

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВИЗАЦИИ: НОВЫЕ УГРОЗЫ И ВЫЗОВЫ

Я. Ю. Болдырева¹⁾, Ю. В. Веселова²⁾

¹⁾ студент, Приволжский Государственный Университет Путей Сообщения, г. Самара, Россия,
boldyreva.y.y@gymn1sam.ru

²⁾ кандидат экономических наук, доцент, Приволжский Государственный Университет Путей
Сообщения, г. Самара, Россия, *veselova-uv@yandex.ru*

Научный руководитель Ю. В. Веселова

*кандидат экономических наук, доцент, Приволжский Государственный Университет Путей
Сообщения, г. Самара, Россия, veselova-uv@yandex.ru*

В статье проводится комплексный анализ трансформации системы экономической безопасности под влиянием процессов цифровизации. Исследуется парадоксальная природа современных цифровых технологий, которые, с одной стороны, выступают драйвером экономического роста, а с другой – создают системные уязвимости в национальной экономике. Методологической основой исследования выступают системный подход и сравнительный анализ. Научная новизна работы заключается в разработке комплексной классификации угроз экономической безопасности, возникающих на разных уровнях цифровой трансформации. Практическая значимость исследования состоит в формулировании конкретных рекомендаций по адаптации механизмов обеспечения экономической безопасности к вызовам цифровой эпохи. Особое внимание уделяется анализу взаимосвязи технологических рисков и социально-экономических последствий цифровизации.

Ключевые слова: экономическая безопасность; цифровая трансформация; киберугрозы; технологический суверенитет; цифровое неравенство; финансовая стабильность; нормативное регулирование.

ECONOMIC SECURITY IN THE ERA OF DIGITALIZATION: NEW THREATS AND CHALLENGES

Ya. Yu. Boldyreva¹⁾, Yu. V. Veselova²⁾

¹⁾ student, Volga Region State University of Railway Transport, Samara, Russia,
boldyreva.y.y@gymn1sam.ru

²⁾ PhD in economics, associate professor, Volga Region State University of Railway Transport, Samara,
Russia, *veselova-uv@yandex.ru*

Supervisor Yu. V. Veselova

*PhD in economics, associate professor, Volga Region State University of Railway Transport, Samara,
Russia, veselova-uv@yandex.ru*

The article provides a comprehensive analysis of the transformation of the economic security system under the influence of digitalization processes. It explores the paradoxical nature of modern digital technologies, which, on the one hand, act as drivers of economic growth, and on the other, create systemic vulnerabilities in the national economy. The methodological basis of the research is a systematic approach and comparative analysis. The scientific novelty of the work lies in the development of a comprehensive classification of threats to economic security arising at different levels of digital transformation. The practical significance of the study consists in formulating specific recommendations for adapting economic security

mechanisms to the challenges of the digital era. Special attention is paid to the analysis of the relationship between technological risks and the socio-economic consequences of digitalization.

Keywords: economic security; digital transformation; cyber threats; technological sovereignty; digital inequality; financial stability; regulatory framework.

Современный этап развития мировой экономики характеризуется глубокой цифровой трансформацией, затрагивающей фундаментальные основы хозяйственной деятельности. Процессы цифровизации, охватывающие производство, распределение, обмен и потребление, создают новую парадигму экономических отношений. Однако наряду с очевидными преимуществами – ростом производительности, оптимизацией бизнес-процессов, созданием инновационных рынков – цифровизация порождает комплекс новых вызовов для национальной экономической безопасности [1, с. 45].

Актуальность темы исследования обусловлена нарастающей противоречивостью воздействия цифровых технологий на экономическую систему. С одной стороны, они выступают катализатором экономического роста, с другой – создают ранее не существовавшие уязвимости. Традиционные механизмы обеспечения экономической безопасности, сформированные в индустриальную эпоху, оказываются недостаточно эффективными для противодействия угрозам цифровой эпохи. Это требует переосмысления подходов к защите национальных экономических интересов.

Целью данного исследования является выявление и системный анализ новых угроз экономической безопасности, возникающих в процессе цифровой трансформации, а также разработка классификации соответствующих вызовов для государства и бизнеса. Для достижения поставленной цели решаются следующие задачи:

- 1) анализ влияния цифровизации на ключевые компоненты экономической безопасности;
- 2) выявление и классификация новых типов угроз экономической безопасности;
- 3) определение системных вызовов для механизмов обеспечения экономической безопасности;
- 4) разработка рекомендаций по адаптации системы экономической безопасности к условиям цифровой трансформации.

Методологической основой исследования выступают принципы системного анализа, методы сравнительного и структурно-функционального анализа, а также статистические методы оценки экономических рисков.

Новые угрозы экономической безопасности в условиях цифровизации

Цифровая трансформация экономики приводит к возникновению качественно новых рисков, которые можно классифицировать по нескольким уровням воздействия.

Киберпреступность как угроза финансовой стабильности.

На макроэкономическом уровне наиболее значимой угрозой выступает киберпреступность, которая эволюционировала от единичных противоправных действий к сложным организованным формам. Современные кибератаки характеризуются высокой степенью автоматизации, использованием искусственного интеллекта и нацеленностью на критическую инфраструктуру. Финансовый сектор становится главной мишенью для киберпреступников – по данным Банка России, только за 2023 год было зафиксировано свыше 120 тысяч успешных атак на кредитные организации [2, с. 112]. Особую опасность представляют атаки на системы межбанковских расчетов, которые могут вызвать цепную реакцию и парализовать работу всей финансовой системы.

Технологическая зависимость и риски цифрового суверенитета. На мезоуровне (отраслевом) ключевой угрозой является технологическая зависимость от иностранных решений в области программного обеспечения и аппаратного обеспечения. Высокая концентрация рынка ИТ-услуг вокруг нескольких международных корпораций создает риски экономического шан-

тажа и скрытого наблюдения. По оценкам экспертов, доля иностранного программного обеспечения в отдельных сегментах российской экономики превышает 80 %, что создает критическую уязвимость [3, с. 28]. Санкционное давление последних лет продемонстрировало реальность угрозы отключения от зарубежных цифровых платформ и сервисов.

Цифровое неравенство и структурные дисбалансы. На микроуровне (региональном и корпоративном) проявляется угроза цифрового неравенства. Интенсивное внедрение цифровых технологий углубляет разрыв между:

- крупными корпорациями и малым бизнесом;
- столичными регионами и периферией;
- разными возрастными и социальными группами населения.

Это приводит к структурным дисбалансам в экономике, усиливает региональную асимметрию и создает предпосылки для социальной напряженности. Автоматизация бизнес-процессов вызывает трансформацию рынка труда – по оценкам Всемирного банка, до 30 % рабочих мест в традиционных секторах могут быть автоматизированы в течение следующего десятилетия [4, с. 91].

На рисунке представлена классификация новых угроз экономической безопасности.

Уровень воздействия	Основные виды угроз	Потенциальные последствия	Субъекты воздействия
Макроуровень (национальная экономика)	Киберпреступность; Таргетированные атаки на КИИ; Финансовые мошенничества с использованием ИИ	Дестабилизация финансовой системы; Нарушение работы критической инфраструктуры; Снижение инвестиционной привлекательности	Государственные органы; Центральный банк; Кредитные организации
Мезоуровень (отраслевая экономика)	Технологическая зависимость; Риски цепочек поставок; Утечка данных и ноу-хау	Потеря технологического суверенитета; Снижение конкурентоспособности отраслей; Накопление технологического долга	Крупные корпорации; Отраслевые министерства; Научно-исследовательские институты
Микроуровень (регионы и компании)	Цифровое неравенство; Автоматизация рабочих мест; Неподготовленность кадров	Рост региональной асимметрии; Структурная безработица; Снижение производительности труда	Малый и средний бизнес; Региональные органы власти; Образовательные учреждения

Систематизация угроз экономической безопасности по уровням воздействия.

Составлено по: [1, с. 46–48; 3, с. 25–30]

Как показывает рисунок, угрозы экономической безопасности в условиях цифровизации носят системный характер и требуют дифференцированного подхода к их нейтрализации на каждом уровне экономической системы.

Системные вызовы для обеспечения экономической безопасности. Противодействие новым угрозам требует преодоления системных вызовов, которые носят междисциплинарный характер.

Нормативно-правовой вызов: «догоняющее» регулирование. Главной проблемой правового обеспечения экономической безопасности является асинхронность развития технологий и законодательства. Цикл разработки и принятия нормативных актов составляет 1–3 года, тогда как технологии кардинально меняются за 6–12 месяцев. Это создает правовые вакуумы в регулировании таких областей, как:

- обработка больших данных (Big Data);
- использование искусственного интеллекта;
- оборот криптоактивов и цифровых валют;
- регулирование платформенной экономики [1, с. 48].

Отсутствие четких правовых рамок затрудняет привлечение к ответственности за новые формы правонарушений и создает правовую неопределенность для бизнеса.

Кадровый и образовательный вызов: дефицит компетенций. Обеспечение экономической безопасности в цифровую эпоху требует принципиально новых профессиональных компетенций. Система образования сталкивается с необходимостью одновременного решения нескольких задач:

- подготовка специалистов в области кибербезопасности (дефицит оценивается в 1,5–2 млн человек в РФ);
- обучение специалистов по работе с большими данными и искусственным интеллектом;
- развитие цифровой грамотности населения как основы противодействия социальной инженерии [3, с. 31].

Существующие образовательные программы зачастую не успевают адаптироваться к быстро меняющимся требованиям цифровой экономики.

Технологический вызов: необходимость опережающего развития. Ключевым условием обеспечения технологического суверенитета является развитие собственной исследовательской и производственной базы. Технологический вызов включает несколько аспектов:

- разработка отечественного программного обеспечения для критической информационной инфраструктуры;
- создание собственных стандартов информационной безопасности;
- развитие производства элементной базы для телекоммуникационного оборудования;
- инвестиции в фундаментальные исследования в области квантовых вычислений и искусственного интеллекта [4, с. 105].

Решение этих задач требует координации усилий государства, бизнеса и научного сообщества.

Проведенное исследование позволяет сделать вывод о многомерном характере угроз экономической безопасности в условиях цифровой трансформации. Выявлено, что цифровизация создает взаимосвязанную систему рисков на макро-, мезо- и микроуровнях экономики. К наиболее значимым угрозам относятся: киберпреступность (макроуровень), технологическая зависимость (мезоуровень) и цифровое неравенство (микроуровень).

Установлено, что эффективное противодействие этим угрозам требует преодоления системных вызовов, главными из которых являются:

- 1) нормативно-правовой вызов – необходимость создания адаптивной системы регулирования цифровой экономики;
- 2) кадровый вызов – преодоление дефицита специалистов в области цифровой безопасности;
- 3) технологический вызов – обеспечение технологического суверенитета через развитие отечественных разработок.

Перспективными направлениями дальнейших исследований могут стать:

- разработка методики оценки уровня цифровых рисков для различных отраслей экономики;
- анализ эффективности мер государственной поддержки импортозамещения в IT-сфере;

- исследование влияния искусственного интеллекта на рынок труда и социальную стабильность;
- разработка моделей публично-частного партнерства в области кибербезопасности.

Библиографические ссылки

1. *Лебедев А. С.* Цифровая экономика: новые угрозы и вызовы для экономической безопасности России // Экономика и бизнес: теория и практика. 2022. № 5-2. С. 45–50.
2. *Трусова Н. С., Вертакова Ю. В.* Проблемы экономической безопасности цифрового общества и пути их решения // Безопасность бизнеса. 2021. № 3. С. 110–115.
3. *Ферова И. С., Козлова С. А., Осадченко Е. А., Подтакова Н. Н.* Экономическая безопасность в эпоху цифровизации: вызовы, риски и стратегии устойчивого развития : монография. М. : SCIENCE, 2023. 180 с.
4. *Стрелина Е. Н., Ходун Э. В.* Проблемы обеспечения экономической безопасности в условиях цифровой трансформации в разных отраслях экономики // Экономические науки. 2022. № 12(217). С. 88–107.
5. *Веселова Ю. В., Тимчук О. Г., Литвинцева К. С.* Виды мошенничества и методы противодействия: Классификация и защита // Вестник СамГУПС. 2025. № 2(68). С. 62–69.