

УДК 338

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ
ЦИФРОВИЗАЦИИ ЭКОНОМИКИ: ВЫЗОВЫ И СТРАТЕГИИ
ОБЕСПЕЧЕНИЯ**

Котанджян А. В.

к.э.н., доцент,

Вятский государственный университет,

Киров, Россия

Рыжкова В. Р.

студент,

Вятский государственный университет,

Киров, Россия

Рычкова Н. А.

студент,

Вятский государственный университет,

Киров, Россия

Аннотация: Глубокие изменения в экономической сфере, обусловленные активным применением технологий «Индустрии 4.0», концепции интернета вещей (IoT), аналитики больших объемов данных и систем искусственного интеллекта, существенно преобразуют структуру ведения бизнеса и функционирования государственного аппарата. Этот прогрессивный процесс, предоставляя очевидные выгоды в части увеличения продуктивности и результативности, создает принципиально новые и значительные риски в сфере защиты информации. Статья посвящена анализу ключевых вызовов ИБ в эпоху цифровизации, исследованию уязвимостей на уровне промышленных предприятий, государственных систем и малого бизнеса, а также систематизации стратегий

Вектор экономики | www.vectoreconomy.ru | СМЭ Эл № ФС 77-66790, ISSN 2500-3666

и инструментов обеспечения защищенности информационного пространства. На основе анализа ряда научных публикаций обобщены современные подходы к построению комплексных систем ИБ, подчеркнута критическая важность человеческого фактора и правового регулирования.

Ключевые слова: информационная безопасность, цифровизация экономики, кибербезопасность, «Индустрия 4.0», угрозы, защита данных.

***INFORMATION SECURITY IN THE CONTEXT OF DIGITALIZATION OF
THE ECONOMY: CHALLENGES AND STRATEGIES FOR ENSURING***

Kotandzhyan A.V.

PhD in Economics, Associate Professor,

Vyatka State University,

Kirov, Russia

Ryzhkova V.R.

Student,

Vyatka State University,

Kirov, Russia

Rychkova N. A.

Student,

Vyatka State University,

Kirov, Russia

Abstract: Deep changes in the economic sphere, caused by the active use of Industry 4.0 technologies, the concept of the Internet of Things (IoT), big data analytics, and artificial intelligence systems, are significantly transforming the structure of

business operations and the functioning of the state apparatus. This progressive process, while providing obvious benefits in terms of increased productivity and efficiency, also poses fundamentally new and significant risks in the field of information security. The article is devoted to the analysis of key challenges of information security in the era of digitalization, the study of vulnerabilities at the level of industrial enterprises, state systems, and small businesses, as well as the systematization of strategies and tools for ensuring the security of the information space. Based on the analysis of a number of scientific publications, modern approaches to building comprehensive information security systems are summarized, and the critical importance of the human factor and legal regulation is emphasized.

Key words: information security, digitalization of the economy, cybersecurity, Industry 4.0, threats, and data protection.

Цифровизация признается технологической основой устойчивого развития и драйвером экономического роста, что отражено в ключевых стратегических документах РФ [1, 2]. Однако интеграция цифровых технологий в производственные и управленческие цепочки значительно усложняет объект защиты. Информационная безопасность в «Индустрии 4.0» охватывает не только данные и средства их обработки, но и динамически изменяющиеся взаимосвязи между субъектами и киберфизическими системами [3]. Объединение и интеграция корпоративных систем формируют унифицированное информационное пространство организации, где слабая защищенность любого компонента может вызвать цепь последовательных сбоев.

Основные угрозы ИБ в условиях цифровой экономики носят комплексный характер. Исследователи выделяют следующие ключевые группы рисков:

1. Технологические угрозы: Атаки на автоматизированные системы управления технологическими процессами (АСУ ТП), SCADA-системы и интернет вещей, которые могут привести не только к утечке данных, но и

- к физическим повреждениям оборудования или нарушению критических процессов [3]. Рост числа кибератак на промышленные предприятия [4].
2. Внешние геополитические угрозы: Использование информационных технологий для воздействия на суверенитет, экономическую и социально-политическую стабильность государства, что отражено в Доктрине информационной безопасности РФ [6].
 3. Внутренние институциональные угрозы: Зависимость от импорта электронных компонентов и программного обеспечения, отставание в разработке и внедрении отечественных ИТ-решений, дефицит квалифицированных кадров в сфере ИБ.
 4. Угрозы конфиденциальности: Массированный сбор и риск утечки персональных и биометрических данных в условиях повсеместной цифровизации услуг [7].
 5. Угрозы, связанные с человеческим фактором: Неосведомленность персонала, инсайдерские угрозы (как умышленные, так и по неосторожности), которые остаются одним из наиболее слабых звеньев в системе защиты [8].

Преобразование подхода к информационной безопасности – необходимый ответ на существующие проблемы. Классическая концепция, ориентированная на базовую защиту, уступает место продвинутой модели кибербезопасности, основанной на прогнозировании и гибкости. Модель для «Индустрии 4.0» включает не только мониторинг и контроль, но и прогнозирование угроз, оценку их воздействия, принятие решений и автоматическое ответное воздействие, образуя замкнутый контур управления безопасностью [3].

Ключевые направления обеспечения ИБ в современных условиях включают:

1. Развитие нормативно-правовой базы: Совершенствование законодательства в области защиты критической информационной инфраструктуры (КИИ), персональных данных и коммерческой тайны. Важным шагом является переход на отечественные криптографические стандарты и программное обеспечение [10].
2. Внедрение передовых технологий защиты: Использование технологий искусственного интеллекта и машинного обучения для анализа больших объемов данных и обнаружения аномалий, применение блокчейна для обеспечения целостности транзакций, внедрение биометрических систем аутентификации [11].
3. Формирование культуры безопасности: Систематическое обучение и повышение осведомленности сотрудников на всех уровнях, от рядовых специалистов до топ-менеджмента, является не менее важным, чем технические меры [8].
4. Комплексный и многоуровневый подход: Защита должна охватывать физический, аппаратный, программный и криптографический уровни, а также организационно-правовые аспекты. Необходимо сочетание средств защиты периметра (межсетевые экраны, системы обнаружения вторжений), защиты конечных точек и управления доступом [12].
5. Государственная поддержка и международное сотрудничество: Стимулирование развития отечественной индустрии ИБ, финансирование исследований, гармонизация стандартов и обмен информацией об угрозах на международном уровне [9].

Особое внимание требуется уделять малому и среднему бизнесу, который зачастую не обладает достаточными ресурсами для построения комплексных систем ИБ, но при этом активно цифровизируется и становится мишенью для атак. Для них актуальны облачные сервисы безопасности, тиражируемые решения и государственные программы поддержки [13].

Цифровизация экономики – объективный и необратимый процесс, несущий как колоссальные возможности, так и серьезные риски для информационной безопасности личности, бизнеса и государства. Анализ современных исследований показывает, что угрозы становятся все более масштабными, изощренными и потенциально разрушительными. Рост киберпреступности свидетельствует о недостаточной эффективности устаревших, реактивных подходов к защите.

Успешное обеспечение ИБ в новых условиях требует системного, проактивного и многостороннего подхода. Он должен интегрировать непрерывное совершенствование законодательства, опережающее внедрение современных технологий (ИИ, блокчейн, квантово-устойчивая криптография), масштабную подготовку кадров и формирование устойчивой культуры безопасности в организациях.

Как отмечают исследователи, инвестиции в информационную безопасность должны рассматриваться не как издержки, а как стратегические вложения в устойчивость, конкурентоспособность и суверенитет в цифровую эпоху [14]. Только комплексное взаимодействие государства, бизнеса и научного сообщества позволит минимизировать риски и реализовать потенциал цифровой экономики, обеспечив надежную защиту ее ключевого актива – информации.

Библиографический список

1. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».
2. Программа «Цифровая экономика российской федерации» утверждена распоряжением правительства РФ от 28.07.2017 г. №1632-Р.
3. Каранина, Е. В. Особенности обеспечения информационной безопасности промышленных предприятий в условиях цифровизации экономики / Е. В. Каранина, М. А. Бортников, Р. Н. Гусейнзаде // Общество. Наука.

- практической конференции. В 2-х томах, Киров, 11–29 апреля 2022 года. Том 1. – Киров: Вятский государственный университет, 2022. – С. 1017-1024. – EDN GTCEIJ.
4. Снастин, В. А. Оценка качества обеспечения информационной безопасности России в условиях цифровизации экономики / В. А. Снастин, Т. П. Харитонов, Г. Ю. Сорока // Международный журнал гуманитарных и естественных наук. – 2021. – № 8-1(59). – С. 105-108. – DOI 10.24412/2500-1000-2021-8-1-105-108. – EDN PZMLQW.
 5. Ефимов, А. А. Современный инструмент цифровой безопасности / А. А. Ефимов, А. А. Морозова // Цифровая экономика глазами студентов : материалы Международной научной конференции, Казань, 12 мая 2023 года. – Казань: ИП Сагиев А.Р., 2023. – С. 355-358. – EDN QXZZMG.
 6. Тарасова, А. А. Информационная безопасность в России в эпоху цифровизации / А. А. Тарасова // Инновации. Наука. Образование. – 2022. – № 49. – С. 1340-1348. – EDN XVAFMS.
 7. Степанова, М. П. Обеспечение информационной безопасности в условиях цифровизации экономики / М. П. Степанова // Экономическая безопасность России: проблемы и перспективы : Материалы XI Международной научно-практической конференции ученых, специалистов, преподавателей вузов, аспирантов, студентов, Нижний Новгород, 17–19 мая 2023 года. – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2023. – С. 104-107. – EDN XNIXGN.
 8. Вилкина, М. В. Информационная безопасность компании в условиях цифровизации экономики / М. В. Вилкина // Современные научные исследования: исторический опыт и инновации : Сборник материалов XIX Международной (политематической) научно-практической конферен-

- ции, Краснодар, 09–10 февраля 2023 года. – Краснодар: Академия маркетинга и социально-информационных технологий - ИМСИТ (г. Краснодар), 2023. – С. 182-188. – EDN VFXQLW.
9. Золотарева, С. А. Информационная безопасность в условиях цифровизации экономики / С. А. Золотарева, Н. А. Суковатицина // Вестник науки. – 2024. – Т. 3, № 6(75). – С. 190-195. – EDN TXJAKW.
10. Фазлыев, Р. Ш. Перспективы развития направления информационной безопасности в условиях цифровизации экономики / Р. Ш. Фазлыев // Электронный экономический вестник Татарстана. – 2021. – № 2. – С. 69-71. – EDN WZCBQG.
11. Назаров, А. Ш. Угрозы информационной безопасности в условиях цифровизации экономики и способы защиты от них / А. Ш. Назаров // Политехнический вестник. Серия: Интеллект. Инновации. Инвестиции. – 2024. – № 2(66). – С. 68-72. – EDN GVVIRN.
12. Силкина, О. Ю. Обеспечение информационной безопасности в условиях цифровизации экономики / О. Ю. Силкина, Р. С. Зарипова // Современные направления развития экономики и управления образованием : Сборник материалов Всероссийской научно-практической конференции с международным участием, Грозный, 27 октября 2022 года. – Грозный-Махачкала: Чеченский государственный педагогический университет, 2022. – С. 212-218. – EDN HLVAWJ.
13. Рагимханова, К. Т. Информационная безопасность в условиях цифровой экономики / К. Т. Рагимханова, З. Л. Хазбулатов, О. М. Танделова // Экономика: вчера, сегодня, завтра. – 2023. – Т. 13, № 1-1. – С. 247-253. – DOI 10.34670/AR.2023.91.15.027. – EDN CITWFN.
14. Бахолдина, Т. Д. Актуальность информационной безопасности в условиях цифровизации экономики / Т. Д. Бахолдина // Образование. Наука. Производство : XIII Международный молодежный форум, Белгород, 08–

09 октября 2021 года. – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2021. – С. 2299-2301. – EDN SXHFIR.