ИНТЕЛЛЕКТУАЛЬНЫЙ СЧЁТЧИК ЭЛЕКТРОЭНЕРГИИ: АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю.А. Пушняк, *независимый эксперт (Республика Молдова)*

The modern electricity smart meter can become a target for hacker attacks. In this report all potential threats are analyzed and the general requirements for meter data security are formulated.

Современный интеллектуальный счётчик электроэнергии может стать мишенью для хакерских атак. В докладе проанализированы все потенциальные угрозы и сформулированы общие требования к информационной безопасности счётчика.

Информационные технологии активно внедряются в область учёта бытового потребления энергоресурсов. Современный интеллектуальный счётчик электроэнергии уже способен выполнять десятки функций и поддерживать двусторонние коммуникации через распределённые сети связи. Эти качества открывают принципиально новые возможности в области учёта, позволяют поставщикам внедрять новые сервисы для потребителей и общими усилиями эффективно решать задачи энергосбережения.

Вместе с тем, возникают и принципиально новые проблемы. На фоне постоянного роста стоимости энергоресурсов и ожидаемого массового (порядка 10^8 точек учёта) распространения интеллектуальных счётчиков по всему миру – становится весьма актуальной и острой проблема обеспечения информационной безопасности. Дело в том, что современный счётчик электроэнергии – это по сути "маленький компьютер", включенный в распределённую сеть связи. Его предок – электромеханический счётчик – часто подвергался разного рода непосредственным атакам со стороны злоумышленников, недобросовестных потребителей. Теперь счётчик становится ещё и потенциальной мишенью для … хакерских атак через сеть связи [1].

Какие меры предпринимаются для решений этой проблемы? Прежде всего, усилиями ряда международных организаций формируется соответствующая нормативная база [2,3], но этот процесс еще далёк от завершения. Кроме того, по мнению автора, некоторые из уже опубликованных положений и рекомендаций имеют весьма спорный характер; среди разработчиков нормативных документов ощущается явная нехватка специалистов по информационной безопасности и криптографии.

Тем временем ведущие мировые производители счётчиков предлага-

ют свои собственные решения. Как правило, эти решения затрагивают лишь некоторые аспекты проблемы и имеют явную маркетинговую направленность. Дело в том, что встроенные средства обеспечения информационной безопасности обходятся производителю достаточно дорого. Они заметно повышают себестоимость счётчика, и, следовательно, либо приводят к его удорожанию, либо снижают долю прибыли при продаже счётчика по прежней цене. В то же время многие производители сознательно или подсознательно недооценивают степень "информационной" угрозы. А если угроза невелика, зачем идти на дополнительные расходы? Этим и определяется отношение большинства производителей к встроенным средствам информационной безопасности - да, формально они реализуются, но реализуются ровно настолько, насколько это необходимо для того, чтобы успокоить потенциального покупателя, который конечно же слышал об этой проблеме, но ничего в ней не понимает ("данные шифруются? – да, разумеется! – ну и замечательно, покупаю!").

Ниже приводится перечень общих требований по информационной безопасности к любому современному счётчику электроэнергии. Перечень был сформулирован автором на основе многолетнего личного опыта проектирования и эксплуатации систем учёта.

Требования:

1. Соответствие требованиям международных стандартов (IEC, DLMS/COSEM и др.)
2. Аутентификация источника при приёме/передаче сообщений
3. Шифрование сообщений
4. Помехоустойчивое кодирование
5. Поддержка режима предоплаты (опционально, для счётчиков с prepayment mode)
6. Безопасный локальный интерфейс для поддержки домашней сети связи
7. Периодическая проверка целостности резидентного программного обеспечения
8. Защита метрологического обеспечения от изменений в процессе эксплуатации
9. Доступ к резидентным программам и данным через оптический порт по паролю
10. Датчик вскрытия крышки счётчика
11. Датчик вскрытия крышки клеммника
12. Датчик наличия внешнего магнитного поля
13. Датчик температуры внутри корпуса
14. Встроенный журнал событий с регламентированным доступом
15. Поддержка аварийных сообщений
16. Безопасное управление настройками счётчика

17. Безопасное изменение резидентного программного обеспечения (upgrade)

В докладе подробно анализируются потенциальные информационные угрозы для счётчика и предлагаются встроенные аппаратные и программные средства, способные эффективно парировать эти угрозы.

Полученные результаты могут быть использованы в качестве справочного руководства при выборе системы централизованного учёта энергоресурсов. Кроме того, эти результаты могут служить основой (аналогией) при разработке аспектов информационной безопасности для других подобных систем, например – для защиты разнообразных оконечных устройств (user appliances) в рамках концепции "Умный дом".

Источники:

1. Bruce Schneier. Hacking Power Networks. CRYPTO-GRAM, February 15, 2008. http://www.counterpane.com
2. Electricity metering - Data exchange for meter reading, tariff and load control. Международные стандарты серии IEC 62056.
3. DLMS/COSEM for smart metering. http://www.dlms.com

ИНФОРМАЦИЯ КАК ТОВАР В XXI ВЕКЕ: АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ НАЦИОНАЛЬНЫМ РЫНКАМ

Анатолий Крапивенский, *ФГОУ ВПО «Волгоградская академия государственной службы» (Российская Федерация)*

The problem of national markets security in the segment of informational products is considered in the given article. Author investigates the phenomenal properties of information as a product and analyzes the paradigm of threats to national security in the above area.

В XXI столетии информация переходит в раздел наиболее востребованных товаров, предлагаемых к продаже или обмену. Современное состояние общества характеризуется лавинообразным ростом процесса "производства, потребления и накопления информации во всех отраслях человеческой деятельности" [1: 3]. Это объясняется объективным увеличением общего трафика информационного контента в соци-