УДК 338.342.44

М.Н. Муратова
ФГБОУ ВО «Российской государственный университет правосудия», Москва, email: 5856740@gmail.com

ЦИФРОВАЯ ЭКОНОМИКА В СОВРЕМЕННЫХ УСЛОВИЯХ РАЗВИТИЯ РОССИИ И ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ключевые слова: цифровизация, цифровая экономика, информационная безопасность, защита данных, бизнес, экономическая деятельность.

Повсеместная цифровизация охватила практически все, как бытовые, так и профессиональные сферы жизнедеятельности человека. Особый интерес представляет анализ вопросов, связанных с развитием цифровой экономики. При этом, несмотря, на ряд преимуществ, которые достигаются с развитием цифровой экономики, актуализируются проблемы, связанные с обеспечением информационной безопасности. Основной целью представленной статьи является выполнение анализа текущего состояния цифровой экономики России, а также ключевых проблем, связанных с информационной безопасностью в новых цифровых условиях. В результате работы представлены текущие тенденции цифровизации экономики нашей страны, а также обоснована необходимость решения проблем, связанных с защитой данных. Автором не только систематизируются тенденции вокруг цифровой экономики в современных условиях развития России, но также формируются рекомендации по обеспечению высокого уровня информационной безопасности и стабильности развития в данном направлении.

M.N. Muratova
Russian State University of Justice, Moscow, email: 5856740@gmail.com

THE DIGITAL ECONOMY IN THE MODERN CONDITIONS OF RUSSIA'S DEVELOPMENT AND THE PROBLEMS OF INFORMATION SECURITY

Keywords: digitalization, digital economy, information security, data protection, business, economic activity.

Widespread digitalization has covered almost all spheres of human life, both domestic and professional. Of particular interest is the analysis of issues related to the development of the digital economy. At the same time, despite a number of advantages that achieved by the development of the digital economy, the problems associated with ensuring information security are becoming more urgent. The main purpose of the presented article is to analyze the current state of the Russian digital economy, as well as key issues related to information security in the new digital environment. As a result of the work, the current trends in the digitalization of the economy of our country are present, as well as the need to solve problems related to data protection is justified. The author not only systematizes the trends around the digital economy in the modern conditions of Russia's development, but also forms recommendations for ensuring a high level of information security and stability of development in this direction.

Цифровизация продолжает стремительно трансформировать мировую экономику и общество, создавая множество возможностей и в то же время вызовов для устойчивого развития. Цифровая экономика (далее – ЦЭ) представляет собой экономическую деятельность, основанную на использовании инновационных цифровых и информационных технологиях (далее – ИТ). По мнению авторов Муратова М.Н., Макарова Е.Е. и Сыщикова Е.Н., интеграция современных цифровых технологий предоставляет возможности существенного повышения эффективности и качества, как производственной деятельности, так и выпускаемой продукции [1]. Вместе с этим, при активной интеграции и применении информационных технологий актуализируются вопросы, связанные с уязвимостью современных предприятий, что подтверждается стремительным ростом числа компьютерных преступлений.

В связи с этим цифровая трансформация экономики неразрывно становится связанной с вопросами обеспечения информационной безопасности (далее – ИБ). ИБ представляет собой комплекс мер, направленных на повышение защищенности информаци-

онных ресурсов организации от внутренних и внешних угроз, реализация которых способна нанести существенный ущерб интересам личности, общества и государству [2]. В рамках представленной статьи более подробно рассматриваются текущие тенденции развития цифровой экономики, а также ставится ряд задач по определению и обеспечению информационной безопасности в данной сфере. Материалы работы могут быть использованы на современных предприятиях и организациях, выступая в качестве руководства по актуализации необходимости обеспечения своей ИБ, а также раскрывая возможный комплекс мер для ее реализации.

Материалы и методы

В рамках работы применен комплекс методов научного исследования, основными из которых являются анализ, синтез и обобщение. Автором настоящей статьи были использованы материалы последних актуальных исследований в области развития цифровой экономики и вызовов, препятствующих активному распространению и использованию инновационных решений.

Результаты исследования

Цифровая экономика представляет собой систему экономических, социальных и технологических отношений, основанных на использовании цифровых технологий, которые напрямую влияют на процессы производства, потребления и обмена информацией [3]. В основе цифровой экономики лежат такие ключевые ресурсы, как данные, знания и информационные технологии, что позволяет ускорять инновации, повышать эффективность управления, а также улучшать взаимодействие между предприятиями, государством и потребителями. Состав цифровой экономики включает цифровую инфраструктуру, которая обеспечивает связь и хранение данных, платформенные технологии, такие как облачные вычисления и интернет вещей, а также цифровые сервисы, предоставляющие удобные и эффективные решения для различных отраслей. Тенденции непрерывного роста цифровизации и развития ЦЭ подтверждаются статистическими исследованиями, которые свидетельствуют о том, что к 2023 году «цифровая зрелость» ключевых отраслей экономики составила более 74% против 64% плановых (по данным ИКС Медиа, автор Николай Носов).

В ЦЭ информация и данные выступают основными факторами производства и основываются на внедрении и использовании цифровых технологий в различных секторах. Она включает в себя преобразование традиционных отраслей через цифровизацию процессов и создание новых бизнес-моделей на базе информационно-коммуникационных технологий. Важной особенностью цифровой экономики является её глобальный характер: использование интернета и цифровых платформ позволяет компаниям, государственным структурам и гражданам взаимодействовать и обмениваться информацией мгновенно, что ускоряет трансформацию экономических процессов и значительно расширяет доступ к ресурсам и услугам.

В рамках ЦЭ выделяются такие элементы, как большие данные, искусственный интеллект, интернет вещей и блокчейн, которые играют ключевую роль в оптимизации и автоматизации операций. Благодаря использованию таких технологий происходит улучшение процессов управления и принятия решений, что приводит к повышению производительности и эффективности работы предприятий. Для бизнеса цифровая экономика предоставляет возможности для создания новых рыночных ниш и оптимизации цепочек поставок, а для общества в целом – улучшает доступ к услугам и качеству жизни. Государственные структуры активно развивают цифровую инфраструктуру и разрабатывают политику поддержки цифровых проектов, стремясь создать условия для безопасного и устойчивого цифрового роста.

Актуальность ЦЭ в России на момент 2024 года обусловлена необходимостью повышения конкурентоспособности национальной экономики, оптимизации государственных и коммерческих процессов, а также ускорения интеграции страны в мировую цифро-

вую экосистему. Россия активно внедряет цифровые технологии в различные сферы – от государственных услуг и финансов до образования и промышленности [4]. Подтверждением являются результаты того же исследования, которое свидетельствует о двукратном росте рынка данных в России в период с 2021 по 2024 годы (200 и 400 миллиардов рублей соответственно). Одной из основных тенденций развития является расширение инфраструктуры, поддерживающей новые поколения сетей и технологий, таких как 5G и искусственный интеллект, что способствует улучшению качества жизни и доступности цифровых сервисов для граждан. Также отмечается тенденция к усилению регулирования и защиты данных, что связано с ростом угроз информационной безопасности в цифровом пространстве. Важным направлением стало внедрение решений для цифровой трансформации предприятий, что позволяет повышать их производительность и создавать новые модели взаимодействия на рынке.

Несмотря на значительные преимущества, развитие цифровой экономики сталкивается с рядом сложных проблем, одной из наиболее острых среди которых является проблема обеспечения информационной безопасности. Эта проблема заключается в необходимости защитить данные и информационные системы от несанкционированного доступа, кибератак, утечек информации и других угроз, которые могут нанести ущерб как отдельным пользователям, так и целым секторам экономики [5]. ИБ становится критической задачей, так как цифровые технологии проникают во все сферы жизни и бизнеса, а количество и сложность киберугроз стремительно растет. Актуальность данной проблемы подтверждается статистическими данными, которые свидетельствуют о 12%-ом росте числа кибератак в период с 2022 по 2023 годы (рис. 1). По последнему аналитическому отчету компании «РТК-Солар» число кибератак во втором квартале 2023 года составило свыше 325 000 инцидентов.

Основные риски для ЦЭ включают угрозы атак на инфраструктуру предприятий и государственных учреждений, шпионские атаки, направленные на кражу интеллектуальной собственности и конфиденциальной информации, а также вредоносное вмешательство в операционные процессы, что может привести к серьезным экономическим и репутационным потерям [6]. Для бизнеса это угроза потери данных клиентов и интеллектуальных активов, что может подорвать доверие клиентов и партнеров, а для государства – риски утечки конфиденциальных данных, влияющие на национальную безопасность (табл. 1).

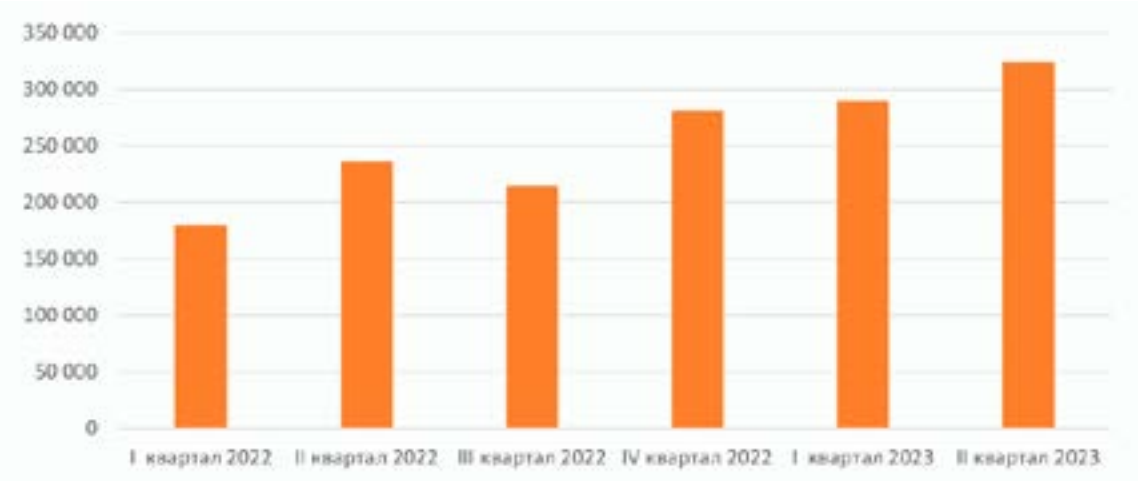

Рис. 1. Динамика роста числа кибератак 2022-2023 гг.

Таблица 1

Угрозы информационной безопасности государства

Угрозы	Субъекты угроз	Мотивы	Объекты атаки	Методы
Информационные войны	Государства	Информационное превосходство, вмешательство в информационные процессы, военные и политические цели	СМИ, интернет, соцсети, электронная почта	Скрытие, смещение понятий, отвлечение, дезинформация, «fake news», слухи, спам
Кибератаки	Государства, спецслужбы, шпионы, активисты, спамеры, хакеры	Уничтожение, искажение, фальсификация, получение доступа к информации	Государственные, корпоративные и частные информационные сети и системы, электронная почта	DoS-атаки, вирусы, черви, перехватчики, фишинг, вишинг, сниффер
Кибершпионаж	Государства, спецслужбы, шпионы, активисты, инсайдеры, спамеры, хакеры	Доступ к военной, оборонной, дипломатической или экономической информации, идеология, личные выгоды	Государственные, корпоративные и частные информационные сети, эл. почта	DoS-атаки, вирусы, черви, перехватчики, фишинг, сниффер, логические бомбы, трояны
Киберпреступность	Государства, спецслужбы, шпионы, активисты, инсайдеры, спамеры, хакеры, коммерческие структуры	Получение политической, личной и финансовой выгоды, кража персональных данных и интеллектуальной собственности и мошенничество	Государственные, корпоративные и частные информационные сети и системы, электронная почта	DoS-атаки, вирусы, черви, перехватчики, фишинг, вишинг, сниффер, логические бомбы, трояны, спам, ботнеты
Кибертерроризм	Террористические группы, отдельные лица	Политические или социальные изменения, пропаганда экстремистского поведения, вербовка	Государственные информационные программы и системы, интернет, электронная почта	DoS-атаки, вирусы, черви, перехватчики, фишинг, бомбы, трояны, удалённое управление, дезинформация
Распространение секретной информации	Инсайдеры	Собственные мотивы и убеждения, принуждение, вербовка	Государственные, корпоративные и частные информационные сети, эл. почта	Сбор секретной информации, которой имеется доступ

Решение этой проблемы очень важно, поскольку в условиях ЦЭ данные и информационные системы являются важнейшими ресурсами. Нарушения в их защите могут привести к массовым сбоям в работе предприятий и государственных структур, снизить доверие к цифровым технологиям, замедлить инновационное развитие и, в конечном итоге, нанести значительный экономический ущерб [7]. Поэтому создание надежных и устойчивых систем защиты данных и управление киберрисками являются важнейшими условиями успешного функционирования и дальнейшего роста цифровой экономики.

Рис. 2. Классификация угроз

Таблица 2

Мероприятия для решения проблемы ИБ в развитии ЦЭ

№	Мероприятия	Состав решения
1	Создание динамичной системы оценки рисков	Регулярная оценка рисков с учетом меняющихся условий и угроз позволит заранее выявлять уязвимости, оптимально распределять ресурсы и своевременно внедрять новые защитные механизмы, повышая устойчивость к кибератакам
2	Внедрение многоуровневой системы защиты данных	Разделение системы защиты на несколько слоев, включая шифрование, доступ по ролям и контроль трафика, позволит минимизировать риски при взломе одной из систем и сохранить целостность данных на других уровнях
3	Использование технологий искусственного интеллекта (AI) для проактивного мониторинга и анализа угроз	Машинное обучение и AI-алгоритмы способны анализировать огромные объемы данных и выявлять аномалии в реальном времени, что позволяет оперативно реагировать на потенциальные угрозы и предотвращать атаки до их реализации
4	Разработка и внедрение строгих политик и регламентов безопасности	Установление четких стандартов для всех сотрудников, включая правила использования устройств, хранения данных и регулярное обновление программного обеспечения, поможет сократить человеческий фактор как одну из основных причин утечек и инцидентов
5	Инвестиции в обучение сотрудников и пользователей	Повышение уровня цифровой грамотности всех участников, связанных с обработкой данных, и обучение реагированию на подозрительные активности помогут минимизировать риски фишинговых атак и других видов мошенничества, направленных на человеческий фактор

Классификация угроз информационной безопасности представлена на рисунке 2.

Обеспечение ИБ в условиях ЦЭ должно быть комплексным, охватывая все уровни и процессы, связанные с обработкой и передачей данных [8]. Для этого необходимо внедрять передовые технологии и инструменты, такие как системы многофакторной аутентификации, шифрование данных, аналитика на основе искусственного интеллекта для предсказания и предотвращения угроз, блокчейн для защиты от манипуляций с данными, а также технологии мониторинга и управления сетевой безопасностью в режиме реального времени. Эти решения позволяют не только повысить устойчивость к атакам, но и существенно сократить вероятность утечек и манипуляций с данными, обеспечивая непрерывность бизнес-процессов и доверие пользователей к цифровым платформам.

Для обеспечения эффективной системы информационной безопасности в условиях цифровой экономики необходимо применять комплексный подход. Он должен включать как технические меры защиты данных и инфраструктуры, так и управленческие и правовые аспекты, такие как регулярные аудиты, мониторинг угроз, управление рисками и обучение сотрудников. Интеграция этих элементов помогает не только предотвратить возможные киберугрозы, но и оперативно реагировать на инциденты, обеспечивая устойчивость и надежность цифровой экосистемы. Для создания комплексной системы информационной безопасности в цифровой экономике автором рекомендуются следующие мероприятия, представленные в таблице 2.

Так, из таблицы 2, динамическая система оценки рисков позволяет оперативно адаптироваться к изменяющимся условиям, что повышает устойчивость к новым формам кибератак. В условиях цифровой экономики, где данные являются основным активом, постоянный мониторинг рисков помогает банкам и другим организациям оптимально распределять ресурсы и заранее внедрять соответствующие меры защиты.

Многоуровневая система защиты данных, благодаря делению на слои с различными уровнями доступа и контроля, делает систему более устойчивой к угрозам. Например, даже при нарушении одного уровня другие остаются защищенными, что минимизирует риск утечки и утраты данных. Это особенно актуально для сложных цифровых экосистем, где большое количество пользователей и систем требуют разноплановой защиты.

Использование технологий AI в мониторинге угроз позволяет анализировать огромные объемы данных в реальном времени и эффективно выявлять аномалии, указывающие на возможные угрозы. AI и машинное обучение способны не только анализировать исторические данные, но и предсказывать возможные сценарии атак, что помогает организациям оставаться на шаг впереди злоумышленников.

Разработка строгих политик безопасности способствует повышению дисциплины среди сотрудников и снижает вероятность инцидентов, связанных с человеческим фактором. Применение четких регламентов обеспечивает соблюдение стандартов на всех уровнях работы с данными, что способствует устойчивости к внутренним угрозам и снижает вероятность утечек из-за ошибок персонала.

Инвестиции в обучение сотрудников также становятся важной составляющей, так как высокий уровень цифровой грамотности помогает не только повысить качество киберзащиты, но и предотвратить инциденты. Обученные сотрудники умеют реагировать на подозрительные активности и предотвращать фишинговые и иные атаки, ориентированные на человеческий фактор, что снижает общий риск для организации.

Данные мероприятия являются основой для создания всесторонней и динамичной системы защиты, которая учитывает разнообразие современных угроз и требования цифровой экономики. Внедрение таких мер позволяет банкам, государственным структурам и предприятиям обеспечить высокий уровень защиты данных и цифровых активов, необходимый для стабильного функционирования и роста. Представленные авто-

ром меры помогут создать устойчивую систему защиты, которая адаптируется к изменяющимся угрозам и позволяет уверенно развиваться цифровой экономике, обеспечивая надежность, непрерывность и высокую степень доверия к цифровым сервисам и инфраструктуре.

Выводы

В ходе анализа текущего состояния и проблем информационной безопасности в цифровой экономике стало очевидно, что, несмотря на значительные преимущества цифровых технологий, их развитие сопровождается серьезными вызовами, особенно в области защиты данных и устойчивости инфраструктуры. Обеспечение информационной безопасности цифровой экономики требует комплексного подхода, охватывающего не только технологические аспекты, но и нормативные, организационные и образовательные меры. Важность внедрения многоуровневых систем защиты и новых технологий, таких как искусственный интеллект и блокчейн, подтверждена возрастающей сложностью киберугроз и критической необходимостью поддержания доверия к цифровым сервисам. Рассмотренные меры и рекомендации создают основу для построения устойчивой и эффективной системы информационной безопасности, способной адаптироваться к меняющимся угрозам и обеспечивать стабильное развитие цифровой экономики. Так, в результате исследования подведены итоги и получены следующие выводы:

1. В рамках первого этапа рассмотрены ключевые характеристики цифровой экономики, ее структура и актуальность в современном мире. Цифровая экономика включает в себя цифровую инфраструктуру, платформенные технологии и цифровые сервисы, которые вместе обеспечивают взаимосвязь между бизнесом, государством и потребителями. Определение ключевых компонентов и значимости цифровой экономики в России на 2024 год показало, что ее развитие обусловлено необходимостью повышать конкурентоспособность и модернизировать различные сектора экономики.

2. Во втором этапе проанализированы проблемы информационной безопасности в цифровой экономике. Стало ясно, что наибольшую угрозу представляют кибератаки, утечки данных и шпионские атаки, которые могут причинить ущерб как бизнесу, так и государственным структурам. Понимание рисков и их последствий, таких как экономические потери и снижение доверия, подчеркивает, что информационная безопасность – это неотъемлемая составляющая эффективного функционирования цифровой экономики.

3. На третьем этапе была выработана стратегия комплексного подхода к информационной безопасности, которая охватывает все аспекты защиты данных и процессов. Рассмотрены технологии и инструменты, такие как многофакторная аутентификация, шифрование, мониторинг на основе AI, блокчейн и сетевой мониторинг, которые обеспечивают высокую устойчивость к угрозам. Также были предложены конкретные авторские рекомендации по созданию надежной системы защиты, включая динамическую оценку рисков, многоуровневую защиту, проактивный мониторинг, запуск Гособлака – единой государственной облачной платформы [9], разработку политик безопасности и обучение сотрудников. Эти меры в совокупности создают прочную основу для устойчивого развития цифровой экономики и повышения уровня безопасности данных и инфраструктуры.

Библиографический список

1. Сыщикова Е.Н., Макарова Е.Е., Муратова М.Н. Обоснование необходимости внедрения непрерывного процесса обеспечения информационной безопасности на предприятиях // Наука Красноярья. 2024. Т. 13. № 1. С. 7-21.

2. Эриашвили Н.Д. Проблемы информационной безопасности в условиях цифровой экономики // Аудиторские ведомости. 2021. № 4. С. 168-172.

3. Барейко С.Н., Кожухина К.А. Экономическая и информационная безопасность России в условиях цифровой экономики // НК. 2019. №5. С. 7-18.

4. Бушуев А.Л., Деревцова И.В., Мальцева Ю.А., Терентьева В.Д. Роль информационной безопасности в условиях цифровой экономики // Baikal Research Journal. 2020. № 1. С. 6-10.

5. Даурова Н. З., Тлехурай-Берзегова Л. Т., Бюллер Е. А., Хотова И. Р. Цифровая экономика в РФ, проблемы и пути их решения // The Scientific Heritage. 2020. № 52-3. С. 26-29.

6. Щербакова Н.В. Проблемы информационной безопасности общества в условиях становления цифровой экономики // Вестник НГУЭУ. 2021. № 1. С. 245-253.

7. Кайгородцев А.А., Кайгородцева Т.Ф. Проблемы обеспечения информационной безопасности России в условиях цифровизации // Society and Security Insights. 2020. № 3. С. 79-89.

8. Любавина Т.В., Мустафина Г.Г., Любавин А.Ю., Чугунова А.А. Цифровая экономика: проблемы и перспективы // ВЭПС. 2022. № 4. С. 143-146.

9. Муратова М.Н. Проблемы экономической безопасности цифрового общества в условиях санкционной политики запада // Инновации. Наука. Образование. 2024. № 104. С. 20-28.