

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2025, Том 17, № s3 / 2025, Vol. 17, Iss. s3 <https://esj.today/issue-s3-2025.html>

URL статьи: <https://esj.today/PDF/50FAVN325.pdf>

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:

Ашурзода, А. Н. Цифровая трансформация как фактор устойчивости экономической безопасности предприятий лёгкой промышленности в условиях кризисных явлений (на примере Республики Таджикистан) / А. Н. Ашурзода // Вестник евразийской науки. — 2025. — Т. 17. — № s3. — URL: <https://esj.today/PDF/50FAVN325.pdf>.

For citation:

Ashurzoda A.N. Digital transformation as a factor in the sustainability of economic security of light industry enterprises in the context of crisis phenomena (using the Republic of Tajikistan as an example). *The Eurasian Scientific Journal*. 2025;17(s3): 50FAVN325. Available at: <https://esj.today/PDF/50FAVN325.pdf>. (In Russ., abstract in Eng.).

УДК 338.24; 004.9; 334.7

Ашурзода Ашур Нурулло

Таджикский технический университет имени М. Осими, Душанбе, Республика Таджикистан
Доцент кафедры «Производственного менеджмента»
Кандидат экономических наук
E-mail: aashurzoda1968@gmail.com

Цифровая трансформация как фактор устойчивости экономической безопасности предприятий лёгкой промышленности в условиях кризисных явлений (на примере Республики Таджикистан)

Аннотация. Исследование раскрывает концептуальные основы применения цифровых технологий в качестве стратегического инструмента обеспечения экономической безопасности предприятий легкой промышленности в условиях современных кризисных вызовов и экономической неопределенности. В работе представлен комплексный анализ процессов цифровой трансформации как катализатора повышения устойчивости промышленных предприятий к внешним и внутренним угрозам экономической безопасности. Проведенное исследование выявляет критические аспекты внедрения цифровых решений в систему антикризисного управления предприятиями легкой промышленности Республики Таджикистан, где данная отрасль демонстрирует лидирующие позиции в регионе Центральной Азии с темпами роста 19 % в 2023 году. Установлено, что цифровизация производственных процессов создает новые возможности для превентивного выявления угроз экономической безопасности через системы мониторинга в режиме реального времени, автоматизированного анализа рисков и прогнозного моделирования. Выявлены специфические киберугрозы и цифровые риски, характерные для предприятий легкой промышленности в условиях развивающихся экономик, включающие недостаточный уровень киберзащиты, ограниченные компетенции персонала в области информационной безопасности, зависимость от импортных технологических решений. Разработана концептуальная модель адаптивной системы управления экономической безопасностью предприятий легкой промышленности, интегрирующая цифровые технологии искусственного интеллекта, больших данных, интернета вещей и блокчейн-решений для повышения устойчивости к кризисным явлениям. Определены приоритетные направления цифровой трансформации предприятий отрасли в контексте формирования антикризисной устойчивости, включающие автоматизацию систем раннего предупреждения, внедрение

технологий предиктивной аналитики, создание цифровых двойников производственных процессов и формирование экосистемы цифрового взаимодействия с поставщиками и потребителями. Исследование обосновывает необходимость формирования национальной стратегии цифровизации легкой промышленности как основы укрепления экономической безопасности отрасли в долгосрочной перспективе.

Ключевые слова: цифровая трансформация; экономическая безопасность; легкая промышленность; антикризисное управление; киберугрозы; адаптивное управление; цифровые технологии; искусственный интеллект; предиктивная аналитика; устойчивость предприятий

Введение

Актуальность исследования обусловлена возрастающей ролью цифровых технологий в формировании новых парадигм обеспечения экономической безопасности промышленных предприятий в условиях глобальной цифровизации экономики и усиления неопределенности внешней среды. Стремительное развитие цифровых технологий создает качественно новые возможности для повышения устойчивости предприятий к кризисным явлениям, одновременно порождая принципиально новые типы угроз и рисков. Легкая промышленность Республики Таджикистан, занимающая лидирующие позиции в регионе по темпам цифровой трансформации, представляет уникальную исследовательскую площадку для анализа взаимосвязи между процессами цифровизации и обеспечением экономической безопасности в условиях развивающейся экономики.

Научная проблема заключается в отсутствии комплексного теоретико-методологического подхода к интеграции цифровых технологий в систему обеспечения экономической безопасности предприятий легкой промышленности, учитывающего специфику антикризисного управления в условиях современных вызовов цифровой экономики и геополитической нестабильности.

Объектом исследования выступают процессы цифровой трансформации предприятий легкой промышленности Республики Таджикистан в контексте обеспечения их экономической безопасности.

Предметом исследования являются механизмы и инструменты интеграции цифровых технологий в систему антикризисного управления экономической безопасностью предприятий легкой промышленности.

Целью исследования является разработка концептуальных основ применения цифровых технологий для повышения устойчивости экономической безопасности предприятий легкой промышленности в условиях кризисных явлений.

Задачи исследования:

1. Проанализировать современные тенденции цифровизации промышленных предприятий и выявить их влияние на систему обеспечения экономической безопасности.
2. Исследовать специфику цифровых угроз и рисков для предприятий легкой промышленности в условиях развивающейся экономики.
3. Разработать модель адаптивной системы управления экономической безопасностью предприятий легкой промышленности на основе цифровых технологий.

Научная новизна исследования состоит в развитии теоретических представлений о роли цифровых технологий в формировании антикризисной устойчивости предприятий легкой промышленности и разработке инновационных подходов к интеграции цифровых решений в систему экономической безопасности.

Практическая значимость работы заключается в возможности использования разработанных рекомендаций для формирования стратегий цифровой трансформации предприятий легкой промышленности и повышения их устойчивости к кризисным воздействиям.

1. Методы и материалы

Теоретико-методологической основой исследования служат фундаментальные положения теории экономической безопасности, концепции цифровой экономики, теории антикризисного управления и адаптивного менеджмента. Методологический подход базируется на системном анализе процессов цифровой трансформации с применением междисциплинарного подхода, интегрирующего достижения экономической теории, теории управления и информационных технологий.

В качестве методов исследования использованы: системный анализ, структурно-функциональный анализ, сравнительный анализ, метод экспертных оценок, SWOT-анализ, методы сценарного планирования и прогнозирования, а также методы математического моделирования для построения адаптивных систем управления. Для анализа цифровых угроз применены методы анализа киберрисков и оценки информационной безопасности.

Информационную базу исследования составили данные о состоянии и тенденциях развития легкой промышленности Республики Таджикистан, материалы международных организаций по цифровизации экономики, аналитические отчеты по кибербезопасности и цифровым угрозам, нормативно-правовые акты в области цифровой экономики и экономической безопасности.

В ходе исследования был проведен анализ научных трудов: М.А. Юсуповой [1], Ш.М. Бобошоева [2], Ш.Ш. Базарова [3], М.Д. Зияевой [4], Х.А. Абдукодилова [5], У.С. Асрорзода [6], Г.В. Коваленко [7], А.Б. Мирсаидова [8], Ф.А. Кодирова [9], И. Аминова [10].

2. Результаты и обсуждения

Современные тенденции цифровизации промышленных предприятий характеризуются переходом от отдельных автоматизированных решений к комплексным цифровым экосистемам, интегрирующим все аспекты производственной и управленческой деятельности. Анализ глобальных трендов показывает, что инвестиции в цифровую трансформацию промышленности в 2024 году превысили 149 млрд рублей, что на 60 % больше предыдущего года, демонстрируя стратегическую важность цифровизации для обеспечения конкурентоспособности предприятий.¹

Цифровая трансформация оказывает многоаспектное воздействие на систему экономической безопасности предприятий, создавая как новые возможности для укрепления защищенности, так и принципиально новые типы угроз. К позитивным аспектам относятся возможности автоматизации мониторинга рисков, внедрения систем предиктивной аналитики для раннего выявления угроз, создания цифровых двойников для моделирования кризисных сценариев и повышения точности принятия управленческих решений.

¹ Digital Transformation Market Size and Growth 2025 to 2034. Режим доступа — URL: <https://www.precedenceresearch.com/digital-transformation-market#:~:text=The%20global%20digital%20transformation%20market%20size%20accounted%20for%20USD%201.18,24.74%25%20from%202025%20to%202034> (дата обращения 12.05.2025).

Анализ состояния цифровизации легкой промышленности Таджикистана выявляет постепенное внедрение цифровых технологий преимущественно в крупных предприятиях отрасли (табл. 1).

Таблица 1

Уровень цифровизации предприятий легкой промышленности Республики Таджикистан по размерам

Размер предприятий	Количество предприятий	Доля с базовой цифровизацией, %	Доля с продвинутой цифровизацией, %	Средний уровень цифровой зрелости
Крупные (> 500 чел.)	15	80,0	33,3	Высокий
Средние (100–500 чел.)	85	55,3	12,9	Средний
Малые (< 100 чел.)	715	22,4	2,8	Низкий
Итого	815	28,7	6,1	Базовый

Составлено автором на основе анализа материалов²

Представленные данные демонстрируют значительную дифференциацию в уровне цифровой зрелости предприятий различного размера, что создает неравномерность в способности противостоять современным угрозам экономической безопасности. Крупные предприятия, обладающие более высоким уровнем цифровизации, имеют лучшие возможности для внедрения современных систем защиты и мониторинга рисков. Спектр цифровых угроз экономической безопасности предприятий легкой промышленности характеризуется высокой динамичностью и постоянным усложнением. Киберугрозы представляют наиболее динамично развивающуюся категорию, при этом эксперты отмечают рост числа кибератак на 80 % в 2024 году.³ Статистический анализ киберинцидентов в промышленном секторе стран СНГ демонстрирует тревожную динамику роста (табл. 2).

Таблица 2

Динамика киберугроз в промышленном секторе стран СНГ в 2023–2024 гг.

Тип угроз	Q2 2023	Q2 2024	Рост, %	Основные цели атак
Программы-вымогатели	145	287	+98 %	Производственные системы, базы данных
Промышленный шпионаж	89	156	+75 %	Технологические данные, коммерческая тайна
DDoS-атаки	234	398	+70 %	Веб-сайты, онлайн-сервисы
Фишинг и социальная инженерия	312	467	+50 %	Учетные данные сотрудников
Атаки на IoT-устройства	67	112	+67 %	Производственное оборудование
Итого	847	1 420	+68 %	Все категории

Составлено автором на основе анализа материалов⁴

² Таджикистан стал первым в Центральной Азии по темпу развития легкого прома | Новости Таджикистана ASIA-Plus. Режим доступа — URL: <https://www.asiaplustj.info/ru/news/tajikistan/economic/20240306/tadzhikistan-stal-pervim-v-tsentralnoi-azii-po-tempu-razvitiya-legkoproma> (дата обращения: 12.05.2025).

Каков уровень цифровизации в Таджикистане? Рассматриваем основные проблемы и решение. Режим доступа — URL: <https://khovar.tj/rus/2024/03/kakov-uroven-tsifrovizatsii-v-tadzhikistane-rassmatrivaem-osnovnye-problemy-i-reshenie/> (дата обращения: 12.05.2025).

Первые шаги цифровой экономики Таджикистана за годы независимости. Режим доступа — URL: <https://www.asiaplustj.info/news/tajikistan/economic/20190918/pervie-shagi-tsifrovoi-ekonomiki-tadzhikistana-za-godi-nezavisimosti> (дата обращения: 12.05.2025).

³ Снижаем цифровые риски: семь мер для руководителя организации | РБК Тренды. Режим доступа — URL: <https://trends.rbc.ru/trends/industry/615b65b39a7947274298822c> (дата обращения: 15.05.2025).

⁴ Аналитические статьи. Режим доступа — URL: <https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/> (дата обращения: 12.05.2025).

Ключевые тренды в кибербезопасности в 2024 году | Wezom. Режим доступа — URL: <https://wezom.com.ua/blog/6-trendov-kiberbezopasnosti-v-2024-godu> (дата обращения: 15.05.2025).

Новые риски кибератак в России и СНГ: полный разбор. Режим доступа — URL: <https://www.f6.ru/cybercrime-trends-annual-report-2024-2025/> (дата обращения: 15.05.2025).

Приведенные данные свидетельствуют о критическом возрастании киберугроз, что требует принятия неотложных мер по укреплению цифровой безопасности предприятий. Особенно тревожным является рост атак программ-вымогателей на 98 %, поскольку данный тип угроз способен полностью парализовать производственную деятельность предприятий.

Экономический ущерб от киберинцидентов для промышленных предприятий характеризуется значительными масштабами и долгосрочными последствиями, которые выходят далеко за рамки технических проблем и оказывают системное воздействие на все аспекты деятельности предприятий. Особенно критичными являются долгосрочные последствия, восстановление от которых может занимать годы.

Адаптивная система управления экономической безопасностью предприятий легкой промышленности должна интегрировать передовые цифровые технологии для обеспечения динамичного реагирования на изменяющиеся угрозы (табл. 3).

Таблица 3

**Компоненты адаптивной системы управления
экономической безопасностью на основе цифровых технологий**

Технологический компонент	Функции в системе безопасности	Преимущества	Риски внедрения
Искусственный интеллект	Предиктивная аналитика угроз, автоматизация реагирования	Скорость анализа, точность прогнозов	Высокая стоимость, сложность настройки
Большие данные (Big Data)	Сбор и анализ разнородной информации о рисках	Комплексность анализа, выявление скрытых закономерностей	Требования к инфраструктуре, конфиденциальность
Интернет вещей (IoT)	Мониторинг производственных процессов в реальном времени	Непрерывный контроль, раннее выявление аномалий	Уязвимости безопасности, сложность управления
Блокчейн	Защита цепей поставок, верификация транзакций	Прозрачность, неизменяемость данных	Энергозатратность, масштабируемость
Облачные вычисления	Резервирование данных, гибкость инфраструктуры	Доступность, масштабируемость	Зависимость от провайдера, риски безопасности

Составлено автором на основе анализа материалов⁵

Представленная система технологических компонентов обеспечивает многоуровневую защиту предприятий от современных угроз при одновременном повышении эффективности операционной деятельности. Ключевым преимуществом такого подхода является возможность автоматизации процессов выявления и реагирования на угрозы, что критически важно в условиях высокой динамики развития киберугроз.

Архитектура адаптивной системы управления экономической безопасностью предприятий легкой промышленности представляет собой многоуровневую структуру (рис. 1).

Представленная архитектура обеспечивает замкнутый цикл управления безопасностью, начиная от непрерывного сбора данных о состоянии предприятия и заканчивая автоматизированным исполнением защитных мер. Ключевым элементом системы является уровень принятия решений, который интегрирует результаты анализа данных с экспертными знаниями для формирования оптимальных стратегий реагирования.

Оценка готовности предприятий легкой промышленности Таджикистана к внедрению адаптивных систем управления экономической безопасностью выявляет существенные различия по уровням развития (табл. 4).

⁵ Тренды информационных технологий для эффективного бизнеса на 2025 год. Режим работы — URL: <https://www.agora.ru/blog/trendy-tsifrovizatsii-korporativnykh-biznes-protsessov-2025/> (дата обращения: 15.05.2025).

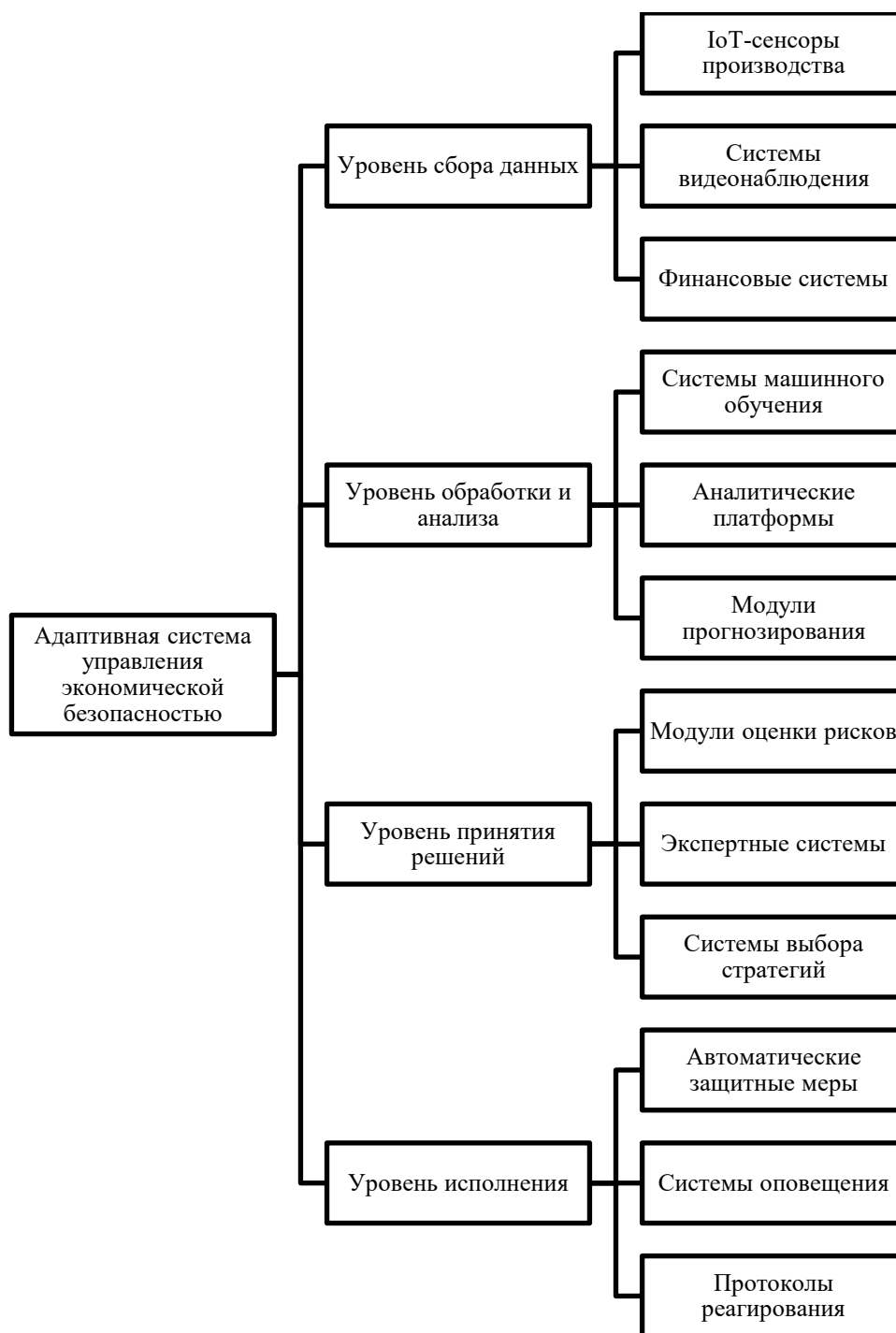


Рисунок 1. Архитектура адаптивной системы управления экономической безопасностью предприятий легкой промышленности (составлено автором)

Результаты оценки показывают, что текущий уровень готовности предприятий к внедрению адаптивных систем экономической безопасности является недостаточным, особенно для малых предприятий. Наиболее критичными являются дефицит кадровых компетенций и ограниченные финансовые ресурсы, что требует разработки специализированных программ поддержки.

Антикризисные стратегии в контексте цифровой трансформации требуют адаптации традиционных подходов к управлению кризисами с учетом специфики цифровой среды (рис. 2).

Таблица 4

Оценка готовности предприятий легкой промышленности Республики Таджикистан к внедрению адаптивных систем экономической безопасности

Критерии готовности	Крупные предприятия	Средние предприятия	Малые предприятия	Средний показатель
Технологическая инфраструктура	7,2	5,4	3,1	4,2
Финансовые ресурсы	6,8	4,9	2,8	3,9
Кадровые компетенции	6,5	4,2	2,5	3,6
Управленческая поддержка	7,8	6,1	4,3	5,4
Организационная культура	6,9	5,2	3,7	4,8
Интеграционные возможности	5,9	4,1	2,9	3,8
Итоговый индекс готовности	6,9	5,0	3,2	4,3

Оценка проводилась по 10-балльной шкале. Составлено автором на основе экспертных оценок состояния цифровизации предприятий легкой промышленности Таджикистана

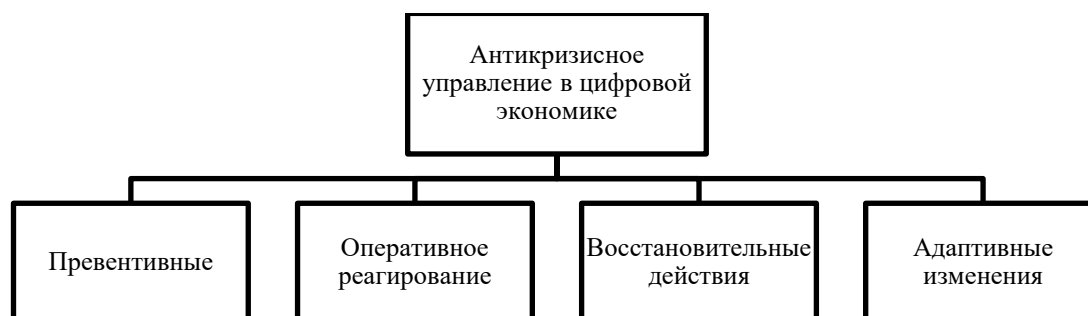


Рисунок 2. Модель антикризисного управления предприятиями легкой промышленности в условиях цифровой трансформации (составлено автором)

Представленная модель отражает циклический характер антикризисного управления в цифровой среде, где каждый этап обогащается возможностями цифровых технологий. Особенностью данного подхода является интеграция элементов машинного обучения и искусственного интеллекта, позволяющих системе постоянно совершенствоваться на основе накопленного опыта.

Экономическая эффективность внедрения цифровых технологий для обеспечения экономической безопасности характеризуется существенным разбросом показателей в зависимости от масштаба и сложности реализуемых проектов (табл. 5).

Таблица 5

Экономическая эффективность внедрения цифровых технологий экономической безопасности

Технологическое решение	Первоначальные инвестиции, тыс. USD	Годовая экономия, тыс. USD	Срок окупаемости, лет	ROI, %	Снижение рисков, %
Базовые системы кибербезопасности	25–50	15–30	1,5–2,0	40–60	70–80
ERP-системы с модулями безопасности	100–200	50–80	1,5–2,5	35–50	50–60
IoT-мониторинг производства	75–150	40–70	1,8–2,2	45–65	60–70
Системы предиктивной аналитики	150–300	80–120	1,5–2,5	50–70	65–75
Комплексные цифровые платформы	500–1 000	200–350	2,0–3,0	35–55	80–90

Составлено автором

Анализ экономической эффективности показывает, что инвестиции в цифровые технологии экономической безопасности характеризуются относительно быстрой окупаемостью и высокой рентабельностью. Особенно эффективными являются базовые системы кибербезопасности, которые при сравнительно небольших инвестициях обеспечивают существенное снижение рисков.

Стратегические рекомендации по развитию цифровой экосистемы экономической безопасности предприятий легкой промышленности должны учитывать специфику национальной экономики и ресурсные ограничения (табл. 6).

Таблица 6

**Стратегические рекомендации по развитию
цифровой экосистемы экономической безопасности**

Уровень воздействия	Рекомендации	Ответственные органы	Сроки реализации	Ожидаемые результаты
Национальный	Разработка национальной стратегии цифровизации легкой промышленности	Правительство, Минпромторг	2025–2027	Создание правовой базы, выделение бюджета
Отраслевой	Создание отраслевого центра цифровых компетенций	Министерство промышленности	2025–2026	Координация проектов, обучение кадров
Региональный	Формирование технопарков и инкубаторов	Региональные администрации	2025–2028	Концентрация ресурсов, синергия проектов
Корпоративный	Внедрение корпоративных программ цифровизации	Руководство предприятий	2025–2030	Повышение эффективности, снижение рисков
Международный	Развитие международного сотрудничества в области цифровизации	МИД, международные организации	2025–2030	Доступ к технологиям, обмен опытом

Составлено автором

Представленные рекомендации предполагают скоординированное воздействие на различных уровнях управления для создания благоприятной экосистемы цифровой трансформации. Ключевым элементом успеха является обеспечение межуровневой координации и синхронизации усилий всех участников процесса.

Выводы

По результатам решения первой задачи исследования установлено, что современные тенденции цифровизации промышленных предприятий характеризуются переходом к комплексным цифровым экосистемам, интегрирующим технологии искусственного интеллекта, больших данных, интернета вещей и блокчейн-решений. Анализ влияния цифровизации на систему экономической безопасности выявил двойственный характер данного процесса: с одной стороны, цифровые технологии создают новые возможности для предиктивного анализа угроз и автоматизации защитных мер, с другой стороны, порождают принципиально новые типы киберугроз, экономический ущерб от которых для промышленных предприятий в среднем составляет \$380 тысяч за инцидент.

В рамках второй задачи выявлена специфика цифровых угроз для предприятий легкой промышленности в условиях развивающейся экономики, характеризующаяся ростом киберинцидентов на 68 % в 2024 году по сравнению с предыдущим годом. Особенно критичным является увеличение атак программ-вымогателей на 98 %, что представляет серьезную угрозу для непрерывности производственных процессов. Анализ готовности предприятий Таджикистана к противодействию цифровым угрозам показал существенную дифференциацию по размерам предприятий: итоговый индекс готовности составляет 6,9 балла для крупных предприятий против 3,2 балла для малых предприятий. Результатом решения третьей задачи стала разработка модели адаптивной системы управления экономической безопасностью, интегрирующей четыре уровня: сбор данных, обработка и анализ, принятие решений и исполнение. Модель обеспечивает замкнутый цикл управления безопасностью с возможностью машинного обучения и постоянного совершенствования алгоритмов защиты. Экономическая эффективность внедрения цифровых технологий экономической безопасности характеризуется сроком окупаемости от 1,5 до 3,0 лет и уровнем ROI от 35 % до 70 % в зависимости от сложности реализуемых решений.

Общие выводы исследования подтверждают гипотезу о критической важности цифровой трансформации для обеспечения устойчивости экономической безопасности предприятий легкой промышленности в условиях современных кризисных вызовов. Установлено, что успешная реализация стратегий цифровизации требует скоординированных усилий на национальном, отраслевом, региональном и корпоративном уровнях при одновременном преодолении финансовых, технических, организационных и регуляторных барьеров. Формирование цифровой экосистемы экономической безопасности должно стать приоритетным направлением развития легкой промышленности Таджикистана в контексте реализации национальной стратегии цифровой экономики и укрепления конкурентоспособности отрасли на международных рынках.

ЛИТЕРАТУРА

1. Юсупова, М.А. Роль промышленности в национальной экономике Таджикистана / М.А. Юсупова — DOI 10.31483/r-112884. // Право, экономика и управление: состояние, проблемы и перспективы: материалы Всероссийской научно-практической конференции с международным участием, Чебоксары, 22 августа 2024 года. — Чебоксары: Общество с ограниченной ответственностью «Издательский дом «Среда», 2024. — С. 83–88 — EDN ZTHFTX.
2. Бобошоев, Ш.М. Экономические условия развития реального сектора экономики в Республике Таджикистан / Ш.М. Бобошоев // Ученые записки Худжандского государственного университета им. академика Б. Гафурова. Серия: Естественные и экономические науки. — 2015. — № 3(34). — С. 115–121. — EDN WAAKRZ.
3. Базаров, Ш.Ш. Легкая промышленность Таджикистана: современное состояние и перспективы развития / Ш.Ш. Базаров, Б.Б. Махкамов // Вестник Таджикского национального университета. Серия социально-экономических и общественных наук. — 2016. — № 2/6(210). — С. 141–148. — EDN XVFZLJ.
4. Зияева, М.Д. Роль предпринимательских структур в развитии промышленности Республики Таджикистан / М.Д. Зияева // Таджикистан и современный мир. — 2022. — № 3(79). — С. 177–186. — EDN CPERWS.
5. Абдукодилов, Х.А. Пути повышения инфраструктуры государственно-частного партнерства в национальной экономике / Х.А. Абдукодилов, М.К. Саидов // Глобальная экономика и национальная безопасность. — 2021. — № 3. — С. 3–13. — EDN VKWZWR.
6. Асрорзода, У.С. Искусственный интеллект в малом и среднем бизнесе Таджикистана: от автоматизации к стратегическому развитию / У.С. Асрорзода, Б.Б. Болтаев // Вестник Таджикского государственного университета коммерции. — 2025. — № 1(56). — EDN ORTUKZ.
7. Коваленко, Г.В. Значение проекта евразийской интеграции во внешней политике Республики Таджикистан / Г.В. Коваленко, Н.Б. Хатамов // Вестник Таджикского национального университета. — 2018. — № 8. — С. 13–18. — EDN LCYKVF.
8. Мирсаидов, А.Б. Механизмы формирования и развития инновационных региональных промышленных систем в Республике Таджикистан / А.Б. Мирсаидов, О.К. Муртазов. — Душанбе: Институт экономики и демографии Национальной академии наук Таджикистана, 2020. — 231 с. — EDN DPTPVS.

9. Кодиров, Ф.А. Конкурентоспособность промышленных предприятий в контексте перехода к цифровой экономике / Ф.А. Кодиров, Е.Ш. Мирзоева // Финансово-экономический вестник. — 2022. — № 4-2(34). — С. 218–228. — EDN UKRFAL.
10. Аминов, И. Национальные особенности и отраслевые проблемы развития предпринимательства в Республике Таджикистан / И. Аминов, Х.И. Аминов // Таджикистан и современный мир. — 2018. — № 3(62). — С. 25–39. — EDN IRDTII.

Ashurzoda Ashur Nurullo

Tajik Technical University named after academician M.S. Osimi, Dushanbe, Republic of Tajikistan
E-mail: aashurzoda1968@gmail.com

Digital transformation as a factor in the sustainability of economic security of light industry enterprises in the context of crisis phenomena (using the Republic of Tajikistan as an example)

Abstract. The study reveals the conceptual foundations of the use of digital technologies as a strategic tool for ensuring the economic security of light industry enterprises in the context of modern crisis challenges and economic uncertainty. The paper presents a comprehensive analysis of digital transformation processes as a catalyst for increasing the resilience of industrial enterprises to external and internal threats to economic security. The study reveals critical aspects of the implementation of digital solutions in the anti-crisis management system of light industry enterprises in the Republic of Tajikistan, where this industry demonstrates a leading position in the Central Asian region with a growth rate of 19 % in 2023. It has been established that digitalization of production processes creates new opportunities for the preventive detection of economic security threats through real-time monitoring systems, automated risk analysis and predictive modeling. Specific cyber threats and digital risks characteristic of light industry enterprises in developing economies have been identified, including an insufficient level of cyber protection, limited personnel competencies in the field of information security, and dependence on imported technological solutions. A conceptual model of an adaptive system for managing the economic security of light industry enterprises has been developed, integrating digital technologies of artificial intelligence, big data, the Internet of things and blockchain solutions to increase resilience to crises. Priority areas of digital transformation of enterprises in the industry in the context of forming anti-crisis resilience have been identified, including automation of early warning systems, implementation of predictive analytics technologies, creation of digital twins of production processes and formation of an ecosystem of digital interaction with suppliers and consumers. The study substantiates the need to form a national strategy for digitalization of the light industry as a basis for strengthening the economic security of the industry in the long term.

Keywords: digital transformation; economic security; light industry; anti-crisis management; cyber threats; adaptive management; digital technologies; artificial intelligence; predictive analytics; enterprise resilience