ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СИСТЕМАХ ИНТЕЛЛЕКТУАЛЬНОГО УЧЕТА

Н.Н. СИДОРЕНКО (АО ГК "Системы и Технологии")

Обеспечение безопасности в системах интеллектуального учета – вопрос, которому на текущий момент не уделяется достаточно внимания как в Российской Федерации, так и за рубежом, что чревато как уже сейчас, так и в ближайшем будущем, фатальными последствиями.

Ключевые слова: *энергетика; энергоресурсы; интеллектуальный учет; приборы учета электроэнергии; потребители электроэнергии; отключение электроэнергии; энергоснабжение; экономика; информационная безопасность; несанкционированное вмешательство; Постановления Правительства РФ N 890 от 19.06.2020 г.; ФЗ N 522 от 27.12.2018 г.; программное обеспечение; программное обеспечение верхнего уровня; импортозамещение; микроэлектронные компоненты; ОС Linux; BigData; построение ИСУ; сертифицированные СЗИ.*

Существенные риски при эксплуатации систем обусловлены наличием в приборах учета (в отличие от давно эксплуатирующихся систем коммерческого учета) функционала, позволяющего осуществлять удаленное параметрирование и управление, как одиночным прибором учета, так и их большими группами, в том числе удаленно ограничивать или прекращать энергоснабжение потребителей.

Наличие возможностей посылки с верхнего уровня систем массовых команд, наличие команд параметрирования, вплоть до изменения внутреннего программного обеспечения счетчика, в совокупности с возможностью отключения энергоснабжения, может привести к ситуации, когда вследствие ошибок в программном обеспечении, или постороннего вмешательства в работу системы, могут быть отключены от энергоснабжения миллионы потребителей. Восстановление энергоснабжения потребует в лучшем случае перепрошивки встроенного программного обеспечения на месте (в крайнем случае – установки перемычки или замены счетчика), что, учитывая возможные масштабы отключений, потребует выполнения работ со сроками, исчисляемыми месяцами.

Учитывая то, что системы интеллектуального учета охватывают не только частных лиц, но и всех потребителей по низкому уровню напряжения (0,4 кВ), отключение может остановить авиа- и железнодорожное сообщение, метро, парализовать работу государственных и частных предприятий, заблокировать людей в поездах метрополитена, лифтах, остановить работу насосных станций, станций водоочистки, систем отопления и т.д., прервать снабжение населения продуктами питания, водой. Список можно долго продолжать.

Примером такой ситуации в РФ может служить авария (начавшаяся с простого возгорания трансформаторов) на ПС Чагино в Москве 23.05.2005, с дальнейшим каскадным отключением других подстанций, при которой, хотя удалось полностью восстановить энергоснабжение за два дня, отключения нанесли существенный ущерб работе органов государственной власти и управления, банков, связи, торговле, промышленным предприятиям, транспорту, здравоохранению, коммунальным службам. По этому примеру можно оценить масштабы проблем, которые вызовет отключение от энергоснабжения на порядки большего количества потребителей, и не на два дня, а на недели или месяцы – последствия будут фатальны для населения и экономики государства.

Впервые на серьезном уровне проблема безопасности была озвучена на конференции Black Hat в США в 2009 году авторитетной компанией IOActive, которая провела собственное исследование уязвимостей систем интеллектуального учета. Результат исследования был неутешительным – несанкционированное вмешательство в работу систем возможно даже без наличия специализированного оборудования и квалификации, команды параметрирования и управления приборами учета большинства производителей передаются без требуемой степени защиты и т.д. К сожалению, на текущий момент ситуация существенно не изменилась как за рубежом, так и в РФ.

Актуальность проблемы безопасности в РФ до недавнего времени была ограничена отсутствием крупных систем интеллектуального учета. Из 76 млн потребителей приборы интеллектуального учета на текущий момент установлены у около 3 млн, существенная часть

которых не входит в состав систем учета, как следствие отсутствия до недавнего времени нормативной базы для подобных систем.

Ситуация изменилась с выходом в декабре 2018 года Федерального Закона N 522 и в июне 2020 года Постановления Правительства РФ N 890, в которых законодательно введено понятие интеллектуального учета, регламентированы взаимоотношения участников розничных рынков электроэнергии, определены требования ко всем компонентам систем – оборудованию, программному обеспечению, каналам связи и т.д.

В Постановлении Правительства РФ N 890 вопросы безопасности описаны в достаточно общем виде, однако в преамбуле постановления определено поручение профильным госструктурам, включая Минэнерго, ФСТЭК и ФСБ, в срок до 01.01.2021 разработать и опубликовать базовую модель угроз безопасности информации, которая определит все необходимые требования к компонентам систем, включая программное обеспечение верхнего уровня, связное оборудование, каналы связи, приборы учета и т.д. Учитывая, что требования, описанные в Постановлении, начнут применяться с 01.01.2022, можно предположить, что производителям вышеуказанных компонентов систем также будет дан срок для приведения в соответствие с новыми требованиями своей продукции.

Однако следует отметить сложности реализации предполагаемых требований по безопасности в РФ, а именно:

- на рынке специализированного программного обеспечения для систем интеллектуального учета, вследствие более низкой себестоимости, присутствуют только решения на базе программных продуктов компаний Microsoft, Oracle, и т.п., что возможно приведет к необходимости, для выполнения новых требований по безопасности, создания принципиально новых программных продуктов на базе решений с открытым кодом;
- в части оборудования риски обусловлены необходимостью применения зарубежных комплектующих, как следствие отсутствия или недостаточной мощности отечественных производств. Также существует проблема более высокой стоимости отечественных комплектующих, при которой, даже при наличии производств на территории РФ, производителями оборудования отдается предпочтение компонентам зарубежных компаний.

Решением вышеописанных проблем может стать только объединение существующих ресурсов крупных участников рынка, производителей оборудования и программного обеспечения с разделением выполнения требуемых работ. При этом возможные шаги выглядят следующим образом:

- Совместная разработка “массового счетчика”. На текущий момент крупные участники рынка сосредоточились на создании сборочных производств приборов учета различных типов, как наиболее маржинальной части создания систем интеллектуального учета. При этом недостаточно внимания уделяется реальным возможностям существующих производств микроэлектронных компонентов (они достаточно низкие с учетом требуемого объема оборудования – более 76 млн только приборов учета, а по ряду компонентов вообще отсутствуют). Также недостаточно внимания уделяется вопросам безопасности, формально – как следствие отсутствия нормативной базы (которая появится к концу 2020 года и основные положения которой известны), фактически – с целью снижения себестоимости и увеличения прибыли. К чему это может привести, описано в начале данной статьи. Совместная разработка позволит минимизировать сроки и расходы, при обязательном выполнении требований по безопасности, с учетом реальных возможностей существующих производств, их расширения, создания производств компонентов, которые вообще сейчас отсутствуют на российском рынке. При этом конкурентный рынок приборов учета можно обеспечить разработкой производителями собственных модификаций “массового счетчика”, создав конкуренцию в части решений с более низкой себестоимостью, дополнительным функционалом, повышенной надежностью и т.д.
- Анализ существующих производств микроэлектронных компонентов в РФ. На текущий момент существует тенденция оценки возможностей производства требуемого оборудования по совокупной мощности сборочных производств без привязки к возможностям производственных мощностей микроэлектронных компонентов, что делает такую оценку далекой от реальности. Более правильным подходом видится оценка производств микроэлектроники, оценка необходимости расширения до требуемого объема производства существующих и создание новых производств компонентов. И только при решении этого вопроса, с параллельным решением вопроса создания не-

обходимого объема сборочных производств, и вопроса, что на этих производствах будут производить (см. выше про "массовый счетчик"), можно говорить о готовности отечественной промышленности к выпуску необходимого для систем интеллектуального учета объема продукции.

- Совместная разработка платформы для дальнейшего создания специализированного программного обеспечения верхнего уровня систем интеллектуального учета. Упрощенно, такая платформа должна быть создана на базе решений с открытым кодом и состоять из операционной системы (возможно на базе существующих российских ОС Linux), базы данных высокого быстродействия с возможностью обработки больших объемов данных (BigData, возможно на базе одного из существующих решений), решений по масштабированию системы для возможности сбора данных с большого количества приборов учета, решений по виртуализации и т.д., исключая специфику функционала для конкретных участников рынка, который они будут дописывать самостоятельно, с учетом собственной производственной необходимости. Такой подход позволит существенно сократить время и сроки для создания программного обеспечения с учетом новых требований, в том числе по безопасности, кратно повысит надежность, и сохранит конкурентный рынок программного обеспечения для подобных систем.

В дополнение необходимо отметить, что на текущий момент недостаточно уделяется внимания специфики внедрения систем интеллектуального учета в части зависимости производства приборов учета и готовности программного обеспечения верхнего уровня и инфраструктуры связи, что может привести к значительному увеличению сроков внедрения систем, их удорожанию, увеличению срока окупаемости и т.д.

Сборочные производства, активно создаваемые сейчас участниками рынка, не смогут работать "на склад", специфика внедрения подобных систем, связанная с необходимостью монтажа и пусконаладочных работ большого количества оборудования, требует максимально короткого промежутка между производством прибора учета и его монтажом у потребителя. Ввиду отсутствия, по разным причинам, в том числе финансовым, возможности двух выездов к точке учета, пусконаладочные работы по точке учета должны быть произведены сразу после монтажа оборудования и включать в себя проверку взаимодействия с системой верхнего уровня, которая к моменту начала монтажных и пусконаладочных работ должна быть создана, испытана, быть в полностью работоспособном состоянии, включать функционал "горячего" резервирования в случае сбоев в работе, и предоставлять возможность выполнения пусконаладочных работ одновременно по большому количеству оборудования.

На текущий момент в России уже существуют системы верхнего уровня, функционально удовлетворяющие требованиям 890 ПП РФ, при этом нужно отметить, что поскольку требования по безопасности еще не разработаны, то после их разработки и утверждения, потребуется доработка данных программных продуктов, проверка и сертификация. Недостаток внимания к данным проблемам может привести к ситуации остановки работы сборочных производств и внедрений систем, ввиду отсутствия возможности массового внедрения выпускаемых приборов учета, что существенным образом скажется на сроках, стоимости и т.д.

В заключение можно отметить, что вопросы безопасности систем интеллектуального учета электроэнергии, ввиду возросших рисков, связанных с участившимися кибератаками, в том числе на объекты критичной инфраструктуры различных государств, а также масштабы возможных проблем, описанных выше, становятся ключевыми для отечественных производителей оборудования и программного обеспечения. Хочется верить, что с официальным выходом к концу 2020 года требований по безопасности (см. выше), подобные решения будут оперативно разработаны и максимально быстро появятся на рынке.

АО ГК "Системы и Технологии"

Главный офис: 600014, г. Владимир, ул. Лакина, д. 8А.
Телефоны: (4922) 33-67-66, 33-79-60, 33-93-68.
Факс (4922) 42-45-02.
E-mail: st@sicon.ru http://www.sicon.ru

Офис в Москве: 123610, г. Москва,
Краснопресненская набережная, д. 12, оф. 920.
E-mail:dvm@sicon.ru

Сидоренко Николай Николаевич *– заместитель директора АО ГК "Системы и Технологии".*