзакций, осуществляемых с помощью информационных технологий. Довольно сложно провести четкую грань между традиционной и цифровой экономикой. Многие организации внедряют информационные технологии, позволяющие им выполнять процессы быстрее и эффективнее. Физические лица также являются частью цифровой экономики, поскольку они участвуют в задачах и транзакциях, которые ранее были им недоступны. Внедрение Интернета Вещей, аналитики больших данных, облачных технологий и социальных сетей продолжает вовлекать все больше людей и организаций в эту экономику.

Современное общество находится в стадии зарождения четвертой промышленной революции (Индустрии 4.0), переходя в эру, в которой сливаются цифровой, биологический и физический мир. В этой цифровой революции возможности и рост экономики зависят от благоприятной нормативно-правовой и деловой среды, готовности информационных технологий к новым парадигмам использования.

Несмотря на множество преимуществ, которые цифровая трансформация может принести потребителям, неоднородность внешней среды, трансграничность, появление новых бизнес-моделей и участие большого числа экономических субъектов могут поставить их интересы под угрозу. Стороны, вовлеченные в процессы цифрового взаимодействия, заинтересованы в том, чтобы часть информации, касающейся их деятельности, конфиденциальной информации или персональных данных, была постоянно доступна и при этом надежно защищена от неправомерного использования. Уничтожение или разглашение конфиденциальной информации, а также дезорганизация процессов ее обработки и передачи наносят серьезный материальный и репутационный ущерб.

Таким образом, остро стоит вопрос обеспечения информационной безопасности технологических процессов обработки данных в организациях. Необходимо широко использовать новые технологии для повышения кибербезопасности [1].

Кибербезопасность и анализ данных являются мощными драйверами, расширяющими возможности цифровой экономики. По мере увеличения цифровой трансформации бизнес-моделей, риск безопасности также возрастает в геометрической прогрессии. Информационные технологии сокращают расстояния между странами, компаниями и рынками, требуя от пользователей данные о пребывании в цифровом пространстве – цифровые следы. Целью данного исследования является определение и изучение вызовов и угроз, с которыми сопряжен процесс цифровой трансформации в экономической сфере.

Согласно рекомендациям международной Организации экономического сотрудничества и развития (Organization of Economic Cooperation and Development, OECD) [2] к рискам цифровой безопасности относят риски, связанные с использованием, развитием и управлением цифровой средой в процессе любой деятельности. Данные риски могут быть результатом сочетания угроз и уязвимостей в цифровом окружении и привести к уменьшению эффективности социально-экономической деятельности. Риски цифровой безопасности по своей природе являются динамическими, что обусловлено физическими законами и спецификой цифрового окружения, а также участием в данных процессах человека.

Правительства стран-участниц OECD прогнозируют рост числа и тяжести последствий инцидентов информационной безопасности в критической цифровой инфраструктуре, которые могут привести к крупномасштабным бедствиям [3]. Эти опасения стимулируют работу государств по обеспечению информационной безопасности критически важных видов деятельности. Например, в последнее время наблюдается увеличение количества

стран, в которых курсы по кибербезопасности преподаются не только в высших учебных заведениях, но также в начальной и средней школе (*рис. 1*).

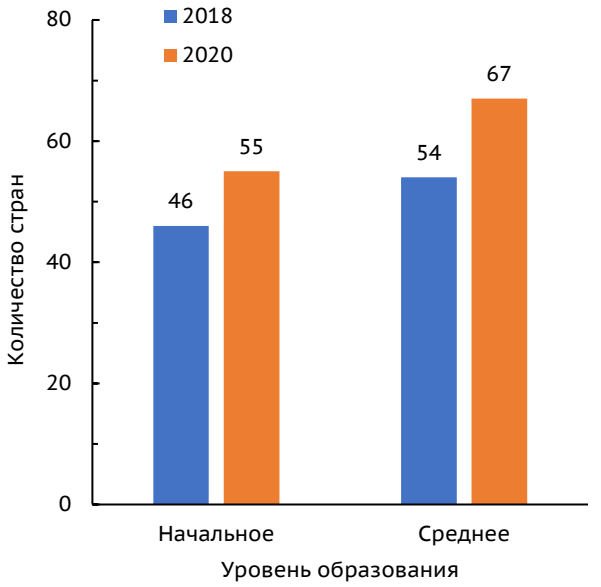

Рис. 1. **Количество стран, внедривших курсы по кибербезопасности в образовательные программы /** *Fig. 1.* **Number of Countries that have Introduced Cyber Security Courses in Educational Programmes**

Источник: [4] / *Source:* [4]

Парадигма цифровой экономики основана на взаимосвязи между данными, принятием управленческих решений и стоимостью бизнеса. С увеличением уровня цифровой трансформации мировое сообщество будет потреблять больше данных, чем когда-либо прежде. Без сомнения, данные могут считаться новой нефтью современности [5]. С 2003 г., каждые 48 часов человечество генерирует больше данных, чем за всю историю с момента зарождения цивилизации [6]. Важность вопроса в том, как общество собирается осмыслить всю эту информацию. Данные обладают удивительным свойством рождать добавленную стоимость при их структуризации и обработке, в том числе с привлечением алгоритмов искусственного интеллекта. Список компаний с самой высокой рыночной капитализацией ярко демонстрирует, что только компании, использующие управление, основанное на данных, показывают стабильные результаты и становятся победителями в цифровой экономике [7].

Всего 10 лет назад компаниям было достаточно присутствовать в Интернете, чтобы продемонстрировать свою инновационность. В настоящее время актуальность такого присутствия еще больше усиливается мобильными приложениями, поскольку компании предоставляют больше услуг в режиме реального времени. Пандемия COVID-19 привела к колоссальному росту Интернет-торговли. Компании, которые ставили своей целью развитие цифровых платформ, были мотивированы пандемией на увеличение усилий по расширению своего цифрового присутствия и ускорение разработки приложений для отслеживания активности потребителей по мере того, как они все чаще используют Интернет. Одновременно можно ожидать аналогичного или большего роста киберпреступности, поскольку возможности для нее расширяются со скоростью, сопоставимой с ростом рынка онлайн-услуг. По мере того, как компании внедряют усовершенствованные цифровые стратегии, им необходимо масштабировать операции по обеспечению безопасности, чтобы обеспечить безопасность своей расширяющейся онлайн-инфраструктуры.

Международные торговые платформы помогают увеличивать продажи малому и среднему бизнесу, используя облачные технологии. С помощью этих платформ они охватывают глобальную аудиторию, а сами платформы предлагают дополнительные услуги, такие как обработка отгрузок и управление клиентами. В основе этого массового роста лежит поток данных, и значительную его часть составляют персональные данные. Персональные данные являются драйвером цифровой революции, а также прямого маркетинга и продажи товаров и услуг. Такие компании, как Google, получают значительную часть своего дохода от профилирования и использования собираемых ими персональных данных, что позволяет напрямую нацеливать пользователей на различные продукты и услуги. Другие сервисные платформы, такие как E-bay, Alibaba и Amazon, предоставляют возможность как использовать данные, так и собирать их.

Прогресс в области облачных технологий дает возможность доступа к услугам и приложения по запросу или с оплатой по мере использования. Облачные технологии также позволили предприятиям начать работу в областях, характеризующихся большим объемом разнородных данных, таких как банковское дело и страхование, в которых сейчас наблюдается рост конкуренции со стороны онлайн-провайдеров, не имеющих физических отделений [8]. Не останавливаясь на достигнутом, банки переходят от предоставления отдельных услуг к предложению готовых решений по запросу клиентов, создавая экосистемы [9]. Недостаточный уровень защиты данных, циркулирующих в подобных экосистемах, влечет риски возможного мошенничества как со стороны сотрудников финансовых организаций, так и внешних злоумышленников [10]. Независимо от уровня защищенности организации-оператора данных существуют критические угрозы раскрытия персональных данных, финансовой и другой конфиденциальной информации.

Значимость киберугроз в том, что без физического вторжения и хищения цифровую экономику можно саботировать с помощью тех же технологий, на которых она основана. Цифровая

экономика не жизнеспособна, если ее информационная безопасность недостаточна. Эта экономика хрупка, и основной угрозой для развития цифровой экономики может стать потеря доверия к технологиям из-за киберугроз [11]. Рост числа кибератак [12] свидетельствует о том, что кибербезопасность стала одним из главных рисков, с которыми компании сталкиваются в условиях все большей цифровизации экономики, и что компаниям необходимо сохранять бдительность, расширяя свои протоколы безопасности, чтобы противостоять угрозе. Это должно вызывать тревогу у компаний, поскольку затраты, которые они могут понести с точки зрения репутации, потери рыночной стоимости и времени, затрачиваемого на устранение нарушения, могут быть огромными. Согласно исследованию [13], среднее время, необходимое организации для выявления нарушения, составило 206 дней, еще 73 дня потребовалось для устранения способствующих ему причин.

С развитием технологии Интернета Вещей и устройств, подключенных к облаку, расширяется и список киберугроз. В настоящее время существуют угрозы, актуальные для целевых устройств, которые связаны между собой использованием технологий Интернета Вещей [14], а также облачных сервисов [15]. Устройства Интернета Вещей подключаются к Интернету так же, как и многие другие устройства, но в силу малой вычислительной мощности у них отсутствуют механизмы безопасности, поэтому они являются легкой целью для злоумышленников [16]. Облачные технологии также получает широкое распространение среди организаций различных сфер деятельности, в том числе предоставляя инструменты для совместной работы (такие, как Cisco WebEx, Zoom, Microsoft Teams и Slack). Они создают новую поверхность атак [17], на которую злоумышленники переносят свой опыт [18]. Облако – это не то же самое, что локальные серверы, где организации могут тщательно следить за безопасностью своих приложений и конфиденциальной информацией. Если волна успешных атак захлестнет крупных поставщиков облачных услуг, будут очевидны огромные потери как материальные, так и репутационные.

Успешные кибератаки предоставляют возможность уничтожать или разрушать объекты инфраструктуры удаленно и анонимно. Например, в секторе здравоохранения многие организации связаны с государственными учреждениями, и, следовательно, утечки данных могут иметь разрушительные последствия [19]. В 2017 г. атака [20] вынудила отложить проведение плановых операций и прием больных и нанесла ущерб Национальной службе здравоохранения Великобритании в 120 млн. долларов США. В июне 2018 г. Сингапур подвергся кибератаке [21], в результате которой были потеряны цифровые данные о здоровье и личности 1.5 млн. граждан, включая данные премьер-министра страны. Успех этих и подобных атак подрывает доверие общественности и потребителей к организациям, ответственным за обработку персональных данных [22, 23].

Значительный процент успешных кибератак произошел в критически важной инфраструктуре, включая энергетику, связь, транспорт, нефть и газ, а также финансовые учреждения [24].

Злоумышленники неоднократно демонстрировали, что могут нанести значительный ущерб экономике с помощью критических уязвимостей. Атака программы-вымогателя WannaCry затронула более 150 стран и 200 тыс. компьютеров [25]. Только небрежность в написании программного кода WannaCry позволила уменьшить скорость распространения и предотвратить глобальную панику, тем не менее причинив ущерб на сумму 4 млрд. долларов США [26]. Реализация недекларированных возможностей и эксплуатация критических уязвимостей распространенного программного обеспечения является серьезной угрозой для цифровой экономики.

В [27] показано, как из-за отсутствия доверия пользователи отворачиваются от цифровой экономики и цифровых услуг. Это также может помочь объяснить отказ пользователей от новых цифровых возможностей в определенных областях. Если рассмотреть Интернет Вещей, даже простые устройства, подключенные к Интернету, могут собирать информацию о людях и их привычках или даже стать угрозой безопасности, превратив их в потенциальные мишени для хакеров, что делает пользователей менее склонными к использованию новых устройств в Интернет, и, тем самым, препятствует росту на перспективном рынке [28]. Недостаток доверия также может нанести ущерб конкуренции в цифровой экономике, поскольку люди с меньшей вероятностью будут использовать конкурирующие услуги, если они мало или совсем не доверяют существующим. Поступая таким образом, они могут непреднамеренно консолидировать существующие монополии в онлайн-сервисах [29].

С момента своего появления Интернет стал опорой современного мира, катализатором инноваций, которые продолжают развиваться и стимулировать экономический рост. Безопасность и конфиденциальность являются неотъемлемыми элементами поддержания и развития цифровой экономики. Успешная цифровизация между пользователями, а также частным рынком и государственным сектором в значительной степени основана на сочетании доверия и удобства. Пока удобство перевешивает риски, потребители будут продолжать пользоваться конкретными услугами. Эффективная защита цифровой среды невозможна без межгосударственного сотрудничества, в рамках которого открытость, готовность делиться информацией о потенциальных угрозах и случаях успешных атак помогают делать правильные выводы и предотвращать угрозы.

Для решения описанных выше проблем следует рассматривать риски информационной безопасности в киберфизических системах на основе методов, используемых в управлении экономическими и социальными рисками [2]. Инфраструктура цифровой экономики должна успешно противостоять угрозам безопасности, действующим в цифровой среде, особенно имеющим целенаправленный характер [30]. При решении задачи защиты цифровой экономики от киберугроз необходимо учитывать, что основное отличие этих систем от традиционных средств обработки информации состоит в том, что их функционирование напрямую связано с физическими или бизнес-процессами, которые в большинстве своем являются необратимыми.

Основные направления повышения информационной безопасности и предотвращения киберугроз состоят в постоянном мониторинге, включающем интеллектуальный анализ данных, инцидентов безопасности и обмен этой информацией на международном уровне. Кроме того, обществу необходимо развивать навыки безопасного взаимодействия с виртуальной средой и базовые знания в области кибербезопасности. Вместе с тем, необходимо руководствоваться принципом «Primum non nocere», т.к. чрезмерное усиление фрагментации экосистемы цифровой экономики, вызванное соображениями безопасности, может замедлить глобальный экономический рост.

Заявление об ответственности авторов

Авторы декларируют отсутствие конфликта интересов, связанных с публикацией данной статьи. Статья отражает результаты совместного исследования авторов.

References

[1] Teoh C.S., and Mahmood A.K. National cyber security strategies for digital economy // Journal of Theoretical and Applied Information Technology. 2017. Vol. 95(23). Pp. 6510-6522. DOI: https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1109%2FICRIIS.2017.8002519

[2] Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document (2015). OECD. URL: https://dx.doi.org/10.1787/9789264245471-en (accessed on 06.03.2021).

[3] Recommendation of the Council on Digital Security of Critical Activities, OECD/LEGAL/0456 (2019). OECD. URL: https://www.oecd.org/digital/ieconomy/recommendation-on-digital-security-of-critical-activities.htm (accessed on 10.03.2021).

[4] Global Cybersecurity Index 2020 (2021). ITU. URL: https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/ (accessed on 12.03.2021).

[5] Kuzmin V. Database // RG.RU. 2020. № 54(8108). URL: https://rg.ru/2020/03/12/mishustin-zaiavil-o-neobhodimosti-sozdaniia-cifrovogo-specnaza-v-rf.html (accessed on 15.03.2021). (In Russ.).

[6] Sieglar M.G. Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003 (2010). TechCrunch. URL: https://techcrunch.com/2010/08/04/schmidt-data (accessed on 13.03.2021).

[7] Global Top 100 companies by market capitalisation (2020). PWC. URL: https://www.pwc.com/gx/en/audit-services/publications/assets/global-top-100-companies-2020.pdf (accessed on 15.03.2021).

[8] Bank budushchego: bez ofisov, sotrudnikov i bez kliyentov? [The bank of the future: no offices, no employees and no clients?] (2018). Klerk.ru. URL: https://www.klerk.ru/buh/articles/477541 (accessed on 10.03.2021). (In Russ.).

[9] Sberbank sozdal strukturu SberX, chtoby prevratit'sya v konkurenta Google [Sberbank created the SberX structure to become a competitor to Google] (2018). The Bell. URL: https://thebell.io/sberbank-sozdal-strukturu-sberx-dlya-konkurentsii-s-google-i-facebook (accessed on 15.03.2021). (In Russ.).

[10] Gref nazval svoyey vinoy utechku dannykh kliyentov Sberbanka [Gref blamed Sberbank's customer data leak] (2019). Lenta.ru. URL: https://lenta.ru/news/2019/11/27/vina/ (accessed on 16.03.2021). (In Russ.).

[11] RAEK: kiberprestupnost' – real'naya ugroza dlya tsifrovoy ekonomiki [RAEC: cybercrime is a real threat to the digital economy] (2017). RAEC. URL: https://raec.ru/live/raec-news/9436 (accessed on 12.03.2021). (In Russ.).

[12] Humayed A., Lin J., Li F., and Luo B. Cyber-Physical Systems Security – A Survey // IEEE Internet of Things Journal. 2017. Vol. 4(6). Pp. 1802-1831. DOI: https://doi.org/10.1109/JIOT.2017.2703172

[13] Joseph R.C. Data Breaches: Public Sector Perspectives // IT Professional. 2018. Vol. 20(4). Pp. 57-64. DOI: https://doi.org/10.1109/MITP.2017.265105441

[14] Mustafayev A.G. The concept of security of the internet of things ecosystem based on software-defined networks // Industrial Automatic Control Systems and Controllers. 2019. Vol. 7. Pp. 62-66. (In Russ.). DOI: https://doi.org/10.25791/asu.07.2019.751

[15] Rafique K., Tareen A.W., Saeed M., Wu J., and Qureshi S.S. Cloud computing economics opportunities and challenges / In Proceedings – 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology, IC-BNMT. 2011. Pp. 401-406. DOI: https://doi.org/10.1109/ICBNMT.2011.6155965

[16] Mustafayev A.G. Monitoring the security of the internet of things infrastructure based on machine learning technologies // Industrial Automatic Control Systems and Controllers. 2020. Vol. 2. Pp. 36-41. (In Russ.). DOI: https://doi.org/10.25791/asu.2.2020.1156

[17] McAfee Uncovers Flood of Attacks on Corporate Cloud Accounts as Companies Work from Home (2020). McAfee. URL: https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=ef81c271-da74-4b80-a203-5dbf9680b8b8 (accessed on 19.03.2021).

[18] Yang P., Xiong N., and Ren J. Data Security and Privacy Protection for Cloud Storage: A Survey // IEEE Access. 2020. Vol. 8. Pp. 131723-131740. DOI: https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1109%2FACCESS.2020.3009876

[19] Walker-Roberts S., Hammoudeh M., and Dehghantanha A. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure // IEEE Access. 2018. Vol. 6. Pp. 25167-25177. DOI: https://doi.org/10.1109/ACCESS.2018.2817560

[20] WannaCry cyber-attack cost the NHS £92m as 19,000

appointments cancelled (2018). The Telegraph. URL: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled (accessed on 19.03.2021).
[21] V Singapure proizoshla samaya krupnaya v istorii strany kiberataka [The largest cyberattack in the history of the country occurs in Singapore] (2018). SecurityLab.ru. URL: https://www.securitylab.ru/news/494576.php (accessed on 15.02.2021). (In Russ.).
[22] Chuang I.-Hs., Weng T.-Ch., Tsai J.-Sh., Horng M.-F., and Kuo Y.-Hw. A Reliable IoT Data Economic System Based on Edge Computing / In Proceedings – 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). 2018. Pp. 1-5. DOI: https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1109%2FPIMRC.2018.8580742
[23] Mehmood A., Natgunanathan I., Xiang Y., Poston H., and Zhang Y. Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications // IEEE Access. 2018. Vol. 6. Pp. 33552-33567. DOI: http://dx.doi.org/10.1109/ACCESS.2018.2841972
[24] Deng R., Xiao G., and Lu R. Defending Against False Data Injection Attacks on Power System State Estimation // IEEE Transactions on Industrial Informatics. 2017. Vol. 13(1). Pp. 198-207. DOI: https://doi.org/10.1109/TII.2015.2470218
[25] Satheesh Kumar M., Ben-Othman J., and Srinivasagan K.G. An Investigation on Wannacry Ransomware and its Detection / In Proceedings – 2018 IEEE Symposium on Computers and Communications. 2018. Pp. 1-6. DOI: https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1109%2FISCC.2018.8538354
[26] "WannaCry" ransomware attack losses could reach $4 billion (2017). CBSNews. URL: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses (accessed on 18.03.2021).
[27] Wernberg-Tougaard Chr. IT-Security Beyond Borders – an Assessment of Trust Levels Across Europe. In book ISSE/SECURE 2007 Securing Electronic Business Processes. 2007. Pp 82-92. DOI: https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1007%2F978-3-8348-9418-2_9
[28] Nazvany 4 glavnyye prichiny, po kotorym na Zapa-de ne pokupayut rossiyskiy khaytek [4 main reasons why Russian hi-tech is not bought in the West] (2020). CNews. URL: https://www.cnews.ru/news/top/2020-03-23_soosnovatel_iot_factory_obyasnil (accessed on 18.03.2021). (In Russ.).
[29] Barony i magnaty: v chem kongress SSHA obvinyayet Kremniyevuyu dolinu [Barons and tycoons: what the US Congress accuses Silicon Valley] (2020). Gazeta.ru. URL: https://www.gazeta.ru/tech/2020/10/07/13309873/monopoly.shtml (accessed on 11.03.2021). (In Russ.)
[30] Ashibani Y., and Mahmoud Q.H. Cyber Physical Systems Ssecurity: Analysis, Challenges and Solutions // Computers & Security. 2017. Vol. 68. Pp. 81-97. DOI: https://www.researchgate.net/deref/http%3A%2F%2Fdx.doi.org%2F10.1016%2Fj.cose.2017.04.005

Информация об авторах / About the Authors

Арслан Гасанович Мустафаев – д-р техн. наук, доцент; профессор, Дагестанский государственный университет народного хозяйства, Махачкала, Республика Дагестан, Россия / **Arslan G. Mustafaev** – Doctor of Technical Sciences, Docent; Professor, Dagestan State University of National Economy, Makhachkala, Republic of Dagestan, Russia
E-mail: Arslan_mustafaev@mail.ru
SPIN РИНЦ 3544-1265
ORCID 0000-0003-3463-4303
Дмитрий Николаевич Кобзаренко – д-р техн. наук; профессор, Дагестанский государственный университет народного хозяйства, Махачкала, Республика Дагестан, Россия / **Dmitry N. Kobzarenko** – Doctor of Technical Sciences; Professor, Dagestan State University of National Economy, Makhachkala, Republic of Dagestan, Russia
E-mail: dmitry@fail.ru
SPIN РИНЦ 9846-8451
Абдулхамид Яхьяевич Бучаев – разработчик программного обеспечения, Дагестанский государственный университет народного хозяйства, Махачкала, Республика Дагестан, Россия / **Abdulhamid Ya. Buchaev** – Software Designer, Dagestan State University of National Economy, Makhachkala, Republic of Dagestan, Russia
E-mail: ayb@dginh.ru

Дата поступления статьи: 5 апреля 2021
Принято решение о публикации: 20 июня 2021

Received: 5 April 2021
Accepted: 20 June 2021