УДК 004.056
https://doi.org/10.31854/2307-1303-2024-12-4-1-12
EDN: RQVZLW

Цифровые двойники как объект и инструмент информационной безопасности

Митяков Е. С.

МИРЭА – Российский технологический университет
Москва, 119454, Российская Федерация

Постановка задачи. *Расширение использования цифровых двойников в критически важных отраслях сопровождается ростом киберугроз, нацеленных как на сами двойники, так и на инфраструктуру, с которой они взаимодействуют. Современные подходы в информационной безопасности либо используют цифровых двойников как инструмент моделирования угроз, либо направлены на их защиту как объектов, однако редко учитывают их двуединую природу. Возникает необходимость в создании двуединой архитектуры, способной интегрировать цифровых двойников в замкнутый контур киберзащиты.* ***Цель исследования:*** *разработка концептуальной модели, обеспечивающей двустороннее взаимодействие цифровых двойников в рамках систем информационной безопасности, где цифровой двойник одновременно выступает как активный предиктивный элемент и как объект защиты.* ***Методы:*** *в работе использованы методы формальной логики, вероятностного моделирования, а также симуляционные подходы для генерации сценариев кибератак. Архитектура модели формализована в виде динамической системы с двумя взаимосвязанными подсистемами – прогнозирования и защиты.* ***Результаты:*** *построена концептуальная модель двустороннего взаимодействия цифровых двойников в системе информационной безопасности, включающая компоненты предикции, симуляции атак, обнаружения аномалий, управления доступом и формальной верификации. Проведен эксперимент с синтетическими данными, моделирующими DDoS-атаки. Продемонстрировано повышение точности прогнозов угроз на 12 % и улучшение устойчивости цифровых двойников к повторным атакам.* ***Новизна:*** *предложена концепция интеграции цифрового двойника как субъекта и объекта информационной безопасности в единой модели с адаптивной корректировкой параметров на основе анализа угроз.* ***Практическая значимость:*** *разработанная модель применима при проектировании защищенных цифровых двойников, а также может использоваться в качестве основы для стандартизации решений в области информационной безопасности.*

Ключевые слова: *цифровой двойник, информационная безопасность, моделирование, киберугрозы, концептуальная модель взаимодействия, симуляция атак, защита цифровых двойников*

Актуальность

Активное внедрение цифровых технологий в промышленность, IoT-устройства, облачные сервисы и корпоративные сети увеличивает поверхность компьютерных атак. Традиционные методы защиты, основанные на реактивном

Библиографическая ссылка на статью:
Митяков Е. С. Цифровые двойники как объект и инструмент информационной безопасности // Информационные технологии и телекоммуникации. 2024. Т. 12. № 4. С. 1–12. DOI: 10.31854/2307-1303-2024-12-4-1-12. EDN: RQVZLW

Reference for citation:
Mityakov E. Digital Twins as an Object and Tool of Information Security // Telecom IT. 2024. Vol. 12. Iss. 4. PP. 1–12. (in Russian). DOI: 10.31854/2307-1303-2024-12-4-1-12. EDN: RQVZLW

обнаружении угроз, зачастую не справляются с динамичными атаками нового поколения – такими как цепочки нулевых уязвимостей, целевой фишинг или атаки на цепочки поставок. Это требует перехода к проактивным подходам, способным прогнозировать угрозы до их реализации.

Цифровые двойники (ЦД) позволяют моделировать поведение цифровых систем в условиях кибератак, тестировать сценарии защиты и оптимизировать процессы восстановления. Например, виртуальные копии промышленных сетей могут имитировать атаки на SCADA-системы, выявляя слабые места без риска для реального оборудования. Однако потенциал ЦД в информационной безопасности (ИБ) ограничен отсутствием универсальных методик их интеграции в системы мониторинга и реагирования, а также нехваткой исследований по адаптации моделей под различные типы угроз. Сами ЦД, будучи сложными цифровыми системами, встроенными в контур функционирования реальных систем, становятся мишенями для злоумышленников. Компрометация их компонентов (например, подмена данных в модели или взлом API) может привести к ложным прогнозам, некорректным решениям и даже каскадным сбоям в реальных системах. Существующие методы защиты ЦД фрагментарны и не учитывают специфику их архитектуры, что требует разработки специализированных решений.

Эффективность ЦД как инструмента ИБ напрямую зависит от их собственной безопасности. Например, двойник IoT-сети, используемый для выявления уязвимостей, должен быть защищен от компрометации, чтобы его анализ оставался достоверным. Это создает двуединую задачу. Во-первых, целесообразно использовать ЦД для моделирования угроз и оптимизации защиты, а во-вторых – обеспечить безопасность самих ЦД. Без решения этой задачи внедрение технологии приведет к парадоксу: инструмент, призванный усиливать информационную безопасность, сам станет ее слабым звеном.

Настоящее исследование направлено на устранение пробелов в области концептуального моделирования ЦД и их защиты. Результаты могут лечь в основу стандартов безопасности для архитектуры ЦД, включая требования к синхронизации данных и аудиту, а также методик обучения специалистов, способных работать с ЦД как в роли защитников, так и в роли объектов защиты. Это особенно актуально для отраслей с высокими требованиями к киберустойчивости, где ошибки в защите ЦД могут иметь катастрофические социально-экономические последствия (например, в сферах деятельности субъектов критической информационной инфраструктуры).

Таким образом, актуальность работы обусловлена необходимостью создания системы, где ЦД одновременно служат инструментом противодействия угрозам и защищены от них.

Анализ современных подходов к применению цифровых двойников в информационной безопасности

ЦД представляет собой виртуальную модель, созданную для отображения с необходимой точностью характеристик и поведения конкретного физического объекта, процесса или субъекта [1]. Это программная сущность, обладающая

способностью моделировать и воспроизводить уникальные свойства своего реального прототипа в цифровой среде. ЦД могут охватывать как отдельные элементы (например, устройства, системы, организации), так и абстрактные категории (например, человеческое поведение или социальные процессы). Объединение данных, получаемых от различных ЦД, позволяет формировать многомерное и целостное представление о функционировании сложных физических и киберфизических и социотехнических систем.

Концепция ЦД возникла как эволюция методов виртуального моделирования, которые сформировались в результате развития автоматизированных систем проектирования (CAD, *аббр. от англ.* Computer Aided Design) и производства (CAM, *аббр. от англ.* Computer Aided Manufacturing), а также в рамках подходов к управлению жизненным циклом изделия (PLM, *аббр. от англ.* Product Lifecycle Management) и системам управления данными о продукте (PDM, *аббр. от англ.* Product Data Management) [2]. Понятие «цифровой двойник» (*от англ.* Digital Twin) было введено М. Гривсом в 2002 г. для обозначения цифровой репрезентации реального изделия или системы, способной функционировать синхронно с физическим объектом в условиях моделирования его поведения и характеристик [3]. В 2017 г. М. Гривс совместно с Дж. Викерсом уточнил данное определение, представив ЦД как виртуальный аналог физического объекта, содержащий исчерпывающие сведения на всех уровнях детализации – от микроструктурных до макроскопических, что позволяет осуществлять интеграцию информации в цифровую модель [4]. Однако подобная трактовка ограничивает сферу применения концепции исключительно физическими объектами и не раскрывает архитектурную основу и функциональную универсальность ЦД, применимых также к процессам, организациям и даже социальным структурам.

Обзор различных определений концепции ЦД выявляет разнообразие подходов к ее трактовке в разных областях. В исследовании [5] ЦД трактуется как совокупность адаптивных моделей, имитирующих функционирование физического объекта в цифровой среде с непрерывной актуализацией данных в реальном времени. В другом подходе [6] ЦД понимается как статичное цифровое отображение реального объекта, без обязательного взаимодействия с ним. В работе [7] ЦД рассматривается более широко – как уникальная цифровая сущность продукта, охватывающая не только его физическую составляющую, но и сопровождающие сервисы. В работе [8] особое внимание уделяется непрерывному двустороннему обмену данными между цифровой моделью и физическим прототипом на всех этапах жизненного цикла. В другом определении ЦД описывается как модель, которая адаптируется к операционным изменениям, прогнозируя будущее состояние физического объекта на основе данных, собранных в реальном времени [9]. Таким образом, несмотря на существующий методологический плюрализм в трактовке концепции ЦД, можно выделить общую черту: независимо от подхода, ЦД представляет собой модель, способную интегрировать данные и адаптироваться к изменениям, обеспечивая взаимодействие между физическим объектом и его цифровым аналогом.

В информационной безопасности потенциал использования ЦД выражается в способности проводить симуляции атак, анализировать риски и управлять

уязвимостями без вмешательства в физическую инфраструктуру. Однако интеграция ЦД с современными технологиями – киберфизическими системами, промышленным интернетом вещей (IIoT, *аббр. от англ.* Industrial Internet of Things) и искусственным интеллектом (ИИ) – формирует не только новые возможности, но и новые векторы киберугроз [10–12]. Например, развитие концепции Интернета ЦД, в которой множество цифровых моделей взаимодействуют в распределенной среде, порождает значительные проблемы в области безопасности и конфиденциальности. Такие аспекты, как децентрализация и информационно-центричная маршрутизация, затрудняют реализацию традиционных средств ИБ. Кроме того, процессы синхронизации между ЦД и их физическими прототипами могут стать уязвимыми точками входа для злоумышленников, особенно в условиях слабой криптографической или сетевой защиты.

В ответ на вызовы безопасности в научной литературе предлагается ряд решений, направленных на повышение защищенности ЦД. Одним из них является создание кибербезопасных ЦД, которые предназначены для моделирования и анализа потенциальных кибератак без влияния на реальные системы. Такие двойники особенно эффективны в критически важных инфраструктурах, где каждая ошибка может привести к катастрофическим последствиям [12]. Также активно исследуются методы применения глубокого обучения для повышения эффективности систем обнаружения вторжений, что обеспечивает более проактивную защиту сетей [13].

Несмотря на прогресс в отдельных направлениях, существующие подходы, как правило, являются частными и не обеспечивают целостную интеграцию между предиктивными и защитными механизмами. Наблюдается нехватка моделей, способных обеспечить двустороннюю связь между компонентами прогнозирования и системами защиты самого ЦД. В частности, редко реализуется механизм, при котором результаты анализа атак напрямую влияют на изменение поведения модели или корректировку параметров безопасности. В связи с этим возникает потребность в разработке модели, в которой ЦД играет двойную роль: как активный элемент в цепочке обеспечения ИБ и как защищаемый актив. Такая модель должна включать механизмы симуляции, предикции, формальной верификации и защиты от угроз в рамках замкнутого цикла управления рисками и обеспечения безопасности.

Концептуальная модель двустороннего взаимодействия цифровых двойников в системе информационной безопасности

Концептуальная модель двустороннего взаимодействия ЦД в области информационной безопасности представляет собой архитектуру, включающую две взаимосвязанные подсистемы: ЦД как инструмент прогнозирования и предотвращения угроз (Подсистема *A*) и механизмы защиты самого ЦД от кибератак (Подсистема *B*). Совокупное функционирование этих компонентов формирует замкнутый цикл обеспечения информационной безопасности, в котором предиктивный и защитный потенциал ЦД реализуется в едином технологическом контуре (рисунок 1).

Рис. 1. Схема модели

Виртуальная копия системы выступает цифровой моделью, синхронно отражающей состояние физической информационной системы. Она содержит структурные параметры (топологию сети, конфигурации устройств) и поведенческие характеристики (профили трафика, типовые сценарии функционирования).

Подсистема A включает следующие компоненты:

1) модуль синхронизации данных – обеспечивает двусторонний обмен информацией между физической и виртуальной (ЦД) компонентами, использует алгоритмы коррекции погрешностей;

2) модуль прогнозирования угроз – использует алгоритмы машинного обучения для анализа исторических данных и выявления аномалий, что позволяет предсказывать, например, вероятность возникновения атаки, основываясь на детектируемых паттернах сетевого трафика;

3) модуль симуляции атак – генерирует виртуальные сценарии киберугроз, с целью тестирования устойчивости защищаемой системы; при этом эффективность защиты можно оценить по времени обнаружения угрозы и точности идентификации вектора атаки.

DOI: 10.31854/2307-1303-2024-12-4-1-12
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2024_4/1-12.pdf

Подсистема B включает следующие ключевые компоненты, обеспечивающие защиту ЦД как самостоятельного объекта:

1) система обнаружения аномалий – отслеживает поведение ЦД на предмет нестандартных действий и возможных угроз; использует шаблоны известных атак и анализ отклонений в поведении модели (сигнатурный и поведенческий анализ); при выявлении подозрительной активности система должна инициировать автоматическую защитную реакцию, направленную на устранение или локализацию угрозы;

2) модуль защиты данных и управления доступом – обеспечивает конфиденциальность и целостность данных ЦД, ограничения взаимодействия с моделью только проверенными пользователями (шифрование данных, аутентификация, защита каналов передачи данных и др.);

3) модуль верификации – обеспечивает регулярную проверку целостности ЦД; при этом верификация включает как технический контроль структуры данных, так и проверку корректности функционирования алгоритмов прогнозирования.

Функционирование модели основывается на интеграции между двумя указанными подсистемами, что обеспечивается двусторонним обменом данными. Прямая связь реализуется через передачу сценариев потенциальных атак, сформированных в ходе симуляции, в систему обнаружения угроз. Это взаимодействие позволяет расширить существующие механизмы распознавания угроз, добавив новые признаки атак. В обратном направлении данные используются для оптимизации процессов синхронизации между ЦД и физическим объектом. В случае выявления попыток вмешательства параметры модели корректируются.

Формализация модели

Формализация концептуальной модели двустороннего взаимодействия ЦД в ИБ требует представления всех ключевых компонентов как формальных сущностей и описания их взаимодействий. Предлагаемая формализация основывается на кибернетическом подходе и может быть представлена в виде динамической системы с двумя подсистемами.

Формализация подсистемы A (прогнозирование, симуляция и синхронизации)

Функционирование ЦД начинается с процесса *синхронизации*, который обеспечивает соответствие между виртуальным состоянием и реальным объектом:

$$D(t) = \Phi(S(t)) + \epsilon(t),$$

где $S(t)$ – состояние физической информационной системы в момент времени t; $D(t)$ – состояние ЦД в момент времени t; Ф – синхронизатор данных между физической системой и ЦД; $\epsilon(t)$ – погрешность, возникающая в результате задержек, неполноты или искажений данных.

Для *прогнозирования* угроз используется модель, предположительно основанная на алгоритмах машинного обучения, что позволяет вычислить апостериорную вероятность возникновения угрозы T_i в момент времени t с учетом текущего состояния ЦД:

DOI: 10.31854/2307-1303-2024-12-4-1-12
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2024_4/1-12.pdf

$$P(T_i \mid D(t)) = f_{ML}(D(t), H),$$

где $P(T_i|D(t))$ – апостериорная вероятность возникновения угрозы T_i, вычисленная на основе данных ЦД, f_{ML} – функция машинного обучения, использующая ретроспективные данные H для прогнозирования.

Для *симуляции* потенциальных атак используется оператор, моделирующий действия злоумышленников на основе состояния ЦД и множества возможных угроз. Вектор атак в момент времени t определяется как:

$$A(t) = \Gamma(D(t), T),$$

где Γ – оператор симуляции атак; $T = \{T_i\}$ – множество возможных угроз.

Формализация подсистемы B (обнаружение аномалий, защита, верификация)

В подсистеме *B* осуществляется *обнаружение аномалий* в поведении ЦД. Для этого используется функция, сравнивающая текущее поведение ЦД с эталонным, определяя отклонения от нормального функционирования:

$$\Delta(t) = \Psi(D(t), M(t)),$$

где $\Delta(t)$ – вектор отклонений (аномалий) в поведении ЦД, выявленный системой мониторинга; Ψ – функция, выявляющая аномалии; $M(t)$ – мета-состояние модели: целостность, достоверность, корректность функционирования ЦД.

При выявлении аномалии активируется *защитная реакция*, которая может включать блокировку, изоляцию или уведомление о потенциальной угрозе и определяется как:

$$R(t) = \Lambda(\Delta(t)),$$

где $R(t)$ – реакция системы защиты на обнаруженные аномалии; Λ – функция принятия решений о мерах защиты на основе уровня возможностей нарушителей по реализации угроз безопасности информации.

Для обеспечения устойчивости модели и ее защиты от возможных вмешательств, регулярно проводится *верификация* ЦД:

$$M(t) = \Theta(D(t)),$$

где Θ – процедура проверки целостности и корректности функционирования ЦД.

Интеграция подсистем A и B

Подсистемы *A* и *B* взаимосвязаны через двусторонний обмен данными. Передача информации о сценариях потенциальных атак из подсистемы *A* в подсистему *B* осуществляется по следующей формуле:

$$\mathrm{Input}_B(t) = A(t).$$

DOI: 10.31854/2307-1303-2024-12-4-1-12
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2024_4/1-12.pdf

В ответ на данные об угрозах, поступающих из подсистемы *A*, подсистема *B* корректирует модель ЦД. Новое состояние ЦД в момент времени $t + 1$ обновляется следующим образом:

$$D(t+1) = D(t) + \Sigma(t),$$

где $\Sigma(t)$ – набор корректирующих воздействий (автоматическая адаптация модели), определяемый по выражению:

$$\Sigma(t) = \Omega(M(t), R(t)),$$

Ω – функция адаптации модели на основе защитных данных, полученных из подсистемы *B*.

Пример моделирования

Для демонстрации работы предложенной модели проведен эксперимент с использованием синтетических данных, имитирующих сетевой трафик. Цель эксперимента – проверить эффективность прогнозирования угроз (Подсистема *A*) и реакции системы защиты (Подсистема *B*) на аномалии. Далее приведем пошаговую процедуру моделирования.

Шаг 1. Генерация данных. Для моделирования сетевой активности был сгенерирован синтетический временно́й ряд, включающий как фоновый трафик, так и имитацию DDoS-атак. Фоновая нагрузка формировалась на основе нормального распределения с параметрами: математическое ожидание $\mu = 1000$ ед/с и стандартное отклонение $\sigma = 100$ ед/с. Аномальные события, соответствующие DDoS-атакам, имитировались в виде всплесков трафика, превышающих значение 3σ. Модельный набор данных описывается функцией:

$$D(t) = \{x_1, x_2, \dots, x_{1000}\}, x_i \sim N(\mu, \sigma^2),$$

где x_i – это отдельное значение в синтетическом временно́м ряду трафика.

Шаг 2. Прогнозирование угроз (Подсистема A). Для оценки вероятности DDoS-атаки была применена модель логистической регрессии. Вероятность наступления атаки при текущем объеме трафика описывается следующим выражением:

$$P(T_{DDoS} \mid D(t)) = 1 / (1 + \exp(-(\alpha \cdot x_{\text{норм}} + \beta)),$$

где α и β – параметры модели, получены на основе сгенерированных данных, соответствующие значениям $\alpha = 0{,}02$ и $\beta = -30$; $x_{\text{норм}}$ – нормализованное значение трафика:

$$x_{\text{норм}} = \frac{(x - \mu)}{\sigma}.$$

DOI: 10.31854/2307-1303-2024-12-4-1-12
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2024_4/1-12.pdf

Шаг 3. Обнаружение аномалий (Подсистема B). Аномалии в сетевом трафике детектировались по следующему критерию: событие классифицировалось как аномальное, если абсолютное отклонение значения трафика от среднего ($|x-\mu|$) превышало три стандартных отклонения (3σ).

На рисунке 2 представлены распределение сетевого трафика и зависимость вероятности DDoS-атаки от объема трафика. Левый график демонстрирует распределение сетевого трафика в нормальных условиях. Гистограмма отражает частотность различных уровней нагрузки, а наложенная кривая нормального распределения с параметрами $\mu = 1000$ и $\sigma = 100$ служит ориентиром для определения статистических отклонений. Красная вертикальная линия указывает на среднее значение трафика, относительно которого оцениваются потенциальные аномалии. Правый график иллюстрирует прогнозирование вероятности возникновения DDoS-атаки в зависимости от текущего состояния трафика. Аномальные значения, превышающие 3σ, выделены красными точками. Они обозначают потенциально опасные ситуации, способные активировать защитные механизмы подсистемы *B*.

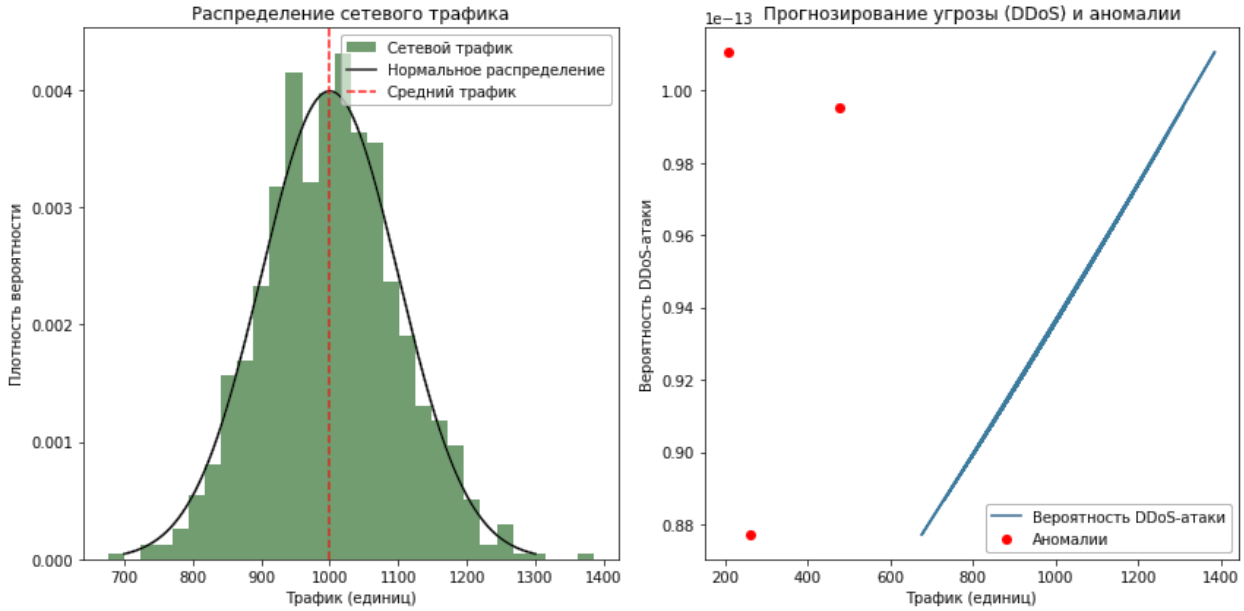

Рис. 2. Распределение сетевого трафика и зависимость вероятности DDoS-атаки от объема трафика

Шаг 4. Адаптация модели. После обнаружения аномалий осуществлялась адаптация модели путем корректировки параметра α:

$$\alpha_{нов} = \alpha + \Delta\alpha,\ \Delta\alpha = 0{,}005 \cdot N_{атак},$$

где $N_{атак}$ – количество зарегистрированных атак.

Обновление параметров обеспечило рост точности прогнозирования на 12 % при повторении аналогичных сценариев.

DOI: 10.31854/2307-1303-2024-12-4-1-12
URL: https://www.sut.ru/doci/nauka/1AEA/ITT/2024_4/1-12.pdf

Заключение

В условиях стремительного развития ИТ и роста киберугроз ЦД выступают одновременно как активный элемент предиктивной киберзащиты и как потенциально уязвимый объект. В статье представлена формализованная модель двустороннего взаимодействия ЦД в контексте ИБ, позволяющая рассматривать их как субъект и объект защиты.

Анализ существующих решений выявил их частность и подтвердил необходимость двуединой архитектуры, сочетающей прогнозирование угроз с механизмами самозащиты ЦД. Предложенная модель, апробированная на синтетических данных, ориентирована на проактивное реагирование и устойчивость к сложным атакам.

Дальнейшие исследования могут быть направлены на развитие адаптивных защитных механизмов, интеграцию ИИ и разработку стандартов безопасной эксплуатации ЦД в критически важных системах.

Литература

1. Савченко О. Цифровые двойники // Научно-технический центр ФГУП «ГРЧЦ». 2023. URL: https://rdc.grfc.ru/2023/08/digitaltwins (дата обращения 12.09.2024)

2. Saaksvuori A., Immonen A. Product Lifecycle Management. Springer Science & Business Media, 2008. 272 p. DOI: 10.1007/978-3-540-78172-1

3. Grieves M. Digital Twin: Manufacturing Excellence Through Virtual Factory Replication // White Paper. 2014. URL: https://www.3ds.com/fileadmin/PRODUCTS-SERVICES/DELMIA/PDF/Whitepaper/DELMIA-APRISO-Digital-Twin-Whitepaper.pdf (дата обращения 10.11.2024)

4. Grieves M., Vickers J. Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems // In: Kahlen J., Flumerfelt S., Alves A. (eds.) Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches. Cham: Springer, 2017. PP. 85–113. DOI: 10.1007/978-3-319-38756-7_4

5. Semeraro C., Lezoche M., Panetto H., Dassisti M. Digital twin paradigm: A systematic literature review // Computers in Industry. 2021. Vol. 130. P. 103469. DOI: 10.1016/j.compind.2021.103469. EDN: MRYHKV

6. Greif T., Stein N., Flath C. M. Peeking into the void: Digital twins for construction site logistics // Computers in Industry. 2020. Vol. 121. P. 103264. DOI: 10.1016/j.compind.2020.103264. EDN: FPNJGR

7. Purcell W., Neubauer T. Digital Twins in Agriculture: A State-of-the-art review // Smart Agricultural Technology. 2022. Vol. 3. P. 100094. DOI: 10.1016/j.atech.2022.100094

8. Trauer J., Schweigert-Recksiek S., Onuma Okamoto L., Spreitzer K., Mörtl M., Zimmermann M. What is a Digital Twin? – Definitions and Insights from an Industrial Case Study in Technical Product Development // Proceedings of the Design Society: DESIGN Conference. Cambridge University Press, 2020. Vol. 1. PP. 757–766. DOI: 10.35199/NORDDESIGN2020.46

9. Melesse T. Y., Di Pasquale V., Riemma S. Digital Twin Models in Industrial Operations: A Systematic Literature Review // Procedia Manufacturing. 2020. Vol. 42. PP. 267–272. DOI: 10.1016/j.promfg.2020.02.084. EDN: AHEYJI

10. Alcaraz C., López J. Digital Twin: A Comprehensive Survey of Security Threats // IEEE Communications Surveys & Tutorials. 2022. Vol. 24. Iss. 3. PP. 1475–1503. DOI: 10.1109/COMST.2022.3171465. EDN: BJJFGD

11. Wang Y., Su Z., Guo S., Dai M., Luan T. H., Liu Y. A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects // IEEE Internet of Things Journal. 2023. Vol. 10. PP. 14965–14987. DOI: 10.1109/JIOT.2023.3263909. EDN: YLZJMQ

12. Николаев А. Цифровые двойники и обеспечение кибербезопасности предприятий Нефтегазовая отрасль // Лаборатория Касперского. 2022. URL: https://ics-cert.kaspersky.ru/publications/reports/2022/10/20/digital-twins-and-ensuring-the-cybersecurity-of-enterprises-oil-and-gas-industry (дата обращения 12.09.2024)

13. Masi M., Sellitto G. P., Aranha H., Pavleska T. Securing critical infrastructures with a cybersecurity digital twin // Software and Systems Modeling. 2023. Vol. 22. PP. 689–707. DOI: 10.1007/s10270-022-01075-0. EDN: JJVVRF

14. Homaei M. H., Mogollon-Gutierrez O., Núñez J. C. S., Vegas M. A., Caro A.L. A Review of Digital Twins and Their Application in Cybersecurity Based on Artificial Intelligence // ArXiv. 2023. DOI: 10.20944/preprints 202310.1127.v1

Статья поступила 18 ноября 2024 г.
Одобрена после рецензирования 11 декабря 2024 г.
Принята к публикации 25 декабря 2024 г.

Информация об авторах

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

https://doi.org/10.31854/2307-1303-2024-12-4-1-12
EDN: RQVZLW

Digital Twins as an Object and Tool of Information Security

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.*

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

Information about Authors

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