УДК 004.056

Проблемы использования цифровых двойников в задачах обеспечения информационной безопасности объектов критической информационной инфраструктуры

Митяков Е. С.

МИРЭА – Российский технологический университет
Москва, 119454, Российская Федерация

Постановка задачи. *В условиях стремительной цифровизации экономики и государственного управления вопросы обеспечения информационной безопасности критической информационной инфраструктуры становятся все более актуальной задачей. Критическая информационная инфраструктура включает в себя объекты, которые играют ключевую роль в функционировании жизненно важных сфер общества, таких как энергетика, транспорт, здравоохранение, промышленность и др. С ростом сложности этих объектов возникает потребность в применении новых технологий для обеспечения их защиты. Одним из таких инструментов является использование цифровых двойников, которые позволяют моделировать угрозы и тестировать меры защиты. Однако интеграция цифровых двойников в задачи информационной безопасности критической информационной инфраструктуры сталкивается с рядом проблем, требующих решения для эффективного внедрения этой технологии.* ***Цель работы*** *заключается в выявлении ключевых проблем, возникающих при использовании цифровых двойников в сфере информационной безопасности критической информационной инфраструктуры.* ***Используемые методы:*** *контент-анализ стандартов, классификация проблем с применением механизма категориальных пар, оценка сценариев использования цифровых двойников в критической информационной инфраструктуре.* ***Новизна:*** *в работе выделены новые аспекты использования цифровых двойников в контексте критической информационной инфраструктуры, связанные с модельными характеристиками, а также проблемами верификации и контроля целостности цифровых моделей. Рассмотрены вопросы безопасности, включая риски применения открытых API и каналов телеметрии, что может стать вектором для атак. Предложен комплекс мер в целях преодоления этих проблем, включая разработку нормативных стандартов для использования цифровых двойников и повышение квалификации специалистов.* ***Результаты:*** *выявлены ключевые проблемы, классифицированные по следующим категориям: технические, связанные с безопасностью, организационные, правовые, а также связанные с некорректным использованием. Каждая категория включает конкретные проблемы, последствия которых варьируются от ошибок в моделях и сниженной эффективности защиты до угроз компрометации критической информационной инфраструктуры и утраты доверия к технологии.* ***Теоретическая / Практическая значимость:*** *результаты работы направлены на совершенствование подходов к обеспечению информационной безопасности критической информационной инфраструктуры с использованием цифровых двойников. Рекомендации по решению выявленных проблем могут быть задействованы для повышения надежности, безопасности и эффективности внедрения и эксплуатации цифровых двойников в системах критической информационной инфраструктуры.*

Ключевые слова: *информационная безопасность, критическая информационная инфраструктура, цифровой двойник, синхронизация данных, моделирование угроз*

Библиографическая ссылка на статью:
Митяков Е. С. Проблемы использования цифровых двойников в задачах обеспечения информационной безопасности объектов критической информационной инфраструктуры // Информационные технологии и телекоммуникации. 2023. Т. 11. № 4. С. 36–47. DOI: 10.31854/2307-1303-2023-11-4-36-47

Reference for citation:
Mityakov E. S. Problems of Using Digital Twins in Ensuring Information Security of Critical Information Infrastructure Facilities // Telecom IT. 2023. Vol. 11. Iss. 4. PP. 36–47. (in Russian) DOI: 10.31854/2307-1303-2023-11-4-36-47

Введение

В эпоху стремительной цифровизации экономики и государственного управления особую актуальность приобретает обеспечение информационной безопасности (ИБ) критической информационной инфраструктуры (КИИ). Согласно Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», КИИ включает в себя объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Под объектами КИИ понимаются информационные системы, информационно-телекоммуникационные сети, а также автоматизированные системы управления, эксплуатируемые субъектами КИИ в энергетике, транспорте, здравоохранении, промышленности, банковской сфере и других социально значимых отраслях.

В условиях цифровизации и увеличения степени автоматизации и сложности технологических процессов, приводящих (как следствие) к росту объема, в том числе, небезопасного ПО, современная КИИ с неизбежностью сталкивается с растущим числом угроз. Традиционные подходы к обеспечению ИБ, ориентированные преимущественно на реактивное устранение последствий инцидентов, оказываются недостаточными для своевременной и эффективной защиты. Это связано с высокой динамикой угроз, усложнением векторов атак и увеличением числа уязвимостей в системах управления. В этих условиях успешное обеспечение ИБ требует внедрения инновационных методов, ориентированных на проактивное выявление уязвимостей, прогнозирование развития угроз и превентивное реагирование на инциденты.

Одним из ключевых инструментов в этой области становится технология цифровых двойников (ЦД), позволяющая моделировать угрозы, оптимизировать процессы восстановления и тестировать меры защиты [1, 2]. Согласно ГОСТ Р 57700.37-2021, ЦД изделия определяется как система, состоящая из цифровой модели изделия и двусторонних информационных связей с изделием и его составными частями. Это позволяет реализовывать поддержку на всех стадиях жизненного цикла изделия (от разработки и производства до эксплуатации и модернизации). ЦД помогает обеспечивать точное отслеживание состояния объекта, проводить виртуальные испытания и оптимизировать эксплуатационные параметры физического изделия. Важным аспектом является то, что ЦД могут значительно снизить затраты на испытания, повысить надежность и ускорить процессы разработки, производства и эксплуатации изделий[1].

Однако объекты КИИ в своей сущности не всегда представляют собой физические объекты. В таком контексте ЦД КИИ, скорее выступают моделью информационной системы или части инфраструктуры, предназначенной для мониторинга, прогнозирования и защиты этих систем от угроз ИБ. Интеграция ЦД в контур задач обеспечения ИБ КИИ гипотетически открывает новые воз-

[1] ГОСТ Р 57700.37-2021. Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения. — М.: Стандартинформ, 2022. – URL: https://docs.cntd.ru/document/1200180928 дата обращений 12.06.2023)

можности в сфере мониторинга, тестирования, анализа и реагирования на инциденты, обеспечивая более высокую точность, скорость и адаптивность защитных мер.

Вместе с тем, внедрение ЦД в систему КИИ порождает новые угрозы и уязвимости: увеличивается поверхность атак, появляются проблемы верификации и контроля целостности моделей и т.д. Кроме того, недостаточная зрелость нормативно-правовой базы в вопросах взаимодействия ЦД и объектов КИИ усложняет реализацию комплексной защиты таких систем. *Целью данной статьи* выступает выявление ключевых проблем, возникающих при использовании ЦД в задачах обеспечения ИБ КИИ.

Концепция цифрового двойника

Для корректного анализа проблем, связанных с применением ЦД в задачах обеспечения ИБ КИИ, целесообразно рассмотреть базовые понятия и взаимосвязь между ЦД, КИИ и ИБ в контексте технических систем.

Концепция цифрового двойника была впервые представлена в 2002 г. профессором Мичиганского университета Майклом Гривзом как методология создания виртуальных реплик физических объектов с двусторонней синхронизацией данных в реальном времени [3]. В основе этой концепции лежит представление о цифровом двойнике как о динамической системе, способной отражать текущее состояние объекта, его поведение и взаимодействие с внешней средой.

Современные технологии позволяют создавать цифровые реплики практически любых физических объектов, используя вычислительные и математические модели. Это достигается за счет анализа данных, полученных от реального объекта, и организации непрерывного информационного обмена между его физической и цифровой формами. На рисунке 1 показана схема связей цифрового двойника с физическим объектом. Стрелками указаны потоки физических (красным цветом) и информационных (синим цветом) данных.

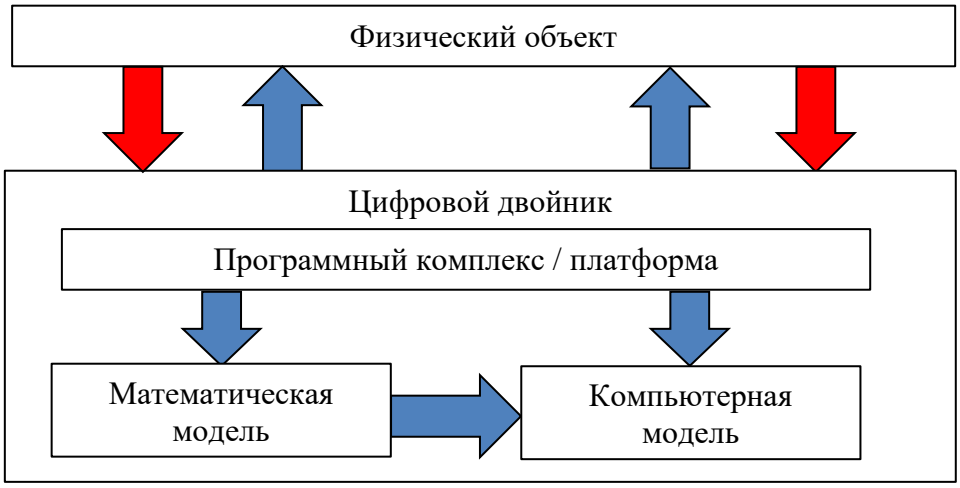

Рис. 1. Иллюстрация схемы связей цифрового двойника с физическим объектом

DOI: 10.31854/2307-1303-2023-11-4-36-47
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_4/36-47.pdf

Согласно [4, 5], для эффективного функционирования ЦД должен обладать рядом ключевых свойств (аналитическая предиктивность, интеграция с физическим объектом, динамическая синхронизация и др.). Эти свойства целесообразно разделить на функциональные (обеспечивающие базовую работоспособность ЦД) и потребительские (отражающие выгоды от его применения), с последующей привязкой к возможностям решения задач в области ИБ. Цифровые двойники, изначально ориентированные на оптимизацию производственных процессов, сегодня активно развиваются как инструменты проактивной ИБ [6]. Их способность имитировать реальные события без риска для физических объектов создает предпосылки для моделирования угроз, тестирования мер защиты, прогнозирования последствий атак и автоматизации процессов обнаружения инцидентов [7–11].

Классификация свойств цифрового двойника представлена в таблице 1. В ней функциональные свойства соотнесены с потребительскими эффектами, которые достигаются при использовании ЦД, а также с возможностями их применения для решения задач информационной безопасности.

Таблица 1 – Классификация свойств цифрового двойника

Функциональные свойства	Потребительские свойства	Возможности для задач ИБ
Аналитическая предиктивность и оптимизация	Прогнозирование поведения систем	Прогнозирование последствий кибератак на объекты КИИ
Интеграция с физическим объектом	Обеспечение виртуального прототипирования	Проведение атак в виртуальной среде без риска повреждения физической системы
Динамическая синхронизация	Поддержание актуальности модели	Оперативное обнаружение изменений и аномалий
Интерактивный контроль	Возможность тестирования сценариев изменений	Отработка действий персонала в условиях виртуальных инцидентов
Высокая точность	Достоверность результатов симуляции	Точная оценка эффективности мер защиты
Мониторинг и анализ	Выявление отклонений и слабых мест	Автоматизация обнаружения признаков атак
Интеграция в производство	Сокращение времени и затрат на разработку	Быстрая адаптация систем безопасности и проведение тестов
Ориентация на безопасность и устойчивость	Проведение виртуальных испытаний на устойчивость	Моделирование воздействия киберугроз и тестирование устойчивости систем
Моделирование «с нуля»	Проектирование безопасных систем еще до их физической реализации	Упреждающее устранение потенциальных уязвимостей
Виртуальное прототипирование	Проверка характеристик объекта на всех стадиях его жизненного цикла	Моделирование угроз и тестирование защитных мер на ранних этапах
Совершенствование моделирования	Повышение качества проектирования и оптимизация процессов	Создание более защищенных и устойчивых систем
Ускорение разработки	Снижение сроков выхода продуктов на рынок	Быстрая разработка и валидация решений в области ИБ

В контексте задач ИБ ЦД используются для симуляции атак, таких как DDoS или эксплуатация уязвимостей IoT-устройств [3]. Технологии искусственного интеллекта, интегрированные в ЦД, позволяют автоматизировать обнаружение аномалий и реагирование на инциденты [12]. Для КИИ это означает возможность прогнозировать последствия атак, например, на узлы управления энергоснабжением или транспортными потоками [13].

Архитектура ЦД, как правило, включает: *физический объект* (оборудование, система управления, транспортный узел и др.); *цифровую модель*, включающую описания структуры, процессов и состояний; *каналы связи*, обеспечивающие сбор телеметрии и управление; *аналитические модули*, в том числе искусственный интеллект и машинное обучение.

Применение цифровых двойников в критической информационной инфраструктуре

Применение ЦД в сфере КИИ находится на пересечении задач управления, цифровизации и ИБ. Их интеграция в существующие системы КИИ позволяет создавать безопасную, адаптивную и интеллектуальную среду для моделирования, мониторинга и защиты жизненно важных процессов. Рассмотрим основные направления использования ЦД на объектах КИИ, типовые сценарии, а также ключевые преимущества и ограничения данной технологии.

Использование ЦД в КИИ должно соответствовать требованиям Федерального закона № 187-ФЗ, а также действующим стандартам и нормативам, устанавливаемым профильными регуляторами в сфере информационной безопасности. При этом важно обеспечить целостность данных, отказоустойчивость и защиту конфиденциальной информации.

В [14–16] декларируются следующие основные принципы применения ЦД в задачах ИБ: двусторонняя синхронизация между физическим и цифровым объектом; модульность для адаптации под разные сегменты КИИ; безопасность данных (соблюдение нормативных требований и стандартов ИБ), а также описываются основные сценарии применения (таблица 2).

Таблица 2 – Сценарии применения ЦД в КИИ

№	Сценарий применения	Описание
1	Моделирование угроз	Воссоздание кибератак для оценки уязвимостей и ущерба
2	Анализ устойчивости	Исследование поведения системы при сбоях, перегрузках, отказах компонентов
3	Тестирование обновлений и интеграций	Проверка совместимости систем, миграции баз данных, взаимодействия при цифровой трансформации
4	Обучение персонала и реагирование	Создание киберполигонов, тренажеров, отработка инцидентов без риска для производственной среды
5	Цифровой аудит и след	Сбор, фиксация и анализ цифрового следа для расследования и построения моделей поведения

Указанные сценарии демонстрируют, что ЦД выходят за рамки простого дублирования объектов и становятся инструментом анализа, обучения и принятия решений в условиях неопределенности и угроз.

Интеграция ЦД в объекты КИИ приносит значительные преимущества, повышая безопасность и эффективность управления системами. Основные из них включают:

– безопасное тестирование, симуляция атак и сбоев без воздействия на реальные объекты;

– снижение времени выявления инцидентов и локализации угроз;

– мониторинг в реальном времени, оперативная актуализация информации о состоянии системы;

– верификация изменений до их внедрения в реальные системы;

– повышение подготовки персонала, возможность для виртуального обучения и отработки сценариев реагирования на инциденты ИБ.

Проблемы использования цифровых двойников в задачах обеспечения информационной безопасности критической информационной инфраструктуры

Несмотря на высокий потенциал ЦД, их использование в сфере защиты КИИ сопряжено с рядом проблем и трудностей, которые надлежит учитывать. Для их последующего анализа и разрешения классифицируем эти проблемы по основанию комбинаций категориальных пар: технические vs организационные, де-юре vs де-факто.

Выбор первой оси классификации обусловлен тем, что ЦД в задачах ИБ представляет собой организационно-техническую систему. Это соответствует традиционному делению защитных мер на технические и организационные. Выбор второй оси связан с существующей практикой: нормативно-правовое регулирование информационной безопасности зачастую отстает от лучших отраслевых практик, в результате чего возникают расхождения между де-юре требованиями и де-факто реалиями.

Получаем следующие сгруппированные проблемы:

– технические де-факто;

– технические де-юре;

– организационные де-факто;

– организационные де-юре.

Результаты категориальной классификации проблем (тенденций) приведены в таблице 3. При этом используется следующая логика описания: «Тенденция → Существует vs Требуется → Следствие ← Причина ← Возможное решение».

Проблемы, возникающие при использовании ЦД в задачах обеспечения ИБ КИИ, не умаляют потенциала последних. Однако для того чтобы они стали полноценным инструментом защиты, необходимо ответить на ряд ключевых вопросов как теоретического, так и практического толка.

DOI: 10.31854/2307-1303-2023-11-4-36-47
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_4/36-47.pdf

Таблица 3 – Тенденции в использовании ЦД в задачах обеспечения ИБ КИИ

Тенденция	Существует	Требуется	Причина	Следствие	Решение
1. Рост сложности цифровых моделей	Ограниченная точность моделирования и высокая ресурсоемкость	Повышение точности моделей при оптимизации использования ресурсов	Ограниченные вычислительные мощности, неточные исходные данные	Ошибки в моделях, снижение эффективности защиты	Оптимизация моделей, использование более мощных вычислительных систем
2. Увеличение объема данных	Задержки синхронизации	Обеспечение актуальности данных в реальном времени	Низкая пропускная способность каналов, несогласованность форматов данных	Устаревание информации, снижение оперативности анализа	Использование более быстрых каналов передачи данных, стандартизация форматов
3. Конвергенция ИБ-систем	Проблемы интеграции ЦД с существующими средствами ИБ	Бесшовная интеграция цифровых двойников	Разнородность систем, отсутствие единого стандарта интеграции	Несовместимость, появление уязвимостей	Разработка стандартов взаимодействия, внедрение универсальных интерфейсов
4. Развитие атак на новые поверхности	Уязвимости в ЦД (например, открытые API, каналы телеметрии)	Усиленная защита сервисов и каналов передачи данных	Недостаточная проработка безопасности компонентов ЦД	Экспозиция данных и нарушение функционирования КИИ	Устранение уязвимостей, внедрение шифрования и защиты каналов связи
5. Рост числа ЦД	Недостаточная защита ЦД как критической системы	Комплексная защита ЦД	Недостаток специфических методик защиты ЦД	Использование ЦД в качестве точки доступа для атак	Разработка безопасных методов проектирования и эксплуатации ЦД
6. Быстрое развитие технологий	Недостаток стандартов эксплуатации ЦД	Стандартизация процессов эксплуатации и обслуживания ЦД	Неопределенность в подходах к эксплуатации и обслуживанию ЦД	Неэффективная интеграция, повышение операционных рисков	Разработка и внедрение отраслевых и международных стандартов для ЦД
7. Дефицит квалифицированных кадров	Недостаточная квалификация специалистов	Подготовка квалифицированных специалистов для работы с ЦД в ИБ	Недостаток профильных образовательных программ	Ошибки при внедрении и эксплуатации технологий	Разработка образовательных программ и сертификационных курсов
8. Правовая неопределенность	Отсутствие правового статуса данных ЦД	Регламентация правового статуса данных, полученных из ЦД	Отставание нормативных документов от технологических реалий	Проблемы использования данных в правовых процедурах	Разработка нормативных актов, определяющих статус данных ЦД в юридической практике

DOI: 10.31854/2307-1303-2023-11-4-36-47
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_4/36-47.pdf

Тенденция	Существует	Требуется	Причина	Следствие	Решение
9. Точность фиксации событий	Несоответствие временных меток данных	Унификация временных меток в рамках всех систем	Несогласованность механизмов синхронизации времени	Недостоверная хронология событий	Внедрение стандартизированных механизмов синхронизации времени
10. Недостаточная зрелость процессов эксплуатации	Ошибочные прогнозы, ложные тревоги, неэффективные реакции	Повышение надежности процессов эксплуатации ЦД	Неверные данные, неправильная интерпретация аналитики	Нарушение работы КИИ, неправильное реагирование на угрозы	Внедрение системы верификации и тестирования данных, улучшение процессов анализа инцидентов
11. Рост числа инцидентов	Потенциальная утрата доверия к технологии после инцидентов	Повышение прозрачности и контроль за эксплуатацией ЦД	Недостаточная отчетность по инцидентам, отсутствие механизмов реагирования	Отказ от использования ЦД, ослабление защиты критических систем	Разработка системы мониторинга инцидентов и процессов управления ими
12. Усиление целевых атак	Потенциальные угрозы через внедрение вредоносных компонентов в ЦД	Комплексная проверка ЦД на наличие уязвимостей и вредоносных элементов	Отсутствие достаточных проверок на уровне проектирования и эксплуатации ЦД	Масштабные нарушения работы систем	Установление строгих процедур тестирования и верификации компонентов ЦД

Анализ результатов категориальной классификации позволяет сделать вывод о том, что эффективное использование ЦД в защите КИИ требует системного подхода, объединяющего технологические, организационные и правовые аспекты. Ключевой задачей является устранение разрыва между формальными нормами (де-юре) и реальными практиками (де-факто). Для этого целесообразно реализовать следующие меры:

– Технические меры (оптимизация моделей, шифрование, стандартизация данных) должны повысить устойчивость ЦД к атакам и обеспечить их работоспособность.

– Организационные решения (подготовка кадров, мониторинг инцидентов, внедрение стандартов) критичны для минимизации человеческих ошибок.

– Правовое регулирование (статус данных ЦД, отраслевые стандарты) необходимо для легитимации технологий.

Для наглядности классификация тенденций, представленных в таблице 3, сведена в двумерную матрицу (таблица 4). В данной матрице каждая тенденция отнесена к одной из четырех категорий в зависимости от характера ее происхождения (технического или организационного), а также от ее проявления в де-факто практике или де-юре нормативной сфере. Номера соответствуют идентификаторам в таблице 3.

Таблица 4 – Распределение проблем использования ЦД по категориям

Тенденции	Де-факто	Де-юре
Технические	Характеристика: связаны с реальной эксплуатацией ЦД, например, сложностью моделей, объемом данных, уязвимостями и несогласованностью технических механизмов. Номера: 1, 2, 4, 9, 10	Характеристика: вызванны отсутствием технических стандартов и методик для разработки, верификации и эксплуатации ЦД. Номера: 5, 6, 12
Организационные	Характеристика: проблемы управления, взаимодействия и кадрового обеспечения, возникающие в практической деятельности при использовании ЦД. Номера: 7, 11	Характеристика: обусловлены отсутствием нормативных требований, методических регламентов и правового статуса для организационного применения ЦД. Номера: 3, 8

Представленная классификация проблем использования ЦД в сфере ИБ объектов КИИ помогает структурировать анализ и определить приоритетные направления реагирования. Такая категоризация является динамичной: по мере развития технологий, управленческих практик и нормативной базы проблемы могут перемещаться между квадрантами. Поэтому важно регулярно пересматривать такую классификацию и адаптировать меры реагирования в соответствии с текущими реалиями.

Достижение устойчивых результатов возможно только при синхронном развитии всех указанных направлений: устранение технических уязвимостей без соответствующего нормативно-правового обеспечения приведет к ограничению масштабируемости решений, тогда как совершенствование нормативной базы без технологической поддержки останется декларативным.

Таким образом, приоритетной задачей выступает формирование согласованной системы, в рамках которой технологические инновации в области ЦД будут сопровождаться адекватным правовым регулированием, наличием подготовленных кадров и отлаженными организационными процессами. При соблюдении этих условий цифровые двойники смогут выполнять роль не только инструмента симуляционного моделирования, но и стать основой для построения устойчивой системы обеспечения безопасности КИИ. Без решения названных проблем, ЦД могут стать дополнительным источником уязвимостей, что приведет к снижению общей безопасности объектов КИИ.

Выводы

Цифровые двойники обладают значительным потенциалом для повышения устойчивости и адаптивности систем ИБ в КИИ. Их применение позволяет проводить моделирование угроз, тестирование защитных решений, оптимизацию процессов реагирования и обучение персонала в условиях, приближенных

к реальным. Вместе с тем, практическое внедрение ЦД сопряжено с рядом нерешенных вопросов, включая технические ограничения, угрозы безопасности, а также отсутствие единых организационно-правовых подходов.

Особое внимание в дальнейшем следует уделить исследованию вопросов, связанных с потенциальным воздействием на цифровые двойники как на активные элементы инфраструктуры. Уже сегодня они функционируют не просто как модели, а как самостоятельные субъекты информационного взаимодействия, участвующие в принятии решений и формировании реакции системы на внешние воздействия. Это требует переосмысления подходов к доверию, управлению и контролю таких компонентов.

Будущие исследования должны быть направлены на разработку теоретических и методологических основ безопасного функционирования ЦД, а также на оценку их воздействия на архитектуру и динамику информационной безопасности КИИ. Формирование научно обоснованных подходов к регулированию, верификации и аттестации цифровых двойников станет ключевым условием их безопасной и эффективной интеграции в КИИ. Таким образом, практическое внедрение ЦД должно идти в тесной связи с научным осмыслением их роли и последствий.

Литература

1. Федорова А. В., Шведенко В. Н. Концепция применения технологии цифровых двойников для объединения информационных систем нескольких предприятий в условиях их слияния // Информационно-экономические аспекты стандартизации и технического регулирования. 2023. № 1 (71). С. 46–51. EDN: JEKBCL

2. Jiang Y., Yin S., Li K., Luo H., Kaynak O. Industrial applications of digital twins // Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 2021. Vol. 379. P. 20200360. DOI: 10.1098/rsta.2020.0360. EDN: PFXCGJ

3. Lu Y., Liu C., Kevin I., Huang H., Xu X. Digital Twin-driven smart manufacturing: Connotation, reference model, applications and research issues // Robotics and Computer-Integrated Manufacturing. 2020. Vol. 61. P. 101837. DOI: 10.1016/j.rcim.2019.101837. EDN: GADGUL

4. Тарануха Н. Л., Семенова С. В., Панков С. Н. Цифровой двойник – эффективный инструмент цифровой трансформации промышленных предприятий // Интеллектуальные системы в производстве. 2023. Т. 21. № 3. С. 11–26. DOI 10.22213/2410-9304-2023-3-11-26

5. Jones D., Snider C., Nassehi A., Yon J., Hicks B. Characterising the Digital Twin: A systematic literature review // CIRP Journal of Manufacturing Science and Technology. 2020. Vol. 29. PP. 36-52. DOI: 10.1016/j.cirpj.2020.02.002

6. Stavropoulos P., Mourtzis D. Digital twins in industry 4.0 // Design and Operation of Production Networks for Mass Personalization in the Era of Cloud Technology. Elsevier, 2022. PP. 277–316. DOI: 10.1016/B978-0-12-823657-4.00010-5. EDN: BSWDIE

7. Tao F., Zhang M., Cheng J., Qi Q. Digital twin-driven product design framework // International Journal of Production Research. 2019. Vol. 57. Iss. 12. PP. 3935–3953. DOI: 10.1080/00207543.2018.1443229. EDN: XIECPS

8. Шекочихин О. В. Объектно-процессная модель данных в управляющих информационных системах // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 2. С. 318–323. DOI: 10.17586/2226-1494-2017-17-2-318-323. EDN: YKMXGJ

9. Золотарев В. В., Лапина М. А. Модель и алгоритм управления информационной безопасностью образовательной организации высшего образования с учетом требований управления на основе данных // Прикаспийский журнал: управление и высокие технологии. 2022. № 4 (60). С. 109–118. DOI: 10.54398/20741707_2022_4_107. EDN: GXZNUS

10. Касимова А. Р., Золотарев В. В., Сафиуллина Л. Х., Балыбердин А. С. Использование цифрового двойника в задачах управления информационной безопасностью // Прикаспийский журнал: управление и высокие технологии. 2023. № 1 (61). С. 49–58. DOI: 10.54398/20741707_2023_1_48. EDN: GVJYUN

11. Хорзова И. С. Применение возможностей киберполигона для подготовки и повышения квалификации специалистов по информационной безопасности // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: Сборник материалов Всероссийской научно-практической конференции (Воронеж, 10 июня 2021 г.). Воронеж, 2021. С. 46–47. EDN: DWKHUU

12. Dirnfeld P., De Donato L., Flammini F., Samanazari M., Vittorini V. Railway Digital Twins and Artificial Intelligence: Challenges and Design Guidelines // Digital Twin Technologies and Smart Cities. 2022. PP. 121–135. DOI: 10.1007/978-3-031-16245-9_8

13. Varghese S. A., Ghadim A. D., Balador A., Alimadadi Z., Papadimitratos P. Digital Twin-based Intrusion Detection for Industrial Control Systems // Proceedings of the International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops, Pisa, Italy, 21–25 March 2022). IEEE, 2022. DOI: 10.1109/PerComWorkshops53856.2022.9767492

14. Söderberg R., Wärmefjord K., Carlson J. S., Lindkvist L. Toward a Digital Twin for real-time geometry assurance in individualized production // CIRP Annals. 2017. Vol. 66. Iss. 1. PP. 137–140. DOI: 10.1016/j.cirp.2017.04.038

15. Петрищева К. Г. Разработка цифрового двойника городской инфраструктуры как инструмента обеспечения информационной безопасности // Российская наука и образование сегодня: проблемы и перспективы. 2022. Т. 4. № 1 (43). С. 53–57. EDN: OXULYW

16. Шекочихин О. В. Современные тенденции управления киберфизическими системами на основе цифровых двойников // Информационно-экономические аспекты стандартизации и технического регулирования. 2021. № 5 (63). С. 33–37. EDN: CWLRZC

Статья поступила 01 ноября 2023 г.
Одобрена после рецензирования 27 ноября 2023 г.
Принята к публикации 25 декабря 2023 г.

Информация об авторе

Митяков Евгений Сергеевич – доктор экономических наук, профессор. профессор кафедры информатики МИРЭА – Российского технологического университета. E-mail: iyao@mail.ru

Problems of Using Digital Twins in Ensuring Information Security of Critical Information Infrastructure Facilities

Mitaykov E.

MIREA – Russian Technological University,
Moscow, 119454, Russian Federation

Problem Statement. *In the context of rapid digitalization of the economy and public administration, ensuring the information security (IS) of critical information infrastructure (CII) has become an increasingly urgent task. CII includes facilities that play a key role in the functioning of vital sectors of society such as energy, transportation, healthcare, industry, and others. As these systems grow in complexity, the need arises for advanced technologies to ensure their protection. One such tool is the use of digital twins (DTs), which enable the modeling of threats and the testing of security measures. However, the integration of DTs into IS tasks within CII encounters a number of challenges that must be addressed for the effective implementation of this technology.* ***The aim of this study*** *is to identify the key challenges associated with the use of digital twins in the context of CII information security.* ***Methods.*** *The research employs the analysis of standards, classification of problems by category (technical, organizational, legal), and evaluation of DT usage scenarios within CII.* ***Novelty.*** *This work identifies new aspects of DT application within CII, particularly related to model characteristics, as well as issues of verification and integrity control of digital models. Security concerns are addressed, including risks associated with open APIs and telemetry channels, which may serve as vectors for attacks. A set of measures is proposed to overcome these challenges, including the development of regulatory standards for DT usage and the enhancement of professional training.* ***Results.*** *Key challenges have been identified and classified into the following categories: technical, security-related, organizational, legal, and those arising from incorrect usage. Each category encompasses specific issues, the consequences of which range from modeling errors and reduced protection efficiency to threats of critical infrastructure compromise and loss of trust in the technology.* ***Theoretical / Practical Significance.*** *The results of this study contribute to improving approaches to ensuring the information security of CII through the use of digital twins. The proposed recommendations for addressing identified challenges can be used to enhance the reliability, safety, and effectiveness of DT implementation and operation in CII systems.*

Keywords: *information security, critical information infrastructure, digital twin, data synchronization, threat modelling*

Information about Author

Evgeny Mityakov − Holder of an Advanced Doctorate in Economics, Professor at the Department of Informatics (MIREA – Russian Technological University).
E-mail: iyao@mail.ru

DOI: 10.31854/2307-1303-2023-11-4-36-47
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2023_4/36-47.pdf