



424000, РМЭ, г. Йошкар-Ола, ул. Карла Маркса, д. 109Б
Телефон: 8 (8362) 33-70-50
<https://trusted.ru>
E-mail: info@trusted.ru



127018, Москва, Суцёвский Вал, 18
Телефон: 8 (495) 995-48-20
<https://CryptoPro.ru>
E-mail: info@CryptoPro.ru

УТВЕРЖДЕНЫ
ЖТЯИ.00102-13 95 01-ЛУ

Средство
Криптографической
Защиты
Информации

КриптоПро CSP
Версия 5.0 R3 KC2
(исполнение 2-КриптоАРМ ГОСТ 3)
Правила пользования

ЖТЯИ.00102-13 95 01
Листов 15

Содержание

1 Назначение СКЗИ и его основные характеристики	5
2 Порядок распространения СКЗИ	6
3 Ключевая система и ключевые носители	7
4 Требования к использованию, встраиванию СКЗИ в прикладные системы и к проведению исследований СФ СКЗИ	8
5 Требования по обеспечению безопасности при эксплуатации СКЗИ	9
6 Требования по криптографической защите	11
Литература	12
Приложение 1. Контроль целостности программного обеспечения	13
Приложение 2. Перечень вызовов, использование которых при разработке систем на основе СКЗИ «КристоПро CSP» версия 5.0 R3 KC2 (исполнение 2-КристоАРМ ГОСТ 3) возможно без дополнительных тематических исследований	14

Аннотация

Данный документ содержит правила использования средства криптографической защиты информации (СКЗИ) «КриптоПро CSP» версия 5.0 R3 KC2 (исполнение 2-КриптоАРМ ГОСТ 3), назначение, ключевую систему, требования и условия эксплуатации.

Документ предназначен для администраторов (администраторов ИБ), осуществляющих установку, обслуживание и контроль за соблюдением требований к эксплуатации средств СКЗИ, для администраторов серверов, сетевых ресурсов предприятия и других работников службы информационной безопасности, осуществляющих настройку рабочих мест для работы со средствами СКЗИ, а также для пользователей СКЗИ.

Инструкции администраторам и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» версия 5.0 R3 KC2 (исполнение 2-КриптоАРМ ГОСТ 3), должны разрабатываться с учетом требований настоящих Правил пользования.

При эксплуатации СКЗИ «КриптоПро CSP» версия 5.0 R3 KC2 (исполнение 2-КриптоАРМ ГОСТ 3) наряду с требованиями настоящих Правил пользования должны также выполняться требования документа ЖТЯИ.00102-03 95 01. КриптоПро CSP. Правила пользования, входящего в комплект эксплуатационной документации СКЗИ «КриптоПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base).

1 Назначение СКЗИ и его основные характеристики

СКЗИ «КriptoПро CSP» версия 5.0 R3 KC2 (исполнение 2-КriptoАРМ ГОСТ 3) предназначено для выполнения следующих функций:

- 1) предоставление графического интерфейса:
 - формирования и проверки ЭП файлов;
 - зашифрования и расшифрования данных в файлах;
 - создания и управления ключевой информацией;
 - почтового клиента (формирования и проверки подписи, зашифрования и расшифрования почтовых сообщений);
- 2) установка защищённого соединения по протоколу TLS;
- 3) защита IMAP/POP3 соединений с сервером входящей почты и SMTP соединений с сервером исходящей почты с использованием протокола TLS;
- 4) предоставление программного интерфейса для работы с криптографическими сообщениями формата CMS, S/MIME и объектами инфраструктуры PKI.

В качестве средства криптографической защиты информации, реализующего функции формирования ключевой информации, хэширования, создания/проверки ЭП, шифрования/расшифрования данных и установки TLS-соединения, используется СКЗИ «КriptoПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base) (ЖТЯИ.00102-03).

В качестве подписываемых файлов и файлов, подпись под которыми проверяется, допускается использовать только текстовые файлы txt, файлы изображений png, jpg и файлы документов doc, docx, odt, odf, xls, xlsx, xml и pdf, архивы zip.

Для просмотра содержимого данных файлов допускается использовать следующие программы:

- ОС Windows: Notepad, Windows Photo Viewer, Microsoft Word, Microsoft Excel, Adobe Acrobat Reader;
- ОС Linux/Unix: vi/vim, Gnome Image Viewer, Libre Office, Qpdfview;
- ОС Аврора: Галерея, Документы, просмотр PDF.

Допускается подключение почтовых серверов, поддерживающих работу по протоколам SMTP, SMTPS, IMAP, IMAPS, POP3.

Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации сведений, составляющих конфиденциальную информацию, осуществляются в соответствии с [1, 2] и другими руководящими документами по обеспечению безопасности информации.

СКЗИ «КriptoПро CSP» версия 5.0 R3 KC2 (исполнение 2-КriptoАРМ ГОСТ 3) при выполнении требований эксплуатационной документации, входящих в комплектацию СКЗИ в соответствии с разделом 4 ЖТЯИ.00102-13 30 01. КriptoПро CSP. КriptoАРМ ГОСТ 3. Формуляр, удовлетворяет требованиям к СКЗИ [3] для СКЗИ класса KC2, требованиям к средствам ЭП [4] для средств ЭП класса KC2 и требованиям [5, 6] для СКЗИ по уровню КСБ.

Использование и встраивание СКЗИ в аппаратные, программно-аппаратные и программные средства связи/системы и проведение исследований среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований должны выполняться в соответствии с [разд. 4](#).

Использование СКЗИ «КriptoПро CSP» версия 5.0 R3 KC2 (исполнение 2-КriptoАРМ ГОСТ 3) с выключенным режимом контроля флага keyAgreement для сертификата ключа получателя **не допускается**. Включение данного режима описано в Руководствах пользователя, входящих в состав эксплуатационной документации на СКЗИ.

2 Порядок распространения СКЗИ

Установочные модули СКЗИ «КристоПро CSP» версия 5.0 R3 KC2 (исполнение 2-КристоАРМ ГОСТ 3) и комплект эксплуатационной документации к нему могут поставляться пользователю Уполномоченной организацией следующими способами:

- 1) на носителе (CD, DVD-диски);
- 2) посредством загрузки через информационно-телекоммуникационные сети (в том числе Интернет).

Для получения возможности загрузки установочных модулей СКЗИ и 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 доступ на страницу загрузки установочных модулей СКЗИ и комплекта эксплуатационной документации. При загрузке пользователем установочных модулей СКЗИ и комплекта эксплуатационной документации Уполномоченной организацией присваивается учётный номер, идентифицирующий экземпляр СКЗИ, предоставленный пользователю.

На странице загрузки вместе с дистрибутивом и документацией размещается отдельная электронная подпись, для проверки которой необходимо использовать утилиту `crverify`, полученную доверенным образом и содержащую ключ проверки данной электронной подписи.

Установка СКЗИ на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ и эксплуатационной документации.

Примечание.

1) Средство контроля целостности (`crverify`) первоначально должно быть получено пользователем на физическом носителе в офисе Уполномоченной организации. Такая утилита считается полученной доверенным образом. Далее полученной доверенным образом признается очередная версия утилиты, полученная любым образом (например, скачанная с сайта <https://cryptopro.ru/>), при условии, что она была проверена другим экземпляром утилиты, полученным ранее доверенным образом, и проверка была успешной.

2) Ключ проверки ЭП, а также информация о нем (дата создания, алгоритм хэш-функции, идентификатор алгоритма подписи) записываются в исходный код утилиты на этапе сборки.

3) Контроль целостности дистрибутива СКЗИ и компонентов среды функционирования (СФ) СКЗИ обеспечивается при помощи утилиты `crverify` в соответствии с Приложением 1 документа ЖТЯИ.00102-03 95 01. КристоПро CSP. Правила пользования, входящего в комплект документации на СКЗИ «КристоПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base).



3 Ключевая система и ключевые носители

СКЗИ «КристоПро CSP» версия 5.0 R3 KC2 (исполнение 2-КристоАРМ ГОСТ 3) предоставляет возможность управления ключами, выработанными средствами провайдера «КристоПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base) и хранящимися в его ключевых контейнерах, а также возможность формирования новой пары ключ ЭП/ключ проверки ЭП (закрытый и открытый ключ шифрования) и создания запроса на выпуск сертификата сформированного ключа проверки ЭП путём использования соответствующих программных инструментов, предоставляемых СКЗИ «КристоПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base).

Общие принципы построения ключевой системы СКЗИ, сроки действия и размеры ключей, правила использования и управления ключевой информацией и ключевыми носителями, а также требования по защите их от НСД подробно описаны в документе ЖТЯИ.00102-03 95 01. КристоПро CSP. Правила пользования, входящем в комплект документации на СКЗИ «КристоПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base).

4 Требования к использованию, встраиванию СКЗИ в прикладные системы и к проведению исследований СФ СКЗИ

СКЗИ «КriptoПро CSP» версия 5.0 R3 KC2 (исполнение 2-КriptoАРМ ГОСТ 3) является функционально законченным программным продуктом, готовым к применению.

Для обеспечения информационной безопасности рабочих мест и информационных систем, использующих СКЗИ, должны быть определены модель возможных угроз и нарушителя и выработана политика безопасности. В зависимости от модели возможных угроз и нарушителя определяется необходимый уровень защиты и, соответственно, необходимый класс СКЗИ.

Возможны следующие варианты применения СКЗИ «КriptoПро CSP» версия 5.0 R3 KC2 (исполнение 2-КriptoАРМ ГОСТ 3):

1) использование графических интерфейсов СКЗИ.

В данном варианте использования СКЗИ дополнительных исследований не требуется.

2) программный вызов команд интерфейса JSON RPC API, приведённых в [Приложении 2](#) настоящего документа.

В данном варианте использования СКЗИ требуется проведение исследований по оценке влияния СФ на СКЗИ.

Оценка влияния СФ СКЗИ на выполнение предъявленных к СКЗИ требований должна выполняться по Техническому заданию, согласованному с 8 Центром ФСБ России.

3) встраивание СКЗИ во вновь разрабатываемое или существующее прикладное программное обеспечение, программно-аппаратные и аппаратные решения.

В данном случае требуется проведение тематических исследований СФ со встроенным СКЗИ как самостоятельного шифровального (криптографического) средства¹.

Исследования по оценке влияния СФ на СКЗИ, а также тематические исследования СФ со встроенным СКЗИ как самостоятельного шифровального (криптографического) средства проводятся в соответствии с порядком, определённым Положением ПКЗ-2005 [2], организациями, имеющими соответствующие лицензии [7] на указанные виды деятельности и необходимую область аккредитации.

При встраивании СКЗИ в прикладные системы должны выполняться требования, приведенные в разделе 4 документа ЖТЯИ.00102-03 95 01. КriptoПро CSP. Правила пользования, входящего в комплект документации на СКЗИ «КriptoПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base).

¹В соответствии с [7] термины «шифровальное (криптографическое) средство» и «средство криптографической защиты информации» (СКЗИ) являются эквивалентными и включают в себя, в том числе, термин «Средство электронной подписи».

5 Требования по обеспечению безопасности при эксплуатации СКЗИ

Должны выполняться требования по обеспечению безопасности при эксплуатации СКЗИ, приведенные в разделе 5 документа ЖТЯИ.00102-03 95 01. КriptoПро CSP. Правила пользования, входящего в комплект документации на СКЗИ «КriptoПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base).

В организации, эксплуатирующей СКЗИ, должен быть назначен **Администратор безопасности**, на которого возлагаются задачи по установке и настройке программно-аппаратных средств, общесистемного и специального ПО, эксплуатируемого совместно с СКЗИ, по установке и первичной настройке СКЗИ, по организации работ по использованию СКЗИ, выработке соответствующих инструкций для пользователей, а также контроля за соблюдением требований по безопасности.

Допускается назначать группу лиц (например, Администратора безопасности СКЗИ и Системного администратора ИС), распределяя между ними приведённые в настоящей эксплуатационной документации обязанности Администратора безопасности с учётом модели угроз и нарушителя ИС, в которой применяется СКЗИ, а также с учетом нормативных документов, определяющих создание такой ИС. В этом случае порядок распределения обязанностей, функций и полномочий между ответственными лицами должен быть зафиксирован в эксплуатационной документации ИС.

Администратор безопасности не должен иметь возможность доступа к конфиденциальной информации пользователей.

Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определённые для эксплуатации лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, применяющего СКЗИ, с документацией на СКЗИ, а также с другими нормативными документами, созданными на её основе.

При размещении технических средств с установленным СКЗИ должны выполняться требования п. 5.2 документа ЖТЯИ.00102-03 95 01. КriptoПро CSP. Правила пользования.

При обработке с помощью СКЗИ конфиденциальной информации, передаваемой по каналам связи, выходящим за пределы контролируемой территории, необходимо:

- 1) Для проводных каналов (электрических и оптических) использовать любое из следующих устройств:
 - Волоконно-оптические линии связи;
 - Оптические развязывающие устройства, устанавливаемые в тракт передачи информации для создания оптоволоконного фрагмента сети;
 - Сертифицированные СКЗИ для передачи информации соответствующего уровня конфиденциальности.
- 2) Для радиоканалов:

Использовать радиоканал GSM, либо GPRS, либо 3G/4G, либо Wi-Fi, либо другой канал мобильной и беспроводной связи, работающий с цифровой модуляцией штатного информационного сигнала.

При установке СКЗИ, общесистемного и специального ПО на ПЭВМ должны выполняться требования п. 5.3 документа ЖТЯИ.00102-03 95 01. КriptoПро CSP. Правила пользования.

До загрузки ОС должен быть реализован контроль целостности файлов, критичных для загрузки ОС, и утилиты `crverify` с использованием модуля доверенной загрузки (ПАК защиты от НСД).

При установке ПО СКЗИ на ПЭВМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ и совместно поставляемых с СКЗИ компонент СФ (в соответствии с Приложением 1 документа ЖТЯИ.00102-03 95 01. КriptoПро CSP. Правила пользования, входящего в комплект документации на СКЗИ «КriptoПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base)).

После завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО СКЗИ, а также его окружения в соответствии с документацией (в соответствии с Приложением 1 документа ЖТЯИ.00102-03 95 01. КriptoПро CSP. Правила пользования, входящего в комплект документации на СКЗИ «КriptoПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base)).

При использовании СКЗИ должны выполняться меры по защите информации от НСД п. 5.4 документа ЖТЯИ.00102-03 95 01. КристоПро CSP. Правила пользования.

Администратор безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии с требованиями п. 5.4 документа ЖТЯИ.00102-03 95 01. КристоПро CSP. Правила пользования.

Дополнительно администратор безопасности должен регулярно (рекомендуемая периодичность — 1 раз в сутки) просматривать и анализировать журнал регистрации выполненных операций (log-файлы).

Должны выполняться требования по обеспечению физической безопасности сервера п. 5.5 документа ЖТЯИ.00102-03 95 01. КристоПро CSP. Правила пользования.

Должны выполняться требования по организации процедуры резервного копирования и хранения резервных копий ключевых носителей п. 5.6 документа ЖТЯИ.00102-03 95 01. КристоПро CSP. Правила пользования.

Должны выполняться требования по подключению СКЗИ для работы по общедоступным каналам передачи данных п. 5.7 документа ЖТЯИ.00102-03 95 01. КристоПро CSP. Правила пользования.

СКЗИ «КристоПро CSP» версия 5.0 R3 KC2 (исполнение 2-КристоАРМ ГОСТ 3) должно использоваться с модулем (средством) доверенной загрузки (МДЗ). Необходимо использовать изделие, сертифицированное ФСБ России. Поставка осуществляется по согласованию с пользователем.

При использовании МДЗ должны выполняться требования по использованию модулей (средств) доверенной загрузки п. 5.8 документа ЖТЯИ.00102-03 95 01. КристоПро CSP. Правила пользования.

6 Требования по криптографической защите

Должны выполняться следующие требования по криптографической защите:

1) Должны выполняться требования по криптографической защите информации, приведенные в ЖТЯИ.00102-03 95 01. КriptoПро CSP. Правила пользования на СКЗИ «КriptoПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base) (ЖТЯИ.00102-03).

2) Настройки операционных систем для работы с СКЗИ должны производиться в соответствии с эксплуатационной документацией на СКЗИ «КriptoПро CSP» версия 5.0 R3 KC2 (исполнение 2-КriptoАРМ ГОСТ 3) и «КriptoПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base) (ЖТЯИ.00102-03).

3) Контролем целостности должны быть охвачены файлы, указанные в [Приложении 1](#).

4) Если проверка целостности компонентов СКЗИ завершается ошибкой, Администратор безопасности должен выявить причину и обстоятельства нарушения целостности СКЗИ и переустановить СКЗИ в соответствии с инструкцией по установке.

5) Периодичность перезагрузки ПЭВМ — 7 дней.

6) Периодичность контроля системы охлаждения процессорного блока ПЭВМ — 1 месяц.

7) При использовании СКЗИ для защиты TLS-соединений в роли TLS-сервера под управлением ОС Windows после установки необходимо выполнить следующие действия по настройке используемых криптографических алгоритмов:

1. Проверить, что отключено использование устаревших криптонаборов (cipher suite-ов), посмотрев либо в контрольной панели СКЗИ КriptoПро CSP (вкладка «Настройки TLS», секция «Сервер»), либо значение ключа `tls_server_disable_legacy_cipher_suites` в ветке реестра `HKEY_LOCAL_MACHINE\SOFTWARE\[Wow6432Node]\CryptoPro\Cryptography\CurrentVersion\Parameters\` (должно быть равно 1).

2. Выполнить перезагрузку компьютера.

При использовании СКЗИ для защиты TLS-соединений в роли TLS-сервера под управлением ОС Linux/Unix после установки необходимо выполнить следующие действия по настройке используемых криптографических алгоритмов:

1. Отключить использование устаревших криптонаборов, установив значение параметра `tls_server_disable_legacy_cipher_suites` равным 1 командой

```
./cpconfig -ini '\config\Parameters' -add long tls_server_disable_legacy_cipher_suites 1
```

2. Выполнить перезагрузку сервиса `cproscsp` командой

```
systemctl restart cproscsp
```

Литература

- [1] Приказ ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну». URL: <http://base.garant.ru/183628/>.
- [2] Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)». URL: <http://base.garant.ru/187947/>.
- [3] Требования к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну.
- [4] Требования к средствам электронной подписи (утверждены приказом ФСБ России от 27 декабря 2011 г. № 796). URL: <https://base.garant.ru/70139150>.
- [5] Специальные требования к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации (СТ-Р).
- [6] Требования по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.
- [7] Постановление Правительства РФ от 16.04.2012 N 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)». URL: http://www.consultant.ru/document/cons_doc_LAW_128739/.

Приложение 1

Контроль целостности программного обеспечения

Модуль `crverify` позволяет осуществлять контроль целостности установленного программного обеспечения в ручном и автоматическом режимах.

Правила использования утилиты `crverify` приведены в Приложении 1 документа ЖТЯИ.00102-03 95 01. КристоПро CSP. Правила пользования, входящего в комплект документации на СКЗИ «КристоПро CSP» версии 5.0 R3 KC2 (исполнение 2-Base)).

Перечень файлов ПО СКЗИ, для которых необходимо обеспечить контроль целостности, содержится в следующих текстовых файлах (txt):

- `cryptoarm-gost-3-win32-x86.files`;
- `cryptoarm-gost-3-win64-x86.files`;
- `cryptoarm-gost-3-linux-x64.rpm-files`;
- `cryptoarm-gost-3-linux64-x86.deb-files`;
- `cryptoarm-gost-3-darwin-x64.files`.

Приложение 2

Перечень вызовов, использование которых при разработке систем на основе СКЗИ «КриптоПро CSP» версия 5.0 R3 KC2 (исполнение 2-КриптоАРМ ГОСТ 3) возможно без дополнительных тематических исследований

Интерфейс КриптоАРМ JSON RPC API

Функция	Описание	Ограничения на использование функции
diagnostics	Получение общей информации о системе и доступности криптографического провайдера.	
signAndEncrypt	Получение параметров криптографических алгоритмов шифрования, создания электронной подписи и проверки электронной подписи.	
startView	Открытие окна приложения КриптоАРМ ГОСТ 3.	
certRequests	Получение параметров для генерации запроса на сертификат.	
certificates	Открытие окон приложения для работы с сертификатами.	
sendMail	Открытие окна почтового клиента.	

Лист регистрации изменений

[illegible]