

Рецензия
на статью «Роль кибербезопасности в обеспечении устойчивости и конкурентоспособности цифровой экономики»
Сулейманова Д.А., Алиев М.А., Магомедова М.А.

Характеристика и актуальность темы

Тема исследования обладает высокой актуальностью в условиях ускоренной цифровизации экономики и роста масштаба киберугроз, влияющих на устойчивость, инвестиционную привлекательность и конкурентоспособность как отдельных организаций, так и национальных экономик в целом. Фокус на кибербезопасности как стратегическом факторе развития цифровой экономики соответствует текущим вызовам и приоритетам государственного и корпоративного управления.

Анализ содержания исследования

Авторы последовательно раскрывают связь между уровнем киберзащиты и устойчивостью цифровых процессов, уделяя внимание как экономическим последствиям киберинцидентов, так и институциональным механизмам противодействия. Сильной стороной является попытка синтеза статистики за 2024–2025 гг. и выделение современных трендов (рост доли критичных инцидентов, усиление социально-инженерных атак, усложнение целевых воздействий). Логика построения работы в целом выдержана: от обоснования проблемы и обзора источников — к анализу угроз, инструментов регулирования и формулированию выводов. Вместе с тем отдельные положения нуждаются в более строгой верификации источниками: ряд количественных оценок (доли инцидентов, динамика, сопоставимость мировых и российских показателей) требует четкого указания первичных баз данных/отчетов и корректного разведения периодов наблюдения, чтобы исключить эффект «несопоставимых выборок».

Теоретическая и практическая значимость

Теоретическая значимость работы состоит в акцентировании кибербезопасности как элемента экономической устойчивости и конкурентных преимуществ цифровой экономики, а не только как технической функции. Практическая значимость проявляется в предложении комплексного подхода к управлению рисками: сочетание регулирования, корпоративных практик, подготовки кадров и развития инструментов (включая ИИ-ориентированные системы защиты и киберстрахование). Представленные выводы могут быть использованы при актуализации корпоративных стратегий ИБ и региональных/национальных программ цифрового развития, особенно в части перехода к риск-ориентированной и предиктивной модели защиты.

Заключение

Статья соответствует тематике научного издания, характеризуется актуальностью, прикладной направленностью и логичностью изложения. При доработке рекомендуется усилить методическую часть: конкретизировать источники статистики, уточнить методику агрегирования показателей и границы применимости приведенных оценок, а также более четко отделить

прогнозные допущения от эмпирически подтвержденных результатов.
Рекомендую данную статью к публикации в научном журнале.

Рецензент - Зотикова Ольга Николаевна, доктор экономических наук,
профессор,

Российский государственный университет имени А.Н. Косыгина
г. Москва, Россия

Reviewer - Zotikova Olga Nikolaevna, Doctor of Economics, Professor,
Kosygin Russian State University, Moscow, Russia

