УДК 338.2 DOI: 10.14451/1.250.40

Теоретические подходы к управлению экономической безопасностью цифрового двойника предприятия

© 2025 **Богданов Илья Александрович**
Ведущий инженер, ООО Газпром трансгаз Сургут, Россия, Сургут.
E-mail: bogdanovilya@ya.ru

© 2025 **Байбулатов Руслан Ямильевич**
Аспирант. Сургутский государственный университет, Россия, Сургут.
E-mail: baybulatov@list.ru

© 2025 **Зубарева Любовь Витальевна**
Доктор экономических наук, профессор кафедры экономических и учетных дисциплин.
Сургутский государственный университет, Россия, Сургут.
E-mail: zlv@mail.ru

Ключевые слова: экономическая безопасность, цифровой двойник, управление, теория управления, риски, угрозы, кибербезопасность, информационная безопасность, цифровая трансформация, моделирование.

Статья рассматривает теоретические подходы к управлению экономической безопасностью цифровых двойников (ЦД) предприятий. Проанализированы существующие концепции управления экономической безопасностью и их применимость к ЦД, выделены специфические угрозы и риски, возникающие при использовании ЦД, связанные с кибербезопасностью, манипулированием данными и интеграцией физических и виртуальных активов. Предложены направления развития теоретической базы управления экономической безопасностью ЦД, включающие адаптацию существующих моделей, разработку новых подходов и учет человеческого фактора.

Введение

В эпоху бурного развития цифровых технологий цифровые двойники (ЦД) приобретают всё большее значение как средство улучшения работы и укрепления позиций компаний на рынке. Создавая виртуальное отражение реального объекта, процесса или системы, ЦД обеспечивают возможность отслеживания, анализа, прогнозирования, оптимизации управления и принятия взвешенных решений [4; 12]. Однако масштабное применение ЦД порождает новые вызовы в области экономической безопасности (ЭБ), вызванные объединением физического и виртуального миров, подверженностью киберугрозам и потенциалом искажения информации [13]. Но несмотря на значительный интерес к ЦД, теоретическая база управления их ЭБ остается недостаточно разработанной. Существующие

методы управления, применяемые к традиционным предприятиям, не в полной мере учитывают специфику ЦД как сложной информационной системы, что требует адаптации и создания новых теоретических методик.

Целью данной статьи является анализ существующих теоретических подходов к регулированию ЭБ и формирование направлений совершенствования теоретической базы управления ЭБ ЦД предприятий.

Цифровой двойник как объект управления экономической безопасностью: сущность и особенности

Цифровой двойник представляет собой виртуальную модель физического объекта, процесса или системы, созданную на основе данных, собранных из разнообразных источников, таких как сенсоры, датчики и прочие устройства [6]. ЦД даёт возможность моделировать поведение реального объекта, предсказывать его состояние и оптимизировать процессы контроля, что способствует повышению эффективности и конкурентоспособности предприятия [2].

Ключевой чертой цифрового двойника выступает неразрывная связь физической и виртуальной реальностей, обеспечивающая постоянный сбор и обработку информации вблизи реального времени. Эта система характеризуется рядом свойств, напрямую влияющих на экономическую защищенность организации:

- **Комплексность и взаимосвязанность:** цифровой двойник объединяет множество различных данных и взаимодействующих систем, формируя сложнейшую сеть отношений и зависимостей. С увеличением числа этих связей возрастает трудность контроля над процессом и предотвращения нарушений экономической безопасности.
- **Интеграция физического и виртуального пространств:** физические объекты предприятия соединяются с виртуальными моделями, что открывает дополнительные каналы воздействия на предприятие через сети передачи данных и вычислительные платформы. Сбой в работе одного элемента системы может вызвать нарушение работы всей инфраструктуры, вплоть до приостановки производства, порождая дополнительные угрозы и риски, связанные с кибербезопасностью и искажением данных.
- **Динамичность и изменчивость:** ЦД постоянно обновляется и изменяется на основе данных, получаемых в режиме реального времени, что требует адаптивных методов контроля ЭБ.
- **Уязвимость к киберугрозам:** ЦД как сложная киберфизическая система подвержен различным киберугрозам, включая несанкционированный доступ, вредоносное программное обеспечение и атаки типа «отказ в обслуживании».
- **Значимость данных:** эффективность ЦД зависит от качества и достоверности данных, используемых для его создания и функционирования. Искажение или потеря данных может привести к ошибочным управленческим решениям и, как следствие, к финансовым убыткам.

Таким образом, управление экономической безопасностью цифрового двойника представляет собой сложную задачу, требующую особого внимания со стороны руководства предприятия. Решение вопросов безопасности ЦД невозможно без учёта общей стратегической политики предприятия, направленной на повышение устойчивости и стабильности всех сфер деятельности.

Факторы, определяющие важность экономической безопасности ЦД:

- Сложность структуры: высокая.
- Тип угрозы: кибератаки.
- Скорость изменений: очень быстрая.
- Уровень конфиденциальности: высокий.
- Чувствительность данных: высокий.

Обзор теоретических подходов к управлению экономической безопасностью

Ресурсный подход

Данный подход направлен на защиту активов организации как материальных, так и нематериальных, которые критически важны для её стабильного функционирования и конкурентоспособности. К ним, в частности, относятся:

- материальные запасы;
- человеческий капитал;
- коммерческая тайна;
- интеллектуальная собственность.

Главная задача системы, построенной на принципах данного подхода, — выявление и обеспечение безопасности наиболее значимых активов. Например, нарушение целостности финансовой отчетности или потеря интеллектуальной собственности может привести к существенным материальным и репутационным рискам.

Преимущества:

- простота понимания и реализации;
- чёткая ориентация на конкретные активы предприятия.

Недостатки:

- недостаточная гибкость при работе со сложными системами вроде цифровых двойников;
- трудности в применении к абстрактным ресурсам, таким как деловая репутация или инновационный потенциал [1].

Функциональный подход

Этот подход предполагает организацию специализированных подразделений, отвечающих за контроль и предотвращение нарушений экономической безопасности. В их компетенцию входит защита коммерческой тайны, мониторинг финансовых потоков и оценка рисков.

Реализация подхода осуществляется посредством постановки четких задач и распределения ответственности между структурными подразделениями компании. Особое внимание уделяется стандартизации процедур и регламентированию требований к защите информации и имущественным правам.

Преимущества:

- способствует созданию целостной системы безопасности;
- позволяет организовать регулярный мониторинг состояния безопасности.

Недостатки:

- ограниченная возможность оперативного реагирования на нестандартные ситуации;
- необходимость постоянного обновления локально-нормативных актов и должностных инструкций [15].

Процессный подход

Процессный подход акцентирует внимание на оптимизации внутренних бизнес-процессов, повышая их прозрачность и управляемость. Суть подхода заключается в своевременном выявлении и устранении любых отклонений от установленных норм, что позволяет минимизировать риски нарушений экономической безопасности.

Ключевые элементы процессного подхода включают:

- регулярную оценку текущего состояния процессов;
- определение индикаторов эффективности;
- контроль соблюдения стандартов и протоколов.

Преимущества:

- улучшение операционной дисциплины;
- возможность быстрого обнаружения отклонений.

Недостатки:

- ограниченная эффективность в противодействии внешним угрозам;
- необходимость в постоянных затратах на поддержание систем мониторинга [9].

Риск-ориентированный подход

Данная стратегия базируется на идентификации потенциальных угроз и оценке вероятности их реализации. После анализа и выявления рисков разрабатываются и внедряются меры по их предотвращению и подготовке к неблагоприятным сценариям.

Основные этапы риск-менеджмента:

1. Идентификация рисков.
2. Оценка вероятности появления рисков.

3. Анализ последствий реализации угроз.
4. Принятие мер профилактики и реакции.

Такой подход позволяет эффективно распределять ресурсы, сосредотачиваясь на наиболее важных направлениях деятельности.

Преимущества:

- гибкость и способность быстро адаптироваться к изменениям внешней среды;
- минимизация финансовых и временных затрат на устранение кризисных ситуаций.

Недостатки:

- высокая зависимость от точности аналитических расчетов;
- отсутствие гарантий полного устранения всех рисков [14].

Системный подход

Системный подход рассматривает предприятие как единое целое, состоящее из взаимосвязанных подсистем: технической, организационной, кадровой и правовой. Для обеспечения надежной защиты от любых угроз, все компоненты должны функционировать согласованно.

Основные компоненты системного подхода:

- организационно-технические мероприятия (использование антивирусных программ, ограничение доступа к чувствительным зонам);
- кадровое обеспечение (регулярные проверки персонала, обучение правилам безопасности);
- правовое регулирование (соблюдение законодательства, разработка внутренней документации).

Данный подход способствует достижению оптимального уровня безопасности, исключая локальное воздействие только на отдельные участки предприятия.

Преимущества:

- универсальность применяемых решений;
- надежность создаваемого защитного барьера.

Недостатки:

- большие затраты на внедрение и обслуживание;
- долгосрочный характер реализации программы [7].

Таблица 1. Преимущества и недостатки теоретических подходов к управлению экономической безопасностью.

Подход	Преимущества	Недостатки
Ресурсный	ясность и простота	низкая гибкость
	ориентация на конкретные активы	
Функциональный	организация целостной системы	затруднения при оперативных реакциях
	стандартизация процедур	
Процессный	улучшение оперативной дисциплины	недостаточное противостояние внешним угрозам
	быстрое обнаружение отклонений	
Риск-ориентированный	гибкость и адаптация	результат зависит от аналитики
	оптимальное расходование ресурсов	
Системный	комплексность и надежность	высокие начальные инвестиции
	всесторонняя защита	длительность внедрения

Направления совершенствования теоретической базы управления экономической безопасностью цифровых двойников предприятия

Применение цифровых двойников на предприятиях создаёт новые угрозы и риски, связанные с нарушением экономической безопасности. Для эффективного контроля необходима модернизация теоретических основ обеспечения безопасности. Рассмотрим подробнее ключевые области совершенствования, выделяя достоинства и недостатки предложенных подходов.

Классификация угроз экономической безопасности цифровых двойников

Одной из приоритетных задач при изучении экономической безопасности цифровых двойников является систематизация потенциальных угроз. По своей природе угрозы делятся на внутренние и внешние.

- Внутренние угрозы возникают внутри самой системы предприятия и связаны с действиями сотрудников или недостаточной организацией внутренних процессов. Например, некорректная настройка серверов, небрежное отношение к паролям, отсутствие регулярных проверок работоспособности программного обеспечения, отсутствие резервного копирования данных [3].
- Внешние угрозы исходят от сторонних субъектов, пытающихся проникнуть в систему предприятия с целью хищения данных, саботажа технологических процессов или нанесения иного вреда. К ним относят кибератаки, вирусы, фишинговые атаки и другие виды вмешательства [5].

Методики оценки рисков экономической безопасности цифровых двойников

Оценка рисков направлена на определение степени вероятности возникновения нежелательных событий и размера потенциального ущерба. Обычно методика оценки рисков состоит из трех этапов:

1. Идентификация рисков. В процессе обеспечения безопасности предприятия проводится тщательный анализ существующих угроз, изучаются их причины и последствия [8].
2. Анализ рисков. На данном этапе рассчитывается вероятность возникновения конкретных угроз и определяется размер возможного ущерба [10].
3. Выбор оптимального способа нейтрализации рисков. Определяются необходимые профилактические меры, выбираются экономически целесообразные варианты защиты [11].

Среди распространённых методов оценки рисков выделяют SWOT-анализ, матрицу рисков и оценку по критерию Вальда.

Матрица рисков используется для наглядного представления результатов оценки рисков и принятия стратегических решений.

Таблица 2. Матрица рисков.

Вид риска	Вероятность	Последствия	Оценка риска
Атака хакеров	Средняя	Средние убытки	Средний риск
Несоответствие стандартам	Высокая	Незначительные убытки	Низкий риск
Потеря данных	Низкая	Крупные убытки	Высокий риск

Модели управления экономической безопасностью цифровых двойников

Разработка моделей управления экономическими рисками является важнейшим этапом улучшения системы безопасности. Одной из успешных практик является модель VDI, предлагающая последовательный алгоритм действий:

1. Vulnerability Assessment (оценка уязвимостей) — выявление слабых мест в системе безопасности.

2. Detection Analysis (анализ инцидентов) — сбор и обработка данных о попытках взлома и нарушениях.
3. Incident Response Planning (планирование реакций на инциденты) — подготовка плана действий на случай инцидента.
4. Investigation (расследование) — изучение произошедших инцидентов и выработка рекомендаций по улучшению защиты.

Ещё одной эффективной моделью является матрица SAFER (Security Assurance Framework Evaluation Routine):

- Security — политика безопасности, включающая совокупность организационных и технических мер, направленных на защиту информации и инфраструктуры от несанкционированного доступа, повреждений и злоупотреблений (установка надежных паролей, многоуровневой авторизации, шифрования данных и т.п.);
- Availability — доступность данных, которая обеспечивает постоянную готовность систем и данных к использованию (создание резервных копий, бесперебойная работой серверов и каналов связи и т.п.);
- Flexibility — гибкость системы, позволяющая эффективно адаптироваться к изменениям внешней среды и внутренним потребностям бизнеса;
- Economy — экономичность затрат, представляющая собой оценку соотношения расходов на меры безопасности и полученных выгод;
- Risk management — управление рисками, предполагающее постоянный мониторинг и анализ потенциальных угроз, проведение оценки их вероятности и возможного ущерба.

Таблица 3. Матрица SAFER.

Компонент	Описание	Уровень значимости
Security	политика безопасности	высокий
Availability	доступность данных	средний
Flexibility	гибкость системы	низкий
Economy	экономичность затрат	средний
Risk management	управление рисками	высокий

Применение этих моделей позволяет провести точную оценку текущие риски и обоснованно принимать решения [3].

Оценка результативности управления экономической защищенностью цифровых двойников

Наличие ключевых показателей необходимо для любой системы управления. К основным показателям относятся:

- Индекс защищённости данных (Data Protection Index);
- Коэффициент рентабельности инвестиций в безопасность (Return on Security Investment Ratio);
- Время восстановления после инцидента (Recovery Time Objective);
- Количество успешно отражённых атак (Number of Successful Attack Mitigations).

Расчет каждого показателя производится индивидуально, с учетом специфики и задач организации [8].

Учёт роли персонала в управлении экономической безопасностью цифровых двойников

Несмотря на технологический прогресс, сотрудники остаются важным элементом производственного процесса, а пренебрежение их влиянием на экономику может привести к нежелательным последствиям. Важно учитывать психологические аспекты и мотивацию для повыше-

ния осознанности и квалификации персонала. Рекомендуется:

- Проведение регулярного обучения сотрудников основам информационной безопасности.
- Использование технологий двухфакторной аутентификации.
- Периодическое тестирование сотрудников на знание правил безопасного пользования IT-ресурсами [10].

Для углубления теоретической базы управления экономической безопасностью цифровых двойников требуется детальный анализ потенциальных угроз, тщательная оценка рисков и внедрение современных моделей управления. Это обеспечит эффективную деятельность предприятий в условиях быстрого цифрового преобразования.

Заключение

Проведённое исследование продемонстрировало, что цифровой двойник предприятия — это сложный объект управления экономической безопасностью, характеризующийся уникальными особенностями и создающий специфические задачи в плане защиты от угроз и рисков. Актуальность темы обусловлена широким внедрением цифровых двойников в производственные процессы, что требует адаптации существующих теоретических подходов и разработки новых методов управления экономической защищенностью.

Теоретический анализ показал, что наиболее эффективными являются комплексные стратегии, учитывающие особенности цифровых двойников как сложных киберфизических систем. Для совершенствования теоретической базы определены следующие направления развития:

- Разработка детализированной классификации угроз экономической безопасности цифровых двойников.
- Совершенствование методики оценки рисков, соответствующей особенностям цифровых двойников.
- Создание комплексных моделей управления экономической безопасностью, учитывающих разнообразие угроз и возможность учёта человеческого фактора.
- Внедрение критериев эффективности управления, позволяющих объективно оценить достигнутый уровень защищённости.

В дальнейшем целесообразно развивать работу по этим направлениям, уделяя особое внимание систематизации потенциальных опасностей, разработке инструментов для анализа рисков и формированию научно обоснованных подходов к обеспечению экономической защищенности цифровых двойников компаний.

Эти направления позволят расширить теоретическую базу и повысить практическую применимость управления экономической безопасностью цифровых двойников предприятий.

Библиографический список

1. *Афанасьев В. Е.* Современные тенденции в управлении экономической безопасностью // Вопросы государственного и муниципального управления. — 2019. — № 2. — С. 56—63.
2. *Белов П. Г.*, *Соколов Б. В.* Цифровые двойники в машиностроении: принципы, технологии, реализация. — СПб. : Издательство Политехнического университета, 2018.
3. *Воронин А. А.* Инструменты и методы оценки экономической безопасности предприятий // Менеджмент в России и за рубежом. — 2019. — № 2. — С. 45—52.
4. *Глазьев С. Ю.* Экономическая безопасность России: теория и реальность. — М. : Экономика, 2007. — 766 с.
5. *Захаров П. Н.* Кибернетическая защита информационных систем. — СПб. : Питер, 2018. — 256 с.
6. *Ильин И. В.*, *Левина А. И.* Цифровые двойники: сущность, структура, применение // International Journal of Open Information Technologies. — 2019. — Т. 7, № 1. — С. 47—55.
7. *Лаврушин О. И.* Банковская система России: современные проблемы и перспективы развития. — М. : Кнорус, 2017. — 352 с.
8. *Матвеенко С. А.* Методы оценки рисков экономической безопасности предприятий малого и среднего бизнеса // Вестник Томского гос. университета. Экономика. — 2019. — № 4. — С. 67—76.
9. *Осипов Г. Л.* Экономическая безопасность предприятий : учебное пособие. — Екатеринбург : УрГЭУ, 2019. — 145 с.

10. *Поляков В. О.* Совершенствование системы экономической безопасности промышленного предприятия // Российское предпринимательство. — 2018. — № 10. — С. 98—106.
11. *Светличная А. В.* Стратегия управления экономической безопасностью фирмы в условиях цифровой трансформации // Журнал прикладной экономики и статистики. — 2020. — № 2. — С. 54—63.
12. *Сенчагов В. К.* Экономическая безопасность: геополитика, глобализация, самосохранение. — М. : Финстатинформ, 2002. — 128 с.
13. *Трофимов О. В.*, *Трофимова Е. А.* Цифровые двойники как инструмент обеспечения устойчивого развития предприятий // Вестник университета. — 2021. — № 1. — С. 108—115.
14. *Федотов А. Ф.* Основы управления рисками в предпринимательской деятельности. — Новосибирск : Новосибирская государственная академия водного транспорта, 2018. — 178 с.
15. *Шульга А. Д.* Система управления экономической безопасностью промышленных предприятий // Научные ведомости Белгородского государственного университета. Серия экономика и управление. — 2018. — № 1. — С. 103—111.