Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Тематическая секция
Криптография в энергетическом секторе

Бондаренко Александр Иванович
Со-руководитель РГ СКАиП технического комитета по стандартизации ТК 26 «Криптографическая защита информации»

МИНИСТЕРСТВО
ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Пресненская наб., д.10, стр.2, Москва, 125039
Юридический адрес: Тверская, 7, Москва
Справочная: +7 (495) 771-8000

_____ №_____

на №_____ от _____

Март 2020 года

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

№_____ от _____

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации направляет на рассмотрение аналитический отчёт ПАО «Интер РАО ЕЭС» о проведении работ по «Анализу и оценки адекватности рискам и угрозам информационной безопасности существующих стандартов киберфизических систем, включая «Интернет вещей»; по разработке проектов стандартов безопасности для киберфизических систем, включая «Интернет вещей», а также – требований и методик проверки киберфизических систем, включая «Интернет вещей», выполненный в рамках реализации мероприятия федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации».

АНАЛИТИЧЕСКИЙ ОТЧЕТ

о проведении работ по:

Анализу и оценки адекватности рискам и угрозам информационной безопасности существующих стандартов киберфизических систем, включая «Интернет вещей»; по разработке проектов стандартов безопасности для киберфизических систем, включая «Интернет вещей», а также – требований и методик проверки киберфизических систем, включая «Интернет вещей».

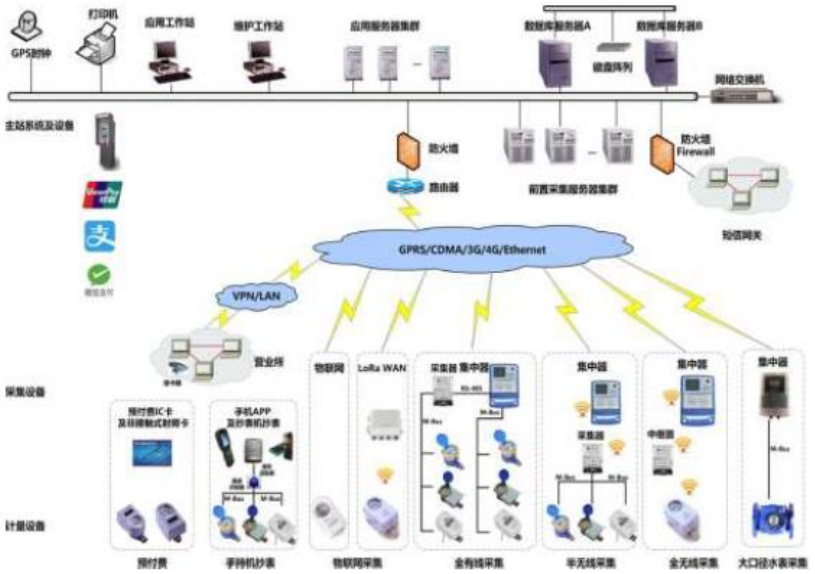
ЗАРУБЕЖНЫЙ ОПЫТ РЕАЛИЗАЦИИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ УЧЕТА ЭНЕРГИИ

Докладчик:
Дата:

Китай

- В данный момент страна находится на 3, завершающем этапе пятилетнего плана построения ИСУЭ.
- Программа контролируется на правительственном уровне Государственной сетевой корпорацией Китая – SGCC.
- Оборудование делают 65 компаний, общий рынок умных счётчиков Китая оценивается в 350 миллионов шт.
- На данный момент есть информация, что все пользователи SGCC оснащены умными счётчиками.
- Лидирующие производители:
  - Jiangsu Linyang Electronics Co., Ltd 6.48%
  - Waision Group Holdings Limited 6.07%
  - Shenzhen Clou Electronics Co., Ltd. 5.95%

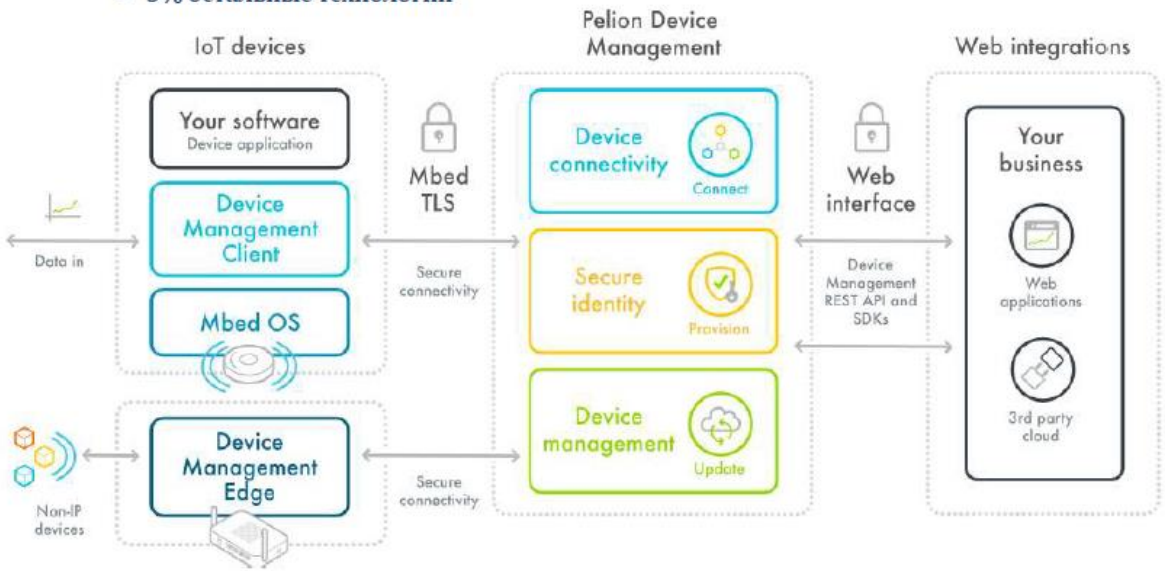
Решение на базе LTE от Huawei, внедренное одной из крупнейших компаний Tianjin Electric Power



- Используемые технологии передачи данных:
  - 40% ZigBEE
  - 35% NB-IoT
  - 10% M-Bus
  - 5% LoRaWAN,
  - 5% RS-485 + GSM
  - 5% PLC и другие

Южная Корея

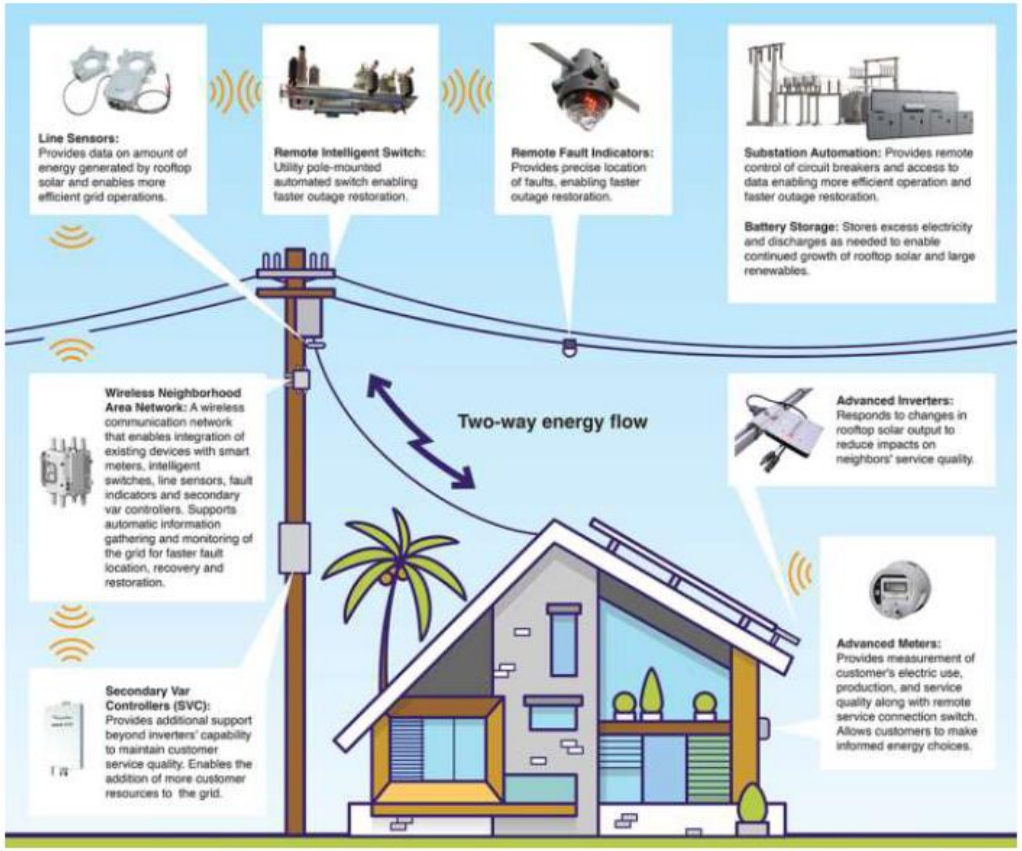
- Контроль за созданием ИСУЭ осуществляет корпорация Korea Electric Power Corporation (KEPCO), владеющая 93% рынка электроэнергии.
- Технологическое решение для ИСУЭ Южной Корее разрабатывает Корейский институт интеллектуальных сетей (KSGI) – подразделение KEPCO
- Наиболее используемые технологии для передачи данных с приборов учета:
  - **65% NB IoT, LTE-M, EC-GSM-IoT (благодаря сотрудничеству с крупнейшими операторами связи KT Corp и LG Uplus)**
  - **20% ZigBee**
  - **10% LoRa**
  - **5% остальные технологии**



Для безопасности данных применяется Mbed TLS

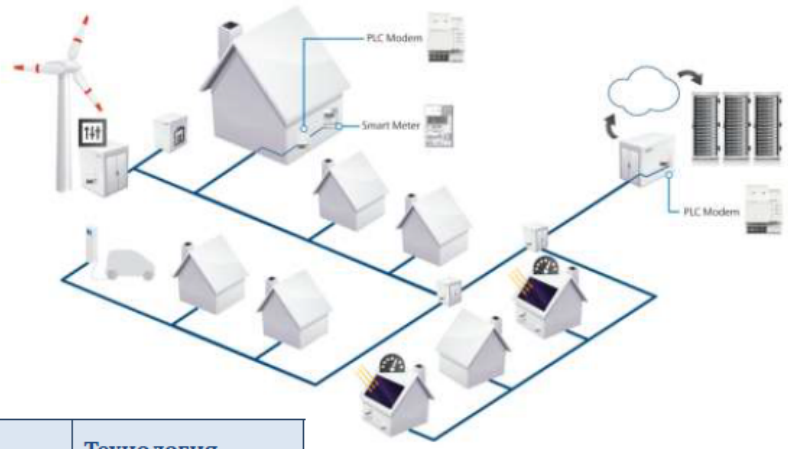
США

- Всего на территории США более 50 сбытовых компаний, из них более 10 крупнейших и 30 крупных. Некоторые из них в данный момент находятся в стадии повсеместного внедрения ИСУЭ на территории влияния:
- NiSource Inc. (одна из крупнейших, обслуживает 7 штатов) – внедряет Smart Grid с 2008 года (вместе с Cisco)
- Exelon Corporation (Чикаго, более 10 млн клиентов). Называют себя лидером в создании интеллектуальных электрических сетей будущего. Выпускают свои умные устройства под маркой ComEd - An Exelon Company
- HAWAIIAN ELECTRIC – в данный момент следует стратегии Grid Modernization Strategy
- Передача данных на промышленных объектах на базеWi-Fi
- Используемые технологии передачи данных с абонентских устройств
  - **60% ZigBee**
  - **30% WiMAX**
  - **8% PLC**
  - **2% другие технологии**



Европа

- Правила разработки «Интеллектуальных сетей» определены в Евросоюзе «Платформой европейских интеллектуальных сетей электроснабжения» (Smart Grid European Technology Platform).
- Всего на территории Европы около 50 энергетических компаний (По 1-5 в каждой стране), входящих в SGETP.
- European Technology & Innovation Platforms (ETIPs) – компания, организованная европейской комиссией для реализации стратегического плана по ИСУЭ в Евросоюзе.
- Дорожная карта с 2017 до 2026 подразумевает полный охват территорий Евросоюза системами интеллектуального учёта.
- Реле отключения нагрузки не является обязательным требованием ИПУ, однако более 70% ПУ оснащены реле.



Страна	Энергетические/ сбытовые компании	Производители оборудования	Технология передачи данных
Испания, Польша, Румыния, Португалия, Швейцария, Великобритания	Red Eléctrica de España (roc.), PSE SA (roc.), Electrica North Transylvania, REN Swissgrid(roc.)	ORBIS, Sogecam Energy, ZIV, Itron, Sagem, L&G, Energa Operator, El Sewedy и др.	PLC: Powerline Intelligent Metering Evolution (PRIME)
Франция, Нидерланды, Бельгия, Германия, Италия , Малайзия	ERDF, RTE, TenneT(roc.), Elia, E.ON, Vattenfall, Enel Tenaga Nasional, Berhad	Maxim, Smart Metering Solution, SIEMENS, Toshiba Corporation, Landis+Gyr S.A.S., EDF, ENEDiS, EVN, Itron Inc., SAGEMCOM ENERGY and TELECOM SAS, Trialog, ACN и др.	PLC: G3

- Большинство ИСУЭ реализуют предоплатный тариф с автоматическим отключением питания при достижении лимитов.
- Технологии построения «Интеллектуальных сетей»
  - 50% **G3-PLC**
  - 48% **PRIME-PLC**
  - 2% различные RF технологии (ZigBee, NB IoT, LPWAN)

PRIME ALLIANCE

Draft Specification for

PoweRline Intelligent Metering Evolution

PRIME ALLIANCE

Prepared by the PRIME Alliance Technical Working Group

- Authentication is guaranteed by the fact that each Node has its own secret key known only by the Node itself and the Base Node.
- Data integrity is guaranteed by the fact that the payload CRC is encrypted.

4.3.8.2.2.2 Cryptographic primitives

The cryptographic algorithm used in this specification is the AES, as specified in FIPS197. The specification describes the algorithm with three possible key sizes; the 128-bit secret key represents a good level of security for preserving privacy up to 2030 and beyond, as specified in SP800-57, page 66, table 4.

AES is used according to the so-called ECB, as specified in SP800-38A. It is a block-ciphering mode where plain text is divided into 128-bit blocks. Padding is applied if the last block is smaller than 128 bits. Padding is implemented with the addition of a bit equal to 1 and as many zeroes as necessary to reach a length of the string to be encrypted as a multiple of 128 bits. Encryption is performed one block at a time, using the same working key for all the data.

eRDF
ÉLECTRICITÉ RÉSEAU DISTRIBUTION FRANCE

PLC G3 PHYSICAL LAYER SPECIFICATION

TITLE

PLC G3 Physical Layer Specification

TYPE	SPECIFICATION	**PROJECT**	PLC G3 OFDM

SECURITY BUILDING BLOCKS

This annex specifies the cryptographic primitives and mechanisms that are used to implement the security protocols in this standard.

B.1 Symmetric-Key Cryptographic Building Blocks

The following symmetric-key cryptographic primitives and data elements are defined for use with all security-processing operations specified in this standard.

B.1.1 Block-Cipher

The block-cipher used in this specification shall be the Advanced Encryption Standard AES-128, as specified in FIPS Pub 197. This block-cipher has a key size *keylen* that is equal to the block size, in bits, *i.e.*, *keylen*=128.