УДК: 004.056

О подходах к обеспечению информационной безопасности цифровых двойников

D.S. Lazorin, D.I. Pravikov, A.Yu. Shcherbakov

On Approaches to the Ensuring Information Security of Digital Twins

Abstract. *The article is devoted to the consideration of existing approaches to ensuring the information security of digital twins and the formulation of proposals for the choice of means to counter various threats, primarily the threat of distortion of the digital twin. It is shown that none of the existing approaches and methods provides the full security of digital twins. The implementation of an integrated approach to ensure the security of digital twins within the framework of specific threat and intruder models that are relevant to them is proposed.*

Keywords: *digital twin, digitalization, information security, threat and intruder model, computer model, multi-level system, digital certificate, data encryption, cryptographic algorithms, machine learning, tokenization.*

Д.С. Лазорин[1]
Д.И. Правиков[2]
А.Ю. Щербаков[3]
[1]Студент РГУ нефти и газа (НИУ) имени И.М. Губкина.
E-mail: lazorindanya@yandex.ru
[2]Кандидат технических наук, руководитель Научно-образовательного центра новых информационно-аналитических технологий, заведующий кафедрой комплексной безопасности критически важных объектов, РГУ нефти и газа (НИУ) имени И.М. Губкина.
E-mail: d_pravikov@mail.ru
[3]Доктор технических наук, профессор кафедры комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) имени И.М. Губкина, ведущий научный сотрудник Государственного университета управления.
E-mail: x509@ras.ru

Аннотация. *Статья посвящена рассмотрению существующих подходов к обеспечению информационной безопасности цифровых двойников и формулированию предложений по выбору средств противодействия различным угрозам, прежде всего угрозе искажения цифрового двойника. Показано, что ни один из существующих подходов и методов не обеспечивает полноценной безопасности цифровых двойников. Предложена реализация комплексного подхода для обеспечения безопасности цифровых двойников в рамках актуальных для них специфических моделей угроз и нарушителя.*

Ключевые слова: *цифровой двойник, цифровизация, информационная безопасность, модель угроз и нарушителя, компьютерная модель, многоуровневая система, цифровой сертификат, шифрование данных, криптографические алгоритмы, машинное обучение, токенизация.*

ВВЕДЕНИЕ

Понятие «цифровой двойник» в настоящее время прочно заняло позиции в современных цифровых технологиях. Данный термин достаточно широк и в первом приближении описывает математическую или компьютерную имитационную модель, связанную с физическим объектом потоками передачи информации, которая может быть отчуждена или отделена от исходного объекта в целях воспроизведения его функционирования или выполнения действий с указанным объектом.

Термин «цифровой» подразумевает под собой набор алгоритмов, которые описывают сам объект и протекающие в нём процессы. Цифровой двойник связан с процессами цифровизации - внедрения в определенные области деятельности и компетенции компаний современных информационных технологий, которые позволяют реформировать её деятельность. Цифровизация является основой современного подхода в том числе и к развитию промышленности, который позволил переосмыслить многие действующие бизнес-процессы корпораций [1].

Программные компоненты систем и физические процессы взаимосвязаны. Цифровой двойник выступает в роли объединяющей цепочки между «настоящим» миром и цифровой реальностью. Например, для того чтобы на предприятии эта цепочка находилось в рабочем состоянии, необходимо непрерывно получать информацию от технологического оборудования. Этим процессам помогают датчики

и сенсоры физического объекта, конструкции или технологической системы. Применение цифрового двойника необходимо для анализа и обновления в реальном времени большого количества данных, получаемых от физического объекта и требующих значительных вычислительных мощностей для их обработки, а также для моделирования и расчёта того, как будет вести себя та или иная конструкция или установка [2].

Актуальность цифровых двойников сегодня общепризнана. Об этом свидетельствуют, в частности, документы Министерства Энергетики [3].

Одной из наиболее острых является проблема информационной безопасности цифровых двойников. Вместе с имитацией процессов объектов физического мира при помощи данной технологии появляется возможность их контролировать, следовательно, не допускать наступления негативных событий. Приоритетной задачей становится обеспечение информационной безопасности организаций и технологических процессов, использующих технологию цифровых двойников.

Специфика обеспечения информационной безопасности в условиях применения технологий цифровых двойников связана с необходимостью применения имитационного моделирования, основанного на использовании характеристик каждого элемента системы и разработке логической цепочки процессов на базе реального объекта.

Также одной из актуальных проблем безопасности цифрового двойника является целенаправленное внесение искажений нарушителем таким образом, что управление объектом становится не оптимальным или невозможным.

ЭЛЕМЕНТЫ СИСТЕМЫ «ФИЗИЧЕСКИЙ ОБЪЕКТ – ЦИФРОВОЙ ДВОЙНИК» (ФОЦД)

Рассмотрим основные компоненты системной целостности, включающей физический объект и виртуальный объект.

1. Физический объект (ФО).
2. Виртуальный объект или специальная модель, соответствующая физическому объекту (цифровой двойник, ЦД).
3. Взаимосвязи в системе, включающей виртуальный объект и физический объект.

Собственно цифровым двойником в этой целостности является второй компонент, который может иметь связи с физическим объектом для его мониторинга и управления (третий компонент системной целостности).

Для объединения в ФОЦД вышеперечисленных частей используются различные, как принято говорить в современной информатике, интеграции, обеспечивающие получение реальных данных от модели ФО, которая может строиться на основе технологий «Интернет вещей» (Internet of Things, сокращённо IoT), а также различных математических моделях. К ним могут относиться, например, CAE-системы (Computer-aided engineering. автоматизированное проектирование), предназначенные для решения инженерных задач [4].

Стоит отметить, что вопрос обеспечения информационной безопасности ЦД конструктивно решается в том случае, если учитываются следующие априорные требования: контроль получаемых от ФО параметров, обеспечение целостности и конфиденциальности при обмене данными, обеспечение доступности и, самое главное, соответствие модели реальному объекту.

Кроме того, в одной из «проекций» цифровой двойник — это симбиоз технологий PLM (Product Lifecycle Management — управление жизненным циклом программных продуктов) и IIoT (Industrial Internet of Things, промышленный интернет вещей). Непосредственно на данный объект могут возникать несанкционированные воздействия, которые тем или иным способом могут повлиять на работу цифрового двойника и привести, как минимум, к неоптимальной его работе или же отказу всей системы, в которой он применяется.

СПЕЦИФИЧЕСКИЕ СВОЙСТВА ЦИФРОВЫХ ДВОЙНИКОВ

С точки зрения системного анализа необходимо выявить специфические свойства и об-

щие требования, которые можно предъявить к ФОЦД.

В первую очередь, это целостность, понимаемая как неразрывная взаимосвязь всех трех компонентов, их актуальность (в смысле соответствия текущему состоянию параметрам), наличие исчерпывающих связей между элементами системной целостности ФОЦД и их полнота.

В этом смысле весьма конструктивным представляется подход к описанию ФОЦД как некоторой платформы или ее части, данный подход будет проанализирован ниже.

С точки зрения реализации угроз ЦД может не соответствовать ФО, который управляется или мониторируется с его помощью.

Проверка соответствия ЦД ФО может проводиться через оценку качества управления. Цифровой двойник должен представлять собой адекватную модель существующего физического продукта или целостного процесса.

При необходимости можно зафиксировать и другие требования: актуальность цифрового двойника, защита канала связи двойника и объекта и т.д.

ОТЛИЧИЕ СТАНДАРТНОЙ МАТЕМАТИЧЕСКОЙ МОДЕЛИ И ЦИФРОВОГО ДВОЙНИКА

Попробуем прояснить весьма важный вопрос, касающийся различия общепринятой математической модели и ЦД.

Математическая модель — комплекс аналитических или вероятностных зависимостей параметров ФО, благодаря которым можно отразить характеристики рассматриваемого объекта или явления, построенных на основе физической модели и взаимодействиях её с окружающей средой. Она необходима для прогнозирования поведения реального объекта, однако всегда демонстрирует различную степень его идеализации.

Модель цифрового двойника — объект, который можно представить в виде физической и виртуальной системы, которая в свою очередь также включает стандартную математическую модель, так что виртуальная система отображает физическую, и наоборот.

Ключевое отличие от математической модели состоит в том, что модель цифрового двойника основывается не на идеализации, а на реальном поведении самого объекта.

ОПИСАНИЕ ОСНОВНЫХ ПОДХОДОВ К БЕЗОПАСНОСТИ ЦИФРОВЫХ ДВОЙНИКОВ

Ниже проанализированы актуальные источники и определены основные подходы и методы обеспечения информационной безопасности, которые могут быть применены к технологии цифровых двойников. Для каждого из них проведено краткое описание, изложена конструктивная критика данных подходов и методов.

Блокчейн-структура

В цифровом двойнике в процессе непрерывного обмена данными отражаются все стадии жизненного цикла физического объекта. Технологии распределенных реестров и, в частности, блокчейн позволяют фиксировать в режиме реального времени и в неизменяемом виде все состояния физического объекта и действия над ним, что является одним из основных условий обеспечения прозрачности, отслеживаемости, целостности и неизменности данных [5]. Блокчейн позволяет обмениваться событиями и уведомлениями, которые хранятся защищенном виде. В целом интеграция с технологией блокчейн обеспечивает безопасное, эффективное, децентрализованное и надежное хранение данных виртуальных моделей [6, 7, 8].

Использование данной технологии позволяет противодействовать угрозе изменения созданных записей, однако недостаточно для обеспечения комплексной безопасности цифровых двойников. В частности, блокчейн-структура не защищает от ложных команд управления и не обеспечивает защиту канала связи ФО и ЦД.

Подход к организации информационного взаимодействия в многоуровневой системе

Единицей межуровневого информационного обмена выступает программная структура особого типа — пакет, построенный по принципу организации сообщений в HTTP(s)-протоколах. Непосредственно метаданные (средства классификации, упорядочивания и характери-

стики данных) источника размещаются в заголовке пакета и позволяют выполнять распознавание соответствующих ресурсов по мере поступления данных. Данные цифрового двойника или его физического прототипа размещаются в теле пакета. Использование в заголовке пакета блока метаданных должно быть компактным и доступным для анализа программными средствами обработки данных.

Токен — специальный ключ, идентифицирующий поступающий запрос. Существует подход к кодированию заголовка с метаданными на основе комбинирования форматов DTDL (Digital Twins Definition Language — язык определения цифровых двойников), предназначенного для семантического описания промышленных цифровых двойников, и JWT (JSON Web Token), обеспечивающего процедуру поддержания сеанса связи между клиентом и сервером в веб-ориентированной архитектуре приложений. Непосредственно метаданные задаются в формате DTDL, а их размещение в заголовке пакета представляет собой программную «свертку» данных в формате токена JWT, заменяющего громоздкое JSON-описание источника данных легковесным текстовым кодом [9].

Согласно открытому стандарту RFC7519 (стандарт для создания токенов доступа, основанный на формате JSON), JWT представляет собой безопасный способ передачи данных между парой участников информационного взаимодействия [10-12].

Данный подход предпочтителен тем, что в его основе лежит обеспечение безопасности в системе взаимодействия между программным продуктом или приложением и сервером, но не затрагиваются другие внутрисистемные процессы цифровых двойников, на которые могут быть направлены потенциальные атаки и взломы.

Система иерархической токенизации элементов системы

Токенизация в одном из определений — процесс замены конфиденциальной информации на равнозначные не конфиденциальные данные с использованием специальных значений (токенов). Для повышения эффективности процессов обмена, обработки данных и безопасности между уровнями системы цифровых двойников предлагается подход, основанный на принципе токенизации информационных ресурсов. Данная технология активно используется для защиты и шифрования в современных системах информационной безопасности, а также для реализации систем блокчейн.

Использование токенизации для разметки источников данных и их физических прототипов, а также результатов их агрегирования на основании пространственной кластеризации (процедуре сбора данных) по заданным признакам обеспечивает безопасность использования цифровых двойников. В соответствии с предлагаемой концепцией информационного взаимодействия элементов системы предполагается маркировка соответствующих наборов данных для идентификации их источника в процессе обработки и анализа данных в составе единого информационного пространства. Так как идентификация является одним из основополагающих факторов обеспечения информационной безопасности, это позволит избежать изменения данных, исходящих от внесистемных источников [13, 14].

Данный метод обеспечивает неизменность данных и идентификацию поступающих к цифровому двойнику запросов, однако не позволяет осуществлять комплексную защиту от угроз, направленных на цифровой двойник, как и технология блокчейн (см.выше).

Digital ID или цифровой сертификат

Эта технология представляет собой относительно новый подход к безопасности и доверию, в рамках которого идентифицируются запросы от верифицированных источников, например, внутрисистемные запросы для управления продуктом, в которых используется цифровой двойник. Благодаря цифровому сертификату можно защититься от более широкого круга действий нарушителя.

Программные приложения, сети и компьютеры могут использовать Digital ID в шифровании, как путь защиты информации перед отправкой его с одной компьютерной системы на другую [15].

Этот метод обеспечивает проверку поступающих запросов, но не рассматривает другие возможные способы нарушения работы цифровых двойников, например, замену посторон-

него ID на истинный.

Методика многоуровневого шифрования команд для управления удалёнными компьютерными системами

Процесс криптографических преобразований сообщений на конечных клиентских устройствах и их передача через сервер в зашифрованном виде называется сквозным шифрованием [16]. На сегодняшний день такой подход к защите данных является одним из наиболее эффективных и приобретает всё большее распространение. Однако применение сквозного шифрования не исключает необходимости защиты данных, которыми обмениваются компоненты информационной системы с сервером, так как часть из них, предназначены непосредственно самому серверу, а значит, не могут быть подвергнуты сквозному шифрованию [17]. Это касается команд для администрирования сервера и страниц с информацией о текущем состоянии процесса мониторинга.

Для всех перечисленных данных необходимо применять транспортное шифрование, то есть шифрование, выполняемое только при передаче через интернет, при котором данные расшифровываются каждым компонентом информационной системы, а при необходимости дальнейшей передачи зашифровываются заново. Таким образом, для обеспечения безопасной передачи данных в системе удалённого мониторинга и управления компьютерами должно быть реализовано многоуровневое шифрование, объединяющее в себе сквозное симметричное шифрование команд между управляющим компьютером и компьютерами пользователей и транспортное шифрование между сервером и управляющим компьютером, а также сервером и компьютерами пользователей.

Безопасность сквозного шифрования основана на том, что ключи для шифрования и расшифрования сообщений доступны только непосредственным участникам взаимодействия. При этом главная проблема реализации сквозного шифрования заключается в безопасной передаче ключей от отправителя к получателю. Для обмена ключами используется один из распространённых видов алгоритмов: симметричный или асимметричный, а также, в некоторых случаях, дополнительно используется разделение секрета или иные протоколы, позволяющие разделить ключи.

Использование асимметричных криптографических алгоритмов в сквозном шифровании порождает несколько дополнительных проблем, таких как аутентификация ключей, проверка личности отправителя, управление цифровыми сертификатами и их подтверждением. Асимметричное шифрование в первую очередь направлено на использование участниками взаимодействия через Интернет, когда нет никаких возможностей отдельной передачи симметричных ключей.

Преимуществом такого метода является следующее: если в системе таких ограничений нет, то все её компоненты находятся под единым административным управлением, разрабатываются и конфигурируются централизованно, к тому же администратор в любой момент имеет доступ к каждому компьютеру, на котором установлено клиентское программное обеспечение. В связи с этим при разработке системы удалённого управления компьютерами целесообразно применение симметричных алгоритмов с использованием предварительного общего ключа PSK (Pre-Shared Key — предварительно опубликованный ключ для шифрования данных перед отправкой, который разделён между двумя сторонами системы взаимодействия).

Использование удалённого управления и мониторинга оборудования в этом случае значительно упростит работу администратора и снизит расходы на поддержание работы информационной системы, а описанные методы защиты не приведут к появлению дополнительных уязвимостей и позволят избежать снижения уровня информационной безопасности цифровых двойников.

В данной методике рассматривается взаимодействие через сеть Интернет, но не предоставляются различные варианты безопасной работы систем при ситуациях, когда доступ к сети может быть нарушен, либо же специально ограничен.

Комплексный подход с использованием машинного обучения и искусственного интеллекта

Существуют решения на основе искусственного интеллекта, способные обнаружить отклонения в технологическом процессе на ранней стадии. Принцип защиты системы основан на выстраивании модели таким образом, чтобы она была готова к попытке «скормить» ей искаженную информацию и могла справиться с атакой. Использование машинного обучения позволит исправлять возникающие искажения, которые обнаруживает искусственный интеллект.

Стоит отметить, что для цифровых двойников, базирующихся на машинном обучении (Machine Learning), основную опасность несут враждебные атаки (Adversarial attacks), основанные на внесении минимальных изменений в данные, которые поступают в цифровую модель. Применительно к заводам и фабрикам это могут быть показания датчиков, интегрированных в производственное оборудование. Изменения, как правило, заключаются в добавлении данных, которые подбираются таким образом, чтобы максимально исказить предсказания, которые формирует модель.

Подобная атака может привести к простоям оборудования, лишним расходам на сырье и другим незапланированным издержкам, которые плохо сказываются на экономической политике предприятия. Следовательно, данный метод привлекает нарушителя возможностью «скармливания искажённой информации».

Использование таких решений на сегодняшний день возможно в качестве дополнительных, потому что они требуют определенного количества времени для обучения работе в самой системе.

Обеспечение безопасности ЦД в рамках концепции многоуровневой платформы

Многоуровневая система (платформа) имеет различные уровни организации, в которых происходят определенные процессы. Верхние уровни обеспечивают бизнес-взаимодействия, а нижние уровни поддерживают информационную безопасность самой платформы. Авторами данного подхода вводится понятие «стек технологий», в котором работа верхних уровней поддерживается нижними уровнями, и предлагается использование интеграционной модели защищенной цифровой платформы, включающей вертикальное разделение по уровням абстракций представления данных и уровням обеспечения информационной безопасности [18].

На основе проанализированных подходов к безопасности цифровых двойников построена таблица 1 **«Некоторые способы обеспечения комплексной безопасности ЦД»**.

Таблица 1

Некоторые способы обеспечения комплексной безопасности ЦД

Информационное взаимодействие в многоуровневой системе	✓
Проверка подлинности поступаемых запросов к модели.	✓
Шифрование данных при передаче по каналам связи.	✓
Решения на основе машинного обучения и искусственного интеллекта.	✓
Соответствие модели реальному объекту.	X

ЗАКЛЮЧЕНИЕ

Проведенный анализ существующих подходов к обеспечению информационной безопасности цифровых двойников позволяет сделать вывод, что практически ни один из предложенных способов в отдельности не обеспечивает комплексной безопасности в рамках актуальных для цифровых двойников моделей угроз и нарушителя. Использование технологий распределенных реестров, метода иерархической токенизации, цифровых сертификатов, многоуровневого шифрования, машинного обучения и искусственного интеллекта на современном уровне весьма оправдано, но направлено на решение частных задач.

В связи с этим целесообразно развивать методологию обеспечения информационной безопасности цифровых двойников в соответствии с концепцией многоуровневой платформы, поскольку в понятие платформы уже включен комплексный подход и иерархия решений от низкоуровневых способов защиты канала связи ФОЦД при помощи криптографических алгоритмов до высокуровневых задач, связанных с проверкой соответствия моделей функционирования ЦД и обеспечения корректности бизнес-процессов, отражаемых цифровым двойником.

При этом отдельные способы обеспечения информационной безопасности могут включать уже готовые решения (например, средства шифрования данных при передаче по каналам связи), а для части методов (направленных, например, на обеспечение соответствия виртуальной модели реальному объекту) необходимо использовать другие средства и подходы, которые будут сформулированы в следующих работах.

СПИСОК ЛИТЕРАТУРЫ

1. Намиот Д. Е., Покусаев О. Н., Куприяновский В. П., Жабицкий М. Г. Цифровые двойники и системы дискретно-событийного моделирования // International Journal of Open Information Technologies. 2021. №9. С. 70-75.

2. Цифровое зеркало. URL: https://www.gazprom-neft.ru/press-center/sibneft-online/archive/2018-september-projects/1863687/ (Дата обращения: 12.01.2022)

3. Паспорт: «Программы инновационного развития» ПАО «Газпром» до 2025 года. URL: https://minenergo.gov.ru/node/4844 (Дата обращения: 13.01.2022)

4. Перспективы использования цифровых двойников на производстве и технологии для их создания. URL: https://controleng.ru/innovatsii/cifrovye-dvojniki/chto/ (Дата обращения: 27.02.2022)

5. Дроговоз П.А., Кошкин М.В. Проекты внедрения технологий блокчейн и интернета вещей в трансграничных цепочках поставок // Управление научно-техническими проектами: сб. материалов III междунар. науч.-техн. конференции. М.: Изд-во МГТУ им. Н.Э. Баумана, 2019. С. 153–156.

6. Гарина И. О. Методический подход к разработке блокчейн-структуры цифрового двойника изделия в машиностроении // Современные наукоемкие технологии. 2020. № 11-1. – С. 15-20. – DOI 10.17513/snt.38331.

7. Mandolla C., Petruzzelli A.M., Percoco G., Urbinati A. Building a digital twin for additive manufacturing through the exploitation of blockchain. Comput. Ind. 2019. Vol. 109. P. 134–152.

8. Freni P., Ferro E., Moncada R. Tokenization and Blockchain Tokens Classification: a morphological framework // IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 2020. P. 1-6, DOI: 10.1109/ISCC50000.2020.9219709.

9. Воробьев А. В. Концепция информационного пакетного взаимодействия в многоуровневой системе цифровых двойников // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2021. Т. 21, вып. 4. С. 532-543. DOI: 10.18500/1816-9791-2021-21-4-532-543.

10. Janoky L., Levendovszky J., Ekler P. An analysis on the revoking mechanisms for JSON Web Tokens

// International Journal of Distributed Sensor Networks. 2018. Vol. 14, iss. 9. P. 1–10. https://doi.org/10.1177/2F1550147718801535

11. Aldya A. P., Rahmatullo A., Arifin M. N. Stateless Authentication with JSON Web Tokens using RSA-512 Algorithm // Journal INFOTEL. 2019. Vol. 11, № 2. P. 36–42. https://doi.org/10.20895/infotel.v11i2.427

12. Rahmatulloh A., Gunawan R., Nursuwars F. Performance comparison of signed algorithms on JSON Web Token // IOP Conference Series: Materials Science and Engineering. 2019. Vol. 550. P. 012023. https://doi.org/10.1088/1757-899X/550/1/012023

13. Marchewka-Bartkowiak K., Nowak K. Get Tokenized... The Specificity of Personal Tokens in the Context of Tokenization and Axiological Categorization // Proceedings of the 3rd International Conference on Economics and Social Sciences. 2020. P. 823-831. DOI:10.2478/9788395815072-081.

14. Cassimon T., de Hoog J., Anwar A., Mercelis S., Hellinckx P. Intelligent data sharing in digital twins: Positioning paper. In: L. Barolli, M. Takizawa, T. Yoshihisa, F. Amato, M. Ikeda, eds. Advances on P2P, Parallel, Grid, Cloud and Internet Computing. 3PGCIC 2020 (Lecture Notes in Networks and Systems, vol. 158). Springer, Cham, 2021, P. 282– 290. https://doi.org/10.1007/978-3-030-61105-7_28

15. Tang S., Wei G. ID-based digital Multisignature scheme // Journal of Circuits, Systems, and Computers. 1999. Vol. 9. No 3-4. P. 223-227. – DOI 10.1142/S0218126699000189.

16. Бытый Д.Э. Методика многоуровневого шифрования команд для системы управления удалёнными компьютерами // Наукосфера. 2021. № 10-1. С. 92-95.

17. Лапонина О.Р. Основы сетевой безопасности : учеб. Пособие / Национальный Открытый Университет «ИНТУИТ». Москва, 2014, 374 с.

18. Правиков Д.И., Глейм А.В., Егоров В.И., Рязанова А.А., Щербаков А.Ю. К вопросу о формулировании системного подхода к исследованиям в области цифровых платформ, распределенных реестров и цифровых активов // Вестник современных цифровых технологий. 2021. № 9. С. 5-14.