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 iOS

ЖТЯИ.00101-01 91 08
Листов 14

2019 г

Содержание

Аннотация

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

Инструкции администраторам 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 iOS используется в программно-аппаратных средах:

Apple iOS 8/9/10/11/12 (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.00101-01 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 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.00101-01 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 CSPпользователь 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 (`cpverify.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 `CPROCSP`, 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 8 документа ЖТЯИ.00101-01 91 01. Руководство администратора безопасности. Общая часть, документа ЖТЯИ.00101-01 96 01. Руководство программиста и п. 1.5 документа ЖТЯИ.00101-01 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 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` 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 Требования по защите от НСД

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

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

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

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

6.2.1 Индивидуальная настройка iOS

В настройках 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.00101-01 95 01. Правила пользования.

6.2.2 Корпоративная настройка iOS

Корпоративная настройка 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.00101-01 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.00101-01 91 01. Руководство администратора безопасности. Общая часть 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 выполняются 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

Задать уровень протоколирования можно в конфигурационном файле для iOS 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 протокола 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

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					