Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1331

(03/2018)

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

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

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

Рекомендация МСЭ-Т X.1331

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.1331

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

Резюме

Домашняя сеть (HAN) в "умных" электросетях − это сеть, находящаяся внутри помещений. В отличие от традиционной HAN, HAN в "умных" электросетях включает устройства "умных" электросетей, например распределенные энергоресурсы (DER), зарядное устройство для электромобилей (EV), бытовую систему управления энергопотреблением (HEMS) и клиентский индикатор потребления энергии (CED). Клиентские потребители электроэнергии и DER подсоединены к HAN таким образом, чтобы клиенты могли включать или выключать нагрузку и DER на основе информации от энергетической компании, чтобы обеспечить максимально эффективное использование электроэнергии. HAN обычно подключена к интернету, и поэтому злоумышленники могут легко получить доступ к HAN и устройствам HAN. Из этого следует, что устройства HAN должны обеспечивать возможности, не позволяющие злоумышленникам взламывать HAN и ее устройства. В Рекомендации МСЭ-Т X.1331 представлен анализ угроз для HAN в "умных" электросетях, требований к безопасности и функций безопасности. Поскольку роль и функции каждого устройства HAN различны, в ней приводятся требования к безопасности и функции безопасности в зависимости от устройств.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1331	29.03.2018 г.	17-я	11.1002/1000/13405

Ключевые слова

Домашняя сеть, руководящие указания по безопасности, требования безопасности, "умная" электросеть.

* 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.1331

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

1 Сфера применения

Настоящая Рекомендация содержит руководящие указания по безопасности для устройств домашней сети (HAN) в системах "умных" электросетей. Настоящая Рекомендация охватывает:

– риски для безопасности, связанные с устройствами и соединениями в HAN;

– требования безопасности, предъявляемые к устройствам и соединениям в HAN;

– функции безопасности устройств и соединений в HAN.

2 Справочные документы

Отсутствуют.

3 Термины и определения

3.1 Термины, определяемые в других документах

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

3.1.1 интерфейс услуг энергоснабжения (energy services interface (ESI)) [b-ITU-T Y.2071]: Набор функций, состоящий из функций шлюза и функций, необходимых для приложений по контролю и управлению услугами "умной" электросети в помещениях клиента.

3.1.2 система накопления энергии (energy storage system (ESS)) [b-ITU-T L.1430]: Физическое устройство или компонент, обладающий способностью накапливать или аккумулировать энергию, вырабатываемую генератором, или энергию, отбираемую у потребителя.

ПРИМЕЧАНИЕ. – ESS обеспечивает функции накопления электроэнергии для использования батарей разного типа. Один из примеров использования накопителя энергии – эффективное реагирование на механизм динамического ценообразования в коммунальной электросети. Электроэнергия накапливается в течение периода ее относительно низкой стоимости, а затем эта накопленная электроэнергия может заменять более дорогостоящую электроэнергию в коммунальной электросети.

3.1.3 домашняя сеть (home area network (HAN)) [b-ITU-T G.9959]: Сеть, к которой можно подключать бытовые электроприборы в помещениях пользователя.

3.1.4 домашняя система управления энергопотреблением (home energy management system (HEMS)) [b-ITU-T Y.4409]: Компьютерная система, содержащая программную платформу по предоставлению базовых услуг поддержки и набор приложений в целях обеспечения функциональных возможностей, необходимых для эффективной работы домашнего оборудования, такого как бытовые электроприборы и аккумуляторные батареи, с тем чтобы гарантировать адекватную безопасность энергоснабжения при минимальных затратах.

ПРИМЕЧАНИЕ. – В "умной" электросети организацию HEMS обеспечивает сеть HAN.

3.1.5 домашний индикатор (in-home display (IHD)) [b-ITU-T Y.4409]: Пользовательское устройство с экраном для представления информации о потреблении электроэнергии в доме. Пользователи могут управлять своими домашними устройствами с помощью пользовательского интерфейса.

ПРИМЕЧАНИЕ. – Информация об управлении и энергопотреблении передается в среде системы связи HAN. Пользовательское устройство с экраном также может быть мобильным или выполненным на базе смартфона, телевизора (с поддержкой протокола Интернет), интернет-видеотелефона, персонального компьютера, планшета или настенной видеопанели.

3.1.6 территориально распределенная сеть (wide area network (WAN)) [b-ITU-T Y.4409]: Сеть связи на основе IP с широким географическим охватом, включающая интернет, к которой подключаются устройства и локальные сети.

3.2 Термины, определяемые в настоящей Рекомендации

В настоящей Рекомендации используются следующие термины.

3.2.1 электромобиль (electric vehicle (EV)): Автомобиль, который можно заряжать от любого внешнего источника электроэнергии и который может одновременно работать в качестве системы энергоснабжения.

Примерами являются чисто электрические транспортные средства, аккумуляторные EV, заряжаемые гибридные EV и заряжаемые гибридные EV с преобразованием энергии. Заряжаемые EV иногда называют автомобилями, способными работать от сети, или автомобилями, заряжаемыми от сети.

3.2.2 местная сеть (neighbourhood area network (NAN)): Сеть доступа, которая позволяет конечным устройствам "умной" электросети и домашним сетям (HAN) подключаться к территориально распределенной сети (WAN).

ПРИМЕЧАНИЕ. – Адаптировано из [b-Smart-O-33].

3.2.3 "умный" электросчетчик (smart meter): Устройство, установленное в помещениях для контроля и управления потреблением электроэнергии бытовыми устройствами "умной" электросети на основе информации о характеристиках спроса.

ПРИМЕЧАНИЕ. – Адаптировано из [b-ITU-T Y.4409].

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AMI	Advanced Metering Infrastructure	Усовершенствованная инфраструктура измерений
CED	Customer Energy Display	Клиентский индикатор энергопотребления
DER	Distributed Electricity Resource	Распределенные энергоресурсы
DG	Distributed Generator	Распределенный генератор
DoS	Denial of Service	Отказ в обслуживании
DTLS	Datagram Transport Layer Security	Протокол дейтаграмм безопасности транспортного уровня
ESI	Energy Services Interface	Интерфейс услуг энергоснабжения
ESS	Energy Storage System	Система накопления энергии
EV	Electric Vehicle	Электромобиль
G/W	Gateway	Шлюз
HAN	Home Area Network	Домашняя сеть
HEMS	Home Energy Management System	Домашняя система управления энергопотреблением
HMAC	Hash-based Message Authentication Code	Код аутентификации сообщений на основе хеширования
ID	Identifier	Идентификатор
IP	Internet Protocol	Протокол Интернет
IHD	In-Home Display	Домашний индикатор
NAN	Neighbourhood Area Network	Местная сеть
TLS	Transport Layer Security	Безопасность транспортного уровня
WAN	Wide Area Network	Территориально распределенная сеть
WPA	Wi-Fi Protected Access	Защищенный доступ Wi-Fi

5 Соглашения

Отсутствуют.

6 Общая модель домашней сети в "умной" электросети

"Умная" электросеть – это интеллектуальная энергосистема, оснащенная информационно-коммуникационными технологиями. С помощью "умной" электросети электроэнергетические компании могут оценивать спрос на электроэнергию на основе информации о потреблении электроэнергии клиентами, собранной от "умных" электросчетчиков. Исходя из этой оценки компании могут управлять ситуацией пиковой нагрузки. Прежде чем нагрузка на электросеть достигнет пиковых значений, компания уменьшит энергоснабжение клиентов или предложит им переключиться на альтернативные источники, созданные распределенными энергоресурсами (DER) в домах клиентов, такие как батареи из гальванических элементов на крыше, электроаккумуляторы или электромобили (EV). Кроме того, клиент может отсрочить или перенести на более ранний срок потребление электроэнергии на основе информации о пиковой нагрузке, полученной от электроэнергетической компании.

Чтобы обмениваться информацией между компанией и клиентом, система оценки или ограничения спроса компании должна быть соединена с устройствами в помещениях клиента, такими как домашняя система управления энергопотреблением (HEMS) или клиентский индикатор энергопотребления (CED). На рисунке 6-1 показаны различные сети в среде "умной" электросети. Как показано на рисунке 6-1, соединение может быть выполнено по нескольким сетям, таким как HAN, сеть доступа [также известная как местная сеть (NAN)] или территориально распределенная сеть (WAN).

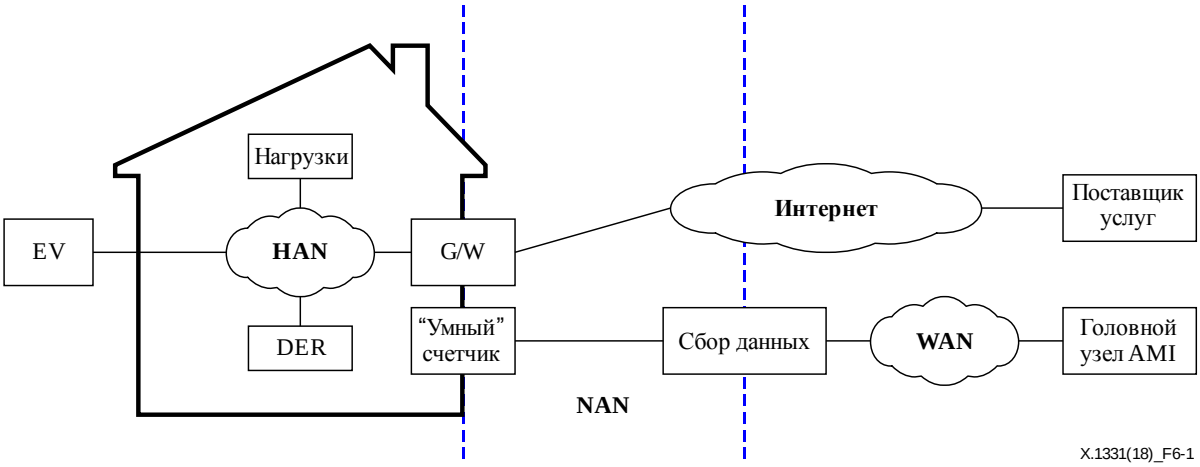

Рисунок 6-1 − Различные типы сетей в "умной" электросети

Сеть HAN связывает электрические нагрузки и источники электроэнергии, имеющиеся в помещениях клиента. Вся информация от устройств HAN должна поступать через HAN в систему базы данных электроэнергетической компании, например, в головной узел усовершенствованной инфраструктуры измерений (AMI), а вся информация от компаний доставляется через HAN в устройства клиента.

Поскольку сеть HAN обычно подключена к интернету, она доступна из интернета. Если злоумышленнику удастся получить доступ к HAN, то устройства, подключенные к HAN, могут быть взломаны и злоумышленник может намеренно изменить информацию, например, об электрических нагрузках. В этом случае злоумышленники смогут управлять устройствами HAN по своему усмотрению. Следовательно, в устройствах, подключенных к HAN, и их соединениях должны применяться меры безопасности.

Прежде чем описывать угрозы, требования и технологии безопасности, следует сформулировать общую модель HAN в "умной" электросети. Общая модель должна отражать все объекты и соответствующие интерфейсы, чтобы прояснить их взаимосвязи.

На рисунке 6-2 показана общая модель HAN в "умной" электросети. В этой сети HAN имеется много элементов, таких как электрическая нагрузка, DER, HEMS, CED [также известная как домашний индикатор (IHD)], интерфейс услуг энергоснабжения (ESI) и "умный" электросчетчик.

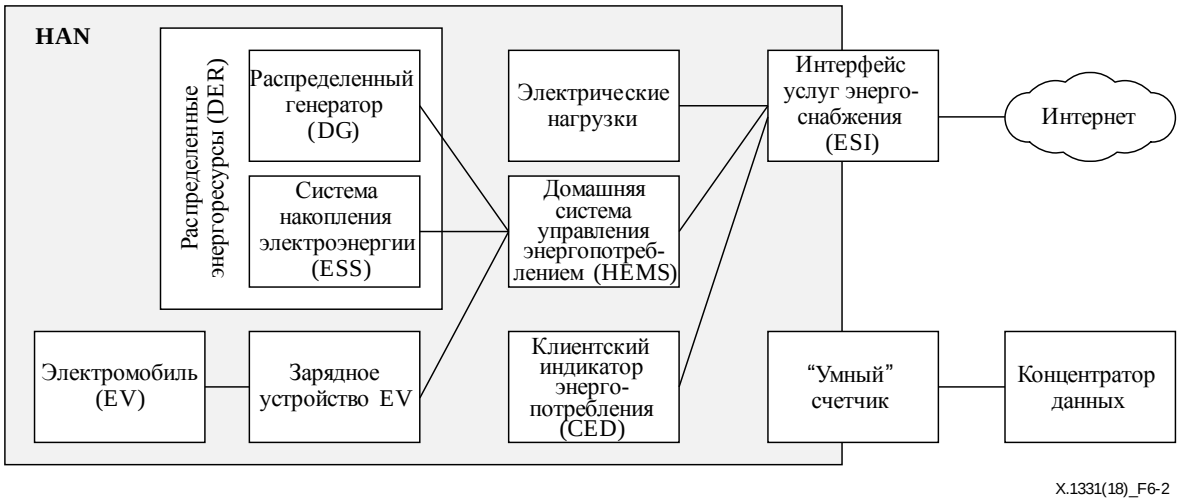

Рисунок 6-2 − Общая модель домашней сети в "умной" электросети

- Электрические нагрузки создают устройства, потребляющие электроэнергию, такие как бытовые электроприборы, кондиционеры и водяные насосы. Нагрузки бывают, как правило, двух типов: "умные" и обычные. "Умные" нагрузки обладают возможностями связи и измерения, отсутствующими у обычных нагрузок. Тем не менее потребление электроэнергии в обычных нагрузках можно контролировать с помощью HEMS, если данное устройство включено в розетку через "умную" штепсельную вилку, обладающую возможностями связи и коммутации. Таким образом в этой Рекомендации в качестве электрических нагрузок рассматриваются как "умные" нагрузки, так и "умные" штепсельные вилки.
- DER, к которым относятся распределенные генераторы (DG) и электрические системы накопления энергии (ESS), представляют собой устройства, предоставляющие электроэнергию для нагрузок. Генераторы DG в составе HAN широко используют источники в виде гальванических батарей.
- EV может быть как нагрузкой, так и DER. Зарядка EV создает нагрузку в HAN, а в качестве DER он обеспечивает электроэнергию для бытовых электроприборов.
- HEMS управляет возможностями электрических нагрузок и DER на основе либо зарегистрированного клиентом графика, либо заранее определенных условий. Основными критериями в рамках этих условий являются цена электроэнергии и сигнал регулирования спроса.
- CED отображает текущую статистику потребления электроэнергии и информацию о цене, так что клиенты могут снизить потребление электроэнергии или изменить свой план энергопотребления.

7 Угрозы для безопасности домашних сетей

В данном разделе перечислены основные угрозы для безопасности HAN. Отметим, что этот раздел ставит своей целью не определение таксономии угроз, а информирование об угрозах, которые операторам HAN необходимо учитывать в первую очередь.

7.1 Утечка данных

Широко известную угрозу для сетей и устройств представляет раскрытие сохраняемых или передаваемых данных. Злоумышленник может интенсивно перехватывать передаваемые данные или получать физический доступ к устройству, чтобы извлечь данные из его памяти. Если данные не защищены, злоумышленник может раскрыть их.

Поскольку в составе HAN широко используется беспроводная связь, можно легко организовать подслушивание внутри HAN или извне. Более того, поскольку объекты в составе HAN во многих случаях связаны с интернетом, к ним можно получить удаленный доступ. Соответственно как переданные, так и сохраненные данные в среде HAN могут стать доступными неавторизованному злоумышленнику.

В среде HAN разного рода конфиденциальные данные, такие как сведения о потреблении электроэнергии, платежная информация и план использования электроэнергии, хранятся в HEMS, CED или "умном" электросчетчике. Эти конфиденциальные данные могут передаваться от или к HEMS и CED через ESI. Раскрытие данных может серьезно повлиять на частную жизнь клиента. Злоумышленник будет знать о его повседневном укладе жизни.

Кроме того, из HEMS и CED по сети связи могут передаваться команды, управляющие режимом работы нагрузок, DER или зарядных устройств EV. Имея доступ к этим данным, злоумышленник может определить, как управлять нагрузками и DER в составе HAN. Эти сведения могут создавать другие угрозы, такие как инъекция вредоносных данных, описываемая в пункте 7.2.

7.2 Фальсификация данных или инъекция вредоносных данных

Неавторизованный злоумышленник может добавить, изменить или удалить информацию, передаваемую между устройствами в составе HAN или хранящуюся в устройствах HAN. В качестве злоумышленника может выступать то или иное лицо, а также та или иная программа или объект в составе HAN. При возникновении такой угрозы может быть нарушена целостность данных. Кроме того, нарушение целостности данных может привести к неправильной работе устройства.

Поскольку к беспроводной сети связи может иметь доступ любой анонимный объект, он может направлять вредоносные данные на объекты в составе HAN. Кроме того, злоумышленник может добавлять данные в существующее соединение с намерением взломать его или передать вредоносные данные. Более того, злоумышленник может получить доступ к памяти объекта HAN, такого как система HEMS, и изменить хранящиеся там данные или добавить вредоносные данные.

Если сигнал о стоимости электроэнергии изменился в сторону повышения, то HEMS может снизить потребление электроэнергии вопреки желанию клиента. Кроме того, злоумышленник может отправить управляющее сообщение, которое приведет к разрядке EV или ESS. К числу других примеров относятся отправка на объект массовых запросов, что приведет к отказу в обслуживании (DoS) данного объекта, изменение значений в файле данных или изменение программы, с тем чтобы изменить поведение того или иного объекта в составе HAN.

7.3 Прерывание связи

Одним из видов прерывания связи является создание помех, которое происходит, когда в результате преднамеренных или непреднамеренных помех линия связи отправителя или получателя становится перегруженной, что фактически делает ее непригодной. Другим примером прерывания связи служит чрезмерное потребление полосы пропускания линии связи путем передачи чрезвычайно больших объемов данных.

Система HEMS в составе HAN должна собирать информацию о состоянии нагрузок и DER, связанных с потреблением электроэнергии, а также получать сведения о стоимости и сигналы управления от электроэнергетической компании или поставщика услуг, с тем чтобы реагировать на поступающие от них запросы по регулированию. Таким образом, чтобы сеть HAN функционировала должным образом, ее средства связи должны поддерживаться в хорошем состоянии.

7.4 Несанкционированный доступ

Несанкционированный доступ может иметь место, если злоумышленник, маскируясь под реального пользователя, получает доступ к таким объектам, как DER, HEMS или CED. После успешной попытки несанкционированного доступа злоумышленник может получить доступ и к другим устройствам.

Чтобы добиться такой цели, он должен быть идентифицирован и аутентифицирован. Для этого злоумышленник может произвести сканирование портов, чтобы проверить, какие уязвимые порты открыты в объекте HAN. При наличии открытых уязвимых портов злоумышленник может

использовать уязвимость устройства HAN. Кроме того, он может получить несанкционированный доступ к "неуязвимой" услуге методом угадывания пароля.

Еще одна из основных угроз – это вредоносное ПО. Вредоносные программы могут заражать устройство HAN, такое как CED, через электронную почту или веб-услугу, а затем распространиться на другие устройства в составе HAN. Если на устройстве HAN установлено вредоносное ПО, оно может получить несанкционированный доступ к его ресурсам и вызвать неправильную работу устройства или вывести его из строя.

7.5 Отрицание участия

Эта угроза может возникнуть, когда злоумышленник (отправитель или получатель) отрицает факт передачи или получения сообщения. Это не приводит к повреждению или сбоям в работе устройств HAN, но может привести к конфликту. В зависимости от характера конфликта возможно, что будет неправильно определена причина неисправности или сбоя в обслуживании.

7.6 Взаимосвязь между угрозами безопасности и домашней сетью

Угрозы безопасности, описываемые в пунктах 7.1–7.5, проявляются в конкретном объекте или линии связи общей модели HAN. Взаимосвязь между угрозами безопасности и объектами HAN показана в таблице 7-1, где белые кружки в ячейках указывают на наличие определенной угрозы для конкретного объекта.

Таблица 7-1 − Взаимосвязь между угрозами безопасности и домашними сетями

Объекты	Раскрытие		Изменение/ инъекция		Прерывание	Несанкциони-рованный доступ	Отрицание участия
	Храня-щиеся данные	Переда-ваемые данные	Храня-щиеся данные	Переда-ваемые данные			
Нагрузка		○		○	○		
DER		○		○	○	○	○
Зарядное устройство EV		○		○	○		○
HEMS	○	○	○	○	○	○	○
CED	○	○	○	○	○	○	○
ESI					○	○	
Линия связи		○		○	○		

8 Требования безопасности домашней сети

В этом разделе описываются требования безопасности высокого уровня с точки зрения четырех основных аспектов безопасности – доступности, конфиденциальности, целостности и неотрекаемости.

8.1 Доступность

Доступность гарантирует, что события, влияющие на сеть, не приведут к отказу в авторизованном доступе к элементам сети, сохраненной информации, информационным потокам, услугам и приложениям. Другими словами, если объекту HAN требуется информация из другого устройства при наличии разрешения, он должен немедленно получить доступ к этому устройству.

Сеть HAN в составе "умной" электросети должна контролировать использование нагрузок, генерирование электроэнергии или ее хранение в DER в соответствии с требованиями электросетей. Когда электроэнергетические компании полагают, что достигнута пиковая нагрузка, в HEMS или CED поступает запрос на снижение потребления или изменение цены, чтобы регулировать спрос на электроэнергию со стороны клиентских устройств. Определить, принят ли запрос, можно на основании условий, зарегистрированных клиентом.

Для этого сценария в первую очередь необходимо обеспечить доступность функциональных возможностей сети и объектов HAN. Если в момент возникновения пикового спроса сеть HAN недоступна, возможно, что HEMS не получит никакого сигнала от электроэнергетической компании, что приведет к повышенным расходам клиента.

8.2 Конфиденциальность

Конфиденциальность гарантирует, что содержание данных не может быть прочитано неавторизованными объектами. Даже в случаях, когда некоторые данные были перехвачены путем подслушивания беспроводного соединения, их конфиденциальность может быть обеспечена, если злоумышленник не в состоянии раскрыть их.

Конфиденциальность требуется для объектов и уязвимых данных в линиях связи на этапах хранения и передачи. К уязвимым данным HAN относятся информация по измерению потребления электроэнергии, командные сообщения, регулирующие режим работы нагрузок и DER, сигналы о цене и запросы электроэнергетической компании по регулированию спроса, а также персональная идентифицируемая информация, хранящаяся в CED.

8.3 Целостность

Целостность гарантирует, что переданные данные не отличаются от исходных. Недавно понятие целостности было дополнено неизменностью состояния системы или устройства относительно исходной конфигурации. Аналогично, первоначально сохраненные данные не должны измениться после процедуры авторизации.

Должна быть обеспечена целостность команд управления и информации о состоянии, передаваемой между HEMS и другими объектами – нагрузками и DER. Кроме того, должна быть защищена целостность данных, передаваемых или принимаемых CED. Чтобы гарантировать функциональные возможности, необходимо также обеспечить целостность набора программ, установленных на каждом устройстве HAN, и самих этих программ.

8.4 Неотрекаемость от участия

Неотрекаемость обеспечивает цифровое доказательство конкретного совершенного действия, связанного с данными, не позволяя физическому лицу или объекту отказаться от этого действия.

В HAN к действиям, потенциально приводящим к конфликту, могут относиться команды регулирования DER и нагрузок, получение сигналов о цене и запросов на регулирование спроса, а также регистрация графика потребления электроэнергии через CED. Таким образом объекты HAN, связанные с этими действиями, должны удовлетворять требованию неотрекаемости. Однако в случае нагрузок их характеристики могут сделать неотрекаемость невозможной. Например, "умная" штепсельная вилка – это простое устройство, не обладающее достаточной памятью и вычислительной мощностью.

8.5 Связь между требованиями безопасности и домашними сетями

В таблице 8-1 показана связь между требованиями безопасности и угрозами безопасности; кружок в ячейке указывает на то, что для устранения или смягчения последствий данной угрозы должно выполняться конкретное требование безопасности.

Таблица 8-1 − Связь между требованиями безопасности и угрозами

			Угрозы для безопасности						
			Раскрытие		Изменение/ инъекция		Прерывание	Несанкцио-нированный доступ	Отрицание участия
			Храня-щиеся данные	Переда-ваемые данные	Храня-щиеся данные	Переда-ваемые данные			
Требования безопасности	Конфиден-циальность	Храня-щиеся данные	○						
		Храня-щиеся данные		○					
	Целостность	Храня-щиеся данные			○			○	
		Переда-ваемые данные				○		○	
	Доступность						○		
	Неотрекаемость								○

Поскольку угрозы для каждого объекта в составе HAN перечислены в таблице 7-1, а требования по каждой угрозе – в таблице 8-1, путем сопоставления этих двух таблиц можно получить требования безопасности для каждого объекта в составе HAN. В таблице 8-2 показано распределение требований безопасности к объектам в составе HAN; кружок в ячейке указывает на то, что для устранения или смягчения последствий данной угрозы каждым объектом должно соблюдаться конкретное требование безопасности.

Таблица 8-2 − Распределение требований безопасности к объектам домашних сетей

		Требования безопасности					
		Доступность	Конфиденциальность		Целостность		Неотрека-емость
			Храня-щиеся данные	Переда-ваемые данные	Храня-щиеся данные	Переда-ваемые данные	
Объекты	Нагрузка	○		○		○	
	DER	○		○		○	○
	Зарядное устройство EV	○		○		○	○
	CED	○	○	○	○	○	○
	HEMS	○	○	○	○	○	○
	ESI	○				○	
	Линия связи	○		○		○	

9 Связь между требованиями безопасности и функциями безопасности

Для удовлетворения требований безопасности, предъявляемых к HAN и ее устройствам, должны применяться определенные функции обеспечения безопасности. К ним относятся шифрование или дешифрование, цифровая подпись, аутентификация сообщений, аутентификация объектов, авторизация, управление доступом, меры для защиты от DoS-атак, аудит и физическая защита. В таблице 9-1 показано, как требования безопасности выполняются с помощью функций безопасности. Кружок в ячейке указывает на то, что данную функцию безопасности можно использовать для удовлетворения конкретного требования безопасности. Следует отметить, что описание каждой из функций безопасности, перечисленных в таблице 9-1, представлено в разделе 10.

Таблица 9-1 – Связь между требованиями безопасности и функциями безопасности

			Функции безопасности							
			Шифрование/ дешифрование	Цифровая подпись	Аутентификация		Управление доступом	Анти-DoS	Аудит	Физическая защита
					Сообщение	Объект				
Требования безопасности	Конфиденциальность	Хранящиеся данные	○							
		Передаваемые данные	○							
	Целостность	Хранящиеся данные		○	○		○			
		Передаваемые данные		○	○		○			
	Доступность					○		○	○	○
	Неотрекаемость			○					○	○

10 Руководящие указания по безопасности для устройств домашней сети в системах "умных" электросетей

10.1 Функции безопасности для нагрузок

В таблице 10-1 перечислены функции безопасности для нагрузок в составе HAN. В ней показано соответствие требований безопасности функциям безопасности, а также приведено описание возможностей для реализации функций безопасности.

Таблица 10-1 − Функции безопасности для нагрузок домашней сети

Требования безопасности	Функции безопасности	Описание
Доступность	Меры по анти-DoS	Следует рассмотреть возможность обнаружения и смягчения последствий DoS-атак.
	Физическая защита	Следует рассмотреть возможность предотвращения несанкционированного физического доступа, чтобы запретить неавторизованным пользователям манипулировать нагрузками или конфигурировать их.
Целостность	Аутентификация сообщений	Следует рассмотреть возможность генерирования и проверки криптографических данных контроля целостности для обеспечения целостности сообщений и команд управления. Криптографические данные контроля целостности можно сгенерировать с помощью механизма кода аутентификации сообщений на основе хеширования (HMAC).
Конфиденциальность	Шифрование и дешифрование	Следует рассмотреть возможность расшифровки зашифрованных командных сообщений от HEMS.

10.2 Функции безопасности для распределенных энергоресурсов

В таблице 10-2 перечислены функции безопасности для DER в составе HAN. В ней показано соответствие требований безопасности функциям безопасности, а также приведено описание возможностей для реализации функций безопасности.

Таблица 10-2 − Функции безопасности для распределенных энергоресурсов в составе домашней сети

Требования безопасности	Функции безопасности	Описание
Доступность	Меры по анти-DoS	Следует рассмотреть возможность обнаружения и смягчения последствий DoS-атак.
	Физическая защита	Следует рассмотреть возможность предотвращения несанкционированного физического доступа, чтобы запретить неавторизованным пользователям манипулировать DER или конфигурировать их.
Целостность	Аутентификация сообщений	Следует рассмотреть возможность генерирования и проверки криптографических данных контроля целостности для обеспечения целостности сообщений и команд управления. Криптографические данные целостности могут генерироваться механизмом HMAC или цифровой подписи.
	Аутентификация объектов	• Следует рассмотреть возможность аутентификации удаленных терминалов, отправляющих сообщения с командами управления. В качестве метода аутентификации может рассматриваться проверка криптографической информации о полномочиях или сертификата. • Следует рассмотреть возможность аутентификации пользователей, пытающихся конфигурировать ресурсы DER или манипулировать ими. Типичным способом аутентификации пользователей является проверка пароля. Альтернативой могут служить биометрические данные, такие как отпечатки пальцев.
	Управление доступом	Следует рассмотреть возможность выдачи разрешения на изменение конфигурации ресурсов DER и манипулирование ими только авторизованным пользователям.
Конфиден-циальность	Шифрование и дешифрование	Следует рассмотреть возможность расшифровки зашифрованных командных сообщений от HEMS.
Неотрекаемость	Цифровая подпись	Следует рассмотреть возможность проверки цифровой подписи, включенной в сообщение с командой управления.
	Аудит	Следует рассмотреть возможность создания и ведения контрольных журналов для обеспечения отчетности. Зарядка и разрядка ESS могут быть важными действиями, которые необходимо регистрировать.

10.3 Функции безопасности для зарядных устройств электромобиля

В таблице 10-3 перечислены функции безопасности для зарядных устройств EV в составе HAN. В ней показано соответствие требований безопасности функциям безопасности, а также приведено описание возможностей для реализации функций безопасности.

Таблица 10-3 − Функции безопасности для зарядных устройств электромобиля в составе домашней сети

Требования безопасности	Функции безопасности	Описание
Доступность	Меры по анти-DoS	Следует рассмотреть возможность обнаружения и смягчения последствий DoS-атак.
	Физическая защита	Следует рассмотреть возможность предотвращения несанкционированного физического доступа, чтобы запретить неавторизованным пользователям манипулировать зарядными устройствами или конфигурировать их.
Целостность	Аутентификация сообщений	Следует рассмотреть возможность генерирования и проверки криптографических данных контроля целостности для обеспечения целостности сообщений и команд управления. Криптографические данные целостности могут генерироваться механизмом HMAC или цифровой подписи.
	Аутентификация объектов	• Следует рассмотреть возможность аутентификации удаленных терминалов, отправляющих сообщения с командами управления. В качестве метода аутентификации может рассматриваться проверка криптографической информации о полномочиях или сертификата. • Следует рассмотреть возможность аутентификации пользователей, пытающихся конфигурировать зарядные устройства или использовать их. Типичным способом аутентификации пользователей является проверка пароля. Альтернативой могут служить биометрические данные, такие как отпечатки пальцев.
	Управление доступом	Следует рассмотреть возможность выдачи разрешения на изменение конфигурации зарядных устройств и манипулирование ими только авторизованным пользователям.
Конфиден-циальность	Шифрование и дешифрование	Следует рассмотреть возможность расшифровки зашифрованных командных сообщений от HEMS.
Неотрекае-мость	Цифровая подпись	Следует рассмотреть возможность проверки цифровой подписи, включенной в сообщения с командами управления.
	Аудит	Следует рассмотреть возможность создания и ведения контрольных журналов для обеспечения отчетности. Начало или прекращение зарядки может быть важным действием, которое необходимо регистрировать.

10.4 Функции безопасности для клиентских индикаторов энергопотребления

В таблице 10-4 перечислены функции безопасности для CED в составе HAN. В ней показано соответствие требований безопасности функциям безопасности, а также приведено описание возможностей для реализации функций безопасности.

Таблица 10-4 − Функции безопасности для клиентских индикаторов энергопотребления в составе домашней сети

Требования безопасности	Функции безопасности	Описание
Доступность	Физическая защита	Следует рассмотреть возможность предотвращения несанкционированного физического доступа, чтобы запретить неавторизованным пользователям применять CED.
Целостность	Аутентификация сообщений	Следует рассмотреть возможность генерирования и проверки криптографических данных контроля целостности для обеспечения целостности сообщений о состоянии, передаваемых HEMS, и команд управления, отправляемых в HEMS. Криптографические данные целостности могут генерироваться механизмом HMAC или цифровой подписи.
	Аутентификация объектов	• Следует рассмотреть возможность аутентификации HEMS. В качестве метода аутентификации может рассматриваться проверка сертификата. • Рассматривается возможность аутентификации пользователей, пытающихся применять CED. Типичным способом аутентификации пользователей является проверка пароля. Альтернативой могут служить биометрические данные, такие как отпечатки пальцев.
	Управление доступом	Следует рассмотреть возможность выдачи разрешения на изменение конфигурации индикаторов CED и эксплуатацию их функций только авторизованным пользователям.
	Целостность приложений	Следует рассмотреть возможность обеспечения целостности приложений для обнаружения приложений, зараженных вредоносными программами или измененных злоумышленниками. Исполняемые файлы или библиотеки могут быть намеренно изменены или удалены злоумышленниками, что приводит к неустойчивости конкретного приложения. С помощью этой функции устройства HAN могут определять, не изменилось ли данное приложение. Примером метода реализации этой функции может служить проверка криптографического кода целостности приложения, который генерируется при установке или обновлении данного приложения.
Конфиден-циальность	Шифрование или дешифро-вание	• Следует рассмотреть возможность шифрования или дешифрования сообщений, передаваемых или принимаемых HEMS, для защиты командных сообщений и сообщений, содержащих личную информацию. • Следует рассмотреть возможность шифрования или дешифрования данных, хранящихся в CED, для защиты личной информации в CED.
Неотрекае-мость	Цифровая подпись	Следует рассмотреть возможность проверки цифровой подписи, включенной в команду управления.
	Аудит	Следует рассмотреть возможность создания и ведения контрольных журналов для обеспечения отчетности.

10.5 Функции безопасности для домашней системы управления энергопотреблением

В таблице 10-5 перечислены функции безопасности для HEMS в составе HAN. В ней показано соответствие требований безопасности функциям безопасности, а также приведено подробное описание возможностей для реализации функций безопасности.

Таблица 10-5 − Функции безопасности для домашней системы управления энергопотреблением в составе домашней сети

Требования безопасности	Функции безопасности	Описание
Доступность	Меры по анти-DoS	Следует рассмотреть возможность обнаружения и смягчения последствий DoS-атак. В частности, услуга, которая используется клиентами для управления нагрузками и DER, должна быть защищена от DoS-атак.
	Физическая защита	Следует рассмотреть возможность предотвращения несанкционированного физического доступа, чтобы запретить неавторизованным пользователям эксплуатировать HEMS.
Целостность	Аутентификация сообщений	Следует рассмотреть возможность генерирования и проверки криптографических данных контроля целостности для обеспечения целостности сообщений о состоянии, поступающих от других устройств (нагрузок, DER и зарядных устройств EV), и команд управления, передаваемых в другие устройства (нагрузки, DER и зарядные устройства EV). Криптографические данные целостности могут генерироваться механизмом HMAC или цифровой подписи.
	Аутентификация объектов	• Следует рассмотреть возможность аутентификации удаленных терминалов. В качестве метода аутентификации может рассматриваться проверка сертификата. Для нагрузок с низкой вычислительной мощностью аутентификация может выполняться путем проверки информации о полномочиях, сгенерированной на основе предварительно распространенного секретного ключа. • Следует рассмотреть возможность аутентификации пользователей, пытающихся эксплуатировать HEMS. Типичным способом аутентификации пользователей является проверка пароля. Альтернативой могут служить биометрические данные и код быстрого ответа.
	Управление доступом	Следует рассмотреть возможность выдачи разрешения на изменение конфигурации системы HEMS и эксплуатацию ее функций только авторизованным пользователям. Необходимо разделить учетные записи администраторов и обычных пользователей. Следует создавать и использовать отдельные учетные записи для разных целей, чтобы ограничить злоумышленникам доступ к конфиденциальной информации, функциям и другим учетным записям, если им удалось взломать одну учетную запись.
	Целостность приложений	Следует рассмотреть возможность обеспечения целостности приложений для обнаружения приложений, зараженных вредоносными программами или измененных злоумышленниками. Исполняемые файлы или библиотеки могут быть намеренно изменены или удалены злоумышленниками, что приводит к неустойчивости конкретного приложения. С помощью этой функции устройства HAN могут определять, не изменилось ли данное приложение. Примером метода реализации этой функции может служить проверка криптографического кода целостности приложения, который генерируется при установке или обновлении данного приложения.
Конфиден-циальность	Шифрование или дешифро-вание	• Следует рассмотреть возможность шифрования или дешифрования сообщений, передаваемых или принимаемых другим объектом в составе HAN, для защиты командных сообщений и сообщений, содержащих личную информацию. • Следует рассмотреть возможность шифрования или дешифрования данных, хранящихся в HEMS, для защиты личной информации в HEMS в случае необходимости.
Неотрекаемость	Цифровая подпись	Следует рассмотреть возможность проверки цифровой подписи, включенной в команду управления.
	Аудит	Следует рассмотреть возможность создания и ведения контрольных журналов для обеспечения отчетности.

10.6 Функции безопасности для интерфейса услуг энергоснабжения

В таблице 10-6 перечислены функции безопасности для ESI в составе HAN. В ней показано соответствие требований безопасности функциям безопасности, а также приведено подробное описание возможностей для реализации функций безопасности.

Таблица 10-6 − Функции безопасности для интерфейса услуг энергоснабжения в составе домашней сети

Требования безопасности	Функции безопасности	Описание
Доступность	Физическая защита	Следует рассмотреть возможность предотвращения несанкционированного физического доступа, чтобы запретить неавторизованным пользователям применять ESI.
Целостность	Управление доступом	• Следует рассмотреть возможность выдачи разрешения на доступ к HAN только авторизованным устройствам. Для точек доступа Wi-Fi следует применять защищенный доступ Wi-Fi (WPA) II со сложным паролем для предотвращения атак методом угадывания пароля. Кроме того, функция широковещательной передачи идентификатора набора услуг должна быть отключена. Для удовлетворения требований безопасности точек доступа Zigbee или Bluetooth должны полностью применяться элементы обеспечения безопасности, указанные в спецификации каждого протокола. • Следует рассмотреть возможность блокировки несанкционированного трафика на основе уникальных ID. В качестве уникального ID может использоваться адрес управления доступом к среде передачи (MAC) или адрес протокола Интернет (IP) устройства.
	Целостность приложений	Следует рассмотреть возможность обеспечения целостности приложений для обнаружения приложений, зараженных вредоносными программами или измененных злоумышленниками. Исполняемые файлы или библиотеки могут быть намеренно изменены или удалены злоумышленниками, что приведет к неустойчивости конкретного приложения. С помощью этой функции устройства HAN могут определять, не изменилось ли данное приложение. Примером метода реализации этой функции может служить проверка криптографического кода целостности приложения, который генерируется при установке или обновлении данного приложения.

10.7 Функции безопасности для соединений

В таблице 10-7 перечислены функции безопасности соединений в составе HAN. В ней показано соответствие требований безопасности функциям безопасности, а также приведено описание возможностей для реализации функций безопасности.

Таблица 10-7 − Функции безопасности для связи в домашней сети

Требования безопасности	Функции безопасности	Описание
Доступность	Меры по анти-DoS	Следует рассмотреть возможность обнаружения и смягчения последствий DoS-атак.
Целостность	Аутентификация сообщений/ объектов	Следует рассмотреть возможность взаимной аутентификации объектов линии связи и сообщений для обеспечения целостности данных линии связи. В качестве подходящего варианта для этого может применяться протокол безопасности транспортного уровня (TLS) или протокол дейтаграмм безопасности транспортного уровня (DTLS) с использованием сертификатов. Для TLS или DTLS следует выбрать надежный криптографический алгоритм.
	Управление доступом	• Следует рассмотреть возможность выдать разрешения на доступ к HAN только авторизованным местным устройствам. • Следует рассмотреть возможность блокировки несанкционированного трафика на основе уникальных ID. В качестве уникального ID может использоваться MAC-адрес или IP-адрес устройства.
Конфиден-циальность	Шифрование или дешифро-вание	Следует рассмотреть возможность шифрования или дешифрования данных, хранящихся в HEMS, для защиты личной информации в HEMS в случае необходимости.

Библиография

[b-ITU-T G.9959] Recommendation ITU-T G.9959 (2015), *Short range narrow-band digital radiocommunication transceivers – PHY, MAC, AR and LLC layer specifications.*

[b-ITU-T L.1430] Recommendation ITU-T L.1430 (2013), *Methodology for assessment of the environmental impact of information and communication technology greenhouse gas and energy projects.*

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

[b-ITU-T Y.4409] Recommendation ITU-T Y.4409/Y.2070 (2015), *Requirements and architecture of the home energy management system and home network services*.

[b-ITU-T Smart-O-33] ITU-T FG-Smart Grid: Smart-O-33Rev.6 (2011), *Smart grid architecture*; http://www.itu.int/en/ITU-T/focusgroups/smart/Documents/smart-o-0033r6_architecture_deliverable.doc

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, 2019 г.