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

# Средство Криптографической Защиты Информации

# КриптоПро CSP Версия 5.0 R2 КС1 Исполнение 1-Base Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows

ЖТЯИ.00101-02 91 02
Листов 40

2021 г

# Содержание

# Аннотация

Настоящее руководство содержит общее описание средства криптографической защиты информации «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base и рекомендации по использованию СКЗИ под управлением операционных систем Windows.

Инструкции администратора безопасности и пользователя различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС Windows, должны разрабатываться с учетом требований настоящего документа.

# Список определений и сокращений

| | |
|---|---|
| CRL | Список отозванных сертификатов (Certificate Revocation List) |
| АРМ | Автоматизированное рабочее место |
| АС | Автоматизированная система |
| ГМД | Гибкий магнитный диск |
| ДСЧ | Датчик случайных чисел |
| HDD | Жесткий магнитный диск (Hard Disk Drive) |
| НСД | Несанкционированный доступ |
| ОС | Операционная система |
| ПАК | Программно-аппаратный комплекс |
| ПО | Программное обеспечение |
| Регистрация | Присвоение определенных атрибутов (адреса, номера ключа, прав использования и т.п.) абоненту |
| Регламент | Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах |
| СВТ | Средства вычислительной техники |
| Сертификат | Электронный документ, подтверждающий принадлежность открытого ключа или ключа проверки электронной подписи и определенных атрибутов конкретному абоненту |
| Сертификация | Процесс изготовления сертификата открытого ключа или ключа проверки электронной подписи абонента в центре сертификации |
| СКЗИ | Средство криптографической защиты информации |
| СОС | Список отозванных сертификатов (Certificate Revocation List) |
| СС | Справочник сертификатов открытых ключей и ключей проверки электронной подписи. Сетевой справочник |
| СФ | Среда функционирования |
| ЦС | Центр Сертификации (Удостоверяющий Центр) |
| ЦР | Центр Регистрации |
| ЭД | Электронный документ |
| ЭП | Электронная подпись |

# 1 Основные технические данные и характеристики СКЗИ

## 1.1 Программно-аппаратные среды функционирования

СКЗИ «КриптоПро CSP» версия 5.0 R2 КС1 исполнение 1-Base функционирует в следующих группах программно-аппаратных сред:

Windows

Windows 7/8/8.1/10/Server 2008 (x86, x64)
Windows Server 2008 R2/2012/2012 R2/2016/2019 (x64)

Со сроками эксплуатации указанных операционных систем можно ознакомиться по адресу:

https://support.microsoft.com/ru-ru/lifecycle/search

**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.00101-02 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 дистрибутива ПО СКЗИ

Установка дистрибутива КриптоПро CSP должна производиться пользователем, имеющим права администратора.

Для установки СКЗИ КриптоПро CSP сначала необходимо установить провайдер, а затем устанавливать остальные модули, входящие в состав комплектации.

**Примечание.** Модуль «КриптоПро CSP Lite» позволяет использовать функции СКЗИ под управлением ОС Windows без инсталляции, подробнее см. КриптоПро CSP Lite.

## 2.1 Установка СКЗИ с помощью мастера установки

Для начала установки программного обеспечения вставьте компакт-диск в дисковод. В стартовом окне выберите удобный для Вас язык установки и дистрибутив, соответствующий используемой операционной системе (см. рис. 1).


Рисунок 1. Установка СКЗИ КриптоПро CSP с диска

**Примечание.** Также установка может производиться с дистрибутива, полученного с сайта ООО «КРИПТО-ПРО». В таком случае пользователю нужно запустить файл дистрибутива CSPSetup.exe.

Откроется приветственное окно мастера установки КриптоПро CSP. Для изменения уровня КС (КС1/КС2/КС3) или языка установки нажмите кнопку **Дополнительные опции**. В открывшемся окне укажите язык установки и требуемый уровень безопасности и нажмите кнопку **Установить** (см. рис. 2).

**Примечание.** По умолчанию в окне установлен флаг **Установить корневые сертификаты**. При установке СКЗИ в хранилище «Доверенные корневые центры сертификации» локального компьютера устанавливаются следующие корневые сертификаты (перечислены значения соответствующих имен субъекта (CN)): CryptoPro GOST Root CA, Минкомсвязь России и Головной удостоверяющий центр.

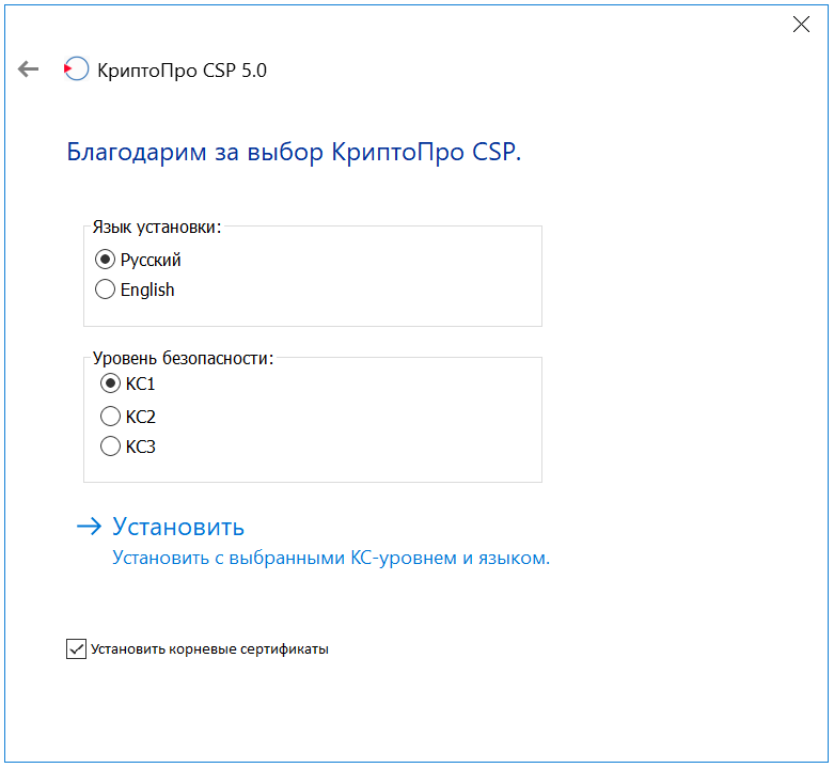



Рисунок 2. Установка СКЗИ КриптоПро CSP

Для дальнейшей установки КриптоПро CSP в окне мастера установки нажмите кнопку **Далее** (см. рис. 3).

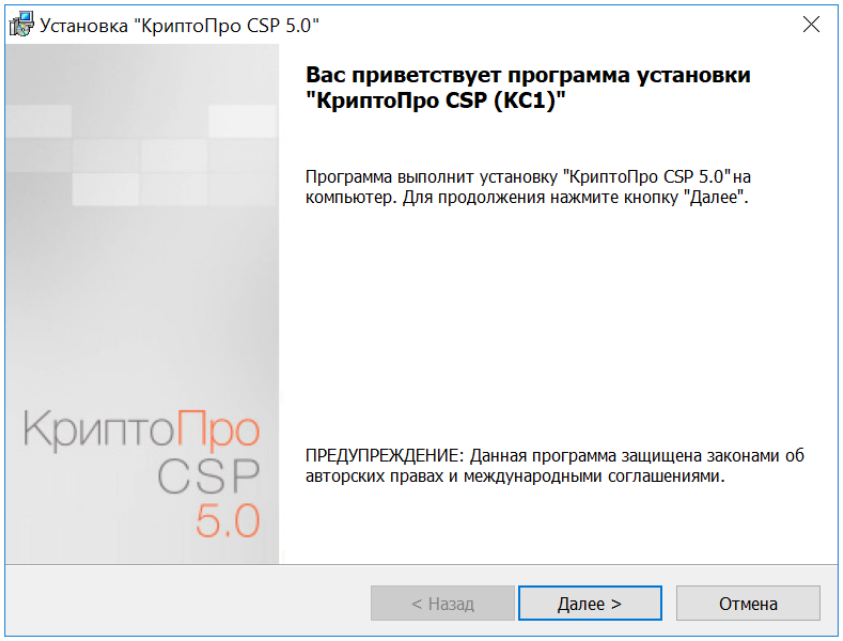



Рисунок 3. Мастер установки КриптоПро CSP

Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. В процессе установки будет предложено зарегистрировать дополнительные считыватели ключевой информации, дополнительные датчики случайных чисел или настроить криптопровайдер на использование

службы хранения ключей. Все эти настройки можно произвести как в момент установки криптопровайдера, так и в любой момент после завершения установки через панель свойств.

После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

## 2.2 Установка СКЗИ из командной строки

Дистрибутивы КриптоПро CSP доступны в виде самораспаковывающегося архива `CSPSetup.exe`, содержащего все платформы и исполнения, и в виде отдельных .msi пакетов.

При установке КриптоПро CSP можно использовать различные параметры командной строки, влияющие на устанавливаемые компоненты, начальную настройку продукта и другое.

**Примечание.** Общие сведения о параметрах командной строки msiexec.exe (Windows Installer) можно посмотреть в документации Microsoft.

Самораспаковывающийся архив построен на базе модифицированного модуля sfx для 7zip, большинство параметров исходного sfx может быть использовано и для `CSPSetup.exe`. Например, установка без диалога Extracting — `-gm2`.

Для установки КриптоПро CSP введите следующую команду в командной строке и укажите необходимые параметры:

```
msiexec /i <полный или относительный путь к .msi-файлу> <параметры>
```

Подробное описание параметров установки СКЗИ содержится в файле `msi-readme.txt`, входящем в состав дистрибутива СКЗИ.

## 2.3 Удаление ПО СКЗИ

Рекомендуется удалять установленное ПО СКЗИ с помощью Панели управления Windows (Панель управления → Программы и компоненты → Удаление программы). После удаления ПО СКЗИ обязательно перезагрузите компьютер.

Для удаления КриптоПро CSP через командную строку введите следующую команду:

```
msiexec /x {50F91F80-D397-437C-B0C8-62128DE3B55E}
```

# 3 Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС Windows необходимо:

1) запомнить текущую конфигурацию КриптоПро CSP (установленные ДСЧ, считыватели, носители, параметры алгоритмов по умолчанию и т.п.);

2) удалить штатными средствами ОС дистрибутив КриптоПро CSP (разд. 2.3);

3) установить аналогичный новый дистрибутив КриптоПро CSP (разд. 2);

4) при необходимости внести изменения в настройки.

**Примечание.** Ключи и сертификаты сохраняются автоматически.

# 4 Настройка СКЗИ

## 4.1 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. Данный режим должен быть включён при инсталляции СКЗИ, либо через контрольную панель КриптоПро CSP, вкладка «Безопасность» (см. рис. 4).

**Примечание.** Отключение режима усиленного контроля использования ключей допускается исключительно в тестовых целях.

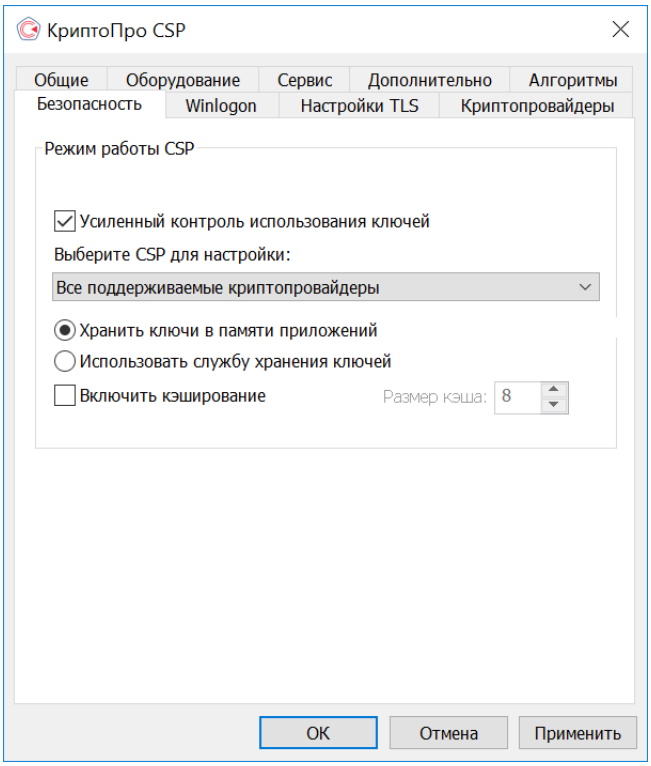



Рисунок 4. Включение режима усиленного контроля использования ключей в контрольной панели КриптоПро CSP

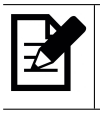
Проверить, включён ли режим усиленного контроля использования ключей, можно в контрольной панели КриптоПро CSP (вкладка «Безопасность»), либо посмотрев значение ключа `StrengthenedKeyUsageControl` в ветке реестра `HKEY_LOCAL_MACHINE\SOFTWARE\[Wow6432Node]\Crypto Pro\Cryptography\CurrentVersion\Parameters\StrengthenedKeyUsageControl`.

Если режим усиленного контроля использования ключей включался не при инсталляции СКЗИ, после включения режима необходимо произвести перезагрузку компьютера.

В криптопровайдере КриптоПро CSP для ключей ГОСТ Р 34.10-2001/2012 реализован дополнительный контроль доверенности сертификата ключа проверки электронной подписи, для чего совершается построение цепочек сертификатов до доверенных ключевых сертификатов, находящихся в хранилище локального

компьютера CryptoProTrustedStore («Доверенные корневые сертификаты КриптоПро CSP», «CryptoPro CSP Trusted Roots»). Данное хранилище сертификатов автоматически создаётся при инсталляции СКЗИ. После успешного завершения инсталляции необходимо в обязательном порядке произвести установку доверенных корневых сертификатов в хранилище CryptoProTrustedStore с помощью оснастки Сертификаты либо с помощью утилиты `certmgr`:

```
certmgr.exe -inst -cert -silent -store mCryptoProTrustedStore -file ca.cer
```



**Примечание.** Работа СКЗИ без установки доверенных корневых сертификатов в хранилище CryptoProTrustedStore допускается исключительно в тестовых целях.

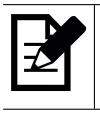
После проведения установки доверенных корневых сертификатов в хранилище CryptoProTrustedStore следует перезагрузить компьютер.

Сертификаты открытых ключей ГОСТ Р 34.10-2001/2012, для которых нельзя построить цепочку к корневым сертификатам в хранилище CryptoProTrustedStore, являются недоверенными. Для их удаления можно воспользоваться утилитами `certmgr` либо `cryptcp`:

```
certmgr.exe -delete -cert -store uMy -dn CN=test-user
```

```
cryptcp.exe -delcert -dn CN=test-user -uMy
```

## 4.2 Отключение функций телеметрии на ОС Windows 10/Server 2016/Server 2019



**Примечание.** Отключение функций телеметрии является обязательным условием эксплуатации СКЗИ под управлением ОС Windows 10/Server 2016/Server 2019.

Для отключения функций телеметрии на ОС Windows 10/Server 2016/Server 2019 необходимо выполнить следующие действия:

1) Проверить наличие и статус сервиса DiagTrack (Панель управления → Система и безопасность → Администрирование → Службы).

2) Если сервис запущен, то остановить его.

3) Удалить запись регистрации сервиса DiagTrack из реестра (Пуск → Выполнить → `regedit`, раздел `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services`. Здесь необходимо найти и удалить папку DiagTrack).

4) Удалить подготовленные к отправке данные, которые сохраняются в четырех файлах с расширением *.rbs, хранящихся в директории `%ProgramData%\Microsoft\Diagnosis`. Имена файлов для production сборок ОС – event00.rbs, event01.rbs, event10.rbs и event11.rbs. Для insider сборок ОС имена могут отличаться, поэтому необходимо удалить все файлы с расширением *.rbs. При возникновении проблем с удалением данных файлов необходимо в свойствах на вкладке «Безопасность» разрешить полный доступ к файлу, а затем удалить.

5) Остановить автоматическую (AutoLogger) ETW сессию AutoLogger-DiagTrack-Listener, которую DiagTrack активирует в процессе своей остановки.

6) Удалить файл, в который автоматическая (AutoLogger) ETW сессия AutoLogger-DiagTrack-Listener сохраняла собранные данные. Путь к файлу хранится в реестровой записи AutoLogger-DiagTrack-Listener в

значении FileName. Конфигурации автоматических (AutoLogger) ETW сессий находятся в ключе реестра `HKLM\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger`. Конфигурация целевой сессии хранится в данном ключе под записью AutoLogger-DiagTrack-Listener. В настоящее время данные сохраняются в файл `%ProgramData%\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-DiagTrack-Listener.etl`.

7) Удалить запись регистрации конфигурации автоматической (AutoLogger) ETW сессии AutoLogger-DiagTrack-Listener из реестра.

Данные действия необходимо выполнять после каждого кумулятивного обновления, поскольку данные обновления являются по сути полной переустановкой ОС и удаленные сервисы восстанавливаются.

## 4.3 Пересчет контрольных сумм системных библиотек ОС

КриптоПро CSP контролирует целостность некоторых библиотек операционной системы Microsoft Windows, которые могут заменяться при установке обновлений ОС. Для корректной работы СКЗИ после обновления ОС необходимо пересчитать контрольные суммы системных библиотек.

Обновить значения контрольных сумм можно с помощью кнопки «Пересчитать хэши» на вкладке «Дополнительно» панели управления КриптоПро CSP или с помощью модуля контроля целостности `cpverify`, выполнив команду:

```
cpverify -addreg -file <libname.dll>
```

Необходимо проконтролировать, что изменены контрольные суммы только следующих системных библиотек:

- certenroll.dll
- crypt32.dll
- cryptsp.dll
- inetcomm.dll
- kerberos.dll
- rastls.dll
- schannel.dll
- sspicli.dll
- wininet.dll

**Примечание.** Обновление контрольных сумм системных библиотек должно производиться пользователем с правами администратора.

## 4.4 Настройка групповых политик управления паролями ключевых контейнеров

Параметры групповой политики можно настраивать локально на каждом компьютере. Настройка локальной групповой политики осуществляется с помощью редактора локальной групповой политики (Local Group Policy Editor).

Для запуска редактора локальной групповой политики нажмите кнопку **Пуск**, введите `gpedit.msc` в поле **Начать поиск**, а затем нажмите клавишу **Ввод**. Также редактор можно открыть в качестве оснастки консоли управления MMC (подробнее см. Открытие локальной групповой политики).

Параметры групповой политики для СКЗИ КриптоПро CSP находятся в папке **Конфигурация компьютера** ⇒ **Административные шаблоны** ⇒ **Классические административные шаблоны (ADM)**

⇒ **КРИПТО-ПРО** ⇒ **КриптоПро CSP** (см. рис. 5).

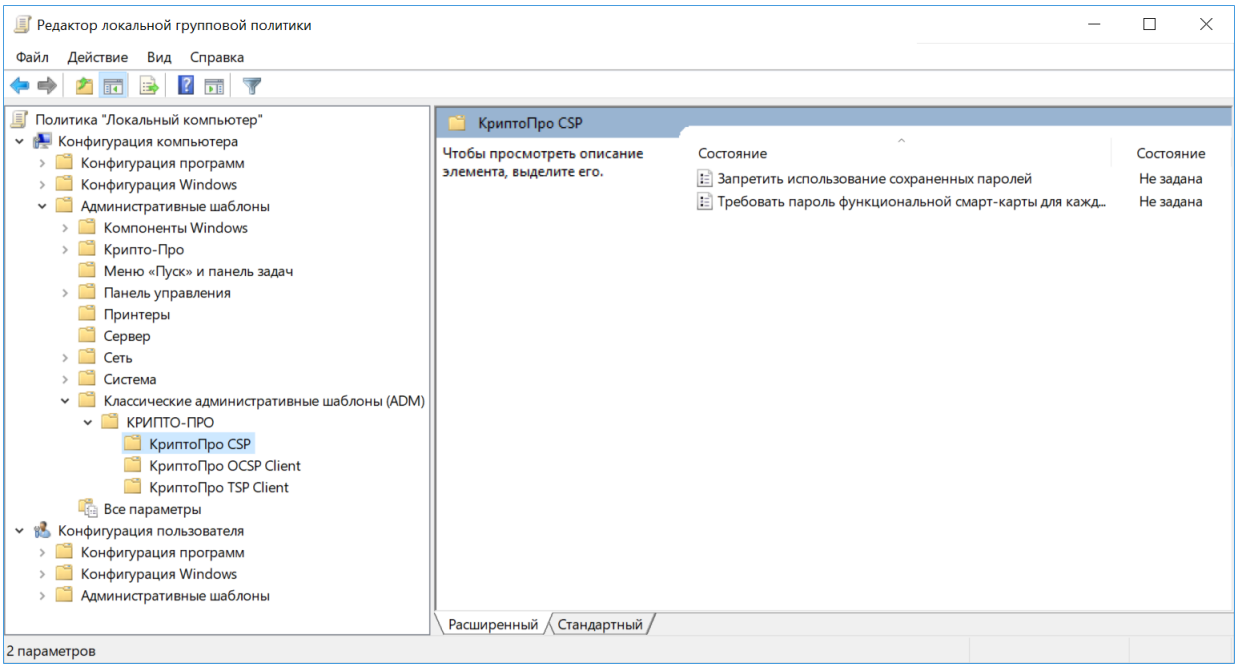



Рисунок 5. Параметры групповой политики для СКЗИ КриптоПро CSP

Аналогичные настройки политик возможно выполнить с помощью установки значений параметров в ветке реестра `HKEY_LOCAL_MACHINE\SOFTWARE\[WOW6432Node]\Crypto Pro\Cryptography\CurrentVersion\Parameters`.

### 4.4.1 Использование сохраненных паролей

При включении параметра групповой политики **«Запретить использование сохраненных паролей»** запрещено использование сохраненных паролей к ключевым контейнерам. Действие параметра распространяется как на использование ранее сохраненных паролей, так и на сохранение вводимых.

Если данный параметр политики включен, для всех ключевых контейнеров в окне аутентификации флаг **Сохранить пароль в системе** не установлен и поле неактивно (см. рис. 6).

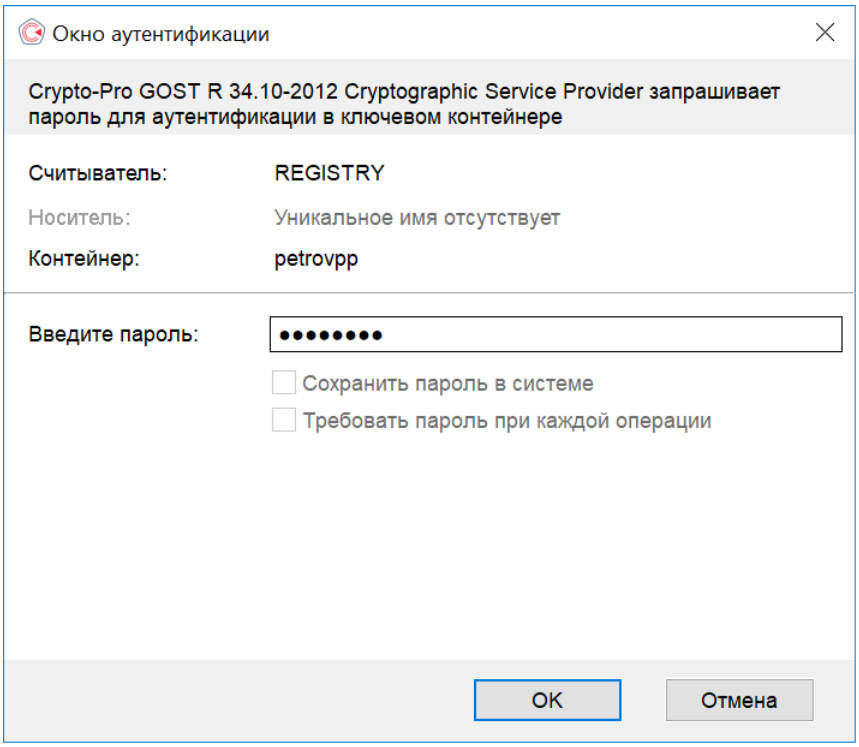



Рисунок 6. Окно аутентификации в контейнере в случае запрета использования сохраненных паролей

Параметру **«Запретить использование сохраненных паролей»** соответствует параметр реестра `HKEY_LOCAL_MACHINE\SOFTWARE\[WOW6432Node]\Crypto Pro\Cryptography\CurrentVersion\Parameters\DisableSavedPasswords`.

### 4.4.2 Требование пароля контейнера/носителя для каждой операции

При включении параметра групповой политики **«Требовать пароль контейнера/носителя для каждой операции»** запрещено сохранение пароля носителя в кэше криптопровайдера. Это означает, что пароль необходимо вводить при каждой операции с носителем и контейнерами.

Параметр групповой политики **«Требовать пароль контейнера/носителя для каждой операции»** может принимать следующие значения:

- Не задано
- Включено (для создаваемых контейнеров) — все генерируемые на компьютере ключи будут иметь повышенный уровень защиты даже без установки флагов **Требовать пароль при каждой операции** в окне аутентификации (см. рис. 7);
- Включено (для открываемых контейнеров) — при открытии для всех контейнеров будут требоваться пароли на каждую операцию;
- Включено (для всех контейнеров) — объединяет 2 предыдущих;
- Отключено

Если данный параметр политики включен, для всех ключевых контейнеров флаг **Требовать пароль при каждой операции** установлен и поле неактивно (см. рис. 7).

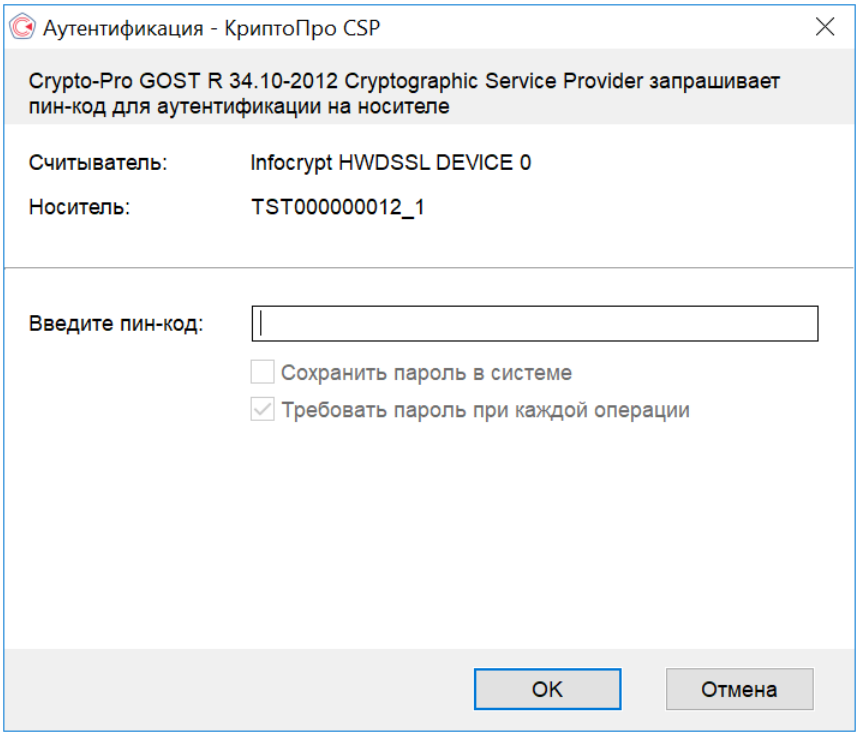



Рисунок 7. Окно аутентификации на носителе в случае запрета сохранения пароля носителя

Если политика не задана, требование пароля определяется значением ключа реестра `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Crypto Pro\Cryptography\CurrentVersion\Parameters\DisableCachePasswords`, который может принимать аналогичные политике значения: 0 — не задано, 1 — для открываемых контейнеров, 2 — для создаваемых контейнеров, 3 — для всех.

# 5 Использование СКЗИ на платформе Microsoft .NET Framework

ПО КриптоПро .NET позволяет использовать средство криптографической защиты информации КриптоПро CSP на платформе Microsoft .NET Framework. КриптоПро .NET реализует набор интерфейсов для доступа к криптографическим операциям .NET Cryptographic Provider:

- хэширование;
- подпись;
- шифрование;
- MAC;
- генерация ключей и т.д.

Кроме того, КриптоПро .NET позволяет использовать стандартные классы Microsoft для высокоуровневых операций:

- разбор сертификата;
- построение и проверка цепочки сертификатов;
- обработка CMS сообщений;
- установление защищенного обмена через SSL/TLS, HTTPS и FTPS;
- XML подпись и шифрование.

Подробную информацию, дистрибутивы, документацию и сценарии использования можно найти на сайте продукта. При использовании должны выполняться требования п. 1.5 ЖТЯИ.00101-02 30 01. Формуляр.

# 6 Состав и назначение компонент ПО СКЗИ

Программное обеспечение СКЗИ КриптоПро CSP при функционировании под управлением ОС Windows состоит из следующих компонент:

1) Сервисные модули;
2) Модули настройки встроенной подсистемы программной среды функционирования (СФ) ОС Windows;
3) СКЗИ КриптоПро CSP, реализующее целевые функции криптопровайдера в форме:
   - библиотек, загружаемых в адресное пространство приложения;
   - криптографического сервиса хранения ключей;
   - криптографического драйвера;
   - библиотек протокола «КриптоПро TLS».
4) Модуль аутентификации в домене Windows;
5) Модуль поддержки сетевой аутентификации КриптоПро TLS.

## 6.1 Сервисные модули

Сервисные модули обеспечивают контроль целостности дистрибутива КриптоПро CSP, его установку и удаление из операционной системы, а также конфигурацию параметров СКЗИ для каждого пользователя.

### 6.1.1 Модуль контроля целостности дистрибутива

Модуль `cpverify.exe` (см. Приложение 1 документа ЖТЯИ.00101-02 95 01. Правила пользования), предназначен для контроля целостности дистрибутива при установке и использовании ПО СКЗИ КриптоПро CSP на компьютере пользователя (поставляется совместно с дистрибутивом).

### 6.1.2 Дистрибутив

Дистрибутив СКЗИ поставляется в виде пакета «Windows Installer» (файл csp-win32-kc1-rus.msi или подобное название. В названии файла установщика присутствует обозначение платформы, для которой он предназначен, класс защиты и язык установки). При запуске файл установщика разворачивает структуры данных дистрибутива во временный каталог и проводит установку ПО СКЗИ.

### 6.1.3 Модуль конфигурации

Модуль `cpanel.cpl` обеспечивает возможность управления пользователем конфигурацией ПО СКЗИ, а также содержит возможности регистрации установленного ПО и получения пользователем дополнительной информации.

### 6.1.4 Модуль Wipefile

Модуль `wipefile` используется для удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях.

### 6.1.5 Модуль контроля целостности в драйвере

Для работы с любым отладчиком модуль контроля целостности в драйвере должен быть отключен. Порядок отключения данного модуля описан в руководстве программиста (CSP_5_0.chm, раздел Архитектура и встраивание СКЗИ на Windows/Unix).

**Примечание.** Отключение модуля контроля целостности в драйвере допускается только в тестовом режиме.

## 6.2 Модули настройки подсистемы программной СФ ОС Windows

Модули предназначены для обеспечения использования ПО СКЗИ в подсистеме программной СФ ОС Windows. Модули также реализуют форматы криптографических сообщений, используемых в защищенной электронной почте (S/MIME), Microsoft Office, Authenticode и функциях CryptoAPI 2.0, форматы сертификатов и их обработку.

**Примечание.** Полный перечень поддерживаемых приложений Microsoft приведен в документе ЖТЯИ.00101-02 95 01. Правила пользования.

Модули настройки классифицируются как подсистема программной СФ и ответственны за использование криптопровайдера со стороны приложений. Они обеспечивают вызов сервиса криптографических функций, но не обрабатывают ключевую и криптографически опасную информацию (не имеют доступа к ключам и т. п.).

### 6.2.1 Модуль расширения и настройки CryptoAPI 2.0

Модуль `cpext.dll` является зарегистрированной в системном реестре Windows динамической библиотекой (DLL) расширения CryptoAPI 2.0 и обеспечивает:

- установку соответствия между идентификаторами объектов (OID) в криптографических сообщениях и сертификатах открытых ключей и функциями СКЗИ;
- формирование и разбор криптографических сообщений и сертификатов открытых ключей.

### 6.2.2 Модули инициализации настройки встроенной подсистемы программной СФ ОС Windows

Модуль инициализации для ОС Windows реализован в виде драйвера `CProCtrl.sys`. Драйвер обеспечивает загрузку определенных динамических библиотек (DLL) в адресное пространство процессов, использующих СКЗИ.

Дополнительно этот модуль осуществляет контроль целостности установленного ПО СКЗИ и подсистемы программной СФ (периодический и при загрузке ОС).

### 6.2.3 Модуль настройки для системного DLL crypt32.dll

Модуль `cpcrypt.dll` загружается в виртуальное адресное пространство каждого процесса, к которому подгружается `crypt32.dll`, для установления перехватов функций, использующих провайдер.

Настройка заключается в добавлении программной СФ возможности обработки идентификаторов алгоритмов, реализуемых криптопровайдером.

### 6.2.4 Модуль настройки для системного DLL inetcomm.dll

Модуль `cpintco.dll` загружается в виртуальное адресное пространство каждого процесса, использующего `inetcomm.dll`, для установления перехватов функций.

Настройка заключается в поддержке дополнительных идентификаторов алгоритмов и возможностей S/MIME, реализуемых криптопровайдером, при использовании в ПО Microsoft Outlook и Microsoft Outlook Express.

### 6.2.5 Модуль настройки для системного DLL certocm.dll

Модуль `cpcertocm.dll` загружается в виртуальное адресное пространство процесса установки центра сертификации (CA) ОС Windows.

Модуль позволяет настроить центр сертификации при его установке так, чтобы поддерживались алгоритмы СКЗИ.

### 6.2.6 Модуль настройки для системного DLL wininet.dll

Модуль `cpwinet.dll` загружается в виртуальное адресное пространство процесса Internet Explorer/Microsoft Edge, если в него отображается `wininet.dll`.

Модуль позволяет правильно отображать алгоритмы КриптоПро TLS в Internet Explorer/Microsoft Edge.

### 6.2.7 Модуль настройки для системного DLL advapi32.dll

Модуль `cpadvai.dll` загружается в виртуальное адресное пространство каждого процесса, использующего `advapi32.dll`, для установления перехватов функций.

Настройка заключается в добавлении возможности обработки идентификаторов алгоритмов, реализуемых криптопровайдером.

### 6.2.8 Модуль настройки для системного DLL kerberos.dll

Модуль `cpkrb.dll` загружается в виртуальное адресное пространство процессов, использующих модуль `kerberos.dll`, и обеспечивает эмуляцию поддержки криптопровайдером стандарта Triple DES.

### 6.2.9 Модуль настройки TLS

Модуль `cpschan.dll` загружается в виртуальное адресное пространство процесса Internet Explorer/Microsoft Edge, если он использует TLS.

Модуль позволят использовать алгоритмы «КриптоПро TLS» в Internet Explorer/Microsoft Edge.

### 6.2.10 Модули настройки MS Office

Модуль `cpMSO.dll` загружается в виртуальное адресное пространство процессов MS Word и MS Excell и позволяет подписывать документы с помощью алгоритмов СКЗИ.

Модуль `cpExSec.dll` загружается в виртуальное адресное пространство процесса MS Outlook, и настраивает его для правильной работы с СКЗИ.

### 6.2.11 Модуль настройки XML

Модуль `cpXML.dll` загружается в виртуальное адресное пространство процессов, использующих XML, и позволяет применять алгоритмы СКЗИ для подписи XML.

### 6.2.12 Модуль настройки контроллера домена

Модуль `cpkdc.dll` загружается в виртуальное адресное пространство процессов доменной аутентификации на контроллере домена и обеспечивает возможность использования для проверки подписи алгоритмов, реализуемых СКЗИ.

## 6.3 СКЗИ «КриптоПро CSP» версия 5.0 R2 КС1 исполнение 1-Base

### 6.3.1 Интерфейсная библиотека криптопровайдера

Интерфейсная библиотека `cpcsp.dll` реализует стандартный интерфейс криптопровайдера, соответствующий спецификации Microsoft Cryptographic Service Provider, и обеспечивает данный интерфейс для обычных приложений через криптографический сервис по RPC, или для привилегированных приложений (имеющих право доступа к устройствам носителей ключевого контейнера) - непосредственно.

### 6.3.2 Интерфейсная библиотека криптографического сервиса

Интерфейсная библиотека `cpcspr.dll` обеспечивает возможность обращения обычных приложений к сервису криптографических функций по протоколу RPC.

### 6.3.3 Реализация криптопровайдера в форме сервиса хранения ключей

Модуль `cpcspi.dll` реализует целевые функции криптографической защиты информации при обращении по RPC с локального компьютера для интерфейсной библиотеки криптографического сервиса.

Модуль обеспечивает:
- хранение и работу с контекстом уровня библиотеки;
- хранение криптографических объектов:
  - ключевых пар (постоянных и временных);
  - открытых ключей (временных);
  - ключей сессий (временных симметричных);
  - объектов функции хэширования.
- выполнение криптографических преобразований.

### 6.3.4 Реализация криптопровайдера в форме подгружаемых библиотек

Интерфейс `cpcspi.dll` реализует целевые функции криптографической защиты информации для Интерфейсной библиотеки криптопровайдера (см. разд. 6.3.1) в варианте функционирования ПО СКЗИ без использования Интерфейса криптографического сервиса (см. разд. 6.3.2).

### 6.3.5 Реализация криптопровайдера в форме драйвера ядра ОС

Интерфейс `cpdrvlib.sys` реализует подмножество целевых функций криптографической защиты информации для Интерфейсной библиотеки криптопровайдера в варианте функционирования ПО СКЗИ в ядре ОС Windows. Драйвер поддерживает выполнение функций шифрования, имитозащиты, хэширования, проверки подписи и выработку ключей согласования на эфемерных ключах. Драйвер не поддерживает работу с пользовательскими ключами.

### 6.3.6 Интерфейсные модули ДСЧ

Обеспечивают реализацию доступа к следующим типам ДСЧ:

| | |
|---|---|
| `bio.dll` | БиоДСЧ |
| `sable.dll` | ДСЧ электронного замка "Соболь" |
| `accord.dll` | ДСЧ АМДЗ "Аккорд" |
| `crypton.dll` | ДСЧ АПМДЗ "КРИПТОН-ЗАМОК" |

| | |
|---|---|
| maxim.dll | ДСЧ АПМДЗ "МАКСИМ-М1" |
| ancud.dll | ДСЧ производства АНКАД |
| vityaz.dll | ДСЧ АПМДЗ "Витязь А" |

### 6.3.7 Панель управления ресурсами СКЗИ КриптоПро CSP

Управление ресурсами СКЗИ КриптоПро CSP осуществляется командным файлом cpanel.cpl через панель управления «Свойства — КриптоПро CSP». К основным средствам управления ресурсами СКЗИ относятся средства управления:

- лицензиями;
- ДСЧ;
- библиотеками считывания ключевой информации;
- закрытыми ключами (ключами ЭП) и сертификатами открытых ключей (ключей проверки ЭП);
- параметрами СКЗИ.

Определение правил пользования данными средствами приводится в документе ЖТЯИ.00101-02 92 01. Инструкция по использованию. Windows.

### 6.3.8 Интерфейсные модули устройств хранения ключевой информации

Модули обеспечивают реализацию доступа к конкретным типам ключевых носителей и считывателей:

| | |
|---|---|
| accord.dll | считыватель АМДЗ "Аккорд" |
| cpfkc.dll | токены и смарт-карты с поддержкой SESPAKE |
| cloud.dll | облачный токен |
| cryptoki.dll | доступ к ключам ФКН через интерфейс PKCS#11 |
| ds199x.dll | носители Dallas Touch Memory (iButton) |
| edoc.dll | платформа eDoc (УЛГ) |
| emv.dll | смарт-карты Gemalto (EMV) |
| esmarttoken.dll | смарт-карты и токены ESMART Token |
| esmarttokengost.dll | смарт-карты и токены ESMART Token ГОСТ |
| fat12.dll | съемные диски и раздел HDD/SDD |
| infocrypt.dll | токены InfoCrypt |
| inpaspot.dll | смарт-карты Alioth |
| jacarta.dll | токены и смарт-карты JaCarta |
| kst.dll | смарт-карты MorphoKST |
| mskey.dll | токены Multisoft MS_Key |

| | |
|---|---|
| novacard.dll | смарт-карты Novacard |
| pcsc.dll | базовый считыватель носителей, поддерживающих интерфейс PC/SC |
| reg.dl | системный реестр |
| ric.dll | смарт-карты Оскар и Форос (Магистра) |
| rosan.dll | смарт-карта Rosan |
| rutoken.dll | смарт-карты и токены Рутокен |
| sable.dll | считыватель электронного замка "Соболь" |
| safenet.dll | смарт-карты и токены Gemalto и SafeNet |

### 6.3.9 Библиотека поддержки доступа к ключевым носителям

Библиотека cpsuprt.dll обеспечивает реализацию общих функций доступа к различным устройствам хранения ключевых носителей.

### 6.3.10 Модуль ASN1

Поддерживает функции преобразования структур данных в машинно-независимое представление.

### 6.3.11 Использование ключей реестра Windows

Установка программного обеспечения должна производиться пользователем с правами администратора. При этом программа установки требует доступ к следующим ключам реестра:

- HKEY_LOCAL_MACHINE — полный доступ;
- HKEY_CLASSES_ROOT — полный доступ.

При использовании СКЗИ и создании ключей пользователей без использования флага CRYPT_MACHINE_KEYSET требуется доступ к следующим ключам реестра:

- HKEY_LOCAL_MACHINE — чтение, перечисление;
- HKEY_LOCAL_MACHINE\SOFTWARE\[WOW6432Node]\Crypto Pro\Settings\Users — создание подключей, чтение, перечисление;
- HKEY_LOCAL_MACHINE\SOFTWARE\[WOW6432Node]\Crypto Pro\Settings\Users\SID — полный доступ; SID — SID пользователя.

При использовании СКЗИ и создании ключей с использованием флага CRYPT_MACHINE_KEYSET дополнительно требуется доступ к следующим ключам реестра:

- HKEY_LOCAL_MACHINE\SOFTWARE\[WOW6432Node]\Crypto Pro\Settings — полный доступ.

Для изменения конфигурации СКЗИ с использованием панели управления (Control Panel), также требуется полный доступ к ключу реестра HKEY_LOCAL_MACHINE\SOFTWARE\[WOW6432Node]\Crypto Pro.

**Примечание.**
1) По умолчанию СКЗИ может использовать до 65536 дескрипторов криптографических объектов. Для увеличения этого значения необходимо добавить в ветку реестра HKEY_LOCAL_MACHINE\SOFTWARE\[WOW6432Node]\Crypto Pro\Cryptography\CurrentVersion\Parameters параметр DWORD, равный требуемому числу описателей, но не более 1048576.

## 6.4 Модуль аутентификации в домене Windows

Модуль `winlogonmgmt.dll` обеспечивает аутентификацию на базе электронной подписи с использованием алгоритмов ГОСТ 34.10-2001 (ГОСТ 34.11-94), ГОСТ 34.10-2012 (ГОСТ 34.11-2012).

Модуль аутентификации обеспечивает разграничение доступа к сети домена Windows либо к локальной машине Windows на основе проверки ЭП, выработанной с использованием ключа доступа, расположенного на ключевом носителе пользователя в ключевом контейнере СКЗИ. Сертификат открытого ключа проверки подписи заносится в систему при регистрации пользователя домена Windows.

## 6.5 Модуль поддержки сетевой аутентификации КриптоПро TLS

Модуль поддержки сетевой аутентификации реализуется в форме подгружаемой библиотеки и реализует подмножество интерфейса Microsoft SSPI (SSP/AP) (см. раздел MSDN). Модуль обеспечивает аутентичное защищенное соединение между пользователем и сервером. `cpssl.dll`, `cpsspap.dll` — при установке модуля аутентификации, поддерживающего аутентификацию в домене, `cpsspcore.dll`, `ssp.dll` — без возможности доменной аутентификации.

### 6.5.1 Инициализация библиотеки SSPI

Производится загрузка библиотеки `Secur32.dll`.

С помощью функции GetProcAddress получается указатель на функцию InitSecurityInterfaceA (InitSecurityInterfaceW в случае компиляции с Unicode).

Вызовом функции InitSecurityInterfaceA (InitSecurityInterfaceW в случае компиляции с Unicode) получается таблица функций SSPI.

Вместо использования GetProcAddress, можно подключить библиотеку импорта `secur32.lib` (входит в MS Platform SDK).

Заполняется структура SCHANNEL_CRED. Поля этой структуры должны быть нулевыми, кроме:
- SchannelCred.dwVersion = SCHANNEL_CRED_VERSION;
- SchannelCred.dwFlags = SCH_CRED_NO_DEFAULT_CREDS | SCH_CRED_MANUAL_CRED_VALIDATION;

Для сервера и не анонимного клиента заполняются также поля:
- SchannelCred.cCreds = 1;
- SchannelCred.paCred = &pCertContext.

**Примечание.** Контекст сертификата pCertContext должен содержать ссылку на закрытый ключ.

Производится вызов функции создания Credentials: AcquireCredentialsHandle с передачей ей структуры SCHANNEL_CRED и имени пакета — UNISP_NAME («Microsoft Unified Security Protocol Provider»).

Инициализация соединения клиентом производится вызовом InitializeSecurityContext без входного буфера, сервером — вызовом AcceptSecurityContext, после чего идет обычный цикл Handshake.

После установления соединения, но до начала передачи данных, приложение должно выполнить проверку параметров соединения и сертификата удаленной стороны.

Для получения сертификата удаленной стороны вызывается функция QueryContextAttributes с

аргументом SECPKG_ATTR_REMOTE_CERT_CONTEXT.

Для построения цепочки сертификатов рекомендуется использование функции CertGetCertificateChain, описанную в MSDN/Platform SDK/Security (с флагами проверки, соответствующими выбранному уровню безопасности). Рекомендуется использовать флаг CERT_CHAIN_CACHE_END_CERT | CERT_CHAIN_REVOCATION_CHECK_CHAIN.

Цепочка сертификатов проверяется функцией CertVerifyCertificateChainPolicy, описанной там же, с аргументом pszPolicy, равным OIDCERT_CHAIN_POLICY_SSL, и аргументом pPolicyPara, заполненным следующим образом:

- ZeroMemory(&polHttps, sizeof(HTTPSPolicyCallbackData));
- polHttps.cbStruct = sizeof(HTTPSPolicyCallbackData);
- polHttps.dwAuthType = AUTHTYPE_SERVER;
- polHttps.fdwChecks = 0;
- polHttps.pwszServerName = pwszServerName;
- memset(&PolicyPara, 0, sizeof(PolicyPara));
- PolicyPara.cbSize = sizeof(PolicyPara);
- PolicyPara.pvExtraPolicyPara = &polHttps

Необходимо, чтобы для каждого сертификата в цепочке pCertContext → pCertInfo → SubjectPublickeyInfo → Algoritm → pszObjId pszObjId заканчивалась на szOID_GR3410.

Вызывается функция QueryContextAttributes с аргументом ulAttribute, равным SECPKG_ATTR_CONNECTION_INFO, для получения параметров соединения и их проверки на выполнение условий:

- ConnectionInfo.dwProtocol == SP_PROT_TLS1_CLIENT;
- ConnectionInfo.aiCipher == CALG_G28147, ConnectionInfo.aiHash == CALG_GR3411;
- aiExch=CALG_DH_EX_EPHEM или CALG_DH_EX_SF;

Шифрование/расшифрование реализуется с помощью функций EncryptMessage()/DecryptMessage().

**Примечание.** Должна быть обеспечена корректная обработка кодов возврата функций SSPI. При этом следует учитывать, что требуется разная обработка в зависимости от того, является код возврата кодом успешного выполнения функции, кодом не фатальной ошибки, не требующей разрыва соединения, или кодом фатальной ошибки, требующей разрыва соединения. Все необрабатываемые коды возврата ошибок должны приводить к разрыву соединения.

Корректное завершение сессии осуществляется вызовом функции ApplyControlToken.

**Требования безопасности:**

1) Применение модуля поддержки сетевой аутентификации допускается только при использовании открытых ключей сервера и клиента, сертифицированных доверенным центром сертификации.

2) Приложением должны обеспечиваться:

- проверка сертификатов в сообщениях Certificate и CertVerify;
- проверка 12 байт в сообщениях Finished клиента и сервера, являющихся имитовставками к информации всего диалога клиент-сервер в процессе установления сессии;
- контроль соответствия имени клиента (сервера) IP-адресу, по которому установлена сессия.

## 6.6 КриптоПро CSP Lite

Модуль «КриптоПро CSP Lite» позволяет работать с конфигурацией СКЗИ под управлением ОС Windows с помощью конфигурационного файла, а не в реестре ОС.

В данном случае работа с конфигурационным файлом СКЗИ, работающим под управлением ОС семейства Windows, аналогична работе под управлением ОС семейства Linux, при которой конфигурационные настройки СКЗИ хранятся в обычном файле конфигурации, располагающимся в файловой системе ОС.

Для разработки на основе СКЗИ приложений требуется подключать в сборку вместо библиотек crypt32/advapi32 библиотеки capi20/capi10. При этом не требуется установка (инсталляция) криптопровайдера.

# 7 Требования по защите от НСД

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме раздела раздела 5 ЖТЯИ.00101-02 95 01. Правила пользования.

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

1) На всех HDD/SSD должна быть установлена файловая система NTFS.

2) Права доступа к системным и критичным каталогам (например, %Systemroot%\System32\config) должны быть установлены в соответствии с политикой безопасности, принятой в организации. На все директории, содержащие системные файлы Windows и программы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем, кроме пользователей Администратор (Administrator), СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ (CREATOR OWNER) и СИСТЕМА (SYSTEM).

3) Должны быть установлены ограничения на доступ пользователей к системному реестру в соответствии с принятой в организации политикой безопасности (например, с помощью ACL).

4) Должна быть исключена возможность удаленного редактирования системного реестра (например, с помощью параметров ветки реестра HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg).

5) Не рекомендуется использовать протокол SMB. В случае необходимости использования протокола SMB следует включить режимы подписи для SMB-пакетов (с помощью установки параметров реестра EnableSecuritySignature и RequireSecuritySignature ветки HKLM\System\CurrentControlSet\Services\LanManServer\Parameters в значение «1») и запретить передачу незашифрованного пароля сторонним SMB-серверам (установив параметр EnablePlainTextPassword ветки реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters в значение «0»).

6) У группы Everyone должны быть удалены все привилегии.

7) Должен быть переименован пользователь Administrator.

8) Должна быть отключена учетная запись для гостевого входа (Guest).

9) Должно быть исключено использование режима автоматического входа пользователя в операционную систему при ее загрузке.

10) Должно быть ограничено с учетом выбранной в организации политики безопасности использование пользователями Планировщика заданий (Task Scheduler).

11) Должны использоваться наиболее защищенные протоколы аутентификации, реализованные в ОС Windows, если функционирование СКЗИ не предусматривает применение других протоколов.

12) По возможности следует применять самые сильные шаблоны безопасности (Templates).

13) Должно быть запрещено использование функции резервного копирования паролей.

14) Должны быть отключены режимы отображения всех зарегистрированных на ПЭВМ пользователей и быстрого переключения пользователей.

15) Должен проводиться регулярный просмотр сообщений в журнале событий Event Viewer с периодичностью не реже 1 раза в неделю.

16) В настройках ОС, отвечающих за ведение журналов событий, необходимо установить режим архивирования журнала при его заполнении, либо ОС Windows должна быть настроена на завершение работы в случае переполнения журнала аудита (например, с помощью групповой политики «Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности»).

17) Должны использоваться только подписанные драйверы.

18) Должен быть исключен доступ анонимного пользователя (null-session) к списку разделяемых ресурсов и содержимому системного реестра (например, с помощью установки параметра реестра RestrictAnonymous ветки HKLM\SYSTEM\CurrentControlSet\Control\Lsa в значение «1»).

19) Необходимо запретить анонимный доступ к именованному каналу SPOOLSS (например, удалив имя SPOOLSS из ключа HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes).

20) Необходимо запретить автоматическое создание скрытых совместных ресурсов (например, с помощью установки параметров реестра AutoShareWks и AutoShareServer ветки HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters в значение «0»).

21) Необходимо отключить кэширование паролей последних 10 пользователей, вошедших в систему (например, с помощью ключа реестра HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon, установив параметр CachedLogonsCount со значением «0»).

22) Необходимо запретить параллельное использование дисководов несколькими пользователями (например, с помощью ключа реестра HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon, установив параметры AllocateFloppies и AllocateCDRoms со значением «1»).

# 8 Требования по криптографической защите

Должны выполняться требования по криптографической защите раздела 6 документа ЖТЯИ.00101-02 95 01. Правила пользования в части, касающейся ОС Windows.

Контролем целостности должны быть охвачены следующие файлы:

## Windows 32-bit

```
\Program Files\Crypto Pro\CSP\accord.dll
\Program Files\Crypto Pro\CSP\ancud.dll
\Program Files\Crypto Pro\CSP\bio.dll
\Windows\system32\certenroll.dll
\Program Files\Crypto Pro\CSP\certmgr.exe
\Program Files\Crypto Pro\CSP\cloud.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpadvai.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpcertocm.dll
\Windows\system32\cpcng.dll
\Program Files\Crypto Pro\CSP\cpanel.cpl
\Program Files\Common Files\Crypto Pro\AppCompat\cpcrypt.dll
\Program Files\Crypto Pro\CSP\cpcsp.dll
\Program Files\Crypto Pro\CSP\cpcspi.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpenroll.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpExSec.dll
\Program Files\Common Files\Crypto Pro\Shared\cpext.dll
\Program Files\Crypto Pro\CSP\cpfkc.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpintco.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpkrb.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpmail.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpmsi.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpMSO.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpoutlm.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cprastls.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpschan.dll
\Windows\system32\cpssl.dll
\Windows\system32\cpsspap.dll
\Program Files\Crypto Pro\CSP\cpsspi.dll
\Program Files\Crypto Pro\CSP\cpsuprt.dll
\Program Files\Common Files\Crypto Pro\Shared\cptools.exe
\Program Files\Crypto Pro\CSP\cpui.dll
\Program Files\Crypto Pro\CSP\cpverify.exe
\Program Files\Common Files\Crypto Pro\AppCompat\cpwinet.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpxml5.dll
\Windows\system32\crypt32.dll
\Program Files\Crypto Pro\CSP\cryptoki.dll
\Program Files\Crypto Pro\CSP\crypton.dll
\Windows\system32\cryptsp.dll
\Program Files\Crypto Pro\CSP\csptest.exe
\Program Files\Common Files\Crypto Pro\AppCompat\detoured.dll
\Program Files\Crypto Pro\CSP\ds199x.dll
```

```
\Program Files\Crypto Pro\CSP\dsrf.dll
\Program Files\Crypto Pro\CSP\edoc.dll
\Program Files\Crypto Pro\CSP\emv.dll
\Program Files\Crypto Pro\CSP\esmarttoken.dll
\Program Files\Crypto Pro\CSP\esmarttokengost.dll
\Program Files\Crypto Pro\CSP\fat12.dll
\Program Files\Crypto Pro\CSP\genkpim.exe
\Windows\system32\inetcomm.dll
\Program Files\Crypto Pro\CSP\infocrypt.dll
\Program Files\Crypto Pro\CSP\inpaspot.dll
\Program Files\Crypto Pro\CSP\jacarta.dll
\Windows\system32\kerberos.dll
\Program Files\Crypto Pro\CSP\kst.dll
\Program Files\Crypto Pro\CSP\maxim.dll
\Program Files\Crypto Pro\CSP\mskey.dll
\Program Files\Crypto Pro\CSP\novacard.dll
\Program Files\Crypto Pro\CSP\pcsc.dll
\Windows\system32\rastls.dll
\Program Files\Crypto Pro\CSP\reg.dll
\Program Files\Crypto Pro\CSP\ric.dll
\Program Files\Crypto Pro\CSP\rosan.dll
\Program Files\Crypto Pro\CSP\rutoken.dll
\Program Files\Crypto Pro\CSP\sable.dll
\Program Files\Crypto Pro\CSP\safenet.dll
\Windows\system32\schannel.dll
\Windows\system32\sspicli.dll
\Program Files\Crypto Pro\CSP\vityaz.dll
\Windows\system32\wininet.dll
\Program Files\Crypto Pro\CSP\wipefile.exe
```

## Windows 64-bit

```
\Program Files\Crypto Pro\CSP\accord.dll
\Program Files (x86)\Crypto Pro\CSP\accord.dll
\Program Files\Crypto Pro\CSP\ancud.dll
\Program Files (x86)\Crypto Pro\CSP\ancud.dll
\Program Files\Crypto Pro\CSP\bio.dll
\Program Files (x86)\Crypto Pro\CSP\bio.dll
\Windows\system32\certenroll.dll
\Windows\SysWOW64\certenroll.dll
\Program Files\Crypto Pro\CSP\certmgr.exe
\Program Files (x86)\Crypto Pro\CSP\certmgr.exe
\Program Files\Crypto Pro\CSP\cloud.dll
\Program Files (x86)\Crypto Pro\CSP\cloud.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpadvai.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpadvai.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpcertocm.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpcertocm.dll
\Windows\system32\cpcng.dll
\Windows\SysWOW64\cpcng.dll
```

```
\Program Files\Crypto Pro\CSP\cpanel.cpl
\Program Files\Common Files\Crypto Pro\AppCompat\cpcrypt.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpcrypt.dll
\Program Files\Crypto Pro\CSP\cpcsp.dll
\Program Files (x86)\Crypto Pro\CSP\cpcsp.dll
\Program Files\Crypto Pro\CSP\cpcspi.dll
\Program Files (x86)\Crypto Pro\CSP\cpcspi.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpenroll.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpenroll.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpExSec.dll
\Program Files\Common Files\Crypto Pro\Shared\cpext.dll
\Program Files (x86)\Common Files\Crypto Pro\Shared\cpext.dll
\Program Files\Crypto Pro\CSP\cpfkc.dll
\Program Files (x86)\Crypto Pro\CSP\cpfkc.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpintco.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpintco.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpkrb.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpkrb.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpmail.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpmail.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpmsi.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpmsi.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpMSO.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpoutlm.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpoutlm.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cprastls.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cprastls.dll
\Program Files\Crypto Pro\CSP\CProCtrl.sys
\Program Files\Common Files\Crypto Pro\AppCompat\cpschan.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpschan.dll
\Windows\SysWOW64\cpssl.dll
\Windows\system32\cpssl.dll
\Windows\system32\cpsspap.dll
\Windows\SysWOW64\cpsspap.dll
\Program Files\Crypto Pro\CSP\cpsspi.dll
\Program Files (x86)\Crypto Pro\CSP\cpsspi.dll
\Program Files\Crypto Pro\CSP\cpsuprt.dll
\Program Files (x86)\Crypto Pro\CSP\cpsuprt.dll
\Program Files (x86)\Common Files\Crypto Pro\Shared\cptools.exe
\Program Files\Crypto Pro\CSP\cpui.dll
\Program Files (x86)\Crypto Pro\CSP\cpui.dll
\Program Files (x86)\Crypto Pro\CSP\cpverify.exe
\Program Files\Common Files\Crypto Pro\AppCompat\cpwinet.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpwinet.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpxml5.dll
\Windows\system32\crypt32.dll
\Windows\SysWOW64\crypt32.dll
\Program Files\Crypto Pro\CSP\cryptoki.dll
\Program Files (x86)\Crypto Pro\CSP\cryptoki.dll
\Program Files\Crypto Pro\CSP\crypton.dll
```

```
\Program Files (x86)\Crypto Pro\CSP\crypton.dll
\Windows\system32\cryptsp.dll
\Windows\SysWOW64\cryptsp.dll
\Program Files\Crypto Pro\CSP\csptest.exe
\Program Files (x86)\Crypto Pro\CSP\csptest.exe
\Program Files\Common Files\Crypto Pro\AppCompat\detoured.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\detoured.dll
\Program Files\Crypto Pro\CSP\ds199x.dll
\Program Files (x86)\Crypto Pro\CSP\ds199x.dll
\Program Files\Crypto Pro\CSP\dsrf.dll
\Program Files (x86)\Crypto Pro\CSP\dsrf.dll
\Program Files\Crypto Pro\CSP\edoc.dll
\Program Files (x86)\Crypto Pro\CSP\edoc.dll
\Program Files\Crypto Pro\CSP\emv.dll
\Program Files (x86)\Crypto Pro\CSP\emv.dll
\Program Files\Crypto Pro\CSP\esmarttoken.dll
\Program Files (x86)\Crypto Pro\CSP\esmarttoken.dll
\Program Files\Crypto Pro\CSP\esmarttokengost.dll
\Program Files (x86)\Crypto Pro\CSP\esmarttokengost.dll
\Program Files\Crypto Pro\CSP\fat12.dll
\Program Files (x86)\Crypto Pro\CSP\fat12.dll
\Program Files (x86)\Crypto Pro\CSP\genkpim.exe
\Windows\system32\inetcomm.dll
\Windows\SysWOW64\inetcomm.dll
\Program Files\Crypto Pro\CSP\infocrypt.dll
\Program Files (x86)\Crypto Pro\CSP\infocrypt.dll
\Program Files\Crypto Pro\CSP\inpaspot.dll
\Program Files (x86)\Crypto Pro\CSP\inpaspot.dll
\Program Files\Crypto Pro\CSP\jacarta.dll
\Program Files (x86)\Crypto Pro\CSP\jacarta.dll
\Windows\system32\kerberos.dll
\Windows\SysWOW64\kerberos.dll
\Program Files\Crypto Pro\CSP\kst.dll
\Program Files (x86)\Crypto Pro\CSP\kst.dll
\Program Files\Crypto Pro\CSP\maxim.dll
\Program Files (x86)\Crypto Pro\CSP\maxim.dll
\Program Files\Crypto Pro\CSP\mskey.dll
\Program Files (x86)\Crypto Pro\CSP\mskey.dll
\Program Files\Crypto Pro\CSP\novacard.dll
\Program Files (x86)\Crypto Pro\CSP\novacard.dll
\Program Files\Crypto Pro\CSP\pcsc.dll
\Program Files (x86)\Crypto Pro\CSP\pcsc.dll
\Windows\system32\rastls.dll
\Windows\SysWOW64\rastls.dll
\Program Files\Crypto Pro\CSP\reg.dll
\Program Files (x86)\Crypto Pro\CSP\reg.dll
\Program Files\Crypto Pro\CSP\ric.dll
\Program Files (x86)\Crypto Pro\CSP\ric.dll
\Program Files\Crypto Pro\CSP\rosan.dll
\Program Files (x86)\Crypto Pro\CSP\rosan.dll
```

```
\Program Files\Crypto Pro\CSP\rutoken.dll
\Program Files (x86)\Crypto Pro\CSP\rutoken.dll
\Program Files\Crypto Pro\CSP\sable.dll
\Program Files (x86)\Crypto Pro\CSP\sable.dll
\Program Files\Crypto Pro\CSP\safenet.dll
\Program Files (x86)\Crypto Pro\CSP\safenet.dll
\Windows\system32\schannel.dll
\Windows\SysWOW64\schannel.dll
\Windows\system32\sspicli.dll
\Windows\SysWOW64\sspicli.dll
\Program Files\Crypto Pro\CSP\vityaz.dll
\Program Files (x86)\Crypto Pro\CSP\vityaz.dll
\Windows\system32\wininet.dll
\Windows\SysWOW64\wininet.dll
\Program Files (x86)\Crypto Pro\CSP\wipefile.exe
```

В случае нарушения целостности системных библиотек в результате обновления операционной системы необходимо пересчитать их контрольные суммы в соответствии с разд. 4.3.

# Приложение А
# Службы сертификации операционной системы Windows

Ведущие мировые производители системного и прикладного программного обеспечения активно интегрируют решения, основанные на Инфраструктуре открытых ключей в операционные системы и приложения. Ярким примером является операционная система Windows, полностью поддерживающая ИОК.

В операционной системе Microsoft Windows в полном объеме реализована Инфраструктура открытых ключей. Эта инфраструктура представляет собой интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих криптографию с открытыми ключами, а также для управления ими.

Инфраструктура открытых ключей предполагает иерархическую модель построения центров сертификации. Такая модель обеспечивает масштабируемость, удобство администрирования и согласованность с растущим числом продуктов и центров сертификации. Простейшая форма иерархии состоит из одного центра сертификации, а в общем случае – из множества с явно определенными отношениями родительский-дочерний.

Инфраструктура открытых ключей, реализованная в операционной системе Microsoft Windows, полностью поддерживает и позволяет создать иерархическую модель центров сертификации (см. рис. 8).

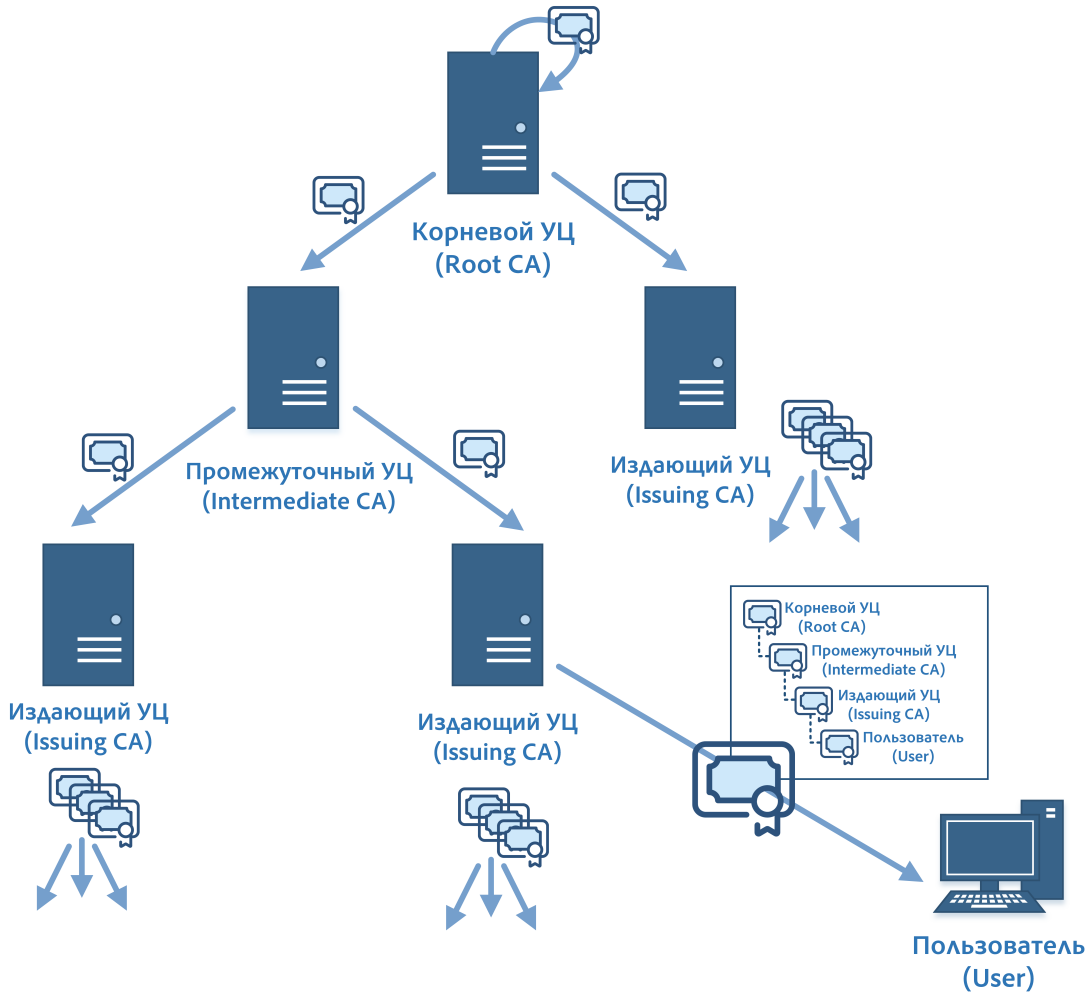



Рисунок 8. Иерархическая модель центров сертификации

В состав служб сертификации операционной системы Windows входят следующие службы и компоненты.

**Сервис сертификации**

Сервис сертификации предоставляет набор служб для выпуска, управления и использования сертификатов открытых ключей в защищенных технологиях и приложениях, использующих ИОК. Сервис сертификации выполняет основную роль в управлении безопасностью технологий и приложений и обеспечивает процесс достоверного и конфиденциального обмена информацией.

**Консоль центра сертификации**

Консоль центра сертификации является рабочим местом администратора безопасности, позволяющим управлять сертификатами открытых ключей (см. рис. 9).

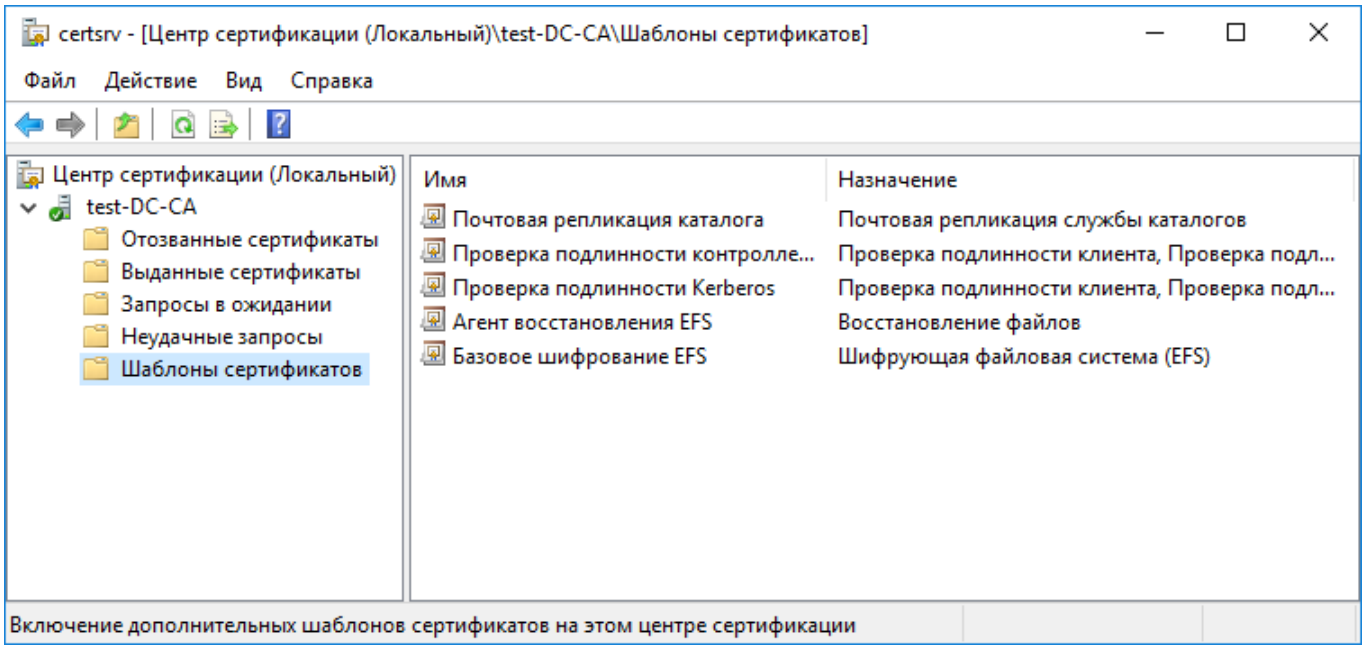



Рисунок 9. Консоль центра сертификации

**Средства расширения функциональности сервиса сертификации**

Средства расширения функциональности сервиса сертификации предоставляют набор методов, позволяющих изменять и развивать функциональность стандартного сервиса сертификации для удовлетворения потребности конкретной прикладной системы или технологии. Эти средства позволяют интегрировать сервис сертификации с различными сетевыми справочниками и приложениями, формировать состав сертификатов открытых ключей, модифицировать процесс управления сертификатами.

**Клиентские средства взаимодействия со службой сертификации**

Клиентские средства предоставляют пользователям различные методы для формирования закрытых ключей, запросов на сертификаты и обработки сертификатов, выпущенных службой сертификации.

Архитектура сервиса сертификации представлена на рис. 10.

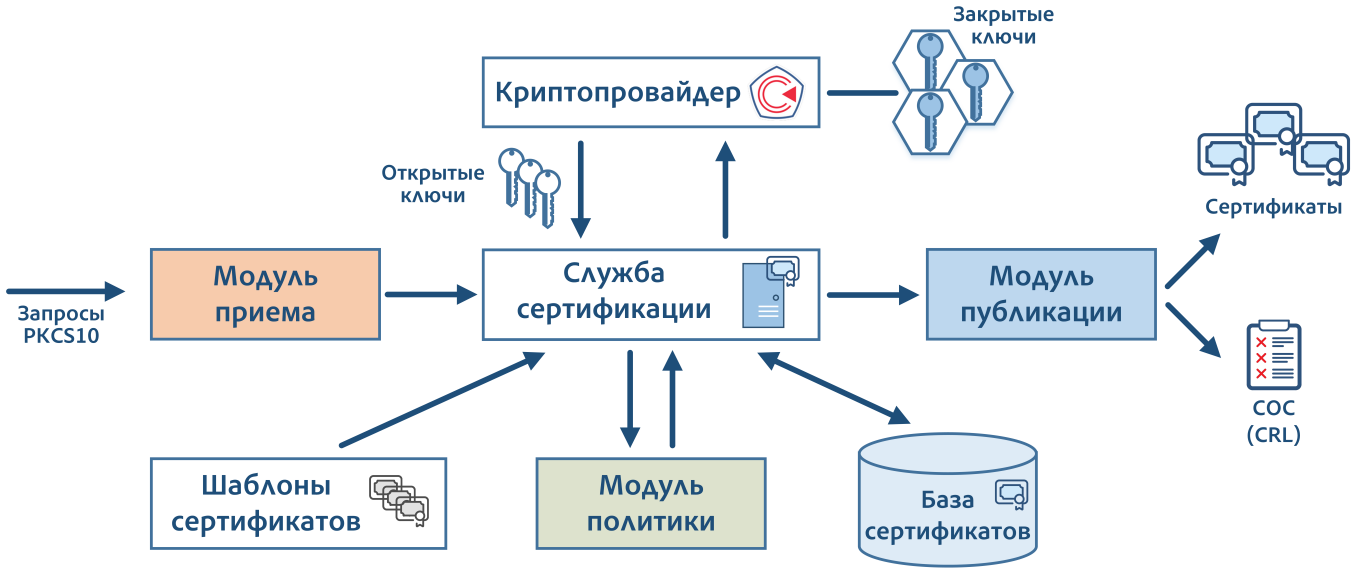



Рисунок 10. Архитектура сервиса сертификации

# Приложение Б
# 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. Б1). Несколько библиотек могут использовать один модуль аудита, возможна и обратная ситуация.

Таблица Б1. Модули аудита

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

Для управления протоколированием модуля аудита необходимо добавить следующие параметры в ветку реестра `HKEY_LOCAL_MACHINE\SOFTWARE\[WOW6432Node]\Crypto Pro\Cryptography\CurrentVersion\Debug`:

1) Для определения уровня протокола — DWORD параметр с именем модуля аудита `name` (см. табл. Б1)

Значением параметра является шестнадцатеричное число, состоящее из 3 частей, вида 0x0XX0YY0ZZ. Старшая часть (XX) определяет вид информации, которая будет записываться в **EventLog**, средняя (YY) — информацию, вывод которой осуществляется в **консоль**, младшая (ZZ) — информацию, отображаемую в **DbgView**.

В каждую часть необходимо установить значение, которое является побитовой суммой необходимых N_DB*-флагов (см. табл. Б2). Максимальное значение уровня логирования в каждой части — 0x3f.

**Примечание.** В EventLog ошибки соответствуют типу события «Ошибка», трассировка — типу события «Информация» («Сведения»), предупреждения — типу события «Предупреждение».

*Примеры использования:*

```
cloud = 0x0100003f // выводить только критические ошибки в EventLog и всю трассировочную
информацию в DbgView модуля облачного провайдера

csp = 0x03000000 // выводить все ошибки (критические и некритические) ядра CSP в EventLog
```

Таблица Б2. Уровни протоколирования

| | |
|---|---|
| N_DB_ERROR = 1 (0x01) | критические ошибки |
| N_DB_WARN = 2 (0x02) | некритические ошибки |
| N_DB_CALL = 4 (0x04) | информация о вызове функции |
| N_DB_LOG = 8 (0x08) | нейтральная информация |
| N_DB_TRACE = 16 (0x10) | отладочная информация |
| N_DB_CRUCIAL = 32 (0x20) | информация о важных событий (например, создание ключа, удаление ключевого контейнера, ...) |

2) Для определения формата протокола — DWORD параметр с именем вида `name_fmt` (см. табл. Б1).

Значением параметра является побитовая сумма необходимых DBFMT_*-флагов (см. табл. Б3).

*Пример использования:*

```
cloud_fmt = 0x00000042 - выводить значение GetLastError и номер нитки для модуля облачного провайдера
```

Таблица Б3. 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 |

**Примечание.** Для применения настроек необходим перезапуск приложения.

# 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 | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |