

424000, РМЭ, г. Йошкар-Ола, ул. Карла Маркса, д. 109Б

Телефоны: 8 (495) 532-11-08

8 (800) 222-11-08

8 (8362) 33-70-50

<https://trusted.ru>

E-mail: info@trusted.ru



127018, Москва, Сущёвский Вал, 18

Телефон: 8 (495) 995-48-20

<https://CryptoPro.ru>

E-mail: info@CryptoPro.ru



Средство

Криптографической

Защиты

Информации

КриптоПро CSP версии 5.0 R2 KC1

Исполнение 1-КриптоАРМ

Руководство администратора

Linux

ЖТЯИ.00101-12 91 02

Листов 17

2021 г

Содержание

Общие сведения о программном продукте	3
Системные требования	3
Поддерживаемые операционные системы	4
1. Установка программного продукта	5
2. Удаление программного продукта.....	6
3. Установка лицензии на программный продукт	7
3.1. Установка лицензии через пользовательский интерфейс.....	7
3.2. Установка лицензии через командную строку	7
4. Диагностика неполадок при запуске приложения	8
4.1. Отсутствует СКЗИ КриптоПро CSP.....	8
4.2. Отсутствует лицензия на КриптоАРМ ГОСТ.....	8
4.3. Отсутствует лицензия на КриптоПро CSP	9
4.4. Не обнаружены сертификаты с привязкой к ключевому контейнеру	10
4.5. Не загружен модуль Trusted Crypto.....	11
4.6. Отсутствуют установленные модули КриптоПро TSP Client 2.0/OCSP Client 2.0	12
5. Включение режима логирования и консоль управления.....	14
6. Использование приложения в замкнутой программной среде ОС Astra Linux Special Edition	16
7. Часто встречающиеся проблемы.....	17
7.1. Не запускается приложение на deb системе	17
7.2. Если раньше работало и перестало.....	Ошибка! Закладка не определена.
7.3. Не импортируются корневые, промежуточные сертификаты, СОС на линукс:	17

Аннотация

Настоящее руководство содержит общее описание СКЗИ КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-КриптоАРМ (далее по тексту — КриптоАРМ ГОСТ), инструкции и рекомендации по использованию СКЗИ под управлением ОС Linux.

Инструкции администратора безопасности и пользователя различных автоматизированных систем, использующих СКЗИ, должны разрабатываться с учетом требований настоящего документа.

Установка, настройка и использование СКЗИ КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС Linux, входящего в комплект поставки, должна осуществляться в соответствии с требованиями и рекомендациями документа ЖТЯИ.00101-02 91 03. КриптоПро CSP. Руководство администратора безопасности. Linux.

Общие сведения о программном продукте

КриптоАРМ ГОСТ - это универсальное приложение с графическим пользовательским интерфейсом для выполнения операций по созданию и проверке электронной подписи файлов, шифрования и расшифрования, управления сертификатами, размещенных в хранилищах криптопровайдера КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.

Приложение КриптоАРМ ГОСТ является кроссплатформенным, и представлено различными установочными дистрибутивами под платформы: Microsoft Windows, Linux, OSX. На каждой из платформ реализована поддержка российских криптографических стандартов посредством использования криптопровайдера КриптоПро CSP версии 5.0 R2 KC1 исполнение 1-Base.

В приложении поддерживается работа с ключевыми носителями Рутокен и JaCarta через криптопровайдер КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.

Поддерживаемые криптопровайдеры

В приложении осуществляется поддержка криптопровайдера КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.

Лицензия на программный продукт

При первой установке приложения активируется временная лицензия сроком на 14 дней. После истечения ознакомительного периода для полноценной работы приложения требуется приобретение и установка лицензии. Без установки лицензии на доступ к ключу ЭП при операциях подписи и расшифрования будут наложены ограничения.

Для приобретения лицензии на программный продукт КриптоАРМ ГОСТ можно обратиться в компанию ООО «Цифровые технологии» или ООО «КРИПТО-ПРО».

Системные требования

Для приложения сформулированы минимальные системные требования к конфигурации оборудования под платформами:

- 2Gb оперативной памяти;
- 200 Mb дискового пространства для установки и работы приложения;

- требование к видеоадаптеру не критично. Должно поддерживаться минимальное разрешение 800x600.

Поддерживаемые операционные системы

КриптоАРМ ГОСТ функционирует под управлением следующих операционных систем:

- CentOS 7/8 (x64)
- ОСь (OS-RT) (x64)
- РЕД ОС 7.1/7.2 (x86, x64, ARM64)
- Ubuntu 19.10/20.04 (x64)
- Astra Linux Special Edition, Common Edition (x64)
- Альт Рабочая Станция 8/9, Альт Сервер 8/9, Альт 8 СП, Альт Образование 8/9 (x64)
- ROSA Enterprise Desktop (RED X4) (x86, x64)
- ROSA Enterprise Linux Desktop, Enterprise Linux Server (x64)
- РОСА КОБАЛЬТ (x64)

1. Установка программного продукта

Для функционирования КриптоАРМ необходим установленный КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base, установка должна производиться в соответствии с требованиями и рекомендациями документа ЖТЯИ.00101-02 91 03. КриптоПро CSP. Руководство администратора безопасности. Linux.

Установка приложения КриптоАРМ ГОСТ на операционную систему Linux может быть выполнена в графическом режиме через мастер установки пакетов, через терминал в режиме командной строки и обычной распаковкой из архива. По умолчанию приложение устанавливается в каталог `/opt/cryptoarm_gost/`.

- В режиме графической установки приложения КриптоАРМ ГОСТ запустите на исполнение файл:

cryptoarm-gost-v2.2.4-linux-x64.rpm для 64-разрядных ОС, основанных на RPM;

cryptoarm-gost-v2.2.4-linux-x64.deb для 64-разрядных ОС, основанных на DEB.

Откроется пакетный менеджер, в котором нужно нажать Установить. Так как установка производится от имени администратора системы, то появится диалог ввода пароля администратора системы (Root).

- Второй способ установки приложения выполняется с помощью командной строки. Для этого нужно запустить терминал и ввести команду:

`sudo dpkg -i cryptoarm-gost-v2.2.4-linux-x64.deb` - для ОС, основанных на Debian (Debian/Ubuntu);

`sudo rpm -i cryptoarm-gost-v2.2.4-linux-x64.rpm` - для ОС, основанных на RPM;

После установки приложения в меню появится ярлык КриптоАРМ ГОСТ.

- В том случае, когда не поддерживается пакетный режим установки приложения, его можно установить из предоставленного архива, распаковав содержимое в каталог `/opt/cryptoarm_gost/`. Распаковку архива необходимо производить с правами администратора.

2. Удаление программного продукта

Удаление приложения КриптоАРМ ГОСТ на операционных системах Linux выполняется через графический интерфейс (пакетный менеджер), либо через терминал в режиме командной строки.

- Удаление приложения КриптоАРМ ГОСТ через графический интерфейс выполняется следующим образом. Нужно открыть менеджер программ (пакетный менеджер) и найти приложение КриптоАРМ ГОСТ. Найденное приложение следует пометить для удаления и нажать на кнопку **Удалить**. После этого программа КриптоАРМ ГОСТ будет удалена с компьютера.

- Второй способ удаления основан на запуске команд в терминале:

`sudo dpkg -P cryptoarm-gost` - для ОС, основанных на Debian (Debian/Ubuntu);

`sudo rpm -e cryptoarm-gost` - для ОС, основанных на RPM;

После выполнения команды приложение будет удалено из операционной системы.

Удаление КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base осуществляется в соответствии с инструкциями документа ЖТЯИ.00101-02 91 03. КриптоПро CSP. Руководство администратора безопасности. Linux.

3. Установка лицензии на программный продукт

Для полноценной работы приложения КриптоАРМ ГОСТ необходима установка лицензионного ключа. Лицензионный ключ представляет собой файл, который необходимо расположить в специально созданном каталоге приложения.

Существуют два вида лицензий – постоянная и временная. Временная лицензия предоставляется с ограниченным сроком действия. Для приобретения постоянной лицензии можно обратиться в компанию разработчика.

Установка лицензионного ключа может производиться как через пользовательский интерфейс, так и с помощью консольных команд, выполняющих копирование файла лицензии в заданный каталог.

3.1. Установка лицензии через пользовательский интерфейс

Установка лицензии через пользовательский интерфейс описана в «Руководстве пользователя».

3.2. Установка лицензии через командную строку

Если установить лицензию через пользовательский интерфейс не получается, то возможна установка лицензии с помощью копирования файла лицензии license.lic в каталог:

`/etc/opt/Trusted/CryptoARM GOST/.`

Если такого каталога нет, то создать.

Примечание. Для последующей установки лицензии пользователями каталог установки лицензии должен иметь права на запись, а минимально необходимые права – права на чтение для пользователей на рабочем месте.

4. Диагностика неполадок при запуске приложения

При обнаружении проблем, затрудняющих дальнейшую работу приложения КриптоАРМ ГОСТ, запускается мастер диагностики приложения. В мастере подробно описываются возникшие неполадки и способы их решения.

4.1. Отсутствует СКЗИ КриптоПро CSP

Приложение КриптоАРМ ГОСТ не работает без установленного в системе СКЗИ КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base. В таком случае при запуске приложения будет предупреждающее сообщение (рис. 4.1)

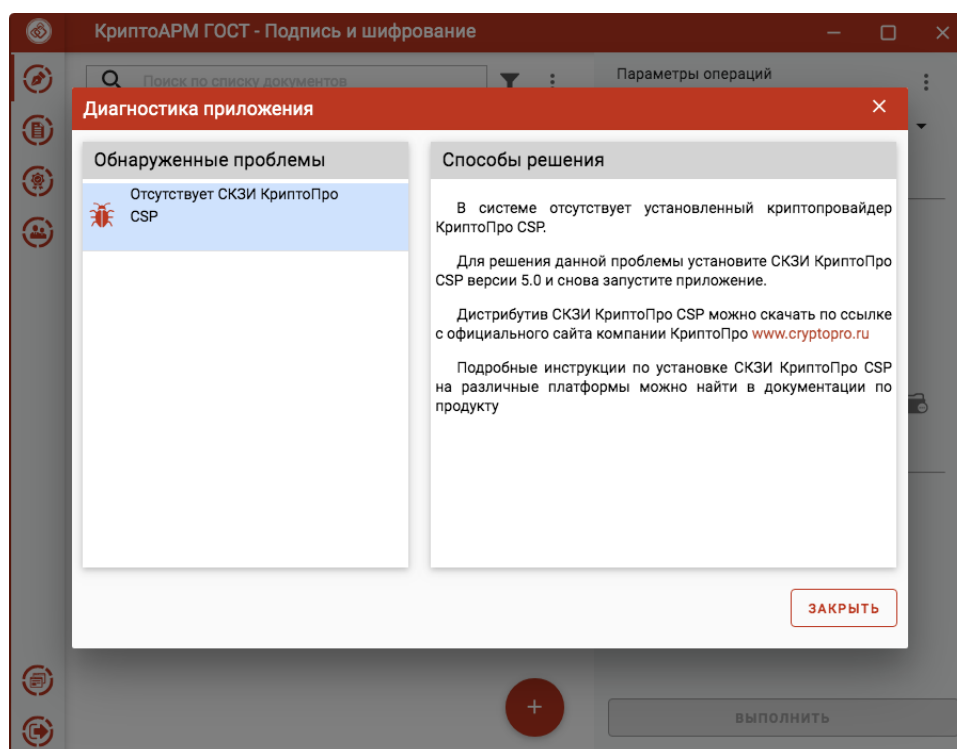


Рис. 4.1 Сообщение об отсутствии СКЗИ КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.

Дальнейшая работа приложения невозможна. Приложение можно только закрыть.

Требуется установка криптопровайдера КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.

4.2. Отсутствует лицензия на КриптоАРМ ГОСТ

Без установленной лицензии на программный продукт КриптоАРМ ГОСТ при запуске приложения возникает предупреждающее сообщение (рис. 4.2).

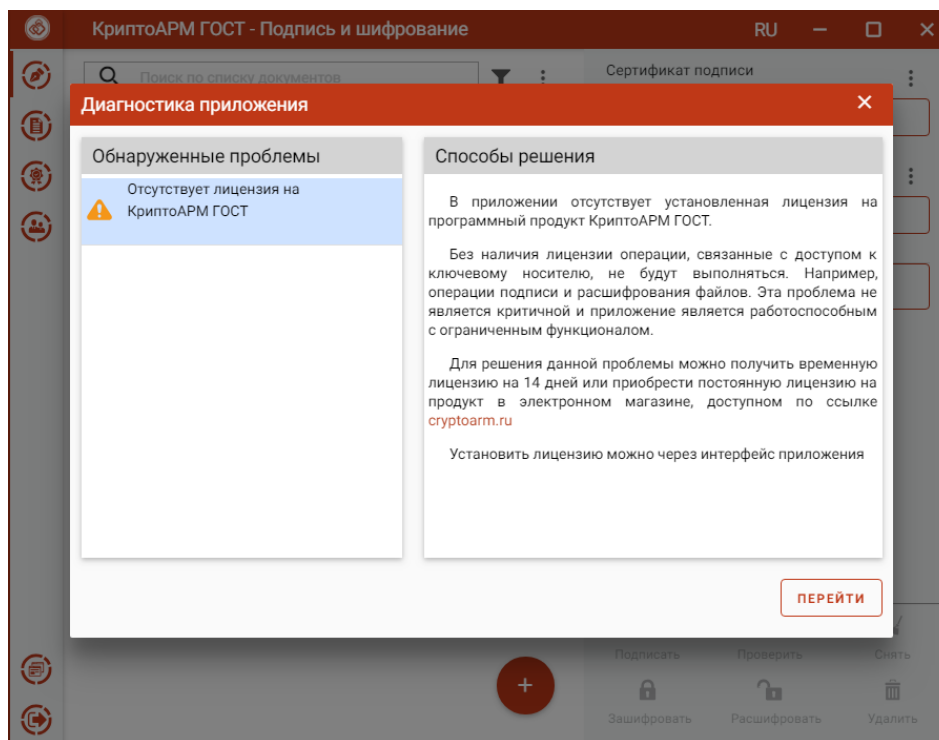


Рис. 4.3 Сообщение об отсутствии лицензии на КриптоАРМ ГОСТ

По кнопке **Перейти** происходит переход на вкладку **О программе**, где можно установить лицензию.

При закрытии мастера диагностики приложение остается работоспособным, но с ограниченным функционалом. Без лицензии не будут выполняться операции, связанные с доступом к ключу ЭП (например, подпись и расшифрование).

Инструкция по установке лицензии в приложении КриптоАРМ ГОСТ описана в п. «[Установка лицензии на программный продукт](#)» данного руководства.

4.3. Отсутствует лицензия на КриптоПро CSP

Без установленной лицензии на программный продукт КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base при запуске приложения возникает предупреждающее сообщение (рис. 4.3).

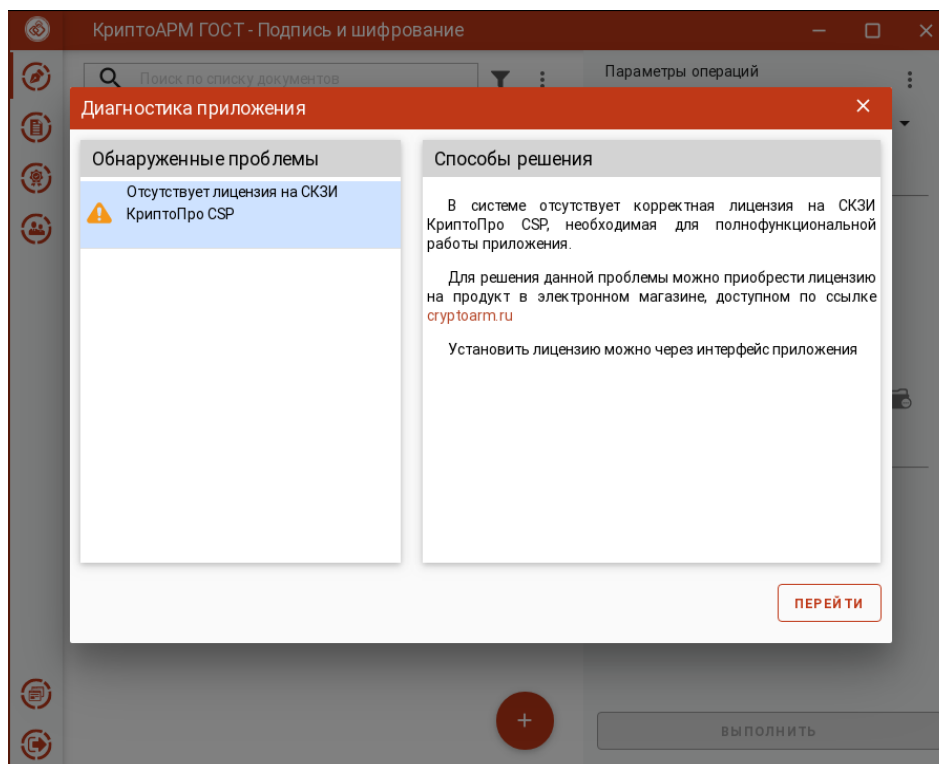


Рис. 4.4 Сообщение об отсутствии лицензии на КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.

По кнопке **Перейти** происходит переход на вкладку **О программе**, где можно установить лицензию.

При закрытии мастера диагностики приложение остается работоспособным, но с ограниченным функционалом. Без лицензии не будут выполняться операции, связанные с доступом к ключу ЭП (например, подпись и расшифрование).

4.4. НЕ ОБНАРУЖЕНЫ СЕРТИФИКАТЫ С ПРИВЯЗКОЙ К КЛЮЧЕВОМУ КОНТЕЙНЕРУ

При отсутствии в личном хранилище сертификатов, с привязкой к ключу ЭП, при запуске приложения возникает предупреждающее сообщение (рис. 4.4)

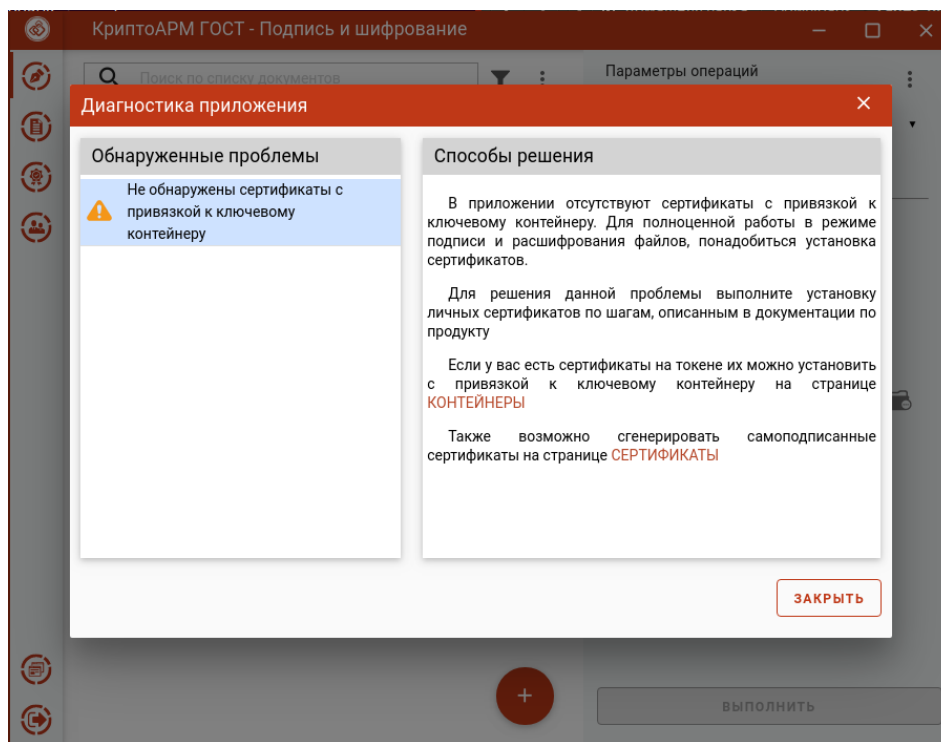


Рис. 4.4 Сообщение об отсутствии сертификатов с привязкой к ключу ЭП

Добавить личный сертификат можно несколькими способами:

- установить со стороннего носителя;
- сгенерировать запрос на сертификат и установить полученный сертификат;
- сгенерировать самоподписанный сертификат.

4.5. НЕ ЗАГРУЖЕН МОДУЛЬ TRUSTED CRYPTO

Приложение КриптоАРМ ГОСТ не работает без модуля Trusted Crypto. В таком случае при запуске приложения будет предупреждающее сообщение (рис. 4.5)

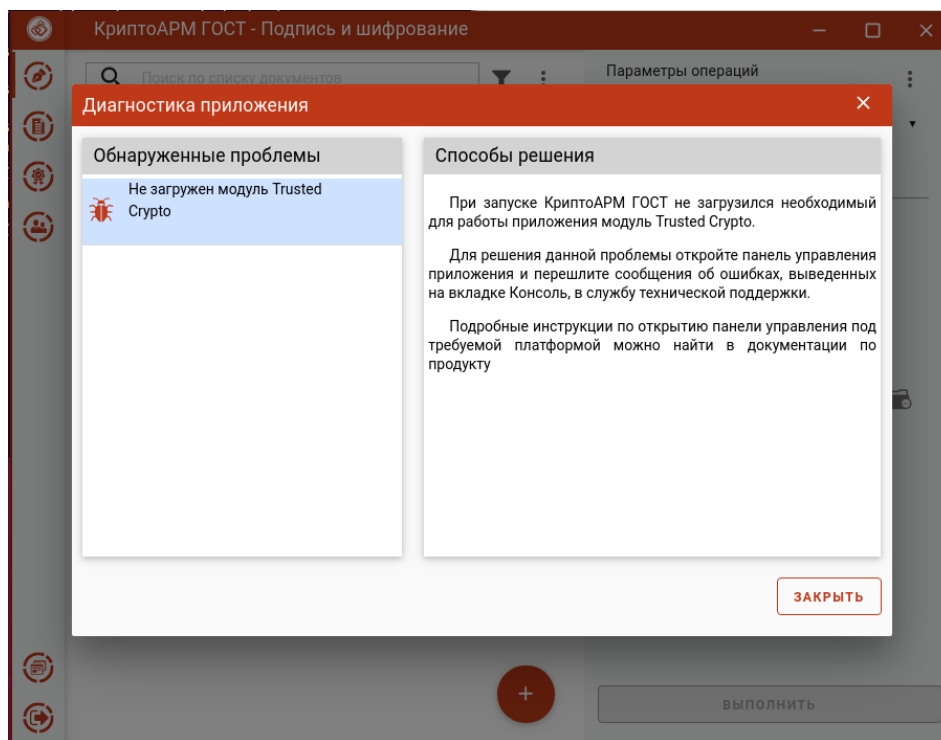


Рис. 4.5 Сообщение об ошибке в модуле Trusted Crypto

Дальнейшая работа приложения невозможна. Приложение можно только закрыть.

Для решения данной проблемы необходимо запустить приложение в консольном режиме, скопировать информацию об ошибке и связаться со специалистами технической поддержки продукта КриптоАРМ ГОСТ. Инструкция по включению консольного режима описана в п. [«Включение режима логирования и консоль управления»](#) данного руководства.

4.6. Отсутствуют установленные модули КриптоПро TSP Client 2.0/OCSP Client 2.0

При отсутствии модулей КриптоПро TSP Client 2.0 или КриптоПро OCSP Client 2.0 возникает информационное сообщение (рис. 4.6)

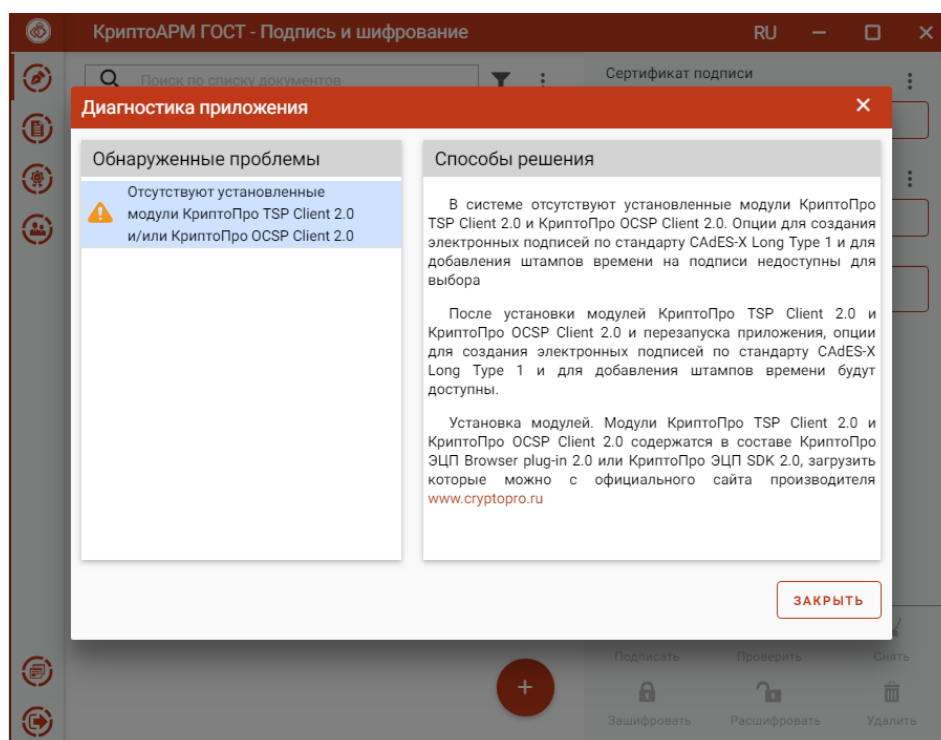


Рис. 4.6 Сообщение об отсутствии установленных модулей КриптоПро TSP/OCSP Client 2.0

Приложение остается работоспособным, но без возможности создавать усовершенствованную подпись или подпись со штампом времени.

Для создания усовершенствованной подписи требуется установка модулей КриптоПро TSP Client 2.0 и КриптоПро OCSP Client 2.0.

5. Включение режима логирования и консоль управления

Примечание. Режим логирования допускается использовать только в целях устранения неисправностей и не должен использоваться при обработке реальных данных.

Приложение КриптоАРМ ГОСТ построено на основе браузера, в котором исполняются скрипты, написанные на языке JavaScript и отображается интерфейс приложения. Ошибки, которые возникают при работе интерфейсной части приложения, связанные с проблемами подключения модулей и других компонент можно отследить в консоли управления, которую предоставляет браузер.

Открыть браузерную консоль приложения КриптоАРМ ГОСТ можно, запустив приложение из командной строки и указав параметр - devtools. Данная команда открывает окно с инструментарием для веб-разработки, где одной из вкладок будет представление консоли.

Для более глубокого анализа причин возникновения ошибок используется включение режима логирования, то есть сохранение служебной информации о выполненных операциях в текстовый файл. Данный режим включается указанием параметра - logcrypto при запуске приложения из командной строки.

Для получения доступа к дополнительной панели управления приложением и включением режима логирования, в терминале ОС Linux нужно ввести команду (рис. 5.1):

`/opt/cryptoarm_gost/cryptoarm-gost devtools logcrypto`

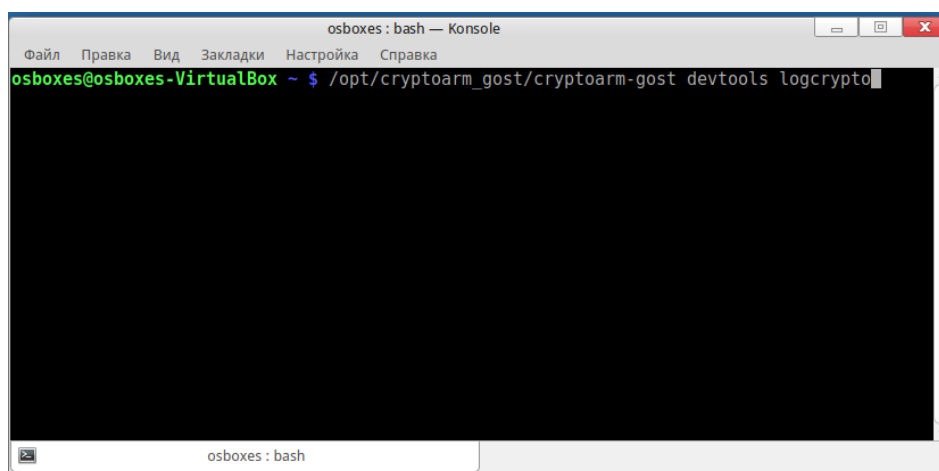
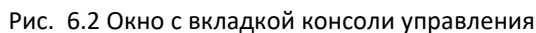


Рис. 6.1 Окно терминала

При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне на вкладке Console отобразится текст ошибки (рис. 5.2).



Журнал логирования представляет собой текстовый файл `cryptoarm_gost.log`, который располагается в каталоге пользователя в папке `.Trusted`.

6. Использование приложения в замкнутой программной среде ОС Astra Linux Special Edition

Для установки КриптоАРМ ГОСТ в замкнутой программной среде (ЗПС) ОС Astra Linux SpecialEdition необходимо:

- скопировать ключ `trusted_pub_key.gpg` в папку `/etc/digisig/keys` (от имени учетной записи администратора через механизм `sudo`);
- обновить диски оперативной памяти с помощью следующей команды:
`sudo update-initramfs -u -k all`
- выполнить перезагрузку системы.

Примечание. Настройка и использование ЗПС должны осуществляться в соответствии с эксплуатационной документацией на ОС Astra Linux Special Edition.

7. Часто встречающиеся проблемы

7.1. НЕ ЗАПУСКАЕТСЯ ПРИЛОЖЕНИЕ НА DEV СИСТЕМЕ

Надо установить библиотеку libgconf-2.s:o.4

```
sudo apt-get install libgconf-2-4
```

7.2. КРИПТОАРМ ГОСТ ЗАВИСАЕТ НА СТАТУСЕ «ПОЖАЛУЙСТА, ПОДОЖДИТЕ...»

Программа зависает на статусе «Пожалуйста, подождите...» при попытке доступа к разделам «Подпись и шифрование» или «Сертификаты». Лицензии при этом действительные.

Возможно установили (потом удалили или нет) другой криптопровайдер, отличный от КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base — будет конфликт. Нужно удалить другой криптопровайдер, потом удалить файл настроек. Для этого нужно закрыть программу ("Выход" в меню или в трее), перейти в каталог пользователя в папку .Trusted\CryptoARM GOST\ и удалить файл settings.json.

7.3. НЕ ИМПОРТИРУЮТСЯ КОРНЕВЫЕ, ПРОМЕЖУТОЧНЫЕ СЕРТИФИКАТЫ, СОС НА ЛИНУКС:

Особенность для пользователей ОС на платформе Альт 64bit- Альт Рабочая Станция 8/9, Альт Рабочая Станция К 8/9, . Альт 8/9 СП, Альт Образование 8/9.

Нужно установить сертификаты через команды КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.