ЦИФРОВЫЕ ДВОЙНИКИ В СИСТЕМАХ УПРАВЛЕНИЯ

Минзов А. С.[1], Невский А. Ю.[2], Баронов О. Р.[3], Немчанинова С.В.[4]

DOI: 10.21681/2311-3456-2024-2-29-35

Цель исследования – *анализ области применения цифровых двойников в системах управления критическими информационными инфраструктурами (КИИ), их классификаций и разработка концептуальной модели взаимодействия цифровых двойников с их физическими сущностями.*

Методология проведения работы. *При проведении исследований использовался системный анализ для анализа области применения цифровых двойников, их классификаций и моделей взаимодействия. При разработке прототипа цифрового двойника использовались математические модели управления рисками информационной безопасности и оценки эффективности систем защиты информации.*

Область применения результатов. *Полученные результаты не противоречат существующим нормативным документам по защите КИИ и могут быть использованы для повышения эффективности систем защиты информации в КИИ на этапах их проектирования и мониторинга работы.*

Научная новизна. *Предложена концетуальная модель цифровых двойников и классификация решаемых ими задач. Разработана модель цифрового двойника для проектирования систем управления информационной безопасностью.*

Ключевые слова: *цифровой двойник, концептуальная модель, информационная безопасность, кибербезопасность, критическая информационная инфраструктура, модель управления рисками.*

DIGITAL TWINS IN CONTROL SYSTEMS

Minzov A. S.[5], Nevsky A. Yu.[6], Baronov O. R.[7], Nemchaninova S. V.[8]

The concept of digital twins is part of the fourth industrial revolution (Industry 4.0). It is based on the mass introduction of information technology and artificial intelligence into industry. This direction is being developed for information and cyber security management systems.

The purpose of the article: *analysis of the scope of application of digital twins in critical information infrastructure management systems, their classifications and development of a conceptual model of the interaction of digital twins with their physical entities.*

Main research methods: *system analysis of existing normative and other documents, set theory and algebra of logic.*

Scientific novelty. *A conceptual model of digital twins and a classification of the problems they solve are proposed. A digital twin model has been developed for the design of information security management systems.*

Keywords: *digital twin, conceptual model, information security, cybersecurity, critical information infrastructure, risk management model.*

1 Минзов Анатолий Степанович, доктор технических наук, профессор, профессор кафедры безопасности и информационных технологий национального исследовательского университета МЭИ, Москва, Россия. E-mail: MinzovAS@mpei.ru

2 Невский Александр Юрьевич, кандидат технических наук, заведующий кафедрой безопасности и информационных технологий национального исследовательского университета МЭИ, Москва, Россия. E-mail: NevskiyAU@mpei.ru

3 Баронов Олег Рюрикович, кандидат технических наук, доцент кафедры безопасности и информационных технологий национального исследовательского университета МЭИ, Москва, Россия. E-mail: BaronovOR@mpei.ru

4 Немчанинова София Вадимовна, старший преподаватель кафдры информационных технологий университета «Дувна», Дубна, Россия. E-mail: sbobylova94@gmail.com

5 Anatoly S. Minzov, Dr.Sc., Professor of the Department of Security and Information Technologies, National Research University MPEI, Moscow, Russia. E-mail: MinzovAS@mpei.ru

6 Alexander Yu. Nevsky, Ph.D., Head of the Department of Security and Information Technologies, National Research University MPEI, Moscow, Russia. E-mail: NevskiyAU@mpei.ru

7 Oleg R. Baronov, Ph.D., Associate Professor of the Department of Security and Information Technologies, National Research University MPEI, Moscow, Russia. E-mail: BaronovOR@mpei.ru

8 Sofia V. Nemchaninova, senior lecturer, Department of Information Technologies, University «Dubna», Dubna, Russia, E-mail: sbobylova94@gmail.com

Состояние вопроса по рассматриваемой проблеме

Термин «цифровой двойник» (Digital twin, сокр. DT) появился более десяти лет назад и до сих пор не имеет четкого определения. Тем не менее интерес к этому направлению постоянно возрастает и особенно в тех областях, где много неформализуемых задач, нечетких значений параметров, случайных и непредвиденных ситуаций в автоматизированных системах управления, критических информационных инфраструктурах и социально значимых информационных системах. DT во многом могут решать часть этих задач на этапах проектирования, внедрения и мониторинга этих систем.

Следует отметить, что концепция цифровых двойников впервые была провозглашена как важная часть четвертой промышленной революции (Industry 4.0), основанный на массовом внедрении информационных технологий в промышленность, масштабной автоматизации бизнес-процессов и распространении искусственного интеллекта [1-2]. Основная цель перехода к концепции Industry 4.0 заключается в «переходе на полностью автоматизированное цифровое производство, управляемое интеллектуальными системами в режиме реального времени в постоянном взаимодействии с внешней средой, выходящее за границы одного предприятия, с перспективой объединения в глобальную промышленную сеть Интернета вещей (киберфизических систем)» [3]. Это определение цели, по нашему мнению, представляет очень поверхностный взгляд на концепцию Industry 4.0 и совсем не отражает главную ее цель – повышение экономической эффективности производства товаров и услуг за счет внедрения новых информационных технологий и искусственного интеллекта в системы управления. К сожалению, в отечественных программных документах эта цель в явном виде не рассматривается, а заявляется о других целях: цифровой трансформации, цифровых двойниках, цифровизации общества, внедрения Интернета вещей и т.д. [4]. Но это только условия достижения главной цели промышленной революции, и они не связаны с экономической эффективностью от внедрения этих технологий. Надо отметить, что такой взгляд на промышленную революцию Industry 4.0 автоматически трансформируется на локальные нормативные акты отдельных субъектов и это вызывает сомнение в успешности реализации этих проектов.

Анализ существующих взглядов на терминологию цифровых двойников, цели их создания, области применения и технологии реализации показал, что единых подходов к решению этих задач сегодня не существует [5–9]. Наиболее полно термин «цифровой двойник» можно определить как виртуальное или виртуально-физическое представление процессов, физических объектов или систем, которое используется в качестве оценки, диагностики, оптимизации и контроля их характеристик при проектировании, принятии решений в различных ситуациях и для эффективного управления реальными системами [4-5]. При этом исходные данные для работы системы цифрового двойника предоставляется непосредственно информационной или автоматизированной системой как результаты её деятельности. В отдельных исследованиях допускается что DT может быть включен непосредственно как функция в состав информационной системы или АСУ.

В другой группе определений DT подчёркивается особенность построения системы цифровых двойников, которую можно охарактеризовать как многоцелевую, многозадачную, виртуальную систему, аналогичную физической системе сложных объектов в различных сферах деятельности и использующую технологии больших данных и методы искусственного интеллекта и машинного обучения [7–9]. В этом определении подчёркивается обязательное использование новых информационных технологий, позволяющих расширить круг решаемых задач в системе управления до уровня принятия отдельных решений. Следует также отметить, что не всегда существует необходимость создания полного аналога физической системы управления в виртуальной среде, а такого рода задачи могут быть реализованы в том случае, если DT и его физическая сущность будут находиться в разных средах, например в агрессивной среде.

Не менее важным остается вопрос определения области применения DT. Наиболее важными из них являются:

1. Проектирование ИС и АСУ. Прежде всего, это возможность исследовать поведение сложных систем до их физической реализации и оценивать их эффективность.
2. Разработка архитектуры системы информационной безопасности.
3. Моделирование поведение ИС и АСУ при различных ситуациях.
4. Оценка эффективности систем по различным критериям.
5. Аудит ИС и оценка их соответствия проектным требованиям.
6. Прогнозирование последствий сценариев инцидентов.
7. Оптимизация процессов управления.
8. Модернизация систем АСУ (АСУТП).
9. Обучение.

Сфера применения цифровых двойников сегодня практически неограничена и определяется только

величиной допустимых затрат на их создание. В литературных источниках наиболее популярными сферами применения цифровых двойников является производство, аэрокосмическая промышленность, здравоохранение, кибербезопасность и медицина [9–14].

Однако несмотря на то, что успешные технологии DT в настоящее время активно исследуются и находят массовое распространение, единой теории и методологии разработки DT сегодня не существует, концептуальные модели цифровых двойников обычно весьма примитивны и рассматривают только ручное управление DT, полуручное с частично автоматическим управлением и DT с автоматическим управлением с использованием методов и технологий искусственного интеллекта и машинного обучения. Кроме того, в литературе рассматриваются также вопросы интеграции различных цифровых двойников в единую среду из различных виртуальную и физическую систему. Однако, эти направления могут рассматриваться только как перспективные разработки, проектированные которых возможно только при решении проблемы со стандартизацией в разработке эталонных моделей и архитектур DT [7].

Концептуальная модель DT

Рассмотрим структурную схему концептуальной модели цифровых двойников для различных направлений их возможного применения (рис. 1). Цифровой двойник представляет собой отдельно созданное приложение, взаимодействующее с физической информационной системой АСУ (АСУТП). Информационная система АСУ обеспечивает функциональный набор выполняемых задач

$$\mathcal{F}o\,(Ao, Xo, So, Go) \rightarrow Yo \qquad (1)$$

где Ao – алгоритмы, реализующие функции управления; Xo – параметры, характеризующие состояние объекта управления; So – система ограничений; Go – цели управления; Yo – результат управления.

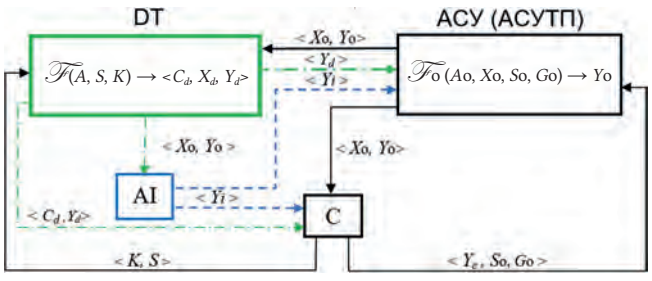

Рис. 1. Концептуальное модель цифрового двойника

Информационная система (1) обычно реализуется в технологиях SCADA-систем (Supervisory Control And Data Acquisition) [15]. Они обычно представляют собой полнофункциональный инструмент для проведения полного цикла работ по проектированию системы сбора данных в телеметрической системе и управлению ими. Управление в SCADA достигается путем задания алгоритмов обработки данных, формированию управляющих команд на исполнительные механизмы, формированию сигналов тревог, настройке баз данных и архивов событий, формированию технологических и оперативных схем отображения информации. Для разработки пользовательского интерфейса имеется библиотека готовых тематических объектов по отображению оперативной и архивной информации, что позволяет решать задачи автоматизации распределенных и локальных объектов. Задачи, которые выполняют DT, обычно в SCADA-системах не предусматриваются, но и не исключаются совсем.

Модель цифрового двойника представлена на левой части рис.1 и имеет следующий вид

$$\mathcal{F}(A, S, K) \rightarrow <C_d, X_d, Y_d> \qquad (2)$$

где A – алгоритмы и модели DT; S – система ограничений; K – критерии эффективности системы управления; C_d – показатели эффективности системы управления; Y_d – результат моделирования управляющего воздействия по ситуации X_d.

Модель DT позволяет проводить мониторинг работы АСУ путем контроля реакций системы на изменения контролируемых параметров как в обычных режимах работы, так и в критических ситуациях. Кроме того, модель DT позволяет определять параметры эффективности работы системы управления физической моделью на этапах ее проектирования, эксплуатации и модернизации. Исходные параметры модели (2) могут быть заданы и в автономном режиме. Это может быть использовано при обучении персонала и при исследовании критических режимов работы физических систем.

Модель DT может включать и систему искусственного интеллекта (Artificial Intelligence, AI). Это расширяет круг задач с использованием цифрового двойника. Применение методов машинного обучения позволяет решать задачи, связанные с классификацией критических ситуаций и обоснования необходимых управляющих действий по ним. При этом формирование модели базы знаний может осуществляться на основе результатов моделирования этих ситуаций на DT.

DT способен также раскрывать информацию, скрытые закономерности и неизвестные корреляции[9]. Возможность записи, контроля и мониторинга

9 Термин «корреляция» рассматривается нами не только как статистический термин, оценки степени линейной статистической связи между переменными, но и как многомерная нелинейная связь между ними.

условий и изменений физической системы позволяет применять прогнозирование сбоев, проверки результатов возможных решений, чтобы избежать ошибок или найти лучшие решения [8].

Пример разработки цифрового двойника для процесса планирования рисков информационной безопасности

Концепция применения DT не обошла вниманием и сферу информационной безопасности. Исследования в этой сфере носят характер выяснения возможностей применения DT в сферах информационной и кибербезопасности. К сожалению, эти исследования ограничиваются общими выводами и не демонстрируют практических результатов. Однако есть исследования претендующие на создание системы управления информационной безопасностью с использованием DT [13,16]. Они основаны на процессном подходе, а управление информационной безопасностью разделяется на 4 уровня: знаний, данных, организации и инфраструктуры [16]. Каждый из этих уровней представляет собой набор процессов, выполняемых DT. Такой подход весьма ограничивает сферу деятельности DT, так в основе системы управления, где принимаются решения, лежит событийно-процессный подход, который сегодня используется в современных системах управления информационной безопасностью [17]. Объединить разные уровни управления информационной безопасностью практически невозможно в этой концепции [16]. Кроме того, в таком представлении невозможно сформулировать цели и задачи отдельных DT. Исходя из этих рассуждения были сформулированы следующие задачи, которые необходимо решать с использованием DT в системах управления информационной и кибербезопасности:

1. Моделирование параметров систем информационной безопасности с заданными начальными параметрами и ориентированными на конечные цели организации.
2. Оценка защищенности информационных систем по контролю параметров архитектуры системы информационной безопасности.
3. Прогнозирование реакции системы управления информационной безопасностью (СУИБ) на возможные инциденты.
4. Расследование инцидентов информационной безопасности на модели DT.
5. Поддержка принятия решений на проектирование и развитие системы информационной безопасности.
6. Оценка эффективности СУИБ по заданным критериям.
7. Обучение специалистов по методологии создания систем информационной безопасности и кибербезопасности.

На наш взгляд этот список неограничен как по созданию новых направлений цифровых двойников, так и путем создания интегрированных систем DT.

Для реализации примера использования цифровых двойников была выбрана первая задача из приведенного списка. Она связана с 5 и 6 задачами. В качестве модели (1) была принята модель построения системы управления информационной безопасностью на основе концепции рисков, изложенной в стандарте[10]. Эта модель основана на архитектуре системы информационной безопасности путем оценки параметров рисков в виде возможных ущербов от реализации инцидентов информационной безопасности [18]. Исходные параметры и результаты решения представлены в следующем виде:

$$Xo = <Nt, Et, Nv, Ev, Na, Ea> \quad (3)$$

$$Yo = < M, V, C, Z >, \quad (4)$$

где Nt, Nv, Na – наименования (коды) угроз, уязвимостей, активов; Et, Ev, Ea – значения возможностей появления угроз, величин уязвимостей и ценностей активов в числовых значениях лингвистических переменных; M – метрики рисков; V, C, Z, U – вариант обработки рисков, контрмеры по защите, затраты, ущерб (риск).

Алгоритм оценки параметров рисков (Ao) основан на схеме обработки рисков, представленной с стандарте[3]. В алгоритме предусмотрен анализ контекста риска[11], оценка возможностей появления угроз (T), оценка значений уязвимостей (V) и оценка ценности информационных активов (A). Эти параметры задаются в форме лингвистических переменных, которым назначаются цифровые метрики (Et, Ev, Ea). Значения метрики риска (M) интерпретируются как относительное числовое значение, которое определяется как сумма значений $M = Et + Ev + Ea$. Например, при значении возможности угрозы равной «средняя» из трех классов угроз (низкая (0), средняя (1), высокая (2)) значение Et равно «1». Очевидно, что этот алгоритм не позволяет решать ни одну из перечисленных задач информационной и кибербезопасности и требуется методика перехода от этих относительных значений риска к абсолютным.

При разработке модели ИС были приняты следующие ограничения (So):

1. Рассматривались риски только для умышленных угроз. Это позволяет значительно сузить круг рисков. Остальные риски – природные и случайные требуют шаблонных действий. Природные риски обычно учитываются при проектировании зданий и сооружений, а случайные риски зависят

10 Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности. ГОСТ Р ИСО/МЭК 27005-20012.

11 Контекст риска – это внешняя и внутренняя среда организации, влияющая на параметры риска.

от надежности оборудования и уровня культуры информационной безопасности, профессиональной этики и подготовки персонала. Управление случайными рисками осуществляется по методологии COBIT 5.0 [17].

2. В модели ИС были применены правила корреляций между параметрами угроз, уязвимостей и ценностью информационных активов. Это в значительной степени позволило повысить определенность оценки параметра угроз.

Алгоритм (Ao) ввиду неопределенности некоторых параметров модели (3), в том числе выбор способа обработки риска и оценки его остаточного значения, реализуется в полуавтоматическом режиме. В дальнейшем, при решении достаточного количества практически задач используется технология машинного обучения.

Целями модели АСУ (Go) являются:

1. Разработка плана обработки рисков информационной безопасности на основе оценки параметров рисков, определения ущерба в относительных значениях и затрат в относительных единицах, сумма которых не превышает предельного значения стоимости информационных активов в плане обработки рисков.
2. Проведение анализа рисков по его отдельным параметрам (угрозам, уязвимостям, активам).
3. Управление рисками путем включения в план новых рисков, определения их приоритетов и значений.

Параметры модели цифрового двойника представлены в следующем виде:

$$X_d = <Nt, Et, Nv, Ev, Na, Ea, M, V, C, Z, U> \quad (5)$$

$$Y_d = < s_z, s_u >, C_d , \quad (6)$$

где U – возможные значения ущерба (риска), выраженные в абсолютных значениях, например в денежных эквивалентах. Эта весьма сложная задача задача решается двумя методами. Первый основан на представлении параметров ущерба в виде нечеткой величины. Для этого задаются границы определения лингвистических переменных, количество термов, вид и параметры функции принадлежности. Применение этого метода не позволяет оценить погрешности показателей эффективности Cd, поэтому использовался второй метод, основанный на имитационном моделировании значений рисков при заданных интервалах их значений. Применение этого подхода к оценке показателей ущерба основано на Центральной предельной теореме, которая утверждает, что сумма достаточно большого количества слабо зависимых случайных величин, имеющих примерно одинаковые масштабы (ни одно из слагаемых не доминирует и не вносит в сумму определяющего вклада), имеет распределение, близкое к нормальному. Устойчивость этих оценок зависит от статистики случайных величин показателей для каждого риска, степени независимости рисков и их количества; s_z, s_u – суммарные значения затрат на принятие мер защиты и возможного ущерба; Cd – показали эффективности системы управления рисками информационной безопасности. К показателям эффективности можно отнести следующие:

a) План обработки рисков при ограничениях на затраты (Cd_1)

$$Cd_1 = \left(\sum_{i=1}^{k} z_i^s < z_0 \right), \; i = \overline{1,k}, \; s = \overline{1,n} \quad (7)$$

b) План обработки рисков при максимальной разнице между оценками возможного ущерба и затрат

$$Cd_2 = \max_S \left(\sum_{i=1}^{k} (u_i^s - z_i^s) \right), \; i = \overline{i,k} \; , \; s = \overline{1,n} \quad (8)$$

c) План обработки рисков при максимальном значении возможного ущерба и ограничениях на затраты

$$Cd_3 = \max_S \left(\sum_{i=1}^{k} (u_i^s - z_i^s) \right) \left(\sum_{i=1}^{k} z_i^s < z_0 \right), \; i = \overline{1,k}, \; s = \overline{1,n} \quad (9)$$

d) План обработки рисков при максимальном значении ущерба и ограничениях на затраты

$$Cd_4 = \max_S \left(\sum_{i=1}^{k} u_i^s \right), \left(\sum_{i=1}^{k} z_i^s < z_0 \right), \; i = \overline{1,k}, \; s = \overline{1,n} \quad (10)$$

В выражениях (7–10) используется переменная s, которая определяет стратегию управления рисками информационной безопасности и, по существу, связана с целью и способом обработки матрицы рисков (5). Каждая стратегия задается приоритетным параметром, по которому упорядочивается матрица

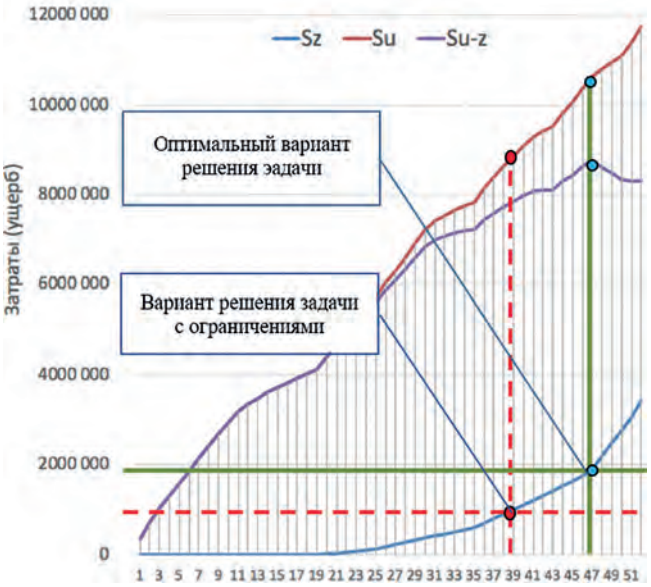

Рис. 2. График определения показателей эффективности плана по критерию CD_2 (оптимальный вариант) и CD_3 (лучший вариант с ограничением по затратам)

рисков. Например, если приоритетным параметром при анализе являются затраты, то матрица рисков представляется в форме упорядоченных по возрастанию или убыванию затрат на каждый риск. На рис. 2 представлено два варианта решения оценки эффективности плана обработки рисков.

Моделирование проводилось на матрице рисков информационной безопасности (5) по заданным параметрам информационных активов организации, уязвимостям и модели угроз. Рассчитывались значения метрик рисков (относительный ущерб). Эти данные передавались в DT, где по заданным абсолютным значениям интервалов рисков моделировались их абсолютные значения на 50 реализациях имитационной модели. По результатам моделирования вычислялось среднее значение параметра s_u и его погрешность. Параметр s_z вычислялся по данным фактических затрат на принятие контрмер защиты. На рис.2 показана первая точка решение задачи Cd_2 (нахождение оптимального варианта при различных стратегиях обработки рисков). Затраты на защиту по этому варианту стратегии (s_1) состаляют 2'000 тыс. руб., при предотвращенном ущербе более 10'000 тыс. руб.

Вторая задача Cd_3 решалась при ограничениях на затраты. По этой же стратегии s_1 и ограничениях по затратам 1'000 тыс. руб. предотвращенный ущерб может составить 9'000 тыс. руб, но при этом могут возникнуть риски с ущербом 3'000 тыс. руб. от принятия[12] последних трех рисков. По этим данным принимается решение.

12 Принять риск, значит согласится с ним, а реакцию на него предусмотреть в плане обеспечения непрерывности процессов.

Заключение

Концепция цифровых двойников является частью четвертой промышленной революции (Industry 4.0), основанной на массовом внедрении информационных технологий в промышленность, масштабной автоматизации бизнес-процессов и распространении искусственного интеллекта. Исследования, проведенные в этой сфере деятельности, показали, что это направление требует безусловного развития в системах управления информационной и кибербезопасности.

В статье, на основе анализа, было уточнено содержание термина «цифровой двойник», определена область его использования и возможные сферы применения. Это позволило разработать вариант концептуальной модели цифрового двойника и описать его входные и выходные параметры.

На примере моделирования конечных параметров систем информационной безопасности с заданными начальными параметрами и целями был показан механизм разработки модели DT. Эта модель может быть использована при проектировании системы управления информационной безопасностью КИИ.

Дальнейшим направлением развития цифровых двойников в сфере информационной и кибербезопасности является разработка нового направления по защите АСУТП с решением задач управления объектом одновременно с анализом состояния системы информационной безопасности АСУТП и последующим прогнозированием его будущего состояния от очередного управляющего воздействия.

Литература

1. *Zheng T. et al. The applications of Industry 4.0 technologies in manufacturing context: a systematic literature review //International Journal of Production Research. – 2021. – Т. 59. – №. 6. – С. 1922-1954.*
2. *Pozzi R., Rossi T., Secchi R. Industry 4.0 technologies: critical success factors for implementation and improvements in manufacturing companies //Production Planning & Control. – 2023. – Т. 34. – №. 2. – С. 139–158.*
3. *Клейменова Л. Что такое индустрия 4.0 и что нужно о ней знать URL https://trends.rbc.ru/trends/industry/5e740c5b9a79470c22dd13e7?from=copy (дата обращения: 23.04.2020).*
4. *Ватутина Л. А., Злобина Е. Ю., Хоменко Е. Б. Цифровизация и цифровая трансформация бизнеса: современные вызовы и тенденции// Вестник Удмуртского университета. Серия «Экономика и право». 2021. №4.*
5. *Morteza Ghobakhloo Industry 4.0, digitization, and opportunities for sustainability // Journal of Cleaner Production, Volume 252/–2020, ISSN 0959-6526, https://doi.org/10.1016/j.jclepro.2019.119869.*
6. *Azeez N. A., Adjekpiyede O. O. Digital Twin Technology: A Review of Its Applications and Prominent Challenges //Covenant Journal of Informatics and Communication Technology. – 2022.*
7. *Duan H, Gao S, Yang X and Li Y. The development of a digital twin concept system [version 2; peer review: 3 approved with reservations]. Digital Twin 2023, 2:10 (https://doi.org/10.12688/digitaltwin.17599.2)*
8. *Fei Tao, Bin Xiao, Qinglin Qi, Jiangfeng Cheng, Ping Ji. Digital twin modeling // Journal of Manufacturing Systems, Volume 64, 2022, Pages 372–389, ISSN 0278-6125/*
9. *Singh, M., Fuenmayor, E., Hinchy, E. P., Qiao, Y., Murray, N., & Devine, D. (2021). Digital twin: Origin to future. Applied System Innovation, 4(2), 36.*
10. *Pokhrel A., Katta V., Colomo-Palacios R. Digital twin for cybersecurity incident prediction: A multivocal literature review // Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops. – 2020. – С. 671–678.*
11. *Masi, M., Sellitto, G. P., Aranha, H. et al. Securing critical infrastructures with a cybersecurity digital twin. Softw Syst Model 22, 689–707 (2023). https://doi.org/10.1007/s10270-022-01075-0*

12. *D. Holmes, M. Papathanasaki, L. Maglaras, M. A. Ferrag, S. Nepal and H. Janicke, «Digital Twins and Cyber Security – solution or challenge?» 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Preveza, Greece, 2021, pp. 1–8, doi: 10.1109/SEEDA-CECNSM53056.2021.9566277.*
13. *Попов А. М., Золотарев В. В., Кунц Е. Ю. Проблема управления информационной безопасностью при создании цифрового двойника дисциплины // Прикаспийский журнал: управление и высокие технологии. – 2022. – №. 2 (58). – С. 109–118.*
14. *Курганова Н. В., Филин М. А., Черняев Д. С., Шаклеин А. Г., Намиот Д. Е. Внедрение цифровых двойников как одно из ключевых направлений цифровизации производства // International Journal of Open Information Technologies. 2019. №5. URL: https://cyberleninka.ru/article/n/vnedrenie-tsifrovyh-dvoynikov-kak-odno-iz-klyuchevyh-napravleniy-tsifrovizatsii-proizvodstva (дата обращения: 12.02.2024).*
15. *Yadav G., Paul K. Architecture and security of SCADA systems: A review //International Journal of Critical Infrastructure Protection. – 2021. – Т. 34. – С. 100433.*
16. *Касимова А. Р., Золотарев В. В., Сафиулина Л. Х., Балыбердин А. С. Использование цифрового двойника в задачах управления информационной безопасностью // Прикаспийский журнал: управление и высокие технологии. 2023. №1 (61).*
17. *Isnaini K. N., Suhartono D. Evaluation of Basic Principles of Information Security at University Using COBIT 5 //MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer. – 2022. – Т. 21. – №. 2. – С. 317–326..*
18. *Минзов А. С., Невский А. Ю., Баронов О. Р. Управление рисками информационной безопасности: Монография / Под редакцией А. С. Минзова. — М. : ВНИИгеосистем, 2019. — 110 с.: ил.*