УДК 004.056:681.5

***Алиев Омар Гамзатович, бакалавр***

*Нижегородский государственный технический университет им. Р.Е. Алексеева, г. Нижний Новгород.*

***Говяжова Софья Александровна*, бакалавр**

*Нижегородский государственный технический университет им. Р.Е. Алексеева, г. Нижний Новгород.*

***Поманисточка Тихон Александрович*, бакалавр**

*Нижегородский государственный технический университет им. Р.Е. Алексеева, г. Нижний Новгород.*

# БЕЗОПАСНОСТЬ MODBUS/TCP В ИНФРАСТРУКТУРЕ INDUSTRY 4.0: УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ

***Аннотация.*** *Предметом исследования является защищённость обмена данными по протоколу Modbus/TCP в промышленных сетях, объектом — сегмент автоматизированной системы управления технологическим процессом, построенный на этом протоколе. Применялись анализ спецификации протокола, систематизация угроз по уровням архитектуры АСУ ТП, риск-ориентированная оценка мер защиты и экспериментальная проверка на лабораторном стенде. Показано, что основные угрозы порождаются свойствами самого протокола: отсутствием аутентификации сторон, контроля целостности и защиты от повторного воспроизведения запросов. Предложен эшелонированный набор мер, предложена оценка его результативности и показано, что суммарная вносимая задержка остаётся в пределах допустимого времени цикла опроса.*

***Ключевые слова:*** *Modbus/TCP, промышленные сети, АСУ ТП, информационная безопасность, модель угроз, сегментация сети, глубокий разбор пакетов, критическая информационная инфраструктура.*

# MODBUS/TCP SECURITY IN THE INDUSTRY 4.0 INFRASTRUCTURE: THREATS AND PROTECTION METHODS

***Abstract.*** *The subject of the study is the security of Modbus/TCP data exchange in industrial networks; the object is a process control system segment built on this protocol. Analysis of the protocol specification, systematization of threats by the levels of the control system architecture, risk-based assessment of protection measures and experimental verification on a laboratory testbed were applied. The main threats are shown to originate from the properties of the protocol itself: the absence of party authentication, integrity control and replay protection. A defence-in-depth set of measures is proposed together with an assessment of its effectiveness, and the total introduced delay is shown to remain within the permissible polling cycle time.*

***Key words:*** *Modbus/TCP, industrial networks, process control system, information security, threat model, network segmentation, deep packet inspection, critical information infrastructure.*

**Актуальность исследования**

Modbus остаётся одним из наиболее распространённых протоколов промышленной автоматизации: он прост в реализации, нетребователен к вычислительным ресурсам и поддерживается практически всеми производителями контроллеров. Вариант Modbus/TCP переносит исходный формат кадра в стек TCP/IP без изменения структуры, из-за чего протокол, разработанный для изолированной последовательной линии, оказывается в маршрутизируемой сети.

В инфраструктуре Industry 4.0 технологический сегмент перестаёт быть изолированным: данные с контроллеров передаются в системы предиктивной аналитики, а промышленные протоколы соседствуют с протоколами промышленного интернета вещей [6, с. 18]. Требования к защите таких систем закреплены Федеральным законом № 187-ФЗ [1] и приказом ФСТЭК России № 31 [2], терминология и модель зон и каналов — ГОСТ Р 56205-2014 [3].

Практика показывает, что выполнение этих требований для сегмента с Modbus/TCP требует компенсирующих мер, поскольку сам протокол средств защиты не содержит.

**Обзор научной литературы по теме статьи**

Вопросы защиты промышленных сетей рассматриваются по трём направлениям. Первое — сопоставление протоколов промышленного интернета вещей по поддерживаемым механизмам безопасности: в [6, с. 22] показано, что применение SSL/TLS и механизмов аутентификации существенно различается между AMQP, MQTT, CoAP и DDS, а часть протоколов опирается на защиту транспортного уровня.

Второе — механизмы аутентификации при взаимодействии компонентов: в [4, с. 150] разобраны схемы межсервисной аутентификации, применимые и к промышленному контуру, если рассматривать контроллер как сервис с ограниченным набором операций. Третье — инструментальный контроль защищённости: в [5, с. 19] описано применение сканера уязвимостей, в [7, с. 45] — многоуровневый подход к валидации входных данных и изоляции обработчиков. Работы, посвящённые непосредственно Modbus/TCP, чаще ограничиваются перечислением уязвимостей без оценки того, какой ценой достигается их нейтрализация в действующем контуре.

**Постановка проблемы исследования**

Объектом исследования выступает сегмент АСУ ТП, построенный на протоколе Modbus/TCP, предметом — угрозы безопасности информации, обусловленные свойствами протокола, и меры их нейтрализации.

Проблема заключается в противоречии между требованиями регуляторов [1, 2] и возможностями протокола. Modbus/TCP не предусматривает аутентификации сторон, контроля целостности сообщений, шифрования и защиты от повторного воспроизведения запросов, а смена протокола на защищённый вариант возможна не всегда: парк контроллеров обновляется медленно. Задачи исследования: систематизировать угрозы по

уровням архитектуры АСУ ТП; сформировать набор мер защиты; предложить оценку его результативности; экспериментально определить вносимую задержку и проверить её допустимость.

**Описание и обоснование методологии исследования**

Систематизация угроз выполнена по уровням архитектуры АСУ ТП (рис. 1). Каждому уровню поставлены в соответствие характерные угрозы, а для сетевого уровня дополнительно указано свойство протокола, делающее угрозу возможной (таблица 1). Перечень сформирован на основе спецификации протокола и терминологии ГОСТ Р 56205-2014 [3].

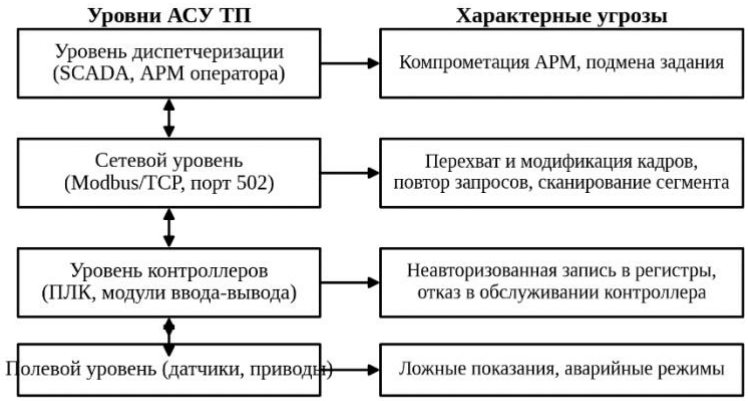


**Рис. 1. Уровни архитектуры АСУ ТП и характерные для них угрозы**

**Таблица 1. Угрозы Modbus/TCP и порождающие их свойства протокола**

| Угроза | Свойство протокола | Последствие |
|---|---|---|
| Подмена управляющей команды | Отсутствие аутентификации сторон | Изменение состояния объекта |
| Модификация данных в передаче | Отсутствие контроля целостности | Ложная картина процесса |
| Повторное воспроизведение запроса | Отсутствие меток свежести | Незапланированное срабатывание |
| Раскрытие технологических данных | Передача в открытом виде | Разведка перед воздействием |
| Обнаружение устройств в сегменте | Фиксированный порт 502 | Составление карты сети |
| Отказ в обслуживании контроллера | Отсутствие ограничения интенсивности | Потеря управления |

Оценка защищённости строится на риск-ориентированном подходе. Совокупный риск сегмента до внедрения мер определяется как

$$R = \Sigma\, p_i \cdot u_i, \qquad (1)$$

где $p_i$ — вероятность реализации i-й угрозы; $u_i$ — ущерб от неё. Введение мер защиты снижает вероятность реализации, но не обнуляет её, поэтому остаточный риск записывается в виде

$$R_{ост} = \Sigma\, p_i \cdot (1 - k_i) \cdot u_i, \qquad (2)$$

где $k_i \in [0, 1]$ — коэффициент результативности совокупности мер, применённых против i-й угрозы. Результативность набора мер оценивается относительным снижением риска

$$E = (R - R_{ост}) / R. \qquad (3)$$

Меры защиты нельзя выбирать по одному лишь критерию (3): каждая из них вносит дополнительную задержку в цикл опроса, а технологический процесс задаёт предельно допустимое время реакции. Отсюда ограничение

$$\Sigma\, \Delta t_j \le T_{доп} - T_{баз}, \qquad (4)$$

где $\Delta t_j$ — задержка, вносимая j-й мерой; $T_{баз}$ — базовое время цикла опроса без средств защиты; $T_{доп}$ — допустимое время цикла. Совместное применение (3) и (4) позволяет отбирать меры по результативности при соблюдении требований реального времени. Эшелонированная схема защиты, принятая в работе, приведена на рис. 2.

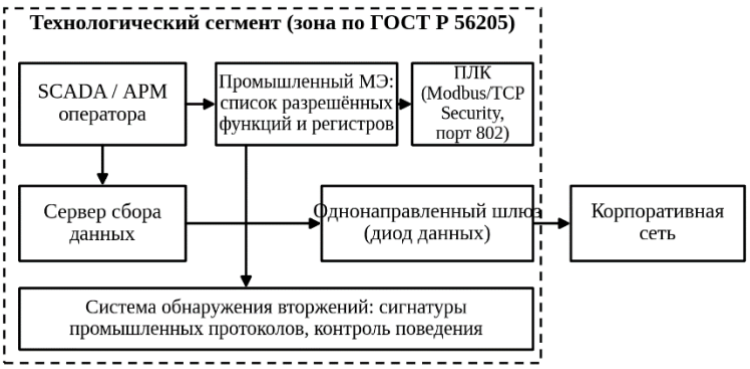


**Рис. 2. Эшелонированная схема защиты сегмента с протоколом Modbus/TCP**

## Результаты исследования

Проверка выполнена на лабораторном стенде: рабочая станция со SCADA-пакетом, два программируемых логических контроллера с

интерфейсом Modbus/TCP, управляемый коммутатор, промышленный межсетевой экран с разбором прикладного протокола и система обнаружения вторжений в режиме зеркалирования трафика. Базовое время цикла опроса составило $T_{баз} = 42$ мс при допустимом $T_{доп} = 100$ мс.

Меры защиты вводились последовательно с измерением вносимой задержки. Сегментация сети и разделение зон средствами управляемого коммутатора задержки не вносят. Списки контроля доступа на межсетевом экране добавили 0,4 мс, разбор прикладного протокола с проверкой допустимых кодов функций и диапазонов регистров — 1,8 мс, туннелирование обмена по TLS в соответствии со спецификацией Modbus Security [8] — 6,5 мс, система обнаружения вторжений в режиме зеркалирования — 0 мс. Суммарная задержка составила 8,7 мс, то есть 15 % от имеющегося резерва в 58 мс, что удовлетворяет условию (4).

Коэффициенты результативности $k_i$ назначались экспертно по трёхуровневой шкале с учётом того, какие меры перекрывают каждую угрозу. Итоговые значения приведены в таблице 2.

**Таблица 2. Меры защиты, нейтрализуемые угрозы и вносимая задержка**

| Мера защиты | Основные нейтрализуемые угрозы | Δt, мс |
|---|---|---|
| Сегментация сети и разделение зон | Обнаружение устройств, разведка | 0 |
| Списки контроля доступа | Подключение посторонних узлов | 0,4 |
| Разбор прикладного протокола | Подмена команды, отказ в обслуживании | 1,8 |
| Туннелирование по TLS (Modbus Security) | Модификация и раскрытие данных, повтор | 6,5 |
| Обнаружение вторжений | Все классы (выявление, не блокирование) | 0 |
| Итого | — | 8,7 |

Расчёт по формулам (1)–(3) при принятых значениях $p_i$, $u_i$ и $k_i$ дал результативность набора $E = 0{,}79$. Наибольший вклад в снижение риска вносит переход на защищённый вариант протокола, наименьший — списки контроля доступа, действующие только против внешних подключений. При

невозможности обновления контроллеров до Modbus Security результативность снижается до E = 0,52, что показывает, насколько сегмент зависит от свойств самого протокола.

**Обсуждение результатов исследования и выводы**

Защищённость сегмента с Modbus/TCP определяется прежде всего компенсирующими мерами сетевого уровня, а не настройками самих контроллеров. Переход на Modbus Security с аутентификацией по сертификатам X.509 и ролевым разграничением доступа [8] закрывает большую часть угроз, но требует обновления оборудования, поэтому в переходный период сегментация и разбор прикладного протокола остаются основными инструментами. Аналогичный вывод о переносе функций безопасности на транспортный уровень сделан при сравнении протоколов промышленного интернета вещей [6, с. 23].

Ограничением работы является экспертный характер оценок $p_i$, $u_i$ и $k_i$: формулы (1)–(3) дают сопоставимые между собой, но не абсолютные значения риска, поэтому применимы для сравнения вариантов защиты, а не для нормирования. Измерения выполнены на стенде с двумя контроллерами; при увеличении числа устройств вклад разбора прикладного протокола будет расти.

Таким образом, систематизированы угрозы Modbus/TCP по уровням архитектуры АСУ ТП с указанием порождающих их свойств протокола, предложен эшелонированный набор мер защиты и критерии его выбора (3)–(4). Экспериментально показано, что полный набор мер вносит 8,7 мс задержки при резерве 58 мс и обеспечивает расчётную результативность E = 0,79. Дальнейшее развитие работы связано с уточнением коэффициентов результативности по данным реальных инцидентов и с оценкой масштабируемости решения на сегменты с десятками устройств.

СПИСОК ЛИТЕРАТУРЫ

1. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : приказ ФСТЭК России от 14.03.2014 № 31. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения: 19.08.2026).

3. ГОСТ Р 56205-2014/IEC/TS 62443-1-1:2009. Сети коммуникационные промышленные. Защищённость (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. М.: Стандартинформ, 2015.

4. Зимина К. И., Лапонина О. Р. Механизмы межсервисной аутентификации в приложениях с микросервисной архитектурой // International Journal of Open Information Technologies. 2023. Т. 11. № 5. С. 146–154. URL: http://injoit.org/index.php/j1 (дата обращения: 19.08.2026).

5. Лапонина О. Р., Малаховский С. А. Использование сканера уязвимостей ZAP для тестирования веб-приложений // International Journal of Open Information Technologies. 2017. Т. 5. № 8. С. 17–26. URL: http://injoit.org/index.php/j1/article/view/466 (дата обращения: 19.08.2026).

6. Селезнев С., Яковлев В. Архитектура промышленных приложений IoT и протоколы AMQP, MQTT, JMS, REST, CoAP, XMPP, DDS // International Journal of Open Information Technologies. 2019. Т. 7. № 5. С. 17–28. URL: http://injoit.org/index.php/j1/article/view/737 (дата обращения: 19.08.2026).

7. Эхлаков О. Системный подход к безопасности пользовательских файлов: от первичной валидации до изоляции в Docker // International Journal

of Open Information Technologies. 2025. Т. 13. № 9. С. 43–49. URL: http://injoit.org/index.php/j1/article/view/2212 (дата обращения: 19.08.2026).

8. MODBUS/TCP Security Protocol Specification. Modbus Organization, 2018. URL: https://modbus.org/specs.php (дата обращения: 19.08.2026).