127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро CSP Версия 5.0 R3 КС1 (исполнение 1-Base) Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux

ЖТЯИ.00101-03 91 03
Листов 49

2024 г

© ООО «КРИПТО-ПРО», 2000-2024. 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 R3 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

Перечень определений и сокращений . . . **6**

1 Основные технические данные и характеристики СКЗИ . . . **7**
1.1 Программно-аппаратные среды функционирования . . . 7
1.2 Ключевые носители . . . 8

2 Установка и удаление СКЗИ . . . **9**
2.1 Перечень и назначение пакетов ПО СКЗИ . . . 9
2.2 Установка СКЗИ с помощью графического инсталлятора . . . 12
2.3 Установка СКЗИ из командной строки . . . 18
2.4 Установка и настройка СКЗИ с помощью КриптоПро Мастер . . . 18
2.5 Установка дополнительного ПО для работы с ключевыми носителями . . . 21
2.6 Удаление СКЗИ . . . 21

3 Обновление СКЗИ . . . **23**

4 Настройка и использование СКЗИ . . . **24**
4.1 Интерфейс СКЗИ . . . 24
4.2 Утилита настройки СКЗИ и конфигурационный файл . . . 24
4.3 Ввод серийного номера лицензии . . . 24
4.4 Настройка оборудования СКЗИ . . . 25
4.5 Установка параметров журналирования . . . 25
4.6 Настройка криптопровайдера по умолчанию . . . 26
4.7 Включение режима усиленного контроля использования ключей . . . 26
4.8 Настройка параметров алгоритмов . . . 26
4.9 Использование СКЗИ с nginx/Apache . . . 27
4.10 Настройка клиентского компонента КриптоПро HSM . . . 28
4.10.1 Настройка ПО СКЗИ КриптоПро CSP . . . 28
4.10.2 Настройка stunnel . . . 29
4.10.3 Регистрация пользователя на ПАКМ . . . 30
4.10.4 Запуск stunnel . . . 31

5 Работа в ОС Astra Linux . . . **32**
5.1 Настройка работы с веб-сервером Apache . . . 32
5.2 Использование СКЗИ в замкнутой программной среде ОС Astra Linux Special Edition . . . 32
5.3 Модуль Check . . . 33

6 Состав и назначение компонент ПО СКЗИ . . . **34**
6.1 Базовые модули СКЗИ . . . 34
6.2 Модули подсистемы программной среды функционирования криптосредства (СФ) . . . 35

7 Требования по обеспечению безопасности при эксплуатации СКЗИ . . . **40**
7.1 Организационно-технические меры защиты от НСД . . . 40
7.2 Дополнительные настройки ОС . . . 40
7.2.1 Ограничение доступа пользователей и настройки пользовательского окружения . . . 41
7.2.2 Ограничения при монтировании файловых систем . . . 41
7.2.3 Настройка сетевых сервисов . . . 41
7.2.4 Ограничение количества «видимой извне» информации о системе . . . 42
7.2.5 Настройка подсистемы протоколирования и аудита . . . 43

8 Требования по криптографической защите **44**

Приложение А. Управление протоколированием **47**

Аннотация

Настоящее руководство содержит общее описание средства криптографической защиты информации «КриптоПро CSP» версия 5.0 R3 КС1 (исполнение 1-Base) и рекомендации по использованию СКЗИ под управлением операционных систем Linux.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» версия 5.0 R3 КС1 (исполнение 1-Base) под управлением ОС Linux, должны разрабатываться с учетом требований настоящего документа.

Перечень определений и сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
CTL	Список доверенных сертификатов (Certificate Trust List)
HDD	Жесткий магнитный диск (Hard Disk Drive)
SSD	Твердотельный накопитель (Solid-State Drive)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БиоДСЧ	Биологический датчик случайных чисел
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
ИС	Информационная система
МДЗ	Модуль доверенной загрузки
МП	Мобильное приложение
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПДСЧ	Программный датчик случайных чисел
ПК	Персональный компьютер
ПО	Программное обеспечение
ПЭВМ	Персональная электронно-вычислительная машина
СВТ	Средства вычислительной техники
СКЗИ	Средство криптографической защиты информации
СФ	Среда функционирования
УЦ	Удостоверяющий Центр
ЦР	Центр Регистрации
ЦС	Центр Сертификации
ЭД	Электронный документ
ЭП	Электронная подпись

1 Основные технические данные и характеристики СКЗИ

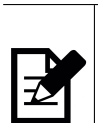
1.1 Программно-аппаратные среды функционирования

СКЗИ «КриптоПро CSP» версия 5.0 R3 КС1 (исполнение 1-Base) функционирует в следующих группах программно-аппаратных сред:

LSB Linux

Дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base (LSB) ISO/IEC 23360

CentOS 7 (x86, x64, POWER, ARM, ARM64)
CentOS 8 (x64, POWER, ARM64)
ТД ОС АИС ФССП России (GosLinux) (x86, x64)
РЕД ОС 7.1/7.2/7.3/8 (x86, x64, ARM64)
Oracle Linux 6 (x86, x64)
Oracle Linux 7 (x64)
Oracle Linux 8/9 (x64, ARM64)
OpenSUSE Leap 15 (x86, x64, ARM, ARM64)
AlterOS (x64)
SUSE Linux Enterprise Server 12/15, Desktop 12/15 (x64, POWER, ARM64)
Red Hat Enterprise Linux 6 (x86, x64)
Red Hat Enterprise Linux 7/8/9 (x64, POWER, ARM64)
Check Point GAiA (x86, x64)
Синтез-ОС.РС (x86, x64)
ПК «СинтезМ-Клиент» в составе КП «ЗОС «СинтезМ» (x64)
ПК «СинтезМ-Сервер» в составе КП «ЗОС «СинтезМ» (x64)
КП «ОС «СинтезМ-К» (x64)
Ubuntu 14.04/16.04 (x86, x64, ARM, ARM64)
Ubuntu 18.04 (x64, ARM, ARM64)
Ubuntu 20.04/22.04 (x64, ARM, ARM64, RISC-V)
Halo OS (x64)
Linux Mint 20/21 (x86, x64)
Debian 8/9/10/11/12 (x86, x64, ARM, ARM64, MIPS)
Лотос (x86, x64)
Astra Linux Special Edition, Common Edition (x64, ARM, ARM64, MIPS, Эльбрус, подсистема x86)
МСВСфера 6.3 Сервер (x64, ARM64)
ThinLinux 2 (x64)
ЕМИАС 1.0 (x64)
Мурена 1.4 (ARM9)
ОС ОН «Стрелец» (x64)
ОС «Атлант» (x64)
ОСОН «ОСнова» 2.0 (x64)



Примечание. При эксплуатации СКЗИ необходимо учитывать, что порядок и сроки эксплуатации операционных систем, в среде которых функционирует СКЗИ, определяются производителями операционных систем. Использование СКЗИ под управлением ОС, для которых не выпускаются обновления, не допускается.

1.2 Ключевые носители

Перечень поддерживаемых ключевых носителей в зависимости от программно-аппаратной платформы отражен в ЖТЯИ.00101-03 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 Установка и удаление СКЗИ

Установка, удаление и обновление ПО осуществляется от имени пользователя, имеющего права администратора — под учётной записью root или с использованием команды sudo.

СКЗИ КриптоПро CSP требует следующей последовательности установки: сначала устанавливается провайдер, затем устанавливаются остальные модули, входящие в состав комплектации.

В ОС Linux для установки, удаления и обновления ПО применяются пакеты (packages). Пакет — архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, использующиеся инсталлятором для конфигурирования среды. В операционных системах Linux используется менеджер пакетов RPM (Red Hat Package Manager), который является гибким инструментом для установки, удаления, обновления и сборки программных пакетов. Пакеты, представленные в виде файла с расширением .rpm, содержат в себе непосредственно файлы ПО и информацию для конфигурирования среды.

Файлы из пакетов устанавливаются в `/opt/cprocsp`.

2.1 Перечень и назначение пакетов ПО СКЗИ

Пакет дистрибутива КриптоПро CSP содержит в себе вложенные пакеты, обеспечивающие работу разных подсистем криптопровайдера. При установке КриптоПро CSP можно выборочно устанавливать эти пакеты. При этом некоторые пакеты являются обязательными и будут установлены в любом случае, некоторые — дополнительными, и их можно устанавливать или не устанавливать в зависимости от предполагаемого использования КриптоПро CSP.

Пакеты зависят друг от друга, поэтому должны устанавливаться по порядку с учётом этих зависимостей, а удаляться в обратном порядке. Условно можно считать правильным порядком тот, который описан в таблице зависимостей и назначения пакетов (см. табл. 1).



Примечание. Конечный состав пакетов дистрибутива зависит от используемой ОС.

Пакеты могут быть независимыми от архитектуры (noarch (для RPM-дистрибутивов) или all (для DEB-дистрибутивов) в имени файла пакета), тогда они устанавливаются на любую архитектуру. Пакеты могут быть предназначены для следующих архитектур:

- AMD64 (x64) — x86_64, amd64;
- ARM64 — aarch64, arm64;
- ARM — armhf;
- Эльбрус (e2k) — e2k, e2kv4, e2k-4c, e2k-8c;
- IA32 (x86) — i386, i486, i686;
- MIPS — mipsel;
- POWER — ppc, ppc64;
- RISC-V — riscv64.

Часто 64-битные ОС одновременно поддерживают и 32-битные приложения, и 64-битные, тогда при необходимости можно устанавливать оба комплекта. Исключением являются драйверы — они устанавливаются в точном соответствии с архитектурой ядра ОС.

В ОС Linux модули ядра не обладают бинарной совместимостью, они привязаны к конкретной версии ядра ОС. Поэтому модуль ядра поставляется в виде пакета .src.rpm. Такой тип пакета позволяет собрать модуль для нужной версии ядра. Для его установки следует при помощи rpmbuild собрать из пакета .src.rpm обычный

пакет .rpm, а затем установить пакет .rpm так же, как и другие пакеты.

На большинстве дистрибутивов сборку пакета .rpm можно осуществить командой:

```
rpmbuild --rebuild --define "kernel_release `uname -r`" <путь к файлу пакета>
```

Для сборки требуется, чтобы на машине были установлены средства сборки (компилятор), а также заголовочные файлы ядра. Заголовочные файлы ядра должны находиться в /lib/modules/ и обычно их можно установить в составе соответствующего пакета из репозитория дистрибутива.

Так как наличие средств отладки и разработки на системах, в которых эксплуатируется СКЗИ, недопустимо, администратор (разработчик СФ) должен собрать пакет на специальном выделенном рабочем месте и обеспечить его доверенную установку в целевую систему.

Таблица 1. Зависимости и назначения пакетов

Имя пакета	Зависимости	Назначение пакета
Пакеты для предварительной установки		
cprocsp-compat-altlinux		Пакет совместимости с ОС AltLinux, устанавливается первым — до lsb-cprocsp-base
cprocsp-compat-armhf		Пакет совместимости с архитектурой ARM с аппаратным FPU, устанавливается первым — до lsb-cprocsp-base
cprocsp-compat-debian		Пакет совместимости с ОС Debian/Ubuntu (не LSB), уснаваливается первым — до lsb-cprocsp-base
cprocsp-compat-gaia		Пакет совместимости с ОС Check Point GAiA, устанавливается первым — до lsb-cprocsp-base
cprocsp-compat-mcst		Пакет совместимости с ОС Эльбрус, устанавливается первым — до lsb-cprocsp-base
cprocsp-compat-suse		Пакет совместимости с ОС SUSE, устанавливается первым - до lsb-cprocsp-base
sobol		Драйвер для ПАК Соболь, требуется при наличии устройства
accord_random		Драйвер ДСЧ Аккорд, требуется при наличии устройства
ifd-rutokens		Драйвер для Rutoken S, требуется при наличии устройства
Обязательные пакеты		
lsb-cprocsp-base		Базовый пакет КриптоПро CSP (устанавливается первым, если не нужны compat-пакеты)
lsb-cprocsp-rdr	lsb-cprocsp-base	Модуль поддержки основных приложений, считывателей и ДСЧ
lsb-cprocsp-kc1	lsb-cprocsp-rdr	Провайдер класса КС1
lsb-cprocsp-kc2	lsb-cprocsp-rdr	Провайдер класса КС2, устанавливается только там, где в этом есть необходимость; в этом случае lsb-cprocsp-kc1 обычно не ставится

lsb-cprocsp-capilite	lsb-cprocsp-rdr, lsb-cprocsp-kc1	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS...)
Дополнительные пакеты		
cprocsp-apache-modssl		Пакет для работы SSL в Apache
cprocsp-certprop	cprocsp-rdr-pcsc, lsb-cprocsp-capilite	Пакет для автоматической установки сертификатов из контейнера
cprocsp-legacy	lsb-cprocsp-capilite	Дополнительные библиотеки КриптоПро CSP для обеспечения обратной совместимости
cprocsp-nginx	lsb-cprocsp-capilite	Сервер nginx с поддержкой алгоритмов шифрования ГОСТ
cprocsp-pki-cades		Пакет с инструментарием разработчика для создания клиентских и серверных приложений для работы с ЭП (в соответствии с CAdES) с использованием российских криптографических алгоритмов
cprocsp-pki-phpcades	cprocsp-pki-cades	Расширение пакета cprocsp-pki-cades для PHP
cprocsp-pki-plugin	cprocsp-rdr-gui-gtk	Пакет для работы КриптоПро ЭЦП Browser plug-in
cprocsp-rdr-cryptoki	lsb-cprocsp-capilite	Модуль поддержки ключей PKCS#11
cprocsp-rdr-relay	lsb-cprocsp-rdr	Модуль поддержки ключей других криптопровайдеров
lsb-cprocsp-import-ca-certs	lsb-cprocsp-capilite	Модуль импорта корневых сертификатов ОС в хранилище корневых сертификатов доверенных ЦС
lsb-cprocsp-rcrypt	lsb-cprocsp-rdr	Пакет с библиотекой libcrypt для шифрования/ расшифрования с поддержкой функции диверсификации PBKDF2 с использованием в качестве PRF функции HMAC_GOSTR3411_512
cprocsp-rdr-gui-gtk	lsb-cprocsp-rdr	Графический интерфейс для диалоговых операций
cprocsp-rdr-pcsc	lsb-cprocsp-rdr	Модули поддержки PCSC-считывателей, смарт-карт
lsb-cprocsp-pkcs11	lsb-cprocsp-rdr	Модуль поддержки PKCS#11
lsb-cprocsp-devel	lsb-cprocsp-base	Пакет для разработчика приложений, использующих КриптоПро CSP
cprocsp-drv		Драйверная библиотека
cprocsp-drv-devel	lsb-cprocsp-devel	Пакет для разработчика драйверов
cprocsp-curl	lsb-cprocsp-capilite	Пакет для работы Curl с поддержкой российских алгоритмов
cprocsp-cptools-gtk	lsb-cprocsp-capilite	Графическое приложение для доступа к основным функциям и настройкам КриптоПро CSP
cprocsp-rdr-cloud	lsb-cprocsp-capilite	Модуль взаимодействия с КриптоПро DSS — КриптоПро Cloud CSP
cprocsp-stunnel	lsb-cprocsp-capilite	Универсальный SSL/TLS туннель
cprocsp-stunnel-msspi	lsb-cprocsp-capilite	Универсальный SSL/TLS туннель с поддержкой интерфейса msspi

cprocsp-xer2print	lsb-cprocsp-base	Скрипты и xsl-шаблоны для конвертации xer-файлов в pdf/ps/html
lsb-cprocsp-ca-certs	lsb-cprocsp-capilite	Корневые сертификаты доверенных ЦС
cprocsp-ipsec-devel	lsb-cprocsp-devel	Пакет для разработчика приложений, использующих КриптоПро IPsec
cprocsp-ipsec-esp	lsb-cprocsp-rdr	Загружаемый модуль ядра IPsec ESP
cprocsp-ipsec-genpsk	lsb-cprocsp-rdr	Модули генерации PSK
cprocsp-ipsec-ike	lsb-cprocsp-rdr	Динамические библиотеки уровня пользователя
cprocsp-ktls	cprocsp-drv	Пакет поддержки TLS уровня ядра ОС
Поддержка считывателей/ДСЧ		
lsb-cprocsp-rdr-accord	lsb-cprocsp-rdr	Модуль поддержки Аккорд-АМДЗ
lsb-cprocsp-rdr-ancud	lsb-cprocsp-rdr	Модуль поддержки устройств производства АНКАД
lsb-cprocsp-rdr-crypton	lsb-cprocsp-rdr	Модуль поддержки АПМДЗ КРИПТОН-ЗАМОК (АНКАД)
lsb-cprocsp-rdr-maxim	lsb-cprocsp-rdr	Модуль поддержки ДСЧ в составе АПМДЗ МАКСИМ М1
lsb-cprocsp-rdr-sobol	lsb-cprocsp-rdr	Модуль поддержки ПАК Соболь
lsb-cprocsp-rdr-vityaz	lsb-cprocsp-rdr	Модуль поддержки ДСЧ в составе АПМДЗ Витязь-А
Поддержка ключевых носителей		
cprocsp-rdr-cpfkc	cprocsp-rdr-pcsc	Модуль поддержки ФКН с поддержкой SESPAKE
cprocsp-rdr-edoc	cprocsp-rdr-pcsc	Модуль поддержки платформы eDoc (УЛГ)
cprocsp-rdr-emv	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт Gemalto (EMV)
cprocsp-rdr-esmart	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт и токенов ESMART
cprocsp-rdr-infocrypt	cprocsp-rdr-pcsc	Модуль поддержки токенов InfoCrypt
cprocsp-rdr-inpaspot	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт Alioth
cprocsp-rdr-jacarta	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт и токенов JaCarta
cprocsp-rdr-kst	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт MorphoKST
cprocsp-rdr-mskey	cprocsp-rdr-pcsc	Модуль поддержки токенов Multisoft MS_Key
cprocsp-rdr-novacard	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт Novacard
cprocsp-rdr-rosan	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт Rosan
cprocsp-rdr-rutoken	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт и токенов Рутокен

2.2 Установка СКЗИ с помощью графического инсталлятора

Для установки КриптоПро CSP необходимо распаковать архив с дистрибутивом средствами ОС и перейти в каталог с распакованной папкой или использовать команду:

```
tar -zxf <имя_дистрибутива>.tgz && cd <имя_дистрибутива>
```

Для установки СКЗИ через графический интерфейс запустите скрипт `install_gui.sh`, входящий в

состав дистрибутива:

```
sudo ./install_gui.sh
```

Откроется приветственное окно инсталлятора СКЗИ (см. рис. 1).

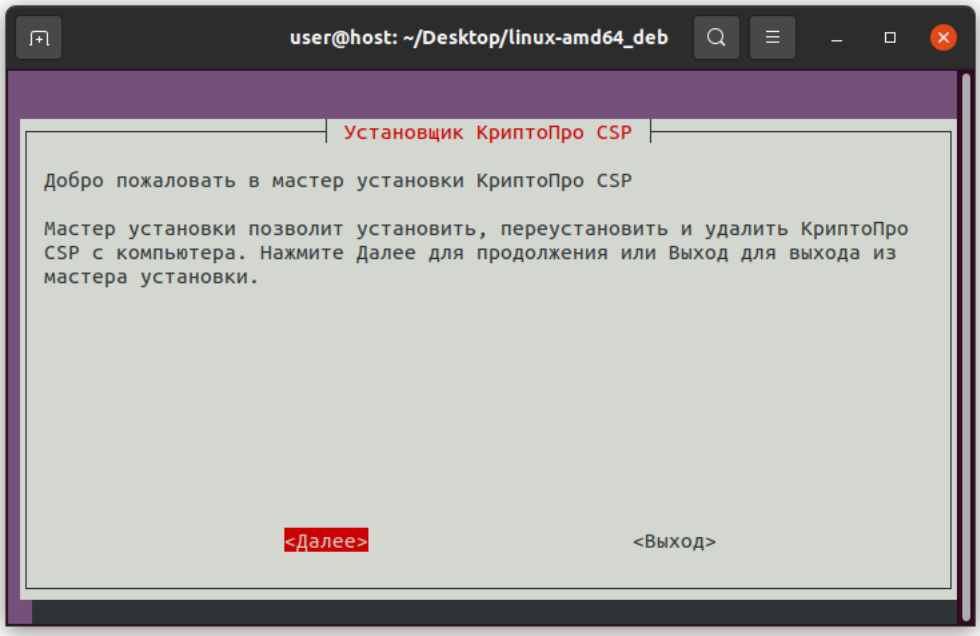


Рисунок 1. Инсталлятор СКЗИ

Нажмите **Далее** для продолжения установки СКЗИ. В следующем окне выводится краткое описание пакетов, доступных для установки (подробнее о пакетах см. табл. 1). Отметьте пакеты, которые будут нужны при работе с СКЗИ, или оставьте выбор по умолчанию и нажмите **Продолжить** (см. рис. 2).

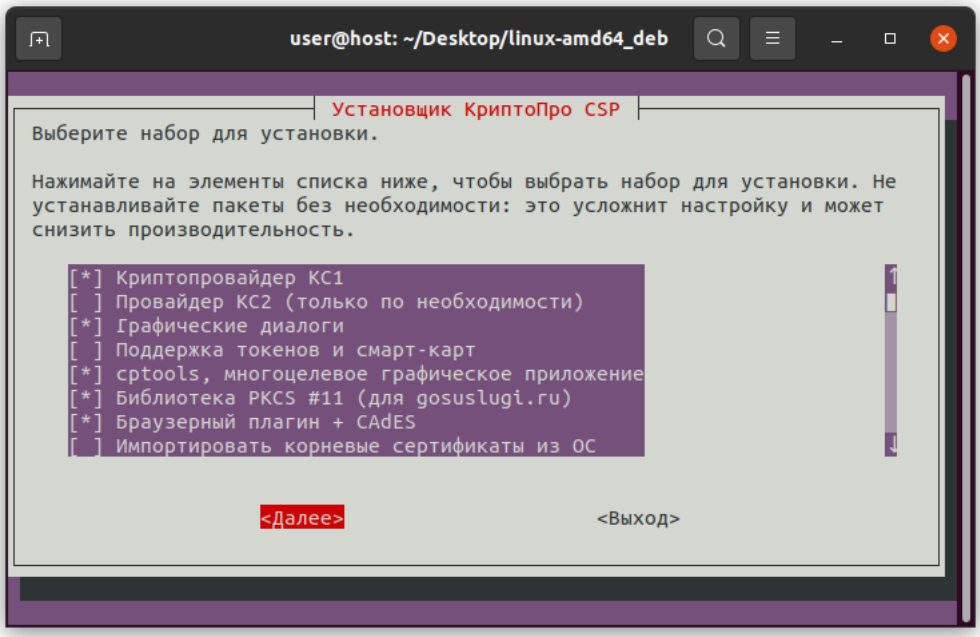


Рисунок 2. Выбор устанавливаемых пакетов СКЗИ

Далее инсталлятор выведет список устанавливаемых модулей (см. рис. 3). Нажмите кнопку **Установить** для начала установки.

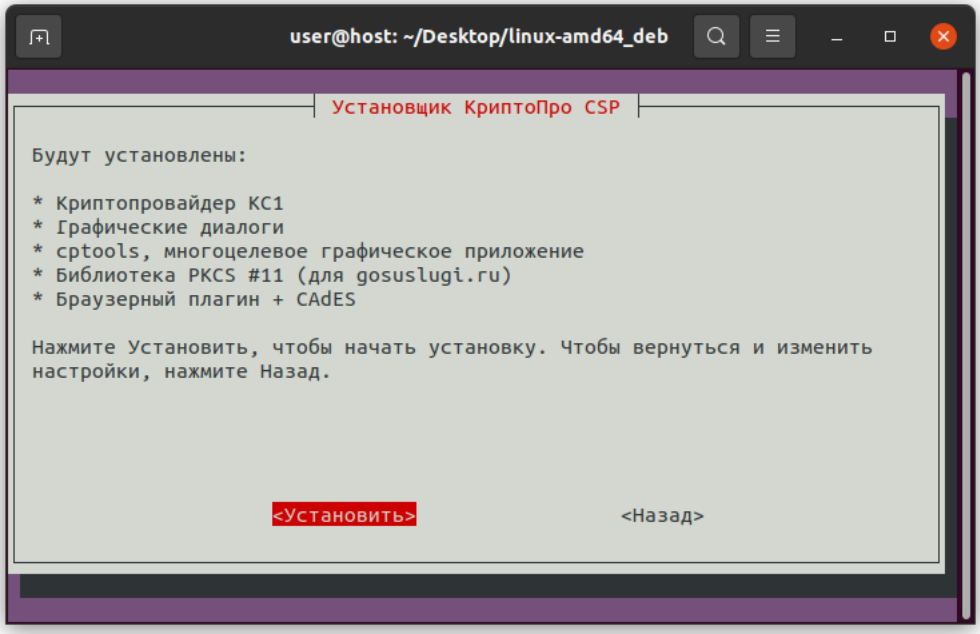


Рисунок 3. Подтверждение списка устанавливаемых пакетов СКЗИ

При успешной установке выводится соответствующее сообщение (см. рис. 4).

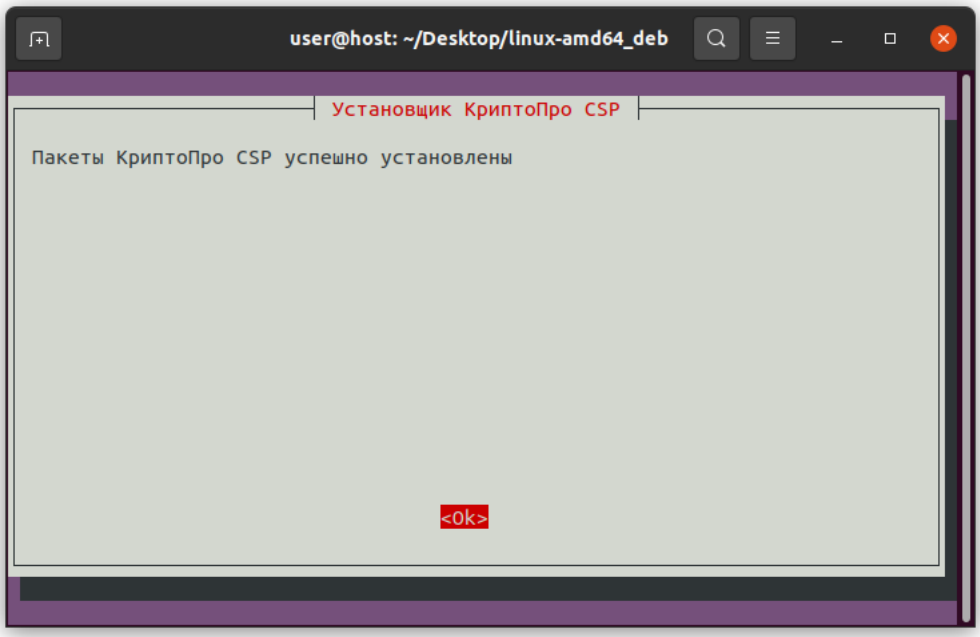


Рисунок 4. Завершение установки СКЗИ

В следующем окне инсталлятором будет предложено ввести серийный номер лицензии (см. рис. 5).

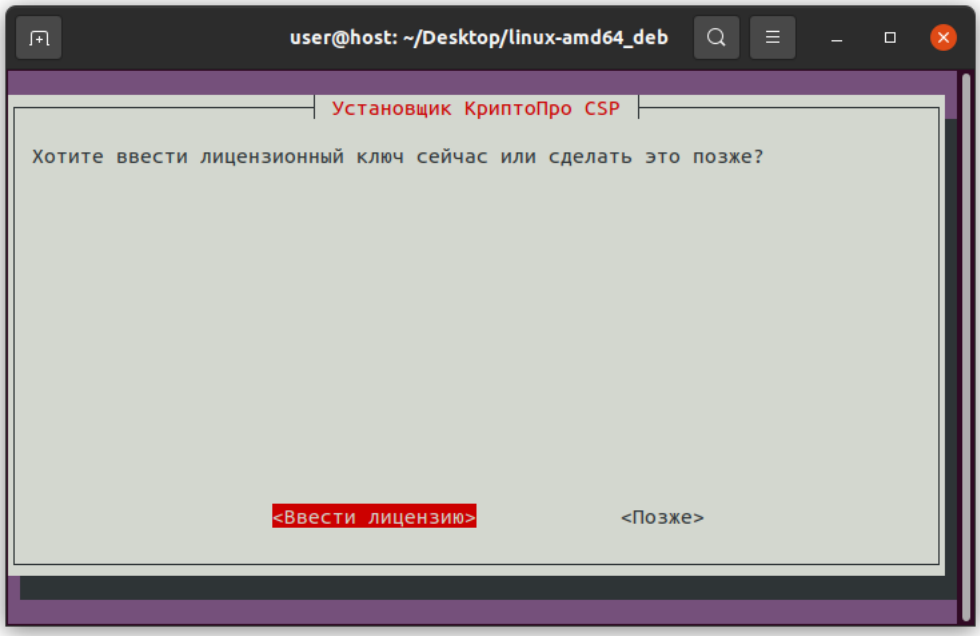


Рисунок 5. Окно предложения ввода лицензионного ключа

Нажмите кнопку **Ввести лицензию** для ввода лицензионного ключа. В открывшемся окне введите серийный номер лицензии и нажмите **Ввести** (см. рис. 6).

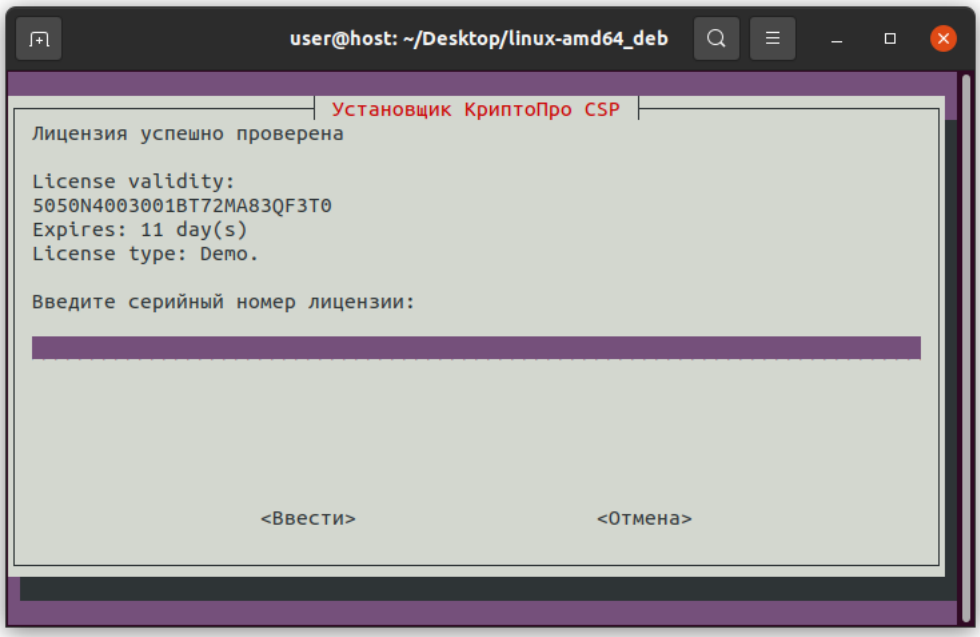


Рисунок 6. Ввод лицензионного ключа КриптоПро CSP

Далее инсталлятор выведет информацию об успешном применении лицензии (см. рис. 7).

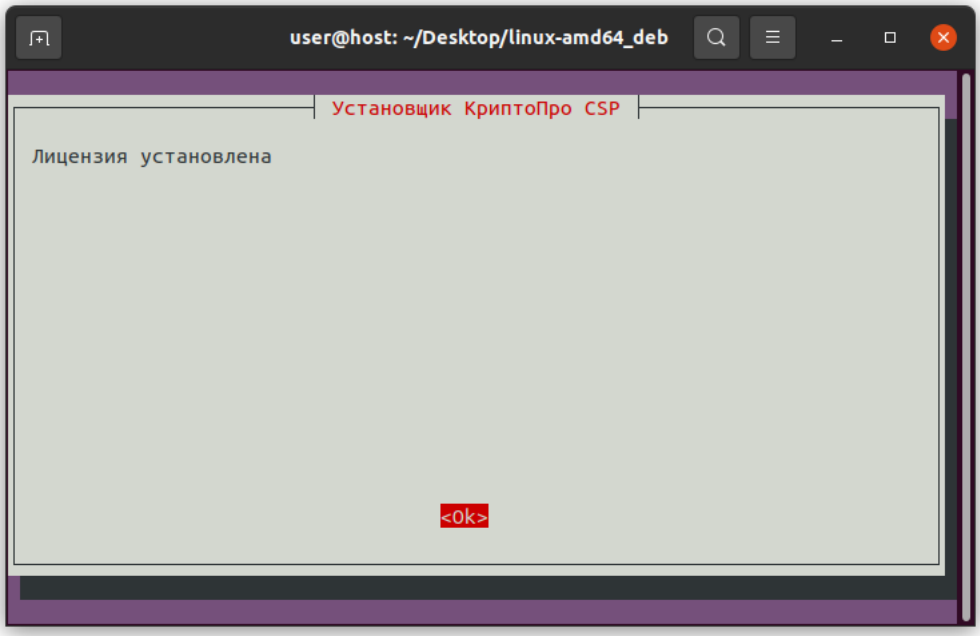


Рисунок 7. Успешный ввод лицензионного ключа

Графический инсталлятор после установки СКЗИ позволяет переустановить пакеты КриптоПро CSP, удалить КриптоПро CSP и ввести/проверить лицензию. Для этого необходимо запустить скрипт `install_gui.sh` и в открывшемся окне выбрать соответствующую операцию (см. рис. 8).

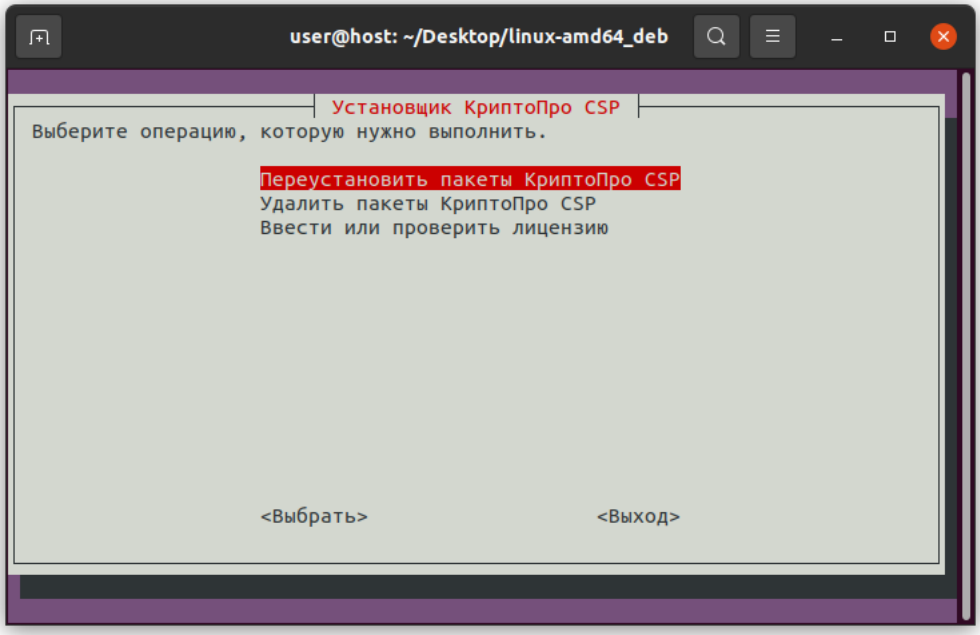


Рисунок 8. Операции с КриптоПро CSP

2.3 Установка СКЗИ из командной строки

Для установки КриптоПро CSP необходимо распаковать архив с дистрибутивом командой:

```
tar -zxf <имя_дистрибутива>.tgz && cd <имя_дистрибутива>
```

Для автоматической установки основных пакетов СКЗИ можно воспользоваться скриптом `install.sh`, входящим в состав дистрибутива:

```
sudo ./install.sh
```



Примечание. Если менеджер файлов ОС позволяет запускать ярлыки (desktop-файлы), запустите ярлык установщика: `install.desktop`.

Для установки пакета используется команда: `sudo rpm -i <файл_пакета>`

Например: `sudo rpm -i ./lsb-cprocsp-base-5.0-5.noarch.rpm`

На ОС, основанных на Debian (Debian/Ubuntu), для установки пакетов используется команда: `sudo dpkg -i <файл_пакета>`

Например: `sudo dpkg -i ./lsb-cprocsp-base_5.0-6_all.deb`



Примечание. Имя устанавливаемого/удаляемого пакета может не включать версию, например: `sudo rpm -e lsb-cprocsp-base`

2.4 Установка и настройка СКЗИ с помощью КриптоПро Мастер

Приложение КриптоПро Мастер позволяет выполнить одновременную установку и настройку КриптоПро CSP и КриптоПро ЭЦП Browser plug-in с параметрами по умолчанию с минимальными действиями пользователя.



Примечание. Для настройки и проверки работы КриптоПро ЭЦП Browser plug-in требуется установленный веб-браузер с поддержкой криптографических алгоритмов ГОСТ.

Для начала процесса установки запустите файл с приложением `cpmaster_linux.run`. Откроется приветственное окно КриптоПро Мастер. Укажите Ф. И. О. и e-mail (необходимы для учета установок) в соответствующих полях и нажмите кнопку **Начать установку** (см. рис. 9).

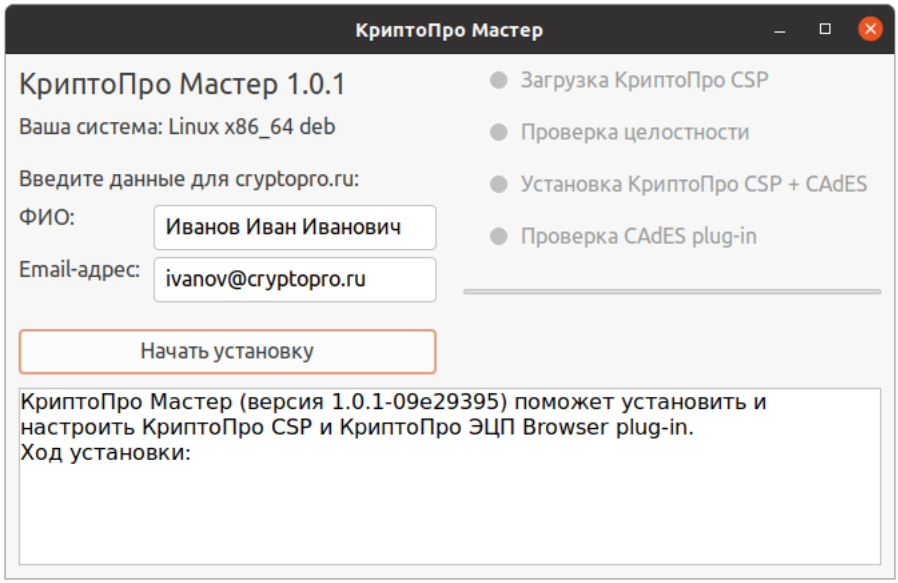


Рисунок 9. Мастер установки и настройки СКЗИ

Процесс выполнения этапов установки обозначается цветовыми индикаторами:

- красный — возникла ошибка,
- желтый — выполняется этап установки,
- зеленый — этап установки успешно завершен.

Дополнительные сведения о ходе установки, возникших ошибках и необходимых дополнительных действиях пользователя указываются в поле «Ход установки».



Примечание. Установка СКЗИ может быть осуществлена только в случае подтверждения целостности полученного дистрибутива.

Если на рабочем месте уже ранее использовалось СКЗИ КриптоПро CSP, КриптоПро Мастер автоматически проверит целостность загруженного дистрибутива с использованием утилиты `cpverify`, установленной ранее в составе СКЗИ КриптоПро CSP.

Если запуск КриптоПро Мастер выполняется на рабочем месте, где ранее не использовалось СКЗИ КриптоПро CSP (отсутствует утилита `cpverify`), или обнаружена устаревшая версия `cpverify`, необходимо **самостоятельно осуществить проверку целостности** загруженного дистрибутива с использованием утилиты `cpverify`, полученной доверенным образом (подробнее см. раздел 2 ЖТЯИ.00101-03 95 01. Правила пользования). Расположение загруженного дистрибутива, а также команда `cpverify`, которую необходимо выполнить для проверки целостности дистрибутива, указаны в поле «Ход установки». В случае успешной проверки целостности дистрибутива для продолжения установки нажмите кнопку **Подтверждаю целостность скачанного дистрибутива** (см. рис. 10).

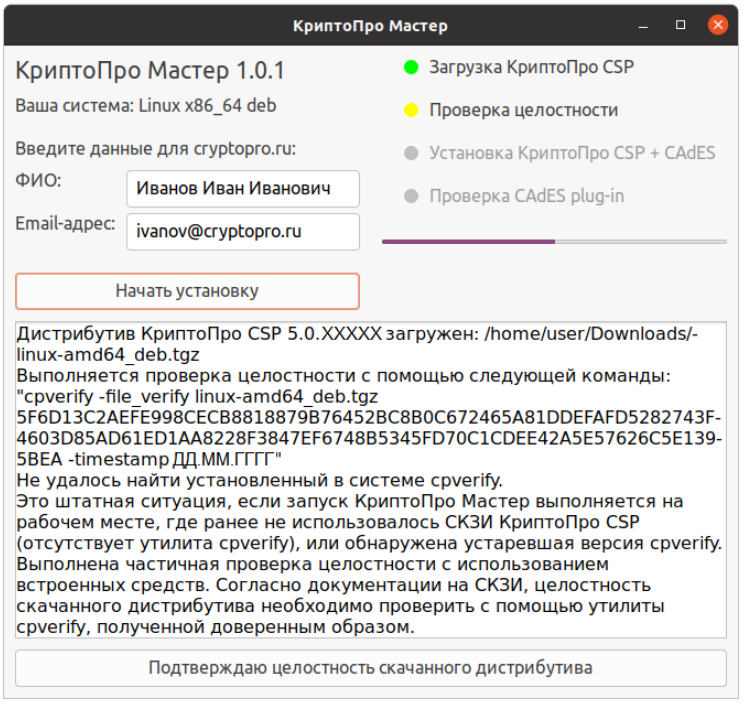


Рисунок 10. Проверка целостности загруженного дистрибутива

После успешной установки КриптоПро CSP и КриптоПро ЭЦП Browser plug-in будет выполнена настройка и проверка работы плагина в веб-браузере с поддержкой ГОСТ алгоритмов.

Если такой браузер уже установлен на рабочем месте, по завершении установки в нем автоматически будет открыта веб-страница проверки работы плагина.

Если на рабочем месте не найден веб-браузер с поддержкой ГОСТ алгоритмов, необходимо самостоятельно осуществить установку такого браузера и открыть в нем страницу проверки работы плагина, указанную в окне (см. рис. 11).

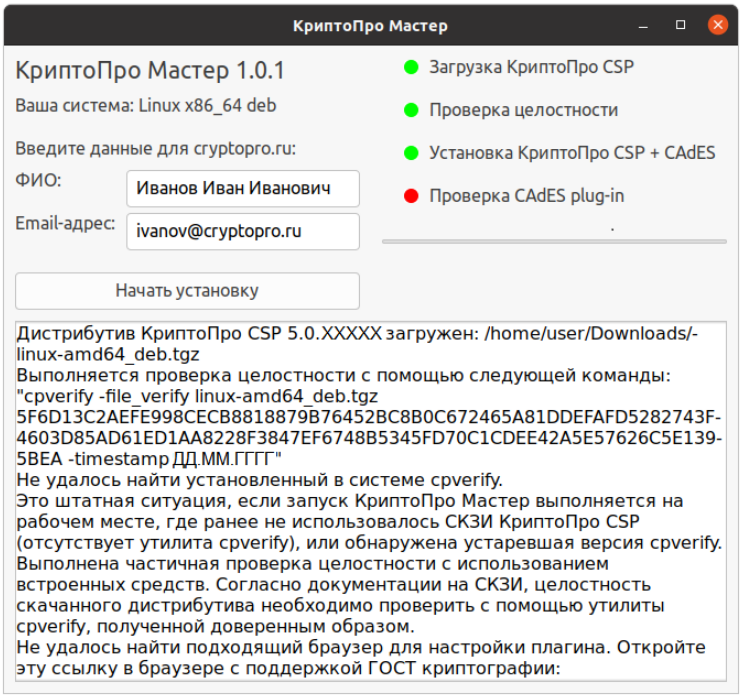


Рисунок 11. Проверка работы плагина

По результатам проверки соответствующая цветовая индикация указывает на корректность установки и настройки КриптоПро ЭЦП Browser plug-in. Также на странице проверки указываются установленные версии КриптоПро CSP и КриптоПро ЭЦП Browser plug-in и сведения об используемых ОС и браузере.

Если все индикаторы цветовые индикаторы в окне приложения КриптоПро Мастер и на странице проверки работы плагина зеленые, установка, настройка и проверка работы плагина были выполнены успешно.

2.5 Установка дополнительного ПО для работы с ключевыми носителями

Для корректной работы с некоторыми ключевыми носителями необходима установка дополнительного программного обеспечения:

- pcscd — пакет обеспечения доступа к смарт-картам через PC/SC;
- libccid — драйвер PC/SC для считывателей смарт-карт USB CCID;
- Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0, Рутокен TLS — библиотека для работы через PKCS#11 интерфейс;
- JaCarta-2 ГОСТ — программный комплекс "Единый клиент JaCarta";
- ESMART Token ГОСТ — ESMART PKI Client;
- Рутокен S — пакет ifd-rutokens расположен в архиве с дистрибутивом (см. табл. 1).



Примечание. Для работы с ключевыми носителями служба pcscd должна быть запущена.

2.6 Удаление СКЗИ

Для удаления СКЗИ КриптоПро CSP используйте скрипт `uninstall.sh`:

```
sudo ./uninstall.sh
```

Для удаления пакета используется команда: `sudo rpm -e <имя_пакета>`

Например: `sudo rpm -e lsb-cprocsp-base-5.0-5`

На ОС, основанных на Debian (Debian/Ubuntu), для удаления пакетов используется команда:

`sudo dpkg -P <имя_пакета_без_версии>`

Например: `sudo dpkg -P lsb-cprocsp-base`



Примечание. Удаление КриптоПро CSP можно произвести с использованием графического интерфейса.

3 Обновление СКЗИ

Для обновления ПО СКЗИ на ОС Linux необходимо:

- запомнить текущую конфигурацию КриптоПро CSP;
  - набор установленных пакетов;
  - настройки провайдера (рекомендуется сохранить текущий конфигурационный файл `/etc/opt/cprocsp/config[64].ini`);
- удалить все пакеты СКЗИ;
- установить аналогичные новые пакеты СКЗИ;
- при необходимости внести изменения в настройки (например, по результату сравнения старого и нового config[64].ini).



Примечание. Ключи и сертификаты сохраняются автоматически.

4 Настройка и использование СКЗИ

4.1 Интерфейс СКЗИ

Доступ к функциям и настройкам СКЗИ возможен как с использованием утилит командной строки (cpconfig, cryptcp, certmgr, stunnel, cpverify, csptest) путём запуска команд для утилит через терминал, так и с помощью графического приложения **Инструменты КриптоПро** (cptools), предоставляющего интерфейс управления ключевыми носителями, контейнерами, сертификатами, CRL и настройками СКЗИ, создания/проверки ЭП, шифрования/расшифрования файлов.

Подробные описания порядка использования указанных утилит приведены в соответствующих инструкциях, входящих в комплект документации СКЗИ.

4.2 Утилита настройки СКЗИ и конфигурационный файл

Настройка СКЗИ осуществляется с помощью утилиты cpconfig, которая входит в состав дистрибутива и расположена в директории /opt/cprocsp/sbin/<название_архитектуры>.

Если установлены пакеты СКЗИ для двух архитектур, например, ia32 и x64, то действия по настройке нужно проводить дважды — для каждой архитектуры с помощью cpconfig из соответствующей папки.

С помощью конфигурационного файла осуществляется настройка ПО СКЗИ КриптоПро CSP. Конфигурационный файл СКЗИ в среде операционных систем Linux является аналогом ветви реестра в операционной системе Windows. В зависимости от ОС месторасположение и имя конфигурационного файла может варьироваться. Для 64-разрядных версий ОС файл имеет имя config64.ini, для 32-разрядных — config.ini.

В LSB совместимых ОС конфигурационный файл расположен в:

```
/etc/opt/cprocsp/
```

4.3 Ввод серийного номера лицензии

При установке программного обеспечения КриптоПро CSP без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия.

Для использования КриптоПро CSP пользователь должен ввести серийный номер с бланка лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).

Для просмотра информации о лицензии выполните:

```
# ./cpconfig -license -view
```

Для ввода лицензии выполните:

```
# ./cpconfig -license -set <серийный_номер>
```

Серийный номер следует вводить с соблюдением регистра символов.

4.4 Настройка оборудования СКЗИ

Утилита cpconfig также предназначена для изменения набора устройств хранения (носителей) и считывания (считывателей) ключевой информации и датчиков случайных чисел. Предустановленными являются считыватели flash-носителей и образ дискеты на жестком диске.

Для просмотра списка настроенных считывателей:

```
# ./cpconfig -hardware reader -view
```

Для просмотра списка настроенных ДСЧ:

```
# ./cpconfig -hardware rndm -view
```

Для консольного БиоДСЧ требуется пакет lsb-cprocsp-kc1. Для добавления консольного БиоДСЧ:

```
# ./cpconfig -hardware rndm -add bio_tui -level 5 -name "Console BioRNG"
```

Для графического БиоДСЧ требуется пакет cprocsp-rdr-gui (или cprocsp-rdr-gui-gtk) и X-сервер. БиоДСЧ регистрируется автоматически при установке указанных пакетов.

Для использования внешней гаммы:

```
# ./cpconfig -hardware rndm -add cpsd -name 'cpsd rng' -level 3

# ./cpconfig -hardware rndm -configure cpsd -add string /db1/kis_1 /var/opt/cprocsp/dsrf/
db1/kis_1

# ./cpconfig -hardware rndm -configure cpsd -add string /db2/kis_1 /var/opt/cprocsp/dsrf/
db2/kis_1
```

Также необходимо скопировать файлы с данными, полученными с помощью «АРМ выработки внешней гаммы». Для этого выполните команды (при условии, что файлы находятся в /tmp/db[1,2]):

```
# cp /tmp/db1/kis_1 /var/opt/cprocsp/dsrf/db1/kis_1

# cp /tmp/db2/kis_1 /var/opt/cprocsp/dsrf/db2/kis_1
```

Для получения подробной справки по cpconfig:

```
# ./cpconfig -help

# ./cpconfig -hardware -help
```

4.5 Установка параметров журналирования

СКЗИ имеет возможность протоколирования событий. Информация записывается в системный журнал. Поддерживается возможность изменения настроек журналирования различных модулей СКЗИ, а также изменения уровня журналирования и формата выводимых отладочных сообщений.

Для получения справки по настройкам журналирования:

```
# cpconfig -loglevel -help
```

Подробнее опции управления протоколированием модулями СКЗИ см. в Приложении А.

4.6 Настройка криптопровайдера по умолчанию

Для просмотра типов доступных криптопровайдеров:

```
# ./cpconfig -defprov -view_type
```

Для просмотра свойств криптопровайдера нужного типа:

```
# ./cpconfig -defprov -view -provtype <provtype>
```

Для установки провайдера по умолчанию для нужного типа:

```
# ./cpconfig -defprov -setdef -provtype <provtype> -provname <provname>
```

Для получения имени провайдера по умолчанию для нужного типа:

```
# ./cpconfig -defprov -getdef -provtype <provtype>
```

4.7 Включение режима 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. После успешной инсталляции необходимо включить данный режим, выполнив команду:

```
#./cpconfig -ini '\config\parameters' -add long 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 или запустить утилиту csptest, предварительно проверив, что зарегистрирован хотя бы один датчик случайных чисел:

```
# ./csptest -keyset -verifycontext -hard_rng
```



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

4.8 Настройка параметров алгоритмов

Для установки параметров алгоритмов (для провайдеров типа 75):

параметры алгоритма шифрования:

```
# ./cpconfig -ini '\config\OID' -add string cipher <OID>
```

параметры алгоритма подписи:

```
# ./cpconfig -ini '\config\OID' -add string sign_el_2001 <OID>
```

параметры алгоритма Диффи-Хеллмана:

```
# ./cpconfig -ini '\config\OID' -add string dh_el_2001 <OID>
```

Для установки параметров алгоритмов (для провайдеров типа 80):

параметры алгоритма шифрования:

```
# ./cpconfig -ini '\config\OID' -add string cipher_2012 <OID>
```

параметры алгоритма подписи:

```
# ./cpconfig -ini '\config\OID' -add string sign_el_2012 <OID>
```

параметры алгоритма Диффи-Хеллмана:

```
# ./cpconfig -ini '\config\OID' -add string dh_el_2012 <OID>
```

Для установки параметров алгоритмов (для провайдеров типа 81):

параметры алгоритма шифрования:

```
# ./cpconfig -ini '\config\OID' -add string cipher_2012 <OID>
```

параметры алгоритма подписи:

```
# ./cpconfig -ini '\config\OID' -add string sign_el512 <OID>
```

параметры алгоритма Диффи-Хеллмана:

```
# ./cpconfig -ini '\config\OID' -add string dh_el512 <OID>
```

Перечень поддерживаемых в КриптоПро CSP идентификаторов криптографических параметров алгоритмов указан в `CSP_5_0.chm`.

4.9 Использование СКЗИ с nginx/Apache

nginx и Apache — ПО с открытым исходным кодом для веб-серверов. Одной из основных функциональностей указанных серверов является построение защищенного соединения с пользователями.

В состав СКЗИ входят доработанные модули nginx и Apache (mod_ssl), обеспечивающие возможность построения защищенного TLS-соединения и работы в рамках этого соединения на ОС семейства Linux с использованием ГОСТ-алгоритмов с помощью вызова функций СКЗИ. При использовании данных модулей для выполнения криптографических операций вместо стандартной OpenSSL-реализации будут вызываться функции SSPI- и CryptoAPI-интерфейсов СКЗИ.

Указанные модули включены в пакеты cprocsp-nginx и cprocsp-apache-modssl дистрибутива СКЗИ.

Примечание. Доработанный модуль nginx является результатом применения патча, автоматически вносящего необходимые изменения в исходный код сервера nginx, и последующей сборки веб-сервера. Указанный патч также включен в комплект поставки СКЗИ для возможности самостоятельного применения к ППО nginx версии 1.22.1 и последующей сборки веб-сервера.
В этом случае исходные тексты nginx версии 1.22.1 скачиваются с официального сайта с последующей проверкой контрольной суммы с использованием утилиты cpverify (параметры по умолчанию):

```
cpverify nginx-1.22.1.tar.gz 7EFCECDDD45DDF90213F7796A0073477D713625A7291861796DB7224995F3B49
```

После применения патча и сборки nginx для исполняемых модулей должна быть зафиксирована контрольная сумма.

Примечание. Отключение в конфигурационном файле флагов sspi_client_verify_local_crl_only, proxy_ssl_verify_local_crl_only и proxy_ssl_verify_ignore_cn допускается только в тестовых целях.

4.10 Настройка клиентского компонента КриптоПро HSM

Для настройки клиентского компонента ПАКМ под управлением ОС семейства Linux необходимо:
- Установить модули СКЗИ КриптоПро CSP (см. разд. 2).
- Выполнить настройку криптопровайдеров (см. разд. 4.10.1).
- Выполнить настройку приложения для создания TLS-туннеля stunnel (см. разд. 4.10.2).
- Выполнить регистрацию нового пользователя ПАКМ (см. разд. 4.10.3).
- Запустить службу stunnel (см. разд. 4.10.4).

Примечание. Для быстрой и корректной настройки криптопровайдеров и stunnel (см. п.п. 4.10.1-4.10.4) на клиенте рекомендуется воспользоваться скриптом channel_k2.sh, включенным в состав дистрибутива ПАКМ.

4.10.1 Настройка ПО СКЗИ КриптоПро CSP

В конфигурационном файле СКЗИ после пункта [Defaults\Provider] необходимо добавить секции (или убедиться в их наличии):

```
[Defaults\Provider\"Crypto-Pro GOST R 34.10-2012 HSM CSP"]
"Image Path" = "/opt/cprocsp/lib/<название_архитектуры>/libcspr.so"
Type = 80
Channel = ".clientk2"
Media = "HSMDB"
"Function Table Name" = CPSRV_GetFunctionTable

[Defaults\Provider\"Crypto-Pro HSM RSA CSP"]
"Image Path" = "/opt/cprocsp/lib/<название_архитектуры>/libcspr.so"
Type = 1
Channel = ".clientk2"
Media = "HSMDB"
"Function Table Name" = CPSRV_GetFunctionTable
```

Примечание. Параметр Channel должен содержать имя сокета, аналогичное имени сокета, указанного в параметре accept в конфигурационном файле stunnel, без пути к файлу (см. разд. 4.10.2).

Если требуется подключение второго HSM, нужно зарегистрировать еще один провайдер (с другим именем) с тем же именем сокета (параметр Channel), указанного в конфигурационном файле stunnel (параметр accept) для второго HSM:

```
[Defaults\Provider\"Crypto-Pro GOST R 34.10-2012 HSM CSP 01"]
"Image Path" = "/opt/cprocsp/lib/<название_архитектуры>/libcspr.so"
Type = 80
Channel = ".clientk2a"
Media = "HSMDB"
"Function Table Name" = CPSRV_GetFunctionTable
```

Таким образом, для обращения к разным HSM с одного клиента нужно использовать разные криптопровайдеры (в примере выше — Crypto-Pro GOST R 34.10-2012 HSM CSP и Crypto-Pro GOST R 34.10-2012 HSM CSP 01).

Для конфигурации PKCS#11 в конфигурационный файл СКЗИ после секции [PKCS11] необходимо добавить секцию (или убедиться в ее наличии):

```
[PKCS11\slot0]
ProvRSA = "Crypto-Pro HSM RSA CSP"
ProvGOST = "Crypto-Pro GOST R 34.10-2012 HSM CSP"
reader = "HSMDB"
#reader = "HDIMAGE"
```

После настройки проверьте работоспособность провайдера с помощью команды:

```
/opt/cprocsp/bin/<название_архитектуры>/csptest -enum -provname "Crypto-Pro GOST R 34.10-2012 HSM CSP" -info
```

И перезапустите службу cprocsp (пример для ОС, использующих Init-скрипты):

```
/etc/init.d/cprocsp stop
/etc/init.d/cprocsp start
```

4.10.2 Настройка stunnel

Настройка stunnel осуществляется с помощью конфигурационного файла stunnel.conf. Если конфигурационный файл stunnel располагается по пути /etc/opt/cprocsp/stunnel/stunnel.conf, запуск stunnel возможен без дополнительных параметров. Иначе при запуске утилиты необходимо указывать путь к файлу конфигурации:

```
/opt/cprocsp/sbin/<название_архитектуры>/stunnel/<путь_к_файлу_конфигурации>
```

Пример конфигурационного файла:

```
setuid = root
setgid = root
pid = /var/opt/cprocsp/tmp/stunnel-K2.pid
output=/var/log/stunnel-K2.log
#socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
debug = 0
max_clients = 25
for_hsm = yes

[clientk2]
client=yes
connect=192.168.70.74:1501
accept = /var/opt/cprocsp/tmp/.clientk2
cert=/root/cert.cer
```

Описание опций stunnel:

`client=yes`	Режим клиента (удаленный сервис использует TLS/SSL)
`connect=[host:]port`	IP-адрес HSM и его порт для канала «K2» (1501)
`accept = [host:]port`	Сокет, который будет слушать `stunnel` (куда будут обращаться приложения по вызовам CryptoAPI)
`cert = cert_file`	Путь к файлу сертификата ключа доступа к HSM (сертификат также должен быть установлен в хранилище сертификатов «My» пользователя, под которым запускается `stunnel`, и иметь там «связку» с закрытым ключом)

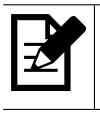
Подробное описание всех возможных опций `stunnel` также приведено в ЖТЯИ.00101-03 93 03. Приложения для создания TLS-туннеля.

Если требуется подключение второго HSM, необходимо дополнительно добавить еще одного слушателя на другой сокет:

```
[clientk2]
client=yes
connect=192.168.70.75:1501
accept=/var/opt/cprocsp/tmp/.clientk2a
cert=/root/client/client2.cer
```

4.10.3 Регистрация пользователя на ПАКМ

Далее в ПАКМ регистрируется новый пользователь, для него формируются ключ и сертификат ключа доступа к ПАКМ.



Примечание. Сформированный ключ доступа должен иметь тот же уровень защиты, что и используемое СКЗИ КриптоПро CSP.

Возможны несколько вариантов формирования ключа и сертификата пользователя:
1) Ключ и сертификат могут быть сформированы на смарт-карте с использованием как LCD

панели ПАКМ, так и Web-интерфейса ПАКМ (ключи на Web-интерфейсе формируются с классом защиты установленного СКЗИ КриптоПро CSP под Windows). В этом случае на машине с ОС Linux надо настроить считыватель смарт-карт и установить сертификат в хранилище «My» со ссылкой на контейнер на смарт-карте.

2) Также возможно сформировать ключи локально на машине с ОС Linux (на носитель HDIMAGE), сформировать PKCS#10-запрос утилитами из состава КриптоПро CSP и через Web-интерфейс ПАКМ по запросу получить сертификат этого ключа. Далее этот сертификат также устанавливается в хранилище «My» с указанием ссылки на ключевой контейнер.

3) Возможна генерация ключа на машине с ОС Windows, генерация контейнера осуществляется на обычный USB-флеш-накопитель. После генерации контейнера необходимо корректно перенести его на машину с ОС Linux одним из следующих способов:

- Скопировать контейнер с помощью утилиты `csptest` в режиме `-keyset`. В конфигурационном файле СКЗИ КриптоПро CSP должны быть зарегистрированы исходный и целевой считыватели (FLASH и HDIMAGE), проверка осуществляется командой:

  ```
  /opt/cprocsp/sbin/<название_архитектуры>/cpconfig -hardware reader -view
  ```

  Полное имя контейнера можно узнать с помощью команды:

  ```
  /opt/cprocsp/bin/<название_архитектуры>/csptest -keyset -enum_cont -fqcn -verifycontext
  ```

- Вручную скопировать каталог контейнера в структуру каталога HDIMAGE и установить соответствующие права на каталог контейнера и файлы. Контейнер копируется в каталог `/var/opt/cprocsp/keys/<имя_пользователя>/`. Необходимо установить права на чтение и запись на контейнер и все файлы внутри.



Примечание. Класс защиты СКЗИ КриптоПро CSP на целевой машине с ОС Linux должен быть не выше класса защиты СКЗИ на машине с ОС Windows, на которой выполнялась генерация ключа.

После генерации ключа и сертификата необходимо:

1) установить сертификат в хранилище «My» со ссылкой на ключевой контейнер:

```
/opt/cprocsp/bin/<название_архитектуры>/certmgr -inst  -cont '\\.\HDIMAGE\contname'
```

2) разместить файл сертификата пользователя (в кодировке DER) в каталоге, указанном в конфигурационном файле `stunnel` (параметр `cert`). Экспорт сертификата в файл осуществляется командой:

```
/opt/cprocsp/bin/<название_архитектуры>/certmgr -exp -dest /root/cert.cer
```

3) установить корневой сертификат ПАКМ в хранилище «root»:

```
/opt/cprocsp/bin/<название_архитектуры>/certmgr -inst -store root -file <путь_к_корневому
_сертификату>
```

4.10.4 Запуск stunnel

После настроек выполняется запуск `stunnel_fork`:

```
/opt/cprocsp/sbin/<название_архитектуры>/stunnel_fork
```

Проверка работоспособности осуществляется с помощью команды:

```
/opt/cprocsp/bin/<название_архитектуры>/csptest -enum -provname "Crypto-Pro GOST R
34.10-2012 HSM CSP" -info
```

5 Работа в ОС Astra Linux

5.1 Настройка работы с веб-сервером Apache

Для обеспечения совместной работы СКЗИ и веб-сервера Apache под управлением ОС Astra Linux необходимо:

1) Установить СКЗИ КриптоПро CSP (см. Установка и удаление СКЗИ).

2) Заменить путь в конфигурационном файле mods-enabled/ssl.load до astra_se_mod_ssl.so из состава СКЗИ.

Примечание. astra_se_mod_ssl.so требует наличия openssl-1.0.

3) Сгенерировать сертификаты пользователю, от имени которого будет запущен сервер Apache.

Примечание. Примеры генерации сертификатов описаны в create_certs.sh, install_root_certs.sh. Рекомендуется не запускать данные примеры, а выполнять генерацию сертификатов аналогично.

4) По умолчанию используется конфигурационный файл sites-enabled/default-ssl.conf. Необходимо заменить указанные в нем сертификаты и выставить параметры, аналогичные cpro.conf.

Для тестирования корректности работы веб-сервера можно воспользоваться скриптом (требуется наличие openssl-1.1.0).

Тестовый скрипт не учитывает ошибки, связанные с верификацией сертификата сервера (т.к. тестируется не клиент, а сервер). Для того, чтобы не было ошибок верификации сертификата на клиенте, необходимо добавить в хранилище root сертификат УЦ, который выдал сертификат сервера.

5.2 Использование СКЗИ в замкнутой программной среде ОС Astra Linux Special Edition

Для установки СКЗИ КриптоПро CSP в замкнутой программной среде (ЗПС) ОС Astra Linux Special Edition необходимо:

1) Указать следующие параметры в файле `/etc/digsig/digsig_initramfs.conf`:

- для ОС Astra Linux SE версии 1.6 и выше:

```
DIGSIG_ELF_MODE=1
```

- для ОС Astra Linux SE версии 1.5:

```
DIGSIG_LOAD_KEYS=1
DIGSIG_ENFORCE=1
```

2) Установить пакет совместимости с помощью следующей команды (для ОС Astra Linux SE версии 1.6 и выше):

```
apt install astra-digsig-oldkeys
```

3) Создать директорию для файла ключа с помощью следующей команды:

```
mkdir -p /etc/digsig/keys/legacy/cryptopro
```

4) Разместить файл ключа cryptopro_pub_key.gpg в директории, созданной на предыдущем шаге, с помощью следующей команды:

```
cp cryptopro_pub_key.gpg /etc/digsig/keys/legacy/cryptopro
```

5) Обновить диски оперативной памяти с помощью следующей команды:

```
sudo update-initramfs -u -k all
```

6) Выполнить перезагрузку ОС.

7) Установить СКЗИ КриптоПро CSP (см. Установка и удаление СКЗИ).

5.3 Модуль Check

В состав СКЗИ входит модуль Check, который представляет собой набор самостоятельных (не требующих установки базовых модулей КриптоПро CSP) программных компонентов, выполняющих функции расчета хэш-значения и проверки ЭП и предназначенных для эксплуатации под управлением ОС СН Astra Linux SE.

Модуль реализован как динамически и статически подключаемые библиотеки. Статически подключаемые библиотеки предназначены для использования только в составе ядра ОС Astra Linux SE с проведением установленным для указанной ОС порядком работ по исследованиям ОС СН Astra Linux SE.

Подробнее интерфейс библиотек описан в документе ЖТЯИ.00101-03 96 04. Руководство программиста. Check.

6 Состав и назначение компонент ПО СКЗИ

6.1 Базовые модули СКЗИ

ПО СКЗИ содержит следующие базовые модули:

`libcsp`	динамически загружаемая библиотека КриптоПро CSP; реализует целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, БиоДСЧ
`libcspr`	обеспечивает удаленный доступ к криптопровайдеру, функционирующему как отдельный сервис
`libcsp_kc2`	динамически загружаемая библиотека КриптоПро CSP (KC2); реализует целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, БиоДСЧ
`drvcsp`	динамически загружаемый модуль ядра; реализует целевые функции криптографической защиты информации (кроме формирования ЭП) и работу с ключами
`libssp`	обеспечивает реализацию протокола сетевой аутентификации КриптоПро TLS (общее описание протокола приведено в документе ЖТЯИ.00101-03 90 01. Описание реализации)
`cpverify`	модуль контроля целостности при установке СКЗИ и функционировании ПО СКЗИ КриптоПро CSP на ПЭВМ пользователя (подробное описание см. в Приложении 1 ЖТЯИ.00101-03 95 01. Правила пользования)
`wipefile`	модуль удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях (подробное описание см. в Приложении 1 ЖТЯИ.00101-03 95 01. Правила пользования)
`cryptcp`	приложение командной строки для работы с сертификатами с использованием инфраструктуры открытых ключей, шифрования/расшифрования сообщений, содержащихся в файлах, создания/проверки электронных подписей и хэширования сообщений, содержащихся в файле или группе файлов (подробное описание см. в ЖТЯИ.00101-03 93 01. Приложение командной строки для подписи и шифрования файлов)
`certmgr`	приложение командной строки для управления сертификатами, списками отзыва сертификатов (CRL) и хранилищами (подробное описание см. в ЖТЯИ.00101-03 93 02. Приложение командной строки для работы с сертификатами)
`certprop`	модуль распространения сертификатов
`stunnel`	приложение для создания TLS-туннеля, предназначенного для создания TLS защищенного соединения между клиентом и локальным (inetd-запускаемым) или удаленным сервером (подробное описание см. в ЖТЯИ.00101-03 93 03. Приложение для создания TLS-туннеля)

`stunnel_msspi`	stunnel с интерфейсом msspi, позволяющим организовывать соединения с поддержкой криптографических алгоритмов ГОСТ
`cptools`	графическое приложение, предоставляющее доступ к основным функциям и настройкам КриптоПро CSP (подробное описание см. в ЖТЯИ.00101-03 92 06. Инструкция по использованию. Инструменты КриптоПро)
`curl`	приложение командной строки для передачи данных с синтаксисом URL (с поддержкой ГОСТ TLS)
`libades-core`	библиотека реализует функции работы CAdES и XAdES
`libnpcades`	библиотека NPAPI для работы КриптоПро ЭЦП Browser plug-in

В названиях дистрибутивов СКЗИ используются следующие обозначения:
- CPRO — префикс;
- csp — криптопровайдер;
- drv — загружаемый модуль ядра ОС;
- [d] (опционально) — указывает на документацию (тестовые примеры);
- i386 – платформа Intel.

6.2 Модули подсистемы программной среды функционирования криптосредства (СФ)

Список модулей подсистемы программной среды функционирования криптосредства и их описание приведено в табл. 4.

Таблица 4. Модули подсистемы программной СФ криптосредства и их описание

Модуль	Описание модуля
libcapi10.so, libcapi20.so	Библиотеки управления сертификатами открытых ключей и обеспечения выполнения криптографических запросов на уровне интерфейсов CryptoAPI 1.0 и CryptoAPI 2.0 соответственно
libcpext.so	Библиотека поддержки взаимодействия с ключами, содержащая вспомогательные функции для работы с ключами
libenroll.so	Библиотека поддержки генерации запросов на сертификаты открытых ключей
liburlretrieve.so	Библиотека поддержки доступа к сетевым ресурсам по URL адресам
genkpim	Приложение командной строки для выработки внешней гаммы
genpsk	Приложение командной строки для генерации и проверки PSK
libcpcurl.so	Библиотека поддержки передачи запросов на сертификаты, CRL и т.п. по сети и работы TLS с поддержкой российских криптографических алгоритмов с КриптоПро CSP в качестве криптопровайдера

ktls_gost.ko	Библиотека поддержки работы TLS с поддержкой российских алгоритмов на уровне ядра ОС
inittst	Модуль для работы с сертификатами, шифрования и расшифрования данных, создания и проверки электронной подписи (ЭП), хеширования данных с использованием сертификатов открытых ключей
cpconfig	Приложение командной строки для конфигурирования СКЗИ (работа с конфигурационным файлом)
libcpalloc.so	Библиотека поддержки управления памятью
libcplib.so	Библиотека поддержки работы с общеиспользуемыми типами
libcppkcs11.so	Библиотека поддержки работы с криптографическими устройствами PKCS#11
libcrypt.so	Библиотека поддержки шифрования, хэширования и кодирования
libcpcdrv.so	Библиотека для разработки и отладки СКЗИ на уровне ядра ОС
libcpcdrv_emul.a	Библиотека для разработки и отладки СКЗИ уровня ядра ОС на уровне приложений
libpkivalidator.so	Библиотека поддержки проверки корректности условий для объектов PKI
librevprov.so	Библиотека поддержки проверки статусов сертификатов
mod_ssl.so, astra_se_mod_ssl.so	Библиотеки поддержки работы протокола SSL с Apache в Linux и Astra Linux SE
librutokens.so	Драйверная библиотека поддержки Рутокен S
librdrrelay.so	Библиотека поддержки стороннего криптопровайдера, подключаемого через интерфейс CP как носитель с неизвлекаемыми ключами
csptest	Приложение командной строки для работы с сертификатами и хранилищами сертификатов, управления криптопровайдерами, ключевыми контейнерами, паролями, считывателями и проведения тестов производительности
Модули взаимодействия с ASN.1 структурами	
der2xer	Модуль для конвертации ASN.1 структур PKI в XER формат (XML) и обратно
libasn1data_XER.so	Библиотека поддержки функций преобразования ASN.1 структур данных в XER формат (XML) и обратно
libcpasn1.so	Библиотека поддержки внешнего интерфейса для работы с ASN.1 структурами
Модули поддержки пользовательского интерфейса КриптоПро CSP	
libcpui.so, libfgcpui.so	Библиотеки поддержки пользовательского интерфейса КриптоПро CSP

xcpui_qt	Модуль поддержки пользовательского интерфейса КриптоПро CSP
Модули поддержки IPsec	
libespdrv.so	Загружаемая библиотека поддержки ESP ядра ОС
libesp_gost.so	Библиотека поддержки протокола ESP уровня пользователя с поддержкой российских криптографических алгоритмов
libike_gost.so	Библиотека поддержки протокола IKE уровня пользователя с поддержкой российских криптографических алгоритмов
Модули поддержки CAdES/XAdES	
libades-core.so	Библиотека, являющаяся общим ядром CAdES и XAdES
libcades.so	Библиотека поддержки внешнего интерфейса усовершенствованной ЭП (C)
libcppcades.so	Библиотека поддержки внешнего интерфейса усовершенствованной ЭП (C++)
libxades.so	Библиотека поддержки внешнего интерфейса усовершенствованной ЭП (XAdES)
Модули поддержки OCSP	
libocsp.so	Библиотека поддержки внешнего интерфейса протокола OCSP
libocspcli.so	Библиотека поддержки интерфейса клиентских приложений (C++) протокола OCSP
ocsputil	Приложение командной строки для работы с протоколом OCSP
Модули поддержки TSP	
libtsp.so	Библиотека поддержки внешнего интерфейса для TSP
libtspcli.so	Библиотека поддержки интерфейса клиентских приложений (C++) протокола TSP
tsputil	Приложение командной строки для работы со штампами времени
Модули поддержки безопасности XML	
libxmlsec.so	Библиотека поддержки работы с подписью и шифрования XML-документов
libxmlsec-mscrypto.so	Библиотека поддержки работы с подписью и шифрования XML-документов при помощи Microsoft CryptoAPI
Модули поддержки работы КриптоПро ЭЦП Browser plug-in	
libnpcades.so	Библиотека поддержки NPAPI для работы с CAdES через браузер
nmcades	Хост Chrome Native Messaging для КриптоПро ЭЦП Browser plug-in

Модули устройств хранения ключевой информации	
librdrsup.so	Библиотека поддержки общих функций доступа к различным устройствам хранения ключевой информации
librdrcloud.so	Библиотека поддержки облачного токена
librdrcpfkc.so	Библиотека поддержки токенов и смарт-карт с поддержкой SESPAKE
librdrcryptoki.so	Библиотека поддержки доступа к ключам ФКН через интерфейс PKCS#11
librdredoc.so	Библиотека поддержки платформы eDoc (УЛГ)
librdremv.so	Библиотека поддержки смарт-карт Gemalto (EMV)
librdresmarttoken.so	Библиотека поддержки смарт-карт и токенов ESMART Token
librdresmarttokengost.so	Библиотека поддержки смарт-карт и токенов ESMART Token ГОСТ
librdrfat12.so	Библиотека поддержки съемных дисков и разделов HDD/SDD
librdrinfocrypt.so	Библиотека поддержки токенов InfoCrypt
librdrinpaspot.so	Библиотека поддержки смарт-карт Alioth
librdrjacarta.so	Библиотека поддержки токенов и смарт-карт JaCarta
librdrkst.so	Библиотека поддержки смарт-карт MorphoKST
librdrmskey.so	Библиотека поддержки токенов Multisoft MS_Key
librdrnova.so	Библиотека поддержки смарт-карт Novacard
librdrpcsc.so	Библиотека поддержки считывания носителей, поддерживающих интерфейс PC/SC
librdrric.so	Библиотека поддержки смарт-карт Оскар и Форос (Магистра)
librdrrosan.so	Библиотека поддержки смарт-карт Rosan
librdrrutoken.so	Библиотека поддержки смарт-карт и токенов Рутокен
Модули считывателей	
librdraccord.so	Библиотека поддержки АМДЗ Аккорд
librdrancud.so	Библиотека поддержки АНКАД КРИПТОН USB-ДСЧ
librdrcrypton.so	Библиотека поддержки АПМДЗ КРИПТОН-ЗАМОК
librdrmaxim.so	Библиотека поддержки АПМДЗ МАКСИМ М1
librdrsbl.so	Библиотека поддержки ПАК Соболь
librdrvityaz.so	Библиотека поддержки АПМДЗ Витязь-А

Модули датчиков случайных чисел	
librdrdsrf.so	Библиотека поддержки ДСЧ ДСДР
librdrrndmbio_tui.so	Библиотека поддержки консольного БиоДСЧ
librdrrndmbio_gui_fgtk.so	Библиотека поддержки графического БиоДСЧ

7 Требования по обеспечению безопасности при эксплуатации СКЗИ

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме раздела 5 ЖТЯИ.00101-03 95 01. Правила пользования.

При использовании СКЗИ под управлением ОС Linux необходимо предпринять дополнительные меры организационного и технического характера и выполнить дополнительные настройки операционной системы. При этом должна решаться задача как обеспечения дополнительной защиты сервера и ОС от НСД, так и обеспечения бесперебойного режима работы и исключения «отказа в обслуживании», вызванного внутренними причинами (например, переполнением файловых систем).

7.1 Организационно-технические меры защиты от НСД

Для ОС Linux дополнительно должен быть реализован следующий комплекс организационно-технических мер защиты от НСД:

1) Всех пользователей, которые не пользуются установленной ОС (включая стандартных пользователей, которые создаются в ОС во время установки, кроме пользователя root), следует удалить.

2) Необходимо установить минимально необходимый в соответствии с принятой в организации политикой безопасности перечень файлов, для которых требуется запуск с правами пользователя root (установлен флаг SUID). Запуск не входящих в этот перечень файлов с установленным флагом SUID должен контролироваться администратором.

3) Рекомендуется ограничить (с учетом принятой в организации политики безопасности) использование пользователями команд планирования задач и пакетной обработки заданий (например, cron и at). Для нормального функционирования системы минимально необходимым является разрешение использования данных команд только пользователю root (например, путем добавления имени root в файл `/etc/<command>.allow`).

4) Должно быть реализовано физическое затирание конфиденциальной информации с использованием программы wipefile из состава СКЗИ.

5) Права доступа к системным и критичным каталогам, общим ресурсам должны быть установлены в соответствии с политикой безопасности, принятой в организации. На все директории, содержащие системные файлы ОС и файлы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем, кроме Владельца (Owner).

6) По окончании работы СКЗИ содержимое виртуальной памяти ОС должно затираться с использованием средств ОС. В случае аварийного останова ПЭВМ, при следующей загрузке необходимо в режиме «single user» очистить область виртуальной памяти программой wipefile, входящей в состав СКЗИ. В случае выхода из строя диска, на котором находится область виртуальной памяти, криптографические ключи подлежат выводу из действия, а диск считается не подлежащим ремонту и уничтожается по правилам уничтожения ключевых носителей.

7.2 Дополнительные настройки ОС

Настройки ОС Linux выполняются путем редактирования (удаления, добавления) различных конфигурационных и командных файлов.

Для сохранения возможности «откатить» внесенные изменения следует сохранять модифицируемые файлы в «безопасном» месте (на внешнем носителе или на не монтируемой автоматически файловой системе).

Желательно скопировать изменяемые файлы (каталоги) с сохранением структуры каталогов.

7.2.1 Ограничение доступа пользователей и настройки пользовательского окружения

Настройка пользовательского окружения заключается в следующих действиях:

1) В файле `/etc/login.defs` следует установить следующие директивы:

- PASS_MAX_DAYS=180 (параметр задаёт максимальное время использования пароля)
- PASS_MIN_DAYS=30 (параметр задаёт минимальное количество дней между сменами пароля)
- PASS_MIN_LEN=8 (параметр задаёт минимальную длину пароля)

2) Для защиты пароля может быть использована библиотека libxcrypt, осуществляющая хранение пароля в виде хэш-значения.

3) В файле `/etc/profile` установить значение umask=022 (параметр задает маску создания файла по-умолчанию)

4) Для пользователя root установить маску режима создания файлов umask=077 или umask=027;

5) В файл `/etc/shells` поместить имена только тех исполняемых файлов оболочек, которые установлены в системе.

6) Удалить файл (если он существует) `/.rhosts` из домашних каталогов всех пользователей, включая учетную запись root.

7) Удалить содержимое файла `/etc/host.equiv`.

8) Запретить rhosts-аутентификацию (например, с помощью комментирования строк, содержащих подстроку "pam_rhosts_auth.so", в файле `/etc/pam.conf`).

9) Проверить идентификаторы пользователя и группы для всех пользователей, перечисленных в файле `/etc/passwd`. Следует убедиться, что не существует пользователей, имеющих идентификатор пользователя 0 и идентификатор группы 0 кроме, возможно, пользователя root.

7.2.2 Ограничения при монтировании файловых систем

- В файле `/etc/fstab` установить опцию монтирования nosuid для файловой системы `/var`.
- Для предотвращения переполнения критичных файловых систем и обеспечения возможности монтирования файловой системы `/usr` в режиме «только для чтения» рекомендуется при инсталляции ОС выделить для файловых систем `/, /usr, /usr/local, /var` разные разделы диска.

7.2.3 Настройка сетевых сервисов

1) Следует ограничить функциональность демона управления сетевыми соединениями xinetd, если он используется в системе (например, с помощью редактирования файла `/etc/xinetd.conf` и файлов в каталоге `/etc/xinetd.d`). Следует запретить следующие сервисы (при их наличии в системе):

- echo
- discard
- daytime
- chargen
- finger
- systat
- netstat
- tftp
- telnet
- nfsd

2) Если не планируется использовать настраиваемый компьютер в качестве маршрутизатора, необходимо отключить пересылку IP-пакетов (IP Forwarding).

3) Следует запретить прием из внешней сети «широковещательных» (broadcast) пакетов, а также передачу ответов на принятые «широковещательные» пакеты;

4) Запустить процедуру регистрации запуска процессов (accounting) (например, с помощью утилит acct или psacct);

5) Если планируется использовать на настраиваемом сервере сервис FTP, необходимо установить перечень пользователей, для которых запрещен (в соответствии с принятой политикой безопасности) доступ к серверу по протоколу FTP (например, путем редактирования файла `/etc/ftpusers`). Следует запретить доступ по FTP для следующих пользователей (при их наличии в системе):

- root
- daemon
- bin
- sys
- sync
- adm
- lp
- mail
- smtp
- uucp
- nuucp
- listen
- nobody
- noaccess

6) Следует ограничить доступ к системным файлам для непривилегированных пользователей (в соответствии с принятой политикой безопасности), например, с помощью выполнения команд (при наличии соответствующих объектов в системе):

```
chown root /etc/mail/aliases
chmod 644 /etc/mail/aliases
chmod 444 /etc/default/login %/etc/securetty
chmod 750 /etc/security
chmod 000 /usr/bin/at
chmod 500 /usr/bin/rdist
chmod 400 /usr/sbin/snoop %tcpdump
chmod 400 /usr/sbin/sync
chmod 400 /usr/bin/uudecode
```

7) Следует обнулить флаг SGID для некоторых исполняемых файлов (при их наличии в системе):

```
chmod g-s /bin/mail
chmod g-s /usr/bin/write
chmod g-s /bin/netstat
chmod g-s /usr/sbin/nfsstat
chmod g-s /usr/bin/ipcs
chmod g-s /sbin/arp
chmod g-s /bin/dmesg
chmod g-s /sbin/swapon
chmod g-s /usr/bin/wall
```

7.2.4 Ограничение количества «видимой извне» информации о системе

Обычно, начальную информацию о системе потенциальный нарушитель получает из системных приглашений, выдаваемых сетевыми службами сервера (telnet-сервер, ftp-сервер и пр.).

Для ограничения количества «видимой извне» информации рекомендуется:

• отказаться от стандартного «заголовка», выводимого сервером ftp при ответе пользователю (например, путем указания в файле `/etc/vsftpd/vsftpd.conf` параметра `ftpd_banner`)

• отредактировать файлы `/etc/issue`, `/etc/banners/ftp.msg` и `/etc/motd` с целью разъяснения пользователям правил и политики доступа к серверу ftp.

7.2.5 Настройка подсистемы протоколирования и аудита

1) Установить права на запись в следующие файлы (при их наличии в системе) только для пользователя root:

- /var/log/authlog
- /var/log/syslog
- /var/log/messages
- /var/log/sulog
- /var/log/utmp
- /var/log/utmpx

2) Если на настраиваемом сервере используется web-сервер, то следует убедиться, что только владелец процесса httpd имеет доступ на запись к протоколам httpd;

3) Ограничить (с учетом выбранной в организации политики безопасности) использование пользователями команд su и sudo — предоставления пользователю административных полномочий.

4) Следует протоколировать попытки использования программ su и sudo, например, с помощью добавления в файл `/etc/syslog.conf` строк:

```
auth.notice         /var/log/authlog
```

или

```
auth.notice         /var/log/authlog, @loghost.
```

Вторая строка аналогична первой, но указывает, что протокол дополнительно передается на сервер сбора протоколов.

5) Следует обеспечить протоколирование неуспешных попыток регистрации в системе в локальном протокол, например, путем выполнения команд:

```
touch /var/adm/loginlog
chown root /var/adm/loginlog
chgrp root /var/adm/loginlog
chmod 644 /var/adm/loginlog
```

6) Следует обеспечить протоколирование сетевых соединений, контролируемых демоном xinetd (включая дату/время соединения, IP-адрес клиента, установившего соединение и имя сервиса, обслуживающего соединение), например, путем добавления в файл `/etc/syslog.conf` строки:

```
daemon.notice                 /var/log/syslog
```

8 Требования по криптографической защите

Должны выполняться требования по криптографической защите раздела 6 документа ЖТЯИ.00101-03 95 01. Правила пользования в части, касающейся ОС Linux.

Необходимо выполнить настройку операционной системы для работы с СКЗИ по разд. 7.2.

Контролем целостности должны быть охвачены файлы:

```
/opt/cprocsp/bin/<название_архитектуры>/astra_se_mod_ssl.so
/opt/cprocsp/bin/<название_архитектуры>/mod_ssl.so
/opt/cprocsp/bin/<название_архитектуры>/certprop
/opt/cprocsp/bin/<название_архитектуры>/cptools
/opt/cprocsp/bin/<название_архитектуры>/curl
/opt/cprocsp/lib/<название_архитектуры>/libcpcurl.a
/opt/cprocsp/lib/<название_архитектуры>/libcpcurl.so.4.5.0
/opt/cprocsp/lib/<название_архитектуры>/libcpcdrv_emul.a
/opt/cprocsp/bin/<название_архитектуры>/cp-genpsk.sh
/opt/cprocsp/bin/<название_архитектуры>/genpsk
/opt/cprocsp/lib/<название_архитектуры>/libesp_gost.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/libike_gost.so.4.0.5
/opt/cprocsp/bin/<название_архитектуры>/der2xer
/opt/cprocsp/bin/<название_архитектуры>/inittst
/opt/cprocsp/lib/<название_архитектуры>/libasn1data_XER.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/libcpasn1.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/libcplib.so.4.0.5
/opt/cprocsp/sbin/<название_архитектуры>/cpnginx
/opt/cprocsp/bin/<название_архитектуры>/ocsputil
/opt/cprocsp/bin/<название_архитектуры>/tsputil
/opt/cprocsp/lib/<название_архитектуры>/libades-core.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/libcades.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/libcppcades.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/libocsp.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/libocspcli.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/libpkivalidator.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/librevprov.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/libtsp.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/libtspcli.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/libxades.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/libxmlsec-mscrypto.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/libxmlsec.so.2.0.0
/opt/cprocsp/bin/<название_архитектуры>/nmcades
/opt/cprocsp/lib/<название_архитектуры>/libnpcades.so.2.0.0
/opt/cprocsp/lib/<название_архитектуры>/librdrcloud.so.4.0.5
/opt/cprocsp/sbin/<название_архитектуры>/oauthapp
/opt/cprocsp/lib/<название_архитектуры>/librdrcpfkc.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrcryptoki.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdredoc.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdremv.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdresmarttoken.so
```

/opt/cprocsp/lib/<название_архитектуры>/librdresmarttokengost.so
/opt/cprocsp/lib/<название_архитектуры>/libfgcpui.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrrndmbio_gui_fgtk.so.4.0.5
/opt/cprocsp/sbin/<название_архитектуры>/xcpui_app
/opt/cprocsp/lib/<название_архитектуры>/librdrinfocrypt.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrinpaspot.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrjacarta.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrkst.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrmskey.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrnova.so.4.0.5
/opt/cprocsp/bin/<название_архитектуры>/list_pcsc
/opt/cprocsp/lib/<название_архитектуры>/librdrpcsc.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrric.so.4.0.5
/opt/cprocsp/sbin/<название_архитектуры>/ccid_reg.sh
/opt/cprocsp/lib/<название_архитектуры>/librdrrelay.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrrosan.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrrutoken.so.4.0.5
/opt/cprocsp/sbin/<название_архитектуры>/channel_k2.sh
/opt/cprocsp/sbin/<название_архитектуры>/stunnel_fork
/opt/cprocsp/sbin/<название_архитектуры>/stunnel_hsm
/opt/cprocsp/sbin/<название_архитектуры>/stunnel_thread
/opt/cprocsp/sbin/<название_архитектуры>/stunnel_msspi
/opt/cprocsp/bin/<название_архитектуры>/certmgr
/opt/cprocsp/bin/<название_архитектуры>/cryptcp
/opt/cprocsp/bin/<название_архитектуры>/csptest
/opt/cprocsp/bin/<название_архитектуры>/csptestf
/opt/cprocsp/lib/<название_архитектуры>/libcapi20.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/libcpext.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/libenroll.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/libssp.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/libsspdrv.a
/opt/cprocsp/lib/<название_архитектуры>/libsspdrv_user.a
/opt/cprocsp/lib/<название_архитектуры>/liburlretrieve.so.4.0.5
/opt/cprocsp/sbin/<название_архитектуры>/cpinstance
/opt/cprocsp/lib/<название_архитектуры>/libcsp.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/libcspr.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/libcsp_kc2.so.4.0.5
/opt/cprocsp/sbin/<название_архитектуры>/cryptsrv
/opt/cprocsp/lib/<название_архитектуры>/libcppkcs11.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/libcrypt.so.1.1.0
/opt/cprocsp/bin/<название_архитектуры>/cpverify
/opt/cprocsp/bin/<название_архитектуры>/csptestlite
/opt/cprocsp/bin/<название_архитектуры>/genkpim
/opt/cprocsp/bin/<название_архитектуры>/wipefile
/opt/cprocsp/lib/<название_архитектуры>/libcapi10.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/libcpalloc.so.0.0.0
/opt/cprocsp/lib/<название_архитектуры>/libcpui.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrdsrf.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrfat12.so.4.0.5

```
/opt/cprocsp/lib/<название_архитектуры>/librdrsup.so.4.0.5
/opt/cprocsp/sbin/<название_архитектуры>/cpconfig
/opt/cprocsp/sbin/<название_архитектуры>/mount_flash.sh
/opt/cprocsp/sbin/<название_архитектуры>/unreg_prov_type_name.sh
/opt/cprocsp/lib/<название_архитектуры>/librdraccord.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrancud.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrcrypton.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrmaxim.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrsbl.so.4.0.5
/opt/cprocsp/lib/<название_архитектуры>/librdrvityaz.so.4.0.5
```



Примечание. Список файлов, охваченных контролем целостности, зависит от установленных модулей и архитектуры ОС.

Приложение А
Управление протоколированием

В состав СКЗИ КриптоПро CSP включена новая система аудита, отличная от предыдущих версий СКЗИ.

Уровень, содержание и методы вывода информации независимо устанавливаются для выделенных модулей аудита (см. табл. А1). Несколько библиотек могут использовать один модуль аудита, возможна и обратная ситуация.

Таблица А1. Модули аудита

Модуль (name)	**Описание**
`capi10`	CryptoAPI 1.0
`capi20`	CryptoAPI 2.0
`ssp`	TLS
`cspr`	клиентский RPC
`cpext`	расширения CryptoAPI
`cloud`	облачный провайдер
`csp`	ядро CSP
`pcsc`	считыватели PC/SC

Для управления протоколированием конкретного модуля аудита (`name`) необходимо задать уровень протоколирования и формат протокола:

1) Для определения **уровня протокола** (`levelmask`):

```
/opt/cprocsp/sbin/<название_архитектуры>/cpconfig -loglevel <name> -mask <levelmask>
```

Значением параметра является шестнадцатеричное число, состоящее из 3 частей, вида 0xXX0YY0ZZ. Старшая часть (XX) определяет вид информации, которая будет записываться в **syslog**, средняя (YY) — информацию, вывод которой осуществляется в **консоль**, младшая (ZZ) — в текущей реализации не используется.

В каждую часть необходимо установить значение, которое является побитовой суммой необходимых N_DB*-флагов (см. табл. А2).

Таблица А2. Уровни протоколирования

N_DB_ERROR = 1 (0x01)	критические ошибки, по умолчанию возведено
N_DB_WARN = 2 (0x02)	некритические ошибки
N_DB_CALL = 4 (0x04)	информация о вызове функции
N_DB_LOG = 8 (0x08)	криптографически важные события: обращения к закрытым ключам, создание и удаление контейнеров
N_DB_TRACE = 16 (0x10)	отладочная информация

2) Для задания **формата протокола** (`formatmask`):

```
/opt/cprocsp/sbin/<название_архитектуры>/cpconfig -loglevel <name> -format <formatmask>
```

или

```
/opt/cprocsp/sbin/<название_архитектуры>/cpconfig -loglevel <name_fmt> -mask <formatmask>
```

Значением параметра является побитовая сумма необходимых DBFMT_*-флагов (см. табл. А3).

Таблица А3. 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

Для просмотра текущих значений уровня и формата протокола:

```
/opt/cprocsp/sbin/<название_архитектуры>/cpconfig -loglevel <name> -view
```

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					