

# Теоретико-методологические вопросы стратегического управления экономической безопасностью в контексте цифровой трансформации экономики

**Тарханова Нина Алексеевна** 

Кандидат экономических наук, доцент

Донбасская национальная академия строительства и архитектуры, г. Макеевка, Россия

E-mail: n.a.tarhanova@donnasa.ru

**Норкина Татьяна Павловна** 

Старший преподаватель

Донбасская национальная академия строительства и архитектуры, г. Макеевка, Россия

E-mail: t.p.norkina@donnasa.ru

**Шестопалова Людмила Валентиновна** 

Старший преподаватель

Донбасская национальная академия строительства и архитектуры, г. Макеевка, Россия

E-mail: l.v.shestopalova@donnasa.ru

## КЛЮЧЕВЫЕ СЛОВА

цифровая экономика, экономическая безопасность, угрозы, риски, цифровая инфраструктура, кибербезопасность, стратегическое управление, цифровые технологии

## АННОТАЦИЯ

Целью данной статьи является развитие теоретико-методологических основ обеспечения экономической безопасности в условиях цифровой трансформации хозяйственных систем. Актуальность работы обусловлена недостаточной адаптацией существующих концептуальных подходов к управлению экономической безопасностью в условиях цифровой трансформации экономики, что требует пересмотра ряда устоявшихся положений экономической теории. Объектом исследования выступает система гарантирования экономической безопасности в процессе цифровизации национального хозяйства. Предметом исследования являются организационно-экономические отношения, возникающие в процессе активизации потенциальных возможностей и нейтрализации угроз экономической безопасности под влиянием цифровой трансформации. В статье осуществлен теоретический анализ категориального аппарата исследуемой предметной области, а именно содержание дефиниций «цифровая экономика» и «экономическая безопасность». По итогам проведенного анализа авторами предложена уточненная трактовка цифровой экономики, под которой предлагается понимать институционально-технологическую среду воспроизводственного процесса, где ключевым фактором производства выступают данные, представленные в цифровом формате. В статье экономическая безопасность трактуется как сложная, многокомпонентная категория, интегрирующая комплекс условий и факторов, необходимых для поддержания устойчивого развития национальной экономики. В ходе исследования предложена авторская расширенная классификация видов экономической безопасности в соответствии с функциональным критерием. Выполнен компаративный анализ парадигм традиционной и цифровой экономики, а также рассмотрено трансформирующее влияние цифровых технологий на состояние защищенности экономической системы. Осуществлена систематизация рисков и вызовов экономической безопасности, возникающих в процессе цифровой трансформации. Проанализированы современные теоретические подходы к управлению экономической безопасностью, на основе чего аргументирована необходимость применения стратегического подхода в условиях цифровизации. Разработана концептуальная модель процесса стратегического управления обеспечением экономической безопасности, ключевой особенностью которой выступает интеграция адаптивного и антиципативного контуров управления, позволяющих своевременно реагировать на изменения внешней среды и прогнозировать потенциальные угрозы. Научная новизна проведенного исследования состоит в развитии категориального

аппарата теории экономической безопасности, систематизации возможностей и угроз для защищенности экономики в условиях ее цифровизации, а также в разработке модели процесса стратегического управления экономической безопасностью, адаптированного к реалиям цифровой трансформации. Практическая значимость полученных результатов определяется возможностью их использования в процессе формирования корпоративных стратегий обеспечения экономической безопасности хозяйствующих субъектов в контексте цифровизации их бизнес-процессов.

JEL codes: O32, D81, L52, F52, C61

DOI: <https://doi.org/10.52957/2221-3260-2026-4-110-127>

Для цитирования: Тарханова, Н.А. Теоретико-методологические вопросы стратегического управления экономической безопасностью в контексте цифровой трансформации экономики / Н.А. Тарханова, Т.П. Норкина, Л.В. Шестопалова. – Текст : электронный // Теоретическая экономика. – 2026. – № 4. – С.110-127. – URL: <http://www.theoreticaleconomy.ru> (дата публикации: 30.04.2026).

## Введение

Устойчивость социально-экономического развития и состояние защищенности национальной экономики находятся в прямой зависимости от решения широкого круга актуальных проблем современности. Важнейшим фактором, детерминирующим данную взаимосвязь, выступают цифровые технологии, оказывающие бинарное (как позитивное, так и негативное) влияние на экономическую безопасность [8, 25]. Интеграция производственных мощностей с цифровыми системами ведет к формированию сложных производственно-технологических сетей, что актуализирует необходимость углубленного изучения воздействия цифровизации на параметры экономической безопасности. Значительная часть отечественных предприятий в новых условиях продолжает руководствоваться устаревшей парадигмой управления в данной сфере. В связи с этим формирование обновленной философии управления экономической безопасностью, ориентированной на качественные преобразования в контексте цифровой трансформации, приобретает высокую теоретическую и практическую значимость.

Исследованию влияния цифровых технологий на экономическую безопасность посвящены труды многих отечественных и зарубежных учёных. Среди российских исследователей, внесших вклад в разработку данной проблематики, следует отметить А. Дмитриев, Л. В. Ганич, Е. Е. Иродова, А. М. Соколова, Л. Е. Красильникова, Е. Д. Баландин, Н. А. Арефьев, М. С. Оборин, М.Д. Воротов, О. Н. Кутайцева, О. В. Толмачева, А. А. Толмачев, В. Л. Поздеев, Е. К. Карпунина, Т. Г. Соболевская и др. [3, 4, 5, 7, 8, 10, 13, 14, 19, 25]. Из зарубежных авторов весомый вклад в изучение данной предметной области внесли Дон Тапскотт, Х. Альбах, И. Ансофф, Б. Бертон, Вонг Чу, П. Догерти, Р. Липси, М. Кникрем, С. Маркович, Х. Мефферт, К. Шваб и др. [24, 25].

В работах указанных авторов проанализированы преимущества, потенциальные риски и угрозы, сопряженные с цифровой трансформацией экономики, а также рассмотрены их влияние на состояние экономической безопасности. Вместе с тем, отдельные аспекты проблемы остаются недостаточно разработанными. В частности, речь идёт о теоретико-методологических основах обеспечения экономической безопасности в условиях поступательного развития цифровой экономики, а также о дефиците комплексных моделей стратегического управления, интегрирующих адаптивный и превентивный инструментарий.

## Материал и методы исследования

Теоретико-методологический базис настоящего исследования сформирован на основе фундаментальных положений теории экономической безопасности, концептуальных разработок в области стратегического менеджмента, а также институциональной экономической теории [1, 17, 23]. Методологический инструментарий включает применение системного и сравнительного

анализа, метода научной абстракции, классификационного подхода, SWOT-анализа, а также методов моделирования экономических явлений и процессов. Эмпирическую основу исследования образуют данные Федеральной службы государственной статистики РФ, АНО «Цифровая экономика» [15], статистические и аналитические публикации Национального исследовательского университета «Высшая школа экономики» [22], а также открытые аналитические отчеты международных организаций, включая ОЭСР и Всемирный банк.

Целевая установка исследования заключается в развитии теоретико-методологических положений стратегического управления экономической безопасностью применительно к условиям цифровой трансформации национальной экономики.

Для достижения поставленной цели в работе определен следующий круг задач:

- осуществить анализ существующих концептуальных подходов к трактовке цифровой трансформации, провести систематизацию и компаративный анализ характеристик традиционной и цифровой экономики;
- исследовать характер воздействия цифровых технологий на состояние экономической безопасности;
- аргументировать необходимость применения стратегического подхода к управлению экономической безопасностью в контексте цифровизации;
- разработать модель процесса стратегического управления обеспечением экономической безопасности в условиях цифровой трансформации.

Выявление вектора влияния цифровизации на состояние экономической безопасности требует предварительного уточнения категориально-понятийного аппарата исследования. Термин «цифровая экономика» в современной научной литературе характеризуется отсутствием единой, общепринятой интерпретации, то есть является полисемантическим. Основоположником понятия принято считать Д. Тапскотта, который в 1995 году охарактеризовал её как экономику, базирующуюся на сетевом интеллекте [27].

Обобщение и систематизация работ отечественных и зарубежных исследователей, в числе которых К. Шваб, М.А. Эскиндаров, В.Г. Халин, Л.В. Ганич [3, 5, 24, 27], позволяет выделить несколько основных подходов к определению исследуемой категории:

- технологический подход, в рамках которого цифровая экономика рассматривается как совокупность сквозных цифровых технологий;
- процессный подход, интерпретирующий её как метод организации и управления бизнес-процессами;
- платформенный подход, трактующий цифровую экономику как среду взаимодействия экономических агентов и создания добавленной стоимости;
- институциональный подход, акцентирующий внимание на формировании новой системы правил, норм и механизмов хозяйствования.

Критический анализ представленных дефиниций показывает, что в большинстве из них фиксируется преимущественно инструментальная сторона рассматриваемого феномена, тогда как институциональные изменения, сопровождающие цифровую трансформацию, остаются за рамками исследования. С позиции авторов, цифровую экономику целесообразно рассматривать как институционально-технологическую среду воспроизводства, где ключевым фактором производства выступают данные в цифровой форме, а их обработка и анализ обеспечивают существенное снижение транзакционных издержек и генерацию сетевых эффектов. Предлагаемая трактовка, в отличие от рассмотренных выше, акцентирует внимание не только на технологической составляющей, но и на трансформации экономических отношений, то есть институциональной структуры хозяйствования.

Для обеспечения методологической корректности последующего анализа принципиальное значение имеет дифференциация смежных, но не тождественных понятий. В современном научном дискурсе такие термины, как «оцифровка» (технический процесс конвертации данных из аналоговой

формы в цифровую), «цифровизация» (оптимизация бизнес-процессов на основе внедрения цифровых технологий) и «цифровая трансформация» (комплексная перестройка бизнес-модели, организационной культуры и ценностного предложения), нередко употребляются как синонимичные, что представляется методологически некорректным.

Согласно позиции, разделяемой большинством исследователей, под оцифровкой следует понимать процесс перевода аналоговой информации в цифровой формат, тогда как цифровизация представляет собой более емкую категорию, отражающую качественные изменения в социальных, экономических и политических процессах. В свою очередь, цифровая трансформация выступает наиболее масштабным процессом, предполагающим фундаментальное переосмысление всех аспектов функционирования экономических систем с учетом культурных, социальных и организационных особенностей на основе реализации системного подхода [4, 5, 18, 25].

Применительно к уровню хозяйствующего субъекта цифровая трансформация бизнеса означает не просто внедрение новейших цифровых технологий, но и радикальное изменение подходов к их использованию, кардинальную ревизию сложившихся практик [12, 18]. Следует также отметить, что цифровые трансформации выступили фактором формирования нового поколения пользователей и потребителей, чьи поведенческие паттерны и ожидания существенно отличаются от предшествующих когорт.

Резюмируя изложенное, можно констатировать, что если цифровизация представляет собой определенные сдвиги в промышленности и бизнесе, возникающие вследствие применения цифровых технологий, то цифровая трансформация знаменует собой глубинные, системные изменения в обществе, являющиеся результатом развертывания цифровизационных процессов.

В последние годы наблюдается устойчивая тенденция к увеличению доли цифрового сектора в структуре валового внутреннего продукта (ВВП). Согласно расчетам АНО «Цифровая экономика», выполненным в 2024 году на основе обновленной методики, базирующейся на реестре аккредитованных ИТ-компаний, вклад отрасли в ВВП России по итогам 2024 года составил 6% [15, 22]. Данный показатель существенно превышает ранее публиковавшиеся оценки Института статистических исследований и экономики знаний НИУ ВШЭ (2,43%), что обусловлено расширением круга учитываемых субъектов, включая издателей игрового контента, образовательные онлайн-платформы, организации электронной торговли и системных интеграторов). По итогам первого полугодия 2025 года поступления налогов и страховых взносов от ИТ-сектора возросли на 20%, численность занятых в отрасли достигла 1,497 млн человек (3,1% от общей занятости), а среднемесячная номинальная заработная плата превысила 190 тыс. руб. [22]. К числу ключевых трендов развития отрасли сохраняются импортозамещение программного обеспечения и аппаратных средств, углубление разработок в области сквозных технологий (искусственный интеллект, большие данные, кибербезопасность), а также наращивание экспортного потенциала отечественных цифровых решений.

Наряду с позитивными сдвигами сохраняется актуальность проблемы цифрового неравенства. Исследование, проведенное платформой hh.ru (2025) демонстрирует, что спрос на ключевые цифровые компетенции (владение SQL, Python, Linux) на 59% сконцентрирован в Москве, что свидетельствует о сохраняющемся «цифровом разрыве» между столичными агломерациями и регионами [6]. Реализуемые государственные программы, включая национальный проект «Цифровая экономика» (2019-2024 гг.) и сменяющий его с 2025 года национальный проект «Экономика данных и цифровая трансформация государства», нацелены на преодоление указанных диспропорций и обеспечение равного доступа к цифровой инфраструктуре [15].

Цифровая экономика демонстрирует принципиальные отличия от традиционной модели хозяйствования, систематизированные в таблице 1.

В традиционной экономической модели в качестве основного ресурса выступают средства производства, включая трудовые ресурсы. В цифровой экономике доминирующим ресурсом

становится информация, соответствующая требованиям полноты, достоверности, точности и оперативного поступления. Трансформации подвергается и характер конкурентной борьбы: соперничество смещается из сферы производства продуктов в плоскость обладания системами управления, функционирующими на базе цифровых платформ.

**Таблица 1** – Сравнительная характеристика цифровой и традиционной экономики [5, 27]

Признак	Традиционная экономика	Цифровая экономика
Основной ресурс экономики	Средства производства	Информация
Преобладающий тип хозяйственных связей	Иерархический тип связи	Основой хозяйственных связей является использование платформ
Конкуренция	За производство и сбыт товаров и услуг	За системы управления на базе цифровых платформ
Сбыт продуктов	Большое количество посредников	Отсутствие посредников. Сбыт продуктов основан на бизнес-модели М2С: производитель - потребитель
Рынок	Выход преимущественно на локальные, региональные, национальные рынки	Выход преимущественно на глобальный рынок. Формирование цифрового рынка труда как отдельного сектора рынка
Темпы изменения в экономике	Относительно медленные	Ускоренные темпы

Специфика информации как ресурса заключается в возможности ее многократного использования, что выгодно отличает ее от традиционных факторов производства. Вместе с тем на современном этапе цифрового развития определяющее значение сохраняет человеческий ресурс, поскольку акценты смещаются в область нематериального производства и интеллектуальной собственности, где конкурентные преимущества формируются благодаря знаниям, компетенциям и практическому опыту работников. В этой связи показательно, что в Российской Федерации лишь 17 % занятых обладают высокой квалификацией, развитыми компетенциями и способностью к решению сложных когнитивных задач. Средний уровень квалификации, позволяющий решать рутинные когнитивные задачи, характерен для 48 % работающих, а низкий уровень квалификации демонстрируют 35 % занятых. Сложившаяся структура квалификационных характеристик работающего населения не соответствует критериям, необходимым для вхождения России в группу стран с развитой цифровой экономикой. Проблема острого дефицита кадров, обладающих развитыми цифровыми и когнитивными компетенциями, требует безотлагательного решения на государственном уровне.

В Российской Федерации сформирована система государственного регулирования, направленная на повышение уровня цифровых компетенций, которая включает реализацию национальных и федеральных проектов, разработку образовательных программ, а также меры поддержки специалистов, занятых в сфере цифровых технологий. Национальный проект «Цифровая экономика», реализация которого осуществлялась в период с 2019 по 2024 год был ориентирован на ускоренное внедрение цифровых технологий в экономику и социальную сферу, формирование благоприятных условий для развития высокотехнологичного предпринимательства и повышение глобальной конкурентоспособности страны. В рамках данного проекта предусматривались мероприятия по подготовке квалифицированных кадров для цифровой экономики, а также ряд федеральных проектов, создававших инфраструктурные и институциональные возможности для

развития соответствующих компетенций.

### Результаты исследования

Анализ показывает, что на состояние экономической безопасности в условиях цифровизации оказывают воздействие две основные группы факторов:

- 1) характер реализуемых моделей управления;
- 2) ключевые проблемы, сопровождающие развития цифровой экономики.

Реализуемые в России и ее регионах программы развития цифровой экономики ориентированы на применение программно-прогностической модели управления экономической безопасностью, приходящей на смену традиционной программно-целевой модели. Сложившаяся система и методы управления, использовавшиеся в предшествующий период, во многих случаях демонстрируют ограниченную эффективность при решении задач обеспечения экономической безопасности в условиях цифровой трансформации.

К числу основных проблем, препятствующих развитию цифровой экономики и создающих угрозы экономической безопасности, относятся:

- недостаточный уровень цифровой грамотности населения, порождающий феномен цифрового неравенства, который негативно сказывается на динамике социально-экономического развития страны;

- повышение требований к компетенциям работников, обусловленное широким распространением информационных технологий, что создает барьеры для определенных категорий граждан, не обладающих необходимыми навыками;

- высвобождение рабочей силы вследствие автоматизации и внедрения цифровых технологий, что порождает проблему трансформации занятости и требует значительных инвестиций в развитие альтернативных сфер приложения труда, включая индустрию отдыха;

- учащение кибератак, повышение уязвимости государственных информационных систем, значительный экономический ущерб от киберпреступлений [4, 8, 25].

Совокупность обозначенных проблем, находящихся в тесной взаимосвязи, формирует системный вызов для обеспечения экономической безопасности. Анализ отечественной и зарубежной экономической литературы показывает, что в настоящее время отсутствует общепринятая дефиниция категории «экономическая безопасность». Первая группа исследователей трактует экономическую безопасность как комплекс экономических, экологических, геополитических и иных условий, обеспечивающих защищенность национальной экономики от деструктивных воздействий и создающих предпосылки для устойчивого развития. Представители второго подхода рассматривают экономическую безопасность как такое состояние экономической системы, которое позволяет проводить суверенную экономическую политику и гарантировать защиту национальных интересов. Третье направление научной мысли акцентирует внимание на независимости и неуязвимости экономических интересов по отношению к потенциальным внутренним и внешним угрозам [17].

С позиции авторов, экономическую безопасность правомерно рассматривать как сложную, многоаспектную категорию, выражающую систему экономических отношений, складывающихся по поводу формирования условий и факторов, обеспечивающих независимое и устойчивое функционирование национальной экономики, а также её способность к перманентному самосовершенствованию.

В традиционной классификации экономической безопасности по функциональному признаку принято выделять информационную, финансовую, экологическую, технологическую, кадровую, правовую составляющие [4, 8, 25]. Представляется, что применительно к современному этапу экономического развития, данный перечень нуждается в дополнении следующими компонентами: добавить кибербезопасность, понимаемая как состояние защищенности цифровых данных, устройств и информационных ресурсов; инновационная безопасность, отражающая способность экономической системы к генерации и внедрению инноваций; инфраструктурная безопасность,

характеризующая уровень развития цифровой инфраструктуры. Включение указанных элементов в классификацию представляется критически значимым, поскольку именно состояние цифровой инфраструктуры и способность к инновационному развитию в определяющей мере обуславливают устойчивость хозяйственной системы к современным вызовам и угрозам.

Проблема классификации экономической безопасности нуждается в углубленной проработке, что позволит более точно идентифицировать ее содержание и структурные элементы. Среди различных видов национальной безопасности экономическая безопасность занимает приоритетное положение, поскольку она непосредственно детерминирует стабильное функционирование национальной экономики и ее отдельных секторов.

При раскрытии сущности и содержания категории «экономическая безопасность предприятия», сложившиеся в научной литературе подходы могут быть сгруппированы в два основных концептуальных направления. Первый подход базируется на противодействии угрозам, второй акцентирует внимание на сохранности собственности и эффективности ее использования. Представлены также синтетические позиции, интегрирующие оба указанных подхода, что представляется наиболее обоснованным, особенно с точки зрения практической реализации [1]. Характер мероприятий по обеспечению экономической безопасности предприятия, разрабатываемых и внедряемых на практике, непосредственно зависит от того, какое определение положено в основу соответствующей стратегии. Принятая трактовка экономической безопасности предопределяет прогнозируемые результаты, объем необходимых инвестиций и иных ресурсов, систему контроля издержек, а также распределение ответственности и функциональных обязанностей между структурными подразделениями предприятия. Экономическая безопасность предприятия представляет собой экономическую категорию, выражающую совокупность экономических отношений по поводу его защищенности от деструктивного воздействия внешних и внутренних угроз и дестабилизирующих факторов, что обеспечивает устойчивую реализацию интересов, запланированных результатов и целевых установок. В данной трактовке экономическая безопасность предприятия раскрывается сквозь призму эффективного использования собственности и качества управления, которое предполагает своевременную идентификацию возникающих угроз и возможностей по их нейтрализации либо минимизации ущерба от их реализации.

В условиях цифровой трансформации хозяйствующего субъекта возникает объективная потребность в формировании комплексной системы обеспечения экономической безопасности, представляющей собой совокупность взаимосвязанных инженерно-технических, правовых, социально-экономических и организационных мероприятий, ориентированных на нейтрализацию реальных и потенциальных угроз [4, 13]. Концептуальная основа построения такой системы базируется на ряде принципов, к числу которых относятся: сочетание превентивных и реактивных мер, непрерывность функционирования, комплексный характер реализуемых мероприятий, экономическая обоснованность, дифференциация и координация действий, подконтрольность руководству, а также соответствие действующему законодательству.

Для целей оценки уровня экономической безопасности в условиях цифровизации экономической наукой разработаны и апробированы на практике различные методические подходы. Среди них выделяются статистический, аналитический, экспертный, нормативно-параметрический методы, а также методы прогнозирования и моделирования (таблица 2).

**Таблица 2** – Методы анализа и оценки экономической безопасности предприятия

Признак классификации	Методы анализа и оценки
Содержание	<ul style="list-style-type: none"> <li>- статистический</li> <li>- аналитический</li> <li>- экспертный</li> <li>- нормативно-параметрический</li> </ul>

Признак классификации	Методы анализа и оценки
	- прогнозирования и моделирования
Цели	- циклический - системный - структурный - процессный
Наличие информации и категория объекта собственности	- доходный - затратный - сравнительный
Используемые показатели	- индикативный - ресурсно-функциональный - ориентированный на принципы программно-целевого управления - ориентированный на взаимодействие с партнерами и клиентами

В зависимости от целевой направленности анализ экономической безопасности предприятий подразделяется на циклический, системный, инфраструктурный, процессный. В рамках оценки экономической безопасности в цифровой среде применяются разнообразные методики установления пороговых значений индикаторов. Наряду с этим существуют подходы к оценке экономической безопасности предприятия, дифференцируемые по используемой базе: доходный, затратный и сравнительный. По критерию применяемых показателей методы оценки и анализа экономической безопасности могут быть классифицированы следующим образом:

- индикативные методы, предполагающие использование системы индикаторов, трактуемых как пороговые значения показателей, характеризующих состояние защищенности предприятия. В рамках данного направления одни авторы обосновывают целесообразность применения многопороговой методики, предусматривающей введение для каждого индикатора нескольких пороговых уровней, которым соответствуют различные состояния (нормальное, умеренное, критическое, катастрофическое). В то же время большинство современных исследователей и практиков придерживаются однопорогового подхода, при котором фиксируются два состояния: нормальное и отклонение от нормы [19];

- ресурсно-функциональные методы, исходящие из предпосылки, что необходимый уровень экономической безопасности достигается в условиях наиболее эффективного использования ресурсного потенциала предприятия;

- методы, ориентированные на применение программно-целевого управления и математического аппарата, где в качестве критериального основания выступает интегрированная совокупность показателей;

- методы, ориентированные на взаимодействие с контрагентами и потребителями, при использовании которых критерием служит маржа безопасности.

Цифровая трансформация экономики характеризуется двойственным характером воздействия на состояние экономической безопасности [8, 10, 25]. Результаты применения методологии SWOT-анализа для оценки влияния цифровой экономики на экономическую безопасность систематизированы на рисунке 1.

S – Сильные стороны	W – Слабые стороны
<ol style="list-style-type: none"> <li>1. Повышение прозрачности и эффективности управленческих процессов.</li> <li>2. Формирование и усиление конкурентных преимуществ.</li> <li>3. Рост стабильности функционирования за счет оперативной идентификации и предупреждения потенциальных рисков и угроз.</li> <li>4. Создание новых инструментов и механизмов противодействия рискам.</li> <li>5. Минимизация масштабов теневой экономики.</li> <li>6. Усиление роли государства в сфере контроля финансовых операций.</li> <li>7. Совершенствование коммуникационного взаимодействия</li> <li>8. Повышение качества производимой продукции и предоставляемых услуг.</li> <li>9. Формирование более благоприятных условий трудовой деятельности.</li> </ol>	<ol style="list-style-type: none"> <li>1. Высокая стоимость внедрения и сопровождения цифровых технологий.</li> <li>2. Неравномерность развития цифровой инфраструктуры в региональном, отраслевом разрезе и на уровне отдельных предприятий.</li> <li>3. Дефицит квалифицированных кадров, обладающих необходимыми цифровыми компетенциями.</li> <li>4. Недостаточная разработанность нормативно-правовой базы, регулирующей цифровую сферу.</li> <li>5. Сохранение цифрового отставания от развитых зарубежных стран.</li> <li>6. Риск роста структурной безработицы вследствие углубления автоматизации и роботизации.</li> <li>7. Низкий уровень цифровой финансовой грамотности населения, непонимание специфики функционирования цифровой экономики.</li> </ol>
O – Возможности	T – Угрозы
<ol style="list-style-type: none"> <li>1. Повышение оперативности и качества принятия управленческих решений.</li> <li>2. Расширение возможностей сбора и анализа больших данных для обоснования решений.</li> <li>3. Увеличение потенциала достижения стратегических целей развития.</li> <li>4. Рост эффективности за счет существенного повышения производительности труда.</li> <li>5. Появление новых источников получения прибыли и создания стоимости.</li> <li>6. Сокращение численности работников, задействованных в цепочке создания ценности.</li> <li>7. Развитие новых бизнес-моделей.</li> <li>8. Улучшение доступа к информации и финансовым услугам.</li> <li>9. Формирование и развитие новых отраслей экономики.</li> <li>10. Расширение возможностей дистанционной занятости.</li> <li>11. Применение технологий цифровых двойников для моделирования и принятия эффективных управленческих решений.</li> </ol>	<ol style="list-style-type: none"> <li>1. Рост различных форм киберпреступности.</li> <li>2. Утечка коммерческой информации и данных, составляющих коммерческую тайну.</li> <li>3. Тенизация операций, осуществляемых в электронной форме.</li> <li>4. Сбои в функционировании финансовых и информационных систем.</li> <li>5. Возникновение угроз безопасности государства, предприятий и домохозяйств.</li> <li>6. Хищение персональных данных, несанкционированный доступ к защищенной информации, несанкционированное списание средств, манипулирование информационными потоками.</li> <li>7. Зависимость от зарубежных поставщиков программного обеспечения и оборудования, порождающая риски в сфере информационной безопасности.</li> <li>8. Алгоритмическая предвзятость, утрата человеческого контроля над процессами принятия решений.</li> <li>9. Уязвимости сетевой инфраструктуры.</li> </ol>

**Рисунок 1** – SWOT-анализ влияния цифровой экономики на экономическую безопасность

Проведенный SWOT-анализ позволяет констатировать наличие амбивалентного характера воздействия цифровой трансформации на экономическую безопасность. Ключевое противоречие проявляется в дихотомии: с одной стороны, повышение эффективности управленческих процессов

благодаря сквозной аналитике данных (сильные стороны), с другой стороны, возрастание энтропии экономической системы вследствие мультипликации векторов киберугроз (угрозы). Особо внимания заслуживает тот факт, что слабые стороны, в частности, дефицит кадров, обладающих цифровыми компетенциями, перестают носить исключительно операционный характер и трансформируются в разряд стратегических ограничителей, препятствующих достижению национальных целей развития [6, 8].

С одной стороны, информационно-коммуникационные технологии открывают новые возможности для повышения эффективности управления экономической безопасностью. Именно цифровая экономика и сопряженные с ней технологии формируют среду, в которой реализуется управление экономической безопасностью, и в современных условиях выступают в качестве ключевых факторов повышения ее уровня. Цифровая трансформация национального хозяйства способствует снижению степени воздействия внешних и внутренних угроз на деятельность экономических агентов, поскольку появляется возможность оперативного выявления и предупреждения потенциальных рисков, что закономерно повышает уровень стабильности функционирования экономической системы. В процессе цифровизации формируется система горизонтальных коммуникаций, обеспечивающая беспрепятственное движение информации по всем уровням управления. Возникает новая парадигма управления – цифровой менеджмент, представляющий собой систему управления, базирующуюся на использовании цифровых технологий в целях обеспечения экономической безопасности, устойчивого развития и повышения конкурентоспособности [21].

С другой стороны, цифровые технологии выступают источником возникновения новых рисков и угроз для государства, бизнес-структур и домохозяйств, что обуславливает необходимость разработки принципиально новых подходов к обеспечению экономической безопасности [4, 24, 25].

Интенсивное развитие цифровизации выступает источником не только новых возможностей, но также рисков и угроз для экономической безопасности национальной экономики [7, 10, 19]. Наряду с традиционными угрозами, включающими разглашение конфиденциальной информации и коммерческой тайны, несанкционированное вмешательство в функционирование информационных и финансовых систем, нарушение целостности баз данных, информационных ресурсов и технологий, в экономике появляются качественно новые угрозы, методы идентификации и нейтрализации которых пока не получили достаточной теоретической и практической проработки. К числу таких новых угроз относятся кибератаки различного характера, неправомерное разглашение персональных данных, внедрение вредоносного программного обеспечения, а также угрозы, сопряженные с обновлением компьютерного программного обеспечения. Указанные обстоятельства обуславливают необходимость широкого внедрения инновационных стратегий управления экономической безопасностью, учитывающих динамический характер цифровой экономики и ее высокую турбулентность.

Развитие системы управления экономической безопасностью предприятия представляет собой динамичный процесс трансформации состояния управленческой системы хозяйствующего субъекта под влиянием рисков и угроз, а также факторов внешней и внутренней среды, что предполагает формирование новых характеристик и свойств управленческой системы, адекватных складывающимся условиям [1, 4, 23].

Необходимо отметить, что в настоящее время отсутствует комплексный методический подход к оценке влияния цифровых технологий на динамику изменения уровня экономической безопасности в силу недостаточности статистических данных и отсутствия унифицированной системы показателей в сферах цифровизации и информатизации осуществить полномасштабную оценку воздействия цифровых технологий на экономическую безопасность на современном этапе не представляется возможным. При этом отдельные виды рисков экономической безопасности поддаются количественной оценке с использованием таких статистических показателей, как среднее квадратическое отклонение, дисперсия и коэффициент вариации [7].

В практике обеспечения экономической безопасности предприятия применяются различные управленческие подходы, среди которых можно выделить следующие: процессный подход, базирующийся на анализе последовательных этапов реализации бизнес-процессов; системный подход, рассматривающий управление экономической безопасностью как неотъемлемый компонент общей системы управления хозяйствующим субъектом; инновационный подход, ориентированный на внедрение новшеств в механизм обеспечения защищенности экономических интересов; проектный, предполагающий разработку и реализацию специализированных проектов в сфере экономической безопасности; адаптационный подход, заключающийся в приспособлении системы экономической безопасности к динамично изменяющимся факторам внешней и внутренней среды; ситуационный подход, основанный на формировании сценариев реагирования применительно к конкретным ситуациям. Каждый из перечисленных подходов обладает определенными достоинствами и ограничениями, что обуславливает целесообразность их комплексного применения. Вместе с тем современные реалии цифровой трансформации, характеризующиеся высокой степенью неопределенности, возрастанием рисков и изменчивостью факторов внешнего и внутреннего окружения, актуализируют необходимость использования стратегического подхода к обеспечению экономической безопасности, ориентированного на достижение долгосрочных целей развития. Ключевым элементом, развивающим и дополняющим данный подход, выступает внедрение концепции антиципативного управления. Согласно определению А. Штангрета и соавторов, антиципативное управление представляет собой систему мер, направленных на предвидение возможных трансформаций внешней и внутренней среды с целью формирования превентивных защитных механизмов. Интеграция антиципативного подхода в стратегическое управление экономической безопасностью обеспечивает возможность перехода от реактивной модели защиты, ориентированной на противодействие уже реализовавшимся угрозам, к проактивной модели, нацеленной на управление будущим состоянием защищенности объекта [10, 23].

Графическая интерпретация авторского подхода к стратегическому управлению экономической безопасностью в условиях цифровой трансформации представлена на рисунке 2.

Разработанная модель, в отличие от традиционных линейных схем, основывается на кибернетическом принципе организации управления с выделением двух контуров. Первый контур (оперативный) ориентирован на управление текущими рисками и реализуется посредством применения регламентных процедур. Второй контур (стратегический/адаптивный) нацелен на управление выявленными «разрывами» между желаемым (целевым) и фактическим уровнем защищенности. Функционирование данного контура предполагает корректировку стратегических ориентиров на основе анализа больших данных и применения инструментов предиктивной аналитики, а также реализацию превентивных защитных мероприятий.

Элементом научной новизны предлагаемой модели выступает включение блока «Антиципативное управление» в структуру стратегического выбора. Если адаптивное управление представляет собой реакцию на уже произошедшие изменения внешней среды, то антиципативное управление базируется на применении форсайт-технологий и выявлении «слабых сигналов» потенциальных угроз. Такой подход позволяет формировать превентивные механизмы защиты до момента актуализации рискованного события.

В ряду важнейших методологических проблем стратегического управления находится вопрос о разработке и четкой регламентации целевых ориентиров, задач, форм и содержания управленческих воздействий, направленных на обеспечение экономической безопасности в условиях цифровой трансформации [1, 23].

Как следует из представленной на рисунке 2 модели, исходным этапом стратегического управления выступает определение стратегических целей, поскольку именно они формируют основу для последующей разработки стратегии развития предприятия. Стратегический анализ ориентирован на идентификацию возможностей и угроз, обусловленных процессами цифровизации, а также

на выявление сильных и слабых сторон хозяйствующего субъекта (SWOT-анализ). Исследование внутренней среды предприятия позволяет диагностировать конкурентные преимущества, формирующиеся в результате внедрения цифровых технологий. Проведение качественного и количественного анализа рисков с их последующей оценкой служит базой для разработки сценариев развития потенциально опасных событий. Процесс выбора стратегии предполагает формирование альтернативных вариантов достижения поставленных целей, их сравнительную оценку и обоснованный выбор оптимальной стратегии, разработку стратегических планов, направленных на снижение рисков цифровизации, а также определение наиболее эффективных методов минимизации рисков. Реализация стратегии представляет собой ключевой этап, поскольку именно в ходе ее осуществления обеспечивается достижение целевых ориентиров. Практическая реализация стратегии осуществляется посредством разработки соответствующих планов, программ, бюджетов и процедур. Завершающим этапом процесса управления экономической безопасностью выступает непрерывный мониторинг и систематический контроль, а также своевременная корректировка стратегии в ответ на изменения внешней и внутренней среды.

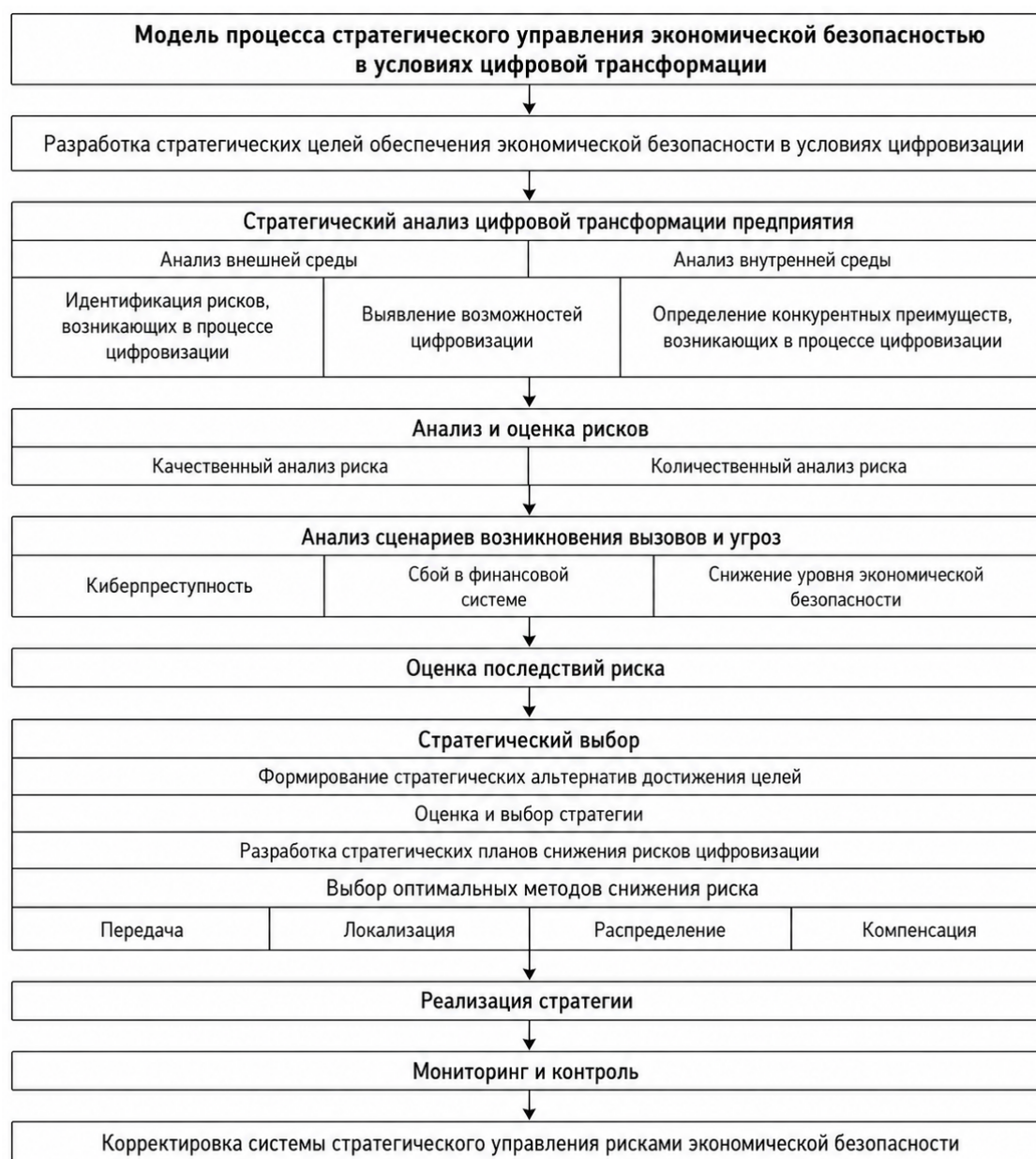


Рисунок 2 – Модель процесса стратегического управления экономической безопасностью в

## условиях цифровой трансформации

Анализ специальной литературы и результатов научных исследований свидетельствует о том, что у значительной части отечественных предприятий отсутствуют сформированные стратегические ориентиры развития системы управления экономической безопасностью в условиях цифровизации, равно как и регламенты реагирования на возникающие угрозы [9, 13].

Под стратегическими ориентирами в данном контексте понимается совокупность регламентов, правил и стандартов, образующих основу для принятия обоснованных управленческих решений и реализации соответствующих мероприятий. Ключевой целью формирования стратегии управления экономической безопасностью в условиях цифровой трансформации выступает повышение конкурентоспособности и наращивание конкурентных преимуществ предприятия на основе формирования надежной системы защиты от угроз и рисков.

Реализация стратегического подхода к управлению экономической безопасностью предполагает формирования интегрированных систем мониторинга и механизмов своевременного реагирования на возникающие угрозы [2, 4]. Архитектура адаптивно ориентированных стратегий управления экономической безопасностью должна базироваться на принципах непрерывного отслеживания динамики внешней и внутренней среды, а также оперативной корректировки стратегических установок в соответствии с изменяющимся ландшафтом рисков и вызовов.

Ключевым фактором, обуславливающим несовершенство действующих систем управления экономической безопасностью на предприятиях в условиях цифровизации, выступает неадекватность применяемых методов и несвоевременность их выбора, что препятствует принятию эффективных управленческих решений. Хозяйствующие субъекты сталкиваются с дефицитом релевантного опыта в части выбора и применения методов управления экономической безопасностью. Цифровая трансформация диктует необходимость применения проактивных методов управления, ориентированных на предупреждение угроз. Представляется обоснованной разработка и внедрение систем мониторинга и анализа рисков, обеспечивающих возможность оперативного реагирования на возникающие угрозы и предотвращения их негативных последствий.

Мониторинг экономической безопасности представляет собой систему комплексного отслеживания, сбора, обработки и анализа информации о состоянии защищенности экономической системы и факторах, оказывающих влияние на ее динамику [2, 14]. Функционирование системы мониторинга базируется на ряде принципов, включающих цифровизацию, непрерывность, прозрачность, интеграцию и аналитическую направленность. В условиях цифровой трансформации экономики представляется целесообразным разработка и практическое внедрение автоматизированной системы мониторинга экономической безопасности, что позволит органам власти и управления своевременно получать актуальную информацию о состоянии защищенности, идентифицировать потенциальные угрозы и принимать оперативные меры по их нейтрализации. Автоматизированная система мониторинга экономической безопасности выступает в качестве эффективного инструмента обеспечения защищенности национальной экономики. Применение подобной системы будет способствовать повышению эффективности управления экономикой на национальном уровне и снижению вероятности реализации угроз экономической безопасности.

Стратегическое управление экономической безопасностью представляет собой процесс формирования долгосрочных ориентиров обеспечения защищенности хозяйственной системы путем разработки стратегии, адаптированной к динамично трансформирующимся факторам внешнего и внутреннего окружения [1, 23]. Применение стратегического подхода позволяет идентифицировать потенциальные угрозы и вызовы на ранних стадиях их возникновения, исключает принятие решений, ориентированных исключительно на краткосрочную целесообразность, а также способствует существенному снижению неопределенности, порождаемой цифровой средой, и минимизации ее негативных последствий для хозяйствующего субъекта. Достижение максимальной результативности стратегического управления экономической безопасностью требует его гибкости и базирования

на инновационных технологических решениях, включая генеративный искусственный интеллект, технологии машинного обучения, обработку больших данных и аналитику, а также распределенные реестры (блокчейн).

Наряду с адаптивным управлением экономической безопасностью целесообразно применение инструментов антиципативного управления. Если адаптивное управление предполагает реализацию комплекса мероприятий, направленных на приспособление системы к изменяющимся условиям внешней среды, то антиципативное управление ориентировано на осуществление защитных мер, имеющих целью предотвращение возникновения либо снижение негативного воздействия факторов внешней и внутренней среды на состояние экономической безопасности. В основе антиципативного подхода лежат экспертные методы, экономико-математическое моделирование, прогнозирование и реализация превентивных защитных механизмов [10, 23].

Необходимо подчеркнуть, что разработка стратегии управления экономической безопасностью в условиях цифровизации является необходимым, но недостаточным условием. Требуется модернизация механизма реализации стратегии, формирование эффективной системы оценки и контроля принимаемых решений, выделение в организационной структуре предприятия специализированного подразделения либо назначение ответственного лица, на которое возлагаются функции по организации управления экономической безопасностью, а также выделение соответствующих финансовых средств и создание специальных резервов, обеспечивающих реализацию управленческих механизмов. Существенную роль играет институциональная поддержка экономической безопасности, призванная обеспечить: совершенствование нормативно-правового регулирования процессов цифровой трансформации; развитие национальной цифровой инфраструктуры; создание цифровых платформ, ориентированных на сбор, анализ и мониторинга показателей экономической безопасности; стимулирование научных исследований в области цифровизации и ее влияния на экономическую безопасность; качественную подготовку специалистов обладающих компетенциями в сфере информационных технологий; развитие международного сотрудничества в противодействии киберпреступности и иным транснациональным угрозам экономической безопасности.

## **Выводы**

Проведенное исследование позволяет заключить, что интеграция цифровых технологий в стратегию развития экономической безопасности предприятий представляет собой необходимое условие их успешной адаптации к трансформирующимся условиям цифровой среды и обеспечения рыночной конкурентоспособности. Разработка стратегии управления экономической безопасностью в условиях цифровизации, равно как и формирование механизма ее практической реализации, выдвигаются в число приоритетных задач современной системы управления рисками и угрозами, что в конечном итоге способствует повышению устойчивости бизнеса в текущих экономических реалиях. Способность хозяйствующего субъекта адаптироваться к происходящим изменениям, принимать решения на основе анализа данных и оперативно восстанавливать операционную устойчивость обеспечивает ему не только конкурентные преимущества, но и возможность оказывать влияние на формирование более устойчивой экономической системы в целом. Обеспечение экономической безопасности в эпоху цифровизации объективно требует реализации комплексного подхода и координации усилий со стороны государства, бизнес-сообщества и институтов гражданского общества.

Результаты проведенного теоретико-методологического исследования позволяют сформулировать ряд выводов, развивающих и дополняющих научные представления о стратегическом управлении экономической безопасностью в условиях цифровой трансформации.

Произведено уточнение сущностных характеристик цифровой экономики в контексте обеспечения экономической безопасности. Обосновано положение, согласно которому цифровая трансформация выступает не только фактором роста производительности, но и источником

генерации системных рисков, включая киберугрозы, углубление цифрового неравенства, а также эрозию институциональных механизмов защиты прав собственности. Указанное обстоятельство обуславливает необходимость применения не ситуационного, а стратегического подхода к управлению защищенностью экономических субъектов.

Предложено дополнение классификации видов экономической безопасности. Аргументирована целесообразность включения в её структуру таких компонентов, как кибербезопасности, инновационная безопасность и инфраструктурная безопасность. Выявлено наличие корреляционной связи между данными элементами: недостаточный уровень инновационной безопасности детерминирует технологическое отставание, что, в свою очередь, повышает степень уязвимости цифровой инфраструктуры и снижает защищенность экономической системы в целом.

В рамках проведенного исследования разработана авторская модель стратегического управления экономической безопасностью, принципиальная новизна которой заключается в интеграции адаптивного и антиципативного управленческих контуров в рамках единой стратегической системы. Такой подход обеспечивает возможность перехода от реактивной модели защиты, ориентированной на противодействие уже реализовавшимся угрозам, к проактивному управлению будущим состоянием защищенности объекта на основе применения инструментов прогнозной аналитики.

Выявлен институциональный разрыв, проявляющийся в противоречии между высокими темпами цифровизации бизнес-процессов и отсутствием на большинстве отечественных предприятий формализованных стратегий управления цифровыми рисками. Существующая система управления экономической безопасностью характеризуется фрагментарностью, что обуславливает актуальность разработки отраслевых методических подходов к оценке эффективности реализуемых стратегий экономической безопасности в цифровой среде.

Теоретическая значимость исследования состоит в приращении научного знания в области адаптации классических положений теории стратегического менеджмента к условиям цифровой турбулентности, характеризующимся высокой степенью неопределенности и динамизма внешней среды.

Практическая значимость полученных результатов заключается в том, что предложенная авторская модель может служить концептуальной основой для разработки корпоративных стратегий обеспечения экономической безопасности, а также для формирования цифровой культуры управления рисками на уровне хозяйствующих субъектов.

В качестве перспективных направлений дальнейших исследований, требующих углубленной проработки, могут быть выделены следующие: разработка количественной методики оценки влияния сквозных цифровых технологий (искусственный интеллект, технологии распределенного реестра, интернет вещей) на систему индикаторов экономической безопасности; формирование систем пороговых значений индикаторов экономической безопасности применительно к предприятиям различных отраслей с учетом их цифровой зрелости; имплементации механизмов государственно-частного партнерства в сфере противодействия трансграничным киберугрозам экономической безопасности.

## СПИСОК ЛИТЕРАТУРЫ

1. Аветисян А.С., Алябьева А.Ю., Андрианова И.Д. и др. Экономическая безопасность: вызовы цифровой экономики [Электронный ресурс] // Монография. Донецк. Изд-во «Донецкий государственный университет». 2025. с. 364. URL: <https://www.elibrary.ru/item.asp?id=82748556&ysclid=mlkny84dbq423845845> (дата обращения: 13.02.2026).
2. Андрос Е.В. Мониторинг экономической безопасности региона в условиях цифровой экономики. [Электронный ресурс] // Материалы IV Междунар. науч.-практ. конф. молодых ученых. Минск. Белорус. гос. ун-т. 2023. С. 34-38. URL: <https://elib.pnzgu.ru/files/eb/CGMS09wFKBp4.pdf> (дата обращения: 27.02.2026).
3. Ганич Л.В. Генезис и современные подходы к определению экономической сущности категории «цифровая экономика» [Электронный ресурс] // Вести Автомобильно-дорожного института. 2022. № 3 (42). С. 33-40. URL: <https://www.elibrary.ru/item.asp?edn=vdplwz> (дата обращения: 13.02.2026).
4. Дмитриев А.В. Внедрение инструментов цифровой безопасности в деятельность организаций [Электронный ресурс] // Вестник Астраханского государственного технического университета. Серия: Экономика. 2025. №. 3. С. 26-35. URL: <https://cyberleninka.ru/article/n/vnedrenie-instrumentov-tsifrovoy-bezopasnosti-v-deyatelnost-organizatsiy/viewer> (дата обращения: 13.02.2026).
5. Иродова Е.Е., Соколов А.М. Анализ этапов развития цифровизации экономики: эволюция, взгляды авторов и подходы к изучению понятия [Электронный ресурс] // Журнал региональной и международной конкурентоспособности. 2025. Т. 5. №. 4. С. 4-14. URL: <https://ystu.editorum.ru/ru/nauka/article/93385/view> (дата обращения: 13.02.2026).
6. IT-специалисты не везде востребованы [Электронный ресурс] // Тюменская правда. 2025. 23 окт. URL: [https://www.tyum-pravda.ru/2025/10/23/it\\_\\_spetsialisty\\_ne\\_vezde\\_vostrebovany/](https://www.tyum-pravda.ru/2025/10/23/it__spetsialisty_ne_vezde_vostrebovany/) (дата обращения: 10.02.2026).
7. Карпунина Е.К., Соболевская Т.Г. Экономическая безопасность регионов и новые цифровые горизонты [Электронный ресурс] // Вестник Тверского государственного университета. Серия: Экономика и управление. 2020. № 4 (52). С. 136-148. URL: <https://www.elibrary.ru/item.asp?id=44511338&ysclid=mlknihr23v385119904> (дата обращения: 13.02.2026).
8. Красильникова Л.Е., Баландин Е.Д. Особенности обеспечения экономической безопасности региона в условиях цифровой трансформации [Электронный ресурс] // Журнал прикладных исследований. 2025. №. 11. С. 108-115. URL: <https://zhpi.ru/ru/nauka/article/110297/view> (дата обращения: 13.02.2026).
9. Кудрявцева Н.Н., Дедов С.В. Проблемы цифровой трансформации предприятий оборонно-промышленного комплекса России в условиях санкционного давления [Электронный ресурс] // Вестник Донецкого национального университета. Серия В. Экономика и право. 2025. № 4. С. 226-236. URL: <https://dongu-vestnik03.ru/index.php/vestnik03/issue/view/39> (дата обращения: 13.02.2026).
10. Кутайцева О.Н., Толмачева И.В., Толмачев А.А., Фишер В.И. Цифровая экономика и экономическая безопасность [Электронный ресурс] // Экономика и бизнес: теория и практика. 2023. № 5-2 (99). С. 68-71. URL: <https://cyberleninka.ru/article/n/tsifrovaya-ekonomika-i-ekonomicheskaya-bezopasnost/viewer> (дата обращения: 13.02.2026).
11. Логвинов В.А., Наливайченко Е.В. Инфраструктурное обеспечение цифрового предпринимательства. [Электронный ресурс] // Теоретическая экономика. 2023. № 12. С. 65-76. URL: <https://ystu.editorum.ru/ru/nauka/article/81142/view> (дата обращения: 27.02.2026).
12. Маркин М.И. Цифровая трансформация промышленных предприятий: экономический аспект [Электронный ресурс] // Теоретическая экономика. 2025. № 9 (129). С. 80-93. URL: <https://ystu.editorum.ru/ru/nauka/article/106690/view> (дата обращения: 27.02.2026).
13. Оборин М.С., Воротов М.Д. Концепция цифровизации бизнес-процессов в металлургическом производстве в условиях санкционных ограничений [Электронный ресурс] // Менеджер. 2025. № 8(114). С. 116-130. URL: [http://new.donampa.ru/images/2025/doc/8114\\_2025.pdf](http://new.donampa.ru/images/2025/doc/8114_2025.pdf) (дата обращения:

13.02.2026).

14. Оборин М.С. Цифровая среда как фактор повышения экономической безопасности региона [Электронный ресурс] // Ученые записки Крымского федерального университета имени В.И.Вернадского. Экономика и управление. 2021. Т. 7 (73.) № 2. С.83-91. URL: <https://cyberleninka.ru/article/n/tsifrovaya-sreda-kak-faktor-povysheniya-ekonomicheskoy-bezopasnosti-regiona/viewer> (дата обращения: 27.02.2026).

15. Национальные проекты [Электронный ресурс] // сайт «Национальные проекты» URL: <https://xn--80aаратремсчfmo7a3с9ehj.xn--p1ai/projects/tsifrovaya-ekonomika/> (дата обращения: 27.02.2026).

16. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента Российской Федерации от 09.05.2017 № 203. URL: <http://www.kremlin.ru/acts/bank/41919> (дата обращения: 13.02.2026).

17. Парфенов Д.А. Развитие механизма обеспечения экономической безопасности в РФ в условиях цифровизации [Электронный ресурс] // Вестник Московского университета. Серия 21. Управление ( государство и общество). 2020. № 4. С. 107-118. URL: [http://vestnik21msu.ru/upload/iblock/ba2/noaddfuvvs2uvvon8dmpx7ckossn2gwo/Ser\\_21\\_2020\\_4\\_Text\\_106\\_122.pdf](http://vestnik21msu.ru/upload/iblock/ba2/noaddfuvvs2uvvon8dmpx7ckossn2gwo/Ser_21_2020_4_Text_106_122.pdf) (дата обращения: 13.02.2026).

18. Петрушевский Р.Ю. Цифровая трансформация как фактор повышения эффективности управления бизнес-процессами хозяйствующих субъектов: модель и инструменты её реализации [Электронный ресурс] // Менеджер. 2025. № 8(114). С. 29-40. URL: [http://new.donampa.ru/images/2025/doc/8114\\_2025.pdf](http://new.donampa.ru/images/2025/doc/8114_2025.pdf) (дата обращения: 13.02.2026).

19. Поздеев В.Л., Старикова М.Ф. Цифровая экономика в контексте экономической безопасности региона [Электронный ресурс] // «Russian journal of management». 2022. Т. 10. № 3. С. 11-15. URL: <https://www.elibrary.ru/item.asp?id=49541122&ysclid=mlkngxkto4939615199> (дата обращения: 13.02.2026).

20. Родина Г.А. Цифровизация как фактор усиления асимметричности информации на арт-рынке [Электронный ресурс] // Теоретическая экономика. 2025. № 12 (132). С. 13-28. URL: <https://ystu.editorum.ru/ru/nauka/article/111855/view> (дата обращения: 27.02.2026).

21. Рудава Н.В. Концептуально-методологические положения инновационно-цифровых преобразований экономической системы [Электронный ресурс] // Теоретическая экономика. 2025. № 9. С. 62-79. URL: <https://ystu.editorum.ru/ru/nauka/article/106688/view> (дата обращения: 27.02.2026).

22. Сапожков О., Петрова В. Цифра повышенной точности: Как эволюционируют оценки вклада ИТ в экономику [Электронный ресурс] // Коммерсантъ. 2025. № 223. 3 дек. URL: <https://www.kommersant.ru/doc/8250125> (дата обращения: 13.02.2026).

23. Соколов Е.Д. Стратегические подходы к управлению рисками при обеспечении экономической безопасности в условиях геополитической нестабильности и глобальных экономических трансформаций [Электронный ресурс] // Вестник евразийской науки. 2025. Т. 17. № 3. URL: <https://esj.today/PDF/40FAVN325.pdf> (дата обращения: 13.02.2026).

24. Шваб К. Четвертая промышленная революция. М.: Эксмо, 2016. 137 с.

25. Arefiev, N. A. Impact of digital technologies on the economic security of enterprises: prospects and threats / N. A. Arefiev, G. S. Ukubassova // Economic Consultant. – 2025. – № 1. – P. 4-18. – URL: <https://econpapers.repec.org/article/risstatec/021529.htm> (дата обращения: 10.02.2026). – DOI: 10.46224/ecoc.2025.1.1.

26. Negroponte, N. Being Digital / N. Negroponte. – New York : Alfred A. Knopf, Inc., 1995. – 243 p. – ISBN 0-679-43919-6.

27. Tapscott, D. The Digital Economy: Promise and Peril In The Age of Networked Intelligence / D. Tapscott. – New York : McGraw-Hill, 1995. – 342 p. – ISBN 978-0070622005.

# Theoretical and methodological issues of strategic management of economic security in the context of digital transformation of the economy

**Tarkhanova Nina Alekseevna**

Candidate of Economic Sciences, Associate Professor  
Donbas National Academy of Civil Engineering and Architecture, Makeyevka, Russia  
E-mail: n.a.tarhanova@donnasa.ru

**Norkina Tatyana Pavlovna**

Senior Lecturer  
Donbas National Academy of Civil Engineering and Architecture, Makeyevka, Russia  
E-mail: t.p.norkina@donnasa.ru

**Shestopalova Lyudmila Valentinovna**

Senior Lecturer  
Donbas National Academy of Civil Engineering and Architecture, Makeyevka, Russia  
E-mail: l.v.shestopalova@donnasa.ru

---

## KEYWORDS

digital economy, economic security, threats, risks, digital infrastructure, cybersecurity, strategic management, digital technologies

## ABSTRACT

The purpose of this article is to develop the theoretical and methodological foundations for ensuring economic security in the context of digital transformation of economic systems. The relevance of this work is due to the insufficient adaptation of existing conceptual approaches to managing economic security in the context of digital transformation of the economy, which requires a revision of several established principles of economic theory. The object of this study is the system of guaranteeing economic security in the process of digitalization of the national economy. The subject of this study is the organizational and economic relations that arise in the process of activating potential opportunities and neutralizing threats to economic security under the influence of digital transformation. The article provides a theoretical analysis of the categorical apparatus of the subject area under study, namely, the content of the definitions of «digital economy» and «economic security». Based on the results of the analysis, the authors propose a refined interpretation of the digital economy, which is defined as the institutional and technological environment of the reproduction process, where data presented in digital format is the key factor of production. In this article, economic security is interpreted as a complex, multi-component category that integrates a set of conditions and factors necessary for maintaining sustainable development of the national economy. The authors propose an expanded classification of types of economic security based on the functional criterion. A comparative analysis of the paradigms of the traditional and digital economy has been performed, and the transforming impact of digital technologies on the state of security of the economic system has been considered. The risks and challenges of economic security that arise during the process of digital transformation have been systematized. The article analyzes modern theoretical approaches to economic security management and argues for the need to apply a strategic approach in the context of digitalization. The authors develop a conceptual model of strategic management of economic security, which integrates adaptive and anticipatory control loops to respond to changes in the external environment and predict potential threats. The scientific novelty of the conducted research consists in the development of the categorical apparatus of the theory of economic security, systematization of opportunities and threats to the security of the economy in the context of its digitalization, as well as in the development of a model of the process of strategic management of economic security, adapted to the realities of digital transformation. The practical significance of the obtained results is determined by the possibility of their use in the process of forming corporate strategies for ensuring the economic security of business entities in the context of digitalization of their business processes.

---