

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЭКОНОМИКИ: ПРОБЛЕМЫ БЕЗОПАСНОСТИ

Абдеева А.Н.,

ГАОУ ВО «Дагестанский государственный университет народного

хозяйства»,

abdeeva@mail.ru

Адзиев А.Р.,

ГАОУ ВО «Дагестанский государственный университет народного

хозяйства»,

adziev_05@mail.ru

Мусаев М.Х.,

ГАОУ ВО «Дагестанский государственный университет народного

хозяйства»,

musaev_m@mail.ru

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, 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.

Ключевые слова: уязвимость, цифровая трансформация, цифровая экономика, анализ данных, кибербезопасность.

DIGITAL TRANSFORMATION OF THE ECONOMY: SECURITY ISSUES

Abdeeva A.N.,

Adziev A.R.,

Musaev M.H.

Abstract. The digital economy is a set of various economic processes carried out with the help of information technologies. The processes of digital transformation, including those associated with the fourth industrial revolution, open up new paradigms for the use of information technologies to consumers. More and more companies are building business processes based on the end-to-end integration of information flows and their continuous analytics, making management decisions based on Big Data. At the same time, these processes create new threat surfaces for a significant number of economic actors. Participants in digital interaction are interested in the confidentiality of critical information or personal data. Thus, the issue of ensuring information security of technological processes of data processing in organizations is acute. The purpose of the study presented in the article is to identify and study the challenges and threats associated with the process of digital transformation in the economic sphere.

Keywords: vulnerability, digital transformation, digital economy, data analysis, cybersecurity.

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 [1]. 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.

Кибербезопасность и анализ данных являются мощными драйверами, расширяющими возможности цифровой экономики [2, 3]. 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) [4, 5] 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.

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. 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 [6, 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.

Инфраструктура цифровой экономики должна успешно противостоять угрозам безопасности, действующим в цифровой среде, особенно имеющим целенаправленный характер. 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 «Прежде всего не вредить», т.к. чрезмерное усиление фрагментации экосистемы цифровой экономики, вызванное соображениями безопасности, может замедлить глобальный экономический рост.

Библиографический список

1. Мустафаев А. Г., Кобзаренко Д. Н., Бучаев А. Я. Цифровая трансформация экономики: угрозы информационной безопасности // *Beneficium*. – 2021. – № 2(39). – С. 21-26.
2. Teoh C.S., Mahmood A.K. National cyber security strategies for digital economy // *Journal of Theoretical and Applied Information Technology*. 2017. Vol. 95(23). Pp. 6510-6522.
3. Мурадова С. А. Цифровая трансформация и её влияние на финансовый сектор России // *Интеллектуальные ресурсы – региональному развитию*. – 2022. – № 1. – С. 192-196.
4. Recommendation of the Council on Digital Security of Critical Activities, OECD/LEGAL/0456 (2019). OECD. – URL: <https://www.oecd.org/digital/ieconomy/recommen-dation-on-digital-security-of-critical-activities.htm> (accessed on 10.03.2021).
5. Global Cybersecurity Index 2020 (2021). ITU. – URL: <https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/> (accessed on 12.03.2021).
6. Гребенюк Е.В., Храмов В.В. Особенности архитектуры system of systems в рамках единого информационного пространства // *Интеллектуальные ресурсы – региональному развитию*. – 2022. – № 2. – С. 174-180.
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).