ПАК «Звезда»

Программно-аппаратный комплекс «Звезда» – разработка НИИМЭ для криптографической защиты информации в Интернете вещей.

Интернет вещей объединяет множество ***конечных*** ***устройств*** различного назначения и обеспечивает их взаимодействие с ***серверами приложений***. Конечные устройства условно делятся на ***датчики***, собирающие и передающие на сервер определенную информацию, и ***актуаторы***, которые выполняют определенные действия согласно предписаниям сервера. Нередко одно конечное устройство совмещает в себе функции датчика и актуатора. Несколько конечных устройств могут быть объединены в группу под управлением контроллера, отвечающего за взаимодействие с сервером. Интернет вещей характерен высокой плотностью конечных устройств и малым объемом передаваемой информации.

На сегодняшний день Интернет вещей – одна из наиболее быстро развивающихся отраслей информационных технологий. По мере проникновения Интернета вещей в различные, порой весьма чувствительные сферы деятельности человека становится очевидной важность защиты передаваемой информации, то есть обеспечение ее целостности, конфиденциальности и аутентичности. Оптимальным решением является организация виртуального защищенного канала передачи данных между конечным устройством и сервером приложений. ПАК «Звезда» разрабатывался с целью решения этой задачи наиболее удобным для практического применения способом. ПАК «Звезда» отличается следующими особенностями:

* Использует компактный протокол защиты передаваемых данных CRISP, специально разработанный для Интернета вещей и стандартизованный в России в 2019 году. Этот протокол устойчив к сбоям, не требует предварительной установки защищенной сессии, все сообщения CRISP являются самодостаточными.
* Применяет российские криптографические алгоритмы последнего поколения, в том числе блочный алгоритм ГОСТ Р34.12-2015 «Магма», алгоритмы вывода сеансовых ключей, криптоконверты для передачи криптографических ключей, алгоритмы выработки и проверки электронной подписи.
* Обеспечивает удаленное управление ключевой информацией, что позволяет не демонтировать устройства для регламентной замены криптографических ключей.
* Подписывает сообщения полноценной электронной подписью, что позволяет конечному пользователю (провайдеру приложения) проверять целостность и подлинность любых, в том числе архивных сообщений, без какой-либо зависимости от провайдера связи и самого ПАК «Звезда».
* Имеет модульную структуру и легко интегрируется как в конечные устройства, так и в серверную инфраструктуру.

ПАК «Звезда» состоит из микросхемы, интегрируемой в конечные устройства, и криптографического сервера, обеспечивающего защиту канала обмена с конечными устройствами и управление криптографическими ключами.

Микросхема была специально разработана и выпущена для данного проекта. Она представляет собой защищенный микроконтроллер для смарт-карт MIK51BC16D с операционной системой Trust 3.30i и интегрированными приложениями «Элемент безопасности конечного устройства (ЭБ)» и «Элемент безопасности криптосервера (ЭБКС)». Микросхема может поставляться в корпусе LGA-40, в виде смарт-карты или СИМ-карты.

Рисунок 1. Структурная схема ПАК «Звезда»

Конечное устройство

**ПАК Звезда**

Радиомодуль

ЭБ

Контроллер

Радиомодем

датчики, актуаторы, управляющий контроллер

Радио-система

АРМ управления криптосервисом

Серверы приложений

Криптосервис

виртуальный защищенный канал

**HSM**

ЭБКС

ЭБКС

ЭБКС

ЭБКС

розовым цветом выделены компоненты криптосервера

оранжевым цветом выделены микросхемы

***Криптосервис*** – программа на сервере, которая подключена между радио-системой провайдера связи и серверами приложений. Он является основным серверным компонентом ПАК «Звезда». Криптосервис взаимодействует с модулем безопасности (HSM) и АРМ-ом управления криптосервисом.

***Автоматизированное рабочее место (АРМ) управления криптосервисом*** – программа с пользовательским интерфейсом, обеспечивающая выполнение всех необходимых для работы криптосервиса процедур настройки, управления и мониторинга.

***HSM*** – аппаратный модуль безопасности, выполняющий роль средства криптографической защиты информации (СКЗИ). HSM представляет собой плату расширения с интерфейсом PCI, на которой установлено несколько микросхем ЭБКС, совместно образующих вычислительный кластер. Число ЭБКС в кластере необходимо выбирать в зависимости от требуемого уровня производительности.

***Элемент безопасности*** (ЭБ) устанавливается в конечное устройство и подключается по стандартному последовательному интерфейсу ISO 7816-3. ЭБ обеспечивает:

* защищенный канал обмена с сервером;
* формирование электронной подписи передаваемых данных;
* поддержку удаленного управления криптографическими ключами.

Помимо основной функции обеспечения защищенного канала передачи данных, ПАК «Звезда» предоставляет ряд важных дополнительных возможностей:

* удаленное управление криптографическими ключами на конечных устройствах;
* выработка электронной подписи сообщений конечными устройствами;
* выработка электронной подписи сообщений криптосервисом;
* обеспечение отказоустйчивости криптосервиса;
* функции удостоверяющего центра по отношению к обслуживаемым конечным устройствам;
* развитые функции мониторинга состояния криптосервиса.

ПАК поддерживает современные криптографические алгоритмы ГОСТ Р34.10-12, ГОСТ Р34.11-12, ГОСТ Р34.12-15, ГОСТ Р34.13-15. Управление ключами осуществляется наиболее безопасным методом – с использованием инфраструктуры открытых ключей. ПАК «Звезда» отвечает требованиям, предъявляемым к СКЗИ класса KC3 и способен обслуживать критическую инфраструктуру. На стороне конечного устройства используется российская микросхема первого уровня, т.е. разработанная и произведенная в России.

В сотрудничестве с партнерами НИИМЭ предлагает решение для беспроводных сетей на основе технологии NB IoT. В этом случае, ЭБ интегрируется с радиомодемом. Возможна интеграция ПАК «Звезда» в другие типы беспроводных и проводных сетей.

На стендовых испытаниях криптосервис с кластером из 8 ЭБКС обеспечил обработку свыше 10 млн операций в сутки при эмуляции работы тестовой сети из 10 тыс. конечных устройств.

Криптосервис и встроенная операционная система Trust 3.30i, используемая в ЭБ и ЭБКС, зарегистрированы в Роспатенте (№2021610059 от 11.01.2021 и №2021611726 от 04.02.2021 соответственно). Первая инсталляция ПАК «Звезда» состоялась в компании МТС. Это бы первый случай, когда АО «НИИМЭ» лицензировала свое серверное программное обеспечение.