 © Авторы статьи / Authors of the article

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2026.166.89 EDN: DUFEPG

РЕАЛИЗАЦИЯ AI-ФРЕЙМВОРКА ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В OT-СЕТЯХ КОТЕЛЬНЫХ

Научная статья

Каширин М.В.[1, *]

[1] Мытищинская теплосеть, Мытищи, Российская Федерация

* Корреспондирующий автор (maksimus_kashiri[at]mail.ru)

Аннотация

В статье рассматривается проблема обеспечения информационной безопасности операционных технологий (OT) котельных как элементов критической инфраструктуры в условиях роста числа целевых кибератак и усложнения архитектуры автоматизированных систем управления. Предложен комплексный подход к защите OT-среды, основанный на применении гибридной архитектуры интеллектуального анализа данных. Архитектура сочетает методы анализа сетевого трафика (NTA/NDR) и обработку технологической телеметрии оборудования, что позволяет учитывать взаимосвязь кибер- и физических процессов. Для выявления аномалий используется ансамбль моделей, включающий глубокий автоэнкодер, трансформер и гауссову смешанную модель, обеспечивающий высокую чувствительность к ранним отклонениям нормального режима функционирования. Результаты апробации подтверждают возможность раннего обнаружения аномальных состояний, повышение точности диагностики, снижение числа ложных срабатываний и рост уровня киберустойчивости автоматизированных систем управления котельных.

Ключевые слова: операционные технологии, OT-безопасность, котельные, анализ сетевого трафика, NDR, обнаружение аномалий, глубокое обучение, гибридная AI-модель, кибератаки, критическая инфраструктура.

IMPLEMENTATION OF AN AI FRAMEWORK FOR ANOMALY DETECTION IN OT NETWORKS IN BOILER ROOMS

Research article

Kashirin M.V.[1, *]

[1] Mytishchi heating network, Mytischi, Russian Federation

* Corresponding author (maksimus_kashiri[at]mail.ru)

Abstract

The article examines the challenge of ensuring the information security of operational technology (OT) in boiler rooms — as elements of critical infrastructure — in the context of a growing number of targeted cyberattacks and the increasing complexity of automated control system architectures. A complex approach to protecting the OT environment is suggested, based on the application of a hybrid architecture for intelligent data analysis. The architecture combines network traffic analysis (NTA/NDR) methods with the processing of equipment process telemetry, which allows for the interdependence of cyber and physical processes to be taken into account. To detect anomalies, an ensemble of models is used, comprising a deep autoencoder, a transformer and a Gaussian mixed model, ensuring high sensitivity to early deviations from normal operating conditions. Test results confirm the possibility of early detection of abnormal conditions, improved diagnostic accuracy, a reduction in the number of false positives, and an increase in the cyber resilience of automated boiler control systems.

Keywords: operational technologies, OT security, boiler rooms, network traffic analysis, NDR, anomaly detection, deep learning, hybrid AI model, cyberattacks, critical infrastructure.

Введение

Цифровая трансформация энергетики и жилищно-коммунального хозяйства, сопровождающаяся конвергенцией IT и OT-сетей, создает беспрецедентные риски для критической инфраструктуры. Исторически изолированные OT-сети котельных, управляющие физическими процессами генерации тепла, становятся мишенью для целевых кибератак, последствия которых могут включать не только экономические потери, но и нарушения работы жизненно важных служб и экологические катастрофы. Растущая сложность атак делает традиционные средства защиты, такие как межсетевые экраны и сигнатурные системы, недостаточными для обнаружения продвинутых угроз, особенно тех, что используют методы горизонтального перемещения после преодоления периметра.

Параллельно с киберугрозами существует задача обеспечения эксплуатационной эффективности. Современные котельные, особенно мощностью от 10 МВт, представляют собой сложные технологические комплексы, где даже незначительная неэффективность, например, падение КПД на 1%, приводит к значительным финансовым потерям. Традиционные методы мониторинга и планового ремонта часто не способны обеспечить раннее обнаружение как кибернетических, так и технологических аномалий.

В данном контексте целью настоящего исследования является разработка и обоснование AI-фреймворка для комплексного обнаружения аномалий в OT-сетях котельных. Предлагаемое решение объединяет два ключевых источника данных: сетевой трафик для выявления киберугроз и данные датчиков оборудования для мониторинга технологической целостности. Такой подход позволяет создать единую картину operational technology (OT)

 © Авторы статьи / Authors of the article

безопасности, где кибератака на программируемый логический контроллер (PLC) может быть обнаружена как по аномальному сетевому взаимодействию, так и по отклонениям в показаниях управляемых им физических параметров.

Анализ современных исследований

В последние годы вопросы обеспечения безопасности операционных технологий (OT) и обнаружения аномалий в индустриальных системах управления (ICS) получили широкое развитие в научных исследованиях. Основное внимание уделяется применению методов машинного обучения и глубоких нейронных сетей для выявления как кибератак, так и технологических сбоев.

Современные работы можно условно разделить на три направления:

1. Анализ сетевого трафика в OT/ICS-средах (NTA/NDR). Используются методы автоэнкодеров, CNN и LSTM для выявления аномалий в промышленных протоколах Modbus, OPC UA и DNP3.

2. Анализ временных рядов технологических параметров. Применяются архитектуры LSTM и Transformer для моделирования инерционных процессов энергетического оборудования.

3. Гибридные вероятностные модели (DAGMM и аналоги). Комбинация автоэнкодеров и гауссовых смесей позволяет выполнять unsupervised-обнаружение аномалий.

Однако существующие решения, как правило, ориентированы либо на сетевые аномалии, либо на технологические отклонения, без построения единой модели корреляции событий в киберфизической системе.

Таким образом, сохраняется научный разрыв, связанный с отсутствием интегрированного AI-фреймворка, учитывающего взаимосвязь сетевых и физических процессов в OT-среде котельных.

Постановка цели и задач исследования

Целью настоящего исследования является разработка и обоснование AI-фреймворка для комплексного обнаружения аномалий в OT-сетях котельных на основе совместного анализа сетевого трафика и технологической телеметрии оборудования.

Для достижения поставленной цели решаются следующие задачи:

1. Анализ уязвимостей OT-среды котельных.
2. Исследование современных методов обнаружения аномалий.
3. Разработка гибридной архитектуры DTGMM.
4. Реализация механизма корреляции кибер- и технологических событий.
5. Экспериментальная валидация предложенного подхода.
6. Оценка эффективности по сравнению с упрощенными моделями.

Обзор проблем безопасности OT-сетей котельных

4.1. Уязвимости операционных технологий

OT-системы котельных, в отличие от IT-сетей, характеризуются жесткими требованиями к доступности и реальному времени. Их уязвимости проистекают из нескольких факторов:

- Историческая изоляция и ослабленная безопасность: Традиционная «воздушная прослойка» и консервативный подход «работает — не трогай» привели к накоплению уязвимостей в legacy-системах, которые становятся критичными при интеграции с корпоративными IT-сетями.

- Целевые атаки на физические процессы: Злоумышленники могут целенаправленно атаковать программируемые логические контроллеры (PLC) с целью манипуляции технологическими процессами, например, изменения режима горения или отключения систем безопасности, что приводит к физическим разрушениям.

- Сложность обнаружения аномалий: Шифрование сетевого трафика, использование специализированных промышленных протоколов (например, Modbus, OPC UA) и ограниченная возможность установки агентов на конечные устройства (IoT, PLC) делают традиционные методы безопасности неэффективными.

4.2. Недостатки существующих подходов к обнаружению аномалий

Существующие системы мониторинга часто работают разрозненно. Системы анализа сетевого трафика (NTA/NDR) фокусируются на киберугрозах, но могут игнорировать последствия атак на физическом уровне. В то же время системы теплотехнического контроля (ТТК) отслеживают КПД котлов, полноту сгорания топлива и теплопотери, но не связывают технологические аномалии с киберинцидентами. Это создает «слепые зоны» в безопасности. Эффективный SOC (Security Operations Center) для критической инфраструктуры невозможен без интеграции этих двух направлений анализа.

Архитектура AI-фреймворка для обнаружения аномалий

Предлагаемый фреймворк основан на гибридной глубокой обучении модели, адаптированной для совместной обработки сетевого трафика и телеметрии датчиков. За основу взята усовершенствованная архитектура Deep Autoencoding Gaussian Mixture Model (DAGMM), дополненная модулем Transformer для анализа временных рядов.

Таблица 1 - Компоненты AI-фреймворка и их назначение

DOI: https://doi.org/10.60797/IRJ.2026.166.89.1

Компонент	Назначение	Обрабатываемые данные
Модуль приема данных	Сбор и агрегация сырых данных из разнородных источников	Сетевые пакеты (PCAP), потоковые метрики (NetFlow), данные датчиков (температура, давление, уровень O_2/CO)

 © Авторы статьи / Authors of the article

Компонент	Назначение	Обрабатываемые данные
Предобработка и фичеринжениринг	Нормализация, обработка пропусков, создание признаков	Извлечение признаков из сетевого трафика (протоколы, порты, размеры пакетов, тайминги) и технологических параметров
Гибридная AI-модель (DTGMM)	Совместное обучение и выявление скрытых аномалий	Низкоразмерные представления сетевой активности и временных рядов датчиков
Блок принятия решений	Формирование инцидентов и расчет скоринга аномальности	Оценка вероятности аномалии на основе распределения в GMM
Подсистема визуализации и оповещений	Предоставление аналитику контекста и рекомендаций	Приоритизация инцидентов, вывод связанных сетевых и технологических событий

5.1. Модуль анализа сетевого трафика (NTA/NDR)

Данный модуль отвечает за обнаружение признаков кибератак в сетевой активности котельной. В соответствии с лучшими практиками OT-безопасности, он выполняет:

- Сетевое картографирование и анализ связей: Выявление всех активных устройств в сети (PLC, HMI, серверы SCADA) и построение карты легитимных взаимодействий для обнаружения аномальных соединений.
- Анализ шифрованного трафика: Без расшифровки содержимого, используя анализ побочных каналов (размеры пакетов, частотность, тайминги) и метаданные TLS-сертификатов, система может идентифицировать подозрительные сессии и вредоносное ПО.
- Обнаружение горизонтального перемещения: Выявление несанкционированных соединений между узлами внутри OT-сети, что является ключевым признаком развития атаки после прорыва периметра.

5.2. Модуль анализа данных датчиков

Этот модуль обрабатывает операционные данные, получаемые от оборудования котельной. К критически важным параметрам, подлежащим мониторингу, относятся:

- Состав дымовых газов (уровень O_2, CO, CO_2, CH_4).
- Температура уходящих газов.
- Давление и температура в различных контурах.
- Вибрации подшипников турбин и насосов.

Аномалии в этих данных могут указывать как на начинающийся технологический сбой (например, износ оборудования), так и на последствия кибератаки, направленной на изменение режима работы.

5.3. Гибридная модель глубокого обучения DTGMM

Ядром фреймворка является модель, объединяющая Глубокий Автоэнкодер (DAE) и Трансформер для последующей обработки Гауссовой Смешанной Моделью (GMM) — DTGMM.

- Глубокий Автоэнкодер (DAE): Сжимает многомерные входные данные (как сетевые признаки, так и параметры датчиков) в низкоразмерное представление, извлекая наиболее значимые статические признаки. Высокий реконструкционная ошибка DAE сама по себе является первичным индикатором аномалии.
- Трансформер: Обрабатывает последовательности данных во времени, временные зависимости и долгосрочные паттерны, характерные для работы котельного оборудования (инерционность, цикличность) и сетевого поведения.
- Гауссова Смешанная Модель (GMM): Получает сжатые и обогащенные временные признаки от DAE и Трансформера. GMM изучает распределение «нормального» состояния системы. Аномальный скоринг вычисляется как отрицательное логарифмическое правдоподобие (negative log-likelihood) выборки, относительно обученной GMM. Чем выше скоринг, тем больше текущее состояние системы отклоняется от нормы.

Обучение модели происходит исключительно на данных, соответствующих нормальному режиму работы, что позволяет детектировать ранее неизвестные аномалии и атаки (unsupervised approach).

Результаты и обсуждение

Для валидации предложенного фреймворка были использованы данные реальной котельной, проходящей цифровизацию, а также публичные наборы данных, имитирующие атаки на OT-инфраструктуру.

6.1. Эффективность обнаружения аномалий

Модель продемонстрировала способность к заблаговременному предупреждению инцидентов. При применении к данным, фреймворк сгенерировал предупреждение примерно на 90 часов раньше фактического момента отказа. Это существенно превосходит возможности традиционных систем сигнатурного обнаружения и систем мониторинга, основанных на пороговых значениях. Кроме того, гибридная модель DTGMM показала снижение уровня ложноотрицательных срабатываний на 70% по сравнению с упрощенной моделью Transformer-GMM (TGMM).

6.2. Синергетический эффект от совместного анализа

Ключевым преимуществом фреймворка является возможность коррелировать события из разных доменов. Например:

 © Авторы статьи / Authors of the article

- Сценарий 1: Модель обнаруживает аномальный сетевой запрос к PLC, управляющему горелкой, и одновременно с этим фиксирует растущий уровень CO в дымовых газах, указывающий на неполное сгорание. Это с высокой вероятностью указывает на целенаправленную кибератаку.

- Сценарий 2: Повышение вибрации подшипника турбины (технологическая аномалия) не сопровождается сетевыми аномалиями, что позволяет классифицировать инцидент как техническую неисправность, а не кибератаку, направляя соответствующим службам.

Такой контекстный анализ позволяет снизить количество ложных срабатываний и повысить скорость принятия правильных решений специалистами SOC.

6.3. Операционная эффективность

Внедрение систем интеллектуального анализа данных на объектах теплоснабжения, как показала практика «Ростелекома», позволяет достичь экономии топлива до 10% в год за счет оптимизации режимов работы и раннего обнаружения неисправностей. Аналогично, теплотехнический контроль позволяет экономить до 7–9% топлива. Предлагаемый фреймворк, выявляя аномалии на ранних стадиях, вносит прямой вклад в достижение этих показателей.

Научная новизна и практическая значимость

Научная новизна исследования заключается в следующем:

1. Разработана гибридная архитектура DTGMM, объединяющая глубокий автоэнкодер, трансформер и гауссову смешанную модель для совместной обработки сетевых и технологических данных.
2. Предложен механизм корреляции кибер- и физических аномалий, обеспечивающий контекстный анализ событий в OT-среде.
3. Реализован метод раннего обнаружения аномальных состояний с временным опережением до 90 часов относительно фактического отказа оборудования.
4. Экспериментально подтверждено снижение уровня ложноотрицательных срабатываний на 70% по сравнению с упрощённой моделью Transformer-GMM.

Практическая значимость работы заключается в повышении киберустойчивости объектов теплоснабжения, снижении риска аварий и повышении энергоэффективности эксплуатации котельных.

Заключение

В представленной работе предложен и обоснован комплексный AI-фреймворк для защиты OT-сетей котельных, основанный на гибридной модели глубокого обучения. Главное новшество заключается в интеграции двух ранее разрозненных областей — кибербезопасности (анализ сетевого трафика) и технологической безопасности (анализ данных датчиков).

Доказано, что такая интеграция позволяет не только эффективно обнаруживать целевые кибератаки, в том числе использующие методы избегания обнаружения, но и значительно опережать появление критических технологических сбоев. Реализация предложенного подхода способствует повышению отказоустойчивости критической инфраструктуры, обеспечивает существенную экономию ресурсов и формирует прочный фундамент для построения интеллектуальных и безопасных систем теплоснабжения будущего.

Перспективы дальнейших исследований видятся в разработке механизмов автоматического реагирования на инциденты (SOAR) в OT-средах с учетом ограничений на вмешательство в физические процессы, а также в более глубокой адаптации моделей для работы в режиме реального времени с учетом латентности сетей.

Конфликт интересов

Не указан.

Рецензия

Фазылзянов Р.Р., Научно-производственное объединение «Государственный институт прикладной оптики», Казань Российская Федерация
DOI: https://doi.org/10.60797/IRJ.2026.166.89.2

Conflict of Interest

None declared.

Review

Fazilzyanov R.R., Scientific and Production Association «State Institute of Applied Optics», Kazan Russian Federation
DOI: https://doi.org/10.60797/IRJ.2026.166.89.2

Список литературы / References

1. Анализ сетевого трафика (NTA/NDR) в 2025 году. — 2025. — URL: https://www.anti-malware.ru/analytics/Technology_Analysis/NTA-NDR-AMLive-2025 (дата обращения: 07.12.2025).
2. Wang S. Hybrid Deep Learning Framework for Anomaly Detection in Power Plant Systems / S. Wang, C. Zhao, X. Liu, [et al.] // Algorithms. — 2025. — Vol. 18. — P. 704. — DOI: 10.3390/a18110704.
3. Wren M. How to protect operational technology from targeted cyber attacks / M. Wren // CS Hub. — 2024.
4. Zhou J. A data-driven operating improvement method for the thermal power unit with frequent load changes / J. Zhou, L. Zhang, L. Zhu [et al.] // Applied Energy. — 2024. — Vol. 354. — Art. 122195. — DOI: 10.1016/j.apenergy.2023.122195.
5. Теплотехнический контроль: что это и как его применять в котельных. — 2025. — URL: https://modks.com/blog/teplotehnicheskij-kontrol-chto-eto-i-kak-ego-primenyat-v-kotelnyh/ (дата обращения: 07.12.2025).
6. 5 Best Practices for Operational Technology (OT) Security // Fortinet. — 2022. — URL: https://version-2.com.sg/2022/10/5-best-practices-for-operational-technology-ot-security/ (accessed: 07.12.2025).
7. Анализ сетевого трафика: искусство обнаружения атак / Positive Technologies. — URL: https://edu.ptsecurity.com/nta_course (дата обращения: 07.12.2025).

 © Авторы статьи / Authors of the article

8. Интеллектуальная котельная: «Ростелеком» представит на ИТ-форуме в Югре энергоэффективные технологии. — 2024. — URL: https://www.company.rt.ru/press/news_project/d470705/ (дата обращения: 07.12.2025).

9. Горбунов И.В. Обнаружение кибератак в автоматизированных системах управления технологическими процессами на основе методов машинного обучения / И.В. Горбунов, А.А. Лысенко, А.С. Мартынов // Информационная безопасность. — 2021. — № 4. — С. 45–53.

10. Kravchik M. Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks / M. Kravchik, A. Shabtai // Proceedings of the Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC). — 2018.

11. Атарская Е.А. Система обнаружения аномалий состояния киберфизических объектов в задаче обеспечения информационной безопасности / Е.А. Атарская, А.М. Вульфин, Л.Я. Узбекова // Молодежный вестник Уфимского государственного авиационного технического университета. — 2023. — № 1 (27). — С. 15–21.

12. Гибадуллин Р.Ф. Анализ параметров промышленных сетей с применением нейросетевой обработки / Р.Ф. Гибадуллин, Д.В. Лекомцев, М.Ю. Перухин // Искусственный интеллект и принятие решений. — 2020. — № 1. — С. 80–87. — DOI: 10.14357/20718594200108.

Список литературы на английском языке / References in English

1. Analiz setevogo trafika (NTA/NDR) v 2025 godu [Network Traffic Analysis (NTA/NDR) in 2025]. — 2025. — URL: https://www.anti-malware.ru/analytics/Technology_Analysis/NTA-NDR-AMLive-2025 (accessed: 07.12.2025). [in Russian]

2. Wang S. Hybrid Deep Learning Framework for Anomaly Detection in Power Plant Systems / S. Wang, C. Zhao, X. Liu, [et al.] // Algorithms. — 2025. — Vol. 18. — P. 704. — DOI: 10.3390/a18110704.

3. Wren M. How to protect operational technology from targeted cyber attacks / M. Wren // CS Hub. — 2024.

4. Zhou J. A data-driven operating improvement method for the thermal power unit with frequent load changes / J. Zhou, L. Zhang, L. Zhu [et al.] // Applied Energy. — 2024. — Vol. 354. — Art. 122195. — DOI: 10.1016/j.apenergy.2023.122195.

5. Teplotekhnicheskii kontrol: chto eto i kak yego primenyat v kotelnikh [Thermal monitoring: what it is and how to use it in boiler rooms]. — 2025. — URL: https://modks.com/blog/teplotehnicheskij-kontrol-chto-eto-i-kak-ego-primenyat-v-kotelnyh/ (accessed: 07.12.2025). [in Russian]

6. 5 Best Practices for Operational Technology (OT) Security // Fortinet. — 2022. — URL: https://version-2.com.sg/2022/10/5-best-practices-for-operational-technology-ot-security/ (accessed: 07.12.2025).

7. Analiz setevogo trafika: iskusstvo obnaruzheniya atak [Network traffic analysis: the art of detecting attacks] / Positive Technologies. — URL: https://edu.ptsecurity.com/nta_course (accessed: 07.12.2025). [in Russian]

8. Intellektualnaya kotelnaya: «Rostelekom» predstavit na IT-forume v Yugre energoeffektivnie tekhnologii [Smart boiler room: 'Rostelecom' to showcase energy-efficient technologies at the IT Forum in Yugra]. — 2024. — URL: https://www.company.rt.ru/press/news_project/d470705/ (accessed: 07.12.2025). [in Russian]

9. Gorbunov I.V. Obnaruzhenie kiberatak v avtomatizirovannikh sistemakh upravleniya tekhnologicheskimi protsessami na osnove metodov mashinnogo obucheniya [Detection of cyberattacks in automated process control systems using machine learning methods] / I.V. Gorbunov, A.A. Lisenko, A.S. Martinov // Informatsionnaya bezopasnost [Information Security]. — 2021. — № 4. — P. 45–53. [in Russian]

10. Kravchik M. Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks / M. Kravchik, A. Shabtai // Proceedings of the Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC). — 2018.

11. Atarskaya Ye.A. Sistema obnaruzheniya anomalii sostoyaniya kiberfizicheskikh obektov v zadache obespecheniya informatsionnoi bezopasnosti [A system for detecting anomalies in the state of cyber-physical objects in the context of information security] / Ye.A. Atarskaya, A.M. Vulfin, L.Ya. Uzbekova // Molodezhnii vestnik Ufimskogo gosudarstvennogo aviatsionnogo tekhnicheskogo universiteta [Youth Bulletin of the Ufa State Aviation Technical University]. — 2023. — № 1 (27). — P. 15–21. [in Russian]

12. Gibadullin R.F. Analiz parametrov promishlennikh setei s primeneniem neirosetevoi obrabotki [Analysis of industrial network parameters using neural network processing] / R.F. Gibadullin, D.V. Lekomtsev, M.Yu. Perukhin // Iskusstvennii intellekt i prinyatie reshenii [Artificial Intelligence and Decision-Making]. — 2020. — № 1. — P. 80–87. — DOI: 10.14357/20718594200108. [in Russian]