УДК 004.056.53 doi: 10.15827/0236-235X.148.600-610 2024. Т. 37. № 4. С. 600–610

Сценарий атаки на автоматизированную систему управления технологическим процессом с учетом уязвимости протокола Modbus TCP

А.А. Конев [1], В.С. Репкин [1]✉, К.И. Цимбалов [1]

[1] Томский государственный университет систем управления и радиоэлектроники (ТУСУР), г. Томск, 634050, Россия

Ссылка для цитирования
Конев А.А., Репкин В.С., Цимбалов К.И. Сценарий атаки на автоматизированную систему управления технологическим процессом с учетом уязвимости протокола Modbus TCP // Программные продукты и системы. 2024. Т. 37. № 4. С. 600–610. doi: 10.15827/0236-235X.148.600-610
Информация о статье
Группа специальностей ВАК: 2.3.6
Поступила в редакцию: 19.03.2024 После доработки: 22.04.2024 Принята к публикации: 27.04.2024

Аннотация. Предметом исследования является компьютерное моделирование процесса реализации сценария атаки на автоматизированную систему управления (АСУ) технологическим процессом (ТП), в котором осуществляется эксплуатация уязвимостей промышленного протокола Modbus TCP. В данной публикации представлен аналитический обзор актуальных научных работ в области безопасности АСУ ТП, формализации и моделирования атак. Описан лабораторный стенд АСУ ТП, на основе которого сформирована компьютерная модель на языке программирования Python, включающая консоль управления (клиент Modbus), программируемый логический контроллер (сервер Modbus) и исполнительный модуль «Грузовой лифт» (графический интерфейс). Для визуализации пользовательского сценария и процессов между компонентами модели построена UML-диаграмма последовательности. Проверка адекватности модели осуществлялась путем сравнения результатов модели и стенда. Также был разработан и формально описан с помощью графической нотации MAL сценарий атаки, в котором эксплуатируются уязвимости протокола Modbus TCP, связанные с отсутствием встроенных механизмов аутентификации и шифрования. Сценарий атаки успешно реализован на модели и стенде с помощью Metasploit Framework. Для устранения возможности эксплуатации уязвимостей определены и протестированы защитные меры в виде протокола WireGuard, который благополучно справился с задачей. Результаты исследования могут быть использованы для обучения специалистов, например, в киберполигонах, для разработки, реализации и формального описания сценариев атак, для анализа уязвимостей протокола Modbus TCP, а также для тестирования программных средств защиты информации.

Ключевые слова: информационная безопасность, обучение специалистов, эксплуатация уязвимости, сценарий атаки, программируемый логический контроллер, Modbus TCP, Metasploit, Python, Meta Attack Language
Благодарности. Работа выполнена при финансовой поддержке Минобрнауки РФ в рамках базовой части госзадания ТУСУР на 2023 – 2025 гг. (проект № FEWM-2023-0015)

Введение. Актуальность кибербезопасности в области *информационных технологий* (ИТ) и промышленности обусловлена увеличением числа атак на данные отрасли и их критической значимостью для государства. Статистика компании MTC RED показывает, что число кибератак на российские ИТ-компании во втором квартале 2023 года по сравнению с аналогичным периодом прошлого года увеличилось в четыре раза, достигнув отметки в 4 тысячи инцидентов (https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире). Наиболее атакуемыми отраслями в первом полугодии 2023 года стали ИТ – 35 % и АСУ технологическим процессом (ТП) – 21 %.

С увеличением зависимости от технологий и цифровых систем промышленные предприятия становятся объектами повышенного внимания злоумышленников, что подчеркивает важность разработки и применения эффективных мер противодействия. Для защиты АСУ ТП необходимо качественно обучать инженеров-технологов и специалистов информационной безопасности, внедрять отечественные средства защиты и строго контролировать соблюдение организационных мер по защите информации [1]. Чтобы эффективно обучить сотрудников организации, нужно применять методики учебного процесса, направленные на получение практических навыков в сфере кибербезопасности. Например, использование тренировочных стендов, киберполигонов или пентест-лабораторий. Получив теоретические знания, специалист закрепляет их в условиях виртуальной имитации реальных событий, что помогает быстрее и качественнее осуществлять мониторинг инцидентов и реагирование на них в будущем. В этой связи в работе проводится моделирование сценария атаки на АСУ ТП в виртуальной среде. Атака реализуется с помощью эксплуатации уязвимостей промышленного протокола Modbus TCP и приводит к неправильной работе исполнительного модуля, а также к нарушению ТП.

Обзор исследований

Совершенствование технологий и увеличение сложности систем управления требуют постоянной оптимизации методов контроля, управления и обеспечения безопасности [2]. Исследования и разработки в данной области становятся регулярной частью инженерной практики. В этой связи проводится обзор научных работ в области безопасности АСУ ТП и моделирования атак, а также рассматриваются утилиты для эксплуатации уязвимостей и способы формального описания сценариев атак.

Информационная безопасность в АСУ ТП

Теме безопасности АСУ ТП в научном сообществе посвящено немало работ. Так, в исследовании [3] применялась нотация EPC (*Event-driven Process Chain*) при разработке моделей угроз для АСУ ТП. Модели могут быть использованы для оценки вероятности реализации угроз, определения связи между уязвимостями и последствиями от их эксплуатации, а также с целью принятия решений в выборе мер безопасности для систем управления. Авторы предлагают применять EPC-модели при разработке и модернизации АСУ ТП, чтобы обеспечить достаточный уровень информационной безопасности и не допустить реализацию описанных сценариев атак. Однако модели угроз не учитывают атаки внутренних нарушителей, поэтому в организации рабочей деятельности обязательно нужно вводить регламенты, политики безопасности и другие организационные меры защиты.

Исследование [4] посвящено описанию проблем, связанных с обеспечением безопасности в АСУ ТП, и анализу способов реализации атак на данные системы с помощью утилит Wireshark, Xerosploit, GoldenEye. При сравнении утилит автор особенно выделил сетевой анализатор Wireshark, так как в нем имеется возможность перехвата информации для последующей её модификации. Его недостатком является отсутствие функционала для расшифровки данных и реализации DoS-атак. Авторы выделяют три способа реализации атак: эксплуатация человеческого фактора, уязвимости сетевых протоколов или аппаратного комплекса. К человеческому фактору относятся социальная инженерия и ошибки рабочего персонала. При атаках на сетевые протоколы возможно вызвать отказ в обслуживании, перехватить сетевые пакеты, несанкционированно прочитать информацию с устройств или изменить информацию в устройстве, подменить сетевой пакет. В случае атак на оборудование используются специальные технические средства для электромагнитного воздействия или закладок в аппаратные комплексы ТП.

Автор публикации [5] анализирует способы нарушения информационной безопасности АСУ ТП, отмечает рекомендации по обеспечению защищенности таких систем и приводит пример атаки, осуществляемой с применением поискового инструмента Shodan. Целью атаки является несанкционированное управление ТП с помощью SCADA-системы, в которой не изменены стандартные логин и пароль, установленные производителем.

Из работ [3–5] можно сделать вывод, что атаки направлены на узлы управления, SCADA-системы, на *программируемые логические контроллеры* (ПЛК), протоколы и БД, а реализуются они с помощью уязвимостей, социальной инженерии или специального оборудования. В данной работе из перечисленных атакуемых объектов в компьютерной модели есть ПЛК и протокол Modbus. Социальную инженерию в рамках виртуальной системы осуществить не получится. Также отсутствует оборудование для проведения, например, электромагнитных атак. В лабораторном стенде используется современный ОВЕН ПЛК200 с последними обновлениями, поэтому в нем отсутствуют известные уязвимости. В некоторых публикациях обсуждаются и проводятся атаки на контроллеры [6, 7]. Первый вариант – это DDoS-атака [6] на основе стохастической сети процессов, а второй – это перегрузка линии электропередачи, к которой подключен ПЛК [7]. Следует отметить, что для защиты системы управления от определенных атак может быть использован сам ПЛК, если его модернизировать под данные цели [7]. В приведенных примерах при реализации атак необходимы определенные технологические решения, которые отсутствуют на момент проведения работ. Соответственно, рассматриваться будут уязвимости протокола Modbus.

Использованные в работах [3, 6] нотации для формального описания процессов атаки не подходят для обучения специалистов. В формализации с помощью EPC отсутствуют достаточный уровень строгости, защитные меры и логическое деление на этапы атаки. Кроме того, сложные сценарии имеют громоздкую EPC-модель. В [6] авторы построили стохастиче-

скую сеть DDoS-атаки, которая отражает алгоритм функционирования системы. Сеть сложна в понимании и не имеет структурных элементов сценария.

В статье [4] утилиты не позволяют использовать эксплойты уязвимостей из БД CVE (*Common Vulnerabilities and Exposures*) и не предоставляют полезной нагрузки, что ограничивает исследовательский потенциал. В [5] классическая атака методом подбора логина и пароля в i.LON SmartServer не сосредоточена на специфических уязвимостях, характерных для систем АСУ ТП. Аналогичная ситуация в публикации [6], где не уделяется достаточного внимания уникальным характеристикам безопасности промышленных систем, так как осуществлена традиционная DDoS-атака.

В рамках данного исследования нерационально применять симуляторы ПЛК наподобие LOGO! Soft Comfort [7] и SIMATIC S7-PLCSIM [3] для проектирования компонентов АСУ ТП. Это связано с отсутствием необходимости использовать сложные, специализированные симуляторы контроллеров, применяемые при изучении его детальной настройки, процессов и программирования. Для решения поставленных задач целесообразнее будет воспользоваться языком программирования Python при реализации виртуального стенда АСУ ТП. Это обусловлено тем, что разработка сценариев атак, уязвимых узлов и чекеров (скрипт, который проверяет наличие уязвимости на целевом хосте) в киберполигоне Ampire, в который будут интегрированы результаты исследования, осуществляется на языке Python. Соответственно, другим специалистам, работающим с Ampire, тоже будет понятна сформированная модель. Кроме того, у данного языка низкий порог вхождения, он достаточно популярен, что дает преимущество в вопросе количества готовых разработок по исследуемой теме. Например, для работы с протоколом Modbus на Python есть специальная библиотека pymodbus.

Уязвимости промышленного протокола Modbus

Несмотря на широкое распространение в АСУ ТП, протокол Modbus слабо защищен. Он был создан во времена, когда вопросы безопасности сетей не получали должного внимания. В этой связи у протокола нет механизмов шифрования и аутентификации. Автор статьи [8] использует Wireshark для перехвата пакетов протокола Modbus TCP и отмечает, что при использовании специального ПО можно модифицировать перехваченные пакеты. Для обеспечения безопасности передачи данных предлагается два решения VPN и DPI. DPI представляет собой метод анализа содержимого пакетов данных в сети. Он может использоваться для обнаружения и блокировки нежелательного трафика, а также для предотвращения атак. Применительно к протоколу Modbus DPI может помочь выявить аномалии в сетевом трафике, свидетельствующие о возможных атаках или модификации передаваемых данных.

В работе [9] разработан виртуальный тестовый стенд для проведения DoS-атак на протокол Modbus путем перегрузки сети, которая приводит к потере связи между устройствами, или с помощью передачи неверных команд. В контексте АСУ ТП, атака типа «отказ в обслуживании» представляет собой критическую угрозу. Такие атаки в состоянии привести к аварии или полной остановке ТП, что может не только нанести огромный ущерб организации или государству, но и представлять серьезную угрозу для природной среды.

С развитием сетевых технологий безопасность протокола Modbus стала более актуальной, так как до сих пор обнаруживаются новые уязвимости. По данным ФСТЭК России, последняя уязвимость, связанная с Modbus, была обнаружена в 2023 году. На момент написания работы в базе ФСТЭК находилось 54 510 уязвимостей, из которых 107 связаны с протоколом Modbus. Реализации атак на протокол Modbus посвящена работа [10]. Автор использует утилиту Metasploit Framework для внедрения в сетевой канал между SCADA-системой и ПЛК с целью несанкционированного чтения и модификации данных. Подлинный сервер Modbus не понимает, что команды отправляет нарушитель, так как отсутствуют механизмы аутентификации. Если установить межсетевой экран, то можно настроить получение пакетов только от определенного IP-адреса, но не стоит забывать, что существует IP-спуфинг. В качестве решения данной проблемы безопасности автор предлагает уделять особое внимание настройке сетевой конфигурации и использовать VPN при передаче информации.

Атака вида «человек посередине» проводится в работе [11] с помощью утилиты Scapy. Для проведения экспериментов была создана виртуальная система, состоящая из трех машин с операционными системами Ubuntu. Реализуется атака ARP poisoning, чтобы нарушитель стал посредником между двумя легальными

устройствами. То есть пакеты идут не напрямую, а через дополнительный сетевой узел. Атака ARP poisoinig происходит в три этапа. На первом этапе нарушитель использует методы, такие как отравление ARP-таблиц, для установления доверия сети к предопределенному маршруту связи. На втором этапе при помощи функции перехвата трафика Scapy злоумышленник захватывает и модифицирует определенные пакеты между клиентом и сервером, оставаясь незамеченным. Третий этап – это удаление записей в ARP-таблицах, что маскирует следы атаки. В результате злоумышленник может изменять конфигурацию сервера Modbus, не раскрывая эти изменения его клиенту. Для защиты системы автор предлагает использовать защищенный канал связи и проверку ARP-запросов на время доставки.

В исследовании [12] представлен сценарий атаки с внедрением ложных команд в передаваемые пакеты для ПЛК. Для поиска открытых портов Modbus использовался NMAP, для анализа трафика – Wireshark. Реализована атака ARP-poisoning, которая проводилась на смоделированную виртуальную систему, состоящую из ScadaBR и OpenPLC, с использованием Python-скрипта. Для эффективной защиты от данной атаки автор предлагает использование специальных брандмауэров, которые разрабатывались для протокола Modbus. Политика безопасности таких брандмауэров работает с применением DPI [8].

В работе [10] для эксплуатации уязвимостей Modbus использовался Metasploit Framework – популярный инструмент для тестирования на проникновение и проверки безопасности систем. В нем есть не только перечень многочисленных эксплойтов, но и готовые полезные нагрузки [13]. В работе [14] утверждается, что Metasploit показал хорошие результаты при его использовании для оценки уязвимостей системы безопасности. Утилита позволяет выполнять сложные шаги, формирующие атаку. При этом с помощью созданной модели машинного обучения определялись наиболее подходящие эксплойты для тестируемой системы. Для обучения модели использовались данные с площадки Hack the Box. Доля верных ответов модели – 33 %, авторы отмечают, что это хорошие результаты для небинарной классификации. В исследовании [15] на языке Pyhton с помощью PyMetasploit была написана автоматизированная эксплуатация уязвимости с идентификационным номером CVE-2022-30781. Утилита позволила не только применить эскплойт multi/http/gitea_git_fetch_rce, но и доставить полезную нагрузку в виде metepreter-сессии.

Фреймворк Metasploit полностью соответствует потребностям в решении поставленных задач. Он бесплатный и обладает обширным функционалом, в том числе модулями для эксплуатации уязвимостей Modbus. Кроме того, существует множество обучающих материалов и документации, что делает его хорошим выбором для проводимого исследования.

Особенности моделирования и формализации компьютерных атак

Во многих исследованиях упоминаются формализация и моделирование атак, при этом они тесно связаны, так как формальное описание существенно упрощает создание модели [16–18]. Формализация важна для создания точных и структурированных описаний атак и угроз в информационных системах. Она способствует наглядному восприятию сложных сценариев атак, позволяет понимать последствия эксплуатации уязвимостей и отражает последовательность действий злоумышленника [16]. Отсутствие формального описания приводит к тому, что специалисты по-разному интерпретируют один и тот же текст, каждый субъективно выделяет наиболее важные элементы и связи между ними [17].

Моделирование, в свою очередь, позволяет имитировать атаки на различные активы, например, на контроллер домена или SCADA-систему. Модель может использоваться для тестирования систем на проникновение [15, 18] и для обучения специалистов, например, в киберполигонах [15, 19, 20]. В исследовании [15] атака моделируется для дальнейшей интеграции в киберполигон. Как упоминалось ранее, для реализации автоматизированной эксплуатации уязвимости в системе, в которой используется ПО Gitea, применяются скрипт на языке Python и фреймворк Metasploit. Также в данной работе приводится формальное описание эксплуатации уязвимости с помощью графической нотации MAL: отмечены шаги злоумышленника и их причины, меры противодействия каждому шагу и используемые системы. MAL способствует понятному и подробному описанию атаки, при этом есть возможность модификации языка под свои потребности. Например, в публикации [16] авторы на основе MAL разработали язык vehicleLang для формализации сценариев атак на транспортные средства. Применимость данного языка оценивалась экс-

пертом в области автомобильной промышленности. Моделирование атак осуществлялось для оценки кибербезопасности систем и оценки времени, затраченного злоумышленником для достижения цели. В [18] создана методология на основе MAL для определения набора контрмер, оценки стоимости мер защиты и для затраченного времени на каждый шаг злоумышленника.

В работе [19] проводится сравнение четырех способов формализации: дерево атак, граф атак, MAL и Cyber Kill Chain. Авторы сделали вывод, что способ формализации зависит от решаемых задач. Дерево атак следует применять, если формальное описание используется для обучения специалистов. Для описания исключительно последовательности атакуемых узлов стоит воспользоваться графом атак. В случае подробного описания действий злоумышленника с указанием IP-адресов и конфигурации сети рекомендуется применить Cyber Kill Chain. Разработчикам сценариев атак будет удобен в использовании MAL, так как в нем учитываются используемые злоумышленником ресурсы, промежуточные активы и меры защиты от каждой уязвимости [20].

Исследователи не оставляют без внимания моделирование атак на сетевую инфраструктуру. Так, в [21] имитационная модель атаки типа Phishing реализована в среде AnyLogic, процесс атаки формально описан с помощью блок-схемы. В результате авторы предлагают использовать полученное решение для оценки защищенности сети и выявления зависимости вероятности атаки от времени в заданных условиях. В [22] для оценки среднего времени осуществления DDoS-атаки на сеть АСУ ТП применялась модель на основе стохастической сети, достоверность которой проверялась с применением экспериментального стенда «Информационная безопасность в индустриальных системах».

В проводимом исследовании будет использован язык MAL как обеспечивающий точное и структурированное описание. В публикациях [16, 18, 20] отмечено, что MAL полноценно справился с задачей формализации. Кроме того, ранее была подчеркнута особенность языка MAL – возможность модификации под конкретные потребности. Еще одним важным преимуществом выбранной нотации является существование фреймворка, который применяется для автоматизированной генерации метаграфов [23]. Как и в статье [22], для оценки адекватности модели и применимости сценария атаки будет задействован лабораторный стенд.

Описание лабораторного стенда АСУ ТП и его виртуальной модели

Лабораторный стенд АСУ ТП, на основе которого формируется модель в виртуальной инфраструктуре, представлен на рисунке 1. В стенде присутствуют основные компоненты промышленности, например, грузовой лифт, ПЛК, печь, пневмопривод, двигатель и т.д. В данном исследовании в качестве исполнительного модуля и для дальнейшей работы взят грузовой лифт. На рисунке 2 представлена структурная схема, отражающая взаимодействие элементов стенда, которые управляют грузовым лифтом.

Для реализации системы управления грузовым лифтом была написана программа на языке ST (Structured Text). Представим исходный код:

```
   // Логика Лифт
   IF start THEN

      IF pos_1 THEN
         pos := 1;
         down := FALSE;
         start := FALSE;
      ELSIF pos_2 THEN
         pos := 2;
         down := FALSE;
         start := FALSE;
      ELSIF pos_3 THEN
         pos := 3;
         start := FALSE;
      ELSE
         down := TRUE;
      END_IF
   ELSE

      IF call_1 OR call = 1 OR wCall_1
OR HMI_call_1 THEN
         call := 1;
         down := TRUE;
         IF pos_1 THEN
            down := FALSE;
            pos := 1;
            call := 0;
         END_IF
      ELSIF call_2 OR call = 2 OR wCall_2
OR HMI_call_2 THEN
         call := 2;
         IF pos = 1 THEN
            up := TRUE;
         ELSIF pos = 3 THEN
            down := TRUE;
         END_IF
         IF pos_2 THEN
            up := FALSE;
            down := FALSE;
```

```
            pos := 2;
            call := 0;
         END_IF

      ELSIF call_3 OR call = 3 OR wCall_3
OR HMI_call_3 THEN
         call := 3;
         up := TRUE;
         IF pos_3 THEN
            up := FALSE;
            pos := 3;
            call := 0;
         END_IF
      END_IF
   END_IF
```

Несмотря на то, что взят лифт, в создаваемой модели присутствует возможность ее модификации и масштабируемости. ПЛК соединен с АРМ, на котором установлена SCADA-система, через интерфейс Ethernet по протоколу Modbus TCP. Между ПЛК и исполнительными устройствами используется интерфейс RS-485, протокол Modbus RTU. Важно отметить основной принцип работы по протоколу Modbus: инициализировать команду может только Modbus-клиент [24].

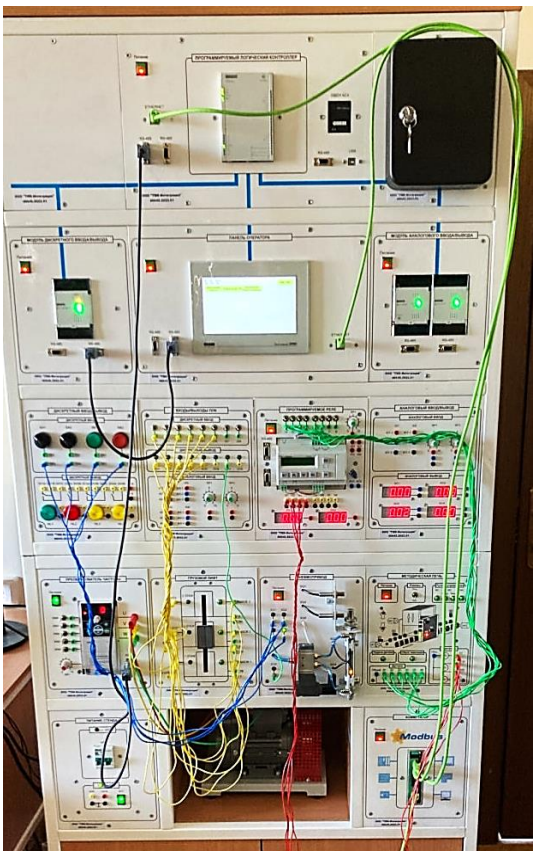

Рис. 1. Лабораторный стенд АСУ ТП

Fig. 1. APCS laboratory stand

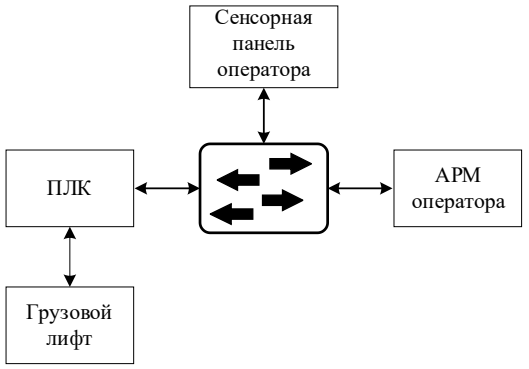

Рис. 2. Структурная схема стенда АСУ ТП

Fig. 2. Block diagram of the APCS stand

Для моделирования стенда в виртуальной среде был использован язык программирования Python 3.11 и библиотека pymodbus 3.5.4. Созданная модель (https://github.com/Volodyanoy/The-automated-control-system-model) включает в себя консоль управления (клиент Modbus), ПЛК (сервер Modbus) и модуль «Грузовой лифт» (графический интерфейс). Консоль управления и ПЛК передают данные по протоколу Modbus TCP. Между ПЛК и лифтом вместо Modbus RTU были использованы возможности объектно-ориентированного программирования – модуль работает путем вызова определенных методов класса. Для визуализации пользовательского сценария и процессов между компонентами модели построена UML-диаграмма последовательности (рис. 3).

Модель сформирована в первую очередь для имитации основных процессов АСУ ТП в виртуальной среде с применением протокола Modbus. Проверка адекватности работы модели осуществлялась на основе 20 сетевых пакетов с различным содержимым. Результаты поведения модели аналогичны результатам лабораторного стенда, что говорит о применимости ее в рамках данного исследования.

Формирование и реализация сценария атаки

Сценарий атаки представляет собой последовательность шагов, которые злоумышленник предпринимает для осуществления недопустимого события в инфраструктуре компании. Недопустимое событие – инцидент информационной безопасности в организации, который приводит к нарушению операционной деятельности [25]. В данной работе недопустимое событие – это нарушение работы ТП из-за некорректной работы исполнительного модуля «Гру-

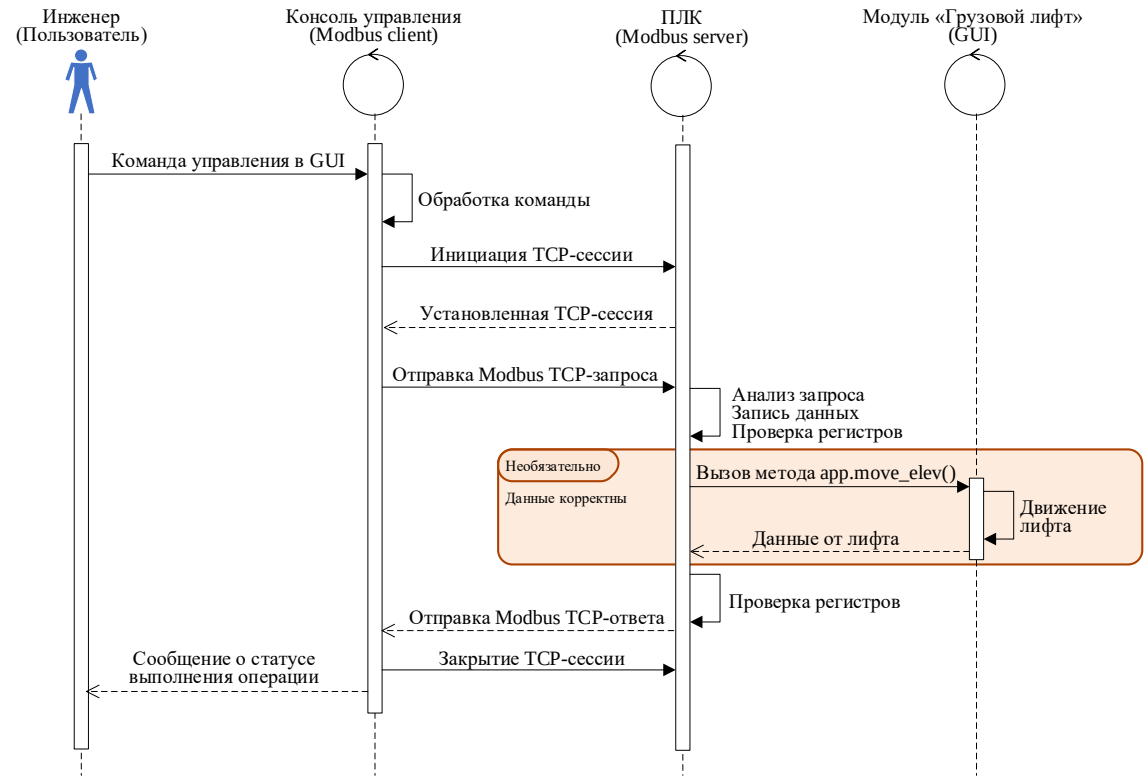

Рис. 3. UML-диаграмма последовательности, отражающая пользовательский сценарий работы с моделью

Fig. 3. UML sequence diagram reflecting user's scenario of working with the model

зовой лифт». Условия реализации сценария: нарушитель преодолел сетевой периметр компании и получил доступ к рабочей станции, которая находится в подсети АСУ ТП.

Для проведения атак применяется Metasploit Framework. Эксплуатация уязвимостей протокола Modbus осуществляется с помощью следующих модулей фреймворка: modbusclient.rb (имитация Modbus-клиента), modbusdetect.rb (обнаружение Modbus-устройств и их ID) и modbus_banner_grabbing.rb (сбор информации об устройствах Modbus). Для просмотра сетевых пакетов используется Wireshark, а для сканирования сети утилита Nmap.

Текстовое описание сценария атаки: нарушитель проводит сканирование сети с помощью Nmap, чтобы найти активные хосты в подсети. У каждого найденного хоста проверяется, открыт ли стандартный Modbus-порт 502. Также нарушитель использует сетевой анализатор трафика для просмотра пакетов, отправителей и получателей. В результате злоумышленник определяет IP-адреса Modbus-устройств и наличие протокола Modbus TCP. Далее применяется утилита Metasploit (modbus_banner_grabbing), чтобы собрать информацию об устройствах, например, сведения о производителе. С помощью модуля modbusdetect определяется ID Modbus-устройств. Теперь нарушитель знает IP-адрес сервера, порт и ID, что позволяет ему использовать модуль «modbusclient» для несанкционированной имитации действий Modbus-клиента. Злоумышленник считывает карту регистров ПЛК, что приводит к нарушению конфиденциальности информации. Затем производится запись данных в регистр ПЛК, то есть нарушается целостность информации. Из-за изменения регистра контроллер отправил исполнительному устройству неверные команды, что привело к нарушению ТП.

Формализация сценария атаки проведена с помощью графической нотации MAL (рис. 4). Текстовое и формальное описания дополняют друг друга, обеспечивая более полное и понятное представление о сценарии.

В результате были сконфигурированы виртуальные машины и успешно реализован сценарий атаки на модели и стенде. Применив защитные меры в виде VPN, которые рекомендуются в [10–12], удалось закрыть уязвимости протокола Modbus TCP, связанные с отсутствием механизмов аутентификации и шифро-

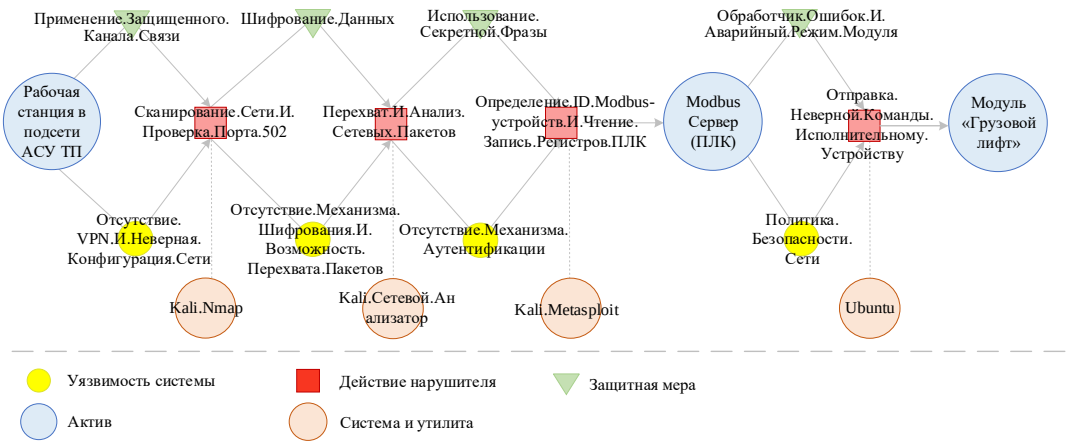

Рис. 4. Формальное описание эксплуатации уязвимостей Modbus TCP с помощью графической нотации MAL

Fig. 4. Formal description of Modbus TCP vulnerability exploitation using MAL graphical notation

вания. Использовался протокол WireGuard, так как он поддерживается в ОВЕН ПЛК 200. Благодаря VPN использование модулей Metasploit безуспешно, а данные в пакетах теперь зашифрованы, соответственно, если нарушитель перехватит пакеты, то не сможет понять их содержимое. Также при сканировании сети не получается обнаружить сервер, а значит, нарушитель не сможет понять, какой хост является Modbus-сервером и открыт ли там порт 502.

Поведение модели соответствует поведению реальной системы при осуществлении атаки как с учетом защитных мер, так и без них. Это свидетельствует об адекватности модели и ее применимости для исследований в области информационной безопасности и для обучения специалистов.

Заключение

В современном промышленном мире безопасность АСУ ТП становится все более важной из-за ее массового применения. Взлом систем управления может привести к серьезным последствиям, включая нарушение производственных процессов, потерю данных, финансовый ущерб или природную катастрофу. Поэтому предприятия должны обеспечивать надежную защиту систем от различных угроз, следовать лучшим практикам безопасности и поддерживать высокий уровень знаний трудового коллектива в данной области.

Качественная подготовка персонала промышленных предприятий, часть из которых относится к субъектам критической информационной инфраструктуры, способствует снижению рисков нарушения информационной безопасности. Представленные в работе компьютерная модель лабораторного стенда АСУ ТП и сценарий атаки, в котором эксплуатируются уязвимости протокола Modbus TCP, связанные с отсутствием встроенных механизмов аутентификации и шифрования, могут быть применены для обучения специалистов практическим навыкам выявления и реагирования на инциденты информационной безопасности. Также результаты исследования можно использовать для анализа уязвимостей протокола Modbus TCP и тестирования программных средств защиты информации. В рамках данной работы были протестированы защитные меры в виде протокола WireGuard, который обеспечил безопасность передачи данных между клиентом и сервером.

Список литературы

1. Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты // Вопросы кибербезопасности. 2019. № 3. С. 63–71. doi: 10.21681/2311-3456-2019-3-63-71.

2. Будников С.А., Коваленко С.М., Бочарова А.И. Методика оценки эффективности систем безопасности автоматизированных систем управления // Вопросы кибербезопасности. 2023. Т. 55. № 3. С. 2–12.

3. Машкина И.В., Гарипов И.Р. Разработка EPC-моделей угроз нарушения информационной безопасности автоматизированной системы управления технологическими процессами // Безопасность информационных технологий. 2019. Т. 26. № 4. С. 6–20. doi: 10.26583/bit.2019.4.01.

4. Цимбалов К.И., Брагин Д.С. Анализ способов нарушения информационной безопасности автоматизированной системы управления технологическими процессами // Электронные средства и системы управления: матер. докладов XIX Междунар. науч.-практич. конф. 2021. № 1-2. С. 137–139.

5. Грачков И.А. Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты // Безопасность информационных технологий. 2018. Т. 25. № 1. С. 90–98. doi: 10.26583/bit.2018.1.09.

6. Богер А.М., Соколов А.Н. Математическая модель воздействия DDoS-атаки на программируемые логические контроллеры АСУ ТП // Безопасность информационного пространства: сб. науч. тр. XXI Всерос. науч.-практич. конф. 2023. № 4. С. 196–198.

7. Ibraheem A., Ibrahim M., Shanshal A. PLC based overcurrent protection of three-phase transmission line. Proc. IMDC-SDSP, 2020. URL: https://eudl.eu/pdf/10.4108/eai.28-6-2020.2298248 (дата обращения: 02.03.2024). doi: 10.4108/eai.28-6-2020.2298248.

8. Fedotov A.A. A research into the vulnerabilities of the Modbus protocol // Современные направления в истории, культуре, науке и технике: матер. Междунар. науч.-практич. конф. 2021. С. 95–97.

9. Rahman A., Mustafa G., Khan A.Q., Abid M., Durad M.H. Launch of denial of service attacks on the modbus/TCP protocol and development of its protection mechanisms. IJCIP, 2022, vol. 39, art. 100568. doi: 10.1016/j.ijcip.2022.100568.

10. Цимбалов К.И., Мосейчук В.А., Брагин Д.С. Атака, нарушающая конфиденциальность и целостность информации в АСУ ТП на основе открытого порта при использовании протокола Modbus TCP // ТУСУР: сб. статей. 2022. № 1-2. С. 161–164.

11. Parian C., Guldimann T., Bhatia S. Fooling the master: Exploiting weaknesses in the Modbus protocol. Procedia Comput. Sci., 2020, vol. 171, pp. 2453–2458. doi: 10.1016/j.procs.2020.04.265.

12. Alsabbagh W., Amogbonjaye S., Urrego D., Langendörfer P. A stealthy false command injection attack on Modbus based SCADA systems. Proc. CCNC, 2023, pp. 1–9. doi: 10.1109/CCNC51644.2023.10059804.

13. Ромейко Д.А., Паюсова Т.И. Обзор возможностей среды Metasploit Framework // Математ. и информ. моделирование: матер. Всерос. конф. молодых ученых. 2022. № 20. С. 318–325.

14. Valea O., Oprisa C. Towards pentesting automation using the Metasploit Framework. Proc. ICCP, 2020, pp. 171–178. doi: 10.1109/ICCP51029.2020.9266234.

15. Конев А.А., Коваленко А.С., Репкин В.С., Семенов Г.Ю. Уязвимость «Gitea Git Fetch Remote Code Execution»: анализ, формализация автоматизированной эксплуатации, меры защиты // Вестн. УрФО. Безопасность в информационной сфере. 2023. № 2. С. 67–73. doi: 10.14529/secur230207.

16. Katsikeas S., Johnson P., Hacks S., Lagerström R. Probabilistic modeling and simulation of vehicular cyber attacks: An application of the Meta attack language. Proc. ICISSP, 2019, vol. 1, pp. 175–182. doi: 10.5220/0007247901750182.

17. Novokhrestov A., Konev A., Shelupanov A., Buymov A. Computer network threat modelling. JPCS, 2020, vol. 1488, art. 012002. doi: 10.1088/1742-6596/1488/1/012002.

18. Wideł W., Mukherjee P., Ekstedt M. Security countermeasures selection using the Meta attack language and probabilistic attack graphs. IEEE Access, 2022, vol. 10, pp. 89645–89662. doi: 10.1109/ACCESS.2022.3200601.

19. Якимук А.Ю., Устинов С.А., Лазарев Т.П., Коваленко А.С. Методы формализации описания сценариев кибератак // Электронные средства и системы управления: матер. докладов. 2022. № 1-2. С. 73–76.

20. Конев А.А., Репкин В.С., Семенов Г.Ю., Сермавкин Н.И. Формирование уязвимого узла «Adobe coldfusion Deserialization of Untrusted Data vulnerability» // Вопросы кибербезопасности. 2024. № 1. С. 75–81. doi: 10.21681/2311-3456-2024-1-75-81.

21. Добрышин М.М., Закалкин П.В. Модель компьютерной атаки типа «Phishing» на локальную компьютерную сеть // Вопросы кибербезопасности. 2021. № 2. С. 17–25. doi: 10.21681/2311-3456-2021-2-17-25.

22. Богер А.М., Соколов А.Н. Математическая модель вектора DDoS-атаки на сетевую инфраструктуру АСУ ТП с использованием метода топологического преобразования стохастических сетей // Вопросы кибербезопасности. 2023. № 4. С. 72–79. doi: 10.21681/2311-3456-2023-4-72-79.

23. Wideł W., Hacks S., Ekstedt M., Johnson P., Lagerström R. The meta attack language – a formal description. Computers & Security, 2023, vol. 130, art. 103284. doi: 10.1016/j.cose.2023.103284.

24. Găitan V.G., Zagan I. Modbus protocol performance analysis in a variable configuration of the physical fieldbus architecture. IEEE Access, 2022, vol. 10, pp. 123942–123955. doi: 10.1109/ACCESS.2022.3224720.

25. Alhaj T.A., Siraj M.M., Zainal A. et al. An effective attack scenario construction model based on identification of attack steps and stages. Int. J. of Inform. Security, 2023, vol. 22, pp. 1481–1496. doi: 10.1007/s10207-023-00701-2.

Software & Systems doi: 10.15827/0236-235X.148.600-610 2024, 37(4), pp. 600–610

Scenario of an attack on an automated process control system taking into account Modbus TCP protocol vulnerability

Anton A. Konev [1], Vladimir S. Repkin [1]✉, Kirill I. Tsimbalov [1]

[1] Tomsk State University of Control Systems and Radioelectronics (TUSUR), Tomsk, 634050, Russian Federation

For citation
Konev, A.A., Repkin, V.S., Tsimbalov, K.I. (2024) 'Scenario of an attack on an automated process control system taking into account Modbus TCP protocol vulnerability', *Software & Systems*, 37(4), pp. 600–610 (in Russ.). doi: 10.15827/0236-235X.148.600-610
Article info
Received: 19.03.2024 After revision: 22.04.2024 Accepted: 27.04.2024

Abstract. The paper focuses on computer modeling of a scenario of an attack on an automated process control system (APCS); the scenario recreates vulnerabilities in the industrial Modbus TCP protocol. The paper presents an analytical review of current scientific works related to automated process control system security, formalization and attack modeling. The authors describe the ACS laboratory stand, which became a base for a computer model in the Python programming language. The model includes a control console (Modbus client), a programmable logic controller (Modbus server) and an executive module "Freight elevator" (graphical interface). Тнєку is a special UML sequence diagram that visualizes the user scenario and the processes between model components. The authors also verified the adequacy of the model by comparing the model and bench results. In addition, they have developed and formally described the attack scenario using graphical notation MAL. It exploits Modbus TCP protocol vulnerabilities related to the lack of built-in authentication and encryption mechanisms. The attack scenario is successfully implemented on the model and bench using Metasploit Framework. To eliminate the possibility of exploiting the vulnerabilities, the authors defined and tested a defense measure in the form of the WireGuard protocol. The protocol safely accomplished the task. The study results can be used to train specialists in cyber range for developing, implementing and formal description of attack scenarios, for analyzing vulnerabilities in the Modbus TCP protocol, as well as for testing software information security measures.
Keywords: information security, specialist training, vulnerability exploitation, attack scenario, programmable logic controller, Modbus TCP, Metasploit, Python, Meta Attack Language
Acknowledgements. The work was carried out with the financial support of the Ministry of Science and Higher Education of the Russian Federation within the framework of the basic part of the TUSUR state task for 2023-2025 (project no FEWM–2023-0015)

References

1. Garbuk, S.V., Pravikov, D.I., Polyansky, A.V., Samarin, I.V. (2019) 'Ensurin APCS information security using the predictive protection method', *Cybersecurity Issues*, (3), pp. 63–71 (in Russ.). doi: 10.21681/2311-3456-2019-3-63-71.
2. Budnikov, S.A., Kovalenko, S.M., Bocharova, A.I. (2023) 'Methodology for assessing the effectiveness of security systems of automated control systems', *Cybersecurity Issues*, (3), pp. 2–12 (in Russ.).
3. Mashkina, I.V., Garipov, I.R. (2019) for 'Development of EPC-Models of threats to information security of the automated process control system', *IT Security*, 26(4), pp. 6–20 (in Russ.). doi: 10.26583/bit.2019.4.01.
4. Tsimbalov, K.I., Bragin, D.S. (2021) 'Analysis of methods for violating the information security of automated control systems for technological processes', *Proc. XIX Int. Sci. and Pract. Conf. Electronic Means and Control Systems*, (1-2), pp. 137–139 (in Russ.).
5. Grachkov, I.A. (2018) 'Information security of industrial control systems: Possible attack vectors and protection methods', *IT Security*, 25(1), pp. 90–98 (in Russ.). doi: 10.26583/bit.2018.1.09.
6. Boger, A.M., Sokolov, A.N. (2023) 'Mathematical model of the impact of DDoS attack on programmable logic controllers of automated process control systems', *Proc. XXI All-Russ. Sci. and Pract. Conf. Security of Information Space*, (4), pp. 196–198 (in Russ.).

7. Ibraheem, A., Ibrahim, M., Shanshal, A. (2020) 'PLC based overcurrent protection of three-phase transmission line', *Proc. IMDC-SDSP*, available at: https://eudl.eu/pdf/10.4108/eai.28-6-2020.2298248 (accessed March 02, 2024). doi: 10.4108/eai.28-6-2020.2298248.

8. Fedotov, A.A. (2021) 'A research into the vulnerabilities of the Modbus protocol', *Proc. Int. Sci. and Pract. Conf. Current Trends in History, Culture, Sci. and Tech.*, pp. 95–97.

9. Rahman, A., Mustafa, G., Khan, A.Q., Abid, M., Durad, M.H. (2022) 'Launch of denial of service attacks on the modbus/TCP protocol and development of its protection mechanisms', *IJCIP*, 39, art. 100568. doi: 10.1016/j.ijcip. 2022.100568.

10. Tsimbalov, K.I., Moseychuk, V.A., Bragin, D.S. (2022) 'Attack violating the confidentiality and integrity of information in automated control systems for technological processes using the MODBUS TCP protocol', *Proc. TUSUR*, (1-2), pp. 161–164 (in Russ.).

11. Parian, C., Guldimann, T., Bhatia, S. (2020) 'Fooling the master: Exploiting weaknesses in the Modbus protocol', *Procedia Comput. Sci.*, 171, pp. 2453–2458. doi: 10.1016/j.procs.2020.04.265.

12. Alsabbagh, W., Amogbonjaye, S., Urrego, D., Langendörfer, P. (2023) 'A stealthy false command injection attack on Modbus based SCADA systems', *Proc. CCNC*, pp. 1–9. doi: 10.1109/CCNC51644.2023.10059804.

13. Romeyko, D.A., Payusova, T.I. (2022) 'Overview of capabilities of the Metasploit Framework environment', Proc. *All-Russ. Conf. Math. and Inform. Modeling*, (20), pp. 318–325 (in Russ.).

14. Valea, O., Oprisa, C. (2020) 'Towards pentesting automation using the Metasploit Framework', *Proc. ICCP*, pp. 171–178. doi: 10.1109/ICCP51029.2020.9266234.

15. Konev, A.A., Kovalenko, A.S., Repkin, V.S., Semenov, G.Yu. (2023) 'Vulnerability «Gitea Git Fetch Remote Code Execution»: Analysis, automated exploitation formalization, and mitigation measures', *Bull. of the UrFD. Security in the Information Sphere*, 48(2), pp. 67–73 (in Russ.). doi: 10.14529/secur230207.

16. Katsikeas, S., Johnson, P., Hacks, S., Lagerström, R. (2019) 'Probabilistic modeling and simulation of vehicular cyber attacks: An application of the Meta attack language', *Proc. ICISSP*, 1, pp. 175–182. doi: 10.5220/0007247901750182.

17. Novokhrestov, A., Konev, A., Shelupanov, A., Buymov, A. (2020) 'Computer network threat modelling', *JPCS*, 1488, art. 012002. doi: 10.1088/1742-6596/1488/1/012002.

18. Wideł, W., Mukherjee, P., Ekstedt, M. (2022) 'Security countermeasures selection using the Meta attack language and probabilistic attack graphs', *IEEE Access*, 10, pp. 89645–89662. doi: 10.1109/ACCESS.2022.3200601.

19. Yakimuk, A.Yu., Ustinov, S.A., Lazarev, T.P., Kovalenko, A.S. (2022) 'Methods of formalization of cyber attack scenarios description', *Proc. Conf. Electronic Means and Control Systems*, (1-2), pp. 73–76 (in Russ.).

20. Konev, A.A., Repkin, V.S., Semenov, G.Yu., Sermavkin, N.I. (2024) 'Formation of vulnerable node «Adobe coldfusion Deserialization of Untrusted Data vulnerability»', *Cybersecurity Issues*, (1), pp. 75–81 (in Russ.). doi: 10.21681/ 2311-3456-2024-1-75-81.

21. Dobryshin, M.M., Zakalkin, P.V. (2021) 'Model of a "Phishing" type of computer attack on a local computer network', *Cybersecurity Issues*, (2), pp. 17–25 (in Russ.). doi: 10.21681/2311-3456-2021-2-17-25.

22. Boger, A.M., Sokolov, A.N. (2023) 'Mathematical model of the vector of a DDoS attack on the ICS using the method of topological transformation of stochastic networks', *Cybersecurity Issues*, (4), pp. 72–79 (in Russ.). doi: 10.21681/ 2311-3456-2023-4-72-79.

23. Wideł, W., Hacks, S., Ekstedt, M., Johnson, P., Lagerström, R. (2023) 'The meta attack language – a formal description', *Computers & Security*, 130, art. 103284. doi: 10.1016/j.cose.2023.103284.

24. Găitan, V.G., Zagan, I. (2022) 'Modbus protocol performance analysis in a variable configuration of the physical fieldbus architecture', *IEEE Access*, 10, pp. 123942–123955. doi: 10.1109/ACCESS.2022.3224720.

25. Alhaj, T.A., Siraj, M.M., Zainal, A. et al. (2023) 'An effective attack scenario construction model based on identification of attack steps and stages', *Int. J. of Inform. Security*, 22, pp. 1481–1496. doi: 10.1007/s10207-023-00701-2.

Авторы

Конев Антон Александрович [1], к.т.н., доцент, kaa@fb.tusur.ru
Репкин Владимир Сергеевич [1], студент, repkin_vova@mail.ru
Цимбалов Кирилл Игоревич [1], аспирант, cki@nti.tusur.ru

[1] Томский государственный университет систем управления и радиоэлектроники (ТУСУР), г. Томск, 634050, Россия

Authors

Anton A. Konev [1], Cand. of Sci. (Engineering), Associate Professor, kaa@fb.tusur.ru
Vladimir S. Repkin [1], Student, repkin_vova@mail.ru
Kirill I. Tsimbalov [1], Postgraduate Student, cki@nti.tusur.ru

[1] Tomsk State University of Control Systems and Radioelectronics (TUSUR), Tomsk, 634050, Russian Federation