Международный союз электросвязи

МСЭ-Т X.1332

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(03/2020)

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

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

Руководящие указания по безопасности услуг интеллектуального учета в "умных" электросетях

Рекомендация МСЭ-Т X.1332

ITU-T

Международный союз электросвязи

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	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	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	
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.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	X.1400–X.1429
Протоколы безопасности	X.1450–X.1459
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
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

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

Рекомендация МСЭ-Т X.1332

Руководящие указания по безопасности для устройств домашней сети (HAN) в системах "умных" электросетей

Резюме

Услуги интеллектуального учета широко распространены по всему миру, для того чтобы повысить эффективность и надежность электросетей путем сбора информации об использовании электроэнергии от потребителей и предоставления такой информации потребителям. Эти данные могут служить для оценки спроса потребителей на электроэнергию, а данные оценки потребления – для корректировки спроса на электроэнергию или изменения режима потребления электроэнергии потребителями благодаря предоставлению им информации об использовании электроэнергии. Вместе с тем при функционировании услуг интеллектуального учета могут происходить нарушения, обусловленные различными угрозами. Например, неверные данные учета могут привести к принятию ошибочных решений по управлению спросом, а злонамеренное использование функций регулирования нагрузки может нанести экономический ущерб и физический вред потребителям. В Рекомендации МСЭ-Т X.1332 содержатся руководящие указания по безопасности услуг интеллектуального учета, которые позволят поставщикам услуг реализовать соответствующие меры защиты для обеспечения безопасности предоставляемых ими услуг. В Рекомендации определены угрозы безопасности услуг интеллектуального учета и способы атак, направленных на эти услуги, а также требования по безопасности и средства обеспечения безопасности для снижения таких угроз и смягчения последствия атак, соответственно.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1332	26.03.2020 г.	17-я	11.1002/1000/14086

Ключевые слова

Передовая инфраструктура учета, руководящие указания по безопасности, "умная" электросеть, услуга интеллектуального учета.

* 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

Стр.

1 Сфера применения 1

2 Справочные документы 1

3 Определения 1

3.1 Термины, определенные в других документах 1

3.2 Термины, определенные в настоящей Рекомендации 1

4 Сокращения и акронимы 2

5 Соглашения по терминологии 2

6 Обзор 2

7 Архитектура услуг интеллектуального учета 3

8 Угрозы безопасности в услугах интеллектуального учета 4

8.1 Угрозы в интерфейсе между измерительным устройством и MDMS 4

8.2 Угрозы в интерфейсе между MDMS и независимым поставщиком услуг 5

8.3 Угрозы в интерфейсе между системой энергокомпании и потребителем 5

9 Требования по безопасности услуг интеллектуального учета 6

9.1 Требования по безопасности учета потребления электроэнергии 6

9.2 Требования по безопасности информации, используемой потребителем 6

9.3 Требования по безопасности информации, используемой независимым поставщиком услуг 6

9.4 Требования по безопасности информации, используемой оператором энергосистемы 7

10 Руководящие указания по безопасности услуг интеллектуального учета 7

10.1 Средства контроля безопасности учета потребления электроэнергии 7

10.2 Средства контроля безопасности информации, используемой потребителем . 8

10.3 Средства контроля безопасности информации, используемой независимым поставщиком услуг 8

10.4 Средства контроля безопасности информации, используемой оператором энергосистемы 8

Библиография 9

Рекомендации МСЭ-Т X.1332

Руководящие указания по безопасности услуг интеллектуального учета в "умных" электросетях

1 Сфера применения

В настоящей Рекомендации содержатся руководящие указания по безопасности услуг интеллектуального учета в "умных" электросетях. В Рекомендации рассматриваются следующие вопросы:

- выявление угроз безопасности и атак, направленных на услуги интеллектуального учета;
- требования по безопасности услуг интеллектуального учета;
- руководящие указания по безопасности услуг интеллектуального учета для выполнения требований по безопасности.

2 Справочные документы

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 регулирование спроса (demand response, DR) [b-ITU-T Y.2071]: функция "умной" электросети, которая позволяет потребителям сократить объемы или изменить свои режимы потребления электроэнергии в периоды пикового спроса, как правило, на основе материального стимула. Механизмы и стимулы для сокращения потребления энергии коммунальными, коммерческими, промышленными и бытовыми потребителями в периоды пикового спроса или угрозы надежности энергоснабжения. Регулирование спроса необходимо для оптимизации баланса предложения электроэнергии и спроса на нее.

3.1.2 оператор энергосистемы (electric power system operator) [b-IEC 60050-617]: сторона, ответственная за безопасное и надежное функционирование части энергосистемы в определенной зоне и за подключение к другим частям энергосистемы.

3.1.3 система управления энергопотреблением (energy management system, EMS) [b-ITU-T Y.2071]: компьютерная система в составе программной платформы, обеспечивающей базовые услуги поддержки, и набора приложений, обеспечивающих функциональные возможности, необходимые для эффективной работы средств производства и передачи электроэнергии при гарантировании надлежащей безопасности энергоснабжения с минимальными затратами.

3.1.4 "**умный**" **счетчик (smart meter)** [b-ITU-T X.1331]: устройство, установленное в помещении для мониторинга и контроля энергопотребления "умными" бытовыми устройствами на основе их информации о регулировании спроса.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 концентратор данных (data concentrator): промежуточное устройство, расположенное между "умным" счетчиком и системами энергокомпаний, основная задача которого заключается в сборе данных, поступающих от "умных" счетчиков, и управлении этими данными.

3.2.2 система управления данными измерений (meter data management system, MDMS): система управления данными измерений (MDMS) собирает и проверяет данные измерений, такие как использование и выработка электроэнергии, а также журналы измерений, проводит их оценку и разрешает редактирование этих данных. MDMS хранит эти данные в течение ограниченного периода времени до их передачи в хранилище данных и делает эти данные доступными для авторизованных систем.

ПРИМЕЧАНИЕ. – Взято из [b-ITU-T Y.2071].

3.2.3 услуга интеллектуального учета (smart metering service): услуга, которая собирает данные о потреблении электроэнергии с помощью "умных" счетчиков и предоставляет обработанную информацию потребителям и энергокомпаниям; независимые поставщики услуг также могут быть участниками данной услуги, используя данные о потреблении электроэнергии с целью предоставления какой-либо услуги или набора услуг клиентам.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

CDMA	Code-Division Multiple Access	Многостанционный доступ с кодовым разделением каналов
DDoS	Distributed Denial of Service	Распределенная атака типа "отказ в обслуживании"
DoS	Denial of Service	Отказ в обслуживании
EMS	Energy Management System	Система управления энергопотреблением
EUIS	Energy Usage Information System	Информационная система энергопотребления
HMAC	Hash-based Message Authentication Code	Код аутентификации сообщения на основе хэш-функции
IHD	In-Home Display	Домашний дисплей
LTE	Long-Term Evolution	Технология долгосрочного развития
MDMS	Meter Data Management System	Система управления данными измерений
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PLC	Power Line Communication	Связь по линиям электропередачи
QoS	Quality of Service	Качество обслуживания
TLS	Transport Layer Security	Безопасность транспортного уровня
VPN	Virtual Private Network	Виртуальная частная сеть

5 Соглашения по терминологии

Отсутствуют

6 Обзор

Услуги интеллектуального учета – одни из основных функций "умной" электросети – широко распространены по всему миру, для того чтобы повысить эффективность и надежность электросетей путем сбора информации об использовании электроэнергии от потребителей и предоставления такой информации потребителям.

"Умный" счетчик измеряет, регистрирует и передает данные об объеме электроэнергии, которую использовал потребитель. Данные измерений передаются циклически, например каждые 5 или 15 минут. Используя эти данные, поставщики услуг интеллектуального учета могут оценивать спрос потребителей на электроэнергию. Согласно такой оценке, они могут повысить надежность электросети, корректируя спрос потребителей на электроэнергию или изменяя их режим энергопотребления.

Поставщики услуг интеллектуального учета могут в режиме реального времени предоставлять клиентам информацию о потреблении ими электроэнергии, а также о тарифах на электроэнергию, оценку их счетов, статистические данные или информацию о тенденциях в изменении энергопотребления. Потребители, используя эти сведения, могут добровольно пытаться снизить свой расход электроэнергии. Например, если поставщик применяет динамическое ценообразование и

изменяет тарифы на основе потребления электроэнергии, клиенты могут отложить или ускорить свою деятельность, связанную с потреблением электроэнергии.

Вместе с тем существуют угрозы, которые могут привести к нарушению функционирования "умных" электросетей. Например, неверные данные учета могут привести к принятию ошибочного решения по управлению спросом, а злонамеренное использование функций регулирования нагрузки может нанести экономический ущерб и физический вред потребителям. Наряду с этим при предоставлении доступа независимым поставщикам услуг к данным измерений следует рассматривать вопрос о защите информации, позволяющей установить личность (PII).

Кроме того, сведения о потреблении электроэнергии, статистические данные и информация о расходах передаются на подключенные к интернету устройства потребителей, такие как смартфоны и карманные компьютеры. Вследствие этого, почти все угрозы, которые могут затронуть мобильные устройства, могут также затронуть и услуги интеллектуального учета.

В настоящей Рекомендации рассматриваются угрозы безопасности услуг интеллектуального учета и определяются требования и возможности защиты для обеспечения безопасности услуг интеллектуального учета.

7 Архитектура услуг интеллектуального учета

Перед описанием требований по безопасности услуг интеллектуального учета определяется архитектура таких услуг, для того чтобы описать все объекты, связанные с услугой интеллектуального учета, и прояснить их взаимосвязь.

В настоящей Рекомендации с целью определения общей модели услуги учета рассматриваются следующие сценарии использования:

- сбор данных о потреблении электроэнергии от измерительных приборов;
- предоставление клиентам информации о тенденциях в потреблении электроэнергии;
- предоставление данных о потреблении электроэнергии независимым поставщикам услуг;
- предоставление данных о потреблении электроэнергии операторам энергосистемы.

На рисунке 7-1 показана архитектура услуг интеллектуального учета для этих сценариев использования. В этой модели существует шесть основных объектов: измерительное устройство, оператор энергосистемы, система управления данными измерений (MDMS), энергокомпания (система энергокомпании), независимый поставщик услуг и потребитель.

Измерительное устройство измеряет расход электроэнергии потребителем и отправляет данные измерений в MDMS энергокомпанию. Энергокомпания обеспечивает информационную систему энергопотребления (EUIS) для информирования потребителей о тенденциях в потреблении электроэнергии. EUIS получает данные измерений от MDMS для выработки статистической информации. Система выставления счетов энергокомпании тоже использует данные измерений. В этой архитектуре EUIS и система выставления счетов рассматриваются как система энергокомпании.

Оператор энергосистемы использует данные измерений для оценки текущего и будущего статуса системы энергоснабжения. Система управления энергопотреблением (EMS) оператора энергосистемы получает данные измерений от MDMS и, используя эти данные, выполняет анализ тенденций в потреблении электроэнергии. Оценка потребления позволяет оператору корректировать объем предложения электроэнергии, для того чтобы энергосистема обеспечивала баланс предложения и спроса.

Потребители имеют "умный" дисплей потребления энергии или "умные" устройства, которые показывают статистические данные потребления энергии и контролируют нагрузку подключенных к ним абонентских сетей. Для доступа к EUIS энергокомпании потребители могут использовать дисплеи нескольких типов, в том числе смартфоны, планшеты, "умные" телевизоры, персональные компьютеры, а также домашние дисплеи (IHD).

Независимый поставщик услуг использует данные измерений для повышения качества обслуживания. Например, компания кабельного телевидения может осуществлять передачу коммерческой рекламы моющих средств для конкретного потребителя, если знает, что этот потребитель в настоящий момент занимается стиркой.

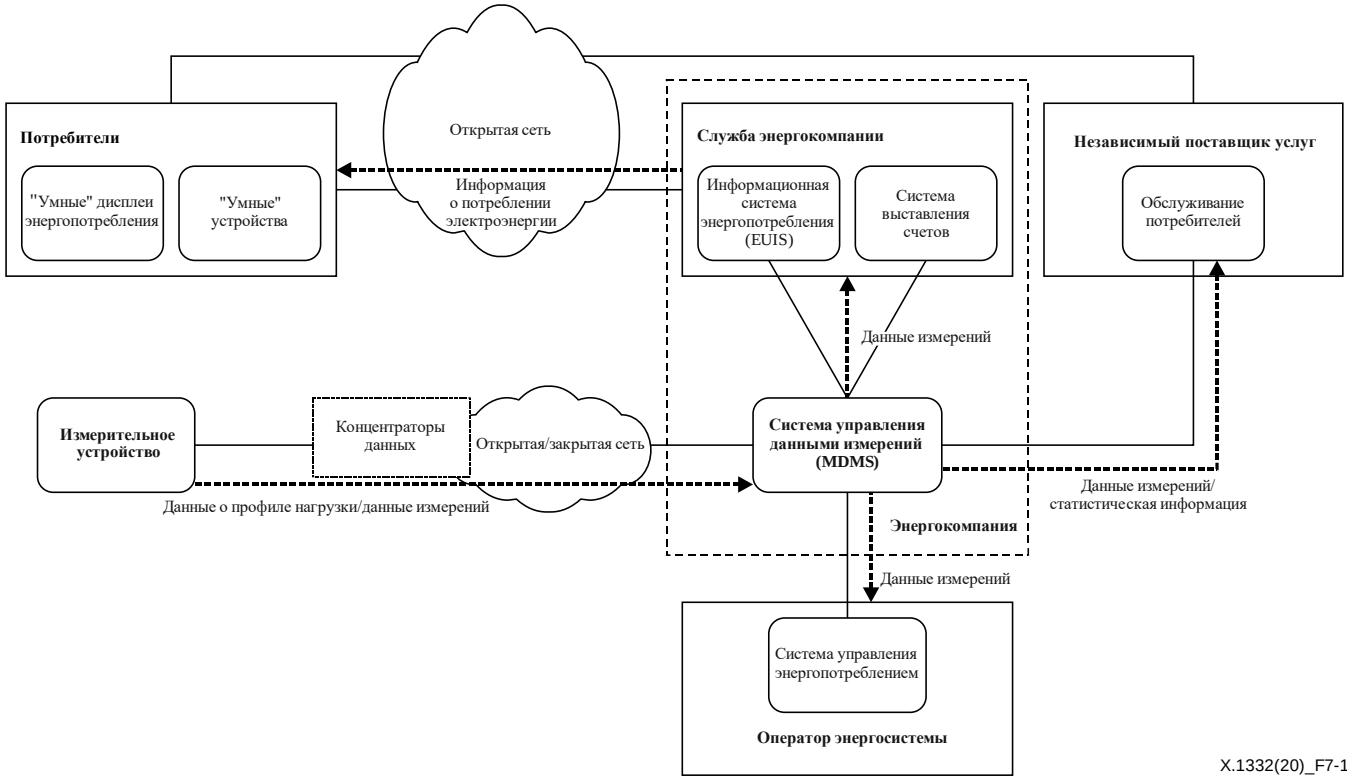

Рисунок 7-1 – Архитектура услуг интеллектуального учета

В этой модели архитектуры учитываются следующие шесть взаимосвязей объектов: измерительное устройство и MDMS, MDMS и EMS, MDMS и система энергокомпании, MDMS и независимый поставщик услуг, потребитель и система энергокомпании, потребитель и независимый поставщик услуг.

Измерительное устройство подсоединено к MDMS по сети. Сеть может быть открытой, как LTE или CDMA, либо закрытой, как PLC или выделенная линия. Независимо от типа сети концентраторы данных группируют данные измерений в какой-либо области и отправляют агрегированные данные в MDMS.

MDMS и EMS взаимодействуют друг с другом по сети электросвязи с гарантированным качеством обслуживания (QoS).

MDMS и система энергокомпании обычно находятся в одной сети. В противном случае они, как правило, взаимодействуют по сети электросвязи с гарантированным QoS.

MDMS может быть соединена с независимыми поставщиками услуг по сети электросвязи с гарантированным QoS.

Ввиду того что потребители используют открытую сеть, например интернет, как система энергокомпании, так и независимый поставщик услуг соединены с потребителями по этой открытой сети. Потребители могут получить доступ к сетям, используя WiFi, LTE и т. д.

8 Угрозы безопасности в услугах интеллектуального учета

8.1 Угрозы в интерфейсе между измерительным устройством и MDMS

Интерфейс между измерительным устройством и MDMS используется для сбора и обработки большого объема данных о потреблении электроэнергии потребителем, включая данные счетчиков, профили нагрузки и измеренные показатели качества электроэнергии. Передаваемые через этот интерфейс данные являются основной целью злоумышленников, которые нарушают услуги интеллектуального учета в результате перехвата, фальсификации и повтора этих данных.

Злоумышленники также стремятся привести к отказу в предоставлении услуг интеллектуального учета, осуществляя распределенные атаки типа "отказ в обслуживании" (DDoS) на MDMS.

Интерфейс между измерительным устройством и MDMS уязвим для нижеследующих угроз.

– Утечка информации: "умные" измерительные устройства (т. е. "умные" счетчики) регулярно отправляют данные об электрической нагрузке (данные измерений) в MDMS через концентратор данных. В "умных" электросетях этот период весьма невелик (например, пять минут или меньше). Вследствие этого, злоумышленники, если им удастся анализировать данные измерений, могут получить сведения об укладе жизни потребителей.
– Фальсификация данных измерений: злоумышленники могут блокировать фактические данные измерений и отправлять в MDMS вместо них ложные данные измерений. Такие атаки приводят к ошибкам оценки спроса, так как MDMS и EMS лишаются доступа к фактическим собранным данным измерений. Эти ошибки могут нарушить баланс между спросом и предложением и, в результате, привести к отключению электроэнергии.
– Фальсификация профиля нагрузки: злоумышленники могут вносить неразрешенные изменения в профили нагрузки, хранящиеся в измерительных устройствах. Система выставления счетов рассчитывает причитающиеся с каждого потребителя суммы на основе его профиля нагрузки, поэтому эта угроза может привести к выставлению неправильных счетов потребителям.
– Отказ в обслуживании (DoS): злоумышленники могут совершать атаку DoS, для того чтобы запустить выполнение вредоносного кода на ряде измерительных устройств или концентраторов данных и переполнить цель (как правило, MDMS) значительным количеством данных или большим числом запросов на обслуживание. Такая атака приводит к замедлению или даже прекращению предоставления услуги интеллектуального учета.

8.2 Угрозы в интерфейсе между MDMS и независимым поставщиком услуг

Интерфейс между MDMS и независимым поставщиком услуг служит для совместного использования данных измерений, с тем чтобы независимый поставщик услуг могут предоставлять различные специализированные услуги каждому потребителю. Ввиду того, что через этот интерфейс может передаваться PII, злоумышленники нацеливаются главным образом на эти данные и нарушают предоставление услуг интеллектуального учета, перехватывая и используя такие данные.

Интерфейс между MDMS и независимым поставщиком услуг уязвим для нижеследующих угроз.

– Взлом PII: злоумышленники могут перехватывать PII, предпринимая атаку для сканирования пакетов или выполняя вредоносный код в подсоединенных к интернету системах независимого поставщика услуг.

8.3 Угрозы в интерфейсе между системой энергокомпании и потребителем

По интерфейсу между системой энергокомпании и устройством, находящимся в помещении потребителя, передается информация различного типа, которая служит для потребителя стимулом участвовать в регулировании спроса. Возможна передача информации о тенденциях в энергопотреблении клиента, ценах на электроэнергию в режиме реального времени, тенденциях в изменении спроса, информации о счетах, а также статистических данных. Фальсифицируя передаваемую информацию, злоумышленники могут побудить потребителя расходовать чрезмерный объем электроэнергии. Еще одной серьезной потенциальной угрозой для системы энергокомпании, подключенной к устройствам, которые расположены в помещении потребителя, является атака DoS.

Интерфейсы между системой энергокомпании и устройством потребителя уязвим для нижеследующих угроз.

– Фальсификация информации о ценах в режиме реального времени: злоумышленники могут подделать информацию о ценах в режиме реального времени, которую передает система энергокомпании потребителям, и таким образом вводить их в заблуждение. В случае если фальсифицированная цена ниже фактической, устройства потребителей (например, "умный" дисплей энергопотребления) могут заставить устройства, которые потребляют электроэнергию (например, электрический автомобиль), увеличить ее расход. Напротив, если фальсифицированная цена выше фактической, потребитель может упустить возможность аккумулировать электроэнергию по более низкой цене.

- Отказ в обслуживании: злоумышленники могут совершать атаку DoS, для того чтобы запустить выполнение вредоносного кода на ряде устройств потребителей и переполнить цель (как правило, EUIS) огромным числом запросов на обслуживание. Такая атака приводит к замедлению или даже прекращению предоставления услуги интеллектуального учета.
- Взлом PII: злоумышленники могут перехватывать PII, предпринимая атаку для сканирования пакетов или выполняя вредоносный код в подсоединенных к интернету устройствах потребителей.

9 Требования по безопасности услуг интеллектуального учета

9.1 Требования по безопасности учета потребления электроэнергии

Учет потребления электроэнергии – одна из важнейших функций услуги интеллектуального учета. При ее надлежащем функционировании MDMS может собирать необходимую информацию для определения тенденций в потреблении электроэнергии, индивидуального режима потребления каждого клиента, составления счетов энергокомпании за электроэнергию и т. д. Кроме того, другие объекты, участвующие в услуге интеллектуального учета, могут использовать эту информацию для надлежащего выполнения своих функций. Следовательно, целостность, подлинность и конфиденциальность данных измерений составляют основные требования по безопасности процедуры сбора информации.

Для надлежащего реагирования на угрозы, существующие в интерфейсе связи между "умным" счетчиком и MDMS, следует учитывать нижеследующие требования по безопасности.

- Должна быть обеспечена сквозная конфиденциальность данных, передаваемых через интерфейс связи между "умным" счетчиком и MDMS.
- Должна быть обеспечена сквозная целостность информационных сообщений между "умным" счетчиком и MDMS, для того чтобы предотвратить несанкционированное изменение данных.
- Должна быть обеспечена защита данных измерений и информации аутентификации, хранящихся на таких устройствах, как "умные" счетчики, концентраторы данных и MDMS, от несанкционированного доступа.
- Должна быть обеспечена подлинность отправителя каждого информационного сообщения.

9.2 Требования по безопасности информации, используемой потребителем

Устройства потребителя могут иметь доступ в систему энергокомпании, подключенную к серверной части энергосистемы, поэтому они являются основной целью атак на услуги интеллектуального учета. Вследствие этого, для этой части услуги интеллектуального учета данные и приложения, которые находятся в устройствах потребителя, должны быть защищены.

В целях смягчения возможных побочных эффектов угроз, существующих в интерфейсе связи между системой энергокомпании и потребителем, следует учитывать нижеследующие требования по безопасности.

- Должна быть обеспечена конфиденциальность данных в интерфейсе связи между потребителем и системой энергокомпании.
- Должна быть обеспечена целостность данных информационных сообщений между потребителем и системой энергокомпании, для того чтобы запретить несанкционированное изменение данных.
- Должна быть обеспечена подлинность отправителя каждого информационного сообщения.
- Должна быть обеспечена защита информации, хранящейся в устройстве потребителя и системе энергокомпании, от несанкционированного доступа.
- Следует учитывать обеспечение целостности приложений в устройстве потребителя.

9.3 Требования по безопасности информации, используемой независимым поставщиком услуг

Основную проблему в этой области составляет обработка данных PII и утечка PII на участке между независимым поставщиком услуг и MDMS.

Для надлежащего контроля угроз, существующих в интерфейсе связи между MDMS и независимым поставщиком услуг, следует учитывать нижеследующие требования по безопасности.

- Должна быть обеспечена конфиденциальность данных в интерфейсе связи между MDMS и независимым поставщиком услуг.
- Должна быть обеспечена целостность данных информационных сообщений между MDMS и независимым поставщиком услуг, для того чтобы запретить несанкционированное изменение данных.
- Должна быть обеспечена подлинность отправителя каждого информационного сообщения.
- Данные PII при предоставления персонализированных услуг следует обрабатывать надлежащим образом, чтобы их раскрытие происходило только с согласия потребителя.
- Данные PII, связанные с измерениями, не следует делать доступными при предоставлении услуг, в которых не используется PII.

9.4 Требования по безопасности информации, используемой оператором энергосистемы

Для надлежащего предупреждения угроз, существующих в интерфейсе связи между MDMS и оператором энергосистемы, следует учитывать нижеследующие требования по безопасности.

- Должна быть обеспечена конфиденциальность данных в интерфейсе связи между MDMS и оператором энергосистемы.
- Должна быть обеспечена целостность данных информационных сообщений между MDMS и оператором энергосистемы, для того чтобы запретить несанкционированное изменение данных.
- Следует разрешать доступ к интерфейсу связи между MDMS и оператором энергосистемы только уполномоченным объектам.
- Не следует делать доступной PII, связанную с измерениями.

10 Руководящие указания по безопасности услуг интеллектуального учета

10.1 Средства контроля безопасности учета потребления электроэнергии

Для выполнения требований по безопасности учета потребления электроэнергии следует рассматривать реализацию нижеследующих средств контроля безопасности в качестве возможностей каждого объекта учета потребления электроэнергии.

- Следует осуществлять контроль доступа к данным измерений в измерительных устройствах, концентраторах данных и MDMS. Следует разрешать доступ к данным о потреблении электроэнергии только уполномоченным объектам.
- Для обеспечения подлинности отправителя следует использовать механизм взаимной аутентификации между измерительным устройством и MDMS.
- Для защиты целостности данных о потреблении электроэнергии, передаваемых в MDMS, следует реализовать меры по аутентификации сообщений. Например, для это цели возможно использовать криптографические коды аутентификации сообщений, такие как HMAC.
- Для защиты данных, используемых для выставления счетов, в качестве меры обеспечения безопасности возможно использовать шифрование данных.
- В MDMS следует выполнять обнаружение нарушений целостности данных и декодирования зашифрованных данных.
- Для безопасного создания, согласования, хранения и обновления криптографических ключей следует реализовать механизм безопасного управления ключами в измерительных устройствах, концентраторах данных и MDMS.
- Для обеспечения конфиденциальности и целостности данных измерений, хранящихся в MDMS, следует использовать механизм защиты.
- Для смягчения последствий атаки DoS возможна реализация мер безопасности в MDMS.

10.2 Средства контроля безопасности информации, используемой потребителем

Для выполнения требований по безопасности информации, используемой потребителем, следует рассматривать реализацию нижеследующих средств контроля безопасности в качестве возможностей каждого объекта.

- Для связи между устройством потребителя и системой энергокомпании следует применять меры безопасности связи, такие как TLS. Следует обеспечить взаимную аутентификацию, аутентификацию и шифрование передаваемых данных между устройством потребителя и системой энергокомпании.
- Для доступа к информации о потреблении электроэнергии следует реализовать аутентификацию и авторизацию пользователя в приложениях, которые предоставляют такую информацию. Система энергокомпании должна разрешать пользователям доступ только к их собственным данным.
- В устройстве потребителя следует обеспечить надежное хранение данных аутентификации пользователя и криптографических ключей для аутентификации пользователя и безопасной связи, а также PII.
- Для обнаружения фальсифицированного приложения при каждом запуске любого приложения на устройстве потребителя следует выполнять действия по проверке его целостности.

10.3 Средства контроля безопасности информации, используемой независимым поставщиком услуг

Для выполнения требований по безопасности информации, используемой независимым поставщиком услуг, следует рассматривать реализацию нижеследующих средств контроля безопасности в качестве возможностей каждого объекта.

- Для предотвращения доступа неавторизованных пользователей к соединению между MDMS и независимым поставщиком услуг может рассматриваться использование выделенной линии.
- Для связи между устройством потребителя и системой энергокомпании следует применять меры безопасности связи, такие как виртуальная частная сеть (VPN). Следует обеспечить взаимную аутентификацию, аутентификацию и шифрование передаваемых данных между устройством потребителя и системой энергокомпании.
- В случае если независимые поставщики услуг имеют доступ к PII, следует на протяжении всего жизненного цикла поддерживать процесс защиты PII [b-GAO-08-343]. Возможно осуществлять удаление персональных данных, если независимому поставщику услуг не требуются данные идентификации.

10.4 Средства контроля безопасности информации, используемой оператором энергосистемы

Для выполнения требований по безопасности информации, используемой оператором энергосистемы, следует рассматривать реализацию нижеследующих средств контроля безопасности в качестве возможностей каждого объекта.

- Для снижения риска несанкционированного доступа к соединению между MDMS и оператором энергосистемы следует использовать выделенную линию.
- Для связи между MDMS и оператором энергосистемы следует применять меры безопасности связи, такие как VPN. Следует обеспечить взаимную аутентификацию, аутентификацию и шифрование передаваемых данных между MDMS и оператором энергосистемы.
- Возможно осуществлять удаление персональных данных, если независимому поставщику услуг не требуются данные идентификации.

Библиография

[b-ITU-T X.1331] Рекомендация МСЭ-Т X.1331 (2018), *Руководящие указания по безопасности для устройств домашней сети (HAN) в системах "умных" электросетей*.

[b-ITU-T Y.2071] Recommendation ITU-T Y.2071 (2015), *Framework of a micro energy grid*.

[b-GAO-08-343] United States Government Accountability Office, GAO-08-343:2008, *Information Security: Protecting Personally Identifiable Information* https://www.gao.gov/new.items/d08343.pdf.

[b-IEC 60050-617] IEC 60050-617:2009, *International Electrotechnical Vocabulary – Part 617: Organization/Market of electricity*.

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
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 межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2020 г.