РАЗРАБОТКА КОМПОНЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОНТРОЛЛЕРНОГО ОБОРУДОВАНИЯ

Я.В. Калинкин, студент гр. 8Т8Б,
И.А. Тутов, ст. преподаватель
Томский политехнический университет
E-mail: yvk36@tpu.ru

Введение

Ежегодно увеличивается доля предприятий, использующих автоматизированные системы управления технологическим процессом (АСУ ТП), и каждую АСУ необходимо обеспечивать средствами информационной безопасности. Согласно статистике лаборатории Касперского, в четвертом квартале 2021 года на территории РФ только на 20.86% компьютеров АСУ были заблокированы вредоносные объекты, причем динамика отрицательная, поскольку в первом квартале данный показатель был равен 31.75%. Также важным показателем является процент атакованных компьютеров АСУ в нефтегазовой отрасли – в 2017 г. данный показатель составил 26.4% [1].

Подобные кибератаки угрожают таким информационным свойствам АСУ, как конфиденциальность, целостность и доступность, причем в данном случае наиболее остро стоит вопрос нарушения целостности информации, т.е. данные и параметры технологического процесса могут изменить лица, не имеющие на это права. Данные свойства АСУ обозначены в приказе ФСТЭК №31 от 14 марта 2014 г. [2].

Примерами последствий успешных кибератак на комплексы АСУ являются отключение злоумышленниками теплоснабжения в финском городе Лаппеэнранта и отключение коммунальных услуг в Мичигане (США) в 2016 году.

Таким образом, целью работы является разработка устройства, позволяющего отслеживать сетевой трафик и состав запросов сетей АСУ ТП и предотвращать вторжения в них.

Концепция разработки

Были проанализированы существующие средства информационной безопасности АСУ. Наиболее известными решениями отечественного рынка являются продукты Kaspersky Industrial CyberSecurity («Лаборатория Касперского»), Industrial Security Incident Manager (Positive Technologies), DATAPK («Уральский Центр Систем Безопасности»). По изучении принципа работы данных программно-аппаратных комплексов был сделан вывод, что на уровне технологических сетей и прикладного уровня протоколов взаимодействия ведется неинтрузивное инспектирование трафика сетей и оценка содержимого фреймов протоколов, однако это оставляет опасность проникновения злоумышленника к управляемому ПЛК и при знании модели и конфигурации контроллера позволяет получить доступ к данным технологического процесса, либо позволяет выяснить конфигурацию устройства с помощью диагностических команд [3].

Таким образом, был сформирован следующий принцип работы устройства для отслеживания сетевого трафика: в линию связи между контроллерным оборудованием и станцией оператора АСУ устанавливается устройство, выполняющее анализ и фильтрацию потока данных, поступающих от станции оператора к контроллерному оборудованию и уведомляющее о нарушении режима функционирования или вторжении в сеть по другому интерфейсу (предполагается также трансляция уведомлений на компьютер специалиста по информационной безопасности).

Для первоначальной разработки был принят протокол взаимодействия Modbus RTU, поскольку данный протокол позволяет объединять до 247 ведомых устройств, имеет открытую структуру и стандарты, а также поддерживается большинством современных ПЛК [4].

Первым этапом разработки программной части была реализация передачи данных посредством универсального асинхронного приемопередатчика (УАПП, UART) между ПК и микроконтроллером AVR ATmega16 с использованием системы прерываний.

Следующим шагом была реализация приема и передачи сообщений формата Modbus RTU. Протокол поддерживает такие функции, как чтение дискретных входов, чтение состояния релейных выходов, запись состояния одного или нескольких релейных выходов, чтение регистров данных, а

также чтение и запись файла. Первоначально было принято решение реализовать функцию записи одного релейного выхода.

Для разработки программной части используется IDE Microchip Studio, а для отладки и тестирования вариантов прошивки МК используются САПР Proteus и программа-терминал 1.9b. Для симуляции запросов ведущего устройства используется программа Modbus Poll.

При получении и успешной обработке фрейма ведомое устройство должно отвечать «эхом», т.е. фреймом, аналогичным запросу. При получении фрейма, данные в котором не поддерживаются разрабатываемым устройством, т.е. не соответствуют уставке, загруженной в МК, микроконтроллер отвечает соответствующим сообщением («Обращение к незадействованному устройству», «Обращение к незадействованному регистру» и т.д.). На рисунках 1 и 2 приведены примеры корректного и некорректного запросов и соответствующих им ответов.

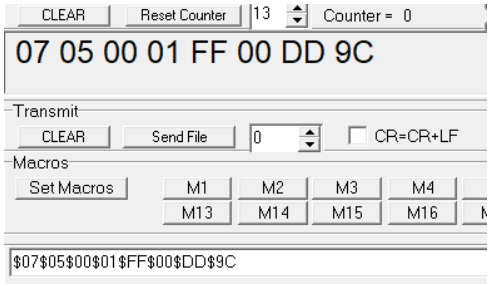

Рис. 1. Ответ «эхо» на допустимую команду записи состояния одного релейного выхода.

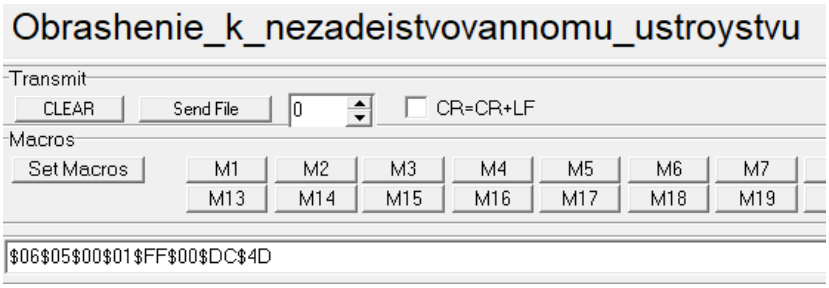

Рис. 2. Ответ устройства на запрос к незадействованному устройству.

Таким образом, на некорректный с точки зрения уставки запрос устройство отвечает соответствующим сообщением.

В дальнейших планах работы над устройством стоят использование МК с расширенными аппаратными возможностями (два аппаратных UART и увеличенный объем памяти программ), разработка экранной формы для компьютера специалиста по информационной безопасности, а также разработка сценария, при котором МК определяет последовательность некорректных запросов как нежелательную активность в сети.

Список использованных источников

1. Kaspersky ICS CERT. Статистика. [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/statistics/ (дата обращения 27.02.22).
2. Приказ ФСТЭК России от 14 марта 2014 г. N 31. [Электронный ресурс]. URL: https://fstec.ru/index?id=868:prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения 27.02.22).
3. Небайкин М. Кибербезопасность АСУ ТП. Обзор специализированных наложенных средств защиты. [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Market_Analysis/ICS-security-review (дата обращения 27.02.22).
4. Интеллект модуль. Краткое описание протокола Modbus/RTU. [Электронный ресурс]. URL: https://intellect-module.ru/downloads/manuals/inode_35D/ModBus_RTU.pdf (дата обращения 21.02.22).