Международный союз электросвязи

МСЭ-Т X.1333

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(01/2022)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

Безопасные приложения и услуги (2) – Безопасность "умных" электросетей

Руководящие указания по безопасности при использовании инструментов удаленного доступа в системах управления, подключенных к интернету

Рекомендация МСЭ-Т X.1333

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды (1)	X.1140–X.1149
Безопасность приложений (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность умных электросетей	**X.1330–X.1339**
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1350–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределения реестра (DLT)	X.1400–X.1429
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
Киберзащита	X.1590–X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
Защита данных	X.1770–X.1789
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1333

Руководящие указания по безопасности при использовании инструментов удаленного доступа в системах управления, подключенных к интернету

Резюме

Инструменты удаленного доступа (remote access tools – RAT) широко используются в системах управления для целей контроля, управления и технического обслуживания, чтобы снизить затраты на техническое обслуживание и минимизировать время реагирования при отказах. RAT обеспечивают возможность удаленного управления системами, но в то же время незащищенная конфигурация RAT и уязвимости в RAT могут значительно увеличить площадь атаки на системы управления. Наиболее серьезную проблему представляет интерфейс доступа к системе управления из внешних сетей, который позволяет открыть злоумышленникам доступ к системе управления из интернета.

В Рекомендации МСЭ-Т X.1333 дано общее представление о безопасном использовании RAT для мониторинга, управления и технического обслуживания. В настоящей Рекомендации определены угрозы для сетевой конфигурации, возникающие при использовании RAT, и представлены руководящие указания по применению безопасной конфигурации и мер безопасности для использования RAT в системах управления, подключенных к интернету.

Обеспечение упорядоченных средств контроля безопасности при использовании RAT было бы полезно для поставщиков цифровых услуг, работающих с системами управления, ввиду сокращения поверхности атак и угроз из внешних сетей. Кроме того, целесообразно было бы выровнять уровни безопасности развитых и развивающихся стран, так как эта проблема имеет не локальный, а глобальный характер.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1333	07.01.2022 г.	17-я	11.1002/1000/14798

Ключевые слова

Система управления, руководящие указания, инструменты удаленного доступа, безопасность.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1333

Руководящие указания по безопасности при использовании инструментов удаленного доступа в системах управления, подключенных к интернету

1 Сфера применения

В настоящей Рекомендации представлены руководящие указания по безопасности при использовании инструментов удаленного доступа (RAT) в подключенных к интернету системах управления в сетях электросвязи. Она охватывает следующие вопросы:

- выявление угроз, связанных с незащищенной конфигурацией RAT, и их влияние на системы управления, подключенные к интернету;
- меры безопасности и их обоснование для защищенной конфигурации RAT;
- руководящие указания по реализации каждой из мер безопасности; и
- пример защищенной конфигурации RAT (см. Дополнение I).

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используется следующий термин, определенный в других документах.

3.1.1 интерфейс человек–машина (human machine interface) (HMI) [b-IEC 61924-2]: Часть системы, с которой взаимодействует оператор. Интерфейс – это совокупность средств, с помощью которых пользователи взаимодействуют с машиной, устройством или системой. Интерфейс предоставляет средства ввода сигналов, позволяющие пользователям управлять системой, и средства вывода сигналов, позволяющие системе информировать пользователей.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
DMZ	Demilitarized Zone	Демилитаризованная зона
DNS	Domain Name Service	Служба доменных имен
DoS	Denial of Service	Отказ в обслуживании
EWS	Engineering Workstation	Инженерная рабочая станция
HMI	Human Machine Interface	Интерфейс человек–машина

ICMP	Internet Control Message Protocol		Протокол управляющих сообщений в интернете
IDS	Intrusion Detection System		Система обнаружения вторжений
IPsec	Internet Protocol Security		Безопасность протокола Интернет
LAN	Local Area Network	ЛС	Локальная сеть
MAC	Media Access Control		Управление доступом к среде передачи
MDM	Mobile Device Management		Управление мобильными устройствами
MDMS	Meter Data Management System		Система управления данными измерений
NAC	Network Access Control		Управление доступом к сети
NFC	Near Field Communication		Связь в ближнем поле
PIN	Personal Identification Number		Персональный идентификационный номер
PLC	Programmable Logic Controller	ПЛК	Программируемый логический контроллер
RAT	Remote Access Tool		Инструмент удаленного доступа
RFID	Radio Frequency Identification		Радиочастотная идентификация
SIEM	Security Information and Event Management		Управление информацией и событиями безопасности
SSH	Secure Shell		Защищенный командный процессор
SSL	Secure Socket Layer		Протокол защищенных сокетов
TLS	Transport Layer Security		Безопасность транспортного уровня
URL	Uniform Resource Locator		Унифицированный указатель ресурса
VM	Virtual Machine	ВМ	Виртуальная машина
VPN	Virtual Private Network		Виртуальная частная сеть

5 Соглашения

В настоящей Рекомендации используются следующие соглашения.

Ключевое слово "следует" или "должен" (should) означает требование, которое рекомендуется, но не является абсолютно необходимым.

Ключевое слово "может" (may) означает необязательное требование, которое допустимо, но не имеет рекомендательного значения.

В тексте настоящей Рекомендации иногда встречается слово "может" (can или could); в этом случае оно обозначает наличие возможности.

Такие слова, как "обязан" (must), "следует" (should), "будет" (will), фигурирующие в Дополнении I, должны толковаться как не несущие нормативного смысла.

6 Обзор использования RAT в системах управления, подключенных к интернету

Системы управления используются для достижения целей производственной деятельности, таких как производство и транспортировка материалов или энергии. Система управления отвечает за обеспечение желаемого результата или решение промышленной задачи. Чтобы гарантировать работоспособность системы управления, операторы контролируют информацию и данные, поступающие от датчиков в промышленных сетях (см. рисунок 1). На основе этих данных и информации операторы могут при необходимости управлять системой. Сервисные инженеры поставщика системы управления могут получить доступ к системе управления для ее обслуживания или решения технических проблем.

Инструменты удаленного доступа (RAT) широко используются в промышленных сетях для контроля, управления и технического обслуживания систем управления, чтобы снизить затраты на техническое обслуживание и минимизировать время реагирования при отказах. Согласно отчету [b-Kruglov et al.], в первом полугодии 2018 года RAT использовались на 31,6% компьютеров систем управления, и это без учета дистанционных подключений к рабочему столу.

В большинстве систем управления RAT обычно используются для решения следующих задач:

- контроль/управление интерфейсом человек–машина (HMI) с рабочей станции оператора;
- контроль/управление HMI с инженерной рабочей станции;
- подключение нескольких операторов к одной рабочей станции оператора;
- подключение удаленных операторов к рабочей станции оператора через внешнюю сеть; и
- техническое обслуживание подключенной к интернету системы управления с компьютера сервисного инженера поставщика системы управления через внешнюю сеть.

Эти сценарии использования показывают, что использование RAT в целях контроля, управления и технического обслуживания системы управления может быть обязательным требованием для эксплуатации систем управления. Помимо этого, использование RAT понизит расходы на техническое обслуживание. Например, в первых трех из упомянутых выше сценариев использования может быть уменьшено количество лицензий на программное обеспечение HMI. Кроме того, современные интеллектуальные устройства также могут использоваться в качестве клиентов RAT. Например, конечные потребители могут контролировать фотоэлектрические элементы (PV) и управлять ими, используя RAT на своих смартфонах.

На рисунке 1 показана общая схема использования RAT в системах управления, подключенных к интернету, на основе приведенных сценариев использования.

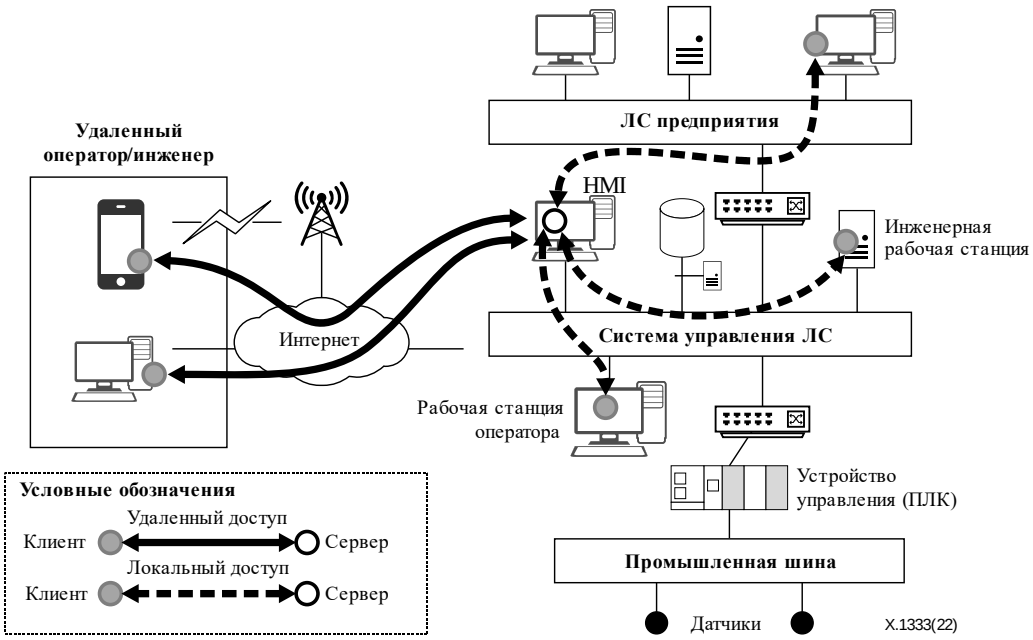

Рисунок 1 – Конфигурация сети для использования RAT в системах управления, подключенных к интернету

В других случаях оперативная система управления организации может использоваться для соединения компактной системы управления с существующими системами управления. Например, на объекте, на котором работает генератор большой мощности, можно использовать новую систему на основе топливных элементов для повышения генерируемой мощности за счет чистой энергии. В системы на основе топливных элементов входят компьютеры HMI, устройства управления, датчики, батареи и другие системы. Таким образом, в этом примере HMI и устройства управления могут быть подключены к одной и той же подсети, расположенной на периферийной стороне системы на основе топливных элементов. На рисунке 2 показана схема использования RAT для доступа к HMI на местах.

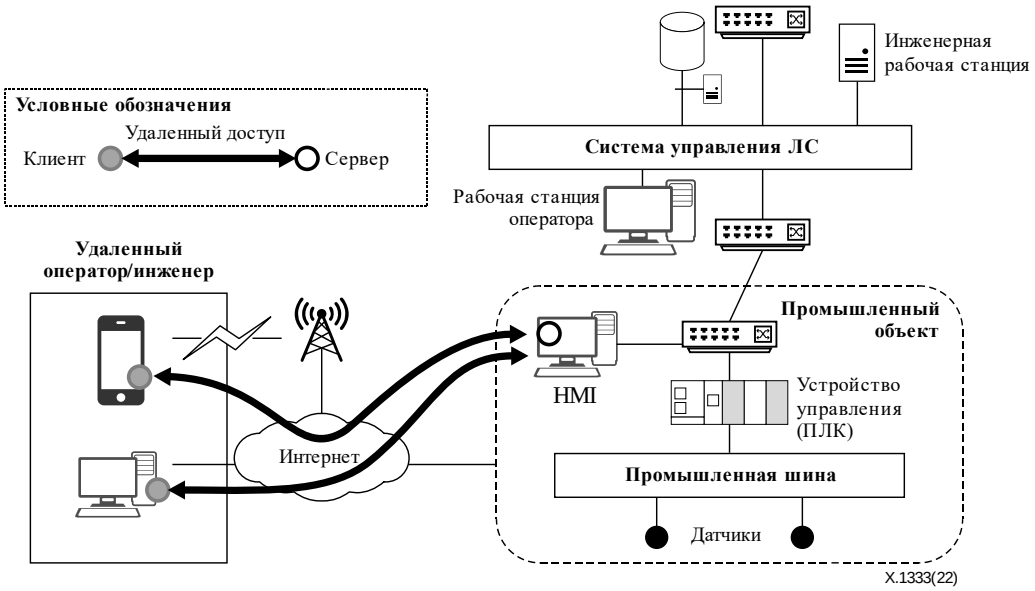

Рисунок 2 – Конфигурация сети для использования RAT в промышленной сети систем управления, подключенных к интернету

RAT обеспечивает возможность дистанционного управления системами, что помогает снизить затраты на техническое обслуживание. Однако в то же время незащищенная конфигурация RAT и уязвимости в RAT могут значительно увеличить площадь атаки на системы управления. Самая серьезная проблема заключается в том, что RAT можно использовать в качестве интерфейса для доступа к системе управления, подключенной к интернету, из внешних сетей, к которым в большинстве случаев можно получить доступ через интернет. Таким образом, как только злоумышленникам удастся взломать клиентский RAT системы управления, подключенной к интернету, они смогут вывести систему из строя. Более того, их действия трудно обнаружить. Поэтому в настоящей Рекомендации основное внимание уделяется подсоединению RAT к системам управления, подключенным к интернету, извне.

7 Угрозы при использовании RAT в системах управления, подключенных к интернету

7.1 Угрозы для клиентских приложений RAT

Клиентские приложения RAT могут быть установлены на клиентском компьютере в удаленном месте или на мобильном устройстве, принадлежащем удаленному оператору или инженеру дистанционного обслуживания. Удаленное местоположение может находиться вне зоны физической защиты организации и логической защиты ее межсетевого экрана. Кроме того, клиентскими компьютерами невозможно надежно управлять, тогда как компьютеры организации находятся под строгим контролем и жестко блокируются. Таким образом, ряд угроз при использовании RAT могут исходить от компьютеров, на которых установлены клиентские приложения RAT.

Следует учитывать перечисленные ниже угрозы (У) для клиентских компьютеров и RAT.

- У1: злоумышленник может использовать уязвимости клиентских компьютеров или RAT для их взлома. Как только злоумышленники получат полный контроль над клиентским компьютером или RAT, они смогут через RAT подключиться к системе управления.
- У2: злоумышленник может взломать систему раздельного туннелирования на клиентском компьютере. Клиентские компьютеры обычно бывают соединены не только с серверами RAT, но и с другими системами, подключенными к интернету. Таким образом злоумышленник, получивший полный контроль над клиентским компьютером, сможет передавать важную информацию, полученную от системы управления, через незащищенное интернет-соединение.
- У3: злоумышленник может установить на клиентский компьютер специальное вредоносное ПО, которое обнаруживает конфиденциальную информацию (например, регистрационный ID и пароль) и передает эту информацию. Получив эту информацию, злоумышленники могут

получить доступ к серверу RAT с помощью клиентского приложения RAT, установленного на любом другом компьютере.

- У4: пользуясь инструментами с открытым исходным кодом, злоумышленник может провести атаку методом перебора, словарную атаку или взлом пароля для получения доступа к серверу RAT.
- У5: злоумышленники могут скрывать свои действия на клиентских компьютерах, удаляя данные журнала регистрации событий. В результате угрозы организация, использующая систему управления, может оказаться не в состоянии отслеживать действия злоумышленников при расследовании инцидента.
- У6: злоумышленник может получить физический доступ к клиентским компьютерам.

7.2 Угрозы для серверов RAT

Сервер RAT может быть установлен на машине HMI в системе управления, подключенной к интернету. Поскольку сервер должен открывать службу, подключенную к интернету, злоумышленник может использовать порт этой службы. Если служба не будет надежно защищена, злоумышленник может через эту службу получить доступ к системе управления.

Следует учитывать перечисленные ниже угрозы для клиентских компьютеров и RAT.

- У7: злоумышленник может использовать уязвимости сервера RAT или машины, на которой установлен сервер RAT, для взлома машины или сервера RAT. Этот вид атаки может привести к тому, что злоумышленник получит полный контроль над системой управления. Например, как только злоумышленники получат доступ к машине или серверу RAT, они смогут повысить свои привилегии на устройстве или получить полный контроль над сервером RAT.
- У8: злоумышленник может проводить атаки типа распределенный отказ в обслуживании (DDoS) и отказ в обслуживании (DoS) на сервер RAT.

7.3 Угрозы для канала связи между клиентом и серверами

Поскольку в системе управления, подключенной к интернету, сервер и клиент RAT соединены через интернет, доступ к каналу связи может получить другой субъект. Если сообщения не зашифрованы или зашифрованы с применением неэффективных методов, содержащих общеизвестные уязвимости, то злоумышленник может воспользоваться ими и получить доступ к передаваемой информации и каналам связи.

Следует учитывать перечисленные ниже угрозы для клиентских компьютеров и RAT.

- У9: злоумышленник может воспользоваться незащищенным каналом связи, получить конфиденциальную информацию (например, регистрационный ID и пароль) и использовать эту информацию для получения доступа к серверу RAT. Когда канал связи защищен с помощью неэффективного метода шифрования, злоумышленник может добиться того же результата. Получив доступ к серверу RAT, злоумышленники могут получить полный контроль над системой управления.
- У10: злоумышленник может воспользоваться слабым протоколом, содержащим общеизвестные уязвимости, чтобы получить доступ к серверу RAT или вызвать отказ в обслуживании пользователей серверов RAT.

8 Руководящие указания по безопасности при использовании RAT в системах управления, подключенных к интернету

8.1 Руководящие указания по безопасности для клиентских приложений RAT

8.1.1 Обновление программного обеспечения

Меры обеспечения безопасности

Программное обеспечение RAT, операционная система и любое другое программное обеспечение на стороне клиента следует поддерживать в актуальном состоянии.

Преследуемая цель

Программное обеспечение может иметь неизвестные уязвимости, используемые при усовершенствованных методах атак. Вновь обнаруженная уязвимость называется "уязвимость нулевого дня". Злоумышленники могут использовать уязвимости нулевого дня для взлома клиентских устройств RAT. В последнее время количество уязвимостей, связанных с программным обеспечением RAT, увеличилось. В 2019 году была обнаружена 31 уязвимость систем удаленного доступа к рабочему столу компьютера по сети (VNC) и ПО подобного типа. Когда обнаруживаются новые уязвимости, поставщики программного обеспечения RAT выпускают обновления для системы безопасности, посредством которых пользователи могут уменьшить влияние уязвимостей. Обновление программного обеспечения – один из простейших способов обеспечить безопасность клиентских устройств.

Руководящие указания по реализации

Чтобы поддерживать программное обеспечение в актуальном состоянии, прежде всего необходимо следить за тем, не появились ли новые обновления. К сожалению, пользователям нелегко выполнять такую регулярную проверку, поэтому следует рассмотреть целесообразность следующего автоматизированного подхода к поддержанию программного обеспечения в актуальном состоянии.

a) Проверка обновлений безопасности должна запускаться всякий раз, когда выполняется клиентское ПО RAT.

b) Если имеется новая версия программного обеспечения или новое обновление безопасности, их следует применить к клиентским программам перед их выполнением.

c) Проверка обновлений безопасности также может запускаться регулярно во время работы клиентского RAT.

d) Если имеется новая версия программного обеспечения или новое обновление безопасности, их следует применить к клиентским программам после завершения их работы.

В некоторых случаях после установки обновления безопасности клиентское устройство RAT необходимо перезапустить. В отличие от обычного клиентского компьютера, клиентские RAT системы управления не могут перезапускаться немедленно, поскольку удаленный оператор/инженер должен постоянно контролировать систему управления. В этой среде в ходе проверки обновлений безопасности обновления устанавливаются после получения подтверждения от пользователя.

Кроме того, должны обновляться операционная система и любое другое программное обеспечение на устройстве, на котором запущено клиентское ПО RAT. Должна поддерживаться функция автоматического обновления операционной системы. Следует регулярно проверять наличие обновлений безопасности для каждого приложения и безотлагательно применять исправления для системы безопасности, когда они станут доступными.

8.1.2 Целостность программного обеспечения

Меры обеспечения безопасности

Должна быть защищена целостность программного обеспечения RAT на стороне клиента.

Преследуемая цель

На стороне клиента может быть установлена модифицированная версия программного обеспечения RAT. Злоумышленник может взломать сервер обновлений или распространять аномальные обновления по электронной почте с применением фишинга. Программное обеспечение RAT, зараженное вредоносным кодом, ведет себя как обычное, но вредоносный код обеспечивает утечку информации или установление соединения со злоумышленником, когда ему это требуется. Таким образом, для предотвращения аномального поведения, вызванного вредоносным ПО RAT, должна быть защищена целостность программного обеспечения RAT.

Руководящие указания по реализации

Поскольку, как упоминалось выше, злоумышленники могут распространять вредоносное программное обеспечение RAT через официальную цепочку поставок, пользователю сложно определить, было ли программное обеспечение модифицировано или нет. Поэтому для защиты целостности программного обеспечения RAT следует использовать процедуру автоматической проверки целостности.

Для осуществления процедуры автоматической проверки целостности должен использоваться следующий подход.

a) Процедура проверки целостности должна запускаться при запуске программного обеспечения или при запуске процедуры обновления.

b) Программное обеспечение или процедуру обновления следует запускать, только если нет никаких признаков того, что программное обеспечение было изменено.

c) Статус процедуры проверки целостности должен отображаться на экране, чтобы пользователь знал, что программное обеспечение работает нормально.

d) Признак целостности программного обеспечения должен создаваться криптографическим методом, чтобы гарантировать, что программное обеспечение не изменено кем-либо еще. Для этого метода следует использовать надежный криптографический алгоритм.

8.1.3 Надежная конфигурация клиентского RAT

Меры обеспечения безопасности

Конфигурация RAT на стороне клиента должна соответствовать политике безопасности организации, которой принадлежит система управления, подключенная к интернету.

Преследуемая цель

Несмотря на то что программное обеспечение RAT может гарантировать надежную связь, безопасное использование RAT возможно только при условии его правильной конфигурации. Как правило, желая избежать неудобств, пользователи не хотят включать функции обеспечения безопасности и использовать надежный пароль. Кроме того, если пользователь не знает, как правильно настроить протокол безопасной передачи данных по протоколу Интернет (IPSec), ошибки в конфигурации повышают вероятность злоупотребления клиентским программным обеспечением RAT.

Руководящие указания по реализации

Чтобы уменьшить вероятность неправильной конфигурации клиентского RAT, лучше, чтобы его настраивала организация, эксплуатирующая систему управления. Следует рассмотреть нижеперечисленные подходы к управлению конфигурацией клиентского RAT в рамках организации.

a) Использование статического адреса протокола Интернет (IP) для сервера RAT. Если для доступа к шлюзу виртуальной частной сети (VPN) или серверу RAT используется унифицированный указатель ресурса (URL), то удаленные операторы/инженеры могут подвергаться нескольким видам атак, таких как фишинг, подмена кеша службы доменных имен (DNS) (спуфинг) и отравление кеша DNS. Использование статического IP-адреса или жестко запрограммированного IP-адреса на стороне сервера позволяет ослабить эти угрозы и обеспечить аутентификацию сервера для удаленных операторов/инженеров по защищенному каналу связи.

b) Решение для управления доступом к сети (NAC) или управления мобильными устройствами (MDM). NAC предоставляет возможности для проверки состояния компьютера или ноутбука, в то время как MDM поддерживает возможности проверки мобильных устройств и управления ими. NAC помогает организациям побудить удаленных операторов/инженеров настроить компьютер, на котором запущен клиентский RAT, проверяя конфигурацию устройства перед установлением соединения. Если устройство настроено неправильно, NAC запретит сетевой трафик от этого устройства до тех пор, пока удаленные операторы/инженеры не исправят настройку. Если удаленные операторы используют для доступа к серверу RAT мобильные устройства, то вместо NAC используется MDM.

c) Образ виртуальной машины (ВМ). Организация, которой принадлежит система управления, может распространять образ виртуальной машины среди удаленных операторов/инженеров. При создании организацией такого образа все конфигурации, относящиеся к клиентскому устройству, VPN-клиенту и клиентскому RAT, должны быть настроены на основе политики безопасности организации. Кроме того, чтобы защитить сам образ виртуальной машины, его следует зашифровать и хранить на устройствах удаленных операторов/инженеров, когда он не используется.

8.1.4 Управление доступом пользователей к клиентским устройствам

Меры обеспечения безопасности

Доступ к клиентскому программному обеспечению RAT должны получать только авторизованные пользователи.

Преследуемая цель

Если доступ к клиентскому программному обеспечению RAT ограничен авторизованными удаленными операторами/инженерами, то возможность злоупотребления клиентским RAT может быть снижена.

Однако действующие на законных основаниях удаленные операторы/инженеры, использующие программное обеспечение RAT, могут временно покинуть рабочее место, и тогда появляется возможность злоупотребления продолжающимся сеансом связи. Поэтому когда удаленные операторы/инженеры прекращают или приостанавливают работу, устройство должно блокироваться. По возвращении удаленных операторов/инженеров к работе с клиентским устройством RAT они могут восстановить сеанс связи, используя установленную процедуру идентификации и аутентификации.

Руководящие указания по реализации

Такой контроль можно реализовать, если удаленные операторы/инженеры используют учетную запись, отличную от учетной записи, используемой для решения обычных задач при запуске клиентского программного обеспечения RAT. Другими словами, удаленный оператор/инженер должен иметь еще одну учетную запись для использования клиентского RAT. Кроме того, для учетной записи должен использоваться надежный пароль.

Эффективный способ решения последней проблемы – блокирование сеанса. Возможны два способа блокирования сеанса: 1) на уровне операционной системы и 2) на уровне приложения. Возможность блокирования сеанса имеется в большинстве операционных систем, поэтому ее следует использовать после определенного периода бездействия. Возможность блокирования сеанса на уровне приложения зависит от программного обеспечения RAT. Таким образом, наличие возможности блокирования сеанса должно быть основным критерием при выборе организацией программного обеспечения RAT для своей оперативной системы управления.

8.1.5 Защита на физическом уровне

Меры обеспечения безопасности

Физический доступ к устройству, на котором запущено клиентское программное обеспечение RAT, должны иметь только авторизованные удаленные операторы/инженеры, а помещение, в котором операторы/инженеры работают с устройствами, должно быть защищено от несанкционированного доступа.

Преследуемая цель

Даже если программное обеспечение устройства и клиентское ПО RAT надежно настроены для правильного использования их функций защиты, само устройство и помещение, в котором оно находится, должны быть защищены от несанкционированного доступа со стороны любых злоумышленников.

Руководящие указания по реализации

Для обеспечения физической защиты устройств, программного обеспечения и их рабочей среды необходимо учитывать следующие факторы:

a) помещение, в котором работают удаленные операторы/инженеры, должно быть защищено соответствующей системой контроля доступа с использованием технологии связи ближнего действия (NFC) или радиочастотной идентификации (RFID). Для более надежной защиты можно рассмотреть возможность использования биометрической системы контроля доступа (отпечатков пальцев, радужной оболочки глаза, распознавания лиц и т. п.);

b) перед входом в помещение должна быть установлена камера видеонаблюдения;

c) устройство, на котором запущено клиентское программное обеспечение RAT, должно быть защищено от кражи с помощью троса с замком или других средств защиты.

8.2 Руководящие указания по безопасности для серверов RAT

8.2.1 Аутентификация пользователей

Меры обеспечения безопасности

Служба RAT должна разрешать пользователям удаленный доступ к ресурсам только с применением двухфакторной аутентификации.

Преследуемая цель

Традиционный способ аутентификации по ID и паролю ненадежен, и факт знания пароля или персонального идентификационного номера (PIN) сам по себе не может гарантировать, что пользователь действительно имеет надлежащее разрешение.

Для идентификации законных пользователей и предоставления им доступа к системным ресурсам на локальном уровне применяются методы управления физическим доступом. В этом случае, даже если злоумышленник знает ID и пароль законного пользователя, ему будет нелегко получить прямой доступ к системным ресурсам. Однако при удаленном доступе применить методы физической защиты и идентификации пользователей непросто. Поэтому вместо методов физической защиты применяется двухфакторная аутентификация, позволяющая снизить вероятность использования чужого ID и пароля, даже если они были украдены.

Руководящие указания по реализации

К факторам аутентификации относится то, что вам известно (фактор знания); то, что вам принадлежит (фактор владения); то, кем вы являетесь (неотъемлемый фактор); и то, где вы находитесь (фактор местоположения). В настоящее время двухфакторная аутентификация, как правило, реализуется через фактор владения и фактор знания или через неотъемлемый фактор и фактор знания.

В последнее время в большинстве мобильных устройств (ноутбуках, планшетах, смартфонах) используются биометрические методы, поэтому лучшим вариантом для двухфакторной аутентификации, вероятно, могут считаться неотъемлемые факторы, включая отпечатки пальцев, радужную оболочку глаза или черты лица.

Однако в некоторых случаях использование биометрических методов невозможно. Например, если удаленные пользователи в рабочее время носят перчатки, не следует использовать отпечатки пальцев. В этих случаях могут применяться факторы владения, такие как криптографические токены.

Большинство программ RAT обеспечивают возможность ограничения времени ожидания при аутентификации. В таком случае сервер RAT отклоняет запрос аутентификации, если он не получает ответ от пользователя в течение определенного времени. Это поможет снизить вероятность атак типа отказ в обслуживании.

8.2.2 Авторизация пользователей

Меры обеспечения безопасности

Учетные записи удаленных пользователей должны иметь лишь минимальные привилегии, необходимые для выполнения соответствующих функций.

Преследуемая цель

Чтобы ограничить негативные последствия атаки, привилегии удаленного пользователя должны быть ограничены минимальными привилегиями, необходимыми для выполнения его функций.

Руководящие указания по реализации

Программное обеспечение RAT, как правило, не предусматривает поддержку детализированного метода авторизации. Большая часть программ RAT позволяет реализовать только режимы двух типов – режим только для чтения и режим полного управления. Таким образом, если злоумышленники смогут получить доступ к серверу RAT, они полностью взломают устройство. Чтобы избежать этой угрозы, привилегии, предоставляемые учетным записям удаленных пользователей, должны быть ограничены минимумом, необходимым для выполнения их функций.

Прежде всего, учетная запись удаленного пользователя не должна быть учетной записью администратора и ей не должны предоставляться права, позволяющие вносить изменения на сервере

RAT. В число ограниченных прав могут входить права установки программного обеспечения, настройки ОС и настройки системы.

Во-вторых, должно также применяться управление доступом к приложению. Учетная запись удаленного пользователя не может запускать никакое программное обеспечение, кроме программного обеспечения системы контроля и управления. Если удаленный пользователь может открыть терминальную программу на машине сервера RAT, то через этот сервер он сможет получить доступ к другим системам. Это создало бы весьма благоприятные возможности для злоумышленников.

8.2.3 Периодическая повторная аутентификация

Меры обеспечения безопасности

Сервер RAT должен периодически аутентифицировать пользователей и клиентские устройства.

Преследуемая цель

Чтобы гарантировать, что удаленным доступом могут пользоваться только авторизованные удаленные операторы/инженеры, сервер RAT должен требовать от них периодической повторной аутентификации во время длительных сеансов удаленного доступа. Это поможет гарантировать, что посторонние лица не смогут воспользоваться функцией удаленного доступа, даже если устройство было украдено во время активного сеанса связи между сервером и клиентом RAT.

Кроме того, повторная аутентификация на уровне сети помогает понизить вероятность атак с перехватом сеанса.

Руководящие указания по реализации

Само программное обеспечение сервера RAT не обеспечивает возможности повторной аутентификации по истечении определенного времени, но большинство шлюзов VPN обеспечивают такую функцию безопасности. Поэтому, чтобы должным образом реализовать такой контроль, следует использовать VPN между клиентом и сервером RAT.

Кроме того, большинство шлюзов VPN предоставляют возможность повторной аутентификации клиента. Следовательно, организация должна реализовать возможности шлюза VPN для аутентификации пользователя или устройства по истечении определенного периода времени. Например, когда связь с RAT осуществляется через протокол безопасности транспортного уровня (TLS) версии 1.3, должно быть включено расширение аутентификации клиента после установления связи. Когда это расширение включено, после установления соединения TLS сервер TLS запрашивает аутентификацию клиента.

8.2.4 Обновление программного обеспечения

Меры обеспечения безопасности

Программное обеспечение сервера RAT, операционная система и любое другое программное обеспечение на серверном устройстве следует поддерживать в актуальном состоянии.

Преследуемая цель

Цели, соответствующие требованию, рассматриваемому в пункте 8.2.4, аналогичны целям, перечисленным в пункте 8.1.1.

Руководящие указания по реализации

Руководящие указания, соответствующие требованию, рассматриваемому в пункте 8.2.4, аналогичны указаниям, перечисленным в пункте 8.1.1.

8.3 Руководящие указания по безопасности для сетей

8.3.1 Управление доступом к сети

Меры обеспечения безопасности

Доступ к сетевым соединениям между сервером и клиентом RAT должен быть разрешен только легитимным пользователям.

Преследуемая цель

Доступ к сетевым соединениям – это один из первых шагов по взлому службы или системы. Злоумышленники могут собрать информацию и данные, передаваемые между сервером и клиентом RAT, и ввести в канал связи фальсифицированные данные, что позволит организовать атаку через посредника, распространение вредоносного ПО или DoS-атаку. Чтобы защитить службу и систему управления RAT, следует перекрыть злоумышленникам доступ к сетевым соединением между сервером и клиентом RAT.

Руководящие указания по реализации

Существует несколько способов контроля доступа к сетевым соединениям и их защиты. Как вариант можно рассмотреть следующие методы.

- Для предотвращения доступа неавторизованных пользователей к соединению между системой управления данными измерений (MDMS) и сторонним поставщиком услуг можно рассмотреть возможность использования выделенной линии.
- Для связи между клиентом и сервером RAT следует применять защищенные соединения, такие как IPsec и протокол защищенных сокетов (SSL) VPN. Трафик RAT должен туннелироваться внутри VPN.
- Если использование VPN невозможно, то удаленный доступ должен осуществляться через TLS версии не ниже 1.3.

При использовании безопасного метода связи, включая VPN и TLS, следует применять надежный криптографический алгоритм. Ряд примеров надежных алгоритмов и значений длины ключей приведены в [b-ITU-T X.1197]. Во время настройки канала связи VPN-шлюз или сервер RAT должны отклонять запросы на установление соединения, если клиент не использует надежные алгоритм и длину ключа.

8.3.2 Взаимная аутентификация на уровне сети

Меры обеспечения безопасности

В канале связи между сервером RAT и клиентом RAT должна применяться взаимная аутентификация.

Преследуемая цель

Следует реализовать метод взаимной аутентификации каналов связи, чтобы клиент RAT мог проверить легитимность сервера RAT перед предоставлением ему учетных данных для аутентификации. Эта функция позволит службе RAT избежать атак через посредника между клиентом и сервером RAT.

Руководящие указания по реализации

Когда в канале связи RAT используется IPsec, SSL VPN или связь через TLS, для взаимной аутентификации следует использовать сертификат сервера и сертификат клиента. Клиент аутентифицирует сервер, проверяя сертификат сервера, чтобы убедиться в легитимности сервера.

Большинство решений VPN предоставляют функцию проверки легитимности сервера, но во многих случаях эта функция не включена. Таким образом, когда для защиты службы RAT в системе управления используется VPN, следует включить опцию аутентификации сервера.

Кроме того, в TLS обычно только сервер аутентифицирует клиента, проверяя его учетные данные, такие как сертификат, поскольку аутентификация сервера необязательна. Поэтому если связь между сервером и клиентом защищена TLS службы RAT, следует требовать взаимного обмена сертификатами между сервером и клиентом.

Наконец, должны быть включены функция блокировки по превышению времени аутентификации и функция ограничения одновременных сеансов. Ключевым моментом для предотвращения атак типа отказ в обслуживании является правильный сброс запросов на соединение, ожидающих ответа на аутентификацию клиента.

8.3.3 Обнаружение аномального поведения в сети

Меры обеспечения безопасности

В сети, к которой подключен сервер RAT, должно осуществляться обнаружение аномального поведения.

Преследуемая цель

Даже если на стороне клиента RAT применяются различные методы безопасности, все же существует вероятность того, что устройство, на котором запущен клиентский RAT, будет взломано. Например, если злоумышленники смогут получить доступ к сети подключенной к интернету системы управления через взломанный клиентский RAT, они также смогут получить доступ к любым ресурсам, доступным серверу RAT. В этой ситуации единственная разница между удаленными операторами/инженерами и злоумышленниками заключается в их поведении. Удаленные операторы/инженеры знают сеть и систему, к которой они подключены, тогда как злоумышленникам необходимо провести разведку, чтобы выяснить, в каком месте сети находится искомый объект. Соответственно, система обнаружения аномального поведения в сети, основанная на анализе сетевого трафика, может помочь в обнаружении кибератак.

Руководящие указания по реализации

Система обнаружения аномального поведения в сети должна отслеживать и проверять все сообщения между клиентом и сервером RAT. Кроме того, в системе управления, подключенной к интернету, система обнаружения должна отслеживать и проверять все сообщения от устройства, на котором запущен сервер RAT, адресованные любым другим устройствам. Таким образом, система обнаружения должна быть размещена в той же подсети, где расположен сервер RAT, и должна собирать трафик от сетевого устройства, в котором разрешена политика зеркального отображения портов. Например, в сети, подобной той, что показана на рисунке 2, разрешена политика зеркального отображения портов сетевого коммутатора в промышленной сети, и система обнаружения собирает трафик из интерфейса, в котором разрешена политика зеркального отображения портов.

Когда применяется метод надежной связи, такой как IPsec, SSL VPN или связь через TLS, то устройство защиты, обеспечивающее защищенный канал связи, должно размещаться на периметре подсети, в которой расположен сервер RAT. Например, устройство VPN следует разместить перед сетевым устройством, чтобы система обнаружения аномального поведения в сети могла проверять все пакеты.

Методы обнаружения можно разделить на три типа: статическое обнаружение, обнаружение злоупотребления и обнаружение аномалий. В среде, в которой используются средства удаленного доступа, следует применять комбинацию из функций выявления злоупотреблений и аномалий для обнаружения известных и неизвестных атак.

8.3.4 Защищенная конфигурация сети

Меры обеспечения безопасности

Сеть, в которой установлен сервер RAT, должна быть правильно сегментирована и изолирована.

Преследуемая цель

Сегментация сети – это разделение сети на несколько более мелких сетей, а изоляция – это применение политики управления обменом данными между хостами. Отделив сеть, в которой установлен сервер RAT, от других сетей, можно предотвратить доступ злоумышленников к другим ресурсам системы управления, даже если сервер RAT взломан.

Руководящие указания по реализации

Сеть, в которой установлен сервер RAT, должна быть отделена от других сетей в системе управления, а обмен данными с сервером RAT должен контролироваться в соответствии с правилами белого списка. Меры безопасности этого типа можно реализовать с использованием концепции демилитаризованной зоны (DMZ). Межсетевой экран разделяет подсеть, содержащую сервер RAT, и в соответствии с его правилами разрешена только авторизованная связь, например 1) между клиентом и сервером RAT и 2) между сервером RAT и другими ресурсами в системе управления. В качестве правил межсетевого

экрана может применяться список управления доступом на уровне обслуживания. Это означает, что правила должны определяться как комбинация IP-адреса и номера порта.

Например, в промышленной сети HMI может быть отделен от других ресурсов межсетевым экраном, как показано на рисунке 3. Межсетевой экран проверяет все входящие и исходящие пакеты сервера RAT в соответствии со своими правилами, и эти правила определяют, каким службам на сервере RAT разрешено связываться с теми или иными службами на других устройствах. По инициативе службы программного обеспечения инженерной рабочей станции (EWS) может устанавливаться связь по HMI с устройством управления (например, программируемым логическим контроллером (ПЛК), как показано на рисунке 3). Связь же по HMI, инициированная защищенным командным процессором (SSH), блокируется межсетевым экраном.

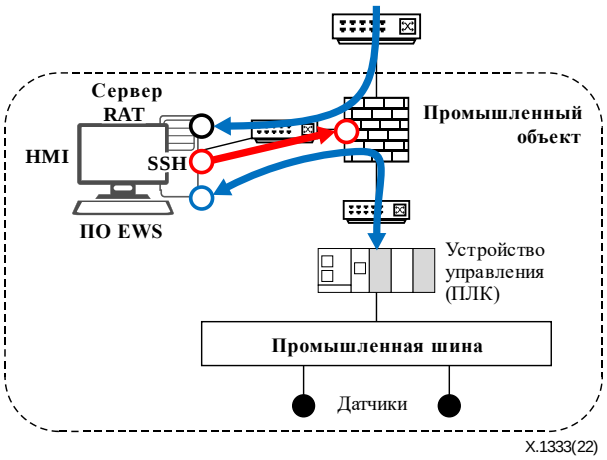

Рисунок 3 – Сегментация и изоляция сети для использования RAT в промышленной сети

8.4 Руководящие указания по безопасности для журналов регистрации событий

8.4.1 Регистрация событий

Меры обеспечения безопасности

События, связанные с безопасностью системы и сети, должны регистрироваться, а журналы регистрации событий должны быть защищены.

Преследуемая цель

Основой управления безопасностью любой системы служат журналы регистрации событий безопасности системы и сети. Просматривая и анализируя события безопасности, можно вовремя обнаружить проблемы безопасности. Таким образом, чем более детализированные журналы событий создаются сервером RAT, тем легче организации обнаружить проблемы безопасности.

Руководящие указания по реализации

Некоторые программы RAT обеспечивают возможность более детального ведения журнала, например с регистрацией событий, связанных с использованием каждого приложения и манипулированием данными на сервере, в то время как другие предоставляют лишь возможности регистрации простых событий, таких как подключение к серверу RAT и отключение от него. Таким образом, при выборе программного обеспечения RAT организации следует учитывать степень детализации журналов регистрации событий безопасности, создаваемых программным обеспечением RAT.

Если программное обеспечение RAT позволяет вести простой журнал регистрации событий, организации также следует учитывать возможность ведения журнала событий операционной системы, поверх которой установлен сервер RAT. Для этого учетные записи удаленных пользователей на сервере должны быть отделены от других учетных записей. В этом случае для выявления аномального поведения администратор безопасности должен просматривать события безопасности, записанные учетной записью удаленного пользователя.

В дополнение к журналу системных событий следует вести журнал событий сети. Должны регистрироваться все запросы на установление соединений RAT и их результаты (то есть успех или

неудача). Более того, должны регистрироваться все события, относящиеся к протоколам удаленного соединения, таким как протоколы терминала, протоколы промышленного управления и протокол управляющих сообщений в интернете (ICMP). Как было сказано выше, на первом этапе злоумышленник обычно проводит разведку системы. Для разведки могут использоваться различные протоколы удаленного соединения. Таким образом, журналы событий сети помогут администраторам безопасности обнаружить аномальное поведение на сервере RAT.

Созданные журналы событий должны надежно храниться на сервере журналов. Если журналы хранятся в локальном хранилище системы, есть вероятность, что злоумышленники подделают журналы или повредят их. Поэтому журналы событий следует хранить на отдельном журнальном сервере.

Администратор безопасности должен регулярно просматривать и анализировать журналы событий.

8.5 Связь между мерами обеспечения безопасности и угрозами безопасности

В таблице 1 показана связь между мерами обеспечения безопасности и угрозами безопасности; кружок в ячейке указывает на то, что для устранения или смягчения последствий данной угрозы должна быть реализована конкретная мера обеспечения безопасности.

Таблица 1 – Связь между мерами обеспечения безопасности и угрозами безопасности

		7.1. Клиенты						**7.2. Серверы**		**7.3. Сети**	
		У1	**У2**	**У3**	**У4**	**У5**	**У6**	**У7**	**У8**	**У9**	**У10**
Клиенты	8.1.1. Обновление программного обеспечения	O									
	8.1.2. Целостность программного обеспечения	O	O								
	8.1.3. Защищенная конфигурация	O	O	O							
	8.1.4. Управление доступом пользователей				O		O				
	8.1.5. Физическая защита						O				
Серверы	8.2.1. Аутентификация пользователей								O		
	8.2.2. Авторизация пользователей						O				
	8.2.3. Периодическая повторная аутентификация						O				
	8.2.4. Обновление программного обеспечения							O			
Сети	8.3.1. Управление доступом к сети									O	
	8.3.2. Взаимная аутентификация								O	O	
	8.3.3. Обнаружение аномального поведения					O				O	O
	8.3.4. Защищенная конфигурация сети										O
Журналы	8.4.1. Ведение журналов					O					

Дополнение I

Пример защищенной конфигурации инструментов удаленного доступа в системе эксплуатации устойчивых источников энергии

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Обзор системы

На генераторах установлено множество датчиков и исполнительных механизмов. Датчики предоставляют данные измерения параметров устройств управления (например, ПЛК на рисунке I.1), и по этим данным операторы следят за состоянием генераторов с помощью HMI или инженерной рабочей станции. В зависимости от статуса операторы управляют исполнительными механизмами через HMI (или инженерную рабочую станцию) и ПЛК. Например, при приближении тайфуна операторы останавливают вращение лопастей ветряной турбины. Сеть, соединяющая датчики, исполнительные механизмы и устройства управления, называется *промышленной сетью*. В промышленной сети для контроля и управления генераторами обычно используется интерфейс человек–машина.

В некоторых случаях генераторы, использующие устойчивые источники энергии, такие как ветер (ветряные турбины), водород (топливные элементы) и солнечная энергия (фотоэлементы), эксплуатируются удаленными операторами. Удаленные операторы контролируют состояние генераторов и управляют ими для достижения эффективной выработки электроэнергии.

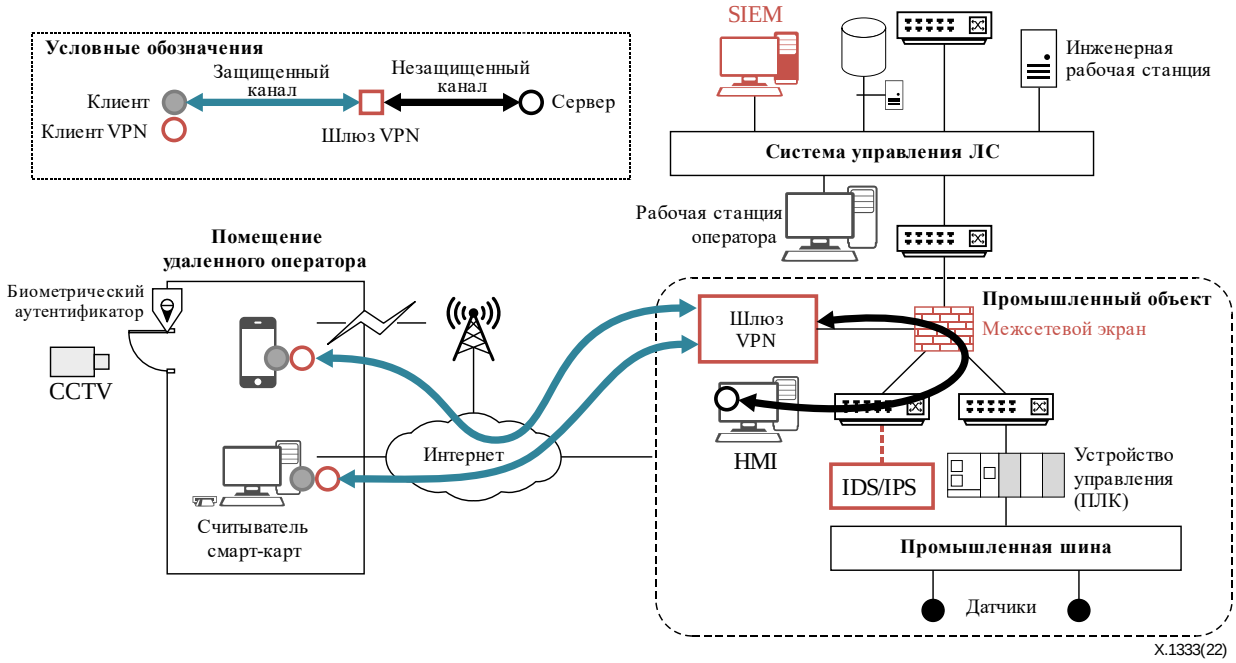

Рисунок I.1 – Пример защищенной сети для системы управления эксплуатацией устойчивых источников энергии

I.2 Защищенная конфигурация

На рисунке I.1 показан пример конфигурации защищенной сети для эксплуатации устойчивых источников энергии. В остальных пунктах этого раздела описаны меры обеспечения безопасности по каждому из компонентов, в число которых входят клиент RAT, сервер RAT, сеть и журнал событий безопасности.

I.2.1 Клиент RAT

Для клиента RAT создается отдельная учетная запись, и доступ к программному обеспечению клиента осуществляется только через эту учетную запись.

Всякий раз, когда удаленный оператор запускает клиентское программное обеспечение RAT, запускаются процессы проверки обновлений и целостности, и перед запуском клиентского программного обеспечения RAT устанавливается обновление.

Клиент NAC проверяет уровень безопасности устройства и блокирует подключение к интернету, если какая-либо настройка безопасности пропущена. Например, если не включены антивирусное программное обеспечение и персональный межсетевой экран, то NAC не допустит установления соединения.

Все устройства, на которых запущен клиентский RAT, эксплуатируются в помещении удаленных операторов. Управление доступом в это помещение осуществляется с помощью биометрического аутентификатора (например, отпечатков пальцев или распознавания лиц) и системы видеонаблюдения, установленной перед дверью в это помещение.

I.2.2 Сервер RAT

При попытке удаленных операторов установить соединение через клиентский RAT требуется двухфакторная аутентификация (например, пароль и смарт-карта). Кроме того, для шлюза VPN и сервера RAT используются статические IP-адреса.

Перед взаимной аутентификацией хост, запрашивающий соединение, фильтруется на шлюзе VPN по IP-адресу и адресу управления доступом к среде передачи (MAC). Кроме того, время сохранения канала связи между VPN-клиентом и VPN-шлюзом составляет 8 часов. Таким образом, через каждые 8 часов удаленные операторы должны повторно предоставлять свой пароль и смарт-карту для VPN-соединения.

Учетные записи удаленных операторов в HMI отделены от других учетных записей, чтобы ограничить права удаленных операторов и создать подробные журналы событий для учетных записей.

I.2.3 Сеть

Канал связи между клиентом и сервером RAT защищается VPN IPsec. Перед подключением к серверу RAT клиент VPN, установленный на устройстве удаленного оператора, должен установить безопасный канал связи со шлюзом VPN. Чтобы обеспечить 128-битовый минимальный уровень защиты, используется криптографический пакет *Suite-B-GCM-256* для VPN IPsec, как указано в [b-IETF RFC 6379]. Для аутентификации IKEv2 применяется *ECDSA-256* для VPN IPsec, как указано в [b-IETF RFC 6380]. Для обеспечения баланса между степенью защиты и накладными расходами установленная продолжительность сеанса SA IKE составляет 24 часа, а сеанса SA IPsec – 8 часов.

Сеть промышленного объекта разделена на два сегмента – DMZ для HMI и промышленная сеть для ПЛК, датчиков и исполнительных механизмов. Кроме того, для разделения сетей между локальной сетью (ЛС) системы управления, промышленной сетью и DMZ расположены межсетевые экраны. Таким образом, поток данных из EWS в HMI для передачи в промышленную сеть разрешен, но любой другой трафик от HMI в любую другую сеть блокируется межсетевым экраном.

В DMZ установлена система обнаружения вторжений (IDS) или IPS, которая и принимает входящий и исходящий сетевой трафик из порта коммутатора, настроенного для зеркального отображения трафика.

I.2.4 Журнал регистрации событий безопасности

События безопасности, генерируемые учетными записями удаленного доступа, регистрируются в системе HMI и передаются в систему управления информацией и событиями безопасности (SIEM). Администратор безопасности организации, эксплуатирующей устойчивые источники энергии, периодически просматривает журналы, используя систему SIEM.

Библиография

[b-ITU-T X.1197] Recommendation ITU-T X.1197 (2012), *Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection.*

[b-IEC 61924-2] IEC 61924-2:2012, *Maritime navigation and radiocommunication equipment and systems – Integrated navigation systems – Part 2: Modular structure for INS – Operational and performance requirements, methods of testing and required test results.*

[b-IETF RFC 6379] RFC 6379 (2011), *Suite B Cryptographic Suites for IPsec*.

[b-IETF RFC 6380] RFC 6380 (2011), *Suite B Profile for Internet Protocol Security (IPsec)*.

[b-Kruglov et al.] Кирилл Круглов, Евгений Гончаров (2018 г.), *Угрозы использования RAT в ICS*, технический отчет, Kaspersky Lab ICS CERT.
https://ics-cert.kaspersky.ru/media/KL_RAT_ICS_RUS.pdf

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и умные города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2022 год