

ГЛОБАЛЬНАЯ ЭКОНОМИКА

Научная статья

УДК 338.1; 339.9

doi: 10.33917/mic-5.124.2025.5–12

Цифровая безопасность международной экономической системы в условиях кризисов

Фадеева Инна Авенировна

кандидат экономических наук, профессор, Дипломатическая академия Министерства иностранных дел Российской Федерации, Москва, Россия, innaf576@mail.ru,

ru, SPIN-код: 3807–7577, <https://orcid.org/0000-0001-5480-8732>

Аннотация. В современных условиях глобализации и цифровизации мировой экономики вопросы обеспечения цифровой безопасности приобретают особую актуальность. Цифровая трансформация экономических отношений, сопровождающаяся активным внедрением информационных технологий, создает новые вызовы для международной экономической системы, особенно в периоды кризисных явлений. Цель исследования состоит в разработке теоретических и методологических основ обеспечения цифровой безопасности международной экономической системы в условиях кризисных явлений. Цифровая безопасность представляет собой комплексную систему мер, направленных на защиту информационных активов и обеспечение устойчивого функционирования экономической системы в условиях цифровизации. В контексте международной экономики она включает защиту критически важной инфраструктуры, обеспечение конфиденциальности и целостности данных, предотвращение кибератак и несанкционированного доступа, а также защиту платежных систем и финансовых транзакций. Кризисные явления существенно влияют на уровень цифровой безопасности, что подтверждается усилением кибератак на удаленных работников, росте случаев мошенничества с государственными выплатами, нарушением работы критически важных систем и ростом уязвимости платежных систем. Кризисные явления создают новые вызовы для системы цифровой безопасности, требующие оперативного реагирования и адаптации существующих механизмов защиты. При этом, международное сотрудничество является ключевым фактором в обеспечении цифровой безопасности, особенно в условиях глобализации экономических отношений.

Ключевые слова: цифровая безопасность, кризис, международная экономика, цифровая трансформация, кибербезопасность

Для цитирования: Фадеева И.А. Цифровая безопасность международной экономической системы в условиях кризисов. Микроэкономика. 2025. №5. С. 5–12. DOI: <https://doi.org/10.33917/mic-5.124.2025.5–12>

GLOBAL ECONOMY

Original article

DIGITAL SECURITY OF THE INTERNATIONAL ECONOMIC SYSTEM IN THE CONTEXT OF CRISES

Inna A. Fadeeva

Candidate of Sciences (Economics), Professor, Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, Moscow, Russia, innaf576@mail.ru

Abstract. In modern conditions of globalization and digitalization of the world economy, the issues of ensuring digital security are becoming particularly relevant. The digital transformation of economic relations, accompanied by the active introduction of information technology, creates new challenges for the international economic system, especially during periods of crisis. The purpose of the research is to develop the theoretical and methodological foundations for ensuring the digital security of the international economic system in the context of crisis phenomena. Digital security is a comprehensive system of measures aimed at protecting information assets and ensuring the sustainable functioning of the economic system in the context of digitalization. In the context of the international economy, it includes protecting critical infrastructure, ensuring confidentiality and data integrity, preventing cyber-attacks and unauthorized access, as well as protecting payment systems and financial transactions. The crisis phenomena significantly affect the level of digital security, which is confirmed by increased cyber-attacks on remote workers, an increase in cases of fraud with government payments, disruption of critical systems and an increase in the vulnerability of payment systems. The crisis phenomena create new challenges for the digital security system, requiring rapid response and adaptation of existing protection mechanisms. At the same time, international cooperation is a key factor in ensuring digital security, especially in the context of globalized economic relations.

Keywords: digital security, crisis, international economy, digital transformation, cybersecurity

For citation: Fadeeva I.A. Digital security of the international economic system in the context of crises. Microeconomics. 2025;5:5–12 (In Russ.). DOI: <https://doi.org/10.33917/mic-5.124.2025.5-12>

Введение

В результате динамичного развития международных экономических отношений в новом тысячелетии под влиянием научно-технического прогресса и углубления международной конкуренции между участниками внешнеэкономической деятельности произошли значительные изменения в формах международных экономических отношений [1].

В современных условиях глобализации и цифровизации мировой экономики вопросы обеспечения цифровой безопасности приобретают особую актуальность [2]. Цифровая транс-

формация экономических отношений, сопровождающаяся активным внедрением информационных технологий, создает новые вызовы для международной экономической системы, особенно в периоды кризисных явлений [3].

Актуальность исследования обусловлена тем, что современные экономические кризисы приобретают качественно новый характер, проявляясь не только в традиционных формах, но и в цифровой сфере. Кибербезопасность становится критически важным фактором устойчивого развития международной экономики, требующим комплексного подхо-

да к защите экономических интересов государств и бизнеса.

Проблема исследования заключается в необходимости разработки эффективных механизмов обеспечения цифровой безопасности международной экономической системы в условиях возрастающих угроз и нестабильности. Особую значимость приобретает вопрос о том, как обеспечить защиту экономических интересов государств и бизнеса в условиях цифровизации при сохранении открытости и эффективности международных экономических отношений.

Цель исследования состоит в разработке теоретических и методологических основ обеспечения цифровой безопасности международной экономической системы в условиях кризисных явлений.

Для достижения поставленной цели необходимо решить следующие задачи:

- проанализировать основы цифровой безопасности в международной экономике;
- выявить основные угрозы цифровой безопасности в условиях экономических кризисов;
- исследовать существующие механизмы обеспечения кибербезопасности на международном уровне;
- разработать рекомендации по совершенствованию системы цифровой безопасности.

Теоретическая значимость работы заключается в развитии концепции цифровой безопасности международной экономической системы, уточнении терминологического аппарата

и систематизации существующих подходов к обеспечению кибербезопасности.

Практическая значимость исследования состоит в возможности использования полученных результатов для совершенствования национальной и международной политики в области обеспечения цифровой безопасности, разработки конкретных мер по защите экономических интересов в условиях кризисных явлений.

Теоретические основы цифровой безопасности в международной экономике

Одной из особенностей нынешнего этапа развития мировой экономики является то, что различные формы институциональной организации экономики развиваются в глобальном измерении [4]. В таких условиях усиливается технологическая взаимозависимость, объединяются рынки и создаются предпосылки для динамичного роста торговли и движения капитала между разными странами (*табл. 1*).

Таким образом, современный этап развития мировой экономики характеризуется тем, что, с одной стороны, геоэкономическая фрагментация сохраняется, и, с другой стороны, на повестку дня поставлены новые задачи по стабилизации состояния окружающей среды и обеспечения энергетической безопасности. Эти процессы имеют глобальный масштаб и сформировались в рамках противостояния

Таблица 1. Аспекты глобальных преобразований в функционировании экономики

Обострение геополитических противоречий и рисков	Рост уровня напряженности в мире
	Необходимость увеличения расходов на безопасность и оборону
Углубление дисбалансов на мировых рынках капитала	Повышение уровня фрагментации мировой экономики
	Повышение вероятности глобальных финансовых и экономических кризисов
	Увеличение разрыва между финансовым и реальным секторами экономики
Увеличение международной миграции	Расширение масштабов виртуальной трудовой миграции
	Снижение уровня барьеров для международной миграции

Таблица 1. Аспекты глобальных преобразований в функционировании экономики (окончание)

Углубление уровня неопределенности в реализации потребительского выбора	Изменение предпочтений и приоритетов потребителей
	Расширение возможностей потребительского выбора
	Рост объемов международной электронной торговли
Углубление цифровой трансформации	Необходимость минимизации негативных последствий цифровизации
Необходимость укрепления институционального потенциала государственных органов	Усиление координации между правительствами и центральными банками
	Сбалансированное взаимодействие между правительствами и антимонопольными органами

Источник: составлено автором.

механизмов, которые предлагаются, с одной стороны, рынком, а с другой, государством, конкурируя за доминирующее положение [5].

Цифровая экономика включает в себя различные институты, которые играют ключевую роль в содействии развития и функционирования цифрового общества и бизнеса, обеспечения инфраструктуры, нормативно-правовой базы, технологических решений и других необходимых элементов для устойчивого роста в цифровом обществе. Институты цифровой экономики включают: инновационные лаборатории и исследовательские центры; активные технологические компании и стартапы; криптовалютные биржи; цифровые агентства и консалтинговые компании; учебные заведения и обучающие платформы; государственные органы, правительственные организации и регулирующие органы; банки, цифровые кассы и финансовые учреждения, работающие в области финансовых технологий; цифровые сети; цифровые платформы, как онлайн-платформы для хранения и обмена различными ценностями [6].

Цифровая безопасность представляет собой комплексную систему мер, направленных на защиту информационных активов и обеспечение устойчивого функционирования экономической системы в условиях цифровизации. В контексте международной экономики она включает защиту критически важной инфраструктуры, обеспечение конфиденциальности и целостности данных, предотвращение кибе-

ратак и несанкционированного доступа, а также защиту платежных систем и финансовых транзакций [7].

В условиях современных экономических кризисов выделяются такие угрозы как кибератаки на финансовые институты, связанные с фишинговыми атаками, мошенничество с платежными системами и кражи конфиденциальных данных. Угрозу информационной инфраструктуре представляют DDoS-атаки (рост в 2024 г. на 120% по сравнению с 2023 г.), вредоносное ПО (рост в 2024 г. на 95% по сравнению с 2023 г.) и нарушение работы критически важных систем [8]. Экономические угрозы состоят в манипуляции с финансовыми рынками, дискриминационных практиках в цифровой торговле, нарушении цепочек поставок. Анализ влияния кризисных явлений на цифровую безопасность в виде экономического ущерба от кибератак приведен в табл. 2.

Таблица 2. Экономический ущерб от кибератак [9]

Сектор экономики	Доля от общего ущерба, %	Среднее количество атак в год
Финансовый сектор	45	12000
Энергетика	25	8500
Здравоохранение	15	6200
Производство	15	7800

Влияние кризисных явлений на цифровую безопасность связано также с тем, что финансовые кризисы приводят к усилению киберпреступности, нарушению работы платежных систем, снижению эффективности систем кибербезопасности, а также к региональным кризисным явлениям.

Угрозы цифровой безопасности в условиях экономических кризисов

Современные санкционные режимы создают новые вызовы международной экономической системе, включающие разрыв технологических цепочек, ограничение доступа к защитному ПО, уязвимость критической инфраструктуры, изменение механизмов обеспечения цифровой безопасности международных институтов.

При этом, для нивелирования негативных последствий кризисных явлений принятые следующие глобальные инициативы: Будапештская конвенция о киберпреступности, программы кибербезопасности ООН и международные стандарты ISO/IEC. В качестве региональных механизмов защиты от кризисных явлений выделяются программы Digital Europe Programme в Европейском Союзе, ASEAN Cybersecurity Cooperation в странах АСЕАН, а также механизмы сотрудничества в сфере кибербезопасности стран ШОС [10].

Анализ данных программ показал, что ключевые направления цифровой безопасности в условиях кризисов состоят в создании специализированных органов по кибербезопасности, разработке национальных стратегий, внедрении систем мониторинга и реагирования, развитии кадрового потенциала и учете особенностей обеспечения цифровой безопасности в условиях кризисов.

Адаптивные механизмы заключаются в принятии ряда антикризисных мер, таких как усиление защиты критически важных объектов, создание резервных систем, внедрение систем быстрого реагирования и развитие систем кибер-разведки [11]. Технологические решения опираются на применение искусственного

интеллекта в кибербезопасности, использовании блокчейн-технологий, систем биометрической аутентификации, а также разработке технологий квантовой криптографии [12].

Модели эффективного управления цифровой безопасностью опираются на применение гибридных моделей, включающих комплексный подход, заключающийся в сочетании технических и организационных мер, интеграции различных уровней защиты и создании многоуровневых систем безопасности.

Адаптивные модели обеспечения цифровой безопасности основываются на внедрении гибких систем управления, характеризующихся быстрой адаптацией к новым угрозам, модульной структурой защиты и наличием возможностей масштабирования.

Механизмы обеспечения кибербезопасности на международном уровне

Практические рекомендации по совершенствованию системы цифровой безопасности в условиях кризисных явлений должны опираться на институциональные меры, включающие организационные решения по созданию международных центров реагирования, развитие систем обмена информацией, формирование единых стандартов безопасности [13]. К технологическим мерам относятся решения о внедрении систем предиктивной аналитики, развитии систем обнаружения вторжений и создании защищенных каналов связи.

Немаловажным является человеческий фактор в обеспечении цифровой безопасности, регулирование которого возможно с применением кадровых мер, таких как повышение квалификации специалистов, проведение регулярных учений по цифровой безопасности, развитие культуры кибербезопасности и оценка эффективности существующих механизмов.

Критериями оценки служат ключевые показатели, включающие время реагирования на инциденты, уровень защищенности критически важных объектов, эффективность

систем мониторинга, а также степень удовлетворенности пользователей.

Рекомендации по совершенствованию системы цифровой безопасности

Выявление перспектив развития системы цифровой безопасности основывается на анализе существующих технологических трендов [14]. Решения по совершенствованию системы цифровой безопасности могут основываться на развитии квантовых технологий, внедрении искусственного интеллекта и создании автономных систем защиты. Однако необходимы и институциональные изменения, заключающиеся в применении новых подходов при формировании международных коалиций, развитии систем глобального мониторинга, а также создании единых стандартов безопасности.

Таким образом, на основе результатов анализа текущего состояния международных экономических отношений становится возможным выбор стратегии, характеризующей пути достижения цели, направленной на обеспечение цифровой безопасности. Предложены основные направления формирования стратегии обеспечения цифровой безопасности в условиях кризисов (табл. 3).

Стратегии, представленные в табл. 3, могут быть использованы как по отдельности, так

и в сочетании, в зависимости от экономического и финансового состояния, а также характера кризисных явлений. Проведенный анализ показывает, что цифровая безопасность международной экономической системы требует комплексного подхода, учитывающего специфику кризисных явлений. Основными направлениями развития системы защиты являются совершенствование институциональной базы, развитие технологических решений, повышение эффективности управления рисками, а также укрепление международного сотрудничества.

Заключение

В результате проведенного исследования цифровой безопасности международной экономической системы в условиях кризисных явлений установлено, что цифровая трансформация мировой экономики создает качественно новые вызовы для обеспечения экономической безопасности на международном уровне. Выявлена прямая корреляция между уровнем цифровизации экономических процессов и уязвимостью международной системы к различным видам киберугроз. При этом традиционные механизмы обеспечения экономической безопасности демонстрируют недостаточную эффективность в условиях цифровой трансформации. Показано, что современные экономические кризисы

Таблица 3. Виды основных стратегий обеспечения цифровой безопасности в условиях кризисов

Основные направления развития	Приоритетные доминирующие области стратегического развития
Стратегия финансовой поддержки ускоренного роста	Ускоренный рост и реализация потенциала развития цифровой экономики с акцентом на экспорт при минимизации импорта. Основное внимание должно быть удалено высокотехнологичным продуктам и цифровому промышленному развитию
Стратегия обеспечения устойчивого экономического роста и цифровой трансформации	Обеспечение эффективного распределения и использования ресурсов при условии наличия достаточного потенциала для такого развития. В случае нерационального использования это может привести к быстрому истощению экономических ресурсов
Антикризисная стратегия расширения глобального рынка	Стратегия направлена, в первую очередь, на преодоление внутренних проблем, с постепенным продвижением на мировой рынок и формированием прочных позиций в международных экономических отношениях

Источник: составлено автором.

приобретают новый характер, обусловленный цифровыми факторами риска. Кибербезопасность становится неотъемлемым элементом комплексной системы обеспечения экономической стабильности на глобальном уровне.

Таким образом, цифровая безопасность международной экономической системы требует комплексного подхода, включающего как технологические решения, так и институциональные механизмы регулирования. Только такой системный подход позволит обеспечить устойчивость глобальной экономики в условиях современных вызовов и угроз.

Литература

1. Кожина В.О., Толмачева И.В. Цифровые данные, отражающие кризисы мировой экономики. Мировая экономика и мировые финансы. 2024. №4. С. 14–23.

2. Chatterjee S., Sarker S. A possible conceptualization of the information systems (IS) artifact: A general systems theory perspectival. Information Systems Journal. 2021. №4. pp. 550–578.

3. Григорьев Л.М. Весна переоценки: как меняется видение мировой экономики международными организациями. Современная мировая экономика. 2024. №1. С. 23–44.

4. Завриев С.К., Борисова О.В. Пандемия COVID-19: экономические и политические последствия. Мировая экономика и международные отношения. 2024. №3. С. 128–136.

5. Аузан А.А. Цифровая экономика как экономика: институциональные тренды. Вестник Московского университета. Серия 6. Экономика. 2019. №6. С. 12–19.

6. Егина Н.А., Балаясова А.А. Проблемы и перспективы формирования институциональной среды цифровой экономики. Экономика и управление: проблемы, решения. 2020. №8. С. 16–33.

7. Лапидус Л.В. Вызовы цифровой экономики как триггеры цифровой трансформации: эволюционная шкала и причинно-следственные связи. Интеллект. Инновации. Инвестиции. 2023. №3. С. 11–27.

8. Сергеев Е.А. Трансформация внешнеэкономической политики Европейского союза в контексте открытой стратегической автономии. Современная мировая экономика. 2024. №2. С. 24–40.

9. Heiets V. Economic socialization on the way to solidary construction of reality. Sociology: theory, methods, marketing. 2024. №4. pp. 27–50.

10. Nilsen T. Varieties of periphery and local agency in regional development. Regional Studies. 2023. №4. pp. 749–762.

11. Зуев В.Н. Дilemma допуска прямых иностранных инвестиций в политике ЕС и США: обеспечение притока капитала и/или усиление контроля стратегических активов? Контуры глобальных трансформаций: политика, экономика, право. 2022. №6. С. 88–109.

12. Колбанев М.О., Палкин И.И. Вызовы цифровой экономики. Гидрометеорология и экология. 2020. №5. С. 156–167.

13. Пыхов П.А. Экономическая безопасность России и ее регионов в современных условиях. Современная экономика: проблемы и решения. 2024. №12. С. 102–113.

14. Andersson F.N. G. Macroeconomic equilibriums, crises and fiscal policy. Global Discourse. 2022. №12. pp. 664–688.

References

1. Kozhina V.O., Tolmacheva I. V. Digital data reflecting global economic crises. Global Economy and Global Finance. 2024;4:14–23.

2. Chatterjee S., Sarker S. A possible conceptualization of the information systems (IS) artifact: A general systems theory perspectival. Information Systems Journal. 2021;4:550–578.

3. Grigoriev L.M. Spring of Reassessment: How International Organizations» Vision of the Global Economy is Changing. Modern Global Economy. 2024;1:23–44.

4. Zavriev S.K., Borisova O. V. COVID-19 Pandemic: Economic and Political Consequences. Global Economy and International Relations. 2024;3:128–136.

5. Auzan A.A. Digital Economy as Economy: Institutional Trends. Moscow University Bulletin. Series 6. Economy. 2019;6:12–19.
6. Egina N.A., Balyasova A.A. Problems and Prospects of Forming the Institutional Environment of the Digital Economy. Economy and Management: Problems, Solutions. 2020;8:16–33.
7. Lapidus L.V. Challenges of the Digital Economy as Triggers of Digital Transformation: Evolutionary Scale and Cause-Effect Relationships. Intelligence. Innovations. Investments. 2023;3:11–27.
8. Sergeev E.A. Transformation of the Foreign Economic Policy of the European Union in the Context of Open Strategic Autonomy. The Modern World Economy. 2024;2:24–40.
9. Heiets V. Economic socialization on the way to solidary construction of reality. Sociology: theory, methods, marketing. 2024;4:27–50.
10. Nilsen T. Varieties of periphery and local agency in regional development. Regional Studies. 2023;4:749–762.
11. Zuev V.N. The dilemma of admitting foreign direct investment in the policies of the EU and the USA: ensuring capital inflows and/or strengthening control over strategic assets? Contours of global transformations: politics, economics, law. 2022;6:88–109.
12. Kolbanev M.O., Palkin I.I. Challenges of the digital economy. Hydrometeorology and Ecology. 2020;5:156–167.
13. Pykhov P.A. Economic Security of Russia and Its Regions in Modern Conditions. Modern Economy: Problems and Solutions. 2024;12:102–113.
14. Andersson F.N. G. Macroeconomic Equilibria, Crises and Fiscal Policy. Global Discourse. 2022;12:664–688.

Автор заявляет об отсутствии конфликта интересов.

Статья поступила в редакцию: 14.07.2025;
одобрена после рецензирования 26.08.2025;
принята к публикации 03.09.2025.

The author declares no conflicts of interest.

The article was submitted 14.07.2025;
approved after reviewing 26.08.2025;
accepted for publication 03.09.2025.

Периодичность издания — 6 номеров в год.

№1 (120) — Февраль:

- Последний срок сдачи статьи в номер — 01 февраля;
- Выход номера — 28 февраля.

№2 (121) — Апрель:

- Последний срок сдачи статьи в номер — 01 апреля;
- Выход номера — 29 апреля.

№3 (122) — Июнь:

- Последний срок сдачи статьи в номер — 01 июня;
- Выход номера — 29 июня.

№4 (123) — Август:

- Последний срок сдачи статьи в номер — 01 августа;
- Выход номера — 29 августа.

№5 (124) — Октябрь:

- Последний срок сдачи статьи в номер — 01 октября;
- Выход номера — 29 октября.

№6 (125) — Декабрь:

- Последний срок сдачи статьи в номер — 01 декабря;
- Выход номера — 25 декабря.

**График выхода
журнала
«Микроэкономика»
в 2025 г.**

