

АНАЛИЗ УЯЗВИМОСТЕЙ АСУ ТП НА ПРИМЕРЕ РАБОТЫ ПРОТОКОЛА MODBUS

Лазарев Т.П., Устинов С.А., студенты 5 курса факультета безопасности

Научный руководитель – Новохрестов А.К., кандидат технических наук, доцент

ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники»

Ключевые слова: Уязвимости, АСУ ТП, протокол ModBus, кибербезопасность, анализ безопасности.

Исследование фокусируется на анализе уязвимостей АСУ ТП. Оценка потенциальных атак предоставляет важные выводы о рисках, связанных с использованием протокола ModBus. Полученные результаты интересны для исследователей, разработчиков и специалистов в области кибербезопасности промышленных управляющих систем.

Введение. Автоматизированная система управления технологическим процессом (АСУ ТП) представляет собой информационную систему, основной задачей которой является управление различными производственными процессами. Система включает в себя множество модулей, ответственных за регулирование различных параметров производства, планирование и оптимизацию рабочих процессов, а также за другие компоненты, необходимые для эффективного управления технологическими процессами.

Цель работы. В контексте работы АСУ ТП, особую роль занимают протоколы связи, используемые в системах автоматизации, определяя не только эффективность передачи данных, но и защищенность производственных процессов [1]. Таким образом цель исследования заключается в оценке влияния протокола ModBus на защищенность АСУ ТП.

Результат исследования: Протокол ModBus, является одним из самых распространенных промышленных протоколов, выступающий ключевой единицей в процессах автоматизации технологических процессов. Основными преимуществами данного протокола является его простота и доступность, однако с ростом его популярности, возрастают и риски угрозы безопасности, с которыми системы автоматизации, использующие протокол ModBus, могут столкнуться.

Несмотря на широкое распространение протокол ModBus не обладает какими-либо механизмами безопасности, что делает его подверженным разнообразным атакам. Ключевым недостатком данного протокола является отсутствие механизмов аутентификации и шифрования данных, что оставляет передаваемую информацию под угрозой перехвата и модификации злоумышленниками.

Еще одним значимым упущением является открытый доступ к устройствам в многих системах, применяющих протокол ModBus, что увеличивает риск несанкционированного доступа и возможность воздействия на управление системами [2]. В силу того, что протокол не обеспечивает контроля доступа или защиты параметров, злоумышленники могут легко вносить изменения в настройки устройств, включая их функциональные особенности, что может привести к серьезным последствиям для промышленных систем. Данный фактор усиливает риски и подчеркивает необходимость принятия эффективных мер по обеспечению безопасности в системах, использующих протокол ModBus.

Применение эффективных стратегий для усиления кибербезопасности в системах, основанных на протоколе ModBus, выступает неотъемлемой частью обеспечения надежной защиты автоматизированных систем управления технологическим процессом. Анализируя уязвимости и риски, связанные с протоколом ModBus, есть необходимость в рекомендациях, которые должны быть направлены на усиление защиты систем, а именно определение сценариев атак и угроз, адаптированных к особенностям протокола, разработку мер по обнаружению и предотвращению попыток несанкционированного доступа, а также формирование рекомендаций по настройке системы для минимизации уязвимостей.

Комплексный анализ воздействия протокола ModBus на ключевые аспекты кибербезопасности АСУ ТП позволяет рассматривать вопросы целостности, доступности и конфиденциальности данных, выделяя возможные уязвимости и риски, связанные с использованием этого протокола.

Детальный анализ целостности данных позволяет определить уровень доступности данных, выявляя уязвимости и риски, связанные с пропускной способностью и эффективностью передачи данных в протоколе ModBus. Примерами могут служить анализ методов шифрования, механизмов контроля доступа и возможных сценариев нарушения целостности данных в использовании протокола ModBus [3].

Кроме того, анализ эффективности передачи данных, задержек при запросах и возможных сценариев отказов, которые могут повлиять на функциональность АСУ ТП, позволяет оценить потенциальные последствия атак и уязвимостей, связанных с протоколом ModBus, для промышленных процессов. Влияние атак на работоспособность и безопасность системы управления, а также возможные экономические и производственные потери, могут привести к таким ситуациям, как отказ в обслуживании (DoS) или вмешательство в параметры промышленных процессов. Такой глубокий анализ позволяет лучше понять и минимизировать риски, связанные с использованием протокола ModBus в промышленных управляющих системах.

В результате выявленного обширного спектра уязвимостей, характерных для протокола ModBus, необходимо провести повышение уровня безопасности данного протокола [4]. Эффективное усиление безопасности Modbus требует использования дополнительных механизмов аутентификации и шифрования данных, представляя собой существенный компонент в стратегии обеспечения надежной защиты передаваемой информации. Разработчикам и администраторам рекомендуется рассмотреть возможность интеграции протоколов виртуальных частных сетей (VPN) и внедрение дополнительных слоев шифрования с целью максимального обеспечения конфиденциальности данных.

Важнейшей частью обеспечения безопасности промышленных систем является строгий контроль как физического, так и логического

доступа к устройствам, использующим протокол Modbus. Данный аспект может быть успешно реализован через внедрение современных брандмауэров, активное использование технологий виртуальных частных сетей (VPN) и применение других передовых методов сетевой безопасности.

Высокую значимость представляет регулярный мониторинг сети и выявление аномального поведения, что играет ключевую роль в предотвращении атак и обеспечении оперативной реакции на них. Введение в действие специализированных систем мониторинга безопасности становится критически важным этапом в процессе обеспечения эффективной и всесторонней защиты [5].

Следующим важным шагом в стратегии минимизации рисков, связанных с уязвимостями протокола Modbus, является систематическое обучение персонала по вопросам безопасности и регулярное обновление программного обеспечения устройств. Эта комплексная стратегия направлена на снижение вероятности возникновения проблем и обеспечение стабильной и защищенной среды, что особенно важно в контексте научных исследований, целью которых является обеспечение безопасности и стабильности протокола Modbus.

Оценка воздействия протокола на целостность, доступность и конфиденциальность данных подчеркивает, что безопасность передаваемой информации является крайне важным аспектом. Исследование механизмов шифрования и аутентификации выявило пробелы, требующие дополнительных улучшений для обеспечения надежной защиты данных.

Заключение. Рекомендации, вытекающие из исследования, включают в себя:

1. Использование дополнительных механизмов аутентификации и шифрования. Применение протоколов VPN для защиты передаваемой информации, добавление слоев шифрования данных.
2. Ограничение физического и логического доступа. Внедрение брандмауэров для контроля доступа, использование механизмов идентификации и аутентификации, а также средств обнаружения вторжения

3. Регулярный мониторинг сети и обнаружение аномального поведения. Проведение систематического мониторинга сети, Внедрение систем противодействия вредоносным программам

4. Внедрение системы мониторинга безопасности. Разработка и внедрение системы безопасности, быстрое реагирование на обнаруженные аномалий или атак.

5. Регулярное обучение персонала по безопасности и обновление ПО. Проведение регулярных тренингов по безопасности для персонала, обеспечение регулярного обновления программного обеспечения устройств.

Данное исследование выявило не только проблемы и риски, но также предоставило конструктивные рекомендации. Создание устойчивых, безопасных и инновационных промышленных систем требует совокупного усилия и внедрения передовых технологий, и данное исследование предоставляет базу для дальнейших разработок в области кибербезопасности промышленных управляющих систем.

В дальнейшем результаты работы могут быть использованы:

1. Разработчиками систем для улучшения безопасности;
2. Специалистами по кибербезопасности для обучения и разработки стратегий;
3. Предприятиями для осознания рисков, образовательными учреждениями для обучения

Таким образом, статья представляет важный источник информации для улучшения безопасности в промышленных автоматизированных системах.

Библиографический список:

1. Линьков В.А. Информационная безопасность АСУ ТП: Централизованные АСУ ТП. Состав и структура АСУ ТП. [Электронный ресурс] – Режим доступа: https://elibrary.ru/download/elibrary_41676106_81055123.pdf
2. Боровков Н.А., Афанасьев М.М. Протоколы ModBus: Разработка системы для автоматизации сбора и отправки данных ModBus-устройств [Электронный ресурс] - Режим доступа: <https://elibrary.ru/item.asp?id=41146775>

3. Калинин Я.В., Тутов И.А. Протокол ModBus: Модуль информационной безопасности в сетях Modbus RTU [Электронный ресурс] - Режим доступа: <https://elibrary.ru/item.asp?id=50494222>

4. Узбеков И. Протокол ModBus: Протокол ModBus [Электронный ресурс] – Режим доступа: https://elibrary.ru/download/elibrary_39178739_82310311.pdf

5. Концепция сетевой безопасности в автоматизированных системах управления технологическим процессом (АСУ ТП) [Электронный ресурс] – Режим доступа: https://elibrary.ru/download/elibrary_42499155_84031045.pdf

VULNERABILITY ANALYSIS OF ACS TP USING THE MODBUS PROTOCOL AS AN EXAMPLE SYSTEM

Ustinov S.A., Lazarev T.P.

Scientific supervisor – Novokhrestov A.K.

Tomsk State University of Control Systems and Radioelectronics

Keywords: *Vulnerabilities, automated control systems, ModBus protocol, cybersecurity, security analysis.*

The study focuses on the analysis of automated process control system vulnerabilities. Evaluating potential attacks provides important insights about the risks associated with using the ModBus protocol. The results obtained are of interest to researchers, developers and specialists in the field of cybersecurity of industrial control systems.