Библиографический список

1. О полиции: Федер. закон от 07.02.2011 № 3-ФЗ (последняя редакция) // Доступ из справ.-правовой системы «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 30.09.2025).

2. О федеральной службе безопасности: Федер. закон от 03.04.1995 № 40-ФЗ (последняя редакция) // Доступ из справ.-правовой системы «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_6300/ (дата обращения: 30.09.2025).

3. Большой толковый словарь русского языка / сост. и гл. ред. С.А. Кузнецов. СПб.: Норинт, 2000. 1536 с.

4. Иванов С.И. Отдельные проблемы реформирования оперативно-розыскного законодательства на современном этапе // Развитие государственности и права в Республике Крым: реалии и перспективы: материалы Всерос. науч.-практ. конф., 5 февраля 2016 года / под общ. ред. С.А. Буткевича. Краснодар: Краснодарский университет МВД России, 2016. С. 298–299.

5. Пестрецов М.А. Противодействие преступным посягательствам на жилье граждан (на примере Республики Крым): монография. Краснодар: Краснодарский университет МВД России, 2017. С. 94–95.

УДК 338.27
ББК 16.8

Пономарёва Г.В. – ст. препод. кафедры
социологии и социальных технологий ТвГТУ
Стукалова Н.А. – доцент кафедры
информатики и прикладной математики ТвГТУ
Гусаров А.А. – ст. препод. кафедры
информатики и прикладной математики ТвГТУ
Семилетова Л.В. – ст. препод. кафедры
информатики и прикладной математики ТвГТУ

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ И КИБЕРБЕЗОПАСНОСТЬ

Аннотация. В современном мире цифровая трансформация стала движущей силой экономического прогресса. Россия, стремясь укрепить свои позиции на глобальной арене, активно внедряет цифровые технологии в государственное управление, бизнес и финансы. Однако этот

процесс сопровождается новыми вызовами, особенно в области кибербезопасности и защиты от экономического шпионажа. В статье рассмотрено, как Россия старается найти баланс между возможностями цифровизации и необходимостью защиты своей цифровой экономики.

Ключевые слова: управление, цифровая трансформация, цифровое решение, кибербезопасность, риски, искусственный интеллект, цифровая экономика.

Сегодня цифровые технологии становятся неотъемлемой частью экономической жизни. Они открывают новые горизонты для бизнеса и государственного управления, но вместе с тем приносят серьезные вызовы, связанные с кибербезопасностью. В настоящее время цифровая экономика является не только инструментом повышения эффективности и прозрачности, но и «полем битвы», где разворачивается экономический шпионаж и растет киберпреступность. В настоящей статье будет исследовано, как цифровые технологии преобразуют экономику, какие угрозы они несут и что можно сделать, чтобы защитить экономику государства от нежелательных внешних воздействий.

Цифровая экономика – это система экономических отношений, основанная на использовании передовых технологий. Она меняет подходы к управлению, производству и взаимодействию между участниками рынка. Одним из ярких примеров является государственная интегрированная информационная система «Электронный бюджет», внедренная в России. Эта платформа объединяет финансовые данные в общее информационное пространство, повышая прозрачность бюджетных процессов. Благодаря платформе граждане, ученые и органы власти получают доступ к отчетам, прогнозам и проектам, а управление государственными финансами становится более открытым и результативным [1].

Назовем ключевые преимущества цифровой экономики:

сокращение трудоемкости (автоматизация процессов снижает затраты времени и ресурсов);

повышение эффективности (цифровые платформы ускоряют принятие решений и улучшают их качество);

инвестиционная привлекательность (регионы, внедряющие цифровые технологии, привлекают больше капитала);

рост производительности (цифровизация стимулирует развитие экономики на всех уровнях).

Эти изменения уже заметны: от локальных информационно-технических проектов происходит переход к масштабной трансформации, где цифровые экосистемы становятся основой экономической деятельности.

Цифровая трансформация открывает перед Россией значительные перспективы. Согласно проведенным исследованиям [2], к 2026 году объем цифровой экономики может достичь 9,6 трлн рублей, что составит 8–10 % ВВП и приблизит страну к уровню развитых экономик.

Цифровые технологии оптимизируют бизнес-процессы, улучшают аналитику данных и повышают качество взаимодействия с клиентами. Одним из ключевых примеров является государственная интегрированная информационная система «Электронный бюджет». Переход на облачные технологии позволяет сократить административные расходы и ускорить принятие решений. Такие инициативы демонстрируют, как цифровизация способствует модернизации экономики и повышению инвестиционной привлекательности регионов. Система «Электронный бюджет» позволяет интегрировать данные о расходах и результатах, а также использовать облачные технологии для упрощения доступа и анализа. Кроме того, цифровая трансформация охватывает различные сектора. Например, компании из 27 отраслей активно внедряют цифровые решения, уделяя внимание автоматизации процессов и управлению данными. Это приводит к росту производительности труда и снижению операционных затрат.

Тем не менее есть и другая сторона. Чем глубже цифровые технологии проникают в экономику, тем уязвимее она становится. Экономический шпионаж и киберпреступность превращаются в серьезные угрозы для компаний и государств. Знания и технологии сегодня ценятся выше сырьевых ресурсов, и страны активно используют спецслужбы для их добычи. Методы шпионажа разнообразны: подкуп сотрудников, внедрение агентов, взлом компьютерных систем, прослушивание и наблюдение [3].

Основные аспекты цифровой трансформации, а также их преимущества и риски приведены в таблице.

Сравнение преимуществ и рисков цифровой трансформации

Аспект	Преимущества	Риски
1	*2*	*3*
Экономический рост	Увеличение ВВП до 8–10 % к 2025 году, рост производительности труда	Убытки от кибератак (1,6–1,8 трлн рублей в 2019 году)
Прозрачность процессов	Улучшение управления финансами через системы, такие как «Электронный бюджет»	Уязвимость к краже данных и саботажу

Окончание таблицы

1	*2*	*3*
Технологический прогресс	Оптимизация процессов, внедрение искусственного интеллекта и облачных технологий	Быстрая адаптация киберпреступников к новым технологиям
Международное сотрудничество	Обмен опытом и лучшими практиками в кибербезопасности	Геополитические напряжения, ограничивающие сотрудничество

Экономический шпионаж – это не просто любопытство конкурентов. Это кража коммерческих секретов, патентов и производственных методов, которая может подорвать репутацию компании, привести к финансовым потерям и даже спровоцировать конфликты с государством. Киберпреступники осваивают новые технологии быстрее многих корпораций. Они используют искусственный интеллект, облачные вычисления и автоматизированные атаки, чтобы эксплуатировать уязвимости цифровых систем.

Приведем примеры рисков:

утечка данных (конфиденциальная информация становится добычей хакеров);

атаки на инфраструктуру (киберпреступления могут парализовать критически важные объекты);

мошенничество (цифровые платформы открывают новые возможности для обмана).

С ростом мобильных технологий и интернета вещей указанные угрозы только усиливаются, а границы между государственной разведкой и частными атаками становятся все более размытыми.

На уровне предприятий эффективная система безопасности включает создание защитных механизмов и управление ими. Это требует не только инвестиций в технологии, но и постоянного контроля за их работой. При этом государства должны развивать экономическую контрразведку, чтобы пресекать шпионаж на ранних стадиях.

Названные системы становятся привлекательной мишенью для киберпреступников. Потенциальные угрозы включают несанкционированный доступ к финансовым данным, саботаж бюджетных процессов или кражу конфиденциальной информации. Конкретные инциденты, связанные с платформой «Электронный бюджет», публично не зафиксированы, однако общий рост кибератак подчеркивает необходимость усиления защиты подобных платформ.

Экономический шпионаж, включающий кражу конфиденциальной информации, технологий и производственных методов, стал одной из главных угроз в международной экономике.

Недавние инциденты свидетельствуют о серьезности проблемы. В январе 2025 года хакеры провели фишинговые атаки на дипломатические организации Казахстана и правительственные сайты Италии. Эти атаки показывают, как киберпространство используется для достижения геополитических и экономических целей [4].

Рост киберпреступности также связан с быстрым развитием технологий, таких как искусственный интеллект и облачные вычисления. По данным аналитиков, в 2019 году убытки российской экономики от кибератак составили 1,6–1,8 трлн рублей, и сейчас эта цифра, вероятно, выросла [5].

Для защиты цифровой экономики Россия разрабатывает комплексные стратегии кибербезопасности. Они включают:

оценку угроз (регулярный анализ потенциальных рисков и уязвимостей);

превентивные меры (внедрение современных технологий защиты, таких как шифрование и системы обнаружения вторжений);

мониторинг и обновление (постоянное наблюдение за киберпространством и обновление систем безопасности);

обучение специалистов (подготовка кадров в области кибербезопасности для противодействия новым угрозам);

экономическую контрразведку (выявление и предотвращение попыток экономического шпионажа на государственном и корпоративном уровнях).

На государственном уровне Россия усиливает киберзащиту критической инфраструктуры. Например, назначение ответственных за цифровую трансформацию в федеральных и региональных органах власти способствует координации усилий в области цифровизации и безопасности.

Международное сотрудничество также играет важную роль. Обмен опытом и лучшими практиками может помочь странам эффективнее противостоять глобальным киберугрозам, однако геополитические напряжения усложняют данный процесс.

Для успешного развития цифровой экономики Россия должна продолжать инвестировать в кибербезопасность, развивать отечественные технологии и готовить квалифицированных специалистов. Международное сотрудничество, несмотря на сложности, может способствовать созданию более безопасного цифрового пространства. Только сбалансированный подход, сочетающий инновации и защиту, позволит нашей стране реализовать потенциал цифровой трансформации, минимизируя риски.

Цифровая экономика – это двигатель прогресса и вместе с тем зона риска. Она обещает рост производительности и прозрачность управления, но без должной защиты может стать мишенью для киберпреступников и шпионов. Успех в данной новой реальности зависит от способности компаний и государств управлять рисками. Инвестиции в кибербезопасность, развитие технологий и международное сотрудничество – это ключевые шаги, которые помогут превратить цифровую экономику в инструмент процветания, а не в источник уязвимостей.

Библиографический список

1. Министерство финансов Российской Федерации. URL: https://www.minfin.ru/ru/ perfomance/ebudget/ (дата обращения: 25.12.2025).

2. European Commission, Secretariat-General. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. URL: https://ec.europa. eu/digital-singlemarket/en/news/digital-single-marketstrategy-europe-com2015-192-final (дата обращения: 20.01.2025).

3. Международное бюджетное партнерство. URL: https://www. internationalbudget.org/openbudget-survey/ (дата обращения: 28.12.2025).

4. Новости цифровой трансформации, телекоммуникаций, вещания и ИТ. URL: http:// www.comnews.ru/ (дата обращения: 15.01.2025).

5. Зейтениди Н.Ю. «Цифровой регион» как платформа. URL: http://bujet.ru/article/394225.php (дата обращения: 05.01.2025).