СЕКЦИЯ 7
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. А. Захаров, А. А. Оленников, З. Н. Афсахов
Тюменский государственный университет, г. Тюмень
УДК 004.94:654.924

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

Аннотация. В статье представлены промежуточные результаты анализа угроз безопасности информационных потоков АСУ ТП, основанные на предыдущем исследовании [1]. Выявлены ключевые уязвимости протоколов Modbus, OPC_UA, включая MITM-атаки и компрометацию сертификатов. Начальные эксперименты на усовершенствованном стенде показали временные задержки. Дальнейшие исследования будут посвящены разработке и внедрению LSTM, стандартов ISA IEC62443, блокчейн-технологиям и цифровым двойникам.

Ключевые слова: АСУ ТП, информационная безопасность, Modbus, OPC UA, деревья атак, CVSS, LSTM, MITM, DoS, сетевая атака, киберугроза, промышленный протокол, блокчейн.

Введение. Современные автоматизированные системы управления технологическими процессами (АСУ ТП) — это важная составляющая любой промышленности, обеспечивающая непрерывность работы критически важных объектов. Однако, как и человеческий организм, они подвержены «инфекциям» в виде киберугроз. Одним из ярких примеров является программа Stuxnet, атаковавшая промышленные системы управления в Иране в 2010 году. Этот вирус нарушил работу центрифуг на ядерном объекте, что наглядно демонстрирует масштаб последствий таких атак [2]. Системы АСУ ТП являются ключевым элементом критической инфраструктуры в энергетике, нефтегазовой отрасли и других секторах экономики. Их интеграция с инженерными сетями и корпоративными ЛВС значительно повышает риски внешнего вмешательства. Например, атаки на энергосистему в Европе 2015 г. [3] и сбои в энергетике Венесуэлы в 2019 г. [4] продемонстрировали, что компрометация промышленных протоколов, таких как Modbus и OPC UA, может привести к катастрофическим последствиям. Это указывает на потенциальную уязвимость АСУ ТП к кибервоздействию. По данным отчета Kaspersky ICS CERT за 2023 год, зафиксирован рост количества инцидентов, в которых активно эксплуатировались уязвимости Modbus и OPC UA [5,6].

Согласно Li et al (2019), метод деревьев атак позволяет структурировать многошаговые сценарии вторжений и формализовать угрозы. Zhao et al (2022) применили LSTM-сети для анализа временных рядов телеметрии в АСУ ТП, обнаружив высокую эффективность в выявлении скрытых аномалий. Davidson и Mustard (2017) указали на возможности блокчейн-технологий для проверки целостности программного обеспечения в промышленных контроллерах. В рамках SCADA-тестбенча, разработанного Teixeira et al (2018), была продемонстрирована применимость методов машинного обучения для обнаружения атак в реальном времени [7-9].

При этом традиционные подходы, основанные на общих требованиях ISO/IEC 27001 и NIST SP 800-82, не охватывают в полной мере специфику уязвимостей промышленных протоколов. Стандарты ISA/IEC 62443 позволяют систематизировать требования к защите компонентов АСУ ТП, но требуют адаптации к конкретным реалиям [10-12].

В рамках предыдущего исследования, описанном в [1], был разработан стенд для анализа атак на систему пожарной сигнализации, интегрированной с инженерными сетями. На основе стенда, изначально предназначенного для анализа поведения компонентов системы пожарной сигнализации в штатном режиме, реализована полноценная платформа для исследования протекающих процессов в АСУ ТП. Однако научный пробел заключается в отсутствии комплексной методологии, объединяющей анализ уязвимостей протоколов Modbus/OPC UA, машинное обучение и блокчейн-технологии для защиты АСУ ТП.

Проблема исследования. Современные АСУ ТП представляют собой сложные гибридные сети промышленной и корпоративной инфраструктуры. С одной стороны, преднамеренная эксплуатация уязвимостей в протоколах Modbus/OPC_UA приводит к прямым нарушениям функций АСУ: например, удаленная подмена управляющих регистров или DoS-атаки приводят к сбоям и авариям. С другой стороны, существующие методы оценки безопасности не учитывают полностью поведение промышленного оборудования и особенности работы контроллеров [13].

Протокол Modbus, несмотря на широкое распространение, не обеспечивает встроенной аутентификации и шифрования. Это делает возможными атаки типа Man-In-The-Middle (MITM), подмену управляющих команд и перехват данных. Протокол OPC UA предусматривает TLS-шифрование и управление сертификатами, однако ошибки в конфигурации могут привести к сбоям и отказам соединения. Кроме того, стандартные инструменты мониторинга не фиксируют некритичные аномалии, возникающие до наступления отказов [14].

Цель настоящей работы — разработать и проверить комплексную методологию анализа угроз информационных потоков в АСУ ТП на примере атак на Modbus и OPC UA.

Научная задача заключается в формализации уязвимостей информационных потоков, построении моделей атак, количественной оценке их критичности и реализации автоматического обнаружения аномалий на основе анализа телеметрии.

Материалы и методы. Работа по методологии анализа угроз выполняется на специализированном лабораторном стенде, включающем программируемый логический контроллер с интерфейсами Modbus TCP и OPC UA, операторскую станцию таких как (HMI и SCADA-сервер). Стенд соединен в локальную сеть и оснащен физическим макетом технологической установки для воспроизведения динамики процесса. Планируется моделирование атак через виртуальные машины, включающие сценарии:

- MITM-атаки на Modbus с перехватом и подменой регистров;
- DoS-атаки на Modbus TCP с насыщением канала запросами;
- Спуфинг сертификатов OPC UA посредством подмены TLS-ключей.

Для формализации угроз будут использоваться деревья атак (Attack Trees), где корень дерева соответствует цели злоумышленника, а ветви — последовательным шагам атаки. Оценка критичности выявленных уязвимостей планируется по шкале CVSS v3.1 с учетом базовых и временных метрик [10].

Для динамического обнаружения аномалий планируется внедрение LSTM-модели: двухслойной сети по 128 нейронов с оптимизацией Adam и learning rate 0,001. Модель будет обучаться на данных штатной работы стенда, после чего аномалии будут фиксироваться при превышении порога ошибки прогноза (MSE > 3q) [15]. Во время последующих экспериментальных этапов будут регистрироваться следующие показатели:

- средняя задержка отклика контроллера (мс);
- доля неуспешных операций (% отказов);
- точность и полнота работы LSTM (Precision, Recall, F1-score).

Результаты. В ходе текущего этапа исследования разработана экспериментальная лабораторная установка, имитирующая автоматизированную систему управления технологическим процессом. В ее состав входят программируемый логический контроллер, SCADA-система и специализированный модуль генерации атак [16,17]. На подготовленном тестовом стенде воспроизводятся типовые технологические процессы, что дает возможность безопасно моделировать угрозы и регистрировать поведение системы при различных сценариях представлены в табл. 1. Такая инфраструктура позволяет гибко конфигурировать сетевые взаимодействия и собирать детальные телеметрические данные.

Таблица 1

Сценарии атак и последствия

Сценарий атаки	*Цель воздействия*	*Примененный метод*	*Предполагаемые последствия*
MITM (Modbus)	Перехват и искажение команд	Подмена пакетов управления	Некорректное выполнение управляющих команд
DoS (Modbus TCP)	Нарушение доступности	Перегрузка запросами	Задержки, отказ соединения с SCADA
Спуфинг (OPC UA)	Подрыв аутентификации	Подделка TLS-сертификатов	Разрыв сессии, сбои в обмене данными

На разработанной платформе реализованы несколько классических сценариев кибератак на АСУ ТП: атака типа «человек посередине» (MITM), атака «отказ в обслуживании» (DoS) и подмена сертификатов в инфраструктуре аутентификации. Каждый сценарий воспроизводится средствами лабораторного стенда с использованием реальных протоколов промышленных сетей. Например, MITM-атака направлена на перехват и модификацию команд управления, DoS-атака — на перегрузку сети ложным трафиком, а подмена сертификатов демонстрирует уязвимость системы аутентификации путем фальсификации цифровых ключей.

Параллельно осуществляется сбор телеметрических данных: регистрируются параметры сети, сигналы с датчиков и логи контроллера как в штатном режиме, так и во время атак. На основе полученного набора данных ведется обучение рекуррентной нейронной сети LSTM для обнаружения аномалий в поведении системы. Модель LSTM обучается на сценариях нормального функционирования, после чего проверяется на данных, полученных при проведении атак. Предварительный анализ обученной модели свидетельствует о ее способности выявлять аномальные паттерны в сетевом трафике и параметрах системы.

Методологическая база работы включает комбинирование деревьев атак, системы оценки уязвимостей CVSS и нейросетевого анализа. Деревья атак формализуют возможные пути компрометации системы, а CVSS позволяет количественно оценивать критичность выявленных уязвимостей. Совмещение этих подходов с анализом телеметрии через нейронные сети образует комплексную схему выявления угроз. Такое сочетание формальных моделей и обучаемых алгоритмов носит научно-инновационный характер, поскольку обеспечивает более полное описание и детекцию угроз в АСУ ТП.

На данном этапе сформирован исходный массив экспериментальных данных и разработаны алгоритмы предварительной обработки. В процессе первоначального анализа были выявлены характерные шаблоны отклонений для каждого сценария атаки, что подтверждает обоснованность выбранного подхода. Дальнейшие эксперименты с расширенным набором данных позволят уточнить выявленные закономерности и подтвердить эффективность LSTM-модели при раннем обнаружении аномалий. В совокупности проделанная работа демонстрирует, что предложенный методический комплекс может быть использован для повышения устойчивости информационных потоков в автоматизированных системах управления технологическими процессами.

Заключение. В настоящей работе выполнена разработка экспериментального каркаса и базовых методов анализа угроз в информационных потоках АСУ ТП. Построен лабораторный стенд с контроллером, SCADA и модулем генерации атак, реализованы ключевые сценарии угроз (MITM, DoS, подмена сертификатов). Это позволило сформировать набор телеметрических данных, необходимый для обучения и тестирования модели обнаружения аномалий. Предложенный методический подход, основанный на сочетании деревьев атак, оценки по CVSS и нейросетевого анализа, обеспечивает комплексное выявление угроз и представляет научную новизну [18].

Хотя экспериментальная работа продолжается, уже отмечается перспективность выбранного направления. Первичные результаты обучения сети LSTM свидетельствуют о возможности автоматизированной идентификации аномальных ситуаций в потоках данных АСУ ТП. Это подтверждает научную новизну исследования: комплексное объединение формальных моделей и методов глубинного обучения для обеспечения безопасности АСУ ТП. Разрабатываемые подходы демонстрируют потенциал практического применения и могут стать основой современных систем мониторинга и защиты промышленных объектов. Работа выполняется и будет продолжена в течение следующих двух лет. В ходе дальнейших исследований запланировано расширение экспериментальной платформы, накопление обширного массива данных и валидация предложенной модели на большем числе сценариев. Окончательные результаты исследования будут оформлены после проведения полного цикла испытаний, что позволит сформулировать конкретные рекомендации по повышению киберустойчивости АСУ ТП.

Перспективы. В ближайшей перспективе планируется существенное расширение исследований по анализу угроз в АСУ ТП. Будет завершено формирование полного корпуса экспериментальных данных и продолжено обучение нейросетевой модели с целью повышения точности обнаружения аномалий [19]. Также запланировано включение дополнительных сценариев атак и отказов, что позволит проверить универсальность и адаптивность предлагаемого подхода. Особое внимание уделяется адаптации методов к различным промышленным протоколам и реальному аппаратному обеспечению.

В течение следующих двух лет планируется завершить экспериментальную часть и подготовить практические рекомендации. Уникальность проекта определяется комплексным применением методик моделирования угроз и машинного обучения для повышения безопасности АСУ ТП. Полученные результаты могут быть использованы в системах мониторинга киберзащиты и интегрированы в реальные инженерные объекты, открывая новые возможности для предотвращения инцидентов и повышения надежности технологических процессов.

СПИСОК ЛИТЕРАТУРЫ

1. Афсахов З. Н. Стенд для имитации штатной и аварийной работы системы пожарной сигнализации при вмешательстве злоумышленника / З. Н. Афсахов, А. А. Оленников // Математическое и информационное моделирование: материалы Всероссийской конференции молодых ученых. — Тюмень, Тюменский государственный университет, 2024. — С. 287-293.
2. Пачеко Ж. Структура безопасности для конечных узлов интернета вещей с нейронными сетями / Ж. Пачеко, В. Х. Бенитес, Ж. Пан. // Международный журнал машинного обучения и вычислений. — 2019. — Т. 9. — С. 381-386.
3. Уайтхед Д. Е. Украина, кибериндуцированное отключение электроэнергии: анализ и практические стратегии смягчения последствий в 2017 году / Д. Е. Уайтхед, К. Оуэнс, Д. Гаммел, Дж. Смит // 70-я ежегодная конференция инженеров защитных реле (CPRE). — Москва : МЭИ, 2017. — С. 1-8.
4. ISA/IEC 62443: Industrial automation and control systems security.
5. Kaspersky ICS CERT. Attacks on industrial sector hit record in second quarter of 2023. Press release (13 Sept. 2023).
6. Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2023 Kaspersky ICS CERT2023.Report (19 март 2024).
7. Li, E., Kang, C., Huang, D., Hu, M., Chang, F., He, L., & Li, X. (2019). Quantitative model of attacks on distribution automation systems based on CVSS and attack trees. Information, 10 (8), 251.
8. Zhao, X., Zhang, L., Cao, Y., Jin, K., & Hou, Y. (2022). Anomaly detection approach in industrial control systems based on measurement data. Information, 13 (10), 450.
9. Davidson M., Mustard S. Will blockchain technology disrupt the ICS world? ISA InTech, 2017.
10. ISO/IEC 27001:2022. Information Security Management Systems — Requirements.
11. NIST SP 800-82 Rev.2. Guide to Industrial Control Systems Security. NIST, 2015.
12. IEC 62443-3-3:2013. Industrial communication networks — System security requirements.
13. Исследование: более 4 000 устройств АСУ ТП уязвимы для удаленных атак.. — 2021. — URL: https://www.infowatch.ru/resources/blog/issledovanie-bolee-4-000-ustroystv-asu-tp-uyazvimy-dlya-udalennykh-atak (дата обращения: 16.04.2024)
14. Промышленные компании: векторы атак. — 2018. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/ (дата обращения: 12.04.2025).
15. Цифровые технологии и проблемы информационной безопасности / под ред. Е. В. Стельмашонок, И. Н. Васильевой. — Санкт-Петербург : Изд-во СПбГЭУ, 2021. — 163 с. ISBN 978-5-7310-5243-6
16. Teixeira M.A., Salman T., Zolanvari M. et al. SCADA System Testbed for Cybersecurity Research. Future Internet. — 2018. — 10(12). — P76.
17. Dragos Inc. FrostyGoop malware using Modbus TCP. Industrial Cyber, 2024.
18. Назначение и задачи SCADA-систем. — 2020. — URL: https://www.tadviser.ru/index.php/Статья:SCADA_назначение_систем (дата обращения: 16.04.2025).
19. Захаров А. А., Оленников А. А., Любушкина Д. Н. «Алгоритм проверки подлинности исполнительных устройств в автоматизированных системах управления технологическим процессом» // «Динамика систем, механизмов и машин». — 2023. — Т. 11, № 4.