

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 iOS

ЖТЯИ.00101-02 91 08
Листов 15

© 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 KC1; 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 КристоПро CSP под управлением ОС iOS	7
3 Установка дистрибутива ПО СКЗИ	8
4 Обновление ПО СКЗИ	8
5 Настройка СКЗИ	8
5.1 Включение режима усиленного контроля использования ключей	8
6 Требования по защите от НСД	9
6.1 Организационно-технические меры защиты от НСД	9
6.2 Дополнительные настройки iOS и операционных систем, к которым устройство подключается через iTunes	9
6.2.1 Индивидуальная настройка iOS	9
6.2.2 Корпоративная настройка iOS	9
6.2.3 Настройка ОС, к которой устройство подключается при помощи iTunes	10
7 Требования по криптографической защите	11
Приложение А. Контроль целостности программного обеспечения	12
Приложение Б. Управление протоколированием	13

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 операционной системы iOS.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС iOS, должны разрабатываться с учетом требований настоящего документа.

Список определений и сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
APM	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» версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС iOS используется в программно-аппаратных средах:

Apple iOS (включая iPadOS) 8/9/10/11/12/13/14 (ARMv7, ARM64)

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

<http://www.apple.com/support/>

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 КриптоПро CSP под управлением ОС iOS

Для операционной системы iOS КриптоПро 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 КриптоПро 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 (Apple Store).

При необходимости для получения возможности активации установочных модулей СКЗИ КриптоПро 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 одновременно с формированием электронной подписи дистрибутивов (на зарубежных криптоалгоритмах, по установленным компанией Apple процедурам) 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 КриптоПро CSP на рабочем месте пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей приложения, модулей СКЗИ КриптоПро CSP и эксплуатационной документации.

3 Установка дистрибутива ПО СКЗИ

Для операционной системы iOS КриптоПро CSP не поставляется в виде конечного приложения. КриптоПро CSP для iOS представляет собой фреймворк для разработки, который содержит в себе объектный файл CPR0CSP, реализующий интерфейс CSP, ресурсы и заголовочные файлы с описанием доступных функций.

Фреймворк не имеет механизма самостоятельной установки в операционную систему. Установка осуществляется в составе прикладной программы, разработанной на основе фреймворка теми средствами, которые предлагает разработчик прикладной программы.

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 01. Руководство программиста и п. 1.5 документа ЖТЯИ.00101-02 30 01. Формуляр.

4 Обновление ПО СКЗИ

Обновление СКЗИ КриптоПро CSP на iOS 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 iOS должен быть включён режим усиленного контроля использования ключей. Режим усиленного контроля использования ключей обеспечивает осуществление контроля срока действия долгосрочных 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` 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 долгосрочных 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 Требования по защите от НСД

6.1 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 эксплуатации СКЗИ на платформе iOS при обработке конфиденциальной информации для конкретного мобильного устройства, работающего под управлением ОС iOS производства компании Apple, 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 iOS при обработке открытой информации, доступ к которой не ограничивается законодательству Российской Федерации. Внос и использование мобильного устройства, работающего под управлением ОС iOS производства компании Apple, 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 iOS 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).

6.2 Дополнительные настройки iOS и операционных систем, к которым устройство подключается через iTunes

6.2.1 Индивидуальная настройка iOS

В настройках ОС iOS в разделе «General — Passcode Lock» необходимо включить пароли. Необходимо задать сложность пароля и настройки для удаления данных в случае неправильного ввода пароля, соответствующие требованиям п. 5.4 документа ЖТЯИ.00101-02 95 01. Правила пользования.

6.2.2 Корпоративная настройка iOS

Корпоративная настройка ОС iOS выполняется при помощи iPhone Configuration utility. Данное ПО можно скачать с [сайта разработчика](#). Документация по утилите также доступна на сайте разработчика. При помощи iPhone Configuration Utility можно создать профиль настройки для устройства и применить его к одному или нескольким устройствам:

1) Создайте профиль со следующими параметрами:

а) В разделе «passcode» выберите «require passcode on device» и установите настройки:

- Maximum passcode age — 180 days
- Passcode history — 6

• Сложность пароля и настройки для удаления данных в случае неправильного ввода пароля должны соответствовать требованиям п. 5.4 документа ЖТЯИ.00101-02 95 01. Правила пользования

б) В разделе «restrictions» отключите все разрешения, которые не являются необходимыми для выполнения работы. Отключите «Allow installing apps». Если эта возможность необходима для работы, её необходимо оставить, но настроить ограничения через средства MDM (см. ниже).

в) Если в организации имеется сервер для управления мобильными устройствами (Mobile device management (MDM) server), то в разделе «mobile device management» необходимо настроить

подключение к нему. Сервер может быть использован для получения настроек (в том числе новых профилей настроек) и приложений.

2) Установите на устройство всё необходимое программное обеспечение и примените конфигурационный профиль. Эти действия также можно сделать централизованно при помощи сервера MDM.

6.2.3 Настройка ОС, к которой устройство подключается при помощи iTunes

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

2) Если на устройстве хранятся закрытые ключи, резервные копии устройства, сделанные при помощи iTunes, 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.

7 Требования по криптографической защите

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

Необходимо выполнить настройку операционной системы для работы с СКЗИ по [разд. 6.2](#).

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, должен рассчитать хэш приложения. Хэш хранится в ресурсах приложения и контролируется средствами КриптоПро CSP при каждом запуске приложения.

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 КриптоПро CSP.

Приложение Б

Управление протоколированием

Уровень, содержание и методы вывода информации независимо устанавливаются для выделенных модулей аудита (см. [табл. Б1](#)). Несколько библиотек могут использовать один модуль аудита, возможна и обратная ситуация.

Таблица Б1. Модули аудита

Модуль (name)	Описание
cap10	CryptoAPI 1.0
cap120	CryptoAPI 2.0
ssp	TLS
cspr	клиентский RPC
cpext	расширения CryptoAPI
cloud	облачный провайдер
csp	ядро CSP
pcsc	считыватели PC/SC

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

Для определения **уровня протокола** (levelmask, см. [табл. Б2](#)):

<name>=<levelmask>

Для задания **формата протокола** (formatmask, см. [табл. Б3](#)):

<name>_fmt=<formatmask>

Например:

csp=1

csp_fmt=57

Таблица Б2. Уровни протоколирования

N_DB_ERROR = 1 (0x01)	критические ошибки
N_DB_WARN = 2 (0x02)	некритические ошибки
N_DB_CALL = 4 (0x04)	информация о вызове функции
N_DB_LOG = 8 (0x08)	нейтральная информация
N_DB_TRACE = 16 (0x10)	отладочная информация
N_DB_CRUCIAL = 32 (0x20)	информация о важных событиях (например, создание ключа, удаление ключевого контейнера, ...)

Таблица Б3. Форматы протокола

DBFMT_MODULE = 0x01	выводить имя модуля
DBFMT_THREAD = 0x02	выводить номер нитки
DBFMT_FLINE = 0x04	выводить номер линии
DBFMT_FUNC = 0x08	выводить имя функции
DBFMT_TEXT = 0x10	выводить само сообщение
DBFMT_HEX = 0x20	выводить HEX дамп
DBFMT_ERR = 0x40	выводить GetLastError
DBFMT_PID = 0x80	выводить идентификатор процесса
DBFMT_PROCESS = 0x100	выводить имя процесса

Лист регистрации изменений

[illegible]