

КОНЦЕПЦИЯ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ЦИФРОВЫХ ДВОЙНИКОВ ДЛЯ ОБЪЕДИНЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ НЕСКОЛЬКИХ ПРЕДПРИЯТИЙ В УСЛОВИЯХ ИХ СЛИЯНИЯ

Федорова А.В., аспирантка ФГБУН ВИНИТИ РАН

Шведенко В.Н., д-р тех. наук, профессор ФГБУН ВИНИТИ РАН, гл. специалист ФГБУ «Институт стандартизации»

В статье даны определения технологии цифровых двойников, представлены их классификация и структура. Авторы рассматривают информационные системы, наиболее подверженные угрозам безопасности согласно исследованиям компании InfoWatch. Показано, что при миграции данных надежной защиты требуют прежде всего информационные системы, в которых хранятся и обрабатываются персональные данные. Сформулирована актуальная идея применения технологии цифровых двойников для обеспечения безопасности бизнес-процессов предприятий в условиях объединения их информационных систем. Представлен возможный алгоритм ее реализации. Статья будет полезна ИТ-специалистам, менеджерам, заинтересованным в повышении эффективности компаний за счет объединения информационных систем.

Ключевые слова: цифровой двойник, цифровая модель, цифровая тень, моделирование, Industry 4.0, информационная безопасность.

ВВЕДЕНИЕ

В современных условиях нередки случаи объединения нескольких предприятий в концерн или поглощение маленьких компаний более крупными и влиятельными. Особое внимание в исследовании удалено технической, а не правовой стороне рассматриваемого вопроса.

Для успешного объединения нескольких информационных систем организации открывают проекты и выделяют значительные ресурсы (финансовые и человеческие). Обеспечение безопасности данных при переносе из одной системы в другую – важная задача в рамках проекта.

Основная цель данной работы – описание концепции применения технологии цифровых двойников для обеспечения безопасности информации в условиях объединения двух информационных систем. Подразумевается, что цифровой двойник создается с целью выявления основных угроз, которые могут возникнуть в этом процессе. Такой малоизученный вариант применения цифровых двойников имеет перспективы развития, особенно в условиях импортозамещения. Перенос данных из одной информационной системы в другую происходит намного чаще, чем это было раньше.

ОСНОВНАЯ ПРОБЛЕМАТИКА СТАТЬИ

В каждой компании существует одна или несколько информационных систем (ИС) для управления:

1. Человеческими ресурсами и расчета заработной платы.
2. Производством.
3. Товарно-материальными ценностями и т. д.

Набор ИС зависит от масштаба компании и уровня автоматизации бизнес-процессов.

При слиянии компаний потребуется перенести данные из информационных ресурсов каждого участника объединения в новую систему либо внести данные в одну из существующих ИС. На данном этапе могут возникнуть первые трудности организационного и технического характера:

1. Наиболее актуальная проблема – нарушение производственного цикла предприятия.
2. Нарушение связи между подразделениями организации, а также приостановка их деятельности, если работа основана на автоматизированных процессах.

3. Соблюдение требований безопасности при миграции данных¹.

Кроме того, необходимо обеспечить безопасность процесса слияния. Об объединении крупных компаний, как правило, становится известно не из официальных источников, а от работников, обеспокоенных своим будущим. С человеческим фактором всегда связаны значительные риски, которые трудно контролировать. Внутренний или внешний нарушитель безопасности может вторгнуться в процесс миграции данных, скомпрометировать их, использовать либо использовать их для перепродажи и личной выгоды. Причины могут быть разными, но задача предприятий – обеспечить безопасность данных при их миграции из одной информационной системы в другую.

Независимо от специфики компании, объема обрабатываемой информации, количества пользователей проблемы при переносе данных из одной информационной системы в другую возникают часто. Например, в 2010-х гг. крупный банк присоединял к своей структуре небольшую банковскую организацию. Соответственно, в его базы данных мигрировали данные клиентов самостоятельной прежде компании. Но не учли тот факт, что у прежнего банка были не только вкладчики, зарплатные клиенты и т.д., но и владельцы счетов с задолженностями. При миграции данных были потеряны знаки «-» у большого количества записей с отрицательными значениями. Получилось, что у должников появились «вклады» на общую сумму примерно 15 млн рублей. Ошибка была обнаружена, данные исправлены. Но ущерб в данном примере можно оценивать в контексте денег и репутации банка.

В других отраслях последствия могут быть плачевнее. Данный пример показывает, что при переносе данных могут возникнуть самые неожиданные ошибки, представляющие угрозу безопасности информации.

Безопасность информации (данных) – это состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность².

Таким образом, для защиты данных двух и более объединяемых информационных систем необходимо уделять должное внимание не только процессу переноса информации, но и тестированию новой объединенной системы. Каким пользователям стоит дать доступ к системе на этом этапе? Какие угрозы безопасности стоит учитывать?

Основное направление исследования в данной работе – концепция применения технологии цифровых двойников для моделирования процесса объединения информационных систем и выявления угроз безопасности в рамках этой процедуры. Такой вариант применение технологии цифровых двойников малоизучен.

У цифрового двойника множество определений. Самые близкие к тематике исследования и их авторы представлены ниже.

Söderberg R., Wärmefjord K. И др.: «Использование цифровой копии физической системы для оптимизации в реальном времени» [1].

Bolton R.N. и др.: «Динамическое виртуальное представление физического объекта или системы в течение всего жизненного цикла с использованием данных в режиме реального времени для понимания, изучения и рассуждения» [2].

Tao F. и др.: «Цифровой двойник – это реальное отображение всех компонентов в жизненном цикле продукта с использованием физических данных, виртуальных данных и данных взаимодействия между ними» [3].

Следует отметить, что в промышленности и научной сфере понятие «цифровые двойники» трактуется по-разному. Так, цифровой двойник – это:

1. Модель готового продукта, способная отражать его основные характеристики, в том числе дефекты, для своевременного их устранения и создания наиболее эффективного и безопасного производства, с непрерывным обновлением, чтобы при расчетах учитывать износ материалов и конструкций для более большой точности оценки вероятностей наступления тех или иных событий.
2. Цифровая модель физического объекта с интегрированными датчиками, которые позволяют имитировать работу объекта в реальном времени, в том числе в составе киберфизических систем [4].

Обобщая эти суждения, можно сказать, что цифровой двойник предоставляет возможность смоделировать поведение объекта в прошлом, на основе чего можно смоделировать его поведение в будущем при различных параметрах воздействующих на него факторов.

На рис. 1 представлена иерархическая зависимость предшествующих созданию цифрового двойника (ЦД) элементов – цифровой модели и цифровой тени. Данные понятия не являются синонимами, они были введены для отображения разной степени связи с реальным объектом.

¹ Миграция данных (migration of data) – передача (перенос) электронных документов из одного формата, носителя или компьютеризированной системы в другую (см. ГОСТ 33647–2015, п. 3.6.7).

² ГОСТ Р 50922–2006. Защита информации. Основные термины и определения (Введ. с 2008–02–01). М.: Стандартинформ, 2008. (п. 2.4.5).



Рис. 1. Этапы создания цифрового двойника

Цифровая модель (Digital Model) – это объект цифрового мира, отображающий существующий или планируемый физический объект. Отличие цифровой модели (далее – ЦМ) заключается в отсутствии автоматического обмена данными. ЦМ работает автономно, без связи с ее физическим аналогом, изменения которого не влияют на ее состояние [3, 5].

Цифровая тень (Digital Shadow) – это отражение реального мира в цифровом, связанного входящими потоками данных от физического и цифровому. Под воздействием изменения состояния физического объекта цифровая тень (далее – ЦТ) также меняет свое состояние.

Цифровой двойник (Digital Twins) – это отражение реального мира в цифровом. Между физическим объектом и ЦД существует двухсторонняя связь, следовательно, при изменении состояния одного меняется состояние другого [6].

Таким образом, в цифровую тень передаются данные реальных состояний, что не позволяет предсказать поведение физического объекта в условиях, в которых он еще не находился. Цифровой двойник, благодаря своим характеристикам, дает возможность прогнозировать поведение реального объекта.

Идея базовой концепции цифрового двойника заключается в том, что в физический объект встроены датчики, получающие и обрабатывающие информацию о его состоянии в определенный период времени. Эта информация передается виртуальному цифровому двойнику, тем самым цифровая модель уточняется. Цифровая модель учитывает все изменения физического объекта, накапливает информацию о его изменениях. Таким образом, по мере уточнения виртуальная модель становится копией физического объекта и может адекватно описывать, прогнозировать его поведение [7].

В таблице представлена краткая классификация цифровых двойников.

ЦИФРОВОЙ ДВОЙНИК		
1. КЛАССИФИКАЦИЯ МАЙКЛА ГРИВЗА		
ПРОТОТИП	ЭКЗЕМПЛЯР	АГРЕГАТОР
Прототип физического объекта, который содержит данные для описания и создания физической версии	Описывает конкретный физический объект, с которым ЦД связан на протяжении его жизненного цикла, содержит различные модели, операции и результат их выполнения, данные датчиков	Объединение других типов ЦД позволяет анализировать состояние физического объекта, сравнивать текущие показатели с показателями, зафиксированными в нежелательных ситуациях
2. КЛАССИФИКАЦИЯ ПО ОБЛАСТИ ПОСТРОЕНИЯ		
ЦД ПРОДУКТА	ЦД ПРОЦЕССА	ЦД СИСТЕМЫ
Виртуальная модель продукта, позволяет проанализировать поведение продукта в различных условиях, выявить возможные проблемы, снизить издержки при выходе продукта	Имитация производственного процесса, позволяет повысить безопасность и эффективность производства посредством разработки на основе ЦД оптимальной методики	Виртуальная модель целого предприятия, используется для оптимизации и внедрения новых бизнес-процессов

Таким образом, цифровой двойник – это прототип информационной системы (продукта), который дает возможность воспроизвести миграцию данных из одной системы в другую, определить угрозы безопасности и протестировать защищенность информации на этапе переноса.

Организации, как уже отмечалось, могут использовать несколько информационных ресурсов. В данной работе рассматриваются информационные системы персональных данных (далее – ИСПДн), имеющие большое значение для защиты информации этого типа. Такое заключение сделано на основе исследования компании InfoWatch. Специалисты отмечают, что в первой половине 2022 г. в мире было похищено на 27,8% меньше единиц информации, чем за тот же период 2021 г. Но при анализе данных выяснилось, что у злоумышленников была определенная цель – похищать только действительно ликвидные на черном рынке данные. Распределение утечек по типам данных отражено на рис. 2 [8].

Как видно на графиках, число утечек растет. Персональные данные представляют наибольший интерес для злоумышленников, которые становятся избирательнее, следовательно, необходимо повышать уровень защиты таких данных.



Рис. 2. Распределение утечек по типам данных, мир – Россия, соответственно: первая половина 2021 г. и 2022 г.

Цель исследовательской работы – создание такого цифрового двойника, который позволит моделировать защиту персональных данных при объединении групп компаний.

Первый этап: создание цифровой модели.

Отметим, что для сужения границ исследования выбраны ИСПДн, но подразумевается, что результат настоящей научной работы можно будет применять в разных областях.

На первом этапе важно определить структуру информационных процессов в организациях. Работа предприятия состоит из взаимодействия всех подразделений, в каждой организации есть установленные бизнес-процессы. Именно это нужно отразить в виде информационных потоков каждой организации, участвующей в слиянии. На основе сведений о функционирующих информационных процессах и потоках можно будет построить структуру информационной системы.

При создании модели данных на выходе можно формализовать представление данных, содержащихся в информационной системе. Процедура основана на методах описания типов и логических структур данных в базах данных (далее – БД), методах манипулирования данными, методах описания и поддержки БД. Выделяют четыре типа модели данных:

1. Иерархическая.
2. Сетевая.
3. Реляционная.
4. Объектная [9].

Таким образом, одна из проблем при миграции данных может быть обусловлена тем, что данные в ИС разных предприятий хранятся в БД, построенных по различным моделям.

Также предстоит определить используемые инструментальные средства, архитектуру и ответить на следующие вопросы:

1. Какая система управления БД используется в организациях, участвующих в объединении?
2. Какова модель физической реализации?

Организации могут использовать ERP-систему для управления данными. У каждой системы свои особенности, по-разному описанные процессы, что также может представлять трудность при переносе данных в новую информационную систему.

Результат первого этапа: цифровая модель информационной системы каждого участвующего в объединении предприятия.

Второй этап: создание цифровой тени.

На этом этапе предстоит наполнить цифровую модель каждой системы данными и настроить односторонний поток, который будет имитировать миграцию данных из одной информационной системы предприятия в другую.

Третий этап: создание цифрового двойника.

На этом этапе необходимо построить модель взаимодействия пользователя с системой: ввод данных, запросы в БД с определенной периодичностью, удаление данных. Также можно имитировать процесс работы пользователей, чтобы понять, как выполнение ими функциональных обязанностей повлияет на новую расширенную систему, как это отразится на загрузке серверов и т. д.

Кроме того, необходимо разработать модель угроз при миграции данных и смоделировать действия злоумышленника. Для этого, согласно идеи научной работы, и нужен цифровой двойник, который не только позволит смоделировать работу системы и пользователей, но и поможет определить, как потенциальный злоумышленник способен повлиять на систему, через какие каналы, какие его действия поставят под угрозу безопасность информации. Использование цифрового двойника даст возможность не проводить тесты безопасности на действующем объекте и не подвергать работоспособность системы реальным угрозам. На этом шаге выяснится потенциальный нару-

шитель (сотрудник организации, внешний злоумышленник и т. д.), какие каналы он использует и какова его цель. В конце предстоит определить меры защиты.

Цифровой двойник, создаваемый только на период объединения информационных систем, не повлияет на текущую работу этих ресурсов. Он создается с целью обеспечения безопасности процесса миграции данных и на определенный промежуток времени. После завершения процесса объединения предприятий необходимость использовании такого цифрового двойника отпадет.

ЗАКЛЮЧЕНИЕ

В работе описана идея применения цифровых двойников в сфере информационной безопасности. Создание цифрового двойника информационной системы позво-

лит проводить аудит безопасности системы с минимальными рисками (в том числе тестирование на проникновение), рассчитывать необходимые мощности серверного оборудования, исходя из объемов информации, настраивать разграничение доступа и т. д. В условиях цифровизации информационная безопасность и цифровые двойники связаны напрямую, их совместное развитие – перспективное направление для науки.

Список использованных источников и литературы

1. Söderberg R. et al. Toward a Digital Twin for real-time geometry assurance in individualized production // CIRP Annals. 2017. T. 66. №. 1. С. 137–140.
2. Bolton R.N. et al. Customer experience challenges: bringing together digital, physical and social realms // Journal of Service Management. 2018. V. 29. No. 5. Pp. 776–808.
3. Tao F. et al. Digital twin-driven product design framework // International Journal of Production Research. 2019. V. 57. No. 12. Pp. 3935–3953.
4. Щекочихин О.В. Современные тенденции управления киберфизическими системами на основе цифровых двойников // Информационно-экономические аспекты стандартизации и технического регулирования. 2021. № 5 (63). С. 33–37.
5. Бурый А.С. Цифровые двойники как основа парадигмы развития прикладных информационных систем // Информационно-экономические аспекты стандартизации и технического регулирования. 2022. № 6 (70). С. 24–32.
6. Шведенко В.Н., Соболев Д.А. Концепция цифровых двойников объектов материальных систем // Информационно-экономические аспекты стандартизации и технического регулирования. 2018. № 5 (45). С. 10.
7. Прохоров А.Н., Лысачев М.Н. Цифровой двойник. Анализ, тренды, мировой опыт. – М.: ООО «АльянсПринт», 2020. – 401 с.
8. Экспертно-аналитический центр InfoWatch. Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года // Электронный журнал. 2022. [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-danniyh-za-1-polugodie-2022-goda_1.pdf. (Дата обращения 17.01.2023).
9. Щекочихин 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.

CONCEPT OF APPLICATION OF THE DIGITAL TWIN TECHNOLOGY FOR THE MERGING OF INFORMATION SYSTEMS OF MULTIPLE ENTERPRISES IN CONDITIONS OF THEIR MERGING

Fedorova A.V., graduate student, VINITI RAN

Shvedenko V.N., Dr. Sc. (Technology), Professor VINITI RAN, Chief Specialist at the FSBI «RSI»

This article describes the idea of using digital twin technology to combine information systems of several enterprises in the conditions of their merging. The relevance of data security under the described conditions is indicated. An algorithm for applying this technology is also presented.

The article describes the digital twins technology, definitions, classification, their structure. An analysis was also made of information systems that are most susceptible to security threats according to research by InfoWatch. Based on the data obtained, it was determined that when migrating data between information systems, the systems in which personal data are stored and processed should be provided with the greatest protection. Based on this, the idea of using digital twin technology to ensure the security of business processes of enterprises in the context of combining their information systems is formulated. The relevance of ensuring this issue is indicated. A possible implementation algorithm under the described conditions is also presented. The article will be useful for information technology professionals, as well as for managers who want to increase the efficiency of their company by combining information systems.

Keywords: digital double, digital model, digital shadow, modeling, Industry 4.0, information security.

References

1. Söderberg R., et al. Toward a Digital Twin for real-time geometry assurance in individualized production. *CIRP Annals*. 2017, vol. 66, no. 1, pp. 137–140.
2. Bolton R.N., et al. Customer experience challenges: bringing together digital, physical and social realms. *Journal of Service Management*. 2018, vol. 29, no. 5, pp. 776–808.
3. Tao F. et al. Digital twin-driven product design framework. *International Journal of Production Research*. 2019, vol. 57, no. 12, pp. 3935–3953.
4. Shchekochihin O.V. Sovremennye tendencii upravleniya kiberfizicheskimi sistemami na osnove cifrovyyh dvojnikov. *Informacionno-ekonomicheskie aspekty standartizacii i tekhnicheskogo regulirovaniya*. 2021, no. 5(63), pp. 33–37.
5. Buryi A.S. Cifrovye dvojники kak osnova paradigmy razvitiya prikladnyh informacionnyh sistem. *Informacionno-ekonomicheskie aspekty standartizacii i tekhnicheskogo regulirovaniya*. 2022, no. 6 (70), pp. 24–32.
6. Shvedenko V.N., Sobolev D.A. Koncepciya cifrovyyh dvojnikov ob'ektov material'nyh system [Concept of digital twins of objects of material systems]. *Informacionno-ekonomicheskie aspekty standartizacii i tekhnicheskogo regulirovaniya* [Information and economic aspects of standardization and technical regulation]. 2018, no. 5(45). P. 10.
7. Prohorov A.N., Lysachev M.N. Cifrovoj dvojnik. Analiz, trendy, mirovoj opyt [Digital twin. Analysis, trends, world experience]. Moscow. OOO «Al'yansPrint». 2020, 401 p.
8. Ekspertno-analiticheskij centr InfoWatch [Expert-analytical center InfoWatch]. Otchyot ob issledovanii utechek informacii ogranicennogo dostupa v I polovine 2022 goda [Report on the study of leaks of restricted information in the first half of 2022].: URL: <https://www.infowatch.ru/sites/default/files/analytics/files/otchyt-ob-utechkakh-dannykh-za-1-polugodie-2022-goda.1.pdf> (Available at 05-01-2023).
9. Shchekochihin O.V. Ob'ektno-processnaya model' dannyh v upravlyayushchih informacionnyh sistemah [Object-process data model in information systems management]. *Nauchno-tehnicheskij vestnik informacionnyh tekhnologij, mekhaniki i optiki* [Scientific and technical bulletin of information technologies, mechanics and optics]. 2017, vol. 17, no. 2, pp. 318–323.