Международный научно-исследовательский журнал
«Прогрессивная экономика»
№ 2 / 2026 https://progressive-economy.ru/vypusk_1/informaczionnaya-bezopasnost-czifrovyh-dvojnikov-v-sistemah-upravleniyah-analiz-ugroz-i-metody-zashhity/
Научная статья / Original article
Шифр научной специальности ВАК: 5.2.3
УДК 65.011.56
DOI: 10.54861/27131211_2026_2_340

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВЫХ ДВОЙНИКОВ В СИСТЕМАХ УПРАВЛЕНИЯХ: АНАЛИЗ УГРОЗ И МЕТОДЫ ЗАЩИТЫ

Булатенко М.А., *доцент, МИРЭА – Российский технологический университет, г. Москва, Россия*
119454 г. Москва, проспект Вернадского, дом 78
ORCID: https://orcid.org/0000-0002-0017-1753
e-mail: mabulatenko@gmail.com

Федин М.А., *профессор, Национальный исследовательский университет «МЭИ», г. Москва, Россия*
111250, Россия, г. Москва, ул. Красноказарменная, д. 14, стр. 1
ORCID: https://orcid.org/0009-0007-7309-0333
e-mail: FedinMA@mpei.ru

Маркин Н.В., *студент магистратуры, МИРЭА – Российский технологический университет, г. Москва, Россия*
119454 г. Москва, проспект Вернадского, дом 78
ORCID: https://orcid.org/0009-0004-9826-4377
e-mail: koljamar77@mail.ru

Аннотация. Целью исследования является анализ особенностей применения цифровых двойников в системах управления, выявление угроз информационной безопасности и разработка методов защиты от киберугроз. В работе использованы методы экспериментального моделирования, сетевого анализа и имитационного тестирования на примере упрощенной модели системы охлаждения серверной стойки. Проведенные эксперименты выявили уязвимости в системе «цифровой двойник – реальный объект» на уровне сетевого взаимодействия, включая возможность перехвата и подмены телеметрии, повторной отправки пакетов и несанкционированного управления физическими параметрами объекта. Результаты исследования демонстрируют, что злоумышленник, получивший доступ к цифровому двойнику, может не только изучить конфигурацию инфраструктуры и выявить уязвимые места, но и использовать полученные данные для подготовки целенаправленных кибератак на реальные объекты. В работе авторами

предложены методы защиты, включающие применение цифровых песочниц для безопасного тестирования, внедрение механизмов аутентификации команд, контроль целостности сообщений и использование баг-баунти программ. Результаты настоящего исследования подтверждают необходимость комплексного подхода к обеспечению безопасности цифровых двойников как критически важного компонента современных систем управления.

Ключевые слова: система управления, угрозы, информационная безопасность, уязвимость, цифровой двойник.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Булатенко М.А., Федин М.А., Маркин Н.В. Информационная безопасность цифровых двойников в системах управления: анализ угроз и методы защиты // Прогрессивная экономика. 2026. № 2. С. 340–357. https://doi.org/10.54861/27131211_2026_2_340.

Статья поступила в редакцию: 18.01.2026 г. Одобрена после рецензирования: 25.02.2026 г. Принята к публикации: 28.02.2026 г.

INFORMATION SECURITY OF DIGITAL DOUBLETS IN MANAGEMENT SYSTEMS: THREAT ANALYSIS AND PROTECTION METHODS

Bulatenko M.A., *Associate Professor, MIREA – Russian University of Technology, Moscow, Russia*
78 Vernadsky Avenue, Moscow, 119454
ORCID: https://orcid.org/0000-0002-0017-1753
e-mail: mabulatenko@gmail.com

Fedin M.A., *Professor, National Research University "MPEI", Moscow, Russia*
111250, Russia, Moscow, Krasnokazarmennaya str., 14, building 1
ORCID: https://orcid.org/0009-0007-7309-0333
e-mail: FedinMA@mpei.ru

Markin N.V., *Master's degree student, MIREA – Russian University of Technology, Moscow, Russia*
78 Vernadsky Avenue, Moscow, 119454
ORCID: https://orcid.org/0009-0004-9826-4377
e-mail: koljamar77@mail.ru

Abstract. The purpose of the study is to analyze the features of the use of digital twins in management systems, identify threats to information security and develop methods to protect against cyber threats. The paper uses methods of experimental modeling, network analysis and simulation testing using the example of a simplified model of a server rack cooling system. The experiments revealed vulnerabilities in the "digital twin – real object" system at the network

interaction level, including the possibility of intercepting and spoofing telemetry, re-sending packets, and unauthorized control of the physical parameters of the object. The results of the study demonstrate that an attacker who has gained access to a digital double can not only study the infrastructure configuration and identify vulnerabilities, but also use the data obtained to prepare targeted cyber-attacks on real objects. In this paper, the author suggests protection methods, including the use of digital sandboxes for secure testing, the introduction of command authentication mechanisms, message integrity control, and the use of bug bounty programs. The results of this study confirm the need for an integrated approach to ensuring the security of digital counterparts as a critically important component of modern control systems.

Keywords: management system, threats, information security, vulnerability, digital twin.

JEL classification: O33, M15.

Conflict of interest. Authors declare that there is no conflict of interest.

For citation: Bulatenko M.A., Fedin M.A., Markin N.V. (2026). Informacionnaya bezopasnostь cifrovy`x dvojnikov v sistemax upravleniyax: analiz ugroz i metody` zashhity` [Information security of digital doublets in management systems: threat analysis and protection methods]. Progressivnaya ekonomika [Progressive Economy], 2, 340–357, https://doi.org/10.54861/27131211_2026_2_340. (In Russ., abstract in Eng.)

The article was submitted to the editorial office: 18/01/2026. Approved after review: 25/02/2026. Accepted for publication: 28/02/2026.

Введение

Цифровые двойники в последние годы стали ключевым инструментом цифровой трансформации предприятий, позволяющим моделировать поведение объектов и процессов в реальном времени. Данная технология активно внедряется в промышленности, энергетике, транспорте, системах жизнеобеспечения и других сферах, где существует необходимость точного прогнозирования состояния оборудования и повышения эффективности управления [1]. Несмотря на наличие высокого потенциала технологии цифровых двойников, ее внедрение сопровождается рядом проблем, связанных с обеспечением информационной безопасности. Рост объема собираемых и обрабатываемых данных, интеграция цифровых двойников с облачными сервисами и промышленными интернет-платформами повышают уязвимость таких систем к кибератакам, что может привести к искажению данных, сбоям в управлении и финансовым потерям.

В этой связи актуальной научной задачей становится исследование особенностей применения цифровых двойников в системах управления. *Целью* исследования является анализ особенностей применения цифровых двойников в системах управления, выявление угроз информационной безопасности и разработка методов защиты от киберугроз.

Обзор литературы

Цифровой двойник представляет собой интегрированную виртуальную модель реального объекта, способную воспроизводить его поведение на

основе данных телеметрии, систем мониторинга, журналов SCADA, IoT-устройств и технологических контроллеров [2]. Авторы рассматривают цифрового двойника как интегрированную модель реального объекта, функционирующую на основе мониторинга и управления, благодаря чему цифровые двойники обеспечивают аналитическую поддержку принятия решений, повышают надежность инфраструктуры и позволяют выявлять неисправности еще до их фактического появления.

Одновременно появляются новые риски, связанные с безопасностью данных, целостностью цифровой модели, защищенностью каналов связи и возможностью использования цифрового двойника злоумышленниками для анализа инфраструктуры и подготовки кибератак (рис. 1) [3; 4].

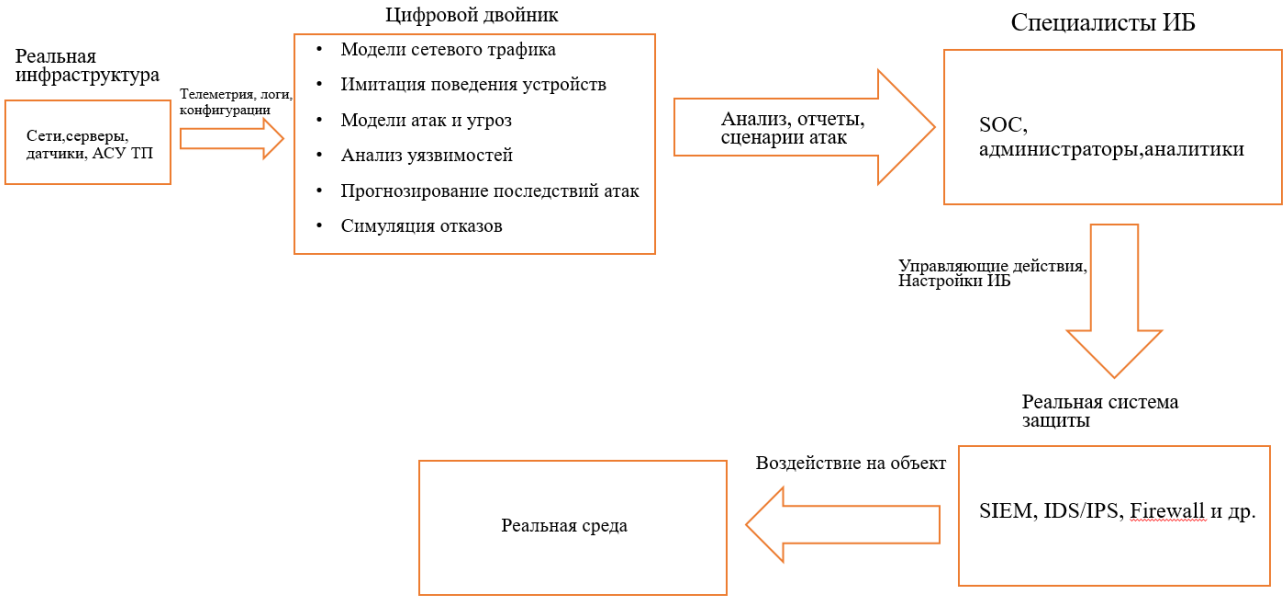

Рис. 1. Представление цифрового двойника
Источник: составлено авторами по данным [3, 4]
Fig. 1. Representation of the digital twin
Source: compiled by the authors based on [3, 4]

Цифровой двойник выполняет ряд функций: мониторинг состояния объекта, анализ динамики процессов, выявление отклонений, прогноз вероятных неисправностей, оценку сценариев воздействия и исследование поведения системы при различных изменениях [5]. Он служит не просто источником данных, а инструментом предиктивной аналитики и имитационного моделирования [6; 7]. Авторы отмечают, что цифровые двойники, которые основанные на данных мониторинга и управления, применяются для повышения надёжности сложных технических систем и выявления потенциальных отказов на этапах жизненного цикла.

С экономической точки зрения внедрение цифровых двойников представляет собой значительные инвестиции для предприятий, которые

должны быть экономически обоснованы. Однако все экономические преимущества могут быть нивелированы в случае успешных кибератак на системы цифровых двойник. При этом атаки, направленные на промышленные системы управления и их цифровые двойники, могут иметь каскадный эффект, приводя к многократному увеличению финансовых потерь из-за остановки производства, повреждения оборудования и репутационных издержек [8]. Авторы рассматривают цифровые двойники как элемент экономических платформ для управления, а также считают, что их внедрение связано с высокими инвестиционными затратами и системными рисками.

Цифровые двойники активно используются в баг-баунти-программах как безопасная среда для поиска уязвимостей. Предприятие предоставляет исследователям не доступ к реальным серверам, а к цифровому двойнику, который полностью повторяет конфигурацию инфраструктуры, что позволяет безопасно выявлять слабые места, тестировать сценарии атак, анализировать ошибки конфигурации и повышать устойчивость системы [9].

Сетевая инфраструктура, обеспечивающая функционирование цифровых двойников, представляет собой совокупность аппаратных и программных средств, включая маршрутизаторы, коммутаторы, сетевые протоколы, серверы приложений, серверы маршрутизации, политики безопасности и механизмы контроля доступа [10]. Авторы рассматривают цифровых двойников в связке с программными платформами управления, говоря, что их функционирование обеспечивается распределённой ИТ-инфраструктурой, которая включает сетевые компоненты, серверные решения и средства интеграции.

Сетевые каналы обеспечивают перенос данных телеметрии, управляющих сигналов и результатов анализа [11]. В статье цифровые двойники рассматриваются как элементы сетевых киберсоциофизических систем, где ключевую роль играет сетевая связка, обмен телеметрическими данными и управляющими воздействиями.

Локальная вычислительная сеть (LAN) представляет собой ограниченный географически сегмент сети организации и обеспечивает высокоскоростной обмен данными между серверами, рабочими станциями и устройствами. В контексте цифровых двойников LAN является основой для передачи телеметрии, конфигураций и аналитических данных, необходимых для актуализации и корректного функционирования модели [12].

Важно отметить различие между цифровой двойников и цифровой песочницей. Если цифровой двойник моделирует поведение реального объекта и зависит от актуальных данных, то песочница имитирует лишь минимально необходимое окружение для анализа угроз и не отражает реальный объект, а предоставляет инструмент для изоляции и диагностики подозрительных процессов [13; 14].

Применение цифровых двойников создает новые векторы атак и увеличивает количество уязвимых точек. Основные угрозы включают

нарушение конфиденциальности данных, подмену телеметрии, атаки на API цифрового двойника, компрометацию IoT-устройств, вмешательство в алгоритмы моделирования и использование цифрового двойника злоумышленниками как полигона для подготовки атак. Если злоумышленник получает доступ к цифровому двойнику, он фактически получает доступ к точной виртуальной копии объекта, что позволяет исследовать логику функционирования системы, тестировать различные сценарии атаки и изучать реакцию систем безопасности без риска обнаружения [15].

Несмотря на ограниченное количество прямых атак на цифровые двойники, существует ряд инцидентов [16; 17]:

– атака Triton в 2017 году, где злоумышленники получили доступ к инженерной модели системы безопасности нефтехимического предприятия, переписали логику контроллеров и попытались вывести объект из строя;

– инцидент BlackEnergy 2015 года, в котором атакующие изучили схемы энергосистемы Украины, топологию подстанций и виртуальные модели переключения нагрузки, а полученные данные использовали для вывода части энергосети из строя;

– атака Colonial Pipeline, произошедшая в 2021 году, при реализации которой были похищены цифровые схемы трубопровода, что позволило злоумышленникам понять уязвимые звенья системы;

– исследования уязвимостей Tesla (2020–2022 гг.) показали, что манипуляция данными сенсоров приводит к нарушению работы цифровой модели автомобиля, что подтверждает уязвимость систем, основанных на цифровых двойниках.

Экономические последствия этих инцидентов были значительными. Например, атака на Colonial Pipeline привела к остановке трубопровода на 6 дней, что вызвало дефицит топлива на восточном побережье США и потери компании в размере около 4,4 млн долларов только в виде выплаченного выкупа, не считая упущенной выгоды и репутационных потерь.

Материалы и методы

Для практической проверки уязвимостей системы «цифровой двойник – реальный объект» на уровне сетевого взаимодействия был разработан экспериментальный стенд. Цель эксперимента – наглядно показать, что при отсутствии механизмов защиты данные цифрового двойника могут быть перехвачены, подменены или повторно использованы злоумышленником.

В качестве исследуемой системы использовалась упрощенная модель охлаждения серверной стойки с одним вентилятором. Реальный объект эмулировался программно и передавал цифровому двойнику телеметрию о температуре и скорости вентилятора по сети в формате JSON. Управление осуществлялось с помощью команд увеличения и уменьшения скорости вентилятора, что соответствует логике реальных систем управления.

Цифровой двойник был реализован как отдельное приложение, которое принимало телеметрию, рассчитывало состояние системы на основе

собственной модели и сравнивало полученные данные с фактическим значениями. Это позволяло выявлять отклонения и аномалии в работе системы. Для анализа сетевого взаимодействия использовался сетевой анализатор Wireshark. Передача данных осуществлялась через локальный сетевой интерфейс, что давало возможность перехватывать и анализировать пакеты без использования внешней сети.

Экспериментальная система состояла из трех основных программных компонентов:

1. Digital_twin.py – реализация логики цифрового двойника, включая прием телеметрии, расчет состояния системы и сравнение модели с полученными данными.

2. Object.py – эмулятор реального физического объекта (системы охлаждения с вентилятором).

3. Operator_console.py – консоль оператора для отправки управляющих команд.

В ходе эксперимента были реализованы различные сценарии атак и ошибок передачи данных, включая пакеты с задержкой, неверной подписью, повторную передачу старых данных и несогласованную телеметрию.

Результаты и обсуждение

На рисунке 2 показано стартовое окно сетевого анализатора Wireshark, используемого в эксперименте для перехвата сетевого трафика между компонентами системы цифрового двойника. В центральной части окна отображается список доступных сетевых интерфейсов, включая проводное подключение Ethernet, беспроводную сеть, а также loopback-адаптер, который применяется для захвата локального трафика. В верхней части окна расположена строка фильтра, предназначенная для ограничения отображаемых пакетов по заданным условиям. Данный этап необходим для выбора источника трафика и подготовки среды к анализу сетевого взаимодействия между цифровым двойником, эмулятором объекта и консолью оператора.

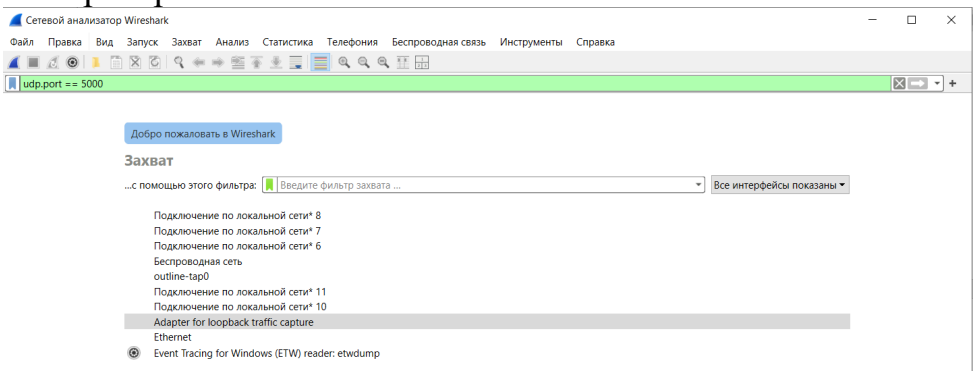

Рис. 2. Стартовое окно сетевого анализатора Wireshark

Источник: составлено авторами

Fig. 2. Wireshark Network Analyzer Start Window

Source: compiled by the authors

В процесс задания фильтра отображения трафика в Wireshark вводится выражение udp.port == 5000, которое ограничивает вывод только теми сетевыми пакетами, которые передаются по протоколу UDP и используют порт 5000 в качестве порта источника или назначения. В рамках эксперимента данный порт используется для обмена управляющими командами и телеметрией между компонентами системы. Применение фильтра позволяет убрать посторонний сетевой трафик и сосредоточиться на анализе данных, относящихся к работе цифрового двойника.

В рабочей директории проекта digital_twin_security (рис. 3) созданы основные программные компоненты экспериментальной системы, что иллюстрирует модульную структуру проекта и разделение функциональности между цифровым двойником, объектом управления и пользовательским интерфейсом. Файл digital_twin.py отвечает за работу цифрового двойника. В нём реализована логика приёма телеметрии от реального объекта, расчёт собственного состояния системы и сравнение модели с полученными данными. Цифровой двойник проверяет корректность сообщений, их актуальность по времени и выявляет расхождения между моделью и реальными значениями. При обнаружении нарушений он формирует предупреждения, которые используются как результаты эксперимента.

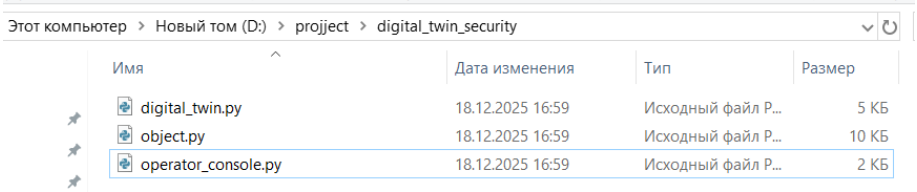

Рис. 3. Рабочая директория проекта digital_twin_security

Источник: составлено авторами

Fig. 3. The working directory of the digital_twin_security project

Source: compiled by the authors

Рассмотрим механизм обнаружения аномалий и контроля целостности данных в цифровом двойнике (рис. 4). В строках терминала отображаются текущие параметры реального объекта и модели цифрового двойника, включая реальную температуру (realT), температуру, вычисляемую моделью цифрового двойника (modelT), скорость вентилятора (fan) и допустимый температурный диапазон. Сообщения с пометкой ALERT указывают на выявление несоответствия данных, когда разница между модельной и реальной температурой превышает допустимое значение.

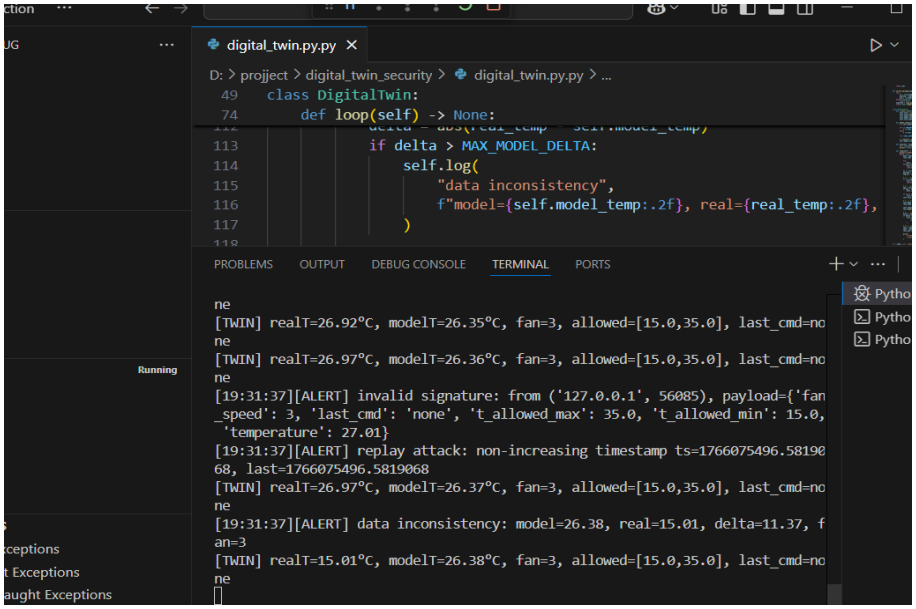

Рис. 4. Фрагмент digital_twin.py

Источник: составлено авторами

Fig. 4. The fragment digital_twin.py

Source: compiled by the authors

Файл object.py представляет собой эмулятор реального физического объекта – системы охлаждения с одним вентилятором. Он рассчитывает температуру в зависимости от скорости вентилятора, принимает управляющие команды увеличения и уменьшения скорости и периодически отправляет телеметрию цифровому двойнику по сети. В рамках эксперимента данный файл моделирует поведение реального оборудования и является источником сетевого трафика.

Рассмотрим реализацию сценариев атак и ошибок передачи данных, которые используются для проверки устойчивости цифрового двойника к сетевым нарушениям и подмене информации (рис. 5). В терминале отображаются сообщения о намеренной отправке некорректных сетевых пакетов, включая пакеты с задержкой, неверной подписью, повторной передачей старых данных и несогласованной телеметрией.

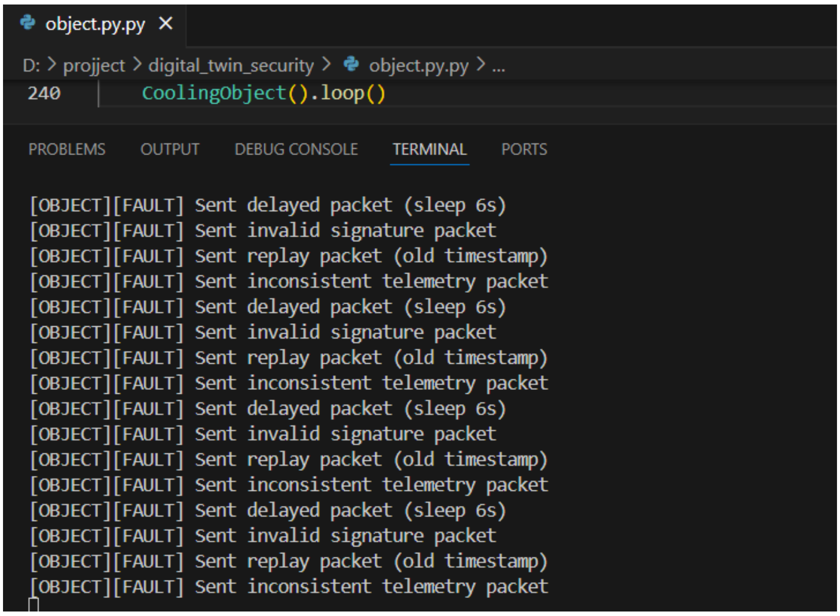

Рис. 5. Фрагмент object.py

Источник: составлено авторами

Fig. 5. The fragment object.py

Source: compiled by the authors

Файл operator_console.py используется для имитации действий легитимного оператора системы (рис. 6). Через него вручную отправляются команды управления вентилятором, такие как увеличение или уменьшение скорости. Консоль оператора позволяет показать нормальный сценарий работы системы и сравнить его с аномальными ситуациями, возникающими при сетевых атаках или подмене данных. После запуска программы оператору предлагается ввод команд управления вентилятором, таких как увеличение или уменьшение скорости вращения. Вводимые команды передаются по сети к эмулятору объекта и далее учитываются цифровым двойником.

Если детально рассмотреть сетевой пакет в Wireshark (рис. 7), можно сформулировать вывод, что передаваемая информация доступна для анализа и интерпретации при отсутствии шифрования. В верхней части окна отображается список перехваченных UDP-пакетов, а в нижней — их структура и содержимое. В правой части видно полезную нагрузку пакета в формате JSON, содержащую параметры управления вентилятором, температурные значения, временную метку и цифровую подпись. В нижней части окна отображаются временные характеристики пакетов и их содержимое, включая временные метки, используемые для выявления атак повторной передачи.

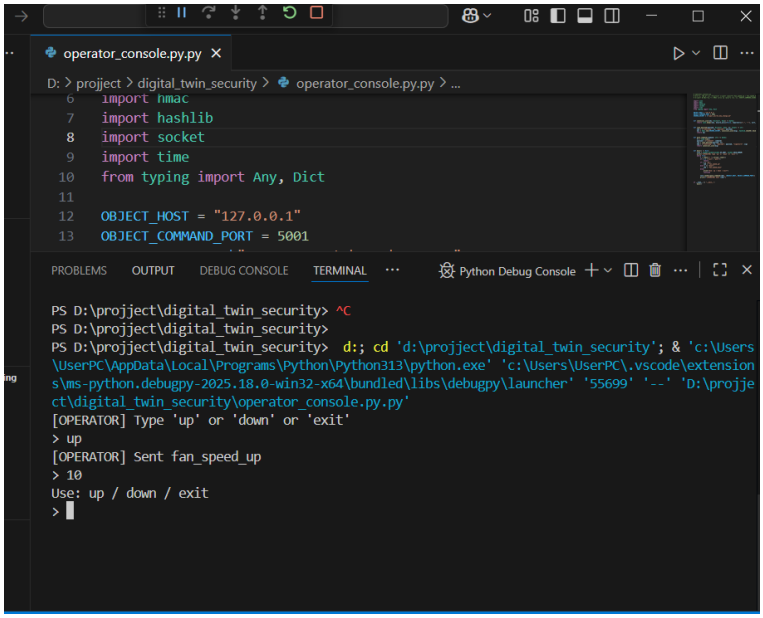

Рис. 6. Фрагмент operator_console.py

Источник: составлено авторами

Fig. 6. The fragment operator_console.py

Source: compiled by the authors

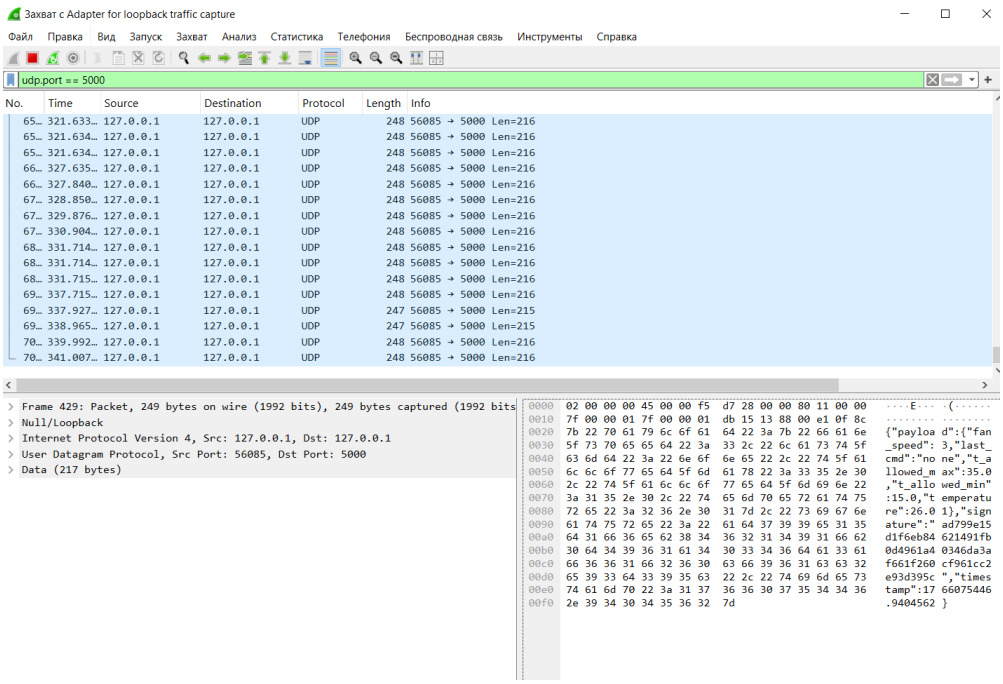

Рис. 7. Сетевой пакет в Wireshark

Источник: составлено авторами

Fig. 7. Network package in Wireshark

Source: compiled by the authors

На рисунке 8 представлен фрагмент работы цифрового двойника в процессе постепенного снижения температуры объекта. В консольном выводе отображается последовательное уменьшение реальной температуры при сохранении высокой скорости вентилятора. Одновременно фиксируются

сообщения о несоответствии данных и события повторной передачи пакетов, что указывает на продолжающееся влияние некорректной телеметрии. Данный рисунок иллюстрирует динамику восстановления температурного режима и реакцию цифрового двойника на изменения состояния объекта во времени.

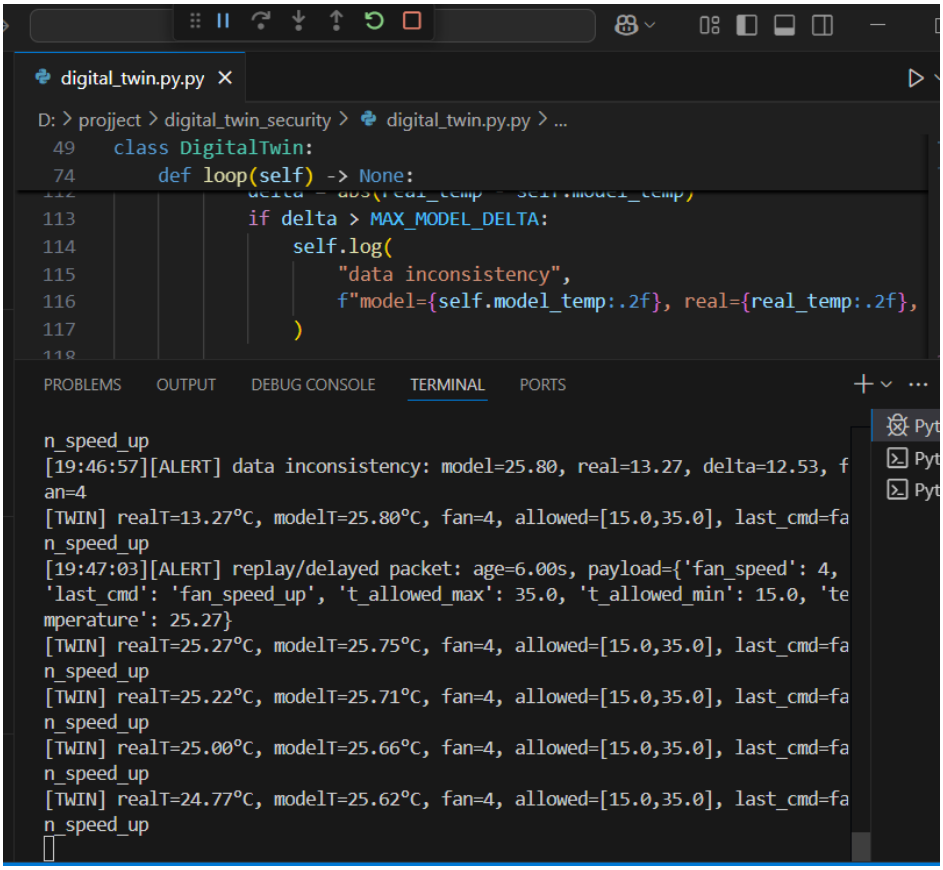

Рис. 8. Фрагмент работы цифрового двойника в процессе постепенного снижения температуры объекта

Источник: составлено авторами

Fig. 8. The fragment of the work of a digital twin in the process of a gradual decrease in the temperature of the object

Source: compiled by the authors

В ходе экспериментальной части были проведены два целенаправленных сценария управления системой охлаждения: искусственное снижение скорости вентилятора с последующим перегревом стойки и увеличение скорости вентилятора до максимального значения с интенсивным охлаждением. Оба сценария показали, что изменение одного управляющего параметра напрямую влияет на температуру внутри стойки и может привести как к аварийному перегреву, так и к нештатному режиму работы оборудования.

Эксперименты продемонстрировали, что при отсутствии механизмов аутентификации и контроля источника команд злоумышленник может отправлять управляющие команды вентилятору, маскируя свои действия под

легитимного оператора. В таком случае цифровой двойник и система управления фиксируют только факт изменения состояния, но не могут однозначно определить, кто именно инициировал данное воздействие. Это создаёт ситуацию, при которой вредоносное управление внешне выглядит как нормальная работа системы.

На основе проведенного исследования и анализа данных о кибератаках на промышленные системы управления можно предложить следующую экономическую модель оценки рисков и затрат на обеспечение информационной безопасности цифровых двойников:

$$NPV = -CAPEX + \sum_{t=1}^{T} \frac{(R_0 - R_1) \cdot L - OPEX}{(1+r)^t},$$

где NPV – показатель экономической эффективности с учетом дисконтирования будущих денежных потоков (чистая приведенная стоимость);

$CAPEX$ – капитальные затраты на внедрение систем безопасности;

$OPEX$ – операционные затраты на поддержание систем безопасности;

R_0 – вероятность успешной кибератаки без системы защиты;

R_1 – вероятность успешной кибератаки с системами защиты;

L – потенциальные потери от успешной кибератаки (включая прямые потери от простоя, затраты на восстановление систем, репутационные потери, юридические последствия);

T – расчетный период оценки;

r – ставка дисконтирования.

Инвестиции в безопасность цифровых двойников являются тем более экономическими обоснованными, чем больше размеры предприятия, в которых потенциальные потери от кибератак значительно превышают затраты на внедрение и поддержание систем.

Заключение

Цифровые двойники существенно повышают эффективность управления сложными техническими системами, обеспечивая прогнозирование состояний, моделирование процессов и сокращение рисков. Однако их применение порождает новые угрозы информационной безопасности, связанные с подменой телеметрии, компрометацией API, атаками на IoT-устройства и использованием цифрового двойника злоумышленниками для подготовки кибератак.

Проведённые эксперименты подтверждают, что злоумышленник может целенаправленно влиять на физическое состояние объекта через управляющие команды, не вызывая немедленного подозрения. Особенно это опасно в системах, где цифровой двойник используется для мониторинга и принятия решений, так как искажение управления может привести к повреждению

оборудования или отказу системы без очевидных признаков атаки. Таким образом, необходимо внедрять механизмы информационной безопасности, такие как аутентификация команд, контроль целостности сообщений, журналирование действий и анализ расхождений между моделью цифрового двойника и фактическим поведением объекта. Без этих мер цифровой двойник может стать уязвимой точкой системы управления, а не инструментом защиты.

Литература

1. Кравченко А.А. Природа, сущность и классификация цифровых двойников // Экономика и управление. 2025. №1. С. 125–134. https://doi.org/10.35854/1998-1627-2025-1-125-134
2. Паршина И.С., Фролов Е.Б. Разработка цифрового двойника производственной системы на базе современных цифровых технологий // Экономика промышленности. 2020. Т. 13. № 1. С. 29–34 https://doi.org/10.17073/2072-1633-2020-1-29-34
3. Гура А.Ю., Жабин М.А., Петухова А.Д. Цифровая личность или цифровой двойник: проблемы существования человека в виртуальном пространстве // Гуманитарный научный вестник. 2025. № 1. С. 199–203. https://doi.org/10.5281/zenodo.14809048
4. Боровков А., Бураков В., Мартынец Е., Рябов Ю., Щербина Л. Цифровая платформа по разработке и применению цифровых двойников (digital twins) CML-BENCH® (часть 1) // САПР и графика. 2023. № 8 (324). С. 42–51.
5. Боровков А., Бураков В. Цифровая платформа по разработке и применению цифровых двойников (digital twins) CML-BENCH® (часть 2) // САПР и графика. 2023. № 9 (325). С. 54–64.
6. Стручалин В.Г., Нарусова Е.Ю. Применение цифрового моделирования и цифровых двойников на этапах жизненного цикла объектов сложных технических систем // Материалы межвузовской научно-практической конференции транспортных вузов «Современные вызовы транспортной отрасли: новые возможности» Санкт-Петербург. М.: Дашков и К, 2025. С. 273–277.
7. Гостева О.В., Пацук О.В. Особенности применения цифровых двойников на российских промышленных предприятиях // Международный научно-исследовательский журнал. 2023. №8 (134). С. 41.
8. Китов В.А., Меденников В.И. Стратегия перехода от цифрового двойника к единой цифровой платформе управления экономикой // Сборник статей XIII Международной научно-практической конференции имени А.И. Китова «Информационные технологии и математические методы в экономике и управлении (ИТиММ-2024)». Москва, 2024. – М.: Изд-во «Российский экономический университет им. Г.В. Плеханова», 2024. – С. 217–224.

9. Хафизов А.М., Борщ И.Д. Общие данные о цифровых двойниках и программных платформах управления цифровыми двойниками // Инновационная наука. 2025. № 5–2. С. 78–79.

10. Лофиченко А.А. Киберсоциофизические системы и сети цифровых двойников: взгляд на будущие экосистемы цифровых двойников // Вестник Луганского государственного университета имени Владимира Даля. 2025. № 2 (92). С. 250–256.

11. Царев М.В., Андреев Ю.С. Цифровые двойники в промышленности: история развития, классификация технологий и сценарии использования // Известия высших учебных заведений. Приборостроение. 2021. № 7. С. 517–531. https://doi.org/10.17586/0021-3454-2021-64-7-517-531

12. Рахманов М.Л., Шишкин А.В. Современные цифровые технологии и цифровой двойник // Качество и жизнь. 2021. № 2 (30). С. 57–59. https://doi.org/10.34214/2312-5209-2021-30-2-57-59

13. Таюрская И.С. Теоретические и практические аспекты создания цифрового двойника организации // Экономика и управление. 2025. № 4. С. 430–441. doi:10.35854/1998-1627-2025-4-430-441

14. Аллакулиев М., Батырова А., Аннабаев С., Атаев А. Цифровые двойники: ключ к цифровой трансформации // Символ науки: международный научный журнал. 2024. Т. 1. № 10–2. С. 40–41.

15. Лычкина Н.Н., Павлов В.В. Концепция цифрового двойника и роль имитационных моделей в архитектуре цифрового двойника // Сборник трудов одиннадцатой всероссийской научно-практической конференции по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика (ИММОД-2023)». Казань, Издательство АН РТ, 2023. С. 139–149.

16. Khan R., Maynard P., McLaughlin K., Laverty D. Sakir Sezer Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid. // Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016. P. 1–11. https://doi.org/10.14236/ewic/ICS2016.7

17. Taiwo Justice Olorunlana, Hamdiya Mohammed (2025) Analysis of the Colonial Pipeline Cybersecurity Incident. International Journal of Science, Architecture, Technology, and Environment. Vol. 02. Iss. 04. https://doi.org/10.63680/jngh0767as

References

1. Kravchenko A.A. Priroda, sushchnost’ i klassifikatsiya tsifrovykh dvoinikov [Nature, Essence and Classification of Digital Twins]. Ekonomika i upravlenie [Economics and Management]. 2025;(1):125–134. https://doi.org/10.35854/1998-1627-2025-1-125-134. (In Russ., abstract in Eng.).

2. Parshina I.S., Frolov E.B. Razrabotka tsifrovogo dvoinika proizvodstvennoi sistemy na baze sovremennykh tsifrovykh tekhnologii [Development of a Digital Twin of a Production System Based on Modern Digital Technologies]. Ekonomika promyshlennosti [Russian Journal of Industrial Economics]. 2020;13(1):29–34. https://doi.org/10.17073/2072-1633-2020-1-29-34. (In Russ., abstract in Eng.).

3. Gura A.Yu., Zhabin M.A., Petukhova A.D. Tsifrovaya lichnost’ ili tsifrovoi dvoinik: problemy sushchestvovaniya cheloveka v virtual’nom prostranstve [Digital Personality or Digital Twin: Problems of Human Existence in Virtual Space]. Gumanitarnyi nauchnyi vestnik [Humanitarian Scientific Bulletin]. 2025;(1):199–203. https://doi.org/10.5281/zenodo.14809048. (In Russ.).

4. Borovkov A., Burakov V., Martynets E., Ryabov Yu., Shcherbina L. Tsifrovaya platforma po razrabotke i primeneniyu tsifrovykh dvoinikov (digital twins) CML-BENCH® (chast’ 1) [Digital Platform for the Development and Application of Digital Twins CML-BENCH® (Part 1)]. SAPR i grafika [CAD & Graphics]. 2023;(8(324)):42–51. (In Russ.).

5. Borovkov A., Burakov V. Tsifrovaya platforma po razrabotke i primeneniyu tsifrovykh dvoinikov (digital twins) CML-BENCH® (chast’ 2) [Digital Platform for the Development and Application of Digital Twins CML-BENCH® (Part 2)]. SAPR i grafika [CAD & Graphics]. 2023;(9(325)):54–64. (In Russ.).

6. Struchalin V.G., Narusova E.Yu. Primenenie tsifrovogo modelirovaniya i tsifrovykh dvoinikov na etapakh zhiznennogo tsikla ob’’ektov slozhnykh tekhnicheskikh sistem [Application of Digital Modeling and Digital Twins at the Life-Cycle Stages of Complex Technical Systems]. In: Materialy mezhvuzovskoi nauchno-prakticheskoi konferentsii transportnykh vuzov “Sovremennye vyzovy transportnoi otrasli: novye vozmozhnosti” [Proceedings of the Interuniversity Scientific and Practical Conference of Transport Universities “Modern Challenges of the Transport Industry: New Opportunities”]. Saint Petersburg. Moscow: Dashkov i K; 2025. P. 273–277. (In Russ.).

7. Gosteva O.V., Patsuk O.V. Osobennosti primeneniya tsifrovykh dvoinikov na rossiiskikh promyshlennykh predpriyatiyakh [Features of the Application of Digital Twins at Russian Industrial Enterprises]. Mezhdunarodnyi nauchno-issledovatel’skii zhurnal [International Research Journal]. 2023;(8(134)):41. (In Russ., abstract in Eng.).

8. Kitov V.A., Medennikov V.I. Strategiya perekhoda ot tsifrovogo dvoinika k edinoi tsifrovoi platforme upravleniya ekonomikoi [Strategy for Transition from a Digital Twin to a Unified Digital Platform for Economic

Management]. In: Sbornik statei XIII Mezhdunarodnoi nauchno-prakticheskoi konferentsii imeni A.I. Kitova “Informatsionnye tekhnologii i matematicheskie metody v ekonomike i upravlenii (ITiMM-2024)” [Proceedings of the XIII International Scientific and Practical Conference named after A.I. Kitov “Information Technologies and Mathematical Methods in Economics and Management (ITiMM-2024)”]. Moscow: Plekhanov Russian University of Economics; 2024. P. 217–224. (In Russ.).

9. Khafizov A.M., Borshch I.D. Obshchie dannye o tsifrovykh dvoinikakh i programmnykh platformakh upravleniya tsifrovymi dvoinikami [General Information about Digital Twins and Software Platforms for Digital Twin Management]. Innovatsionnaya nauka [Innovative Science]. 2025;(5-2):78–79. (In Russ., abstract in Eng.).

10. Lofichenko A.A. Kibersotsiophizicheskie sistemy i seti tsifrovykh dvoinikov: vzglyad na budushchie ekosistemy tsifrovykh dvoinikov [Cyber-Socio-Physical Systems and Digital Twin Networks: A View on Future Digital Twin Ecosystems]. Vestnik Luganskogo gosudarstvennogo universiteta imeni Vladimira Dalya [Bulletin of Lugansk State University named after Vladimir Dal]. 2025;(2(92)):250–256. (In Russ.).

11. Tsarev M.V., Andreev Yu.S. Tsifrovye dvoiniki v promyshlennosti: istoriya razvitiya, klassifikatsiya tekhnologii i stsenarii ispol’zovaniya [Digital Twins in Industry: Development History, Technology Classification and Use Scenarios]. Izvestiya vysshikh uchebnykh zavedenii. Priborostroenie [Journal of Instrument Engineering]. 2021;(7):517–531. https://doi.org/10.17586/0021-3454-2021-64-7-517-531. (In Russ., abstract in Eng.).

12. Rakhmanov M.L., Shishkin A.V. Sovremennye tsifrovye tekhnologii i tsifrovoi dvoinik [Modern Digital Technologies and the Digital Twin]. Kachestvo i zhizn’ [Quality and Life]. 2021;(2(30)):57–59. https://doi.org/10.34214/2312-5209-2021-30-2-57-59. (In Russ., abstract in Eng.).

13. Tayurskaya I.S. Teoreticheskie i prakticheskie aspekty sozdaniya tsifrovogo dvoinika organizatsii [Theoretical and Practical Aspects of Creating a Digital Twin of an Organization]. Ekonomika i upravlenie [Economics and Management]. 2025;(4):430–441. https://doi.org/10.35854/1998-1627-2025-4-430-441. (In Russ., abstract in Eng.).

14. Allakuliev M., Batyrova A., Annabaev S., Ataev A. Tsifrovye dvoiniki: klyuch k tsifrovoi transformatsii [Digital Twins: The Key to Digital Transformation]. Simvol nauki: mezhdunarodnyi nauchnyi zhurnal [Symbol of Science: International Scientific Journal]. 2024;1(10-2):40–41. (In Russ.).

15. Lychkina N.N., Pavlov V.V. Kontseptsiya tsifrovogo dvoinika i rol’ imitatsionnykh modelei v arkhitekture tsifrovogo dvoinika [The Concept of a Digital Twin and the Role of Simulation Models in Digital Twin Architecture]. In: Sbornik trudov odinnadtsatoi Vserossiiskoi nauchno-prakticheskoi konferentsii po imitatsionnomu modelirovaniyu i ego primeneniyu v nauke i promyshlennosti “Imitatsionnoe modelirovanie. Teoriya i praktika (IMMOD-2023)” [Proceedings of

the 11th All-Russian Scientific and Practical Conference on Simulation Modeling and Its Application in Science and Industry “Simulation Modeling. Theory and Practice (IMMOD-2023)”]. Kazan: Publishing House of the Academy of Sciences of the Republic of Tatarstan; 2023. P. 139–149. (In Russ.).

16. Khan R., Maynard P., McLaughlin K., Laverty D., Sezer S. Threat analysis of BlackEnergy malware for synchrophasor-based real-time control and monitoring in smart grid. In: Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research; 2016. P. 1–11. https://doi.org/10.14236/ewic/ICS2016.7. (In Eng.).

17. Olorunlana T.J., Mohammed H. Analysis of the Colonial Pipeline cybersecurity incident. International Journal of Science, Architecture, Technology, and Environment. 2025;2(4). https://doi.org/10.63680/jngh0767as. (In Eng.).