

УДК 004.056.53
<https://doi.org/10.32362/2500-316X-2026-14-5-41-54>
EDN XGETAP



НАУЧНАЯ СТАТЬЯ

Адаптивный анализ угроз информационной безопасности на киберфизическом стенде с использованием цифрового двойника автоматизированной системы управления технологическими процессами энергообъекта

О.В. Трубиенко ¹, Е.С. Митяков ^{1, @}, А.А. Лоскутов ², А.Л. Куликов ²

¹ МИРЭА – Российский технологический университет, Москва, 119454 Россия

² Нижегородский государственный технический университет им. Р.Е. Алексеева, Нижний Новгород, 603155 Россия

@ Автор для переписки, e-mail: mityakov@mirea.ru

• Поступила: 10.03.2026 • Доработана: 11.05.2026 • Принята к опубликованию: 13.07.2026

Резюме

Цели. Основной целью исследования является экспериментальная верификация предложенного подхода к адаптивному анализу угроз информационной безопасности на объектах критической информационной инфраструктуры с использованием цифрового двойника автоматизированной системы управления технологическими процессами (АСУ ТП) энергообъекта.

Методы. В работе применен системный подход, включающий моделирование типовых сценариев угроз на полунатурном киберфизическом стенде, генерацию синтетических многомерных временных рядов телеметрии в цифровом двойнике и итеративное дообучение модели обнаружения угроз на основе ансамблевого алгоритма Random Forest¹. Сравнение выполнено между стратегией прямого дообучения на данных стенда и стратегией, полностью основанной на синтетических данных, сгенерированных цифровым двойником. Эффективность оценивалась с учетом как результативности обнаружения угроз, так и уровня защищенности эксплуатационной среды. Для количественной оценки использовалась авторская метрика, учитывающая компромисс между полнотой обнаружения и рисками вмешательства в работу реального оборудования.

Результаты. Экспериментально подтверждена работоспособность предложенного подхода: использование цифрового двойника обеспечивает качество обнаружения угроз, сопоставимое с прямым дообучением на реальном оборудовании, при существенно более высоком уровне защищенности. На основе анализа смоделированных атак в цифровом двойнике сформулированы и верифицированы две защитные меры

¹ Random Forest (случайный лес) – алгоритм машинного обучения, который использует ансамбль решающих деревьев для повышения точности предсказаний. [Machine-learning algorithm that uses an ensemble of decision trees to improve the accuracy of predictions.]

на уровне прикладной логики АСУ ТП: корреляционное правило в SCADA-системе² для проверки логической согласованности телеметрии и адаптивный пороговый контроль, учитывающий текущий режим работы энергообъекта. Их внедрение позволило повысить точность обнаружения при сохранении полноты и дополнительно усилить защищенность системы. Проведенная серия из ста независимых экспериментов подтвердила статистическую значимость полученных результатов. Разработанные защитные меры продемонстрировали устойчивость к различным режимам функционирования энергообъекта.

Выводы. Предложенный подход позволяет осуществлять адаптивный анализ угроз информационной безопасности без прямого взаимодействия с реальным оборудованием, что соответствует требованиям функциональной безопасности и нормативным ограничениям, действующим в отношении объектов критической информационной инфраструктуры.

Ключевые слова: автоматизированная система управления технологическими процессами, критическая информационная инфраструктура, цифровой двойник, адаптивный анализ угроз, обнаружение атак, машинное обучение, телеметрия, функциональная безопасность, защитные меры, киберфизический стенд

Для цитирования: Трубиенко О.В., Митяков Е.С., Лоскутов А.А., Куликов А.Л. Адаптивный анализ угроз информационной безопасности на киберфизическом стенде с использованием цифрового двойника автоматизированной системы управления технологическими процессами энергообъекта. *Russian Technological Journal*. 2026;14(5):41–54. <https://doi.org/10.32362/2500-316X-2026-14-5-41-54>, <https://elibrary.ru/XGETAP>

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

RESEARCH ARTICLE

Adaptive analysis of information security threats on a cyber-physical testbed using a digital twin of an energy facility automated process control system

Oleg V. Trubienko ¹, Evgeny S. Mityakov ^{1, @}, Anton A. Loskutov ²,
Aleksandr L. Kulikov ²

¹ MIREA – Russian Technological University, Moscow, 119454 Russia

² R.E. Alekseev Nizhny Novgorod State Technical University, Nizhny Novgorod, 603155 Russia

@ Corresponding author, e-mail: mityakov@mirea.ru

• Submitted: 10.03.2026 • Revised: 11.05.2026 • Accepted: 13.07.2026

Abstract

Objectives. The study set out to experimentally verify a proposed approach to adaptive cyber threat analysis for critical information infrastructure facilities using a digital twin of an industrial control system (ICS) for a power facility.

² Supervisory Control and Data Acquisition – система надзора и сбора данных – комплекс программно-аппаратных средств для мониторинга и управления промышленными или инженерными объектами в реальном времени. [Supervisory Control and Data Acquisition (SCADA) is a system for supervising and collecting data, comprising a set of software and hardware tools for monitoring and managing industrial or engineering facilities in real time.]

Methods. The system-engineering approach involved modeling representative cyber-attack scenarios on a semi-natural cyber-physical testbed and generating synthetic multivariate time series telemetry within a digital twin. The threat detection model was then iteratively retrained based on the Random Forest³ ensemble algorithm. Strategies involving direct retraining on testbed data were compared with those relying solely on synthetic data generated by the digital twin. The evaluation criteria encompassed both the effectiveness of threat detection and the level of operational environment security. The authors' proprietary metric, which considers the trade-off between threat detection recall and the risk of interfering with the real equipment operations, was used for quantitative assessment.

Results. The feasibility of the proposed approach was experimentally confirmed. The use of a digital twin provides a level of threat detection quality comparable to direct retraining on physical equipment while ensuring a substantially higher level of operational security. Based on the analysis of simulated attacks within the digital twin, two defensive measures were formulated and verified at the application logic level of the ICS: (1) a correlation rule for the SCADA⁴ system to validate the logical consistency of telemetry and (2) an adaptive multi-threshold control mechanism that accounts for the current operational mode of the power facility. Implementing these measures improved detection precision while maintaining recall to further enhance the system's overall security. A series of a hundred independent experiments confirmed the statistical significance of the obtained results. The protective measures developed demonstrated resilience to various operating modes of the considered energy facility.

Conclusions. The proposed approach is suitable for carrying out adaptive cyber threat analysis without direct interaction with physical equipment, thereby complying with functional safety requirements and regulatory constraints applicable to critical information infrastructure facilities in the Russian Federation.

Keywords: automated process control system, critical information infrastructure, digital twin, adaptive threat analysis, attack detection, machine learning, telemetry, functional safety, security measures, cyber-physical testbed

For citation: Trubienko O.V., Mityakov E.S., Loskutov A.A., Kulikov A.L. Adaptive analysis of information security threats on a cyber-physical testbed using a digital twin of an energy facility automated process control system. *Russian Technological Journal*. 2026;14(5):41–54. <https://doi.org/10.32362/2500-316X-2026-14-5-41-54>, <https://elibrary.ru/XGETAP>

Financial disclosure: The authors have no financial or proprietary interest in any material or method mentioned.

The authors declare no conflicts of interest.

ВВЕДЕНИЕ

Адаптивный анализ угроз информационной безопасности (ИБ) объектов критической информационной инфраструктуры (КИИ) представляет собой процесс выявления и оценки потенциальных нарушений, при котором механизмы защиты способны корректироваться в ответ на изменения технологического процесса, конфигурации системы или актуализацию угроз ИБ. В отличие от традиционных методов, основанных на статическом анализе сетевого трафика, фиксированных порогах или сигнатурном подходе, адаптивные методы направлены на повышение защищенности за счет учета динамики функционирования реального объекта [1, 2].

Автоматизированные системы управления технологическими процессами (АСУ ТП) энергообъектов подвержены угрозам ИБ, реализация которых

способна привести к нарушению технологических режимов, отказу оборудования или искажению данных оперативного контроля. При этом особенности эксплуатации объектов КИИ – требования к непрерывности работы и запрет на несанкционированное вмешательство – существенно ограничивают применение методов, требующих обучения на реальных инцидентах или активного тестирования в рабочей среде [3]. Действующие нормативные документы Российской Федерации не содержат методических подходов к адаптации систем обнаружения угроз ИБ в условиях отсутствия размеченных данных и невозможности испытаний на реальном оборудовании. Модель угроз, разрабатываемая для объекта КИИ в соответствии с методикой ФСТЭК России⁵, определяет актуальные способы реализации угроз, но не регламентирует механизмы ее непрерывного обновления в ходе эксплуатации⁶.

³ Machine-learning algorithm that uses an ensemble of decision trees to improve the accuracy of predictions.

⁴ Supervisory Control and Data Acquisition (SCADA) is a system for supervising and collecting data, comprising a set of software and hardware tools for monitoring and managing industrial or engineering facilities in real time.

⁵ Федеральная служба по техническому и экспортному контролю. <https://fstec.ru/>. Дата обращения 14.02.2026. [Federal Service for Technical and Export Control. <https://fstec.ru/> (in Russ.). Accessed February 14, 2026.]

⁶ Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. от 28.08.2024). <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239>. Дата обращения 14.02.2026. [Order No. 239 of the FSTEC of Russia, dated December 25, 2017, “On the approval of requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation” (as amended on August 28, 2024). <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239> (in Russ.). Accessed February 14, 2026.]

В соответствии с методическим документом ФСТЭК России от 05.02.2021 «Методика оценки угроз безопасности информации»⁷ модель угроз для АСУ ТП энергообъекта строится на трех взаимосвязанных компонентах:

- источники угроз (внешние атаки через каналы связи с диспетчерскими уровнями, действия персонала, подрядчиков и вендоров);
- уязвимости информационной системы (отсутствие аутентификации в промышленных протоколах, стандартные учетные данные, недостаточная сегментация сети);
- критичность защищаемых активов (технологический процесс передачи и распределения электроэнергии, целостность параметров телеметрии, корректность функционирования релейной защиты и автоматики).

Ключевыми угрозами для рассматриваемого класса объектов выступают внедрение ложных данных в каналы телеметрии, отказ в обслуживании устройств сбора данных, несанкционированное изменение конфигурационных параметров, а также ошибки персонала. Особую опасность представляют угрозы, нарушающие целостность телеметрии при сохранении доступности: такие воздействия маскируются под штатные переходные процессы и способны приводить к ошибочным решениям оператора либо ложным срабатываниям автоматики.

Федеральный закон № 187-ФЗ⁸ предписывает обеспечение безопасности объектов КИИ, но требует проведения соответствующих мероприятий без нарушения технологического процесса. Прямое тестирование защитных мер на действующем энергооборудовании исключено из-за рисков отказа оборудования и нарушения электроснабжения. Данное обстоятельство обосновывает необходимость применения изолированных сред (например, цифровых двойников (ЦД) и киберфизических стендов) для безопасной проверки средств обнаружения угроз

и обработки сценариев реагирования на компьютерные атаки.

В настоящей статье представлены результаты экспериментальной апробации подхода к адаптивному анализу угроз ИБ, выполненной на киберфизическом стенде лаборатории «Цифровое моделирование электроэнергетических систем в реальном времени». Цель работы – демонстрация возможности повышения защищенности АСУ ТП энергообъекта посредством использования изолированной среды для формирования и оценки адаптивных моделей обнаружения без взаимодействия с действующей инфраструктурой.

Отметим, что данное исследование представляет собой первый этап устойчивого научного взаимодействия между московской и нижегородской школами в области кибербезопасности промышленных и энергетических систем. Интеграция компетенций РТУ МИРЭА⁹ в области ЦД и анализа угроз ИБ с экспертизой НГТУ им. Р.Е. Алексеева¹⁰ в области релейной защиты и функционирования энергетических систем создает основу для формирования единой методологии адаптивной защиты объектов КИИ, соответствующей требованиям технологического суверенитета Российской Федерации [4–6].

СОСТОЯНИЕ ПРОБЛЕМЫ ИССЛЕДОВАНИЯ

Современные системы обнаружения угроз ИБ, применяемые на объектах КИИ, включая объекты АСУ ТП в энергетике, все чаще сталкиваются с фундаментальными ограничениями статических и неадаптивных подходов. Такие решения, основанные на сигнатурном анализе, жестких порогах или моделях машинного обучения, обученных на фиксированных наборах данных, быстро теряют актуальность в условиях динамически эволюционирующих тактик злоумышленников и изменяющихся режимов функционирования объектов [7, 8].

Одним из существенных недостатков статических механизмов обнаружения угроз ИБ является их ограниченная способность к обобщению за пределами условий, заданных в обучающей выборке. Модели, обученные на данных, характерных для конкретных протоколов, сетевых топологий или известных типов атак, демонстрируют значимое снижение

⁷ Методика оценки угроз безопасности информации: метод. документ ФСТЭК России от 05.02.2021. <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g>. Дата обращения 14.02.2026. [Methodology for assessing information security threats: Method document of the FSTEC of Russia, dated February 05, 2021. <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g> (in Russ.). Accessed February 14, 2026.]

⁸ Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». <https://fstec.ru/dokumenty/vse-dokumenty/zakony/federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz>. Дата обращения 14.02.2026. [Federal Law No. 187-FZ of July 26, 2017, “On the Security of the Critical Information Infrastructure of the Russian Federation.” <https://fstec.ru/dokumenty/vse-dokumenty/zakony/federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz> (in Russ.). Accessed February 14, 2026.]

⁹ МИРЭА – Российский технологический университет. <https://www.mirea.ru/>. Дата обращения 10.07.2026. [MIREA – Russian Technological University. <https://www.mirea.ru/> (in Russ.). Accessed July 10, 2026.]

¹⁰ Нижегородский государственный технический университет им. Р.Е. Алексеева. <https://www.ntnu.ru/>. Дата обращения 10.07.2026. [R.E. Alekseev Nizhny Novgorod State Technical University. <https://www.ntnu.ru/> (in Russ.). Accessed July 10, 2026.]

эффективности при переносе в новые операционные среды или при столкновении с ранее неизвестными угрозами [9, 10]. Данное ограничение приобретает особую значимость в промышленных системах управления, где высокое разнообразие архитектурных решений, наличие унаследованных компонентов и различия в отраслевых стандартах затрудняют разработку универсальных и масштабируемых решений.

Дополнительную проблему представляет высокий уровень ложных срабатываний систем обнаружения угроз ИБ, обусловленный недостаточным учетом физического состояния технологического процесса [11]. Интеграция разнородных данных телеметрии без адекватной контекстуализации нередко приводит к ошибочной интерпретации штатных переходных режимов как аномальных событий. Это создает избыточную операционную нагрузку на персонал и снижает доверие к системе в целом [8, 12].

Следующее ограничение обусловлено эксплуатационными особенностями промышленных систем. Непрерывный характер технологических процессов, строгие требования к функциональной безопасности и длительные циклы валидации затрудняют регулярное обновление и дообучение моделей обнаружения угроз. Прямое тестирование и адаптация таких моделей на реальных объектах КИИ представляют собой технически сложную задачу и сопряжены со значительными экономическими и операционными рисками [7, 13].

Цифровой двойник объекта КИИ может рассматриваться в качестве инструмента, позволяющего преодолеть существующие барьеры. Он обеспечивает создание виртуальной реплики объекта защиты, в которой допустимы безопасное моделирование сценариев кибератак, генерация синтетических многомерных временных рядов телеметрии, имитирующих как нормальное функционирование, так и проявления угроз ИБ, а также итеративное дообучение моделей обнаружения без нарушения работы реального объекта [14, 15]. Результаты ряда исследований свидетельствуют о том, что применение ЦД способствует существенному повышению качества обнаружения угроз и одновременному снижению уровня ложных срабатываний [16, 17]. Например, в работе [16], посвященной применению ЦД для обнаружения киберугроз в системах управления водочистными сооружениями, показано, что интеграция физической модели технологического процесса и методов машинного обучения обеспечивает значение F1-меры¹¹ до 0.96 при уровне ложных срабатываний

менее 2.5%. Другие исследования подтверждают, что итеративное дообучение моделей обнаружения угроз на синтетических данных, генерируемых ЦД, обеспечивает эффективное выявление атак, маскирующихся под штатные переходные режимы технологического процесса [18, 19].

Тем не менее, существующие решения в основном носят концептуальный или прототипный характер и ограничиваются либо моделированием физических процессов, либо обнаружением аномалий без формализованной процедуры адаптации защитных моделей [20, 21]. Особенно остро ощущается дефицит количественных экспериментальных исследований, проведенных на полунатурных киберфизических стендах, которые бы воспроизводили реальные условия функционирования энергообъектов с использованием промышленного оборудования [22, 23]. Кроме того, остаются недостаточно изученными вопросы интеграции ЦД в процесс повышения защищенности объектов КИИ, включающий генерацию синтетических данных, оценку эффективности защитных мер и снижение зависимости от данных реальных инцидентов [24, 25]. Отсутствие единых методологий и метрик, учитывающих результативность обнаружения угроз и эксплуатационные ограничения КИИ, дополнительно затрудняет сравнение и внедрение таких решений [26, 27].

Таким образом, несмотря на очевидный потенциал ЦД, научное сообщество сталкивается с необходимостью разработки и экспериментальной верификации подхода к адаптивному анализу угроз ИБ, который был бы реализуем на киберфизических стендах, соответствовал требованиям и условиям промышленной эксплуатации и обеспечивал бы измеримое повышение уровня защищенности объектов КИИ.

ОПИСАНИЕ ЛАБОРАТОРНОГО ОБОРУДОВАНИЯ

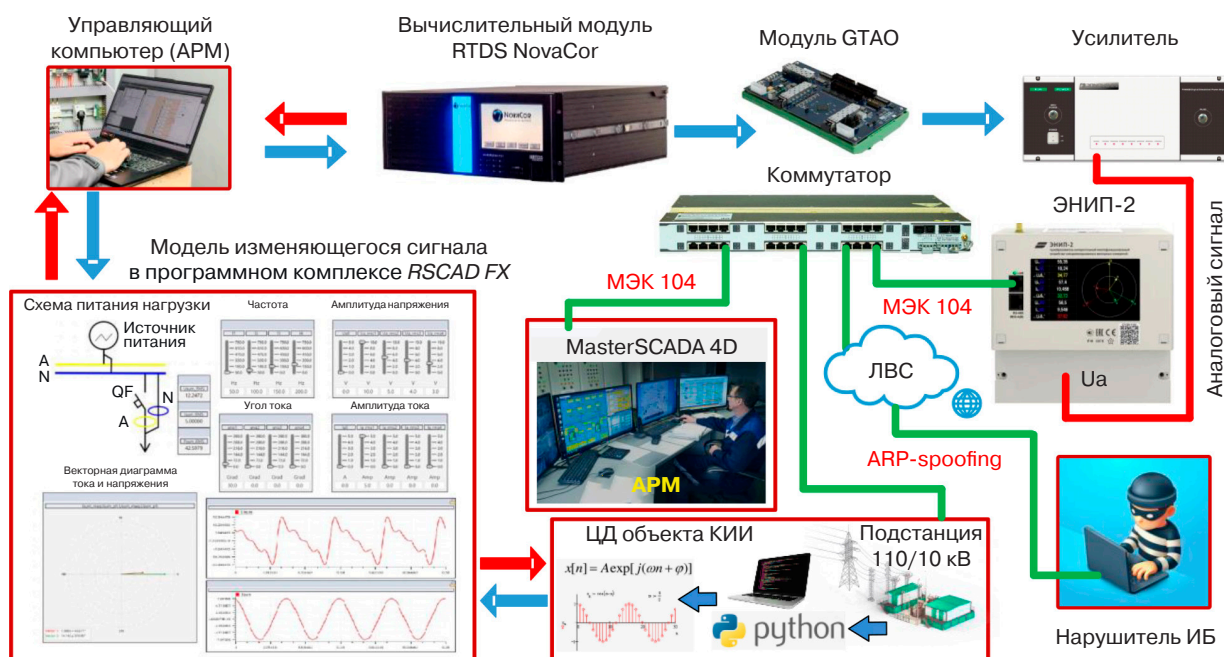
Экспериментальная база включает киберфизический стенд на базе программно-аппаратного комплекса реального времени (real-time digital simulator, RTDS) NovaCor¹² (Канада), который включает в себя программную часть в виде прикладного программного комплекса для моделирования *RSCAD FX* и аппаратную часть в составе: вычислительного модуля (Rack) NovaCor, модуля аналоговых выходов GTAO (gigabit-transceiver analogue output), комбинированного усилителя PA460Bi (производитель – PONOVO, Китай) и вспомогательного

¹¹ Метрика оценки качества моделей классификации, которая представляет собой гармоническое среднее между точностью (Precision) и полнотой (Recall). [F1 score is a metric for evaluating the quality of classification models, calculated as the harmonic mean of precision and recall.]

¹² <https://www.nntu.ru/structure/view/podrazdeleniya/nil-cmes> (in Russ.). Дата обращения 10.07.2026. / Accessed July 10, 2026.

Передача данных (измерений) происходит в SCADA-систему (MasterSCADA 4D¹⁴), осуществляющую мониторинг технологического процесса

В дополнение к имитационной RSCAD-модели в стенд интегрирован ЦД энергообъекта, формирующий выдаваемые сигналы в ЛБС с помощью скрипта на языке Python, позволяя запустить циклическую процедуру реализации искажений сигналов. Комбинация ЦД и RSCAD-модели позволяет запустить процедуры обучения, тестирования, дообучения модели обнаружения угроз, а также адаптацию алгоритма в процессе имитации реальной эксплуатации. Цифровой двойник получает телеметрические данные от стенда в реальном времени, а также может передавать сгенерированные синтетические данные обратно в стенд для тестирования алгоритмов обнаружения угроз (рис. 1).



ARP-spoofing – сетевая атака, которая использует уязвимости протокола ARP (Address Resolution Protocol, протокол разрешения адресов). U_a – канал напряжения, $x(n)$ – значение сигнала в момент времени n , A – амплитуда сигнала, ω_n – частота, φ – начальная фаза. Обозначения элементов схемы здесь и далее соответствуют обозначениям, принятым в ГОСТ 2.710-81¹⁵

¹⁵ ГОСТ 2.710-81. Межгосударственный стандарт. *Единая система конструкторской документации. Обозначения буквенно-цифровые в электрических схемах*. М.: Издательство стандартов; 1985. [GOST 2.710-81. Interstate Standard. *Unified system for design documentation. Alpha-numerical designations in electrical diagrams*. Moscow: Izd. Standartov; 1985 (in Russ.).]



Рис. 2. Внешний вид киберфизического стенда

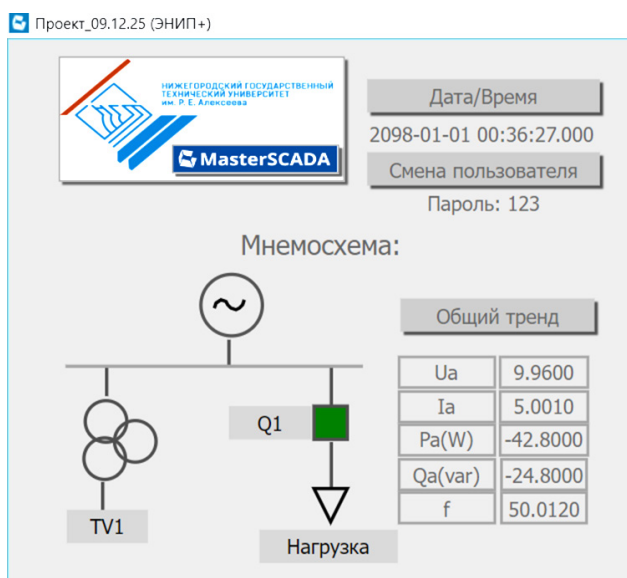


Рис. 3. Рабочее окно диспетчера в MasterSCADA 4D

В стенде возможна имитация кибератаки злоумышленником в виде подмены данных телеметрии (MITM¹⁶-атака) через ARP-spoofing. Состав стенда, а также поддержка известных промышленных протоколов (IEC 61850 (GOOSE/SV)¹⁷, DNP3¹⁸, Modbus¹⁹, IEC 104 и др.), делает его уникаль-

¹⁶ Man-in-the-Middle (человек посередине) – кибератака, при которой злоумышленник перехватывает и потенциально изменяет коммуникацию между двумя сторонами. [A man-in-the-middle attack is when an attacker intercepts and potentially alters communication between two parties.]

¹⁷ https://www.rosseti.ru/upload/iblock/d1c/xp3uhk4fqbwckdcon4b7yaf4t6coi53l/CTO_56947007-25.040.30.309-2020изм1.pdf (in Russ.). Дата обращения 10.07.2026. / Accessed July 10, 2026.

¹⁸ <https://www.dnp.org/About/Overview-of-DNP3-Protocol>. Дата обращения 10.07.2026. / Accessed July 10, 2026.

¹⁹ <https://www.modbus.org/modbus-specifications>. Дата обращения 10.07.2026. / Accessed July 10, 2026.

ным, обеспечивая высокую степень приближения к реальным условиям эксплуатации объектов КИИ.

Стенд поддерживает следующие функции:

- генерацию одномерной и многомерной телеметрии технологических параметров (ток, напряжение, мощность) с контролируемыми шумами и дрейфом;
- имитацию воздействий, соответствующих типовым сценариям угроз ИБ (внедрение ложных данных (MITM), DoS²⁰-воздействия, подмена команд, скрытые смещения сигналов);
- динамическую модификацию статистических свойств телеметрического потока для моделирования переходов между режимами работы (например, дневной/ночной график нагрузки);
- сбор и вычисление метрик эффективности систем обнаружения угроз ИБ;
- реализацию многокритериальной оценки защищенности;
- фиксацию параметров каждого экспериментального запуска и логирование промежуточных результатов.

МЕТОДИКА И РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТА

Экспериментальное исследование проводилось на киберфизическом стенде с использованием ЦД, интегрированного в программную среду RSCAD FX и синхронизированного с программно-аналитическим комплексом RTDS. Цель эксперимента – оценить эффективность адаптивного подхода к обнаружению угроз ИБ с применением ЦД. Основное внимание уделено проверке гипотезы о том, что использование ЦД в комбинации с RSCAD-моделью энергообъекта реального времени позволяет исключить необходимость дообучения моделей на данных реального объекта КИИ, сохраняя высокое качество обнаружения угроз и соблюдая ограничения, накладываемые требованиями функциональной безопасности и непрерывности эксплуатации.

Общий объем серии экспериментов составил 100 независимых запусков. Методика исследования включала четыре этапа.

Этап 1. Подготовительный

На данном этапе разворачивалась конфигурация киберфизического стенда и инициализировался ЦД АСУ ТП, синхронизированный с RTDS NovaCor. На основе телеметрии, зарегистрированной в условиях штатного (нормального) режима функционирования стенда, осуществлялось

²⁰ Denial-of-service attack (отказ в обслуживании) – хакерская атака на вычислительную систему с целью довести ее до отказа. [A denial-of-service attack (DoS) is an attack on a computer system by hackers, intended to cause it to fail.]

обучение базовой модели обнаружения угроз ИБ, построенной с использованием ансамблевого алгоритма Random Forest²¹. Выбор данного алгоритма обусловлен его устойчивостью к шуму, способностью выявлять нелинейные зависимости между параметрами технологического процесса и обеспечивать интерпретируемость принятых решений.

Для формирования признаков описания применялся метод скользящего окна длиной 40 отсчетов (40 мс при частоте дискретизации 1 кГц). Каждое окно преобразовывалось в 17-мерный вектор признаков, включающий:

- статистические характеристики (среднее, стандартное отклонение, медиана, межквартильный размах, медианное абсолютное отклонение);
- разностные показатели (изменения за 1, 5 и 10 отсчетов);
- автокорреляционные коэффициенты (лаги 1 и 5);
- спектральные дескрипторы (энергия низкочастотных и высокочастотных компонент, их отношение);
- локальные статистики (локальное стандартное отклонение, z-оценка, коэффициент линейного тренда).

Такой набор признаков позволяет учитывать стационарные свойства сигнала и его динамические особенности, характерные для переходных процессов и аномальных воздействий. Обучающая выборка формировалась из данных штатного режима с последующим синтезом аномальных примеров путем инъекции контролируемых отклонений, имитирующих типовые сценарии угроз ИБ. Для устранения дисбаланса классов в алгоритме обучения применялась стратегия взвешивания, что позволило избежать смещения модели в сторону преобладающего класса нормального функционирования без искусственного дублирования примеров. Базовая модель обучалась единожды и служила отправной точкой для последующих стратегий адаптации.

Одновременно формировалась унифицированная методологическая основа для сравнения стратегий обнаружения угроз. Для всех подходов использовались идентичные процедуры формирования обучающих и тестовых выборок, а также единый набор оценочных метрик. Различия между стратегиями заключались исключительно в механизме адаптации модели в ходе тестового периода.

В рамках исследования были рассмотрены две стратегии:

- стратегия А – дообучение модели на реальных фрагментах данных из тестового периода, в которых были выявлены ложнопущенные

срабатывания, с последующим повторным обучением модели;

- стратегия В – выявленные ложнопущенные случаи используются для генерации синтетических примеров угроз в виртуальной среде ЦД; полученные данные интегрируются в обучающую выборку и применяются для адаптивного дообучения модели без прямого вмешательства в работу стенда.

Под *операциями адаптации* в настоящей работе понимается процесс формирования обучающих примеров (аномальных и нормальных) и их использование для итеративного дообучения модели обнаружения угроз. Объем операций адаптации V измеряется количеством таких обучающих примеров. Обозначим V_{real} – число примеров, полученных непосредственно из телеметрии стенда, на основе RSCAD-модели, а V_{DT} – число синтетических примеров, сгенерированных в среде ЦД. Для стратегии А весь объем операций адаптации V_{total} выполняется непосредственно на реальном оборудовании ($V_{\text{real}} = V_{\text{total}}$, $V_{\text{DT}} = 0$). В случае стратегии В адаптация осуществляется полностью в виртуальной среде $V_{\text{real}} = 0$, $V_{\text{DT}} = V_{\text{total}}$.

Этап 2. Проведение экспериментальной серии

Телеметрия формировалась как временной ряд, отражающий поведение параметров электрической сети, с базовым колебательным компонентом (50 Гц и гармоники), аддитивным авторегрессионным шумом и переменной дисперсией. Угрозы ИБ моделировались как контролируемые отклонения сигнала (тока и/или напряжения) в RSCAD-модели и ЦД, внедряемые в IEC 104-трафик.

Для воспроизведения динамики электрической сети использовалась комбинированная модель сигнала $S(t)$, включающая детерминированную $S_d(t)$ и стохастическую $\varepsilon(t)$ компоненты:

$$S(t) = S_d(t) + \varepsilon(t). \quad (1)$$

Детерминированная компонента описывается соотношением:

$$S_d(t) = A_0 + \sum_{k=1}^n A_k \sin(\omega_k t + \varphi_k), \quad (2)$$

где составляющие включают постоянную составляющую A_0 сигнала и n гармонических компонент (k – номер гармонической составляющей), кратных первой гармонике 50 Гц ($k = 1$), с амплитудами A_k (в амперах или вольтах), частотами $\omega_k = 2\pi \cdot 50k$ (рад/с) и фазовыми сдвигами φ_k (рад), моделирующих различные типы колебаний в энергосистеме, обусловленные спецификой электрической нагрузки.

Значения параметров сигнала были выбраны эмпирически: $A_0 = 0.5$, $A_1 = 10.0$ ($\omega_1 = 314$, $\varphi_1 = 0$),

²¹ Random Forest (случайный лес) – алгоритм машинного обучения, который использует ансамбль решающих деревьев для повышения точности предсказаний. [Random Forest is a machine learning algorithm which uses an ensemble of decision trees to improve the accuracy of predictions.]

$A_2 = 0.8$ ($\omega_2 = 682$, $\varphi_2 = \pi/4$, $A_3 = 3.0$ ($\omega_3 = 942$, $\varphi_3 = 0$), $A_4 = 0.8$ ($\omega_4 = 1256$, $\varphi_4 = \pi/2$). Стохастическая часть сигнала моделировала измерительные шумы:

$$\varepsilon(t) = r\varepsilon(t - \Delta t) + \sqrt{1 - r^2}\xi(t)\sigma(t), \quad (3)$$

где $r = 0.6$ – коэффициент авторегрессии; $\xi(t) \sim N(0, 1)$ – стандартный гауссовский шум, $\sigma(t) = \sigma_0 + \sigma_0 \sin(\omega_s t)$ – функция переменного стандартного отклонения, $\omega_s = 0.015$ рад/с – угловая частота модуляции волатильности; Δt – шаг дискретизации по времени. В экспериментах частота дискретизации составила $f_s = 1000$ Гц ($\Delta t = 0.001$ с). Сигнал $S(t)$ соответствует мгновенным значениям тока или напряжения, измеряемым в местах установки измерительных преобразователей типа ЭНИП-2 (Mergin Units²²), выполняющих операцию аналого-цифрового преобразования и конвертации сигнала в цифровой вид по протоколу IEC 104 в сеть Ethernet.

В рамках эксперимента была реализована одна типовая угроза ИБ – внедрение ложных данных (spoofing), направленная на подмену значений телеметрии в каналах передачи данных между ЭНИП-2 и MasterSCADA 4D. Атака моделировалась как скрытое воздействие, маскирующееся под естественные переходные процессы, такие как коммутация выключателей или изменение величины и характера нагрузки. Математическая модель атаки описывается выражением:

$$A_{\text{imitation}}(t) = \theta \left(1 - e^{-\frac{t-t_0}{\tau}} \right) + \delta, \quad (4)$$

где $\theta = 0.25$ – максимальная амплитуда изменения параметра; $\tau = 30$ отсчетов (0.03 с при частоте дискретизации 1000 Гц) – постоянная времени нарастания; $\delta = -0.12$ – постоянное смещение; t_0 – момент начала атаки, выбираемый в диапазоне 35–40% длины временного ряда (1750–2000-й отсчет при общей длине 5000 отсчетов).

Атака внедрялась в поток данных IEC 104 между ЭНИП-2 и MasterSCADA 4D, что приводило к искажению отображаемых у диспетчера значений, что, в свою очередь, может приводить к ложному срабатыванию технологической автоматики или защиты. При этом в действительности все изменения оставались в пределах допустимых норм, включая качество электрической энергии согласно ГОСТ 32144–2013²³.

²² Объединяющий модуль. [The unifying module.]

²³ ГОСТ 32144–2013. Межгосударственный стандарт. *Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения*. М.: Стандартинформ; 2014. [GOST 32144-2013. Interstate Standard. *Electric energy. Electromagnetic compatibility of technical equipment. Power quality limits in the public power supply systems*. Moscow: Standartinform; 2014 (in Russ.).]

В рамках исследования под аномалией понимается статистически значимое отклонение поведения параметра телеметрии от ожидаемой модели функционирования системы, вызванное нарушением физически обоснованных взаимосвязей между технологическими параметрами. При реальной аварии изменение одного параметра (например, рост тока при коротком замыкании) сопровождается предсказуемыми изменениями смежных величин (падение напряжения, изменение мощности, срабатывание защит), сохраняя причинно-следственную согласованность. Кибератака, имитирующая аварию путем подмены данных в канале связи, нарушает эти взаимосвязи: искажается значение отдельного параметра без соответствующих изменений в смежных каналах телеметрии и без физических проявлений в первичном оборудовании. Именно это расхождение между отображаемым состоянием в АСУ ТП и физической реальностью служит основанием для формирования метки аномалии при разметке обучающих данных.

Для каждого запуска формировались сбалансированные обучающая (5000 отсчетов) и тестовая (3500 отсчетов) выборки, включающие как фрагменты телеметрии штатного режима, так и участки с инъекцией угрозы ИБ. Обе стратегии оценивались на одних и тех же наборах данных, сгенерированных в условиях полунатурного моделирования на стенде, что обеспечивало корректность сравнительного анализа.

Этап 3. Сбор и обработка результатов

Метки аномалий формировались с учетом ограничений реальных систем обнаружения. При формировании обучающей выборки вероятность корректного детектирования каждой точки атаки искусственно задавалась равной 70% для имитации несовершенства разметки. Начальные и конечные 10 отсчетов каждого атакующего участка исключались из разметки во избежание граничных эффектов. Ложные срабатывания искусственно вводились с частотой 0.5%, что соответствует частоте ложных срабатываний (англ. False Positive Rate, FPR) $FPR = 0.005$, путем случайного выбора точек из штатного режима. Для преобразования временных рядов применялась методика скользящего окна длиной 40 отсчетов с формированием 17-мерного признакового вектора, описанного в этапе 1.

Для каждой стратегии проводился сбор и анализ следующих метрик:

- полнота (Recall), точность (Precision), частота ложных срабатываний;
- F_2 -мера ($\beta = 2$), отражающая приоритет полноты обнаружения угроз над точностью;
- метрика, объединяющая результативность обнаружения и уровень защищенности эксплуатационной среды:

$$\Psi = F_2(1 - \rho), \quad (5)$$

где $\rho = \alpha V_{\text{real}}/V_{\text{total}}$, $V_{\text{total}} = V_{\text{real}} + V_{\text{DT}}$, значения V_{real} и V_{DT} определены в соответствии со стратегией адаптации (см. этап 1), α – весовой коэффициент, отражающий относительную опасность (риск) вмешательства в работу стенда при дообучении на реальном оборудовании. Значение $\alpha = 0.08$ выбрано эмпирически, исходя из экспертной оценки соотношения риска нарушения технологического процесса и ценности получаемых данных.

Этап 4. Интерпретация результатов

Заключительный этап включал анализ полученных данных. Были приняты допущения об адекватности стенда реальным энергообъектам, репрезентативности смоделированных угроз ИБ и корректности метрик. Ограничения связаны с тем, что стенд, несмотря на высокую степень приближения к реальности, остается контролируемой средой.

Результаты по итогам 100 независимых запусков представлены в таблице.

Результаты эксперимента показали, что стратегия В (с использованием ЦД) обеспечивает сопоставимое качество обнаружения угроз при значимо более высоком уровне защищенности эксплуатационной среды (анализ распределений подтвердил, что в подавляющем большинстве запусков $\Psi_B > \Psi_A$). На основе анализа выявленных уязвимостей и паттернов успешно детектированных атак были сформулированы и протестированы в среде ЦД конкретные меры защиты.

Поскольку смоделированная угроза представляла собой внедрение ложных данных в каналы телеметрии IEC 104, адаптация была сфокусирована на улучшении семантического и логического контроля поступающей информации. На основе анализа выявленных в ходе экспериментов паттернов ложных срабатываний и пропусков атак в конфигурацию стенда были внедрены две дополнительные меры, реализуемые штатными средствами MasterSCADA 4D и направленные на повышение качества обнаружения:

1. Корреляционное правило логической проверки телеметрии. При срабатывании модели машинного обучения об аномалии параметра система автоматически анализирует журнал событий

за предшествующий интервал на наличие операторских команд или срабатываний автоматики, которые могли бы физически обусловить наблюдаемое изменение. Отсутствие таких событий при резком изменении параметра повышает приоритет сигнала и интерпретирует его как потенциальную кибератаку. Данное правило направлено на снижение ложных срабатываний в переходных режимах.

2. Адаптивный многоуровневый пороговый контроль. Статические пороги критических параметров заменены режимно-зависимыми, учитывающими текущую нагрузку энергосистемы. Это позволило надежнее отделять штатные колебания от атак с малым смещением.

Серия из 50 дополнительных запусков с идентичными параметрами показала следующие результаты по сравнению с исходной конфигурацией стратегии В:

- точность детектирования атак увеличилась на 5–8% (с 0.502 до 0.541 в среднем);
- полнота сохранилась на том же уровне (~0.867);
- метрика защищенности Ψ продемонстрировала рост в среднем на 0.025.

Таким образом, использование ЦД, интегрированного с физической моделью объекта в среде RSCAD FX и синхронизированного с аппаратным комплексом реального времени RTDS NovaCor, позволило верифицировать стратегии обнаружения угроз ИБ и на основе анализа смоделированных атак синтезировать защитные меры на уровне прикладной логики АСУ ТП. Данный подход реализует принцип минимального вмешательства, предоставляя методику безопасного совершенствования систем защиты без прямого взаимодействия с реальным оборудованием.

ЗАКЛЮЧЕНИЕ

Настоящая работа стала отправной точкой межвузовского научно-технического сотрудничества между РТУ МИРЭА и НГТУ им. Р.Е. Алексеева. Формирование такой кооперации отвечает стратегическим задачам консолидации отечественной научной экспертизы в условиях цифровой трансформации критически важных отраслей экономики.

Проведенное исследование подтвердило гипотезу о том, что ЦД АСУ ТП энергообъекта может быть

Таблица. Сравнительные показатели стратегий обнаружения по итогам 100 независимых экспериментов (среднее значение $\pm$ стандартное отклонение)

Стратегия	F_2 -мера	Полнота	Точность	FPR	Ψ
A	0.745 ± 0.032	0.854 ± 0.051	0.531 ± 0.057	0.019 ± 0.004	0.689 ± 0.030
B	0.741 ± 0.030	0.868 ± 0.046	0.502 ± 0.058	0.021 ± 0.004	0.742 ± 0.031

использован для адаптивного анализа угроз ИБ без прямого вмешательства в эксплуатационную среду. Эксперимент на полунатурном киберфизическом стенде на базе программно-аппаратного комплекса RTDS, воспроизводящем реальные условия функционирования объекта КИИ, продемонстрировал, что стратегия, основанная исключительно на синтетических данных, генерируемых ЦД, обеспечивает уровень обнаружения угроз, сопоставимый со стратегией, предполагающей дообучение модели на реальных данных стенда. При этом она превосходит последнюю по метрике Ψ .

Результаты работы имеют принципиальное значение для практики защиты КИИ. В условиях, когда прямое тестирование и адаптация систем обнаружения угроз на реальном оборудовании либо запрещены, либо экономически и операционно нецелесообразны, киберфизические стенды моделирования технологических процессов на энергообъектах в реальном времени, а также ЦД становятся инструментами повышения защищенности. Они позволяют реализовать циклический процесс «моделирование – обучение – оценка – адаптация» в изолированной, но репрезентативной среде.

Важным подтверждением практической ценности подхода стало успешное применение ЦД для синтеза защитных мер. Были разработаны и протестированы два механизма повышения защищенности на уровне логики АСУ ТП: корреляционная проверка событий в SCADA и режимно-зависимые пороги. Их внедрение в конфигурацию стенда позволило повысить точность детектирования на 5–7% при сохранении полноты (~ 0.865) и дополнительно увеличить значение метрики Ψ на 0.02–0.03.

Вместе с тем, полученные выводы открывают пространство для научной дискуссии. Во-первых, остается открытым вопрос о границах применимости синтетических данных: насколько точно ЦД способен воспроизводить все возможные режимы работы и способы реализации угроз. Во-вторых, предложенная метрика Ψ , хотя и формализует компромисс между результативностью и защищенностью, требует дальнейшей верификации и, возможно, расширения за счет учета дополнительных

факторов, таких как стоимость ложных срабатываний или время реакции на инцидент. Наконец, следует отметить, что сам подход к адаптации, основанный на итеративном дообучении, не является универсальным решением. Его эффективность напрямую зависит от качества первоначальной модели и от степени соответствия между ЦД и реальным объектом.

БЛАГОДАРНОСТИ

Исследование выполнено за счет гранта Российского научного фонда № 25-29-00362, <https://rscf.ru/project/25-29-00362/>.

ACKNOWLEDGMENTS

The study was supported by the Russian Science Foundation, grant No. 25-29-00362, <https://rscf.ru/project/25-29-00362/>.

Вклад авторов

О.В. Трубиенко – анализ литературы, постановка задачи, написание и редактирование статьи.

Е.С. Митяков – идея исследования, обоснование математической модели, интерпретация результатов, написание и редактирование статьи.

А.А. Лоскутов – создание экспериментальной базы, проведение экспериментов, анализ результатов, написание и редактирование статьи.

А.Л. Куликов – руководство экспериментами, обеспечение работы лабораторного оборудования, написание и редактирование статьи.

Authors' contributions

O.V. Trubienko – performed literature review, formulated the research problem (conceptualization), wrote the original draft, and reviewed and edited the manuscript.

E.S. Mityakov – conceived the study, justified the mathematical model, performed formal analysis and interpreted the results, wrote the original draft, and reviewed and edited the manuscript.

A.A. Loskutov – developed the experimental infrastructure, conducted the experiments, analyzed the results, wrote the original draft, and reviewed and edited the manuscript.

A.L. Kulikov – supervised the experiments, operated laboratory equipment, and reviewed and edited the manuscript.

СПИСОК ЛИТЕРАТУРЫ

1. Полтавцева М.А. Управление адаптивным мониторингом информационной безопасности КФС. *Защита информации. Инсайд*. 2021;3:47–53.
2. Митяков Е.С., Адиев М.М. Функциональная модель анализа угроз информационной безопасности объектов критической информационной инфраструктуры на основе цифрового двойника. *Информатизация и связь*. 2025;4:144–150. <https://doi.org/10.34219/2078-8320-2025-16-4-144-150>
3. Гавдан Г.П., Иваненко В.Г., Рыбалко Э.П., Рыбалко Д.П. Устойчивость функционирования объектов критической информационной инфраструктуры. *Безопасность информационных технологий*. 2022;29(4):53–66. <https://doi.org/10.26583/bit.2022.4.05>

4. Лоскутов А.А., Куликов А.Л., Пелевин П.С., Симапов А.С. Методы выявления киберугроз на цифровых подстанциях. *Электротехника*. 2025;10:59–69.
5. Куликов А.Л., Лоскутов А.А., Зинин В.М. Нормативно-технические аспекты обеспечения информационной и кибербезопасности объектов цифровой электроэнергетики. *Вопросы кибербезопасности*. 2025;6(70):101–115. <https://doi.org/10.21681/2311-3456-2025-6-101-115>
6. Kulikov A., Loskutov A., Bezdushniy D., Petrov I. Decision Tree Models and Machine Learning Algorithms in the Fault Recognition on Power Lines with Branches. *Energies*. 2023;16(14):5563. <https://doi.org/10.3390/en16145563>
7. Kayan H., Nunes M., Rana O., Burnap P., Perera C. Cybersecurity of Industrial Cyber-Physical Systems: A Review. *ACM Comput. Surv.* 2021;54(11s):1–35. <https://doi.org/10.1145/3510410>
8. Koay A., Ko R., Hettema H., Radke K. Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. *J. Intell. Inf. Syst.* 2022;60:377–405. <https://doi.org/10.1007/s10844-022-00753-1>
9. Al-Abassi A., Karimipour H., Dehghantanha A., Parizi R. An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. *IEEE Access*. 2020;8:83965–83973. <https://doi.org/10.1109/ACCESS.2020.2992249>
10. Ali J., Ali S., Balushi T., Nadir Z. Intrusion Detection in Industrial Control Systems Using Transfer Learning Guided by Reinforcement Learning. *Information*. 2025;16(10):910. <https://doi.org/10.3390/info16100910>
11. Ayodeji A., Liu Y., Chao N., Yang Li-gun. A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. *Nucl. Eng. Technol.* 2020;52(12):2687–2698. <https://doi.org/10.1016/j.net.2020.05.012>
12. Jeffrey N., Tan Q., Villar J. A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems. *Electronics*. 2023;12(15):3283. <https://doi.org/10.3390/electronics12153283>
13. Rahman U., Ahmed H., Khan M., Saqlain M., Siddiqui S., Akhtar E. Comprehensive Cybersecurity Risk Assessment Framework for Industrial Control Systems (ICS) and SCADA Environments: Identifying Threats, Vulnerabilities, and Mitigation Strategies. *Glob. Res. J. Nat. Sci. Technol.* 2025;3(3):134–164.
14. Gehrmann C., Gunnarsson M. A Digital Twin Based Industrial Automation and Control System Security Architecture. *IEEE Trans. Ind. Inform.* 2020;16(1):669–680. <https://doi.org/10.1109/TII.2019.2938885>
15. He R., Chen G., Dong C., Sun S., Shen X. Data-driven digital twin technology for optimized control in process systems. *ISA Trans.* 2019;95:221–234. <https://doi.org/10.1016/j.isatra.2019.05.011>
16. Sayghe A. Digital Twin-Driven Intrusion Detection for Industrial SCADA: A Cyber-Physical Case Study. *Sensors*. 2025;25(16):4963. <https://doi.org/10.3390/s25164963>
17. Homaei M., Tarif M., Avilla M., Caro A. Causal Digital Twins for Cyber-Physical Security: A Framework for Robust Anomaly Detection in Industrial Control Systems. *arXiv preprint*. arXiv:2510.09616. 2025. <https://doi.org/10.48550/arxiv.2510.09616>
18. Varghese S., Ghadim A., Balador A., Alimadadi Z., Papadimitratos P. Digital Twin-based Intrusion Detection for Industrial Control Systems. In: *2022 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. 2022. P. 611–617. <https://doi.org/10.1109/PerComWorkshops53856.2022.9767492>
19. Castellani A., Schmitt S., Squartini S. Real-World Anomaly Detection by Using Digital Twin Systems and Weakly Supervised Learning. *IEEE Trans. Ind. Inform.* 2020;17(7):4733–4742. <https://doi.org/10.1109/TII.2020.3019788>
20. Jeremiah S.R., El Azaoui A., Xiong N.N., Park J.H. A comprehensive survey of digital twins: Applications, technologies and security challenges. *J. Syst. Archit.* 2024;151:103120. <https://doi.org/10.1016/j.sysarc.2024.103120>
21. Smagowicz J., Szwed C., Wiśniewski M. Application of Digital Twin in Ensuring Cyber-Security in Manufacturing Processes Management. *Scientific Papers of Silesian University of Technology Organization & Management Ser.* 2025;224:457–476. <https://doi.org/10.29119/1641-3466.2025.224.25>
22. Cheng R., Hou L., Xu S. A Review of Digital Twin Applications in Civil and Infrastructure Emergency Management. *Buildings*. 2023;13(5):1143. <https://doi.org/10.3390/buildings13051143>
23. Masi M., Sellitto G., Aranha H., Pavleska T. Securing critical infrastructures with a cybersecurity digital twin. *Softw. Syst. Model.* 2023;22:689–707. <https://doi.org/10.1007/s10270-022-01075-0>
24. Jiang Y., Wang W., Ding J., Lu X., Jing Y. Leveraging Digital Twin Technology for Enhanced Cybersecurity in Cyber-Physical Production Systems. *Future Internet*. 2024;16(4):134. <https://doi.org/10.3390/fi16040134>
25. Vitale F., Guarino S., Flammini F., Faramondi L., Mazzocca N., Setola R. Process Mining for Digital Twin Development of Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Inform.* 2025;21(1):866–875.
26. Alhamam N., Rahman A., Aljughaiman A. A Comprehensive Review on Cybersecurity of Digital Twins Issues, Challenges, and Future Research Directions. *IEEE Access*. 2025;13:45106–45124.
27. Ootom S. Risk auditing for Digital Twins in cyber physical systems: A systematic review. *J. Cyber Secur. Risk Audit*. 2025;1:22–35. <https://doi.org/10.63180/JCSRA.THESTAP.2025.1.3>

REFERENCES

1. Poltavtseva M.A. CPS adaptive information security monitoring control. *Zashchita informatsii. Insaid*. 2021;3:47–53 (in Russ.).
2. Mityakov E.S., Adiev M.M. Functional model for threat analysis in critical information infrastructure based on digital twin. *Informatizatsiya i svyaz' = Informatization and Communications*. 2025;4:144–150 (in Russ.). <https://doi.org/10.34219/2078-8320-2025-16-4-144-150>
3. Gavdan G.P., Ivanenko V.G., Rybalko E.P., Rybalko D.P. Sustainability of the functioning of critical information infrastructure facilities. *Bezopasnost' informatsionnykh tekhnologii = IT Security (Russia)*. 2022;29(4):53–66 (in Russ.). <http://doi.org/10.26583/bit.2022.4.05>

4. Loskutov A.A., Kulikov A.L., Pelevin P.S., et al. Method for Detecting Cyber Threats at Digital Substations. *Russ. Electr. Engin.* 2025;96(10):853–863. <http://doi.org/10.3103/S1068371225701184>
[Original Russian Text: Loskutov A.A., Kulikov A.L., Pelevin P.S., Simanov A.S. Method for Detecting Cyber Threats at Digital Substations. *Ehlektrrotekhnika*. 2025;10:59–69 (in Russ.).]
5. Kulikov A.L., Loskutov A.A., Zinin V.M. Regulatory and technical aspects of ensuring information and cybersecurity of digital electric power industry facilities. *Voprosy kiberbezopasnosti*. 2025;6(70):101–115 (in Russ.). <https://doi.org/10.21681/2311-3456-2025-6-101-115>
6. Kulikov A., Loskutov A., Bezdushniy D., Petrov I. Decision Tree Models and Machine Learning Algorithms in the Fault Recognition on Power Lines with Branches. *Energies*. 2023;16(14):5563. <https://doi.org/10.3390/en16145563>
7. Kayan H., Nunes M., Rana O., Burnap P., Perera C. Cybersecurity of Industrial Cyber-Physical Systems: A Review. *ACM Comput. Surv.* 2021;54(11s):1–35. <https://doi.org/10.1145/3510410>
8. Koay A., Ko R., Hetteema H., Radke K. Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. *J. Intell. Inf. Syst.* 2022;60:377–405. <https://doi.org/10.1007/s10844-022-00753-1>
9. Al-Abassi A., Karimipour H., Dehghantanha A., Parizi R. An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System. *IEEE Access*. 2020;8:83965–83973. <https://doi.org/10.1109/ACCESS.2020.2992249>
10. Ali J., Ali S., Balushi T., Nadir Z. Intrusion Detection in Industrial Control Systems Using Transfer Learning Guided by Reinforcement Learning. *Information*. 2025;16(10):910. <https://doi.org/10.3390/info16100910>
11. Ayodeji A., Liu Y., Chao N., Yang Li-gun. A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. *Nucl. Eng. Technol.* 2020;52(12):2687–2698. <https://doi.org/10.1016/j.net.2020.05.012>
12. Jeffrey N., Tan Q., Villar J. A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems. *Electronics*. 2023;12(15):3283. <https://doi.org/10.3390/electronics12153283>
13. Rahman U., Ahmed H., Khan M., Saqlain M., Siddiqui S., Akhtar E. Comprehensive Cybersecurity Risk Assessment Framework for Industrial Control Systems (ICS) and SCADA Environments: Identifying Threats, Vulnerabilities, and Mitigation Strategies. *Glob. Res. J. Nat. Sci. Technol.* 2025;3(3):134–164.
14. Gehrmann C., Gunnarsson M. A Digital Twin Based Industrial Automation and Control System Security Architecture. *IEEE Trans. Ind. Inform.* 2020;16(1):669–680. <https://doi.org/10.1109/TII.2019.2938885>
15. He R., Chen G., Dong C., Sun S., Shen X. Data-driven digital twin technology for optimized control in process systems. *ISA Trans.* 2019;95:221–234. <https://doi.org/10.1016/j.isatra.2019.05.011>
16. Sayghe A. Digital Twin-Driven Intrusion Detection for Industrial SCADA: A Cyber-Physical Case Study. *Sensors*. 2025;25(16):4963. <https://doi.org/10.3390/s25164963>
17. Homaei M., Tarif M., Avilla M., Caro A. Causal Digital Twins for Cyber-Physical Security: A Framework for Robust Anomaly Detection in Industrial Control Systems. *arXiv preprint*. arXiv:2510.09616. 2025. <https://doi.org/10.48550/arxiv.2510.09616>
18. Varghese S., Ghadim A., Balador A., Alimadadi Z., Papadimitratos P. Digital Twin-based Intrusion Detection for Industrial Control Systems. In: *2022 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. 2022. P. 611–617. <https://doi.org/10.1109/PerComWorkshops53856.2022.9767492>
19. Castellani A., Schmitt S., Squartini S. Real-World Anomaly Detection by Using Digital Twin Systems and Weakly Supervised Learning. *IEEE Trans. Ind. Inform.* 2020;17(7):4733–4742. <https://doi.org/10.1109/TII.2020.3019788>
20. Jeremiah S.R., El Azzaoui A., Xiong N.N., Park J.H. A comprehensive survey of digital twins: Applications, technologies and security challenges. *J. Syst. Archit.* 2024;151:103120. <https://doi.org/10.1016/j.sysarc.2024.103120>
21. Smagowicz J., Szwed C., Wiśniewski M. Application of Digital Twin in Ensuring Cyber-Security in Manufacturing Processes Management. *Scientific Papers of Silesian University of Technology Organization & Management Ser.* 2025;224:457–476. <https://doi.org/10.29119/1641-3466.2025.224.25>
22. Cheng R., Hou L., Xu S. A Review of Digital Twin Applications in Civil and Infrastructure Emergency Management. *Buildings*. 2023;13(5):1143. <https://doi.org/10.3390/buildings13051143>
23. Masi M., Sellitto G., Aranha H., Pavleska T. Securing critical infrastructures with a cybersecurity digital twin. *Softw. Syst. Model.* 2023;22:689–707. <https://doi.org/10.1007/s10270-022-01075-0>
24. Jiang Y., Wang W., Ding J., Lu X., Jing Y. Leveraging Digital Twin Technology for Enhanced Cybersecurity in Cyber-Physical Production Systems. *Future Internet*. 2024;16(4):134. <https://doi.org/10.3390/fi16040134>
25. Vitale F., Guarino S., Flammini F., Faramondi L., Mazzocca N., Setola R. Process Mining for Digital Twin Development of Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Inform.* 2025;21(1):866–875.
26. Alhamam N., Rahman A., Aljughaiman A. A Comprehensive Review on Cybersecurity of Digital Twins Issues, Challenges, and Future Research Directions. *IEEE Access*. 2025;13:45106–45124.
27. Ootom S. Risk auditing for Digital Twins in cyber physical systems: A systematic review. *J. Cyber Secur. Risk Audit.* 2025;1:22–35. <https://doi.org/10.63180/JCSRA.THESTAP.2025.1.3>

Об авторах

Трубиенко Олег Владимирович, к.т.н., доцент, заведующий кафедрой КБ-2 «Информационно-аналитические системы кибербезопасности», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: trubienko@mirea.ru. Scopus Author ID 57213680467, SPIN-код РИНЦ 1668-5640, <https://orcid.org/0000-0002-6809-8732>

Митяков Евгений Сергеевич, д.э.н., профессор, заведующий кафедрой КБ-9 «Предметно-ориентированные информационные системы», Институт кибербезопасности и цифровых технологий, ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: mityakov@mirea.ru. Scopus Author ID 55960540500, SPIN-код РИНЦ 5691-8947, <https://orcid.org/0000-0001-6579-0988>

Лоскутов Антон Алексеевич, д.т.н., доцент, старший научный сотрудник, лаборатория «Автономные гибридные электроэнергетические комплексы», доцент кафедры «Электроэнергетика, электроснабжение и силовая электроника», ФГБОУ ВО «Нижегородский государственный технический университет им. Р.Е. Алексеева (603155, Россия, Нижний Новгород, ул. Минина, д. 24). E-mail: loskutov_aa@nntu.ru. Scopus Author ID 57205467115, ResearcherID A-4809-2014, <https://orcid.org/0000-0003-2228-596X>

Куликов Александр Леонидович, д.т.н., профессор, кафедра «Электроэнергетика, электроснабжение и силовая электроника», ФГБОУ ВО «Нижегородский государственный технический университет им. Р.Е. Алексеева (603155, Россия, Нижний Новгород, ул. Минина, д. 24). E-mail: inventor61@mail.ru. Scopus Author ID 56496375600, <https://orcid.org/0000-0003-1092-7136>

About the Authors

Oleg V. Trubienko, Cand. Sci. (Eng.), Associate Professor, Head of the Department of Information and Analytical Cybersecurity Systems, Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: trubienko@mirea.ru. Scopus Author ID 57213680467, RSCI SPIN-code 1668-5640, <https://orcid.org/0000-0002-6809-8732>

Evgeny S. Mityakov, Dr. Sci. (Eng.), Professor, Head of the Department “Subject-Oriented Information Systems,” Institute of Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: mityakov@mirea.ru. Scopus Author ID 55960540500, RSCI SPIN-code 5691-8947, <https://orcid.org/0000-0001-6579-0988>

Anton A. Loskutov, Dr. Sci. (Eng.), Senior Researcher, Laboratory of Autonomous Hybrid Electric Power Complexes; Associate Professor, Department of Electric Power Engineering, Power Supply, and Power Electronics, R.E. Alekseev Nizhny Novgorod State Technical University (24, Minina ul., Nizhny Novgorod, 603155 Russia). E-mail: loskutov_aa@nntu.ru. Scopus Author ID 57205467115, ResearcherID A-4809-2014, <https://orcid.org/0000-0003-2228-596X>

Aleksandr L. Kulikov, Dr. Sci. (Eng.), Professor, Department of Electric Power Engineering, Power Supply, and Power Electronics, R.E. Alekseev Nizhny Novgorod State Technical University (24, Minina ul., Nizhny Novgorod, 603155 Russia). E-mail: inventor61@mail.ru. Scopus Author ID 56496375600, <https://orcid.org/0000-0003-1092-7136>