DOI: 10.22184/1992-4178.2021.202.1.116.129

Интегрированные технологии информационной безопасности в СнК «Скиф» для мобильных и встраиваемых систем

Я. Петричкович, д. т. н.[1], Д. Кузнецов[1], С. Корольков[1], А. Иванников[1], И. Аликберов[2], Т. Солохина, к. т. н.[1], Л. Меньшенин[1]

УДК 004.318 | ВАК 05.27.01

В АО НПЦ «ЭЛВИС» разработана 11-ядерная гетерогенная система на кристалле «Скиф» (1892ВА018), предназначенная для построения мобильных и встраиваемых интеллектуальных систем для связных, телекоммуникационных, навигационных, мультимедийных приложений, мультисенсорной обработки сигналов, робототехнических систем, планшетов, умных камер, систем мониторинга – там, где требуется сложная обработка информации в условиях ограниченного энергопотребления и обеспечения доверенности. В статье рассмотрены ключевые особенности интегрированной технологии информационной безопасности и обеспечения доверенности, реализованной как в отдельной СнК «Скиф», так и в составе единой отечественной технологической платформы, предлагаемой НПЦ «ЭЛВИС».

Мобильные и встраиваемые устройства стали важной частью нашей повседневной жизни – они используются для хранения персональных данных, банковской информации, доступа к различным услугам и сервисам, а также обеспечения граничных вычислений (edge computing), то есть организации локальных вычислений в непосредственной близости к сенсорам, включая расчет навигационных координат. При этом существенно вырос риск реализации угроз информационной безопасности, в связи с чем на передний план выходит задача обеспечения защиты данных и конфиденциальности в устройствах и различных системах, в частности системах критической информационной инфраструктуры (КИИ).

«Для обеспечения КИИ отечественными доверенными решениями объективных препятствий нет», – отмечал президент Ассоциации разработчиков компьютерных технологий доверия и безопасности «Доверенная платформа» А. И. Тихонов [1]. АО НПЦ «ЭЛВИС» совместно с партнерами участвует в создании отечественных доверенных платформ, предлагая для российского рынка три новые линейки микросхем, каждая со своей экосистемой (комплект СнК «Элиот», «Скиф» и «Рободеус»), как единую технологическую платформу управления жизненным циклом систем КИИ [2, 3, 4].

[1] АО НПЦ «ЭЛВИС».

[2] ООО «ТрастЛаб».

КЛЮЧЕВЫЕ ОСОБЕННОСТИ СнК «СКИФ»

Гетерогенная СнК «Скиф» (1892ВА018), разработанная в дизайн-центре АО НПЦ «ЭЛВИС» по проектным нормам 28 нм, предназначена для широкого круга мобильных и встраиваемых приложений, в том числе для применения в системах критической информационной инфраструктуры (КИИ) [1]. Решение этих задач существенно усложняется из-за жестких требований к СнК – обеспечения ограниченного управляемого энергопотребления при широком наборе выполняемых функций, доверенности и защиты обработки информации.

В СнК «Скиф» реализована архитектура, которая поддерживает:

- мультимедийные возможности;
- встроенную навигацию;
- связные приложения на базе технологии программно-определяемого радио (SDR);
- цифровую обработку сигналов (DSP);
- искусственный интеллект (ИИ);
- развитую экосистему ПО;
- встроенную систему безопасности.

В АО НПЦ «ЭЛВИС» вместе с партнерами создана многоуровневая архитектура безопасности СнК «Скиф», учитывающая современные мировые и отечественные стандарты в области обеспечения безопасности и основанная на концепции безопасной среды исполнения (Trusted Execution Environment, TEE) консорциума Global Platform.

Система безопасности СнК обеспечивает высокий уровень защищенности и доверия ко всему устройству за счет использования встроенных аппаратных средств и программных сервисов безопасности, изолированных от ПО пользователя.

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ АППАРАТНОЙ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ

Мобильные устройства находят все более широкое применение в таких областях, как здравоохранение, развлечения, социальные медиа, банковские платежи, защита мультимедийного контента (DRM) и системы цифровой передачи контента. Все эти приложения работают с чувствительными и персональными данными, что требует обеспечения высоких уровней безопасности и конфиденциальности устройств в целом.

Для обеспечения защищенных мобильных вычислений мировыми консорциумами и технологическими гигантами был предложен ряд программно-аппаратных решений, таких как Secure Element (SE), Trusted Platform Module (TPM), Trusted Execution Environment (TEE). Все эти решения представляют собой реализацию интегрированной платформы аппаратной безопасности, обеспечивающей гарантии целостности, доступности и конфиденциальности исполняемых приложений и ассоциированных с ними данных, а также обладают устойчивостью к различным атакам на ПО.

Проблема защиты отечественного информационного пространства и объектов критической инфраструктуры от внешнего воздействия – важнейшая задача для обеспечения независимости страны. Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Постановление Правительства РФ от 10 июля 2019 года № 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и Приказ ФСТЭК России № 76 от 2 июня 2020 года «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к СТЗИ и СОБИТ» способствуют выполнению данной задачи на территории России.

Smart Card

Одним из наиболее известных решений по обеспечению информационной безопасности является Smart Card – компактная карта со встроенной микросхемой, предназначенной для аутентификации пользователей, хранения ключевой информации и проведения криптографических операций в изолированной защищенной среде. Карты появились еще в 1983 году и сегодня используются в широком спектре приложений – от идентификатора абонента сети связи и удостоверения личности до платежного банковского средства. Условно можно выделить два типа карт – контактные (с интерфейсом ISO 7816) и бесконтактные (в соответствии со стандартом ISO / IEC 14443). По функциональности карты можно разделить на карты памяти (содержат некоторое количество данных и механизм разграничения доступа к ним) и интеллектуальные карты (содержат микропроцессор и возможность управлять данными на карте).

Типичная Smart Card содержит 8 / 16 / 32-битный микроконтроллер, постоянную память, или ROM (объемом до 32 Кбайт), для хранения встроенного программного обеспечения, память EEPROM для постоянного хранения данных с возможностью записи, оперативную память RAM для временного хранения данных. Кроме того, карты оснащены ресурсами для выполнения криптографических операций (поточного и блочного шифрования, подписи, хэширования, выработки ключевой информации).

Ряд смарт-карт для ответственных областей применения обладают высокой стойкостью ко взлому, в том числе с использованием физических каналов атак.

Другим распространенным решением является стандарт Secure Element (SE), разработанный Global Platform. По функционалу данное решение имеет много общего со Smart Card, обладает высокой стойкостью ко взлому и включает в свой состав микроконтроллер, память ROM, RAM, EPPROM, а также криптографический сопроцессор. Распространены три формата исполнения: UICC – всем привычная SIM-карта, eSE – встроенное решение и решение в виде карты SD. Основные применения – платежные системы (интеграция с NFC), системы биометрической идентификации и в качестве встроенного корня безопасности.

Для расширения функционала SE и обеспечения совместимости ПО был разработан стандарт Java Card, который позволяет одновременно устанавливать на карту и исполнять набор приложений (applet), написанных на подмножестве языка Java. Основными компонентами платформы Java Card являются (рис. 1):

- виртуальная машина, интерпретирующая байт-код приложений и выполняющая его верификацию;
- набор программных интерфейсов, реализующих взаимодействие между приложениями и ресурсами микросхемы, такие как криптографические операции или работа с хранилищем;
- среда исполнения JCRE;
- аппаратная изоляция (Firewall) между приложениями и средой исполнения.

Внедрение Java Card позволило обеспечить гибкость и внедрить процесс управления приложениями (Application Provisioning). Состав ПО, исполняемого на карте, определяется не только компанией-изготовителем карты, но также может задаваться в процессе персонализации под

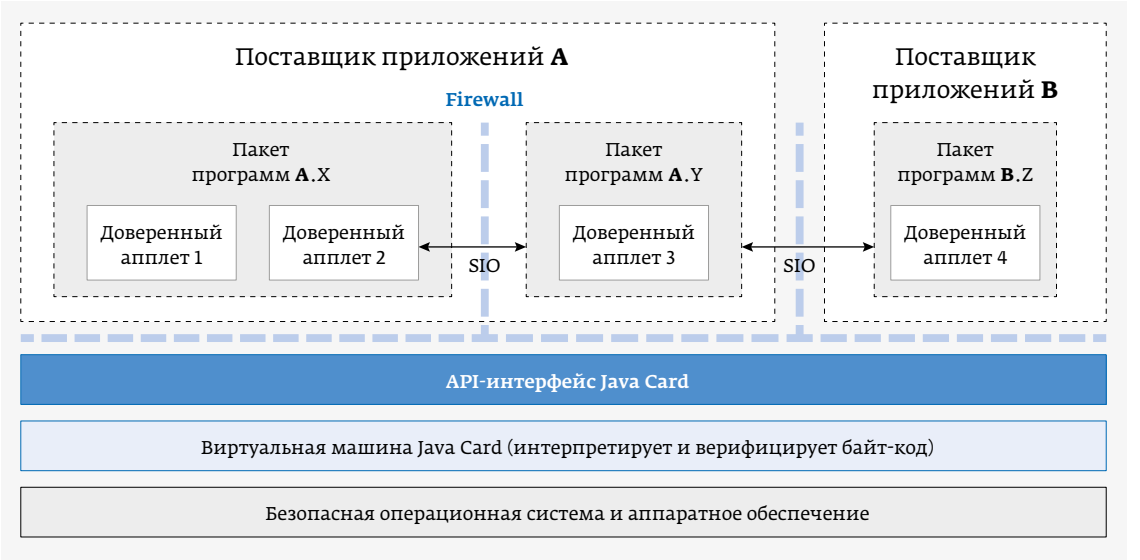

Рис. 1. Архитектура Java Card

продавца, выпускающего карту (Issuer Centric Smart Card Owner Model, ICOM), или управляться конечным потребителем (User Centric Smart Card Owner Model, UCOM).

Модель ICOM позволяет выпускающему карту полностью контролировать ее программное обеспечение – устанавливать, удалять, управлять настройками, предустанавливать приложения. Ресурсы карты не разделяются между разными поставщиками приложений и недоступны пользователю.

Преимущества модели ICOM:

- карта полностью контролируется выпускающей стороной; выпускающая сторона полностью управляет жизненным циклом изделия;
- централизованное управление позволяет получить высокий уровень безопасности;
- пользователь никак не может повлиять на набор приложений, что обеспечивает стабильность контролируемого окружения;
- протоколы обмена полностью задаются выпускающей стороной.

Но данная модель имеет и ряд недостатков – одну смарт-карту нельзя использовать для разных сервисов, любое обновление требует обращения к выпускающей стороне, что существенно усложняет расширение сервисов. Для решения данной проблемы была предложена модель UCOM, в рамках которой пользователи управляют набором приложений и сервисов, запрашивая их у провайдеров.

Дальнейшим развитием SE стало появление технологии Host-based Card Emulation (HCE), позволяющей эмулировать карту на процессоре без необходимости использования дискретного элемента. Операционная система выполняет эмуляцию элемента безопасности, обеспечивая протокол обмена, но при этом не обладая нужной степенью безопасности. Ключевая информация обрабатывается программно на той же платформе, что и прочие пользовательские приложения, что существенно повышает вероятность осуществления успешной атаки. Поэтому данное решение не рекомендуется использовать для приложений, чувствительных к безопасности, таких как банковские платежи.

Доверенный платформенный модуль (Trusted Platform Module, TPM)

Если смарт-карты и микросхемы SE решали проблему безопасности мобильных устройств, то в качестве одного из наиболее успешных подходов для обеспечения безопасности персональных компьютеров следует отметить стандарт Trusted Platform Module (TPM), созданный в рамках консорциума Trusted Computing Group, объединившего таких ведущих мировых производителей, как Intel, AMD, IBM, Microsoft и др. Модуль TPM является устойчивым ко взлому отдельным процессором безопасности, выполняющим криптографические операции со своим уникальным ключом-идентификатором. Одно из основных применений TPM – реализация корня безопасности (Root of Trust, RoT), повышающего уровень контроля за поведением системы и невозможности запуска неавторизованного ПО.

TPM обеспечивает процедуру измеряемой загрузки системы (Measured Boot). В начале загрузки системы выполняется процесс расчета контрольных сумм и проверка цифровых подписей всех загружаемых модулей. Рассчитанные контрольные суммы сохраняются в модуле TPM в специальных регистрах конфигурации платформы (PCR) (рис. 2). Далее предусмотрена процедура проверки соответствия контрольных сумм ожидаемым посредством удаленной аттестации. Рассчитанные значения в криптографически защищенном виде передаются на удаленный сервер, который удостоверяет целостность (Remote Attestation).

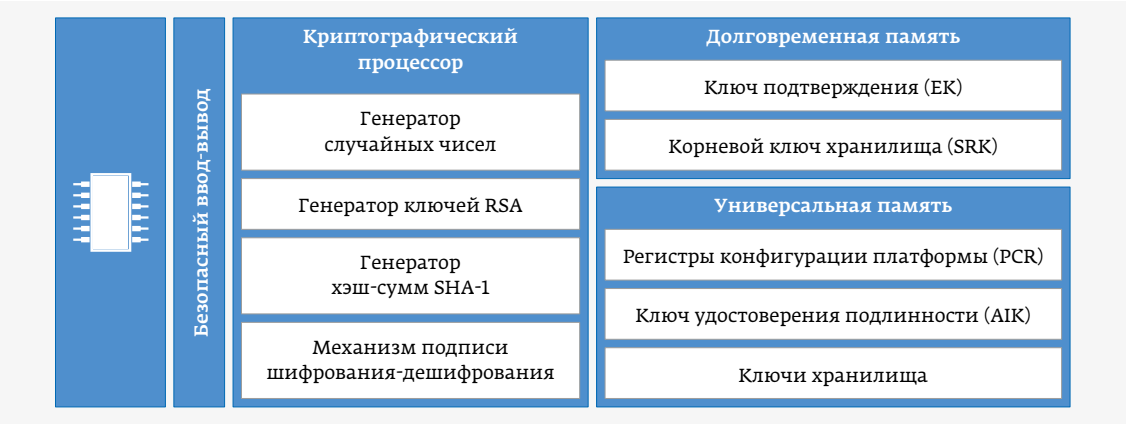

Рис. 2. Ключевые компоненты TPM

Две другие функции (Binding и Sealing) позволяют реализовать доверенное хранилище. Процедура Binding обеспечивает формирование ключевой пары на основе уникального корневого ключа доверенного хранилища (Storage Root Key). Процедура Sealing дополнительно обеспечивает привязку к конфигурации платформы на основе значения регистров PCR. Это препятствует возможности расшифровать контент на другой машине или в скомпрометированном окружении.

Вторая версия стандарта TPM допускает пять различных вариантов реализаций:

- отдельная микросхема – обычно обеспечивает максимальную безопасность;
- часть большой микросхемы – обычно имеет меньшую устойчивость к атакам по физическим каналам;
- программная реализация, исполняемая в защищенном окружении общего процессора (TEE);
- программная реализация, исполняемая в режиме гипервизора на процессоре общего назначения;
- программная эмуляция без механизма защиты и изоляции – наименьший уровень безопасности.

Безопасная среда исполнения (Trusted Execution Environment, TEE)

Есть целая группа подходов, реализующих функции безопасности посредством разделения общих аппаратных ресурсов и работающих параллельно с основной операционной системой. TEE включает два ключевых механизма – аппаратную изоляцию доверенных приложений от недоверенных приложений и функционал доверенного хранилища ключевой информации. Так как операции осуществляются на процессоре общего назначения, то обычно в защищенном режиме объем ресурсов памяти и производительность много выше, чем возможности микроконтроллера смарт-карты или выделенного процессора безопасности TPM.

Кроме стандартизованной реализации Global Platform TEE имеется ряд подобных решений, разработанных ранее компаниями – участниками рынка.

Решение Intel Trusted eXecution Technology (TXT) – это набор аппаратных расширений для процессоров и чипсетов Intel с возможностями безопасности, такими как измеряемая загрузка и защищенное выполнение. Решение полагается на аппаратный RoT, совместимый с TPM. Технология Intel предоставляет аппаратные механизмы, которые помогают защититься от программных атак и защищают конфиденциальность и целостность данных, хранящихся или созданных на компьютере.

Аналогичная технология от AMD – Secure Virtual Machine – также позволяет обеспечить защиту и дополнительно очистку памяти после завершения операций.

Данные технологии ориентированы на предоставление функций безопасности для виртуальных машин и применяются на рынке серверов и облачных вычислений.

Одной из первых реализаций технологии TEE для мобильных устройств стало решение M-Shield от компании Texas Instruments. Решение основано на концепции SE и дополнительно включает выделенные аппаратные средства ввода-вывода, крипто-DMA, а также процессор безопасности (Secure State Machine), выполняющий мониторинг и применение политик безопасности и предотвращающий попытки несанкционированного доступа и несанкционированной активности. Впоследствии TI отказалось от этой технологии и адаптировало ARM TrustZone.

Технология ARM TrustZone представляет собой набор ресурсов для реализации TEE на платформе ARM (рис. 3). В ее основе лежит понятие безопасного и небезопасного мира. Состояние безопасного мира определяется выделенным битом NS, который влияет на все ресурсы микросхемы – атрибуты транзакций на шине, значение линеек кэш-памяти и др., что позволяет гарантированно обеспечить разделение доступа к ресурсам памяти, отладочному функционалу и портам ввода-вывода, а также определяется выделенным режимом работы процессорного ядра – monitor mode.

При этом ARM TrustZone не включает в себя все компоненты, которые требуются для реализации безопасности;

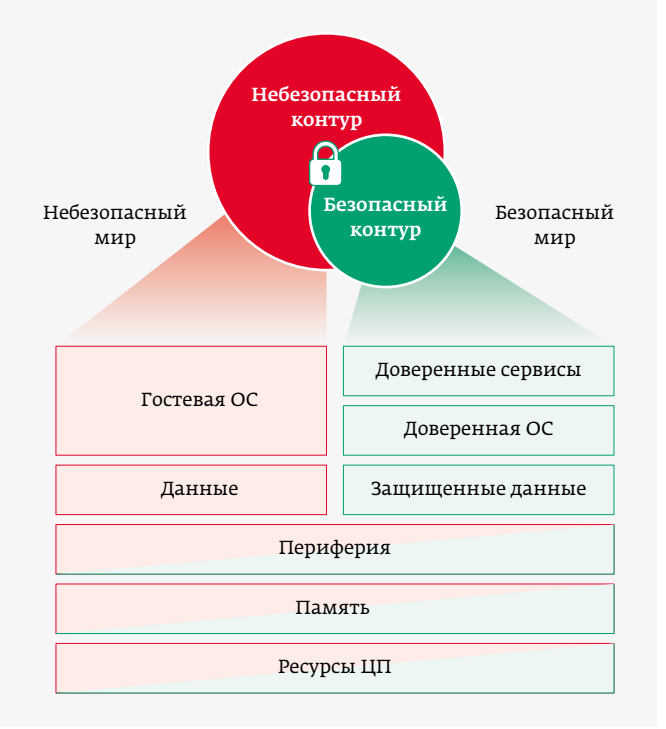

Рис. 3. Технология ARM TrustZone

необходима реализация процедуры доверенной загрузки и начальной инициализации монитора безопасности.

В качестве примеров реализации можно отметить AMD Secure Processor и Samsung KNOX.

AMD Secure Processor представляет собой решение на базе ARM СнК, объединенное в общий чипсет и предоставляющее TPM поверх TEE. Решение предназначено для приложений DRM, платежных сервисов и аутентификации пользователя.

Samsung KNOX является решением безопасности для мобильных применений. Его отличительные особенности – механизм блокировки устройства в случае непрохождения проверки подлинности загружаемого кода, а также поддержка удаленной аттестации безопасности устройства.

Global Platform TEE

Основными взаимодействующими компонентами в рамках концепции Trusted Execution Environment, представленной в документации консорциума Global Platform, являются: клиентское приложение (Client Application, CA), реализация Trusted Execution Environment (так называемый TEE Framework), доверенные приложения (Trusted Application, TA).

Реализация TEE предоставляет ряд интерфейсов для использования доверенными приложениями, например Trusted Storage API – интерфейс доверенного хранилища, криптографические функции. Полное описание предоставляемых функций изложено в спецификации TEE Internal Core API Specification, Version 1.2.1, GPD_SPE_010.

Необходимыми условиями успешной реализации TEE является наличие аппаратного корня доверия и доверенная загрузка.

Корень доверия – это заведомо доверенный компонент системы, доверие к которому закладывается на этапе производства устройства и который, в свою очередь, позволяет верифицировать состояние других частей системы во время загрузки устройства и его эксплуатации.

Корень доверия предназначен для надежного хранения данных, предназначенных для загрузки устройства, средств защиты от отката, средств привязки программных компонент к процессору или СнК. Корень доверия состоит из надежного хранилища информации, аппаратных и программных средств, обеспечивающих безопасный доступ к хранимой в нем информации.

Под надежным хранением понимается обеспечение неизменности хранимой информации в течение всего жизненного цикла устройства. Хранилище может обеспечивать однократную запись данных в хранилище на этапе производства или первоначальной конфигурации, а также в процессе эксплуатации устройства.

Хранилище информации может содержать в себе следующие данные.

- Идентификатор устройства. Идентификатор устройства может однократно записываться на этапе производства чипа или на этапе производства устройства. Он может применяться для идентификации устройства программным обеспечением и для обеспечения идентификации устройства при сетевом взаимодействии.
- Ключи, сертификаты, хэши сертификатов. Эти данные могут однократно записываться на этапе производства чипа или на этапе производства устройства, что обеспечивает возможность для производителя устройства применять прошивки независимо от производителя чипа. Ключи и сертификаты применяются для обеспечения безопасной загрузки устройства и для привязки прошивки к устройству или группе устройств. При этом необходимо обеспечить доступ к ключам и сертификатам на как можно более раннем этапе загрузки ПО, то есть на уровне начальной загрузки.
- Номера версий прошивок. Значение может увеличиваться в процессе эксплуатации устройства. Номер версии проверяется на этапе безопасной загрузки и обеспечивает защиту от отката на предыдущие версии прошивок устройства.

Начальный загрузчик может запускаться из накристального ПЗУ чипа или из внешнего (по отношению к чипу) ПЗУ. Во втором случае не обеспечивается

защита от атак, связанных с наличием физического доступа внутрь корпуса устройства или связанных с подменой обновлений.

После подачи питания или сброса начинается выполнение ядром программного кода первичного загрузчика из доверенного накристального ПЗУ.

Пример возможной последовательности безопасной загрузки вторичными загрузчиками описан в Global Platform Device Technology Boot TEE Requirements Version 1.0 и представлен на рис. 4 в части этапов загрузки 2 и 3.

Доверенное хранилище предоставляет возможности длительного хранения произвольных данных доверенных приложений и ключевой информации. Сервис доверенного хранилища целесообразно использовать для хранения влияющих на безопасность данных. Для обеспечения конфиденциальности данных реализация доверенного хранилища использует компоненту криптографического сервиса для генерации ключей и шифрования, и дешифрования данных.

В качестве программного интерфейса используется набор функций Cryptographic Operations API TEE Internal Core API.

Таблица 1. Сравнение подходов к обеспечению информационной безопасности

Критерий	SE	TEE	TPM
Высокая устойчивость к физическим атакам	+		+
Доверенный ввод и доверенный дисплей		+	
Высокая производительность		+	+
Большой объем защищенного хранилища		+	
Гарантии уровней безопасности	+	+	+

Сравнение подходов

Сравнение наиболее распространенных подходов к обеспечению информационной безопасности представлено в табл. 1.

Можно сделать вывод, что наибольшую функциональность обеспечивают решения семейства TEE. При этом для достижения более высоких требований безопасности необходимо использовать дискретные компоненты безопасности, такие как SE или TPM.

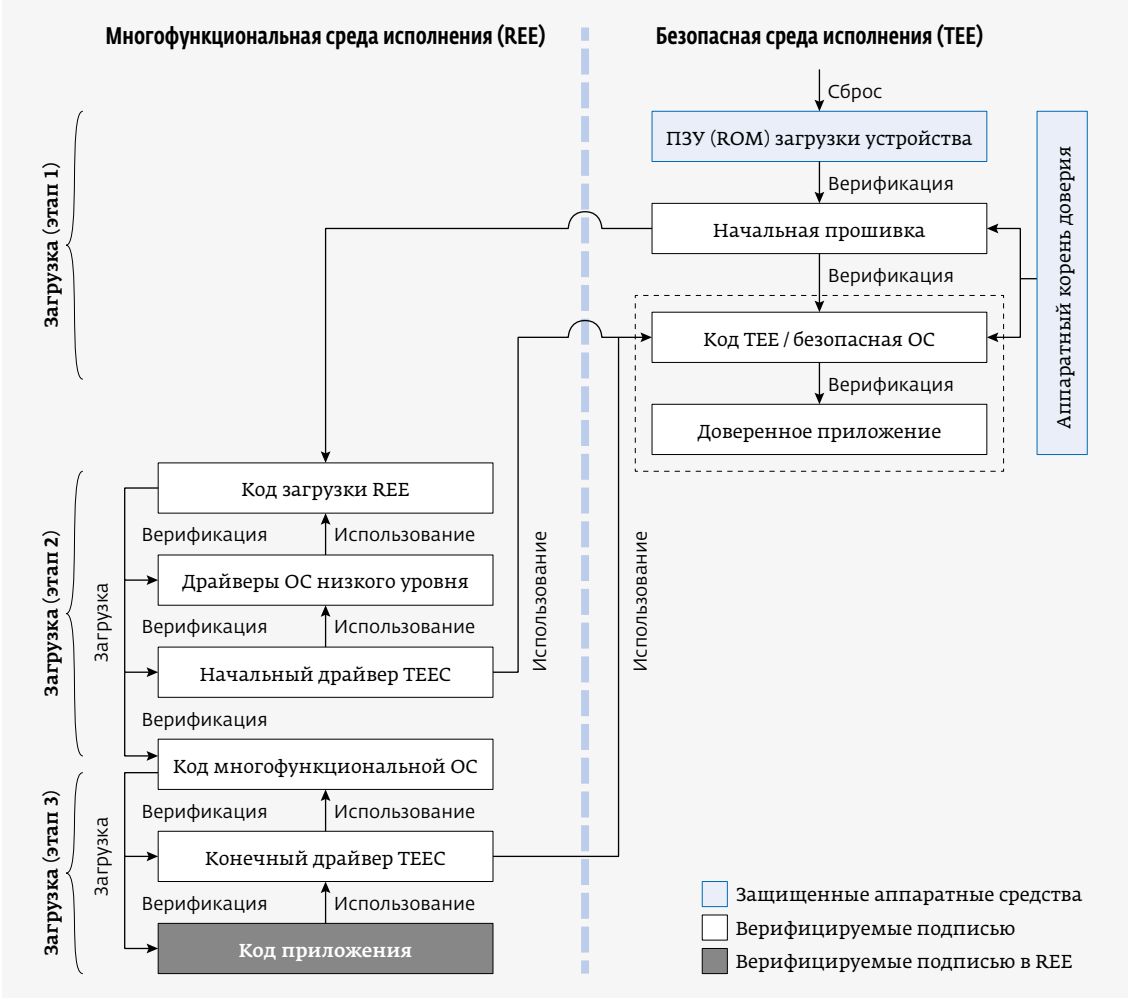

Рис. 4. Пример последовательности безопасной загрузки

СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА РОССИЙСКОМ РЫНКЕ

Средства и модули доверенной загрузки (СДЗ, МДЗ) являются одним из основных средств обеспечения защиты информации и предназначены для защиты от угроз несанкционированного доступа (НСД) в соответствии с требованиями регуляторов и нормативно-правовых актов в области защиты информации.

Несанкционированный доступ (далее – НСД) к информации является наиболее вероятной угрозой информационной безопасности. Реализация НСД может привести к утечке защищаемой информации. Для снижения этих рисков применяются средства (модули) доверенной загрузки, которые:

- проводят контроль целостности загружаемых файлов и сверяют их с эталонными значениями, хранимыми в недоступной для операционной системы памяти;
- обеспечивают идентификацию и аутентификацию пользователей до загрузки операционной системы;
- осуществляют запрет загрузки нештатных копий операционной системы с недоверенных внешних носителей информации.

СДЗ и МДЗ созданы для усиления встроенных средств защиты операционных систем, а именно для усиления аутентификации и идентификации пользователей, защиты от НСД к защищаемой информации.

ФСТЭК России предъявляет жесткие требования для защиты от НСД к информации, среди которых обязательное использование СДЗ. Выполнение требований регулятора в первую очередь необходимо для тех организаций, которые в своей деятельности сталкиваются с обработкой персональных данных, информации, содержащей сведения, составляющие государственную тайну, а также защиты существующих информационных систем.

На современном российском рынке информационной безопасности представлено множество СДЗ и МДЗ. Необходимость использования сертифицированных ФСТЭК решений для МДЗ и СДЗ и является главной причиной их востребованности на российском рынке.

В решениях СДЗ и МДЗ зарубежных производителей не реализованы необходимые требования российского законодательства в области информационной безопасности. В частности, не в полной мере выполняются требования, предъявляемые к средствам доверенной загрузки (приказ ФСТЭК России от 27 сентября 2013 года № 119). Для каждого типа СДЗ определено шесть классов защиты (класс 1 – самый высокий, класс 6 – самый низкий), а также вводится понятие профилей защиты СДЗ, которые соответствуют конкретному типу и классу защиты СДЗ. Профиль защиты – это набор обязательных требований, выполнение которых необходимо для сертификации продукта.

В своих руководящих документах ФСТЭК России строго определяет минимально необходимую функциональность для СДЗ и МДЗ. К основным функциям СДЗ и МДЗ относятся [5]:

- необходимость идентификации и аутентификации пользователя на этапе загрузки устройства;
- контроль целостности загрузочных областей жесткого диска, операционной системы и файлов;
- осуществление загрузки только с разрешенных источников;
- регистрация событий безопасности и контролируемых средством доверенной загрузки.

ОСНОВНЫЕ СЦЕНАРИИ ПРИМЕНЕНИЯ СнК «СКИФ»

Оценка возможных сценариев применения конечного устройства на базе СнК определяется исходя из следующих факторов:

- категоризация конечных устройств исходя из характерных условий применения устройств;
- оценка характеристик, влияющих на безопасность типовых конструктивных решений.

Далее для каждой категории конечных устройств определяется список возможных сценариев его применения.

Конечные устройства на базе СнК «Скиф»

Для оценки возможных сценариев применения рассмотрим следующие типы перспективных конечных устройств на базе СнК «Скиф»:

- мобильное устройство (МУ): смартфон, планшет;
- сетевое оборудование: CPE-маршрутизатор, коммутатор, P/PE-маршрутизатор;
- контроллер АСУ ТП;
- IoT-шлюз;
- прочее пользовательское оборудование: ТВ-приставка, ТВ, принтер, развлекательная система автомобиля;
- тонкий клиент/терминал, десктоп;
- ноутбук;
- БПЛА, автомобильный контроллер управления.

Оценка типовых условий эксплуатации устройства на базе СнК «Скиф» приведена в табл. 2.

Из табл. 2 следует, что указанные устройства можно сгруппировать следующим образом:

- мобильные устройства пользователя (МУ): пользовательское оборудование, ноутбук и др.;
- инфраструктурное корпоративное и операторское оборудование: IoT-шлюз, сетевое оборудование, контроллер АСУ ТП;
- устройства для работы корпоративных пользователей: тонкий клиент/терминал и десктоп;
- системы управления автономных устройств.

Типовые конструктивные особенности категорий устройств приведены в табл. 3.

Таблица 2. Типовые условия эксплуатации

Условия эксплуатации	МУ	IoT-шлюз	Контроллер АСУ ТП	Сетевое оборудование	Прочее пользовательское оборудование	Тонкий клиент, десктоп	Ноутбук	БПЛА, автомобильные системы
Обеспечение конфиденциальности информации	+	+		+	+	+	+	
Обеспечение целостности информации	+	+	+	+	+	+	+	+
Обеспечение доступности		+	+	+				+
Наличие регулярных обновлений ОС и драйверов	+				+	+	+	
Возможность утери/хищения устройства	+				+		+	
Наличие контролируемого физического доступа к устройству		+	+	+		+	+	+
Работа в режиме онлайн	+	+	+	+	+	+	+/–	
Многопользовательский доступ	+					+	+	
Возможность установки ПО пользователем	+				+		+	

Для устройств категорий, указанных в табл. 3, характерны следующие задачи использования или требования к их функциональным возможностям по обеспечению безопасности:

- доверенная загрузка;
- безопасное обновление ПО;
- защищенное хранилище, криптографические контейнеры и пр.;
- доверенный криптомодуль/криптопровайдер;
- защита видеоконтента;
- мобильная оплата;
- доверенный канал управления;
- резервная система управления, аварийная защита;
- возврат в безопасное состояние.

Кроме того, целесообразно рассмотреть сценарии применения, не являющиеся характерными или типовыми, но которые необходимо учесть ввиду запросов партнеров, к примеру – обеспечение криптографической защиты, в соответствии с действующими требованиями регулятора.

Целевые сценарии использования устройств

Для различных категорий устройств характерны задачи использования, представленные в табл. 4.

Таблица 3. Типовые конструктивные особенности категорий устройств

Типовые конструктивные особенности	Мобильное устройство	Сетевое оборудование и IoT-шлюз	Тонкий клиент	Автономные системы
Наличие консольных портов		+		+
Наличие съемных загрузочных носителей	+		+/–	
Наличие дополнительных сетевых контроллеров (включая радио) и интерфейсов	+	+		+
Наличие доверенных устройств в/в (клавиатура, мышь, LCD и биометрические датчики)	+	+		
Наличие стабилизированной системы питания		+		+
Наличие резервных элементов питания	+	+/–		+
Наличие средств контроля вскрытия корпуса				+/–
Наличие UEFI		+/–	+/–	

Таблица 4. Перечень характерных задач использования

Задачи использования	Мобильное устройство	Сетевое оборудование и IoT-шлюз	Тонкий клиент	Автономные системы
Доверенная загрузка	+	+	+	+
Безопасное обновление ОС и системного ПО	+	+	+	
Защищенное хранилище, криптографические контейнеры и пр.	+	+	+	+
Доверенный криптомодуль/криптопровайдер	+	+	+	+
Мобильная оплата	+		+	
Использование доверенных устройств в/в	+	+	+	
Защита видеоконтента	+		+	
Доверенный канал управления	+	+	+	+
Резервная система управления, аварийная защита		+		+
Возврат в безопасное состояние		+		+
Сертифицированное по старшим классам СКЗИ	+	+	+	

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СнК «СКИФ»

Информационная безопасность устройства, проектируемого на базе СнК «Скиф», достигается благодаря использованию встроенных аппаратных средств обеспечения безопасности и использования безопасного (защищенного) ПО.

СнК «Скиф» может быть аппаратно или программно сконфигурирована в режиме со включенной безопасностью или в режиме с отключенной безопасностью.

В режиме включенной безопасности доступна технология «Доверенное ядро» для всей микросхемы и технология ARM TrustZone для кластера ARM-ядер общего назначения.

В режиме отключенной безопасности доступна технология ARM TrustZone для кластера ARM-ядер общего назначения.

В состав микросхемы входят три контура безопасности: доверенный (кластер «доверенного ядра»), связной (связной кластер) и контур общего назначения.

Система обеспечения безопасности микросхемы следует концепции Trusted Execution Environment (TEE) компании Global Platform, описанной в документе TEE System Architecture Version 1.1, и концепции Trusted Base System Architecture (TBSA) компании ARM, описанной в документе Trusted Base System Architecture.

Ко встроенным аппаратным средствам безопасности относятся:

- технология «доверенного ядра»;
- технология безопасной аппаратной загрузки;
- хранение «секретов» в защищенной однократно-программируемой памяти (OTP);
- технология аппаратной изоляции транзакций между кластерами безопасности СнК;
- технология ARM TrustZone в кластере общего назначения;
- аппаратные примитивы синхронизации между кластерами в СнК «Скиф».

Технология «Доверенное ядро» в СнК «Скиф»

В микросхеме «Скиф» используется технология «Доверенное ядро» (рис. 5). Технология позволяет спроектировать безопасное устройство, которое обеспечивает следующие характеристики:

- обеспечение цепочки доверия с момента подачи питания на устройства до загрузки операционной системы;
- управление настройками микросхемы, питанием, частотами блоков микросхемы доверенным ядром;
- настройка прав взаимного доступа к блокам микросхемы, к памяти, прав на обработку прерываний доверенным ядром;
- управление отладкой микросхемы;
- обеспечение устройства доверенным реальным временем;
- обеспечение аппаратной средой для выполнения доверенных приложений.

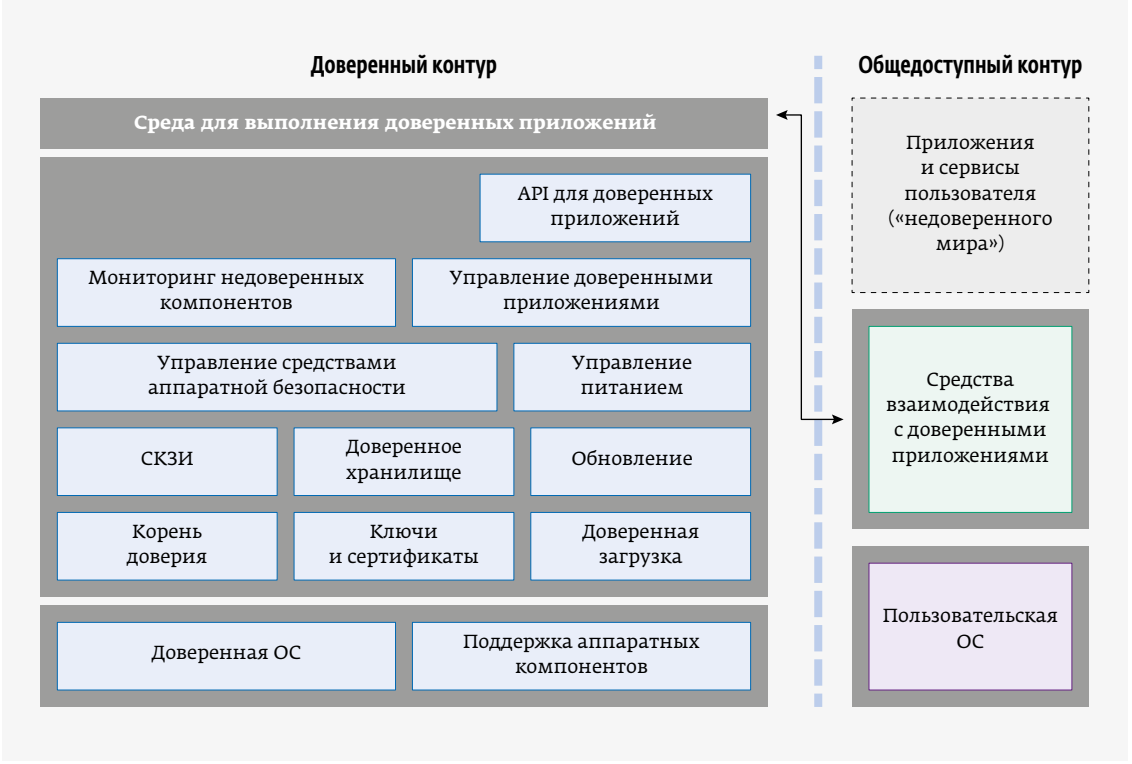

Рис. 5. Особенности «Доверенного ядра» СнК «Скиф»

«Доверенное ядро» является аппаратным кластером для доверенной среды исполнения. В состав «доверенного ядра» входят:

- RISC0 – доверенное процессорное ядро архитектуры MIPS32;
- FUSE – доверенные fuse-элементы (однократно прожигаемые конфигурационные элементы);
- OTP – доверенное хранилище ключевой информации;
- RTC – доверенный таймер реального времени;
- MFBSP – доверенный конфигурируемый периферийный контроллер СнК (режимы SPI, GPIO);
- модули управления частотами, питания, глобальных сбросов.

Аппаратная конфигурация режимов безопасности выполняется путем программирования fuse-элементов (однократно прожигаемые конфигурационные элементы). Состояние fuse-элементов задается производителем устройства.

Доверенное хранилище OTP является накристальной энергонезависимой памятью, состоящей из 128 32-разрядных слов с дополнительными ECC-битами. В OTP-памяти возможно хранить уникальные ключи устройства, ключевую информацию, номера версий прошивок, информацию, определяемую производителем устройства.

Модуль управления частотами, питанием, глобальными сбросами отвечает за формирование частот, питания, общих сигналов сброса для всех подсистем микросхемы и за формирование частот, питания, внутренних сигналов сброса для блоков подсистемы.

Технология безопасной аппаратной загрузки СнК «Скиф»

Безопасная аппаратная загрузка СнК «Скиф» осуществляется программой BootROM, зашитой в накристальную ROM-память микросхемы «Скиф». BootROM может осуществлять небезопасную загрузку или безопасную загрузку. Тип и алгоритм загрузки определяется состоянием OTP-памяти, состоянием fuse-элементов, состоянием сигналов на выводах микросхемы.

В режиме безопасной загрузки (safe boot) BootROM выполняет загрузку с выполнением ряда проверок:

- проверку целостности (хэш-сумм) образов, заголовков образов;
- аутентификацию загружаемых образов;
- расшифровку загружаемых образов.

Возможен режим небезопасной загрузки (unsafe boot), когда BootROM выполняет загрузку без выполнения проверки на целостность загружаемых данных, аутентификации и расшифровки.

В безопасном режиме загрузки BootROM загружает последовательность (цепочку) образов, содержащих ключи шифрования, подписи, загружаемые образы. В первом загружаемом образе на источнике загрузки должен находиться корневой сертификат. BootROM проверяет, совпадает ли хэш его ключа с тем, что записан в OTP-памяти, и в случае успеха сертификат принимается. Далее

в памяти находятся образы с сертификатами нижних уровней в порядке их подписи.

Пример загрузки последовательности загружаемых образов представлен на рис. 6, в котором используется корневой сертификат Root, сертификат A, подписанный Root, сертификаты B и C, подписанные с помощью A.

Первым во флеш-памяти должен находиться корневой сертификат (Root), за ним A, за ним B, C и D в порядке подписи. Схема валидации сертификатов и образа для этого примера также показана на рис. 6.

Технология безопасности в системе коммутации СнК «Скиф»

В СнК «Скиф» предусмотрено несколько уровней доступа и, соответственно, уровней запросов в системе коммутации микросхемы (в порядке убывания уровня доступа):

- доверенный уровень (trusted) – запросы от доверенного контура и внутри него от его компонентов;
- связной уровень (sdr) – запросы от связного контура и внутри него от его компонентов;

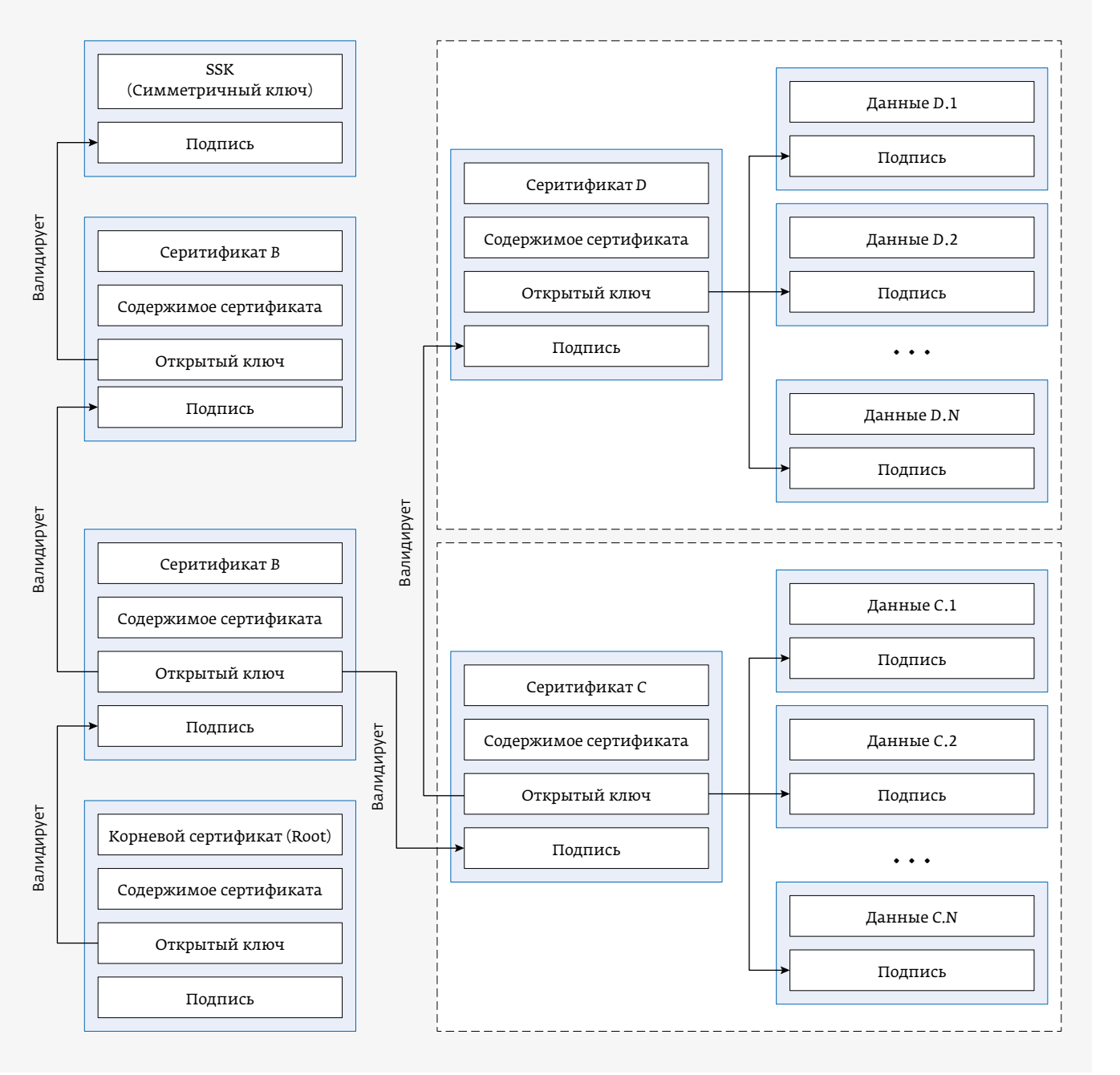

Рис. 6. Пример цепочки загружаемых образов

- безопасный уровень (secure) – запросы от компонентов общего контура в рамках архитектуры ARM TrustZone, помеченные как безопасные;
- общий уровень (non-secure) – запросы от компонентов общего контура в рамках архитектуры ARM TrustZone, помеченные как небезопасные.

Области памяти имеют аналогичные уровни доступа, соответствующие тому, какого уровня запросы допустимы к этой области. Более высокий уровень доступа для запроса означает, что для него допустимы обращения к областям памяти с уровнями равными, либо ниже его. То есть для запросов trusted допустимы обращения к областям trusted, sdr, secure и non-secure, для запросов sdr – к областям sdr, secure, non-secure и т. д.

Технология ARM TrustZone в кластере общего назначения

Технология ARM TrustZone в СнК «Скиф» обеспечивает дополнительный уровень безопасности СнК и является набором расширений безопасности СнК для повышения защищенности приложений, исполняющихся в кластере общего назначения. ARM TrustZone предполагает, что процессор ARM находится в защищенном (secure) или незащищенном (non-secure) состояниях. Изоляция между двумя состояниями достигается за счет изоляции регистровых банков, настройки изоляции памяти, прерываний. Программный переход между состояниями возможен через монитор безопасности (secure monitor).

Оперативная память, доступная кластеру общего назначения, разбивается на секторы с атрибутами возможного доступа (secure или non-secure).

Аппаратные примитивы синхронизации между кластерами в СнК «Скиф»

Система может быть сконфигурирована таким образом, чтобы кластер общего назначения и связной кластер не имели бы прямого доступа к регистрам доверенного ядра, регистрам управления питания и частотами. Для взаимодействия между кластерами используется технология аппаратных «почтовых ящиков» (Mailbox), которые позволяют реализовать следующие примитивы синхронизации:

- общую память;
- сигнальный семафор;
- блокирующий семафор.

Структура модуля Mailbox представлена на рис. 7.

Программное обеспечение микросхемы «Скиф»

Стек программного обеспечения пользовательской аппаратно-программной платформы микросхемы «Скиф» состоит из системного ПО и прикладного ПО, решающего требуемую задачу. Для разработки конечной прошивки необходимы средства разработки программ.

Средства разработки и отладки программ поставляются АО НПЦ «ЭЛВИС». В состав средств входят: компилятор C/C++ и средства отладки программ для каждого процессорного ядра (ARM Cortex A53, MIPS32, Elcore50) микросхемы «Скиф» [3].

Системное ПО классифицируется по признакам принадлежности к кластеру, а также принадлежности кластера к безопасной или небезопасной области СнК (рис. 8).

Для кластера общего назначения (CPU) в качестве операционной системы небезопасного мира используются ОС общего назначения Linux, Android или операционная система реального времени. В качестве операционной системы безопасного мира предполагается применение отечественной защищенной ОС с сервисами безопасности от партнеров.

Для связного кластера в качестве операционной системы безопасного мира используется ОСРВ для ядра Elcore50, на базе которой возможно разработать приложения с вычислительными возможностями Elcore50, а также вычислительных ускорителей SDR-подсистемы СнК. Программное обеспечение доверенного ядра работает в безопасном аппаратном контуре, состоит из загрузчика,

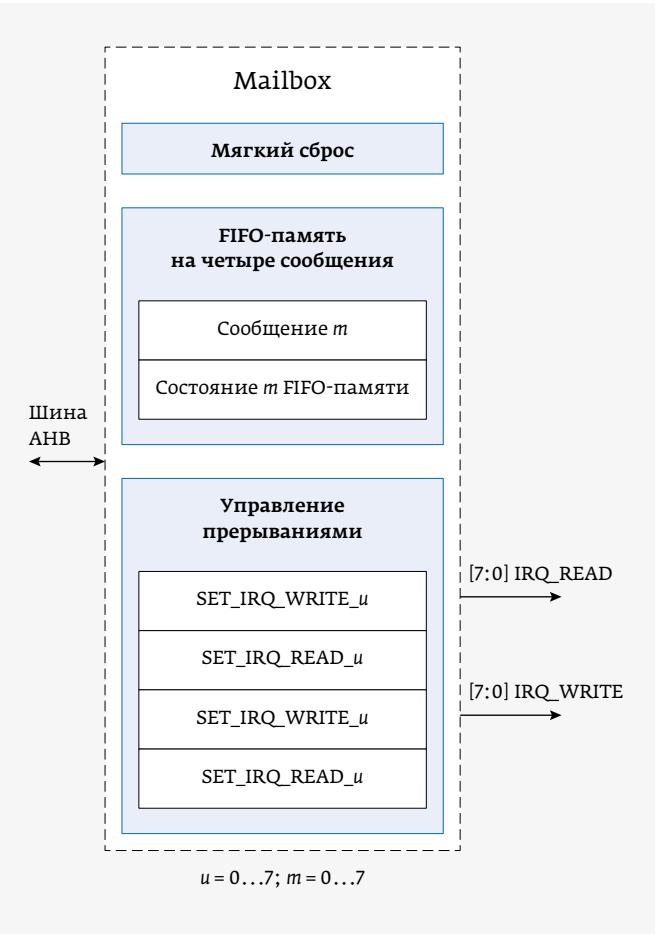

Рис. 7. Структура модуля Mailbox

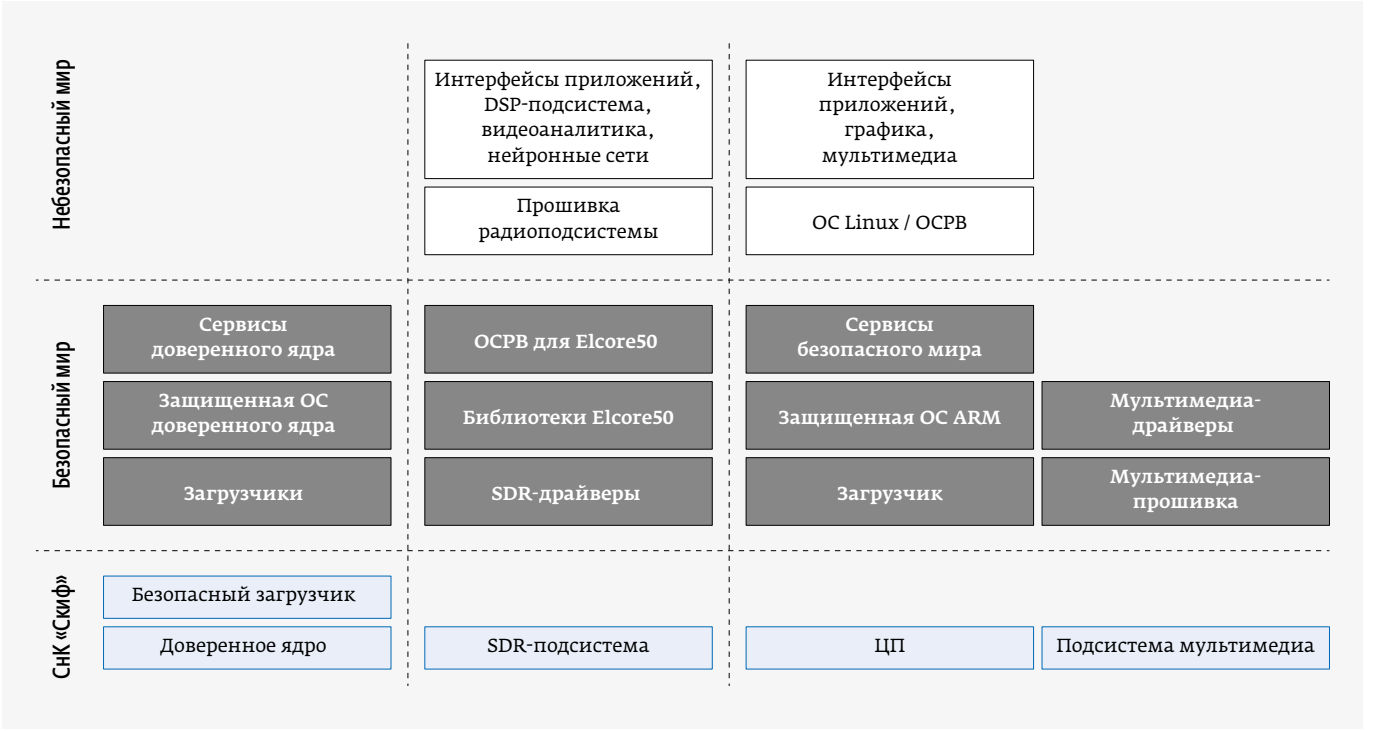

Рис. 8. Структура системного ПО СнК «Скиф»

сервисов безопасности, защищенной операционной системы доверенного ядра. Разработчик конечного устройства может выстраивать финальную прошивку, выбирая и конфигурируя необходимые компоненты из обозначенного ПО в соответствии с решаемыми задачами.

Роль и место безопасности как части жизненного цикла изделия

На рис. 9 представлена упрощенная модель жизненного цикла устройства. Устройство на каждом этапе жизненного цикла находится в среде с той или иной степенью доверенности с точки зрения безопасности.

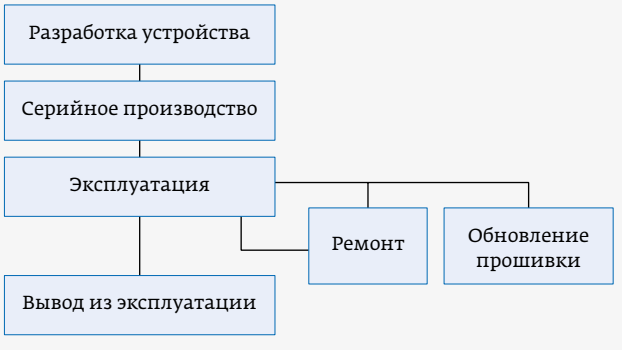

Рис. 9. Модель жизненного цикла устройства

Перечислим основные требования, предъявляемые к каждому этапу жизненного цикла.

На этапе разработки защищенного устройства требуется:

- доступ к отладочным интерфейсам;
- доступ к интерфейсам ввода-вывода отладочной информации;
- ограничение доступа разработчиков к защищенной информации, загружаемой в устройство.

На этапе серийного производства защищенного устройства требуется:

- обеспечение процедуры прошивки уникальной информации в каждое устройство;
- обеспечение процедуры прошивки секретов в OTP-память (key provisioning);
- ограничение доступа операторов к защищенной информации, загружаемой в устройство.

На этапе эксплуатации защищенного устройства требуется:

- обеспечение защиты от предполагаемых угроз;
- обеспечение процедур ремонта, обновления прошивок при необходимости.

Вывод из эксплуатации не должен приводить к обнародованию защищенной информации, находящейся в устройстве (содержимое прошивки, ключевой информации). Встроенные аппаратные возможности микросхемы «Скиф» и возможности ПО позволяют выполнить обозначенные требования.

Возможности применения СнК «Скиф»

Как упоминалось выше и как следует из мирового опыта, достижение высоких уровней защищенности СнК «Скиф» должно опираться на аппаратные ресурсы микросхемы, а также на программно реализованные на базе этих ресурсов технологии и механизмы доверенности и безопасности. СнК «Скиф» предоставляет такие возможности разработчикам устройств для широкого круга применений. Это достигается благодаря использованию встроенных в микросхему аппаратных решений отечественной разработки, наличию SDK и средств, предоставляющих разработчику устройства возможности простой интеграции механизмов безопасности в свой продукт. Кроме того, у разработчиков устройств имеется возможность размещения собственных программных решений для обеспечения безопасности в аппаратно защищенных областях микросхемы.

СнК «Скиф» позволяет реализовать описанные выше технологии безопасности, такие как программная реализация TPM, SE, реализация GP TEE, а также обеспечить выполнения требований российских регуляторов в части доверенной загрузки, криптографии, встроенных операционных систем и др. Важным является и то, что, в отличие от зарубежных аналогов, имеются возможности проведения верификации на самых низких уровнях программного и аппаратного обеспечения, что позволяет говорить о высоком уровне доверенности.

ЗАКЛЮЧЕНИЕ

Развитие и широкое применение цифровых информационных и коммуникационных технологий имеет решающее значение для повышения конкурентоспособности экономики и эффективности государственного управления, а также решения социальных задач. Цифровая информационная сфера, развиваемая в рамках программы «Цифровая экономика», является системообразующим фактором жизни общества.

Последние достижения, такие как переход к пятому поколению связи (5G), внедрение систем искусственного интеллекта, а также такое важное событие, как пандемия, все более ускоряют процесс цифровизации экономики и поднимают на новый уровень задачу обеспечения информационной безопасности всех элементов цифровой инфраструктуры.

Доверенная СнК «Скиф», для которой АО НПЦ «ЭЛВИС» вместе с партнерами обеспечивает несколько уровней аппаратной и программной защиты, соответствующих требованиям российских регуляторов и лучшим мировым практикам, может быть определена на сегодняшний день, как один из лучших отечественных продуктов для российского рынка мобильных и встраиваемых применений, особенно для КИИ.

Совместно с партнерами создана архитектура безопасности микросхемы «Скиф», учитывающая современные мировые стандарты в области безопасности и основанная на концепции Trusted Execution Environment (TEE) консорциума Global Platform. Система безопасности микросхемы обеспечивает высокий уровень защиты и доверия ко всему устройству за счет использования встроенных аппаратных средств и программных сервисов безопасности, изолированных от ПО пользователя.

АО НПЦ «ЭЛВИС» совместно с компаниями-партнерами работает над созданием доверенной защищенной экосистемы, объединяющей платформу для Интернета вещей (линейка СнК «Элиот»), встраиваемых применений (СнК «Скиф») и реализации «защищенных облаков» (СнК «Рободеус»).

Все решения объединены общей концепцией построения и интегрированными технологиями обеспечения информационной безопасности, опирающимися как на передовые открытые международные стандарты, так и учитывающими действующие требования к информационной безопасности в Российской Федерации.

Передовые характеристики и богатые функциональные возможности позволят реализовать потребителями этой отечественной защищенной экосистемы широкий спектр аппаратуры, а интегрированные технологии безопасности должны в перспективе стать неотъемлемой частью всей создаваемой отечественной ЭКБ, обеспечивая надежность и информационную безопасность всех элементов цифровой инфраструктуры в РФ.

ЛИТЕРАТУРА

1. **Тихонов А. И.** Для обеспечения КИИ отечественными доверенными решениями объективных препятствий нет. Нужна только воля к победе // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2020. № 10. С. 10–16.
2. **Петричкович Я. Я., Солохина Т. В., Кузнецов Д. А., Меньшенин Л. В., Беляев А. А. и др.** RoboDeus – 50-ядерная гетерогенная СнК для встраиваемых систем и робототехники // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2020. № 7. С. 52–63.
3. **Петричкович Я. Я., Солохина Т. В., Кузнецов Д. А., Меньшенин Л. В., Беляев А. А. и др.** «Скиф» – система на кристалле для мобильных и встраиваемых систем связи, навигации и мультимедиа // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2020. № 8. С. 120–129.
4. **Петричкович Я. Я., Солохина Т. В., Кузнецов Д. А., Меньшенин Л. В., Путря Ф. М. и др.** «Элиот» – система на кристалле для Интернета вещей // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2020. № 10. С. 122–130.
5. https://www.anti-malware.ru/analytics/Market_Analysis/SDZ-MDZ-russia-market-overview.