Баранов Егор Валерьевич
студент, кафедра управления в технических системах,
ГУАП,
РФ, г. Санкт-Петербург

ЦИФРОВЫЕ ДВОЙНИКИ В ПРОМЫШЛЕННОСТИ: АКТУАЛЬНЫЕ ВЫЗОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: Статья посвящена анализу актуальных вызовов в области информационной безопасности, возникающих при внедрении и эксплуатации цифровых двойников в промышленном секторе. Рассматриваются особенности цифровых двойников как объекта защиты и выделены основные угрозы их безопасности: правовые, организационные, технические и технологические. Предложены направления по обеспечению безопасности при интеграции цифровых двойников в критическую инфраструктуру.

Ключевые слова: цифровые двойники, информационная безопасность, промышленность, критическая информационная инфраструктура, киберугрозы, промышленный интернет вещей, искусственный интеллект.

Введение. Повсеместное распространение технологий Индустрии 4.0 приводит к тому, что промышленные предприятия активно создают сложные киберфизические системы, что соответствует общемировым трендам цифровизации. В этом контексте цифровые двойники (ЦД)— виртуальные динамические модели, синхронизированные с физическими объектами, — перестают быть лишь инструментом проектирования и становятся ключевым элементом операционного управления. Однако их интеграция в реальные производственные циклы, особенно в сферах, связанных с критической информационной инфраструктурой (КИИ), порождает принципиально новые риски. Если кибератака на традиционную информационную систему ведет к утрате данных, то компрометация цифрового двойника, управляющего, к примеру, энергосетью или нефтепроводом, способна инициировать реальную техногенную катастрофу [6]. Таким образом, проблема защиты ЦД выходит за рамки классической кибербезопасности, превращаясь в вопрос обеспечения национальной и технологической безопасности.

Цель данного исследования — систематизировать и проанализировать современные вызовы в области информационной безопасности, возникающие при внедрении и эксплуатации цифровых двойников в промышленном секторе.

Специфика цифрового двойника как объекта защиты. В отличие от статичной цифровой модели, цифровой двойник характеризуется непрерывным двусторонним обменом данными с физическим объектом [2]. Эта особенность коренным образом меняет схему защиты. Во-первых, граница атаки расширяется, включая не только традиционные ИТ-активы, но и всю цепочку данных: от датчиков (уровень Интернета вещей, IoT) через сети передачи до

вычислительных мощностей, на которых функционирует модель. Уязвимость любого звена этой цепи ставит под угрозу защиту всего двойника и может привести к искажению или неточности всего ЦД.

Во-вторых, возникает феномен «цифрового заражения». Злоумышленник, получивший контроль над двойником, может не только искажать его поведение, но и передавать деструктивные команды на физический объект. Например, в нефтегазовой отрасли целенаправленное изменение виртуальной модели трубопровода может спровоцировать нештатное давление в реальной системе, ведущее к разгерметизации. Более того, скомпрометированный двойник можно использовать для маскировки реальной аварии, подменяя данные с датчиков на штатные показатели, что не позволит оператору вовремя среагировать.

Угрозы информационной безопасности цифровых двойников. Использование ЦД в сфере защиты критической информационной инфраструктуры (КИИ) связано с рядом угроз. Виды угроз приведены в Таблице 1:

Таблица 1- Виды угроз информационной безопасности цифровых двойников.

Виды угроз	Описание
Правовые (отсутствие нормативных требований, технических стандартов и правового статуса для применения ЦД)	Правовая неопределенность: норм, регулирующих эксплуатацию, аудит и безопасность ЦД. (Сложность вызывает сама процедура категорирования цифрового двойника)
	Применение некорректного ЦД. (Незаконное копирование элементов или полного копирования двойника)
Организационные (управление и кадровое обеспечение, возникающее в практической деятельности при использовании ЦД)	Некорректное внедрение и эксплуатация технологий.(Обусловлены дефектами сетевой архитектуры и топологии)
	Дефицит квалифицированных кадров для работы ЦД в области ИБ. (Эффективная защита требует от специалистов глубоких знаний в промышленной автоматизации, Data Science и кибербезопасности)
Технические угрозы (уязвимость алгоритмов , достоверность данных,верификация и эксплуатация ЦД)	Уязвимость алгоритмов и моделей.(ЦД всё больше используют ИИ и машинное обучение. Изменения во входных данных могут вызывать катастрофические ошибки в работе)
	Угрозы целостности и достоверности данных. (Функционирование ЦД зависит от качества входящих данных, что порождает риски

	целенаправленных атак и позволяет манипулировать показаниями. Несертифицированное или устаревшее ПО. Создание «лживого двойника», чьи прогнозы и решения основаны на недостоверной информации)
	Обеспечение безопасности программных платформ и компонентов, на которых строятся ЦД. (Использование готовых решений и библиотек с открытым исходным кодом создает риски, связанные с наличием невыявленных уязвимостей. Ускоренный переход на отечественное ПО может происходить без должного цикла тестирования на устойчивость к целевым кибератакам. Необходимость создания строгих процедур верификации и сертификации используемого ПО).
Технологические (внедрение и эксплуатация ЦД)	Сложности интеграции различных систем и источников данных. (Разнообразие протоколов и стандартов передачи данных, несовместимость с устаревшими системами)
	Системные атаки- кибератаки. (Несанкционированный доступ к информационным системам. Уязвимость в технологиях, ошибках конфигурации или поведении пользователей. Проникновение в инфраструктуру, с целью нарушить её работу или украсть данные)

Помимо вышеперечисленных угроз, значительным барьером остается организационное сопротивление и недостаточная осведомленность руководящего состава промышленных предприятий. Технические специалисты не всегда могут убедительно донести до руководителей высшего звена всю серьезность киберугроз для ЦД, поскольку склонны воспринимать их как абстрактные ИТ-риски, а не как прямую угрозу физическому производству. Это приводит к недофинансированию программ кибербезопасности, игнорированию рекомендаций по архитектурной защите и возложению ответственности на традиционные ИТ-подразделения, не обладающие компетенциями в области промышленных систем. Преодоление этого разрыва между техническими и управленческими звеньями является критически важным условием для выстраивания эффективной системы защиты.

Вместе с тем, наблюдаются шаги по систематизации требований к подобным сложным киберфизическим системам. Инициативы регуляторов, в частности ФСТЭК России [4], постепенно смещаются от защиты статичных ИС к регулированию процессов непрерывного обмена данными, что составляет основу функционирования цифровых двойников. Параллельно в рамках ведомственных проектов, таких как «Цифровая промышленность»

Минпромторга России, формируются предпосылки для отраслевых стандартов, касающихся оценки цифровой зрелости и безопасности технологических процессов [3]. Несмотря на то, что эти усилия пока носят фрагментарный характер и не предлагают целостной правовой модели для ЦД, они задают вектор для будущей работы по созданию нормативного поля [5].

Перспективные направления обеспечения безопасности цифрового двойника. Для преодоления существующих проблем необходимо применять комплексные меры, направленные на противодействие всем категориям угроз:

1. Правовые. Разработка отраслевых стандартов и методических рекомендаций, конкретизирующих требования к защите ЦД в рамках законодательства о КИИ. Стимулирование создания образовательных программ, готовящих специалистов, способных работать на стыке операционных и ИТ.

2. Организационные. Перспективным направлением представляется разработка и внедрение архитектурных систем, изначально предполагающих враждебное окружение. Речь идет о принципах «минимальных привилегий» и «нулевого доверия» (Zero Trust) [7,12], применяемых к потокам данных между физическим объектом и его двойником. Каждый запрос на изменение состояния или получение данных подвергается строгой аутентификации и авторизации, независимо от его источника.

3. Технические. Ключевым направлением является развитие систем проактивного мониторинга и прогнозирования угроз, основанных на анализе поведения ЦД. Вместо поиска известных образцов вредоносного кода, такие системы отслеживают аномалии в работе модели — отклонения вычислительной сложности, нештатные шаблоны обращений к данным, логические несоответствия между прогнозом и реальными показателями. Машинное обучение может использоваться для формирования «цифрового отпечатка» нормального поведения двойника, что позволяет с высокой точностью выявлять целенаправленные атаки, включая те, что направлены на алгоритмы ИИ, и инициировать ответные меры до наступления необратимых последствий [3].

4.Технологические. Разработка и внедрение специализированных протоколов безопасности для всего жизненного цикла ЦД. Обязательное сквозное шифрование информации от сенсора до вычислительного кластера, внедрение систем активного мониторинга аномалий в поведении модели, а также создание защищенных «песочниц» для тестирования двойников без риска для реального производства.

Заключение. Цифровые двойники открывают перед промышленностью беспрецедентные возможности не только по повышению эффективности, но и безопасности

производственных процессов. Однако их киберустойчивость становится критическим фактором, определяющим не только экономический успех предприятия, но и его способность избегать катастрофических инцидентов. Актуальные вызовы носят системный характер, проистекая из технологической сложности самих двойников, правового запаздывания и кадрового дефицита. Исследования должны быть сконцентрированы на разработке архитектур безопасных двойников, формализации моделей угроз для систем с искусственным интеллектом и создании эффективных механизмов их сертификации. Только так можно будет реализовать потенциал этой технологии, минимизировав сопутствующие ей риски для промышленности.

В качестве первоочередных мер, способных существенно повысить уровень защищенности промышленных цифровых двойников, представляется целесообразным сосредоточить усилия на нескольких направлениях. Архитектурный принцип «нулевого доверия» (Zero Trust) позволяет выстроить систему верификации каждого запроса в цепи взаимодействия между физическим объектом и его виртуальной репликой. Разработка специализированных профилей защиты и требований сертификации программных компонентов, используемых в таких системах, создаст основу для их безопасной интеграции. Одновременно с этим формирование системы проактивного мониторинга, основанной на анализе поведенческих аномалий цифрового двойника, позволит выявлять целевые атаки на ранних стадиях их реализации.

Библиографический список

1. Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 07.04.2025) «О безопасности критической информационной инфраструктуры Российской Федерации». – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=501334 (дата обращения: 13.11.2025).

2. ГОСТ Р 57700.37-2021. Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения. – Введ. 2021-09-16. – М.: Стандартинформ, 2021. – URL: https://meganorm.ru/mega_doc/norm/gost-r_gosudarstvennyj-standart/10/gost_r_57700_37-2021_natsionalnyy_standart_rossiyskoy.html (дата обращения: 13.11.2025).

3. Распоряжение Правительства РФ от 07.11.2023 № 3113-р «Об утверждении стратегического направления в области цифровой трансформации обрабатывающих отраслей промышленности...». – URL: http://government.ru/docs/50038/ (дата обращения: 13.11.2025).

4. Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 28.08.2024) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». URL:

https://normativ.kontur.ru/document?moduleId=1&documentId=481283 (дата обращения: 13.11.2025).

5. Ведомственный проект «Цифровая промышленность» Министерства промышленности и торговли Российской Федерации. URL: https://digital.gov.ru/uploaded/files/vedomstvennyij-proekt-tsifrovaya-promyishlennost.pdf (дата обращения: 13.11.2025).

6. Митяков Е. С. Цифровые двойники и безопасность критической информационной инфраструктуры: правовые и технологические аспекты // Национальная безопасность и стратегическое планирование. – 2024. – № 4. – С. 29-34. – DOI: https://doi.org/10.37468/2307-1400-2024-4-29-34. (дата обращения: 13.11.2025).

7. Джо Ли .Что такое принцип минимальных привилегий? Последнее обновление 2025/10/09 URL: https://www.trendmicro.com/ru_ru/what-is/what-is-zero-trust/principle-of-least-privilege.html (дата обращения: 16.11.2025).

8. Цифровизация промышленности 2024: аналитический обзор. – CNews, 2024. – URL: https://www.cnews.ru/reviews/tsifrovizatsiya_promyshlennosti_2024 (дата обращения: 15.11.2025).

9. Лавренко Е. В., Мечикова М. Н. Цифровая трансформация промышленности: российский и зарубежный опыт // Вестник СИБИТа. – 2022. – № 1. – С. 25-31. – URL: https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-promyshlennosti-rossiyskiy-i-zarubezhnyy-opyt (дата обращения: 14.11.2025).

10. Карташева Н. В. Цифровая трансформация в промышленности [Электронный ресурс] / Н. В. Карташева // Центр оценки и кадрового развития специалистов в области цифровой трансформации (Рекрутинговый центр) Президентской академии РАНХиГС. – Москва, 2023. – URL: https://cdto.work/2023/05/25/cifrovaja-transformacija-v-promyshlennosti/ (дата обращения: 13.11.2025).

11. Казанбиева А. Х., Гасанова А. Д. Инновационные подходы к цифровой трансформации в современной промышленности России: перспективы и вызовы // Вестник Академии знаний. – 2024. – № 3 (62). – С. 215-223. – URL: https://cyberleninka.ru/article/n/innovatsionnye-podhody-k-tsifrovoy-transformatsii-v-sovremennoy-promyshlennosti-rossii-perspektivy-i-vyzovy (дата обращения: 14.11.2025).

12. Волков С. И. Принцип нулевого доверия: что это и зачем бизнесу.Бизнес 16 сентября 2025 URL: https://www.xcom.ru/blog/business/printsip-nulevogo-doveriya-chto-eto-i-zachem-biznesu/(дата обращения: 16.11.2025).