«Сибирский государственный университет телекоммуникаций и информатики»

(ФГОБУ ВПО «СибГУТИ»)

Межрегионального учебного центра переподготовки специалистов

Уважаемый Попов Иван Васильевич, Работа мала по объему, присылалась ранее. Доработать в примерах, связанных с угрозами и средствами защиты. Доработку выделить желтым фоном.

Дисциплина

Основы информационной безопасности

Контрольная работа

Тема реферата: Обеспечение информационной безопасности в SCADA-системах

Выполнил: Попов И.В.

Группа: ИСТ-11

Вариант: 07+11=18

Проверил: Киселев А.А.

Новосибирск 2024

Содержание

[Введение 3](#_Toc126412376)

[1. Система SCADA 4](#_Toc126412377)

[2. Информационная безопасность в SCADA-системах 7](#_Toc126412378)

[Заключение 13](#_Toc126412379)

[Список использованных источников 15](#_Toc126412380)

**Введение**

В настоящее время системы класса SCADA (Supervisory Control And Data Acquisition, Диспетчерское управление и сбор данных) являются весьма эффективной технологией автоматизированного управления динамическими системами во многих отраслях промышленности. Современные SCADA-системы имеют схожие возможности и принципы функционирования, которые позволяют решить типовые задачи, такие как: диспетчерский мониторинг и сбор данных о протекании технологического процесса, управление при наличии четких алгоритмов и полной формализованной модели объекта управления.

Рассмотрим в рамках этой работы обеспечение информационной безопасности систем SCADA.

Целью данной работы является изучение темы: "Обеспечение информационной безопасности в SCADA-системах".

Основными теоретическими и методологическими источниками при написании данной работы послужили издания отечественных авторов и публикации, которые посвящены раскрытию исследуемой нами темы.

Работа состоит из введение, основной части, заключение с выводами по работе, снабжена списком использованных источников.

**1. Система SCADA**

Термин «SCADA» охватывает процессы сбора информации реального времени с удаленных объектов для обработки, анализа и возможного управления этими объектами. Здесь под реальным временем понимается режим работы автоматизированной системы обработки информации и управления, при котором существуют жёсткие ограничения на ее временные характеристики.

Ошибочно считать, что реальное время всегда означает «быстро». Правильнее сказать, что реальное время означает «вовремя». Другими словами, система реального времени гарантирует, что отклик происходит за требуемое время. Системы реального времени бывают двух типов: системы жесткого реального времени и системы мягкого реального времени.

Системы жесткого реального времени не допускают никаких ошибок[[1]](#footnote-1). Иными словами, жёсткое реальное время – это такой режим работы системы, при котором нарушение временных ограничений равнозначно отказу системы. Мягкое реальное время – режим работы системы, при котором нарушения временных ограничений приводят к снижению качества работы системы.

SCADA (Supervisory Control And Data Acquisition) - диспетчерское управление и сбор данных. SCADA это система автоматизации технологических процессов, которая используется для сбора информации от датчиков и отдалённых, измерительных приборов, передачи данных в операторскую, их отображения для контроля и управления. SCADA , как правило, система логически или физически изолированная, от других сетей в системе критической инфраструктуры.

Некоторые считают, что если система SCADA не подключена к интернету, то они застрахованы от кибератак. Такие рассуждения невероятно далеки от истины.

Системы SCADA могут подвергаться таким физическим угрозам как вывод из строя одного или нескольких модулей, также и киберугрозам в виде атак дистанционно или изнутри. В обоих случаях это может привезти к следующим нежелательным последствиям:

- Потеря жизни ϖ Финансовый ущерб

- Кража/потеря информации

- Сбои и остановка работы объекта в целом

- Физическое разрушение

- Отказ/обвал периферийной техники

- Отказ/обвал Центра управления SCADA / Операторской.[[2]](#footnote-2)

SCADA (Supervisory Control And Data Acquisition) – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления. SCADA может являться частью АСУ ТП, АСКУЭ, системы экологического мониторинга, научного эксперимента, автоматизации здания и т. д. SCADA-системы используются во всех отраслях хозяйства, где требуется обеспечивать операторский контроль за технологическими процессами в реальном времени. Данное программное обеспечение устанавливается на компьютеры и, для связи с объектом, использует драйверы ввода-вывода или OPC/DDE серверы. Программный код может быть, как написан на одном из языков программирования, так и сгенерирован в среде проектирования.

В основе большинства из ныне существующих SCADA-систем лежит платформа Microsoft Windows, так как подобного рода системы предлагают наиболее гибкие, полные и расширяемые решения в области HMI. Усиление позиций Microsoft на рынке ОС АСУ ТП влечёт соответствующую реакцию со стороны разработчиков SCADA-систем (например, Siemens) для множества различных платформ, которая заключается в приоритезации дальнейшего развития именно платформы Windows NT. Таким образом, основу глобального рынка программного обеспечения SCADA-систем на данный составляет ОС MS Windows NT, тогда как её предшественники, такие как MS DOS, стремительно вытесняются. Использованию Windows также способствует отлаженный механизм коммуникаций с драйверами оборудования различных производителей, определяющий универсальность ОС.[[3]](#footnote-3)

**2. Информационная безопасность в SCADA-системах**

Уязвимости в АСУ ТП могут возникать в результате недостатков, неправильного или ненадлежащего технического обслуживания технических платформ, включая аппаратную часть, операционные системы и приложения, а также благодаря неполным, несоответствующим или попросту несуществующим руководящим документам и политикам в области ИБ. Данные уязвимости могут быть уменьшены благодаря различного рода средств контроля безопасности, таких как проведение обновлений ОС и приложений, контроль физического доступа, специализированное ПО в области информационной безопасности (например, антивирусное ПО).

Корпоративная политика безопасности может уменьшить число уязвимостей определяя обязательное использование парольной защиты или, например, регламентируя параметры обслуживания или требования в отношении подключения модемов к компонентам АСУ ТП. Факторы риска современных АСУ ТП (SCADA-систем) базируются на необходимости поддержки их конкурентоспособности на рынке ПО (расширяемость, адаптируемость и т. д.). Также на факторы риска SCADA-систем влияет опасность осуществления их аудита и реализации необходимых изменений.

Таким образом, среди факторов риска современных SCADA-можно выделить следующие: внедрение стандартизованных протоколов и технологий со списком известных уязвимостей, связанность сети системы управления с другими сетями (например, сетью ИТсистемы), широкая доступность и распространение технической информации и документации о системах управления, высокие риски проведения аудита, высокие риски внесения исправлений. Актуальные сценарии проведения современных атак на SCADAсистемы включают атаку при помощи эксплойта, атаку злоумышленным служащим, а также управление посредством внедрения вируса.

Сетевая архитектура современных предприятий объединяет компоненты корпоративной сети и компоненты АСУ ТП, что обуславливает уязвимость SCADA-систем перед атаками с использованием эксплойтов. В данной схеме для корпоративной, внутренней и управляющей сети используются свои собственные межсетевые экраны. Однако, зачастую, на практике межсетевые экраны заменяются простыми маршрутизаторами (сетевыми коммутаторами), таблицы маршрутизации которых могут дополнительно быть неправильно настроены с точки зрения ИБ. В некоторых небезопасных случаях все три сети (корпоративная, внутренняя и управляющая) могут быть объединены воедино без использования каких-либо сетевых инструментов[[4]](#footnote-4).

Одной из проблем практически всех АСУ ТП и SCADA-систем является невысокая защищённость от злонамеренных действий конечных пользователей – управляющего и обслуживающего персонала (например, инженеров, операторов, администраторов и т. д.). Под понятием «инсайдер» подразумевается сотрудник компании, имеющий непосредственный доступ к конфиденциальным данным, системе безопасности, управляющему, сетевому или производственному оборудованию. Негативные действия инсайдера могут иметь как случайный характер, вызванный ошибкой или невнимательностью персонала, так и преднамеренный, обусловленный сознательным желанием вывести из строя АСУ ТП предприятия или создать чрезвычайное происшествие.

Современные вирусы используют уязвимости ОС, позволяющие производить повышение уровня привилегий до уровня администратора. Они используют специальные методы загрузки ПО, позволяющие не быть замеченными антивирусами, программами анализа поведения и программами для предотвращения вторжений.

Вирусное ПО может самостоятельно осуществлять вредоносную деятельность или создавать скрытый канал для последующей атаки системы злоумышленником. Первым шагом злоумышленника при атаке эксплойтом, как правило, является взлом и взятие под контроль некоторого элемента корпоративной сети, с которого впоследствии производится последующая атака элемента внутренней сети.

Примером может служить атака через сервер системы системного анализа и разработки программ (SAP) к серверу логирования, расположенному во внутренней сети. Взлом может быть осуществлён во время приёма/передачи данных системных журналов, дневной статистики, данных о текущих заказах, данных о текущем спросе и др. Имея в распоряжении сервер логирования (как правило, устройство класса Windows Server), злоумышленник может вывести его из строя, скрыть предыдущие атаки, получить доступ к чтению и редактированию конфиденциальных данных[[5]](#footnote-5).

Следующим шагом атаки злоумышленника является попытка взлома одного из элементов управляющей сети (SCADA-системы), выполняемая с использованием ранее захваченного элемента внутренней сети. Атакующий продвигается от сервера логирования к станции HMI, расположенной внутри управляющей сети. Проникновение может быть осуществлено во время обмена данными системных журналов и системной статистики, а также посредством протокола OPC и сервисов домена (domain services). Захват станции HMI (как правило, устройство класса Windows Workstation) позволяет злоумышленнику управлять настройками, манипулировать данными о текущем технологическом процессе в целях обмана сотрудников. Необходимо отметить, что для создания мнимой картины функционирования технологического процесса необходим захват и синхронизированное управление всех станций HMI, что предполагает наличие межпрограммного взаимодействия[[6]](#footnote-6).

Далее атака может идти в направлении сервера приложений, обслуживающего управляющие рабочие станции, посредством информационного обмена в рамках чтения/записи текущих параметров процесса и настроек, аварийных оповещений, диагностики управляющей шины. Управление сервером приложений (как правило, устройством класса Windows Server) позволяет осуществлять фальсификацию данных о технологическом процессе для вышестоящих компонентов (например, сервера логирования), нарушать синхронизацию отдельных компонентов SCADA-системы или продолжить атаку в направлении управляющих рабочих станций или PLC. Захват управляющей рабочей станции (как правило, устройства класса Windows Server или Windows Workstation) позволяет злоумышленнику получить доступ к PLC.

Доступность PLC позволяет управлять его работой, просматривать, модифицировать и обновлять ПО для PLC[[7]](#footnote-7).

Наиболее вероятный сценарий запланированной атаки инсайдером на АСУ ТП включает в себя несколько этапов. На первом этапе происходит создание дополнительного контура управления системой для перехвата управления и вызова аварийной ситуации. Как правило, подобные действия совершаются от имени подставного пользовательского (операторского) аккаунта в целях сокрытия следов действий инсайдера. После проведения атаки управляющий контур самоуничтожается, стирая максимально возможно количество информации в системных журналах. Выполнение данных действий может включать необходимость изменения ПО контроллеров (например, контроллера ПАЗ), что может быть осуществлено при помощи программного скрипта, выполняющего записанные ранее действия.

На втором этапе ключевые элементы АСУ ТП заражаются вредоносным ПО, позволяющим в нужный момент вывести оборудование из строя или нарушить работоспособность компьютера, имитирую атаку устройства злоумышленником. Дальнейшие действия инсайдера могут развиваться по следующей схеме. В запланированное сотрудником-инсайдером время начинается имитация атаки компьютеров АСУ ТП злоумышленниками.

Нормальная работа станций управления нарушается, сотрудники предприятия оказываются в замешательстве. Критически важное управляющее оборудование самостоятельно отключается, аварийные блокировки не срабатывают, производственное оборудование остаётся без управления. Выполнение технологического процесса нарушается, возникает существенный риск создания ЧП. Во время процедуры расследования подобного инцидента будет выявлено заражение станций вредоносным ПО, отмечены действия операторов по созданию аварийной ситуации, а также выявлен отказ системы противоаварийной защиты.

Таким образом, вина в произошедшем событии ложится на плечи неизвестного злоумышленника, заразившего систему вирусом и атаковавшего её. Злоумышленникинсайдер остаётся вне подозрений.

Для примера атаки вирусом-червём рассмотрим классического представителя данной категории вирусов – Stuxnet[[8]](#footnote-8). В качестве первого из аргументов в пользу его сложности необходимо отметить факт того, что вирус способен распространяться тремя совершенно разными путями, а именно:

– посредством инфицированных отчуждаемых носителей данных (например, USBфлеш-накопитель);

– посредством трафика внутри локальной сети;

– посредством инфицированных файлов проекта Siemens[[9]](#footnote-9).

Вирус инфицирует компьютеры посредством USB-флеш-накопителей (даже в случае выключенного автозапуска) путём ранее неизвестной уязвимости (MS10-046), связанной с ярлыками (файлами с расширением \*.lnk). Версии Stuxnet, выпущенные до марта 2010, распространялись при помощи USB-флеш-накопителей путём уязвимости, связанной с автозапуском, нежели с расширением \*.lnk. Вирус распространяется по локальной сети на компьютеры с наличием сетевых ресурсов в общем доступе путем регистрации всех учетных записей пользователей компьютера и домена. Затем программа пытается использовать все доступные сетевые ресурсы для того, чтобы скопировать и выполнить себя на удалённом ресурсе, тем самым заражая удалённый компьютер[[10]](#footnote-10).

Вирус распространяется по локальной сети, предоставляя сервис печати с помощью уязвимости нулевого дня в Windows Print Spooler (MS10-061). Вирус распространяется по локальной сети посредством уязвимости MS08-067 Windows Server Service Vulnerability (MS08-067). Вирус инфицирует компьютеры, использующие базу данных Siemens WinCC, с помощью внутренних неизменяемых системных паролей, подключаясь к SQL-серверу в целях передачи и исполнения копии вируса. Вирус распространяется, копируя себя в любые найденные файлы проектов Siemens STEP 7 (файлы с расширением \*.S7P, \*.MCP и \*.TMP), а затем исполняясь автоматически при открытии проекта[[11]](#footnote-11).

**Заключение**

Системы SCADA требуют особого внимания к вопросам информационной безопасности, так как потенциальные кибератаки и информационные злоупотребления могут привести к катастрофическим последствиям, начиная от потери конфиденциальной информации и вплоть до нарушения технологического процесса, поломок оборудования и крупных аварий.

Кибератаки различаются по объектам нападения: атаки на данные и атаки на системы управления. Атаки первого типа имеют целью нарушение конфиденциальности, целостности, либо доступности информации. Большинство сетевых атак относятся к этой категории, включая похищение номеров кредитных карт, взлом сайтов и DoS-атаки. Атаки на системы управления ставят задачей выведение из строя или получение контроля над операциями, используемыми для поддержания физической инфраструктуры: контролирующими водные ресурсы, электросети, железные дороги и т.п. Несмотря на реальность подобных атак, эксперты по безопасности утверждают, что пока кибератаки могут явно привести только к временной недоступности достаточно критичных данных, но не к потере человеческих жизней или разрушению физической инфраструктуры.

Обеспечение информационной безопасности системы SCADA нужно рассматривать как часть глобальной политики безопасности компании, что требует организации и выполнения мер безопасности и политики на нескольких уровнях:

- Определение политики безопасности;

- Обеспечение безопасности сети SCADA системы и операционной среды;

- Обеспечение безопасности приложений SCADA системы;

- Обнаружение неавторизированного доступа и вторжений извне;

- Регулирование физического доступа к SCADA системе.

Политика безопасности становится существенным элементом в сегодняшней корпоративной сети. Политика безопасности – регламентирующий документ, который позволяет организации и ее управляющему составу сформулировать четкие, ясные и понятные цели, задачи, правила и формальные процедуры, с помощью которых проектируются и организуются положения и архитектура системы информационной безопасности.

**Список использованных источников**

Безопасность систем SDACA и АСУ -ТП [Электронный ресурс] URL: https://modcon.ru/wp-content/uploads/2014/04/SCADA-Security-rus.pdf (дата обращения: 24.03.2024)

В Windows закрыты опасные уязвимости, использованные червем Stuxnet [Электронный ресурс] URL: https://www.cyberforum.ru/security/thread166039.html (дата обращения: 24.03.2024)

Вирус STUXNET - оружие нового поколения [Электронный ресурс] URL: https://cyberleninka.ru/article/n/virus-stuxnet-oruzhie-novogo-pokoleniya (дата обращения: 24.03.2024)

Вострецова Е.В. Основы информационной безопасности : учеб. пособие для студ. вузов. Екатеринбург, 2019. URL: https://elar.urfu.ru/bitstream/10995/ 73899/3/978-5-7996-2677-8\_2019.pdf (дата обращения: 24.03.2024).

Зюзев А.М., Нестеров К.Е., Головин И.С. SCADA-системы : учеб. электрон. текстовое изд. Екатеринбург, 2009. URL: https://study.urfu.ru/Aid/Publication/ 9022/1/Zyuzev\_Nesterov\_Golovin.pdf (дата обращения: 24.03.2024).

Матвейкин, В.Г. Применение SCADA-систем при автоматизации технологических процессов / В.Г. Матвейкин. – М. : Машиностроение, 2020. – 272 c

Россинская Е.Р. Современные способы компьютерных преступлений и закономерности их реализации / Е.Р. Россинская, И.А. Рядовский // Lex Russica. — 2019. — № 3 (148). — С. 87-99.

Щагин А.В., Демкин В.И., Кононов В.Ю., Кабанова А.Б. Основы автоматизации техпроцессов: Учебное пособие. – М.: Высшее образование, 2019.

Чичкарёв, Е.А. Системный анализ сложных систем управления / Е.А. Чичкарёв. – Пермь : ПГТУ, 2018. – 59 с.

SCADA - система [Электронный ресурс] URL: https://elatro.ru/products/sistemy-asu-tp/scada-sistemy/ (дата обращения: 24.03.2024)

1. Щагин А.В., Демкин В.И., Кононов В.Ю., Кабанова А.Б. Основы автоматизации техпроцессов: Учебное пособие. – М.: Высшее образование, 2019. [↑](#footnote-ref-1)
2. Безопасность систем SDACA и АСУ -ТП [Электронный ресурс] URL: https://modcon.ru/wp-content/uploads/2014/04/SCADA-Security-rus.pdf (дата обращения: 04.02.2023) [↑](#footnote-ref-2)
3. SCADA - система [Электронный ресурс] URL: https://elatro.ru/products/sistemy-asu-tp/scada-sistemy/ (дата обращения: 04.02.2023) [↑](#footnote-ref-3)
4. 2. Вострецова Е.В. Основы информационной безопасности : учеб. пособие для студ. вузов. Екатеринбург, 2019. URL: https://elar.urfu.ru/bitstream/10995/ 73899/3/978-5-7996-2677-8\_2019.pdf (дата обращения: 01.04.2021). [↑](#footnote-ref-4)
5. Россинская Е.Р. Современные способы компьютерных преступлений и закономерности их реализации / Е.Р. Россинская, И.А. Рядовский // Lex Russica. — 2019. — № 3 (148). — С. 87-99. [↑](#footnote-ref-5)
6. Зюзев А.М., Нестеров К.Е., Головин И.С. SCADA-системы : учеб. электрон. текстовое изд. Екатеринбург, 2009. URL: https://study.urfu.ru/Aid/Publication/ 9022/1/Zyuzev\_Nesterov\_Golovin.pdf (дата обращения: 10.04.2021). [↑](#footnote-ref-6)
7. Чичкарёв, Е.А. Системный анализ сложных систем управления / Е.А. Чичкарёв. – Пермь : ПГТУ, 2018. – 59 с. [↑](#footnote-ref-7)
8. В Windows закрыты опасные уязвимости, использованные червем Stuxnet [Электронный ресурс] URL: https://www.cyberforum.ru/security/thread166039.html (дата обращения: 04.02.2023) [↑](#footnote-ref-8)
9. Вирус STUXNET - оружие нового поколения [Электронный ресурс] URL: https://cyberleninka.ru/article/n/virus-stuxnet-oruzhie-novogo-pokoleniya (дата обращения: 04.02.2023) [↑](#footnote-ref-9)
10. Матвейкин, В.Г. Применение SCADA-систем при автоматизации технологических процессов / В.Г. Матвейкин. – М. : Машиностроение, 2020. – 272 c [↑](#footnote-ref-10)
11. [↑](#footnote-ref-11)