DOI 10.46320/2077-7639-2025-7-140-140-145

Влияние цифровизации на экономическую безопасность государства через оценку выгод и затрат

Мухамадиярова А.К., Абрамова С.Р., Редников Д.В.

Цифровизация представляет собой значимый, но крайне неопределённый фактор экономической безопасности государства и ее влияние не может быть оценено однозначно как исключительно позитивное или негативное. Основным фактором укрепления национальной экономической безопасности в цифровую эпоху является не отказ от трансформации, а ее эффективное и безопасное управление, что требует непрерывного и тщательного анализа соотношения выгод и затрат на всех уровнях – от конкретных инфраструктурных проектов до национальной стратегии. Целью данного анализа является комплексное исследование данного соотношения, выявление ключевых факторов, определяющих баланс между позитивными эффектами цифровизации и порождаемыми ею новыми вызовами для экономической безопасности. В исследовании выявлено, что только комплексный подход, основанный на постоянном мониторинге и балансировке выгод и затрат, позволит использовать колоссальный потенциал цифровизации, минимизируя сопутствующие угрозы национальной экономической безопасности, а формирование национальных систем оценки цифровых рисков и их интеграция в процессы стратегического планирования становится критически важной задачей для суверенных государств.

ДЛЯ ЦИТИРОВАНИЯ ГОСТ 7.1–2003

Мухамадиярова А.К., Абрамова С.Р., Редников Д.В. Влияние цифровизации на экономическую безопасность государства через оценку выгод и затрат // Дискуссия. — 2025. — № 7(140). — С. 140–145.

КЛЮЧЕВЫЕ СЛОВА

Выгоды, затраты, цифровая трансформация, цифровая среда, цифровые риски.

DOI 10.46320/2077-7639-2025-7-140-140-145

The impact of digitalization on the economic security of the state through the assessment of benefits and costs

Mukhamadiyarova A.K., Abramova S.R., Rednikov D.V.

Digitalization is a significant, but extremely uncertain factor in the economic security of the state, and its impact cannot be assessed unambiguously as exclusively positive or negative. The main factor in strengthening national economic security in the digital era is not the rejection of transformation, but its effective and safe management, which requires continuous and thorough analysis of the ratio of benefits and costs at all levels – from specific infrastructure projects to national strategy. The purpose of this analysis is a comprehensive study of this ratio, identifying the key factors that determine the balance between the positive effects of digitalization and the new challenges it generates for economic security. The study found that only an integrated approach based on continuous monitoring and balancing of benefits and costs will make it possible to use the enormous potential of digitalization, minimizing the associated threats to national economic security, and the formation of national systems for assessing digital risks and their integration into strategic planning processes is becoming a critical task for sovereign states.

FOR CITATION APA

Mukhamadiyarova A.K., Abramova S.R., Rednikov D.V. The impact of digitalization on the economic security of the state through the assessment of benefits and costs. *Diskussiya [Discussion]*, 7(140), 140–145.

KEYWORDS

Benefits, costs, digital transformation, digital environment, digital risks.

ВВЕДЕНИЕ

Цифровая трансформация экономики перестала быть факультативной тенденцией; она представляет собой фундаментальный сдвиг, детерминирующий конкурентоспособность и устойчивость национальных хозяйственных систем в XXI веке. Процесс цифровизации экономики понимается как глубокое внедрение цифровых технологий (информационно-коммуникационные технологии, большие данные, искусственный интеллект, интернет вещей, блокчейн) в производственные процессы, системы управления, финансовые операции и предоставление государственных услуг, оказывает амбивалентное воздействие на экономическую безопасность государства. Экономическая безопасность трактуется как состояние защищенности национальной экономики от внутренних и внешних угроз, обеспечивающее ее суверенитет, устойчивость, способность к прогрессивному развитию и удовлетворению жизненно важных потребностей общества: *«...социально-экономическое развитие регионов в современных условиях направлено на обеспечение безопасности через*

повышение уровня цифровой зрелости» [1, с. 194]. Ключевым аспектом понимания этого влияния является проведение систематической оценки соотношения выгод (потенциал роста, эффективности, устойчивости) и затрат (финансовые вложения, возникающие риски и уязвимости), сопряженных с цифровой трансформацией.

ОСНОВНАЯ ЧАСТЬ

Цифровизация создает новые парадигмы экономической деятельности, трансформируя традиционные понятия производительности, конкуренции и стоимости. Ее влияние на экономическую безопасность носит полярный характер, выступая мощным драйвером экономического роста через повышение производительности труда за счет автоматизации, оптимизации логистики и управления цепочками поставок, развития инновационных отраслей и сервисов, а также расширения доступа к глобальным рынкам для малого и среднего бизнеса. С другой стороны, она генерирует новые классы рисков: усиление зависимости от критически важных иностранных технологий и инфраструктуры, рост уязвимости к кибератакам на объекты критической информационной инфраструктуры (ОКИИ), цифровое неравенство регионов и социальных групп, возникновение угроз для конфиденциальности и суверенитета данных граждан и государства, а также потенциальную дестабилизацию рынков труда: *«…значение проблем цифровых угроз увеличиваются вследствие малой подготовленности предприятий. По результатам опроса Аналитического центра НАФИ, около 70% отечественных предпринимателей считают кибератаки маловероятными или невозможными; тем не менее, более половины из опрошенных сталкивались с сбоями оборудования, вирусами и подвергались попыткам применения мошеннических схем»* [2, с. 125]. Оценка чистого эффекта цифровизации на экономическую безопасность требует тщательного взвешивания этих разнонаправленных факторов: *«Разрыв в цифровых технологиях и незавершенность цифровых инфраструктур представляют собой широко распространенную угрозу, препятствующую получению положительных результатов от цифровизации в интересах МСП»* [3, с. 401].

Для систематической оценки влияния цифровизации на экономическую безопасность необходим структурированный подход, основанный на принципах анализа выгод и затрат (Cost-Benefit Analysis, CBA) [4], адаптированного к специфике цифровой трансформации и задачам национальной безопасности. Данный подход предполагает идентификацию, количественную и качественную оценку всех значимых положительных результатов (выгод) и отрицательных последствий (затрат и рисков) цифровизации в контексте ключевых компонентов экономической безопасности.

Позитивное влияние цифровизации на экономическую безопасность проявляется через несколько ключевых каналов: это значительный рост экономической эффективности и производительности, автоматизация рутинных операций, внедрение систем предиктивной аналитики для оптимизации запасов и производственных циклов, развитие платформенных решений для B2B и B2G взаимодействия снижают транзакционные издержки и повышают общую продуктивность экономики, что укрепляет макроэкономическую стабильность и конкурентоспособность; цифровизация стимулирует инновационное развитие, создавая условия для появления принципиально новых отраслей (например, разработка ИИ, большие данные, квантовые вычисления), бизнес-моделей (шеринг-экономика, подписка на ПО) и высокотехнологичных рабочих мест, что диверсифицирует экономику и снижает ее зависимость от сырьевого экспорта, то есть диверсификация является ключевым элементом устойчивости; развитие цифровых государственных сервисов (e-government) и систем управления на основе данных повышает эффективность государственного администрирования, прозрачность принятия решений, качество предоставления публичных услуг и уровень борьбы с коррупцией, что способствует институциональной устойчивости. Цифровые технологии (IoT, спутниковый мониторинг, системы предиктивного обслуживания) значительно повышают устойчивость критической инфраструктуры (энергетика, транспорт, коммуникации) к техногенным сбоям и природным катастрофам, обеспечивая непрерывность функционирования жизненно важных систем. Цифровизация финансового сектора (FinTech, RegTech) способствует повышению финансовой стабильности через улучшение систем мониторинга рисков, противодействия отмыванию денег и финансированию терроризма, а также расширение финансовой инклюзии.

Реализация потенциала цифровизации сопряжена со значительными затратами и генерирует новые риски, непосредственно угрожающие экономической безопасности [5]. Первичными являются прямые финансовые затраты: масштабные инвестиции, необходимые для создания и модернизации цифровой инфраструк-

туры (высокоскоростной интернет, дата-центры, сенсорные сети), разработки и внедрения сложного ПО (включая системы ИИ), приобретения дорогостоящего оборудования и обеспечения кибербезопасности. Для многих государств, особенно развивающихся, это создает существенную бюджетную нагрузку и может приводить к росту государственного долга или необходимости привлечения иностранных инвестиций с потенциальными условиями. Более значимыми являются системные риски, где киберугрозы представляют собой наиболее острую и растущую опасность. Атаки на ОКИИ (энергосистемы, финансовые учреждения, транспортные узлы, системы госуправления) способны парализовать экономику, нанести колоссальный финансовый ущерб и подорвать доверие населения. Сложность и стоимость обеспечения адекватного уровня киберзащиты постоянно возрастают, цифровизация резко увеличивает поверхность атаки, технологическая зависимость от иностранных решений (импорт ПО, микроэлектроники, телекоммуникационного оборудования) создает критическую уязвимость. Экономические санкции, политическое давление или прекращение поддержки со стороны стран-производителей ключевых технологий могут дестабилизировать целые отрасли и инфраструктуру, поэтому формирование «цифрового суверенитета» становится императивом безопасности. Риски, связанные с данными, включают угрозы конфиденциальности персональных данных граждан, утечки коммерческой тайны и стратегически важной информации, а также вопросы суверенитета над национальными данными массивами, особенно при их хранении или обработке за рубежом. Социально-экономические риски включают углубление цифрового неравенства (цифровой разрыв между регионами, социальными группами, поколениями), что ведет к социальной напряженности и ограничивает инклюзивность роста. Автоматизация и внедрение ИИ могут привести к структурной безработице в ряде секторов, требующей масштабных программ переобучения и социальной адаптации, что создает нагрузку на бюджет и риски социальной нестабильности [6]. Наконец, существует риск монополизации цифровых рынков глобальными технологическими гигантами, что может подавлять национальный бизнес, искажать конкуренцию и создавать каналы внешнего влияния [7].

Для принятия обоснованных решений в области цифровой политики и обеспечения экономической безопасности необходимы попытки количественной оценки соотношения выгод (B) и затрат (C) цифровизации. Это сложная задача из-за трудностей измерения нематериальных выгод (например, повышение качества услуг) и оценки вероятности и масштаба рисков (например, кибератака), тем не менее, можно предложить концептуальные модели:

Чистая приведенная стоимость (NPV) цифровых инвестиций с учетом рисков:

Эта модель расширяет традиционный NPV, включая поправку на риск (R), связанный с угрозами экономической безопасности.

$$NPVs = \sum [(Bt - Ct) / (1 + r)^t] - R \quad (1)$$

где:

NPVs – Чистая приведенная стоимость проекта цифровизации с учетом безопасности (Security-adjusted NPV).

Bt– Ожидаемые выгоды в период t (рост ВВП, снижение издержку, повышение налоговых поступлений, социальные выгоды в денежном выражении).

Ct – Прямые и косвенные затраты в период t (инвестиции, эксплуатационные расходы, затраты на киберзащиту).

r – Ставка дисконтирования.

R – Оценка потенциальных потерь от реализации рисков для экономической безопасности (ожидаемый ущерб от кибератак, стоимость восстановления после сбоев из-за импортозависимости, социально-экономические издержки цифрового разрыва). R может оцениваться как $R = \sum (pi * Li)$, где *pi* – вероятность реализации i-го риска, *Li* – ожидаемый ущерб от него.

Проект считается приемлемым с точки зрения экономической безопасности, если $NPVs > 0$, и его выгоды с поправкой на риски перевешивают затраты.

Индекс цифровой эффективности безопасности (Digital Security Efficiency Index – DSEI) – индекс пытается агрегировать ключевые показатели, отражающие баланс между уровнем цифровизации, ее экономическими результатами и уровнем защищенности от угроз.

$$DSEI = \alpha * (DI / DImax) + \beta * (EG / EGmax) - \\ - \gamma * (CRI / CRImax) - \delta * (TD / TDmax) \quad (2)$$

где:

DI– Уровень цифровизации экономики (напр., интегральный индекс, включающий проникновение ШПД, использование облаков, ИИ, IoT бизнесом и госсектором).

DImax – Максимально возможный (или эталонный) уровень DI.

EG– Экономическая отдача от цифровизации (напр., вклад цифрового сектора в ВВП, рост производительности в цифровизованных отраслях).

EGmax – Максимально возможный (или эталонный) уровень EG.

CRI – Индекс киберрисков (отражающий частоту и тяжесть инцидентов, уязвимость ОКИИ).

CRImax - Максимально возможный (или наихудший) уровень CRI.

TD – Уровень технологической зависимости (напр., доля импорта критических ИТ-компонентов и ПО).

TDmax – Максимально возможный (или критический) уровень TD.

$\alpha, \beta, \gamma, \delta$ – Весовые коэффициенты ($\alpha + \beta + \gamma + \delta = 1$), отражают относительную важность каждого фактора для экономической безопасности. Значения коэффициентов γ и δ обычно выше, так как риски напрямую угрожают безопасности.

Чем выше значение DSEI (ближе к 1), тем более эффективно и безопасно для экономики проходит цифровая трансформация. Снижение индекса сигнализирует о росте рисков или снижении отдачи.

Модель затраты-эффективность мер безопасности (Cost-Effectiveness of Security Measures – CESM) – модель фокусируется на оценке конкретных мер по снижению цифровых рисков (например, внедрение системы обнаружения вторжений, создание резервных мощностей, развитие отечественных ИТ-решений).

$$CESMj = (Rreductionj) / (Cj) \qquad (3)$$

где:

CESMj – Затрато-эффективность меры j.

Rreductionj – Снижение совокупного риска R (рассчитанного как в модели NPV_s) в результате реализации меры j.

Cj – Затраты на реализацию и поддержку меры j.

Приоритет должен отдаваться мерам с наибольшим значением *CESMj* обеспечивающим максимальное снижение риска на единицу затраченных ресурсов.

Баланс между позитивными эффектами и рисками цифровизации для экономической безопасности не является статичным, а определяется комплексом факторов:

1. Развитые страны обладают большими ресурсами для инвестиций и развитой ИТ-индустрией, снижая зависимость и повышая способность противостоять угрозам.
2. Эффективное госуправление, прозрачность, сильные регуляторы в сфере данных и конкуренции, современное законодательство о кибербезопасности и цифровом суверенитете критически важны для минимизации рисков.
3. Наличие квалифицированных ИТ-специалистов, киберзащитников и цифровой грамотности населения является ключевым условием успешной и безопасной трансформации.
4. Наличие национальной цифровой стратегии, четко увязанной со стратегией экономической безопасности, и эффективная координация между государством, бизнесом и академическим сообществом.
5. Участие в разработке международных норм кибербезопасности, обмен информацией об угрозах, сотрудничество в борьбе с киберпреступностью.

ЗАКЛЮЧЕНИЕ

Выгоды цифровизации в виде роста эффективности, инноваций, устойчивости инфраструктуры и качества госуправления значительны и необходимы для поддержания конкурентоспособности, но сопутствующие риски – киберугрозы, технологическая зависимость, уязвимость данных, социальное расслоение – носят стратегический характер и способны нанести ущерб, соизмеримый или превышающий потенциальные выгоды. Представленные модели количественной оценки (NPVs, DSEI, CESM) предоставляют концептуальную основу для принятия решений, хотя их практическое применение требует развития методологии сбора данных и оценки рисков. Успех цифровой трансформации как фактора усиления, а не ослабления экономической безопасности, будет определяться способностью государства и общества осуществлять масштабные инвестиции не только в технологии, но и в киберзащиту, развитие отечественных компетенций и решений, человеческий капитал и эффективные институты управления рисками. Только комплексный подход, основанный на постоянном мониторинге и балансировке выгод и затрат, позволит использовать колоссальный потенциал цифровизации, минимизируя сопутствующие угрозы национальной экономической безопасности. Формирование национальных систем оценки цифровых рисков и их интеграция в процессы стратегического планирования становится критически важной задачей для суверенных государств.

Список литературы

1. *1. Деревянко, В. Э.* Современные проблемы экономической безопасности регионов Российской Федерации в условиях цифровизации экономики / В. Э. Деревянко // Криминологический журнал. – 2022. – № 3. – С. 191-194. – DOI 10.24412/2687-0185-2022-3-191-194. – EDN OATBFV.
2. *2. Сигунова, Т. А.* Обеспечение экономической безопасности предприятий отраслевого сектора в условиях цифровизации экономики / Т. А. Сигунова // Вопросы региональной экономики. – 2022. – № 3(52). – С. 115-128. – EDN UHUPYA.
3. *3. Морозов, В. В.* Влияние цифровизации на экономическую безопасность малых и средних предприятий / В. В. Морозов // Актуальные вопросы современной экономики. – 2022. – № 5. – С. 399-401. – EDN KHYHKM.
4. *4. Вагдатли, Т., Петроутсату, К.* Подходы к моделированию анализа затрат и выгод на протяжении жизненного цикла дорожной инфраструктуры: критический обзор и направления на будущее // Здания. – 2023. – Т. 13. – №. 1. – С. 94. – DOI: 10.3390/buildings13010094.
5. *5. Кирищиева, И. И. и др.* Риски и угрозы экономической безопасности в цифровой экономике // Веб-конференции SHS. – EDP Sciences, 2021. – Т. 110. – С. 01028. – DOI 10.1051/shsconf/202111001028.
6. *6. Ревина, С. Н.* Информационная безопасность в условиях цифровизации таможенных органов / С. Н. Ревина, А. А. Горбунова, В. М. Дворянчиков // Евразийский юридический журнал. – 2024. – № 4(191). – С. 438-440. – DOI 10.46320/2073-4506-2024-4-191-438-440. – EDN DZIJOL.
7. *7.* Лиюси. Управление техническими и технологическими инновациями в цифровой экономике / Лиюси, Ф. И. Аржаев // Human Progress. – 2024. – Т. 10, № 6. – DOI 10.46320/2073-4506-2024-6a-16. – EDN LPSQRY.

References

1. *1. Derevyanko, V. E.* Modern problems of economic security of the regions of the Russian Federation in the context of digitalization of the economy / V. E. Derevyanko // Criminological journal. – 2022. – № 3. – Pp. 191-194. – DOI 10.24412/2687-0185-2022-3-191-194. – EDN OATBFV.
2. *2. Sigunova, T. A.* Ensuring economic security of enterprises of the industry sector in the context of digitalization of the economy / T. A. Sigunova // Issues of regional economics. – 2022. – № 3 (52). – Pp. 115-128. – EDN UHUPYA.
3. *3. Morozov, V. V.* The impact of digitalization on the economic security of small and medium-sized enterprises / V. V. Morozov // Actual issues of modern economics. – 2022. – № 5. – Pp. 399-401. – EDN KHYHKM.
4. *4. Vagdatli, T., Petroutsatou, K.* Modeling approaches to life cycle cost–benefit analysis of road infrastructure: a critical review and future directions // Buildings. – 2023. – Vol. 13. – № 1. – Pp. 94. – DOI: 10.3390/buildings13010094.
5. *5. Kirishchieva, I. et al.* Risks and threats to economic security in the digital economy // SHS Web of Conferences. – EDP Sciences, 2021. – Vol. 110. – P. 01028. – DOI 10.1051/shsconf/202111001028.
6. *6. Revina, S. N.* Information Security in the Context of Digitalization of Customs Agencies / S. N. Revina, A. A. Gorbunova, and V. M. Dvoryanchikov // Eurasian Law Journal. – 2024. – No. 4(191). – Pp. 438-440. – DOI 10.46320/2073-4506-2024-4-191-438-440. – EDN DZIJOL.
7. *7.* Liyusi. Management of Technical and Technological Innovations in the Digital Economy / Liyusi, F. I. Arzhayev // Human Progress. – 2024. – Vol. 10, No. 6. – DOI 10.46320/2073-4506-2024-6a-16. – EDN LPSQRY.

Информация об авторах

Мухамадиярова А.К., кандидат экономических наук, доцент, доцент кафедры управления в ОВД Уфимского юридического института МВД России (г. Уфа, Российская Федерация).

Абрамова С.Р., кандидат исторических наук, доцент кафедры экономико-правового обеспечения безопасности Института истории и государственного управления Уфимского университета науки и технологий (г. Уфа, Российская Федерация).

Редников Д.В., старший преподаватель кафедра экономико-правового обеспечения безопасности Института истории и государственного управления Уфимского университета науки и технологий (г. Уфа, Российская Федерация).

Information about the authors

Mukhamadiyarova A.K., Ph.D. in Economics**,** Associate Professor, Associate Professor of the Department of Management in the Internal Affairs Bodies of the Ufa Law Institute of the Ministry of Internal Affairs of the Russian Federation (Ufa, Russian Federation).

Abramova S.R., Ph.D. in History, Associate Professor of the Department of Economic and Legal Security of the Institute of History and Public Administration of the Ufa University of Science and Technology (Ufa, Russian Federation).

Rednikov D.V., Senior Lecturer at the Department of Economic and Legal Security of the Institute of History and Public Administration of the Ufa University of Science and Technology (Ufa, Russian Federation).