Особенности криптозащиты информации

в интеллектуальных системах учета электрической энергии

Валерий АНДРЕЕВ,
к. ф.-м. н., заместитель генерального директора АО «ИВК» по научно-исследовательской работе

Электроэнергетика, без преувеличения, возглавляет перечень отраслей промышленности, объекты которых относятся к критической информационной инфраструктуре (КИИ). Любой сбой в энергосистемах мгновенно сказывается на работе промышленных предприятий, газо- и нефтепроводов, банков, транспорта, офисных зданий, больниц, школ, домохозяйств и миллионов других объектов на всей территории страны. Один из критических аспектов – обеспечение защиты данных, которые циркулируют в интеллектуальных системах учета электрической энергии (ИСУЭ) и передаются по общим каналам связи.

Согласно Федеральному закону № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» объектами защиты в автоматизированных системах управления, к которым относятся ИСУЭ, являются программного-аппаратные и программные средства, входящие в состав системы и циркулирующая в ней информация.

Базовая модель угроз и нарушителя ИСУЭ

Системный подход к обеспечению защиты ИСУЭ заложило Министерство энергетики Российской Федерации. Ведомством разработана «Базовая модель угроз безопасности информации в интеллектуальных системах учета электрической энергии (мощности)». Документ опирается на постановление Правительства РФ от 19 июня 2020 г. № 890 «О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)», которым установлены требования по защите информации, обрабатываемой в интеллектуальной системе учета электрической энергии (ИСУЭ), от несанкционированного доступа к ней при ее сборе, передаче и хранении.

«Базовая модель» устанавливает необходимость применения СКЗИ в ИСУЭ для защиты информации, передаваемой по общедоступным каналам связи. В частности, документ содержит систематизированный перечень угроз безопасности информации, которые влияют на обеспечение устойчивого функционирования ИСУЭ. «Базовая модель» – методический документ для ИБ-специалистов, которые организуют и реализуют меры защиты информации, передаваемой по каналам связи.

Однако базовая модель не ориентирована на конкретные практические применения и не содержит информации о вариантах нейтрализации угроз. Поэтому для владельцев ИСУЭ закон предусматривает возможность создания частных моделей угроз. Такие модели позволяют, во-первых, конкретизировать действия внутреннего или внешнего нарушителя, точнее описать угрозы компьютерных атак и компьютерных инцидентов, во-вторых, ориентироваться на уже реализованные

> Именно контур граничных вычислений защищен сегодня наиболее слабо.

и реализуемые мероприятия по обеспечению информационной безопасности ИСУ.

ИСУЭ имеет трехзвенную архитектуру. На нижнем уровне функционируют миллионы датчиков, счетчиков электроэнергии и других устройств, которые установлены непосредственно на объектах. Они регистрируют параметры функционирования линий передачи электроэнергии и передают эти данные в режиме, близком к режиму реального времени, на второй уровень, который образуют сотни тысяч интеллектуальных контроллеров. Эти устройства взаимодействуют и с нижним, и с верхним уровнями ИСУЭ. Во-первых, ведут интеллектуальный учет и первичную обработку данных, поступающих с датчиков, обратно на датчики передают управляющие сигналы. Во-вторых, агрегируют полученные с контроллеров данные и передают их на третий, верхний уровень – в информационные системы анализа и учета данных, развернутые на локальных объектах.

Первый и второй уровни ИСУЭ образуют систему граничных (распределенных) вычислений. Они проводятся в пределах досягаемости конечных устройств. Такой подход позволяет сокращать время сетевого отклика, более эффективно использовать пропускную способность сети. Сбор и первичный анализ данных осуществляются непосредственно в месте генерации потоков данных.

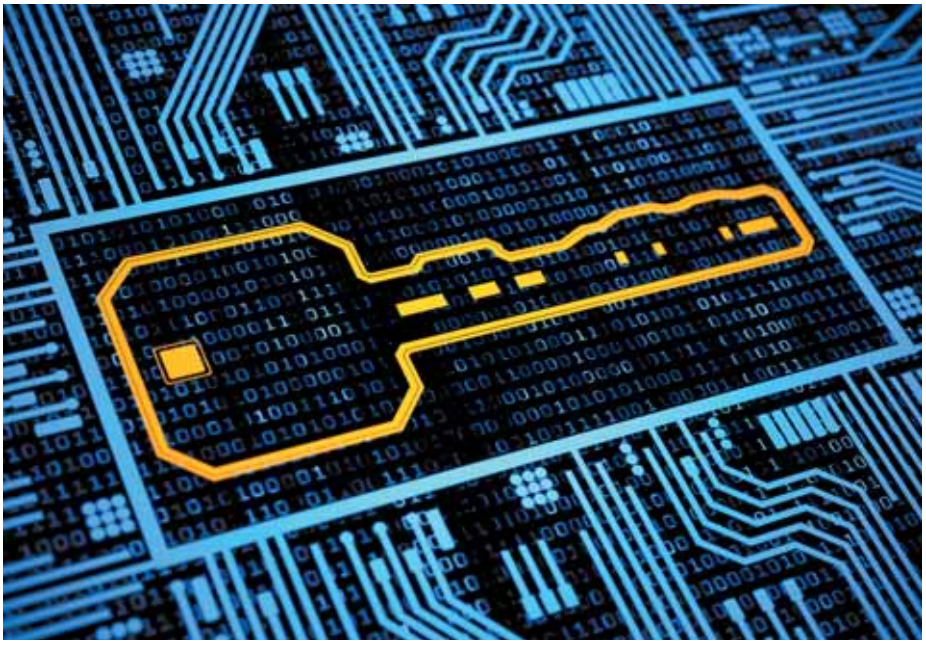
Именно контур граничных вычислений защищен сегодня наиболее слабо. Практически все конечные устройства и часть контроллеров первого и второго уровней находятся «на улице», вне контролируемой зоны, поэтому их невозможно собрать в один защищенный контур. Злоумышленникам относительно несложно получить к ним доступ. Данные передаются по беспроводным каналам связи в «сыром», не зашифрованном виде (например, в виде HTML-файлов), с использованием пакетной радиосвязи общего пользования – надстройки над технологией мобильной связи GSM. Незашифрованные первичные данные, которые передаются по открытым каналам связи, достаточно легко перехватить. Если злоумышленник завладеет данными пула устройств, он может агрегировать и анализировать их, чтобы составить достаточно адекватную картину объекта и использовать эту информацию для вмешательства в работу информационных систем.

На втором уровне системы граничных вычислений несанкционированные действия может совершать «внутренний» злоумышленник – сотрудник организации, знающий, как изменить настройки устройств.

Криптографическая защита ИСУЭ: задачи и решения

Для защиты ИСУЭ «Базовая модель» предусматривает применение сертифицированных ФСБ России средств криптографической защиты информации (СКЗИ). С 1 января 2024 г. применение СКЗИ стало обязательным на уровне ИВК и уровне ИВКЭ для трехуровневой модели ИСУЭ. Система криптографической защиты включает:

- приборы учета со встроенным СКЗИ;
- устройства сбора и передачи данных в защищенном исполнении. Они предназначены для реализации функций групповой защиты приборов учета. Сами приборы учета могут применяться без СКЗИ или с СКЗИ, выполняющими только функцию аутентификации устройства в режиме считывания показаний;
- подсистема криптографической защиты ИСУЭ. Она играет роль «шлюза» для взаимосвязи между элементами ИСУЭ и криптографическими программно-аппаратными комплексами;
- криптографические программно-аппаратные комплексы – серверные СКЗИ, выполняющие криптографические операции с данными;
- подсистему электронной регистрации СКЗИ, осуществляющую регистрацию, ввод в эксплуатацию СКЗИ и управление криптографическими ключами;
- центр доверия, выполняющий функции создания криптографических ключей и ключевых документов.



[1] *Угрозы компьютерных атак и компьютерных инцидентов обозначены в Федеральном законе от 26.07.2017 № 187-ФЗ.*

Как уже отмечалось, устройства ИСУЭ первого и второго уровней размещаются вне контролируемой зоны, поэтому защищать каждый прибор учета или устройство сбора и передачи данных наложенными средствами защиты нецелесообразно. Невозможно установить межсетевые экраны и криптошлюзы на всем периметре инфраструктуры.

Оптимальный вариант защиты – встраиваемые криптографические средства защиты. Однако устройство, в которое имплементирована функциональность крипто, превращается в СКЗИ. На территории Российской Федерации производство, эксплуатация и ремонт криптосредств – лицензируемый вид деятельности. Но предприятия энергетического сектора не имеют соответствующих лицензий и сертифицированных специалистов в штате, поскольку раньше не работали с криптосредствами. Это серьезная проблема. Ее решение потребует от организаций не только формирования пула новых устройств и их сертификации, но и повышения квалификации сотрудников, что может повлечь рост тарифов и отпускных цен.

Другая задача – налаживание массового производства устройств в России. Чтобы стать полноценными криптосредствами, контроллеры должны быть российского производства, климатически- и вандалоустойчивыми, обладать длительным жизненным циклом, достаточной вычислительной мощностью и реализовать функции шифрования каналов связи в соответствии с сертификационными требованиями регулятора. Массовый выпуск таких криптосредств пока не налажен, но созданы прототипы контроллерных чипов на процессорах ARMv7 и ARMv8. Например, производственное объединение «Микрон» уже производит подобные чипы, а компания «Миландр» – счетчики и контроллеры на их основе. Для того, чтобы обеспечить уровень доверия системы, достаточный для передачи данных по беспроводным каналам связи, необходимо оснастить устройства операционной системой, созданной на основе российского репозитория.

Регуляторам также необходимо создать нормативную базу разработки новых интеллектуальных приборов учета и замены старых устройств новыми.

Регуляторам необходимо создать нормативную базу разработки новых интеллектуальных приборов учета и замены старых устройств новыми.

Новые конечные устройства первого уровня будут передавать зашифрованные данные на второй уровень – на интеллектуальные контроллеры. Здесь появится дополнительная наложенная криптоструктура: ЦУК (центр управления ключами шифрования) и криптошлюз, через которые будут передаваться данные. На этом уровне будут выполняться их расшифровка и первичная обработка, а затем чистые данные отправятся на третий уровень, в центр анализа информации.

Обмен информацией между СКЗИ первого и второго уровней требует шифрования данных и, соответственно, использования криптографических ключей на каждом устройстве.

Однако здесь есть серьезная проблема: для миллионов устройств потребуются миллионы ключей. Длина уникального ключа должна быть внушительной, а объем – около 2 Мб. Это резко повышает требования к аппаратной части. Поэтому, скорее всего, централизованные вычисления в такой среде невозможны – они будут неподъемными с точки зрения работы с ключами. По крайней мере, до перехода на квантовые технологии.

Создание СКЗИ для ИСУЭ

Рынок российских комплексных решений для защиты систем ИСУЭ пока формируется, российские компании трудятся над разработкой всех компонентов комплекса обеспечения безопасности.

Наша компания сотрудничает с разработчиками российского ПО и микроэлектроники, регуляторами и заказчиками в рамках отработки структурных, алгоритмических и программно-технических решений подсистемы СКЗИ трактов связи ИСУЭ, позволяющей использовать предлагаемые решения с различными типами (и конструктивными исполнениями) ИВКЭ и ИВК без их существенной доработки.

Специалисты компании сформировали типовые модели угроз информационной безопасности и действий нарушителя информационной безопасности. Решается задача по реализации доступных по стоимости и технологии производства СКЗИ для ИВКЭ, не зависящих от среды материальной реализации ИВКЭ.

В условиях жесткого дефицита кадров специалисты работают над реализацией СКЗИ ИВКЭ с таким уровнем защиты от инвазивных атак, который бы позволял вести установку и присоединение модулей СКЗИ ИВКЭ работниками нелицензированных организаций. Эту же проблему должна решить создаваемая технология массового производства компонентов СКЗИ для ИСУЭ в Российской Федерации. Еще одна задача – их внедрение с минимальным участием организаций, лицензированных на производство и эксплуатацию.

Прорабатывается реализация СКЗИ для ИВК без необходимости использования удостоверяющего центра и громоздких протоколов взаимодействия, ведется разработка высокопроизводительных средств для формирования ключевой информации и ее записи в СКЗИ. ■