Марина СОРОКИНА:

«Без встроенной криптографии невозможно обеспечить информационную безопасность устройств автоматизации»

Перечень отраслей, в которых сохраняется повышенный спрос на продукты ИБ для объектов критической информационной инфраструктуры, расширяется. Сегодня это не только электроэнергетика, нефтегазовая, металлургическая и транспортная отрасли, но и сельскохозяйственное производство, коммунальные службы, проектирование сложных проектов. Создание индустриальных средств защиты информации – одно из приоритетных направлений деятельности компании «ИнфоТеКС», которая принимала участие в разработке криптографического протокола для промышленных систем. О тенденциях в сегменте ИБ, преимуществах новых решений, направлениях их развития рассказала руководитель продуктового направления компании «ИнфоТеКС» Марина Сорокина.

– Как вы оцениваете востребованность решений для защиты информации на промышленных предприятиях в динамике последних лет? Как развивается отрасль индустриальной кибербезопасности в целом, и как меняется спрос на продукты «ИнфоТеКС»?

– Этот год только начался, поэтому давать оценку сложно, но в целом тенденции на рынке информационной безопасности (ИБ) в прошлые годы были схожи, и я не вижу никаких причин для их изменения в ближайшем будущем. Спрос на решения по защите информации для промышленных предприятий сохраняется на высоком уровне. При этом на фоне повышенного спроса на продукты ИБ для объектов критической информационной инфраструктуры (КИИ) в электроэнергетике, нефтегазовой, металлургической и транспортной отраслях в прошлом году было реализовано много проектов в сферах, которые не относятся к КИИ напрямую, например, в сельском и коммунальном хозяйствах, для проекта «умный город». Кроме того, вырос спрос и на защиту IIoT-систем. Это связано с появлением требований по защите внедряемых технологий от владельцев предприятий. Запросы по использованию средств криптографической защиты информации (СКЗИ) в интеллектуальных системах учета электроэнергии (ИСУЭ) также продолжают быть актуальными. Все это в совокупности привело к трехкратному росту спроса на продукты «ИнфоТеКС».

– Что нового «ИнфоТеКС» может предложить промышленным предприятиям?

– Разработка индустриальных средств защиты информации является одним из приоритетных направлений деятельности компании «ИнфоТеКС». Продукты данного направления условно разделены в нашем портфолио на две категории: встраиваемые и наложенные СКЗИ.

Мы активно развиваем решение ViPNet SIES – комплекс встраиваемых СКЗИ для защиты систем IIoT и АСУ. В перечень продуктов решений ViPNet SIES входят, в частности, программно-аппаратный комплекс ViPNet SIES Core, который является СКЗИ, обеспечивающим выполнение криптографических операций для программируемых логических контроллеров (ПЛК) и устройств сбора и передачи данных (УСПД), и ViPNet SIES Core Nano – СКЗИ, реализованное в виде миниатюрного чипа, для установки в датчики и прочие IIoT-устройства. Благодаря использованию протокола CRISP наши средства защиты не вносят существенных задержек в систему, стабильно работают

на плохих каналах и практически не создают дополнительную нагрузку на сети связи. Продукты ViPNet SIES также обеспечивают эффективную защиту данных в ИСУЭ. По нашим оценкам, уже в 2024 г. в ИСУЭ должно быть установлено порядка 10 тыс. устройств с такими СКЗИ.

Большое внимание в прошлом году мы уделили тематическим исследованиям крипточипа ViPNet SIES Core Nano, добавили ему функциональности. Появилась возможность создавать временные связи на краткосрочных ключах для защиты данных между двумя устройствами, что обеспечило востребованный сценарий их обслуживания. Появилась возможность защиты данных, передаваемых от одного отправителя нескольким получателям одновременно, таким образом мы обеспечили «групповые коммуникации».

Продолжаем активно работать над созданием продуктов, сопровождающих настройку и эксплуатацию крипточипа ViPNet SIES Nano: выпустили первую версию АРМ первичной настройки ViPNet SIES Nano Loader, в прошлом году на свет появилась первая версия ключевого центра ViPNet SIES HSM для генерации ключей со сроком жизни до 16 лет, в ближайшие месяцы появится центр управления ViPNet SIES MC, который сможет работать не только с SIES Core Nano, но и с любым другим крипточипом, работающим по протоколу CRISP.

Мы активно развиваем решение ViPNet SIES – комплекс встраиваемых СКЗИ для защиты систем IIoT и АСУ.

Если говорить про наложенные средства защиты, наши шлюзы безопасности, то в прошлом году появилось два новых исполнения ViPNet Coordinator IG100 I4 с производительностью до 160 Мбит/с, работающих на оптических каналах связи, и выпущенный в конце 2023 г. шлюз безопасности нового, пятого, поколения – ViPNet Coordinator IG100 I5 с производительностью до 55 Мбит/с и поддерживающий технологию PoE. Именно это поколение шлюзов безопасности мы будем развивать в ближайшие годы.

В прошлом году появилось два новых исполнения ViPNet Coordinator IG100 I4 с производительностью до 160 Мбит/с, работающих на оптических каналах связи.

– «ИнфоТеКС» является одним из ведущих вендоров по разработке встраиваемых СКЗИ для промышленности. Расскажите про реализованные проекты и планы на 2024 г.

– Учитывая особенности архитектуры систем промышленной автоматизации и предъявляемых к ним требований, защищать каждое устройство системы наложенными средствами защиты нецелесообразно: это затратно, долго и сложно в обслуживании. Установить межсетевые экраны и криптошлюзы на всем периметре инфраструктуры для каждого устройства невозможно. Здесь целесообразно использовать только встраиваемые СКЗИ: решение масштабируется вне зависимости от количества устройств и территориального распределения, для каждого типа устройств устанавливаются специализированные СКЗИ. Мы считаем, что без встроенной криптографии невозможно обеспечить информационную безопасность устройств автоматизации, поэтому активно развиваем решение ViPNet SIES.

Сейчас на рынке много проектов, прежде всего нацеленных на защиту IIoT. Один их самых популярных запросов – защита IIoT-систем с использованием протокола LoRaWAN. Мы работаем со всеми российскими крупными разработчиками оконечных устройств и шлюзов, применяющих технологию LoRaWAN. За последний год реализовали несколько пилотных проектов в нефтегазовой отрасли и электроэнергетике, где данные при передаче по LoRaWAN защищаются с помощью СКЗИ ИнфоТеКС – криптомодуля ViPNet SIES Core и крипточипа ViPNet SIES Core Nano.

Самым масштабным можно считать совместный проект с НТЦ «Нартис». В прошлом году мы завершили интеграцию СКЗИ ViPNet SIES Core в коммуникационный шлюз CG-ZB-02, который стал первым шлюзом с интегрированным средством криптографической защиты информации на рынке компонентов ИСУЭ. Коммуникационные шлюзы выполняют роль устройств сбора и передачи данных (УСПД) в ИСУЭ и используются для передачи показателей приборов учета с помощью беспроводной технологии ZigBee в информационно-вычислительные

комплексы (ИВК). В качестве СКЗИ для коммуникационных шлюзов НТЦ «Нартис» был выбран программно-аппаратный комплекс ViPNet SIES Core. Сегодня это единственный в России сертифицированный СКЗИ для встраивания в компоненты ИСУЭ на уровне УСПД, обладающий возможностью эксплуатации вне контролируемой зоны. Плодотворное сотрудничество лидеров рынка, которые не боятся первыми предлагать заказчику решения в такой сложной отрасли, позволяет российской электроэнергетике развиваться в соответствии с потребностями времени и выполнять предъявляемые требования.

– Какие факторы мешают применению встраиваемых средств защиты информации?

– Основная проблема связана с нехваткой компетенций. Профильный инженерный состав с соответствующим образованием в области АСУ плохо разбирается в вопросах ИБ и применении криптографических средств для защиты своих систем. И, к сожалению, инженеров до сих пор практически не учат основам ИБ, никто не рассказывает им, как защищать тот или иной промышленный протокол, какие сценарии нужны устройству, чтобы оно устойчиво работало в современной системе. Этому учат в той или иной мере специалистов по информационной безопасности, но они не понимают, как работает то или иное устройство автоматизации со своей логикой. Понимая эту проблему, мы пришли к мысли о необходимости учить кибербезопасности и криптографии отраслевых инженеров и делать это на тех учебных площадках, где они проходят базовую подготовку, т. е. в отраслевых вузах.

В ходе работы над проектом по защите электроэнергетики мы договорились с НИУ «МЭИ» о возможности организации на базе кафедры релейной защиты и автоматизации энергосистем специализированной фирменной лаборатории «ИнфоТеКС». Там мы сможем учить молодых инженеров грамотно и правильно применять наши промышленные решения, криптографические модули ViPNet SIES непосредственно в элементах автоматики, которые используются в построении систем электроэнергетики. На учебных комплексах смогут проходить практику не только студенты университета, но и действующие инженеры в рамках курсов повышения квалификации. Для нас важно, чтобы у работников отрасли, которые отвечают за безопасность конечных объектов, была практическая возможность протестировать наши решения и научиться применять их в своей деятельности.

Мы считаем, что практику взаимодействия с НИУ «МЭИ» необходимо транслировать на другие отраслевые площадки. Так, у нас есть положительный опыт организации похожей лаборатории в ТУСУР, где ведется подготовка в первую очередь инженерного состава для решения задач автоматизации разных отраслей экономики.

> Программно-аппаратный комплекс ViPNet SIES Core – сегодня единственный в России сертифицированный СКЗИ для встраивания в компоненты ИСУЭ на уровне УСПД.

– Одним из главных событий рынка ИБ АСУ ТП в последние месяцы стала стандартизация криптографического протокола для промышленных систем. Компания «ИнфоТеКС» принимала непосредственное участие в его разработке. Расскажите об этом.

– Протокол защищенного обмена для индустриальных систем был утвержден в феврале текущего года, и компания «ИнфоТеКС» выступила здесь в качестве разработчика первого национального стандарта РФ, описывающего криптографический протокол.

CRISP (CRyptographic Industrial Security Protocol) – неинтерактивный протокол защищенной передачи данных, разработанный для применения в индустриальных системах. Разработка данного протокола велась специально для индустриальных систем, чтобы обеспечить передачу компактных блоков промышленных данных и отказаться от достаточно высоких требований к вычислительным мощностям и каналам связи, которые предъявляются при использовании протоколов на основе CMS-сообщений (Cryptograghic Message Syntax).

Свойства протокола CRISP позволяют с его помощью защищать данные, передаваемые как в TCP/IP-сетях, так и в сетях, построенных не на основе стека протоколов TCP/IP, например, при использовании технологий узкополосной передачи LPWAN. Применять новый национальный стандарт можно в качестве слоя защиты для протокола LoRaWAN RU, NB-IoT, ZigBee, XNB, а также для ряда промышленных протоколов. Высокая энергоэффективность позволяет использовать криптографический протокол не только в АСУ ТП, но и в IIoT-системах, где устройства традиционно имеют питание от батарейки или получают его из среды функционирования. Мы используем криптографический протокол CRISP в продуктах решения ViPNet SIES. ■