127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

КРИПТОПРО

Средство
Криптографической
Защиты
Информации

КриптоПро CSP
Версия 5.0 КС1
1-Base
Руководство администратора
безопасности.
Использование СКЗИ
под управлением ОС Android

ЖТЯИ.00101-01 91 10
Листов 16

2019 г

Содержание

Список сокращений **5**

1 Основные технические данные и характеристики СКЗИ **6**
1.1 Программно-аппаратные среды функционирования 6
1.2 Ключевые носители 6

2 Установка, обновление и удаление дистрибутивов ПО СКЗИ **7**

3 Состав и назначение компонент ПО СКЗИ **8**
3.1 Структура СКЗИ 8
3.2 Состав ПО СКЗИ 8

4 Встраивание СКЗИ в прикладное ПО **10**

5 Требования по защите от НСД **11**
5.1 Организационно-технические меры защиты от НСД 11
5.2 Дополнительные настройки ОС Android и операционных систем, к которым подключается устройство 12
5.2.1 Индивидуальная настройка Android 12
5.2.2 Настройка ОС, к которой подключается устройство 12

6 Требования по криптографической защите **13**

Приложение А. Контроль целостности программного обеспечения **14**

Приложение Б. Управление протоколированием **15**

Аннотация

Настоящее Руководство дополняет документ ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть при использовании СКЗИ под управлением ОС Android.

СКЗИ КриптоПро CSP под управлением ОС Android является криптопровайдером Java и предназначено для защиты конфиденциальной информации.

Инструкции администратора безопасности и пользователям различных автоматизированных систем, использующих СКЗИ КриптоПро CSP версия 5.0 КС1 Исполнение 1-Base, должны разрабатываться с учетом требований настоящего документа.

Список определений и сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск (Hard Disk Drive)
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
Регистрация	Присвоение определенных атрибутов (адреса, номера ключа, прав использования и т.п.) абоненту
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах
СВТ	Средства вычислительной техники
Сертификат	Электронный документ, подтверждающий принадлежность открытого ключа или ключа проверки электронной подписи и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа или ключа проверки электронной подписи абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей и ключей проверки электронной подписи. Сетевой справочник
СФ	Среда функционирования
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭП	Электронная подпись

1 Основные технические данные и характеристики СКЗИ

1.1 Программно-аппаратные среды функционирования

СКЗИ КриптоПро CSP версии 5.0 КС1 (ЖТЯИ.00101-01) под управлением ОС Android функционирует в программно-аппаратных средах на платформе Android 8/9 под управлением Java-машины **ART (Android Runtime)**.

Со сроками эксплуатации операционных систем, в среде которых функционирует СКЗИ, можно ознакомиться по адресу:

http://developer.android.com/index.html

1.2 Ключевые носители

Перечень поддерживаемых ключевых носителей в зависимости от программно-аппаратной платформы отражен в ЖТЯИ.00101-01 30 01. КриптоПро CSP. Формуляр, п. 3.9.

Использование носителей других типов допускается только по согласованию с ФСБ России.

Примечание. В состав дистрибутива СКЗИ входят библиотеки поддержки всех перечисленных носителей, но не входят драйверы для ОС. По вопросам получения драйверов необходимо обращаться к производителям соответствующих устройств.

2 Установка, обновление и удаление дистрибутивов ПО СКЗИ

Инсталляция, деинсталляция и обновление СКЗИ КриптоПро CSP 5.0 КС1 под управлением ОС Android производится в составе прикладной программы, разработанной с применением СКЗИ, либо с помощью дистрибутива, полученного по доверенному каналу. При этих действиях следует руководствоваться документацией от производителя прикладной программы или разработчика СКЗИ.

К установке и эксплуатации программного обеспечения, имеющего в своем составе СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие эксплуатационную документацию на соответствующие программные средства.

При установке программного обеспечения СКЗИ необходимо соблюдать следующие требования:

1) Инсталляция и использование СКЗИ должны осуществляться на устройстве без прав суперпользователя (root).

2) Запрещена установка приложений из недоверенного источника на мобильной устройство с установленным СКЗИ.

3) Установленное программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

4) Устройство, на которое устанавливается СКЗИ, следует получать у доверенного производителя, проверяя наличие подтверждающих работоспособность документов.

5) Перед установкой СКЗИ необходимо проверить программное обеспечение ПЭВМ на отсутствие вредоносного ПО и программных закладок. В том числе, необходимо убедиться в отсутствии на устройстве приложений, установленных из недоверенного источника.

6) Необходимо предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части устройства с установленным СКЗИ.

3 Состав и назначение компонент ПО СКЗИ

Основной архитектурной особенностью ПО СКЗИ КриптоПро CSP под управлением ОС Android является то, что подсистема программной среды функционирования криптосредства (СФ) не имеет непосредственного доступа к ключевой и криптографически значимой информации. Все операции с закрытыми ключами, незавершенными значениями хэш-функций и т.п. осуществляются в недоступных пользователю объектах; операции экспорта отсутствуют.

3.1 Структура СКЗИ

Общая структура СКЗИ КриптоПро CSP под управлением ОС Android представлена на рис. 1.

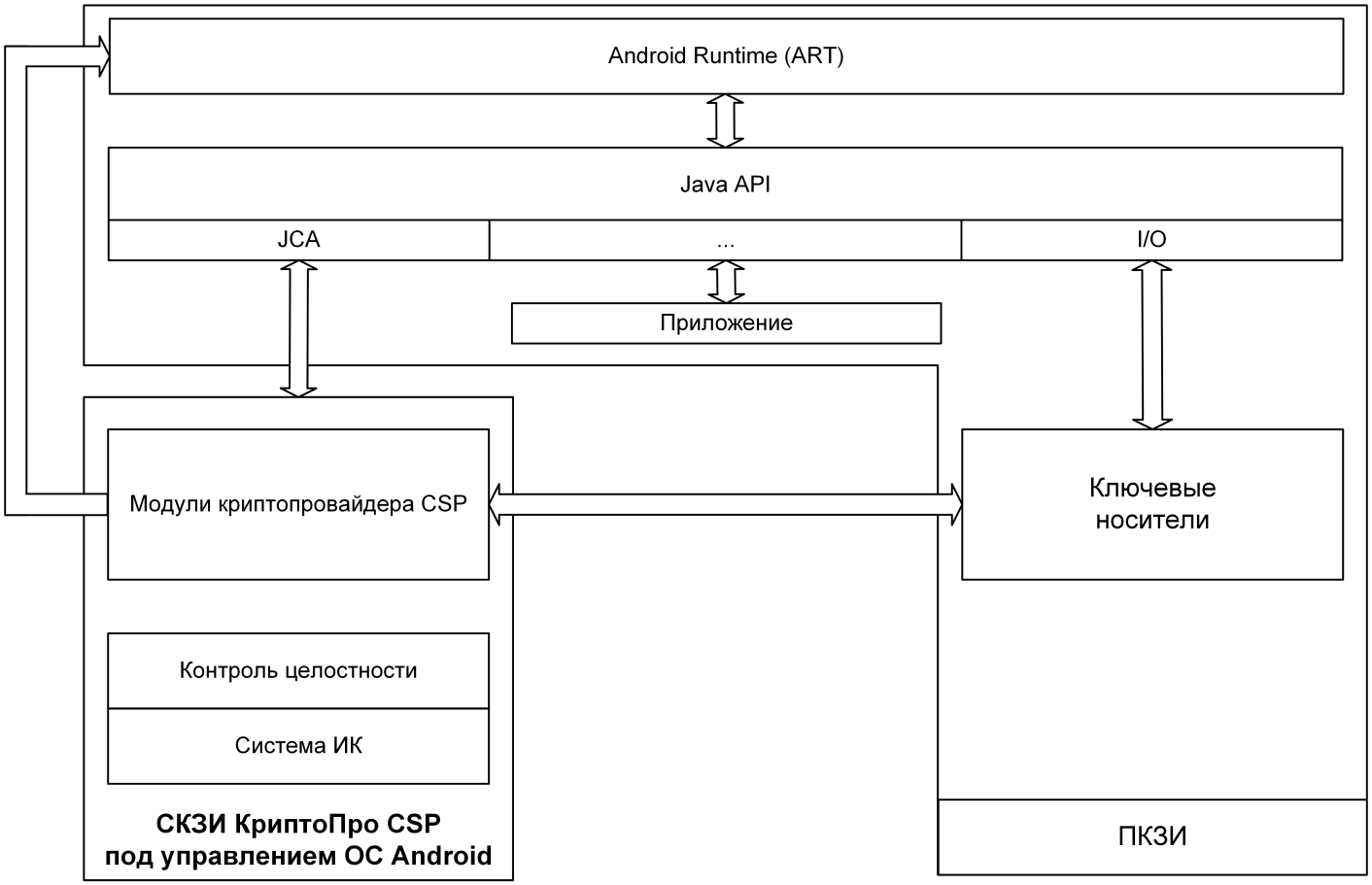

Рисунок 1. Структура СКЗИ КриптоПро CSP

3.2 Состав ПО СКЗИ

В состав СКЗИ КриптоПро CSP входят:
- Библиотеки криптопровайдера для исполнений по уровню КС1;
- Библиотеки шифровального провайдера для исполнений по уровню КС1;
- Нативная библиотека cpjni;
- Подсистема контроля целостности;
- Датчик случайных чисел (ДСЧ).

В состав подсистемы программной СФ входят следующие компоненты:
- ASN.1 модуль;

- Модуль поддержки ASN.1;
- Модуль запроса сертификатов;
- Подсистема настройки провайдера;
- Модули поддержки считывателей и носителей;
- Java-машина.

4 Встраивание СКЗИ в прикладное ПО

Для обеспечения защиты электронных документов и создания защищенной автоматизированной системы в первую очередь используют криптографические методы защиты, которые позволяют обеспечить защиту целостности, авторства и конфиденциальности электронной информации и реализовать их в виде программных или аппаратных средств, встраиваемых в автоматизированную систему.

Использование криптографических средств требует, как правило, применения также организационно-технических мер защиты.

Следует отметить, что вновь разрабатываемые подсистемы программной СФ и прикладное ПО, использующие сертифицированные СКЗИ должны удовлетворять требованиям к СКЗИ в части корректности использования СКЗИ и в части проверки влияния на СКЗИ со стороны ПО. Поэтому, в соответствии с российскими законами, встраивание СКЗИ могут производить организации, имеющие лицензию на право проведения таких работ, а работы по встраиванию должны проводиться в соответствии с Положением ПКЗ-2005.

При создании защищенной автоматизированной системы необходимо определить модель угроз и политику ее безопасности. В зависимости от политики безопасности определяется необходимый набор криптографических функций и организационно-технических мер, реализуемых в создаваемой системе.

СКЗИ КриптоПро CSP под управлением ОС Android в первую очередь предназначено для встраивания в прикладное программное обеспечение. Функции СКЗИ КриптоПро CSP под управлением ОС Android могут быть использованы:

- через интерфейс функций JCA, что позволяет применять весь инструментарий Java. Для этих целей разработчики могут воспользоваться программной документацией, содержащейся в Java 2 SDK, а также поставляемым тестовым ПО. Подробная информация содержится в документе ЖТЯИ.00101-01 96 02. КриптоПро CSP. Руководство программиста JavaCSP.
- в стандартном прикладном ПО Java.

При встраивании СКЗИ КриптоПро CSP под управлением ОС Android в прикладное программное обеспечение или использовании его в составе стандартного прикладного ПО должны выполняться следующие требования:

1) При использовании ключей проверки ЭП должна быть обеспечена целостность и идентичность ключа проверки ЭП. Это может быть реализовано:

- путем заверения ключа проверки ЭП доверенной стороной (например, в случае использования сертификатов ключей проверки подписи);
- путем доверенного распространения и хранения ключей проверки ЭП в виде справочников.

2) При использовании сертификатов ключей проверки подписи, заверенных подписью доверенной стороны, должна быть обеспечена безопасная доставка и хранение сертификата ключа ЭП доверенной стороны, с использованием которого проверяются остальные сертификаты ключей проверки пользователей.

3) Криптографическое средство, с помощью которого производится заверение ключей проверки ЭП или справочников ключей проверки ЭП, должно быть сертифицировано по классу, соответствующему принятой политике безопасности.

4) Для отзыва (вывода из действия) ключей проверки подписи должны использоваться средства, позволяющие произвести авторизацию отзывающего лица (в этих целях может быть использован список отозванных сертификатов, заверенный ЭП доверенной стороны).

5) При вызове функций СКЗИ в прикладном программном обеспечении необходимо, при возникновении критических исключений блокировать криптографические вызовы, а при возникновении других исключений, корректно их обрабатывать. (см. руководство программиста).

5 Требования по защите от НСД

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме раздела 5 документа СКЗИ ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть.

При эксплуатации СКЗИ на платформе Android при обработке конфиденциальной информации для конкретного мобильного устройства, работающего под управлением ОС Android, должны выполняться действующие в Российской Федерации требования по защите открытой (конфиденциальной) информации от утечки по техническим каналам. Данное требование не предъявляется в случае эксплуатации СКЗИ на платформе Android при обработке открытой информации, доступ к которой не ограничивается согласно законодательству Российской Федерации. Внос и использование мобильного устройства, работающего под управлением ОС Android, в помещениях, в которых ведутся переговоры секретного содержания или проводятся работы секретного характера, без проведения его специальных исследований и специальной проверки запрещаются.

При использовании СКЗИ КриптоПро CSP под управлением ОС Android необходимо предпринять дополнительные меры организационного и технического характера и выполнить дополнительные настройки операционной системы. При этом ставится задача не только обеспечить дополнительную защиту устройства и ОС от НСД, но и обеспечить бесперебойный режим работы и исключить возможности «отказа в обслуживании», вызванного внутренними причинами (например, переполнением файловых систем).

5.1 Организационно-технические меры защиты от НСД

1) При использовании СКЗИ на устройствах, подключенных к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей.

2) Право доступа к устройству с установленным ПО СКЗИ предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ.

3) На технических средствах, оснащенных СКЗИ, должно использоваться только лицензионное программное обеспечение фирм-производителей.

4) На мобильном устройстве не устанавливаются средства разработки и отладки ПО. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ.

5) Должны быть приняты меры по исключению несанкционированного доступа к устройствам, на которых установлены СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе с указанными устройствами. В случае такой необходимости должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, устройства, на которых эксплуатируется СКЗИ, и защищаемую информацию.

6) Должно быть запрещено оставлять без контроля устройства, на которых эксплуатируется СКЗИ, после ввода ключевой информации. В иных случаях, оставляя устройство с установленным СКЗИ без контроля, необходимо заблокировать экран устройства.

7) Из состава системы должно быть исключено оборудование, которое может создавать угрозу

безопасности ОС Android. Также необходимо избегать использования нестандартных аппаратных средств, имеющих возможность влиять на функционирование устройства или ОС Android.

8) После инсталляции ОС Android следует установить все рекомендованные производителем операционной системы программные обновления и программные обновления, связанные с безопасностью, существующие на момент инсталляции.

5.2 Дополнительные настройки ОС Android и операционных систем, к которым подключается устройство

5.2.1 Индивидуальная настройка Android

В настройках ОС Android в разделе «Security» необходимо включить поддержку парольного входа. Необходимо задать сложность пароля и настройки для удаления данных в случае неправильного ввода пароля, соответствующие требованиям п.5.4 документа ЖТЯИ.00101-01 95 01. Правила пользования.

5.2.2 Настройка ОС, к которой подключается устройство

1) Выполните рекомендации по дополнительной настройке ОС из руководства администратора безопасности для соответствующей ОС.

2) Если на устройстве хранятся закрытые ключи, резервные копии устройства должны быть зашифрованы. Для этого:

- Установите на компьютер, к которому подключается устройство, ПО для шифрования файлов (например, КриптоПро EFS).
- Выполните резервное копирование данных устройства на компьютер.
- С помощью ПО для шифрования файлов выполните зашифрование резервной копии.

6 Требования по криптографической защите

Должны выполняться требования по криптографической защите раздела 6 документа ЖТЯИ.00101-01 91 01.КриптоПро CSP. Руководство администратора безопасности. Общая часть в части, касающейся ОС Android.

Необходимо выполнить настройку операционной системы для работы с СКЗИ по разд. 5.2.

Контролем целостности должен быть охвачен исполняемый файл прикладной программы, в состав которой входит СКЗИ.

Приложение А
Контроль целостности программного обеспечения

Программное обеспечение СКЗИ КриптоПро CSP имеет средства обеспечения контроля целостности ПО СКЗИ, которые должны выполняются периодически.

Разработчик прикладной программы, содержащей СКЗИ КриптоПро CSP под управлением ОС Android, должен рассчитать хэш приложения. Хэш хранится в ресурсах приложения и контролируется средствами КриптоПро CSP при каждом запуске приложения, а также при нажатии на кнопку «Проверить» на вкладке **Целостность** панели КриптоПро CSP под управлением ОС Android (подробнее см. раздел «Проверка целостности» документа ЖТЯИ.00101-01 92 03. Инструкция по использованию СКЗИ под управлением ОС Android).

Если в результате периодического контроля целостности появляется сообщения о нарушении целостности контролируемого файла, пользователь обязан прекратить работу и обратиться к администратору безопасности. Администратор безопасности должен проанализировать причину, приведшую к нарушению целостности, и в случае необходимости переустановить приложение, содержащее ПО СКЗИ КриптоПро CSP.

Приложение Б
Управление протоколированием

Задать уровень протоколирования можно в конфигурационном файле для ОС Android в секции [debug]. Формат записи в файле:

<название модуля>=<уровень журналирования>

<название модуля>_fmt=<формат протокола>

Например:

cpcsp=1

cpcsp_fmt=57

Значением параметра <уровень журналирования> является битовая маска:

N_DB_ERROR = 1 # сообщения об ошибках

N_DB_LOG = 8 # сообщения о вызовах

Значением параметра <формат протокола> является битовая маска:

DBFMT_MODULE = 1 # выводить имя модуля

DBFMT_THREAD = 2 # выводить номер нитки

DBFMT_FUNC = 8 # выводить имя функции

DBFMT_TEXT = 0x10 # выводить само сообщение

DBFMT_HEX = 0x20 # выводить HEX дамп

DBFMT_ERR = 0x40 # выводить GetLastError

Также возможно логирование информации в КриптоПро JCP, которое включается с помощью утилиты adb, входящей в состав Android SDK.

Для включения протоколирования в КриптоПро JCP:

adb shell setprop log.tag.<TAG> <LEVEL>

Например:

adb shell setprop log.tag.JCP DEBUG

adb shell setprop log.tag.JCP INFO

Лист регистрации изменений

Лист регистрации изменений									
№ п/п	Номера листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					