

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



Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 5.0 R2 KC1

Исполнение 1-Base

Руководство администратора
безопасности.

Использование СКЗИ
под управлением ОС Android

ЖТЯИ.00101-02 91 11
Листов 17

© ООО «КРИПТО-ПРО», 2000-2021. Все права защищены.

Авторские права на средство криптографической защиты информации КриптоПро CSP и эксплуатационную документацию к нему зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент). Документ входит в комплект поставки программного обеспечения СКЗИ КриптоПро CSP версии 5.0 R2 КС1; на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО «КРИПТО-ПРО» документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

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 Особенности распространения СКЗИ КриптоПро CSP под управлением ОС Android	7
3 Установка дистрибутива ПО СКЗИ	8
4 Обновление ПО СКЗИ	8
5 Настройка СКЗИ	9
5.1 Включение режима усиленного контроля использования ключей	9
6 Состав и назначение компонент ПО СКЗИ	10
6.1 Структура СКЗИ	10
6.2 Состав ПО СКЗИ	11
7 Требования по встраиванию и использованию ПО СКЗИ	12
8 Требования по защите от НСД	13
8.1 Организационно-технические меры защиты от НСД	13
8.2 Дополнительные настройки ОС Android	13
9 Требования по криптографической защите	14
Приложение А. Контроль целостности программного обеспечения	15
Приложение Б. Управление протоколированием	16

Аннотация

Настоящее руководство содержит общее описание средства криптографической защиты информации «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base и рекомендации по использованию СКЗИ под управлением операционных систем Android.

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

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС Android, 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
СФК	Среда функционирования комплекса
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» версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС Android функционирует в программно-аппаратных средах на платформе Android 8/9/10/11 под управлением Java-машины **ART (Android Runtime)**.

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

<https://developer.android.com>

1.2 Ключевые носители

Перечень поддерживаемых ключевых носителей в зависимости от программно-аппаратной платформы отражен в ЖТЯИ.00101-02 30 01. КриптоПро CSP. Формуляр, п. 3.10.

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 Особенности распространения СКЗИ КристоПро CSP под управлением ОС Android

Для операционной системы Android КристоПро CSP может поставляться двумя способами:

- 1) в виде фреймворка для разработки;
- 2) в составе прикладной программы.

В первом случае фреймворк распространяется в соответствии с требованиями раздела 2 документа ЖТЯИ.00101-02 95 01. Правила пользования.

Во втором случае прикладная программа, которая содержит СКЗИ КристоПро CSP, и комплект эксплуатационной документации поставляется пользователю Уполномоченной организацией способом, определенным в документации на прикладную программу, например:

- 1) посредством загрузки прикладной программы в корпоративной сети;
- 2) посредством загрузки в сети Интернет (Google Play).

При необходимости для получения возможности активации установочных модулей СКЗИ КристоПро CSP пользователь направляет свои учётные данные Уполномоченной организации. Учётные данные могут быть направлены посредством заполнения специализированной регистрационной формы на сайте Уполномоченной организации.

После получения Уполномоченной организацией учётных данных пользователю предоставляется лицензионный код. Лицензионный код может вводиться как в окне панели управления СКЗИ, так и устанавливаться в составе сертификата открытого ключа пользователя, а также его ввод может быть реализован средствами прикладной программы.

Разработчики программного обеспечения должны вычислять значения контрольных сумм дистрибутивов разрабатываемого продукта при помощи средства контроля целостности (срverify.exe или иного сертифицированного средства). Данные значения контрольных сумм должны быть зафиксированы в документации на разрабатываемый продукт.

Документацией на прикладную программу также должна быть учтена необходимость проверки указанной контрольной суммы до установки дистрибутива.

Активация СКЗИ КристоПро CSP на рабочем месте пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей приложения, модулей СКЗИ КристоПро CSP и эксплуатационной документации.

3 Установка дистрибутива ПО СКЗИ

Для операционной системы Android КриптоПро CSP не поставляется в виде конечного приложения. КриптоПро CSP для Android представляет собой фреймворк для разработки. Файлы библиотек содержит в себе реализацию интерфейса CSP и вспомогательных функций. Доступные функции описаны в заголовочных файлах из состава фреймворка.

Установка ПО СКЗИ КриптоПро CSP под управлением ОС Android производится в составе прикладной программы, разработанной с применением СКЗИ. При этих действиях следует руководствоваться документацией от производителя прикладной программы.

Для установки необходимо иметь права администратора на данной рабочей станции/устройстве.

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) На технических средствах, оснащенных СКЗИ, возможно использование только лицензионного программного обеспечения фирм-изготовителей.
- 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) Рекомендуются установка средств защиты от НСД при использовании СКЗИ в соответствии с классом КС1.
- 6) Перед установкой СКЗИ необходимо проверить программное обеспечение на отсутствие вирусов и программных закладок.
- 7) Необходимо предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части устройства с установленным СКЗИ.

4 Обновление ПО СКЗИ

Обновление СКЗИ КриптоПро CSP под управлением ОС Android осуществляется в составе приложения, включающего в себя КриптоПро CSP, согласно инструкциям от производителя приложения.

5 Настройка СКЗИ

5.1 Включение режима усиленного контроля использования ключей

При встраивании СКЗИ КриптоПро CSP в приложения под управлением ОС Android должен быть включён режим усиленного контроля использования ключей. Режим усиленного контроля использования ключей обеспечивает осуществление контроля срока действия долговременных ключей электронной подписи и ключевого обмена, контроля доверенности ключей проверки электронной подписи и контроля корректного использования программного датчика случайных чисел. Для включения этого режима в конфигурационный файл `config.ini` (`config64.ini`) в раздел `[Parameters]` необходимо добавить строку:

```
StrengthenedKeyUsageControl = 1
```

Для обеспечения корректного функционирования провайдера в части выработки электронной подписи, а также работы с временными ключами (в частности, для работы в рамках TLS-соединения без аутентификации клиента) и генерации случайных данных необходимо произвести выработку долговременных ключей, предварительно проверив, что зарегистрирован хотя бы один датчик случайных чисел.



Примечание. Использование СКЗИ без включения режима усиленного контроля использования ключей разрешается исключительно в тестовых целях.

6 Состав и назначение компонент ПО СКЗИ

Основной архитектурной особенностью ПО СКЗИ КриптоПро CSP под управлением ОС Android является то, что 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.

6.1 Структура СКЗИ

Общая структура СКЗИ КриптоПро CSP под управлением ОС Android представлена на [рис. 1](#).

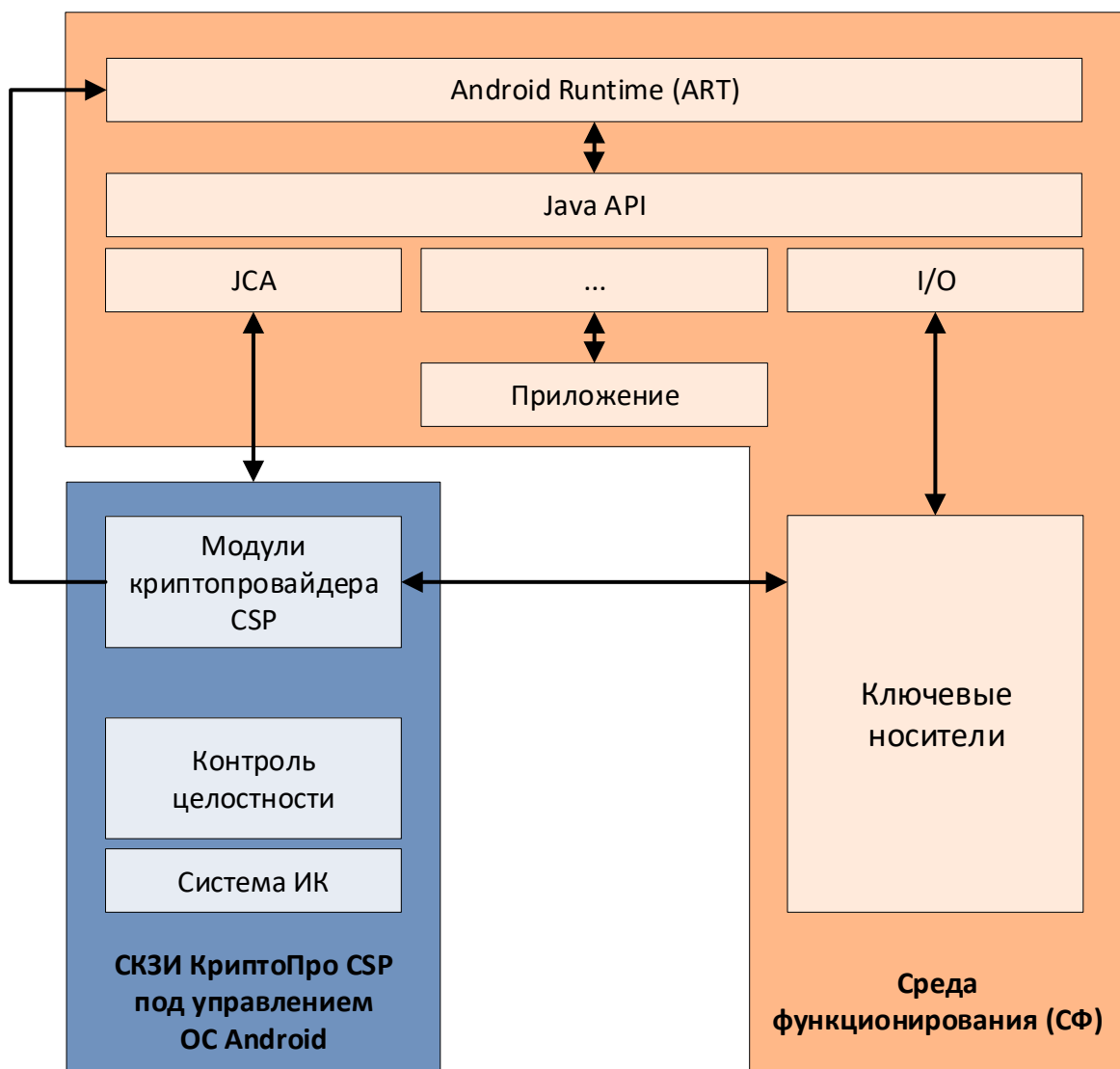


Рисунок 1. Структура СКЗИ КриптоПро CSP

6.2 Состав ПО СКЗИ

В состав программного обеспечения СКЗИ для платформы Android входят СКЗИ КриптоПро CSP и программная среда функционирования криптосредства (СФ).

В состав СКЗИ КриптоПро CSP входят:

- Библиотеки криптопровайдера для исполнений по уровню КС1;
- Библиотеки шифровального провайдера для исполнений по уровню КС1;
- Нативная библиотека `srjni`;
- Подсистема контроля целостности;
- Датчик случайных чисел (ДСЧ).

В состав СФ входят следующие компоненты:

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

7 Требования по встраиванию и использованию ПО СКЗИ

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.00101-02 96 02. КриптоПро CSP. Руководство программиста JCSP.
- 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 КриптоПро CSP в прикладном программном обеспечении необходимо, при возникновении критических исключений блокировать криптографические вызовы, а при возникновении других исключений, корректно их обрабатывать (подробнее см. ЖТЯИ.00101-02 96 02. КриптоПро CSP. Руководство программиста JCSP).

Встраивание СКЗИ в прикладное ПО должно осуществляться в соответствии с требованиями раздела 4 документа ЖТЯИ.00101-02 95 01. Правила пользования, документа ЖТЯИ.00101-02 96 02. КриптоПро CSP. Руководство программиста JCSP. и п. 1.5 документа ЖТЯИ.00101-02 30 01. Формуляр.

При использовании СКЗИ КриптоПро CSP под управлением ОС Android должны выполняться следующие условия:

- 1) должно быть запрещено использование Accessibility Service;
- 2) мобильное устройство не должно иметь root прав;
- 3) приложения должны функционировать на мобильном устройстве с установленным средством антивирусной защиты;
- 4) обязательна установка всех патчей обновлений;
- 5) должна быть запрещена установка ПО из недоверенного источника.

8 Требования по защите от НСД

8.1 Организационно-технические меры защиты от НСД

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме раздела 5 ЖТЯИ.00101-02 95 01. Правила пользования.

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).

8.2 Дополнительные настройки ОС Android

Индивидуальная настройка ОС 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 политике безопасности.

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.

9 Требования по криптографической защите

Должны выполняться требования по криптографической защите раздела 6 документа ЖТЯИ.00101-02 95 01. Правила пользования в части, касающейся ОС Android.

Необходимо выполнить настройку операционной системы для работы с СКЗИ по [разд. 8.2](#).

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 выполняться 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.00101-02 92 03. КриптоПро CSP. 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:

srcsp=1

srcsp_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

[illegible]