Как обеспечить информационную безопасность граничных вычислений КИИ

Валерий АНДРЕЕВ,
заместитель генерального директора по науке и развитию, компания ИВК, к. ф.-м. н.

Проблема критической информационной инфраструктуры остается острой. Для ее решения недостаточно перевести КИИ на российский софт и вычислительную технику. Необходимо обеспечить безопасность граничных вычислений на периметре информационных систем и за его пределами.

Как организованы граничные вычисления в КИИ

Критическая информационная инфраструктура имеет трехзвенную архитектуру. Первый уровень – это миллионы датчиков, счетчиков электроэнергии и подобных устройств, установленных непосредственно на объектах. Они регистрируют параметры работы нефте- и газопроводов, линий передачи электроэнергии, железнодорожных путей и т. п. Практически все они находятся в поле, вне контролируемой зоны КИИ. Эти данные в режиме, близком к режиму реального времени, поступают на второй уровень, который образуют сотни тысяч интеллектуальных контроллеров. Они осуществляют интеллектуальный учет и первичную обработку данных, а также передают на датчики управляющие сигналы. Контроллеры находятся на границе периметра КИИ. Агрегированные данные они передают на третий, верхний уровень – в информационные системы анализа и учета данных, развернутые на локальных объектах. Это информационные системы коммерчески и юридически независимых предприятий (например, «Россети Сибирь», «МРСК Юга» и др.).

Первый и второй уровни КИИ образуют систему граничных (распределенных) вычислений, осуществляемых в пределах досягаемости конечных устройств. Такой тип вычислений позволяет сокращать время сетевого отклика, более эффективно использовать пропускную способность сети. Сбор и первичный анализ данных осуществляются непосредственно в месте генерации потоков данных в отличие от централизованных систем, которые предполагают передачу данных и их последующую обработку в ЦОД. Эта модель эффективна, поскольку вычисления производятся на конечных устройствах и данным не нужно преодолевать километры сетей, чтобы добраться до ЦОД.

Риски системы граничных вычислений КИИ

На сегодняшний день контур граничных вычислений КИИ защищен наиболее слабо. Бреши в системе ее безопасности чреваты рисками нарушения штатной работы объектов КИИ. Эти нарушения могут приводить к обесточиванию целых районов, в которых находятся промышленные предприятия, дома, больницы, школы и другие социальные объекты, к сбоям в работе электростанций, газо- и нефтепроводов, вплоть до экологических катастроф разного масштаба. Поэтому задача номер один – обеспечить безопасность системы граничных вычислений КИИ. Особенно острой эта задача становится в связи с переходом экономики на модель «Индустрия 4.0», которая характеризуется стремительным ростом цифровых промышленных сетей ключевых отраслей экономики, включая нефтегазовую, пищевую, химическую промышленность, городские инфраструктурные

объекты, распределение электроэнергии, водоснабжение, воздушный, автомобильный и железнодорожный транспорт.

Риски системы граничных вычислений КИИ можно разделить на две категории – внешний нарушитель и внутренний нарушитель.

Поле деятельности внешнего нарушителя – это беспроводные каналы связи, неконтролируемая зона, в которой работают конечные устройства и часть контроллеров, а также передача данных по стандартизованным каналам связи беспроводным подключением в открытом виде.

Большую дыру в системах граничных вычислений создает беспроводная система передачи данных. В ее составе – беспроводные каналы связи (General Packet Radio Service – пакетная радиосвязь общего пользования, надстройка над технологией мобильной связи GSM). Данные по ним часто передаются в сыром, незашифрованном виде.

Вторая проблема – размещение конечных устройств, образно говоря, на улице, вне контролируемой зоны. Злоумышленникам проще получить доступ к таким устройствам. Но архитектурное преимущество этой модели состоит в использовании единых унифицированных стандартов обмена данными между устройствами их сбора и передачи, например протокола ПАО «Россети» СПОДЭС. В июле 2020 г. Федеральное агентство по техническому регулированию и метрологии «Росстандарт» утвердило его в качестве национального стандарта Российской Федерации, выпущен ГОСТ Р 58940-2020 «Требования к протоколам обмена информацией между компонентами интеллектуальной системы учета и приборами учета». За один год СПОДЭС прошла путь от корпоративного стандарта до национального стандарта Российской Федерации.

На втором уровне системы граничных вычислений несанкционированные действия может совершать злоумышленник, являющийся сотрудником организации. Внутренний злоумышленник – профессионал, он знает, как изменить настройки, умеет отключать и включать устройства. Для этого использует закрепленную в отраслевых стандартах функциональную возможность управляющих воздействий с устройств второго уровня на средства сбора первичной информации. К примеру, синхронизация времени со службой единого времени на центральном объекте. Для энергетических систем это реальный риск обесточивания объектов оборонного значения, транспорта, здравоохранения.

Как обезопасить систему граничных вычислений КИИ

Незашифрованные первичные данные, которые сегодня передают конечные устройства по открытым каналам связи, достаточно легко перехватить. Сами по себе они не имеют особой ценности, поскольку требуют агрегации и анализа. Но если злоумышленник владеет данными не одного, а пула устройств, он может не только составить представление об объектах КИИ, но и удаленно управлять ими недекларированным способом. Ряд организаций решает задачу обеспечения безопасности системы граничных вычислений с помощью корпоративной ролевой модели. Она регламентирует порядок работы с системой и меры ответственности. В частности, регламентируется порядок доступа должностных лиц к системе и коллективная ответственность за возможные негативные последствия. Но такая практика введена не везде и имеет ряд недостатков, связанных с большими затратами времени на коллективное выполнение рутинных операций. Современные технологии позволяют создать доверенную среду КИИ более простым, экономным способом, а главное – более надежным.

Риски системы граничных вычислений КИИ можно разделить на две категории – внешний нарушитель и внутренний нарушитель.

Принципиальной задачей является формирование криптосредств для защиты каналов связи и всей системы граничных вычислений в целом. Эту задачу можно разбить на несколько подзадач, решить которые предстоит государству, отраслям и индустрии ИТ.

Чтобы стать полноценными криптосредствами КИИ, контроллеры должны удовлетворять ряду требований: быть российского производства, климатически- и вандалоустойчивыми, обладать длительным жизненным циклом, достаточной вычислительной мощностью и реализовывать функции шифрования каналов связи в соответствии с сертификационными требованиями регулятора, в частности, реализовать ГОСТ-ированные алгоритмы шифрования типа «Магма» или «Кузнечик».

Устройство, в которое имплементирована функциональность крипто, приобретает статус криптосредства. Работа с криптосредствами – лицензируемый вид деятельности на территории Российской Федерации. Такая лицензия требуется организациям и специалистам, которые эти средства производят, эксплуатируют и ремонтируют. Однако до сего дня организации ТЭК, транспорта и других отраслей реального сектора не работали с криптосредствами, потому они

не имеют соответствующих лицензий и в их штате нет сертифицированных специалистов. Возникает гигантская проблема нехватки специализированных профессиональных кадров, которые могли бы с этими средствами работать. Ее решение предполагает глубокие внутренние изменения отраслей. Новый вид деятельности требует от организаций колоссальных затрат, формирования пула новых устройств, увеличения штатов, как следствие – повышения тарифов и отпускных цен.

Другая задача – налаживание массового производства устройств со встроенными криптосредствами в России, поскольку контур их функционирования должен быть доверенным. Кроме того, криптосредства должны быть недорогими и устойчивыми к российскому климату. Наша промышленность пока не готова к массовому производству криптосредств, но прототипы контроллерных чипов на процессорах ARMv7 и ARMv8 уже созданы, например производственным объединением «Микрон». Компания «Миландр» и ряд других российских предприятий начали производить подобного рода чипы, а также счетчики и контроллеры их основе. Но в отсутствие массового спроса производство пока ограничивается небольшими партиями под заказ. Ситуация может измениться, когда появятся процессоры на архитектуре RISC-V. Это открытая архитектура, которую развивает международный академический проект. В нем принимают активное участие и российские разработчики, которые работают над созданием устройств на процессорах RISC-V. «Микрон» уже анонсировал производство устройств с процессором RISC-V и производительной операционной системой. Правда, пока это ОС на основе Debian и к степени ее доверенности есть вопросы. При наличии ОС, созданной на основе российского репозитория, в устройства «Микрона» можно интегрировать средства криптографической защиты, обеспечив таким образом высокий уровень доверия системы, достаточный для передачи данных по беспроводным каналам связи. Надо отметить, что процессоры RISC-V – дело будущего, сегодня доминирующей в этом сегменте остается архитектура ARMv7.

Еще одна задача – разработка средств, способов и методики интеграции новой инфраструктуры с унаследованной. Проблемы с «взаимопониманием» систем могут привести к сбоям в работе объектов КИИ.

Регуляторам предстоит разработать нормативную базу, побуждающую владельцев КИИ и частных пользователей выполнить планомерную замену старых устройств новыми. При этом затраты потребителей на приобретение интеллектуальных приборов учета и их оперативное включение в информационные системы должны быть минимальными.

Любая криптографическая система основана на использовании криптографических ключей. Для новой инфраструктуры граничных вычислений необходимо создать центр управления ключами шифрования (ЦУК). Управление ключами играет важнейшую роль в обеспечении конфиденциальности обмена информацией между устройствами первого и второго уровней системы граничных вычислений КИИ. Новые конечные устройства первого уровня будут передавать зашифрованные данные на второй уровень – на интеллектуальные контроллеры. Здесь появятся дополнительная наложенная криптоструктура – ЦУК и криптошлюз, через которые будут «ходить» данные. На этом уровне будут выполняться их расшифровка и первичная обработка, а затем чистые данные отправятся на третий уровень, в центр анализа информации.

Если какое-либо устройство первого уровня вскрыто или повреждено, сигнал поступает в Центр управления ключами. Он реагирует мгновенно: присваивает этому объекту статус скомпрометированного и навсегда исключает ключевую пару из списка доверенных. По такой схеме сегодня работает российский информационно-вычислительный программно-аппаратный комплекс «Пирамида», предназначенный для контроля и учета энергопотребления. С помощью ИВК его верхний контур реализован на доверенной платформе – российских компьютерах «Эльбрус» с сертифицированной ОС «Альт 8 СП».

Однако здесь возникает серьезная проблема: для миллионов устройств потребуются миллионы ключей. Одной только компании «Россети» будет необходимо порядка 100 млн штук. Соответственно в случае строго централизованной архитектуры системы в целом длина уникального ключа должна быть внушительной, а объем – около 2 Мб. Это резко увеличивает 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. Значит, реализация задач Индустрии 4.0 на существующих вычислителях возможна лишь в виде граничных вычислений. Она не централизуется в связи с требованием обеспечения доверенной среды криптографическими средствами.

Готовность рынка и ближайшие перспективы

Приходится признать, что у индустрии ИТ пока нет комплексных решений для построения защищенных информационно-измерительных систем. Но они будут формироваться по мере решения перечисленных выше задач. В частности, компания ИВК сотрудничает с регуляторами в подготовке предложений для реализации средств криптографической защиты систем граничных вычислений КИИ, для создания ключей с длительными сроками хранения, для простой имплементации средств криптографической защиты в текущую инфраструктуру, для применения уже существующих сертифицированных решений (в том числе разработок компании) для работы с новой инфраструктурой. ■