127 018, Москва, Сущевский вал, д.18
Телефон: (495) 995 4820
Факс: 4095) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 4.0 R4 КС1

1-Base

Руководство администратора безопасности

Использование СКЗИ под управлением ОС iOS

ЖТЯИ.00087-03 91 08
Листов 17

2018 г.

Содержание

Аннотация

Настоящее Руководство дополняет документ «ЖТЯИ.00087-03 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» v 4.0 R4, должны разрабатываться с учетом требований настоящего документа.

Список сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
ITU-T	Международный комитет по телекоммуникациям (International Telecommunication Union)
IETF	Internet Engineering Task Force
АС	Автоматизированная система
АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск
КП	Конечный пользователь
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 ключа проверки электронной подписи или открытого ключа и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата ключа проверки электронной подписи или открытого ключа 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.
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭП	Электронная подпись

1. Основные технические данные и характеристики СКЗИ

1.1. Программно-аппаратная среда

СКЗИ «КриптоПро CSP» v 4.0 R4 под управлением iOS используется в программно-аппаратных средах iOS версии 8.0, 8.0.1, 8.0.2, 8.1, 8.1.1, 8.1.2, 8.1.3, 8.2, 8.3, 8.4, 8.4.1, 9, 9.0.1, 9.0.2, 9.1, 9.2, 9.2.1, 9.3, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.5, 10, 11, 12 (ARMv7, ARM64).

Со сроками эксплуатации операционных систем, в среде которых функционирует СКЗИ, можно ознакомиться по адресу http://www.apple.com/support/.

1.2. Ключевые носители

В качестве ключевых носителей ключей ЭП и закрытых ключей выступает устройство iPad/iPod/iPhone, а также другие устройства, указанные в п.3.8 ЖТЯИ.00087-03 30 01. Формуляр.

	1. 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. 1. Хранение закрытых ключей на iPad/iPod/iPhone допускается только при условии распространения на iPad/iPod/iPhone требований по обращению с ключевыми носителями (п.6.7 ЖТЯИ.00087-03 91 01. Руководство администратора безопасности общая часть). 2. Все вышеперечисленные носители используются только в качестве пассивного хранилища ключевой информации без использования криптографических механизмов, реализованных на устройстве. 3. Использование носителей других типов - только по согласованию с ФСБ России.

2. Установка дистрибутива ПО КриптоПро CSP

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, реализующий функции CSP, ресурсы и заголовочные файлы. 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 пунктом 6 настоящего документа.

3. Порядок распространения СКЗИ КриптоПро CSP

Для операционной системы iOS «КриптоПро CSP» распространяется в составе прикладной программы с соблюдением, в целом, требований раздела 2 документа «ЖТЯИ.00087-03 91 01. Руководство администратора безопасности. Общая часть». Прикладная программа (приложение), которая содержит СКЗИ «КриптоПро CSP» и комплект эксплуатационной документации к нему могут поставляться пользователю Уполномоченной организацией двумя способами:

1. Посредством загрузки прикладной программы в корпоративной сети;
2. Посредством загрузки в сети Интернет (Apple Store);

Для получения возможности активации установочных модулей СКЗИ «КриптоПро CSP» и получения комплекта эксплуатационной документации 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 и доступ к сайту для загрузки комплекта эксплуатационной документации. В момент предоставления лицензионного кода Уполномоченной организацией присваивается учётный номер, идентифицирующий экземпляр СКЗИ «КриптоПро CSP», предоставленный пользователю. Лицензионный код может вводиться, как в окне панели управления СКЗИ «КриптоПро CSP», так и устанавливаться в составе сертификата открытого ключа пользователя, а также его ввод может быть реализован средствами прикладной программы.

Вместе с указанными данными пользователю предоставляются контрольные суммы установочных модулей приложения и документации. Контрольные суммы рассчитываются в соответствии с ГОСТ Р 34.11-2012 или ГОСТ Р 34.11-94 с учётом RFC 4357. Пользователь должен проверить и убедиться в целостности приложения в окне панели управления СКЗИ «КриптоПро CSP». Пользователь должен проверить и убедиться в целостности документации с использованием утилиты cpverify.exe, входящей в состав СКЗИ «КриптоПро CSP», либо иным другим сертифицированным ФСБ России шифровальным (криптографическим) средством, реализующим ГОСТ Р 34.11-2012 или ГОСТ Р 34.11-94 соответственно.

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.

Разработчики программного обеспечения одновременно с формированием электронной подписи дистрибутивов (на зарубежных криптоалгоритмах, по предполагаемым 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.

Получение значений контрольных сумм данных, скачанных с сайта, не гарантирует аутентичность значений. Рекомендуется получать значения контрольных сумм дистрибутива по доверенному каналу (в офисе ООО «КРИПТО-ПРО», у официальных дилеров, у разработчиков прикладного ПО, использующего функции СКЗИ).

Данный метод не гарантирует защиту дистрибутива от подмены. В случае получения дистрибутива СКЗИ уровня защиты КС1 использовать данный метод не рекомендуется. Для уровней защиты КС2, КС3 скачивание дистрибутива с сайта запрещено.

4. Обновление СКЗИ КриптоПро CSP

Обновление «КриптоПро CSP» на iOS осуществляется в составе приложения, включающего в себя «КриптоПро CSP» согласно инструкциям от производителя приложения.

5. Состав и назначение компонент программного обеспечения 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, ресурсы и заголовочные файлы. Объектный файл CPROCSP содержит в себе реализацию интерфейса CSP и вспомогательных функций. Доступные функции описаны в заголовочных файлах из состава фреймворка.

6. Встраивание СКЗИ КриптоПро CSP в прикладное ПО

При встраивании СКЗИ КриптоПро CSP в прикладное программное обеспечение должны выполняться требования раздела 17 документа «ЖТЯИ.00087-03 91 01. Руководство администратора безопасности. Общая часть», документа «ЖТЯИ.00087-03 96 01. Руководство программиста» и п. 1.5 документа «ЖТЯИ.00087-03 30 01. Формуляр».

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.

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

7. Требования по организационно-техническим и административным мерам обеспечения эксплуатации СКЗИ

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме разделов 15 и 16 документа СКЗИ ЖТЯИ.00087-03 91 01. Руководство администратора безопасности. Общая часть.

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.

7.1. Общие меры защиты от НСД ПО с установленными СКЗИ для iOS

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).

К организационно-техническим мерам относятся:

- обеспечение физической безопасности устройства;
- установка программных обновлений;
- организация процедуры резервного копирования и хранения резервных копий.

Дополнительные настройки iOS касаются следующего:

- ограничение доступа пользователей и настройки пользовательского окружения;
- ограничение сетевых соединений;
- ограничения на запуск процессов и установку программ;
- дополнительные настройки ядра ОС;
- настройка сетевых сервисов;
- ограничение количества "видимой извне" информации о системе;
- настройка подсистемы протоколирования и аудита.

7.1.1. Организационно-технические меры

1. Обеспечение физической безопасности устройства

Следует исключить возможность доступа неавторизованного персонала к устройству. Для этого необходимо либо осуществлять личный контроль за устройством, либо хранить его в запираемом сейфе.

Доступ персонала к устройству должен быть регламентирован внутренним распорядком эксплуатирующей организации и должностными инструкциями.

2. Организация процедуры резервного копирования и хранения резервных копий

При определении регламента резервного копирования и хранения резервных копий следует обеспечить ответственное хранение резервных копий и определить процедуру выдачи резервных копий ответственному персоналу и уничтожения вышедших из употребления носителей (лент, однократно записываемых дисков и пр.).

Резервные копии должны храниться в запираемых сейфах либо в зашифрованном виде на ЭВМ.

Стандартными мерами по организации ответственного хранения носителей являются:

- маркировка носителей;
- составление описи хранимых носителей с указанием серийных (инвентарных) номеров, дат записи носителей, фамилией сотрудника, создавшего копию для каждого шкафа(сейфа);
- периодическая сверка описи и содержимого сейфов (шкафов);
- организация ответственного хранения и выдачи ключей от сейфов (шкафов);
- возможное опечатывание (опломбирование) сейфов(шкафов).

Уничтожение вышедших из употребления носителей должно производиться комиссией с составлением акта об уничтожении.

3. При использовании СКЗИ «КриптоПро CSP» на ПЭВМ, 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.

4. Право доступа к рабочим местам с установленным ПО СКЗИ «КриптоПро CSP» предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ «КриптоПро CSP».

5. На технических средствах, оснащенных СКЗИ «КриптоПро CSP» должно использоваться только лицензионное программное обеспечение фирм-производителей.

6. На компьютере, к которому подключается устройство, не устанавливаются средств 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 «КриптоПро CSP».

7. Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства СКЗИ «КриптоПро CSP», по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях. Также необходимо обеспечить невозможность использования устройства с установленным СКЗИ посторонним лицам, не являющимися пользователями устройства.

8. Должно быть запрещено оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ «КриптоПро CSP» после ввода ключевой информации.

9. Из состава системы должно быть исключено оборудование, которое может создавать угрозу безопасности iOS. Также необходимо избегать использования нестандартных аппаратных средств, имеющих возможность влиять на функционирование устройства или iOS.

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

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

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 политике безопасности.

Корпоративная настройка iOS

Корпоративная настройка iOS выполняется при помощи iPhone Configuration utility. Данное ПО можно скачать с сайта разработчика: http://www.apple.com/support/ . 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:

a) В разделе "passcode" выберите "require passcode on device" и сделайте настройки:

- Maximum passcode age – 30 days
- Passcode history 6
- Задайте сложность пароля и настройки для удаления данных в случае неправильного ввода пароля, соответствующие политике безопасности организации.

b) 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 "mobile device management" (см. ниже).

c) Если в организации имеется сервер для управления мобильными устройствами(Mobile device management 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 iPad всё необходимое программное обеспечение и примените конфигурационный профиль. Эти действия также можно сделать централизованно при помощи сервера Mobile device management.

Настройка ОС, к которой устройство подключается при помощи iTunes

1. Выполните рекомендации по дополнительной настойке 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 зашифрования может быть использовано ПО КриптоПро EFS.

7.2. Требования по размещению технических средств с установленным СКЗИ

При размещении технических средств с установленным СКЗИ:

- Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию.
- Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ, сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.
- В случае планирования размещения СКЗИ в помещениях, где присутствует речевая, акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и (или) установлены технические средства и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, технические средства иностранного производства, на которых функционируют программные модули СКЗИ, должны быть подвергнуты специальной проверке по выявлению устройств, предназначенных для негласного получения информации».

8. Требования по криптографической защите

Должны выполняться требования:

1. Использование только лицензионного системного программного обеспечения.

2. Раздел 16 документа ЖТЯИ.00087-03 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть

3. Перед началом работы должен быть проведен контроль целостности. Контролем целостности должны быть охвачен файл, указанный в п. 16.

4. Настройка операционной системы для работы с СКЗИ по п. 7.1.2.

5. При инсталляции СКЗИ должны быть обеспечены организационно-технические меры по исключению подмены дистрибутива и внесения изменений в СКЗИ после установки.

6. Исключение из программного обеспечения ПЭВМ с установленным СКЗИ средств отладки.

7. Пароль, используемый для аутентификации пользователей, должен содержать не менее 8 символов алфавита мощности не менее 10. Периодичность смены пароля – не реже одного раза в 3 месяца.

8. Периодичность тестового контроля криптографических функций - 10 минут.

9. Ежесуточная перезагрузка ПЭВМ.

10. Периодичность останова ПЭВМ - 1 месяц.

11. **Запрещается** использовать режим простой замены (ECB) ГОСТ 28147-89 для шифрования информации, кроме ключевой.

12. Должно даваться предупреждение о том, что при использовании режима шифрования CRYPT_SIMPLEMIX_MODE материал, обрабатываемый на одном ключе, автоматически ограничивается величиной 4 MB.

13. Должно быть запрещено использование СКЗИ для защиты телефонных переговоров без принятия в системе мер по защите от информативности побочных каналов, специфических при передаче речи.

14. При эксплуатации СКЗИ необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К).

15. Контролем целостности должен быть охвачен исполняемый файл приложения, в которое входит СКЗИ.

Приложение 1. 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 2. 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 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

Лист регистрации изменений

Лист регистрации изменений									
	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					