

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 KC1

(исполнение 1-Base)

Руководство администратора

безопасности.

Использование СКЗИ

под управлением ОС Windows

ЖТЯИ.00101-03 91 02
Листов 75

© 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	5
1 Основные технические данные и характеристики СКЗИ	6
1.1 Программно-аппаратные среды функционирования	6
1.2 Ключевые носители	6
2 Установка и обновление СКЗИ	7
2.1 Установка КриптоПро CSP с помощью мастера установки	7
2.2 Установка КриптоПро CSP из командной строки	16
2.3 Установка и настройка СКЗИ с помощью КриптоПро Мастер	17
2.4 Установка ПО Клиент КриптоПро HSM	19
2.5 Обновление КриптоПро CSP	24
3 Удаление СКЗИ	25
3.1 Удаление КриптоПро CSP	25
3.2 Удаление ПО Клиент КриптоПро HSM	25
4 Настройка и использование СКЗИ	26
4.1 Включение режима усиленного контроля использования ключей	26
4.2 Доступ к локальным смарт-картам через RDP	27
4.3 Очистка кэша контейнеров закрытых ключей и кэша паролей при блокировке рабочей станции	28
4.4 Отключение функций телеметрии на ОС Windows 10/11/Server 2016/Server 2019/Server 2022	29
4.5 Пересчет контрольных сумм системных библиотек ОС	29
4.6 Настройка групповых политик управления паролями ключевых контейнеров	31
4.6.1 Использование сохраненных паролей	31
4.6.2 Требование пароля контейнера/носителя для каждой операции	32
4.7 Настройка использования Microsoft Edge в режиме интеграции с Internet Explorer	33
4.8 Настройка клиентского компонента КриптоПро HSM	35
4.8.1 Устанавливаемые криптопровайдеры	35
4.8.2 Дополнительные настройки параметров клиента ПАКМ	39
4.8.3 Настройка конфигурации с несколькими ПАКМ	42
5 Состав и назначение компонент ПО СКЗИ	50
5.1 Дистрибутив	50
5.2 Использование ключей реестра Windows	50
5.3 Базовые модули СКЗИ	50
5.4 Модули настройки подсистемы программной СФ ОС Windows	51
5.5 Модули подсистемы программной СФ СКЗИ	53
5.6 Модули КриптоПро ЭЦП Browser plug-in	56
5.7 Модуль поддержки сетевой аутентификации КриптоПро TLS	58
5.7.1 Инициализация библиотеки SSPI	58
5.8 КриптоПро CSP Lite	59
6 Требования по обеспечению безопасности при эксплуатации СКЗИ	61
7 Требования по криптографической защите	63
8 Использование СКЗИ на платформе Microsoft .NET Framework	71
Приложение А. Управление протоколированием	72

Аннотация

Настоящее руководство содержит общее описание средства криптографической защиты информации «КриптоПро CSP» версия 5.0 R3 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 R3 KC1 (исполнение 1-Base) под управлением ОС Windows, 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)

APM 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 KC1 (исполнение 1-Base) функционирует в следующих группах программно-аппаратных сред:

Windows

Windows 7*/8/8.1 (x86, x64)
Windows 10 (x86, x64, ARM64)
Windows 11 (x64, ARM64)
Windows Server 2008 (x86, x64)
Windows Server 2008 R2/2012/2012 R2/2016/2019/2022 (x64)

**Версия Embedded/Embedded POSReady*

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.00101-03 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 обновление 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 КриптоПро CSP с помощью мастера установки

Для установки программного обеспечения вставьте компакт-диск в дисковод (см. [рис. 1](#)).



Рисунок 1. Установка СКЗИ КриптоПро CSP

Выберите удобный для Вас язык установки и дистрибутив, соответствующий используемой операционной системе.



Примечание. Также установка может производиться с дистрибутива, полученного с сайта ООО «КРИПТО-ПРО». В таком случае пользователю нужно запустить файл дистрибутива CSPSetup-5.0.exe.

В начальном окне Мастера установки нажмите кнопку **Установить**, чтобы начать установку КриптоПро CSP в конфигурации KC1 и языком операционной системы (см. [рис. 2](#)).

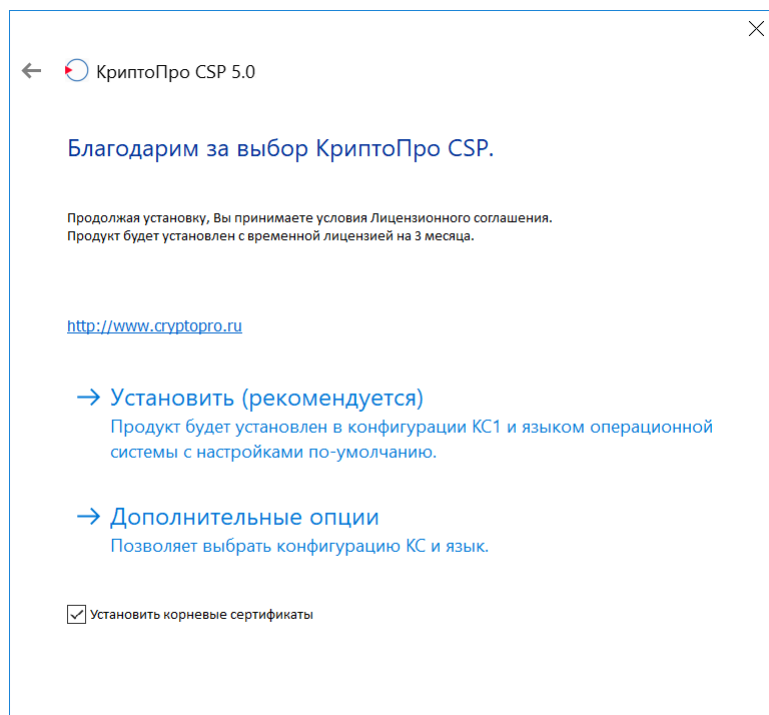


Рисунок 2. Начало установки

СКЗИ КриптоПро CSP обеспечивает классы защиты КС1, КС2, КС3 согласно требованиям ФСБ России. Для изменения конфигурации КС или языка установки нажмите кнопку **Дополнительные опции**. В открывшемся окне укажите язык установки и требуемый уровень безопасности и нажмите кнопку **Установить** (см. [рис. 3](#)).

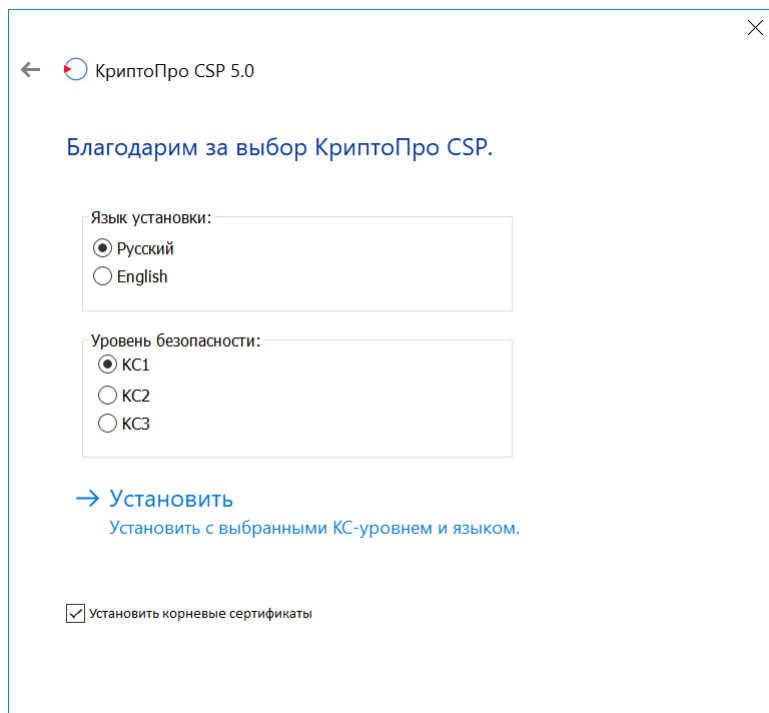


Рисунок 3. Выбор языка установки и уровня КС

Откроется Мастер установки КриптоПро CSP (KC1) (см. [рис. 4](#)).

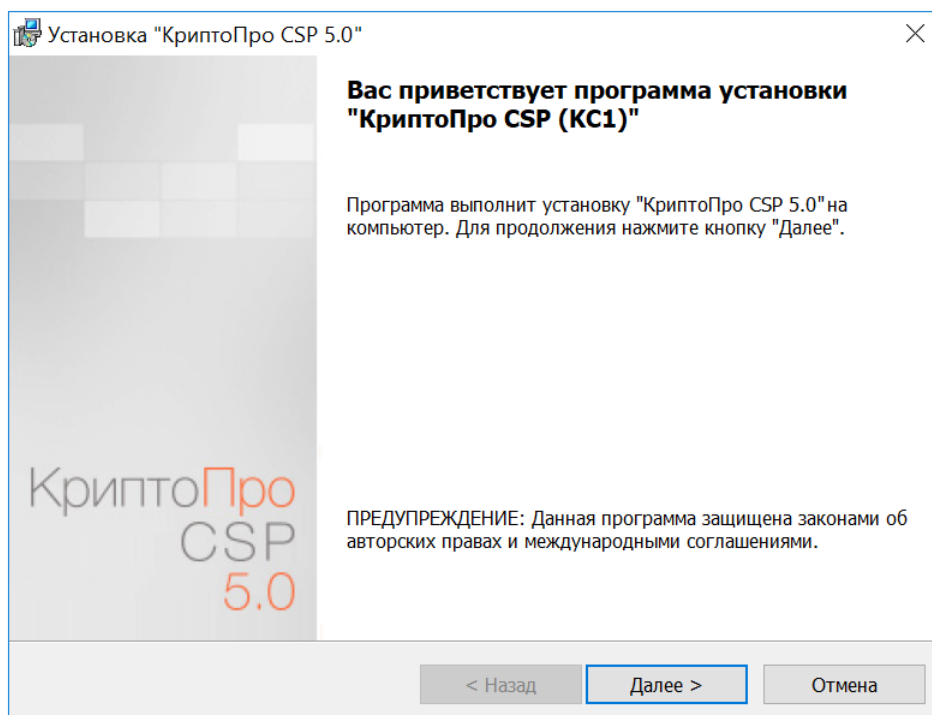


Рисунок 4. Приветственное окно Мастера установки КриптоПро CSP

Если на машине была установлена более ранняя версия СКЗИ КриптоПро CSP, то в окне появится информация об обновляемой версии (см. [рис. 5](#)).

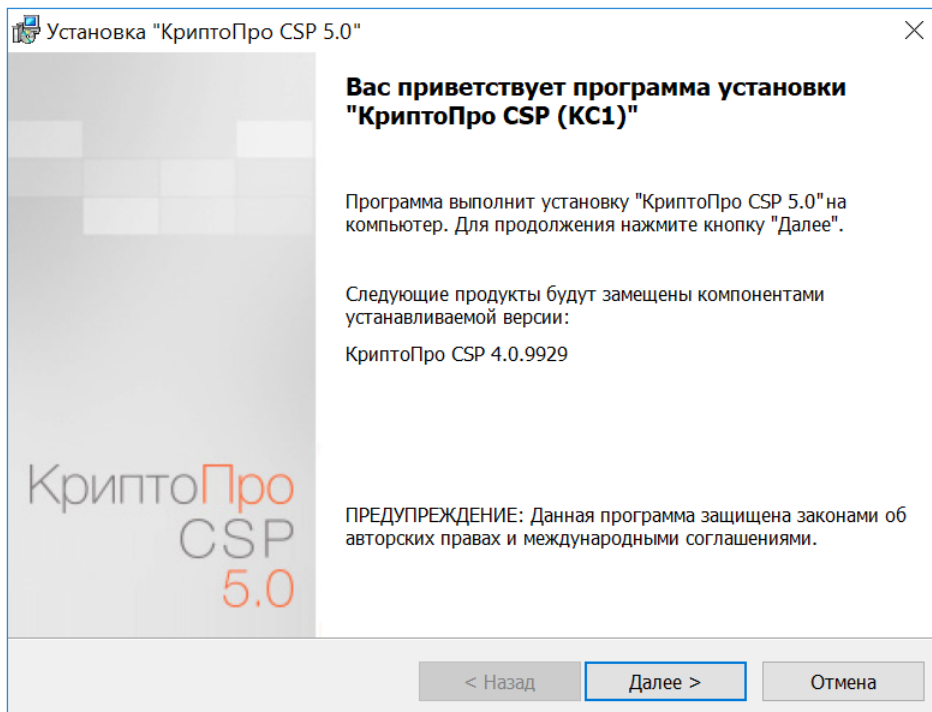


Рисунок 5. Установка КриптоПро CSP с замещением компонентов

Для продолжения установки КриптоПро CSP нажмите кнопку **Далее**. Внимательно прочитайте

лицензионное соглашение, которое выводится при первой установке (см. [рис. 6](#)).

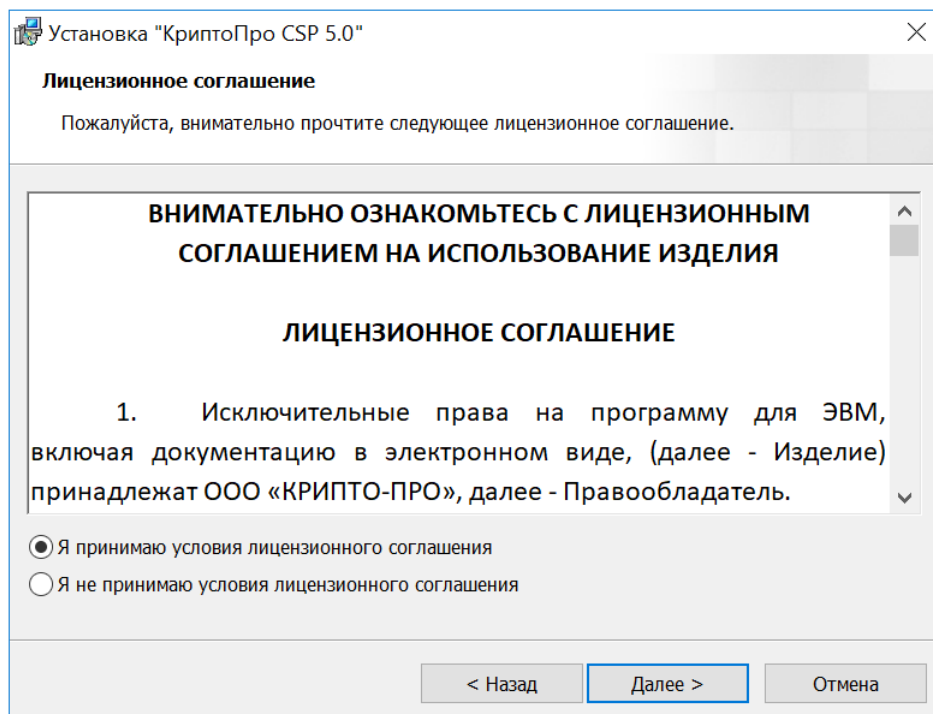


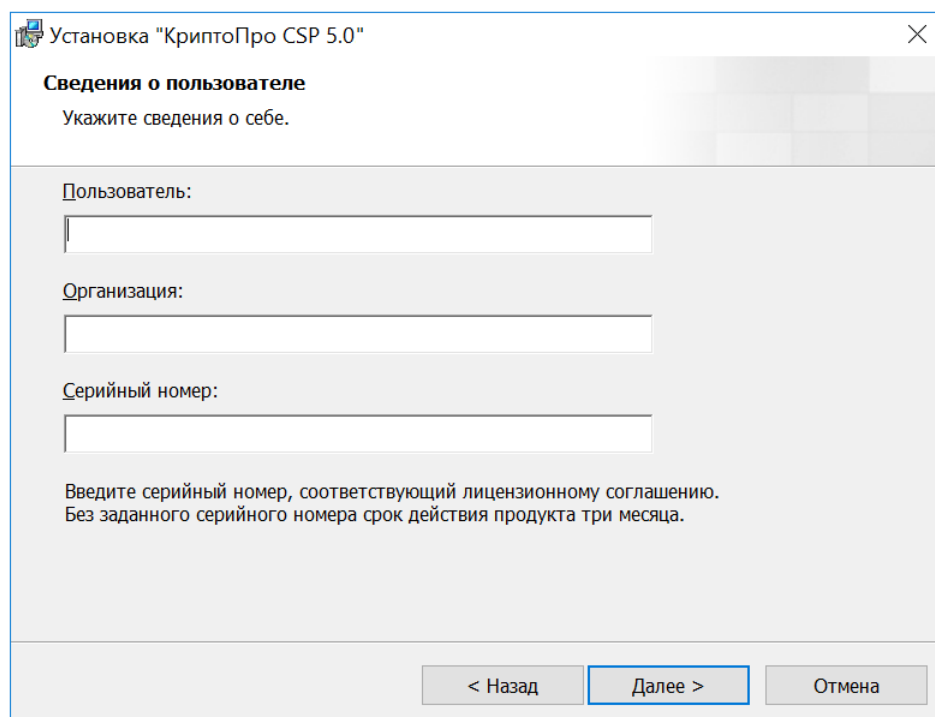
Рисунок 6. Лицензионное соглашение

В процессе установки может быть предложено:

- ввести серийный номер лицензии криптопровайдера (подробнее см. Раздел 2.3 ЖТЯИ.00101-03 92 01. Инструкция по использованию. Windows);
- зарегистрировать дополнительные считыватели ключевой информации (подробнее см. Раздел 2.4 ЖТЯИ.00101-03 92 01. Инструкция по использованию. Windows);
- настроить криптопровайдер на использование службы хранения ключей (подробнее см. Раздел 2.6 ЖТЯИ.00101-03 92 01. Инструкция по использованию. Windows);

Эти параметры можно изменить после завершения установки через панель управления КриптоПро CSP.

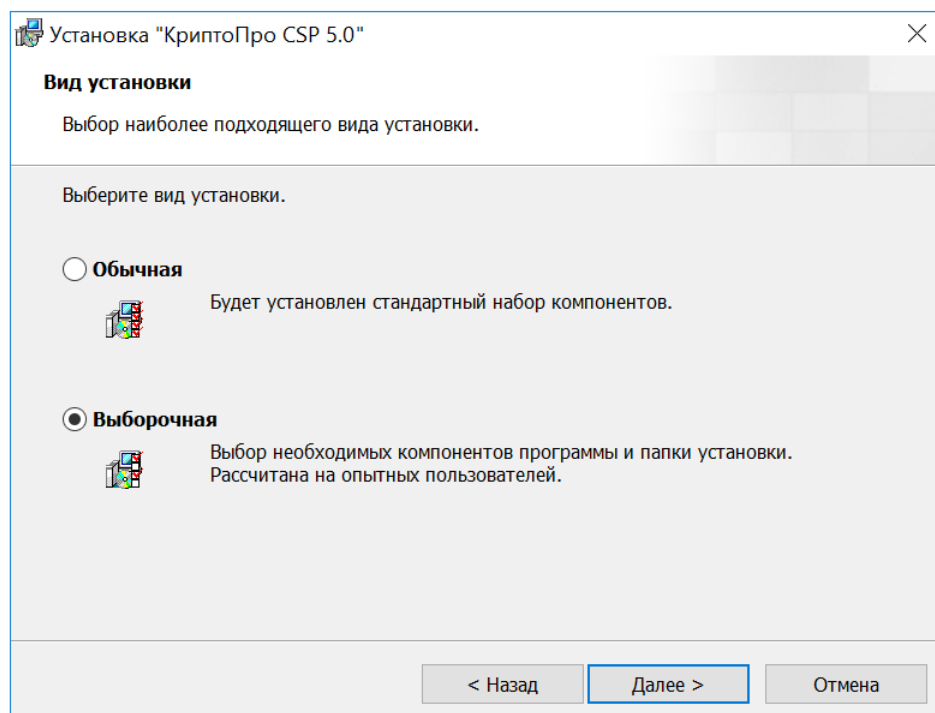
В окне «Сведения о пользователе» заполните сведения о себе и укажите серийный номер продукта (см. [рис. 7](#)). Без введенного серийного номера КриптоПро CSP устанавливается с временной лицензией на 3 месяца.



The screenshot shows the 'Установка "КриптоПро CSP 5.0"' window with the 'Сведения о пользователе' (User Information) tab selected. The window contains three text input fields: 'Пользователь:' (User), 'Организация:' (Organization), and 'Серийный номер:' (Serial number). Below these fields, a note states: 'Введите серийный номер, соответствующий лицензионному соглашению. Без заданного серийного номера срок действия продукта три месяца.' (Enter the serial number corresponding to the license agreement. Without a specified serial number, the product's validity period is three months). At the bottom, there are three buttons: '< Назад' (Back), 'Далее >' (Next), and 'Отмена' (Cancel). The 'Далее >' button is highlighted with a blue border.

Рисунок 7. Сведения о пользователе

В окне «Вид установки» выберите подходящий вид установки КриптоПро CSP (см. [рис. 8](#)).



The screenshot shows the 'Установка "КриптоПро CSP 5.0"' window with the 'Вид установки' (Installation Type) tab selected. The window contains two radio button options: 'Обычная' (Typical) and 'Выборочная' (Custom). The 'Обычная' option is described as 'Будет установлен стандартный набор компонентов.' (Standard set of components will be installed). The 'Выборочная' option is selected and described as 'Выбор необходимых компонентов программы и папки установки. Рассчитана на опытных пользователей.' (Selection of necessary program components and installation folder. Designed for experienced users). At the bottom, there are three buttons: '< Назад' (Back), 'Далее >' (Next), and 'Отмена' (Cancel). The 'Далее >' button is highlighted with a blue border.

Рисунок 8. Выбор вида установки

По умолчанию (вид установки **Обычная**) устанавливаются только основные файлы для работы СКЗИ (для Windows Server 2008 по умолчанию также устанавливается «Драйверная библиотека CSP»). При необходимости (вид установки **Выборочная**) можно изменить набор компонентов для установки (см. [рис. 9](#)).

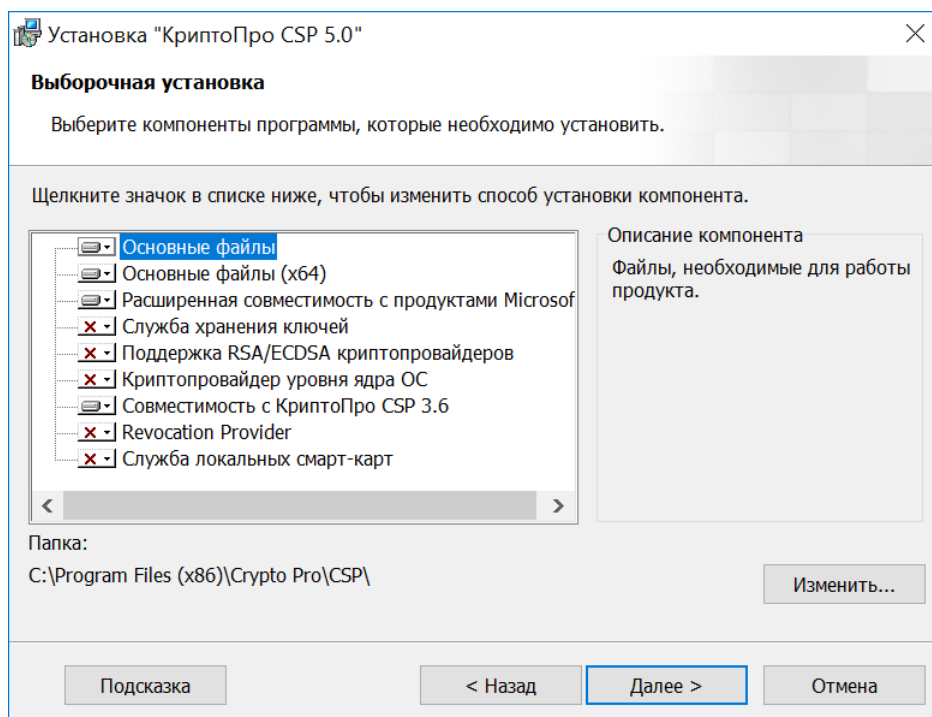


Рисунок 9. Выборочная установка

Для установки доступны следующие компоненты:

- **Расширенная совместимость с продуктами Microsoft** — обеспечивает совместимость с такими приложениями, как Microsoft Office, Outlook Express, Internet Explorer. Необходим для входа в систему по смарт-картам и TLS.
- **Служба хранения ключей** — обеспечивает хранение, использование и кэширование ключей в отдельном сервисе ОС (только для пассивных хранилищ ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене).
- **Поддержка RSA/ECDSA криптопровайдеров** — обеспечивает взаимодействие с криптопровайдерами, поддерживающими алгоритмы RSA и ECDSA. Не допускается использовать для защиты информации, отличной от тестовых данных.
- **Криптопровайдер уровня ядра ОС** — необходим для работы криптопровайдера в службах и ядре Windows (TLS-сервер, EFS, IPsec).
- **Совместимость с КриптоПро CSP 3.6** — регистрирует имена провайдеров, совместимые с КриптоПро CSP 3.6. Необходим только при наличии в хранилище «Личные» сертификатов, установленных с КриптоПро CSP 3.6.
- **Revocation Provider** — механизм проверки текущего статуса сертификата с использованием OCSP. Является дополнением к стандартному механизму Windows проверки статуса сертификата на основе списка отозванных сертификатов (COC, CRL). Кроме этого предоставляет возможность использования COC, выпущенных по правилам, описанным в RFC 3280.
- **Служба локальных смарт-карт** — обеспечивает доступ к локальным смарт-картам по RDP. Настройка службы описана в [разд. 4.2](#).



Примечание. В состав SDK СКЗИ входит описание параметров командной строки установщика Windows (файл `sdk\chm\msi-readme.txt`), которые удобно использовать для автоматического развертывания дистрибутива.

После нажатия на кнопку **Далее** Мастером установки предлагается запланировать или отменить установку библиотек поддержки считывателей (см. [рис. 10](#)).

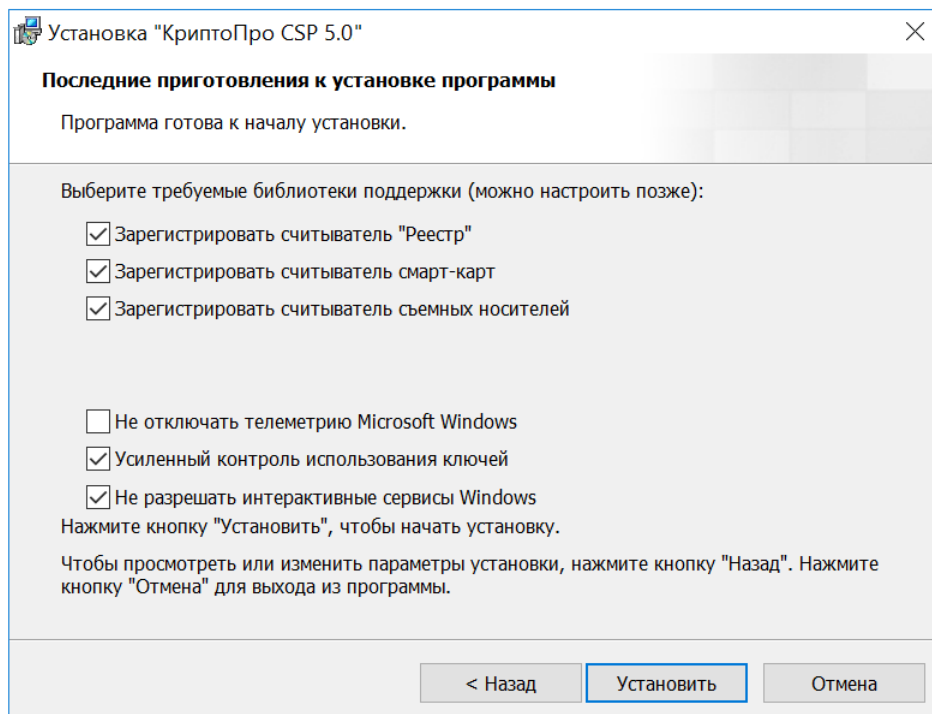


Рисунок 10. Выбор библиотек поддержки, установка усиленного контроля использования ключей и управление сервисами Windows

В окне возможно установить некоторые параметры ОС Windows — службы телеметрии и интерактивных сервисов. По умолчанию при установке СКЗИ на ОС Windows происходит остановка служб телеметрии.



Примечание. Отключение функций телеметрии является обязательным условием эксплуатации СКЗИ под управлением ОС Windows 10/11/Server 2016/Server 2019/Server 2022 (подробнее об отключении телеметрии см. [разд. 4.4](#)).

Также необходимо включить режим усиленного контроля использования ключей. Данный режим осуществляет контроль срока действия долговременных ключей электронной подписи и ключевого обмена, контроль доверенности ключей проверки электронной подписи и контроль корректного использования программного датчика случайных чисел.



Примечание. Использование СКЗИ КриптоПро CSP без включения режима усиленного контроля использования ключей разрешается только в тестовых целях.

При выборе усиленного контроля использования ключей появится окно предупреждения с перечнем необходимых действий для корректной настройки криптопровайдера (см. [рис. 11](#)).

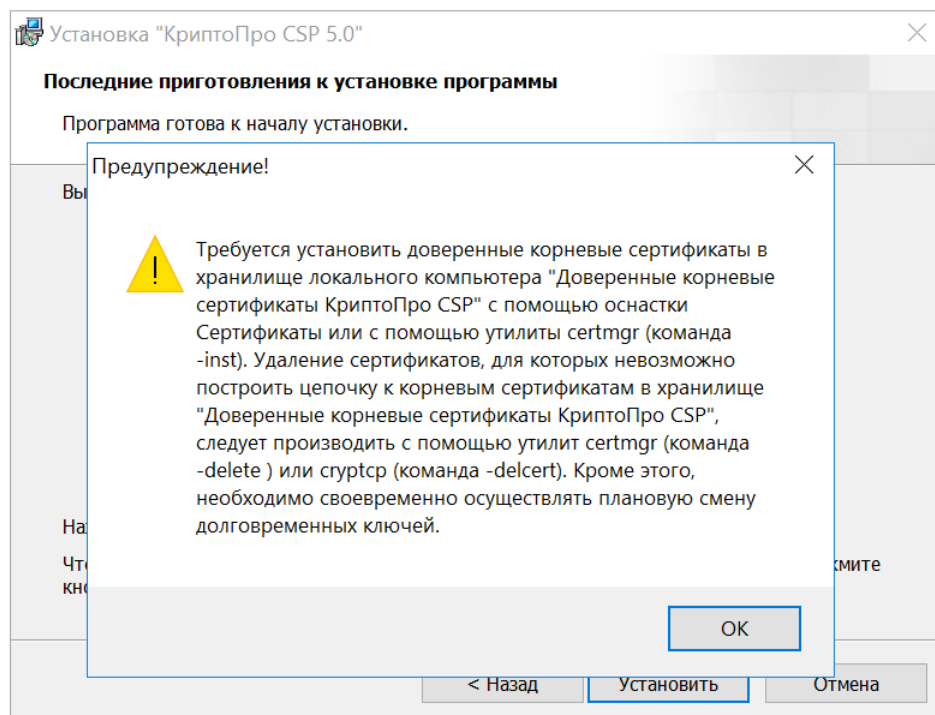


Рисунок 11. Установка усиленного контроля использования ключей

Для начала установки СКЗИ КриптоПро CSP нажмите кнопку **Установить**. В окне Мастера установки будет отображено текущее состояние процесса установки (см. [рис. 12](#)).

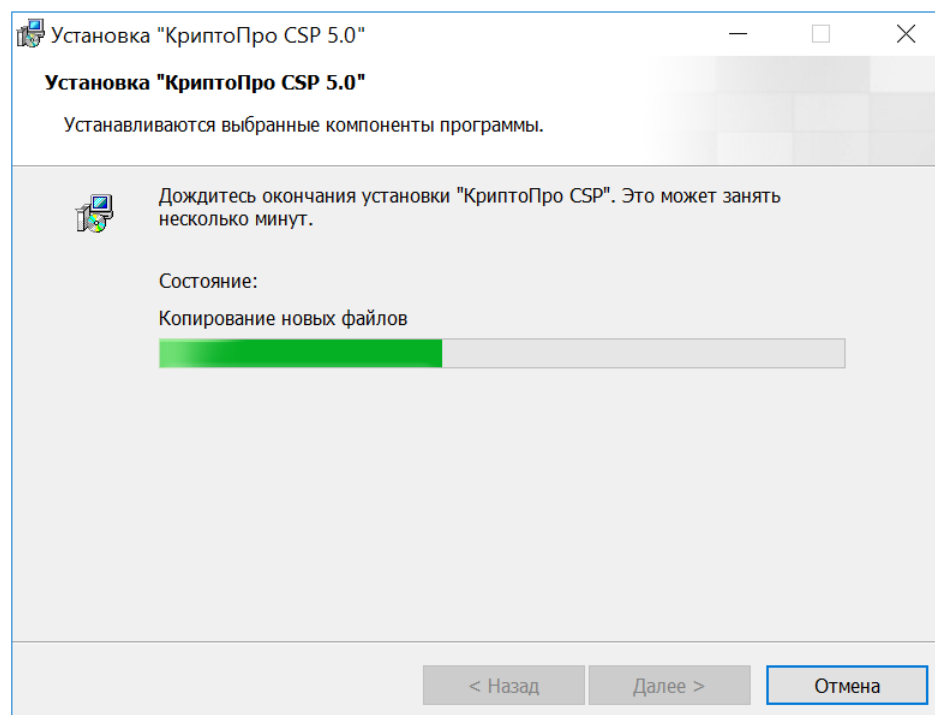


Рисунок 12. Процесс установки КриптоПро CSP

При установке криптопровайдера с включенным режимом усиленного контроля использования ключей будут запрошены данные с ДСЧ. В случае ошибки получения данных будет отображено окно ошибки (см.

рис. 13).

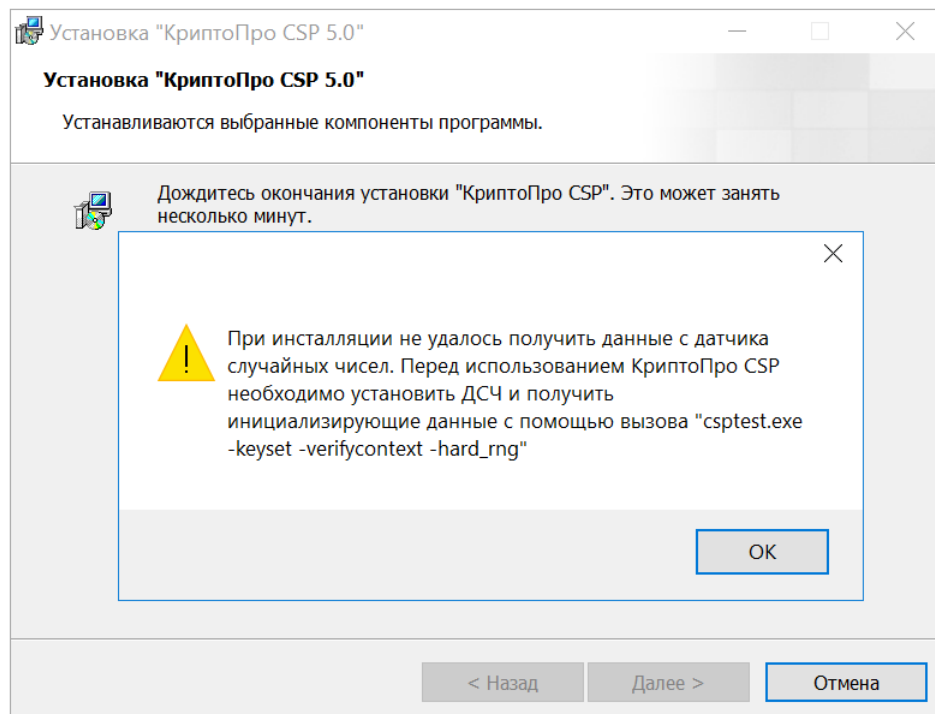


Рисунок 13. Окно ошибки получения данных с ДСЧ

В этом случае при начале работы пользователя в системе с установленным СКЗИ КриптоПро CSP необходимо проверить, что зарегистрирован хотя бы один физический датчик случайных чисел (например, биологический ДСЧ, внешняя гамма или аппаратный ДСЧ).

После завершения установки СКЗИ с включенным режимом усиленного контроля использования ключей **необходимо в обязательном порядке** установить доверенные корневые сертификаты в хранилище сертификатов локального компьютера «CryptoProTrustedStore» («Доверенные корневые сертификаты КриптоПро CSP», «CryptoPro CSP Trusted Roots») с помощью оснастки **Сертификаты** либо с помощью утилиты certmgr.exe:

```
certmgr.exe -inst -cert -silent -store mCryptoProTrustedStore -file <имя файла сертификата>
```

При завершении установки всех компонентов криптопровайдера Мастер сообщит об успешной установке КриптоПро CSP (см. [рис. 14](#)). Нажмите кнопку **Готово** для выхода из программы установки.

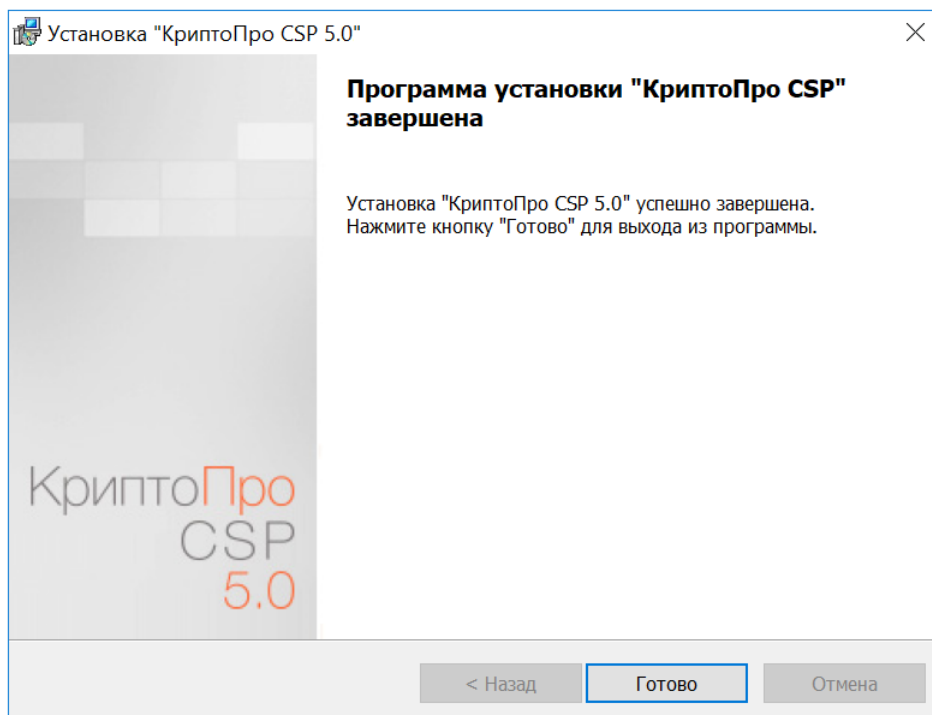


Рисунок 14. Завершение установки КриптоПро CSP

Если программой установки будет предложена перезагрузка компьютера (см. [рис. 15](#)), нажмите кнопку **Да** для завершения установки и применения изменений криптопровайдера.

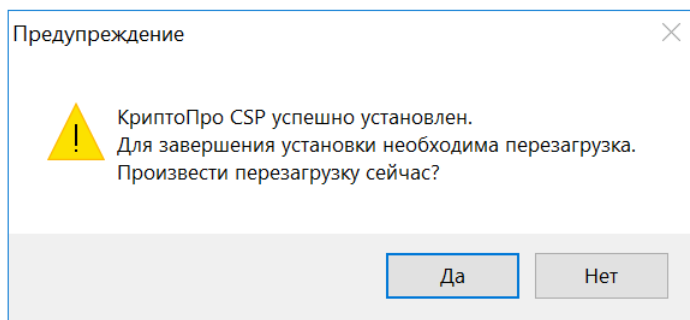


Рисунок 15. Перезагрузка компьютера после установки

2.2 Установка КриптоПро CSP из командной строки

Дистрибутив КриптоПро CSP доступен в виде самораспаковывающегося архива CSPSetup-5.0.exe, содержащего пакеты установщика СКЗИ для всех поддерживаемых архитектур и исполнений, 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 msixec.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-5.0.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 sdk\chm\msi-readme.txt, входящем в состав дистрибутива СКЗИ.

2.3 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 исполняемый файл `crpmaster.exe`. 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. 16](#)).

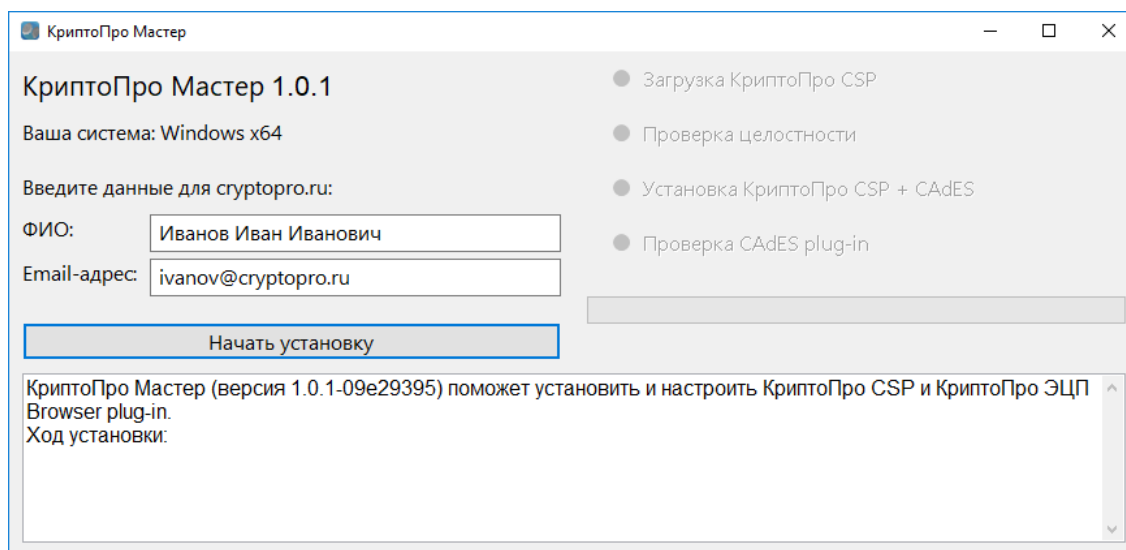


Рисунок 16. Мастер установки и настройки СКЗИ

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 `crverify`, установленной ранее в составе СКЗИ КриптоПро CSP.



Если запуск КриптоПро Мастер выполняется на рабочем месте, где ранее не использовалось СКЗИ КриптоПро CSP (отсутствует утилита `crverify`), или обнаружена устаревшая версия `crverify`, необходимо **самостоятельно осуществить проверку целостности** загруженного дистрибутива с использованием утилиты `crverify`, полученной доверенным образом (подробнее см. раздел 2 ЖТЯИ.00101-03 95 01. Правила пользования). Расположение загруженного дистрибутива, а также команда `crverify`, 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. 17](#)).

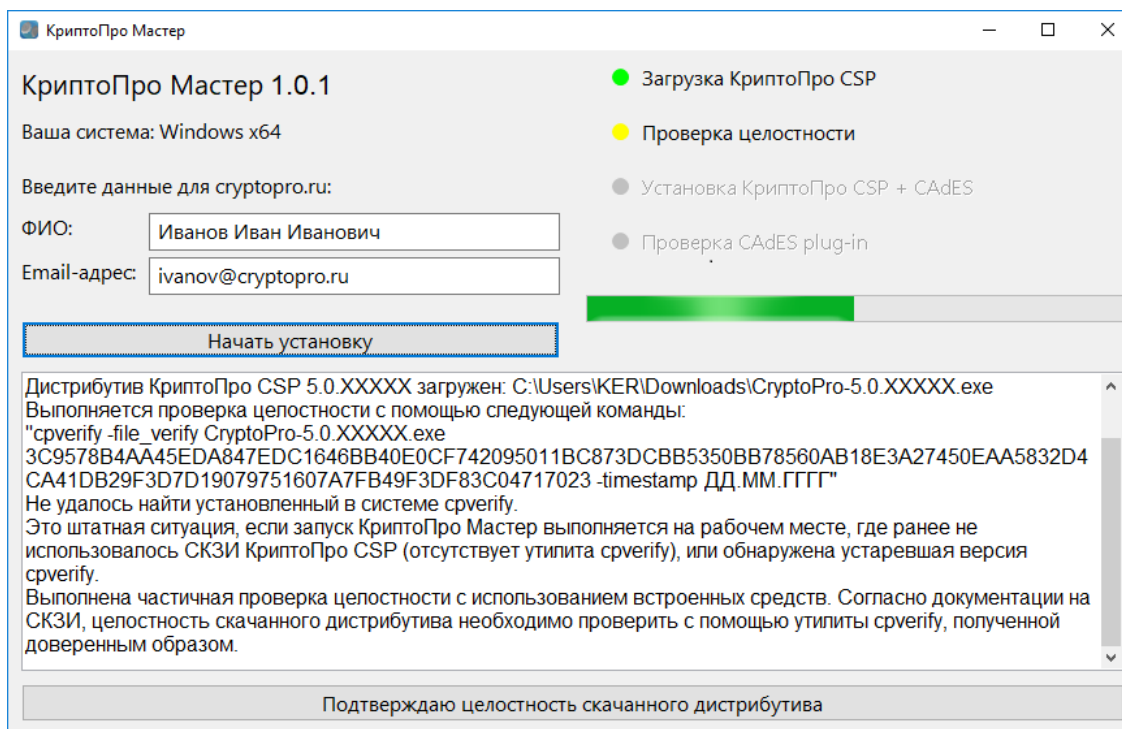


Рисунок 17. Проверка целостности загруженного дистрибутива

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. 18](#)).

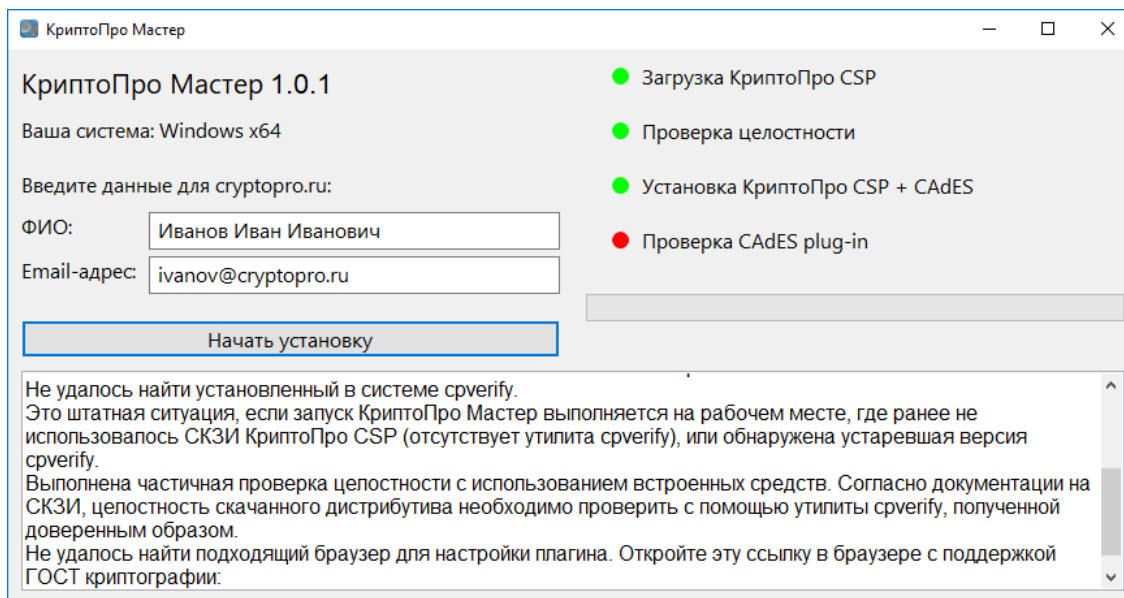


Рисунок 18. Проверка работы плагина

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 цветовой индикации в окне приложения КриптоПро Мастер и на странице проверки работы плагина зеленые, установка, настройка и проверка работы плагина были выполнены успешно.

2.4 Установка ПО Клиент КриптоПро HSM

При использовании СКЗИ КриптоПро CSP в качестве клиентского компонента ПАКМ «КриптоПро HSM» необходимо дополнительно установить ПО Клиент КриптоПро HSM (КриптоПро HSM Client), предоставляющее графический интерфейс настройки клиента ПАКМ.

Установка программного обеспечения Клиент КриптоПро HSM (КриптоПро HSM Client) осуществляется пользователем, имеющим права администратора на локальном компьютере.

Дистрибутивы ПО Клиент КриптоПро HSM доступны в виде самораспаковывающегося архива HSMSetup-2.0.exe, содержащего пакеты установщика ПО для всех поддерживаемых архитектур, и в виде отдельных .msi пакетов.

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



Примечание. Общие сведения о параметрах командной строки msixexec.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 HSMSetup-2.0.exe. Например, установка без диалога Extracting — -gm2.

Для установки ПО Клиент КриптоПро HSM введите следующую команду в командной строке и укажите необходимые параметры:

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

Для установки приложения необходимо выбрать программу установки в зависимости от используемого языка операционной системы и типа процессора:

- hsm-win32-eng.msi
- hsm-win32-rus.msi
- hsm-x64-eng.msi
- hsm-x64rus.msi

Необходимо запустить нужную программу и следовать инструкциям, которые предлагает Мастер установки (см. [рис. 19](#)).

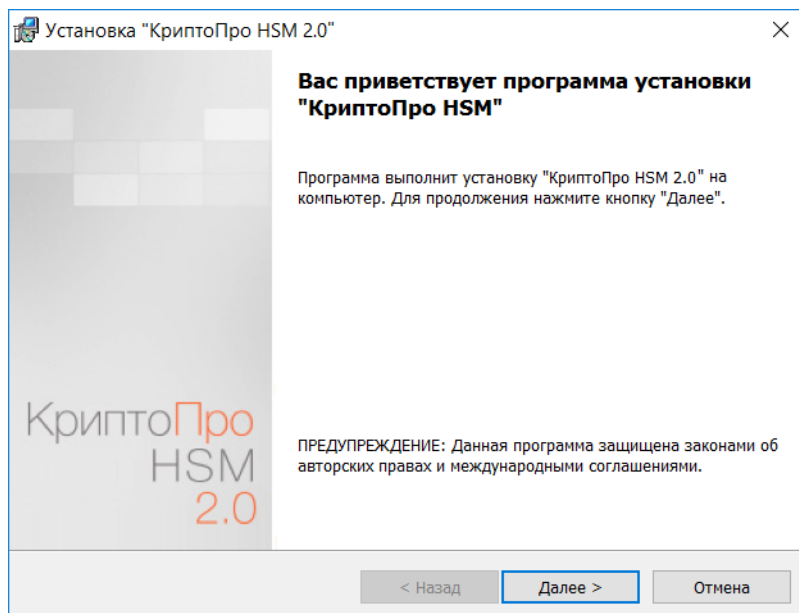


Рисунок 19. Мастер установки ПО Клиент КриптоПро HSM

Нажмите кнопку **Далее**. В следующем окне прочитайте лицензионное соглашение и, в случае согласия с ним, отметьте поле **Я принимаю лицензионное соглашение** и нажмите **Далее** (см. [рис. 20](#)).

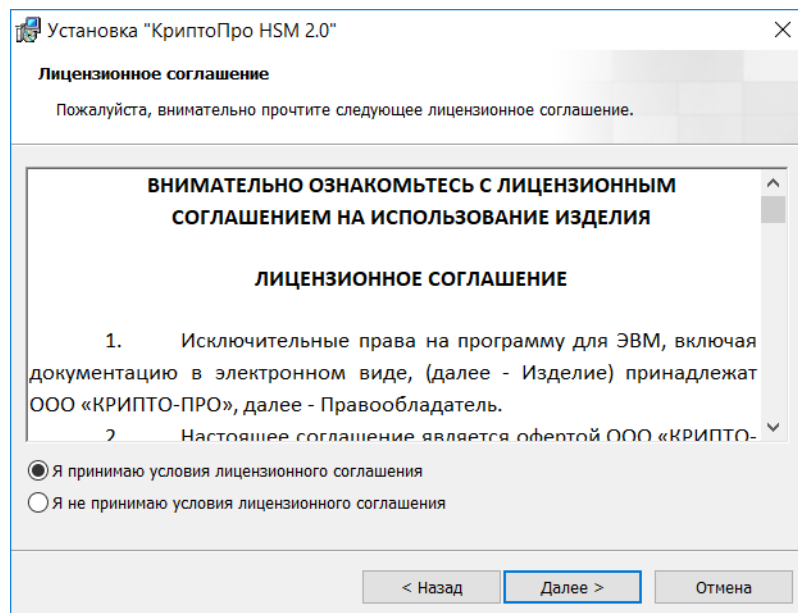


Рисунок 20. Лицензионное соглашение ПО Клиент КриптоПро HSM

В следующем окне введите имя пользователя и название организации и нажмите **Далее** (см. [рис. 21](#)).

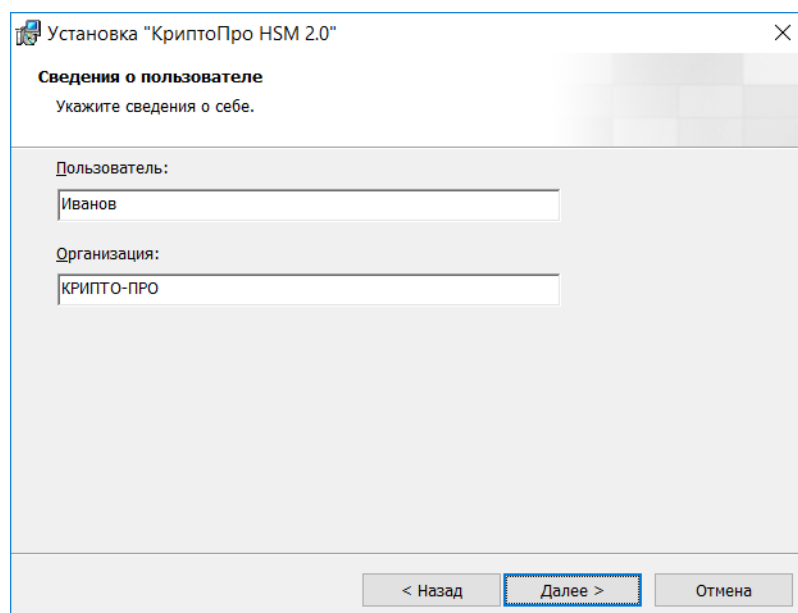


Рисунок 21. Сведения о пользователе

В следующем окне выберите вид установки и нажмите кнопку **Далее** (см. [рис. 22](#)).

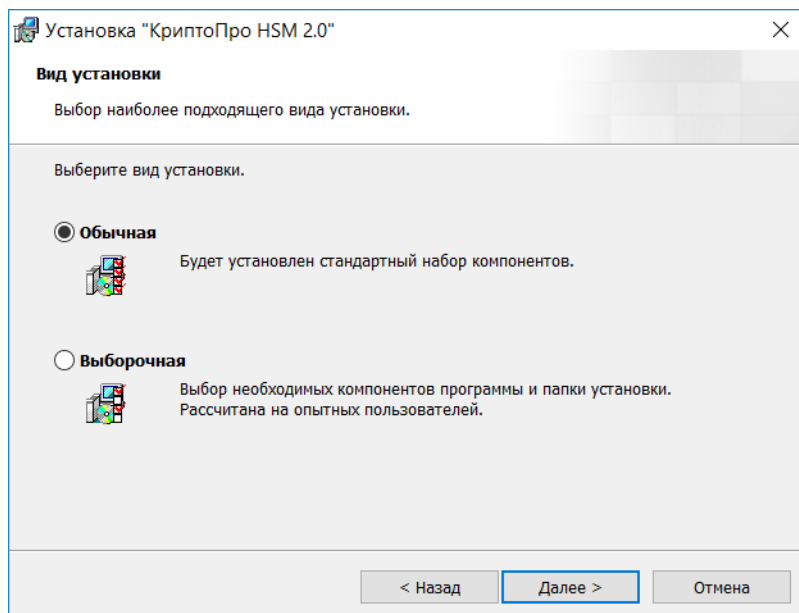


Рисунок 22. Выбор вида установки ПО Клиент КриптоПро HSM

На последнем этапе установки доступны настройка использования телеметрии Windows и включение усиленного контроля использования ключей (см. [рис. 23](#)).



Примечание. Отключение функций телеметрии является обязательным условием эксплуатации СКЗИ под управлением ОС Windows 10/11/Server 2016/Server 2019/Server 2022 (подробнее об отключении телеметрии см. [разд. 4.4](#)).



Примечание. Использование ПО Клиент КриптоПро HSM без включения режима усиленного контроля использования ключей разрешается только в тестовых целях.

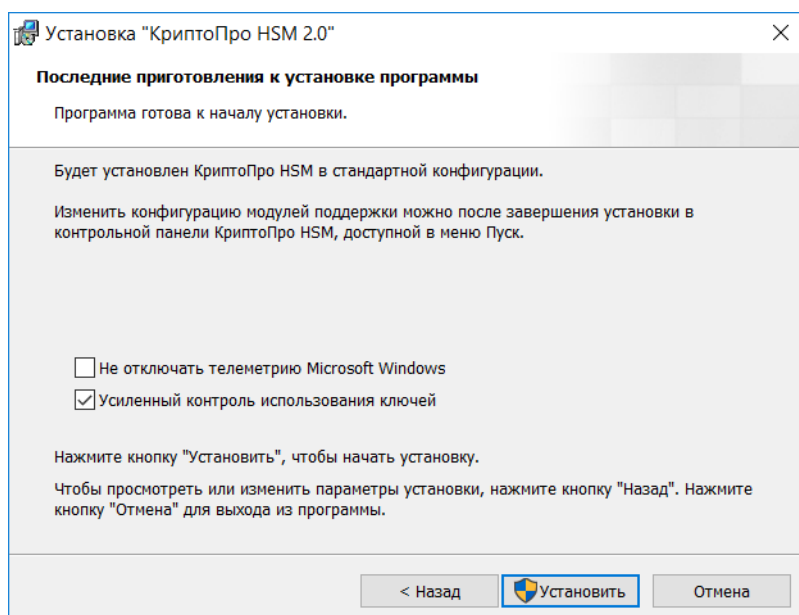


Рисунок 23. Настройка использования телеметрии Microsoft Windows и усиленного контроля использования ключей

При выборе усиленного контроля использования ключей появится окно предупреждения с перечнем необходимых действий для корректной настройки криптопровайдера (см. [рис. 24](#)).

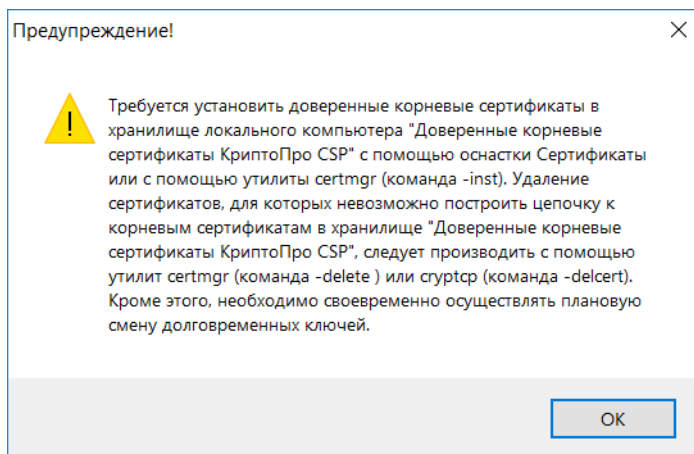


Рисунок 24. Перечень необходимых действий для корректной настройки криптопровайдера при использовании усиленного контроля использования ключей

Для начала установки нажмите кнопку **Установить** и дождитесь окончания установки (см. [рис. 25](#)).

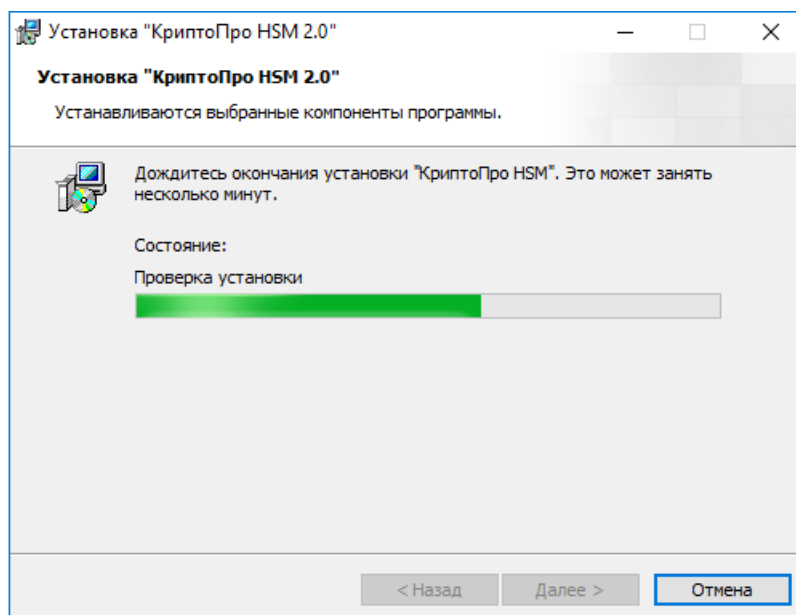


Рисунок 25. Установка ПО Клиент КриптоПро HSM

Нажмите кнопку **Готово** для выхода из программы установки (см. [рис. 26](#)).

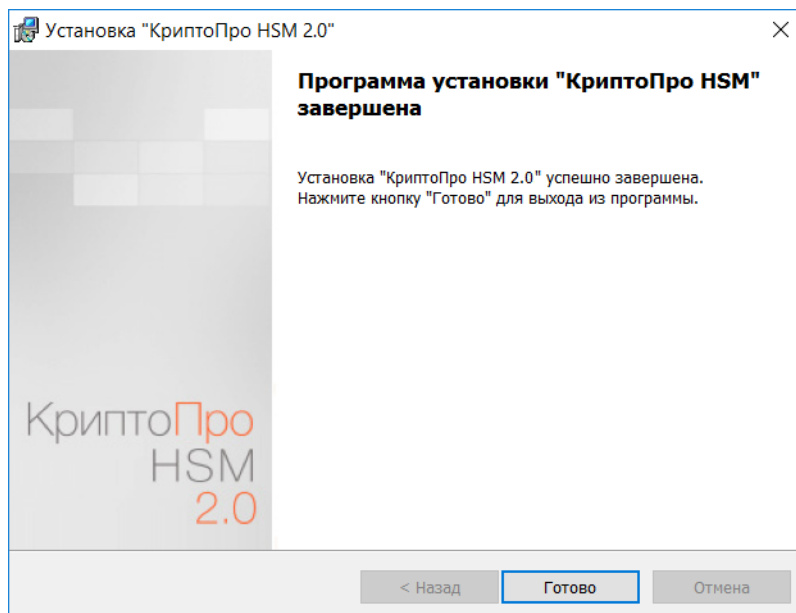


Рисунок 26. Завершение установки ПО Клиент КриптоПро HSM

После успешного завершения работы Мастера установки необходимо перезагрузить операционную систему. После перезагрузки на панели задач появится новый значок

2.5 Обновление КриптоПро CSP

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. 3.1](#));
- 3) установить аналогичный новый дистрибутив КриптоПро CSP ([разд. 2](#));
- 4) при необходимости внести изменения в настройки.



Примечание. Ключи и сертификаты сохраняются автоматически.

3 Удаление СКЗИ

Удалить СКЗИ КриптоПро CSP и ПО Клиент КриптоПро HSM (КриптоПро HSM Client) может только пользователь, имеющий права администратора на локальном компьютере.

3.1 Удаление КриптоПро CSP

Рекомендуется удалять установленное ПО СКЗИ с помощью Панели управления Windows (Панель управления → Программы и компоненты → Удаление программы). В списке установленных программ необходимо выделить «КриптоПро CSP» и нажать кнопку **Удалить** (см. [рис. 27](#)). После удаления ПО СКЗИ необходимо перезагрузить компьютер.

Для удаления КриптоПро CSP через командную строку введите следующую команду:

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

3.2 Удаление ПО Клиент КриптоПро HSM

Рекомендуется удалять установленное ПО Клиент КриптоПро HSM с помощью Панели управления Windows (Панель управления → Программы и компоненты → Удаление программы). В списке установленных программ необходимо выделить «КриптоПро HSM» и нажать кнопку **Удалить** (см. [рис. 27](#)).

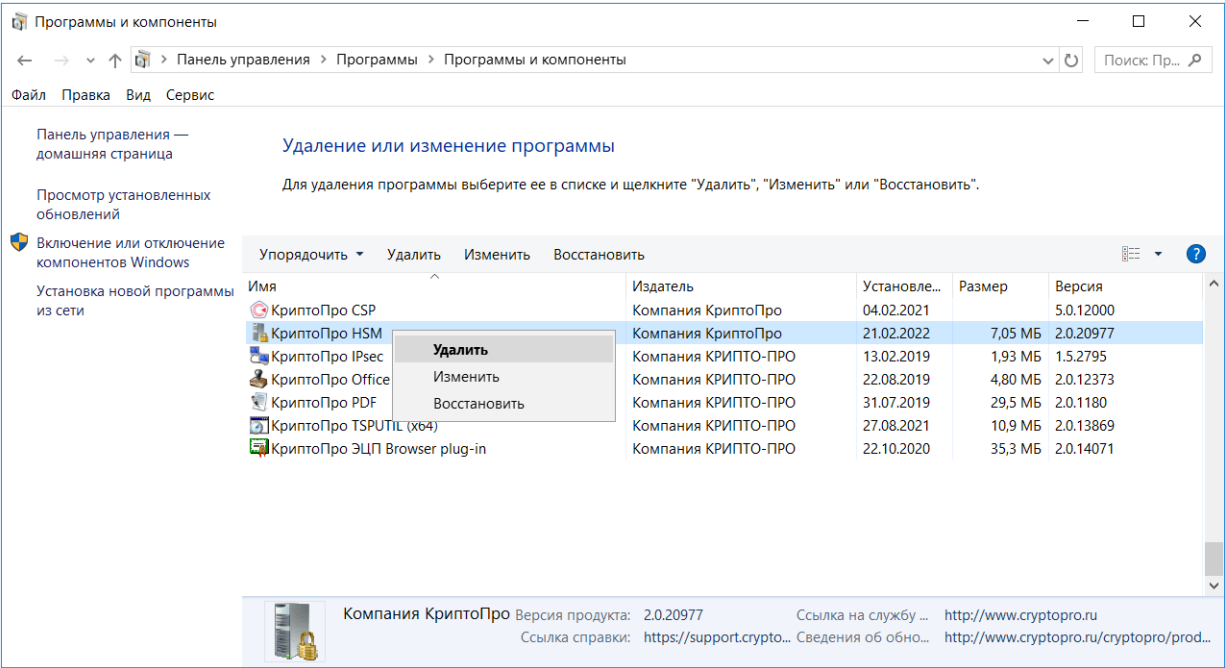


Рисунок 27. Удаление ПО

4 Настройка и использование 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. 28](#)).



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

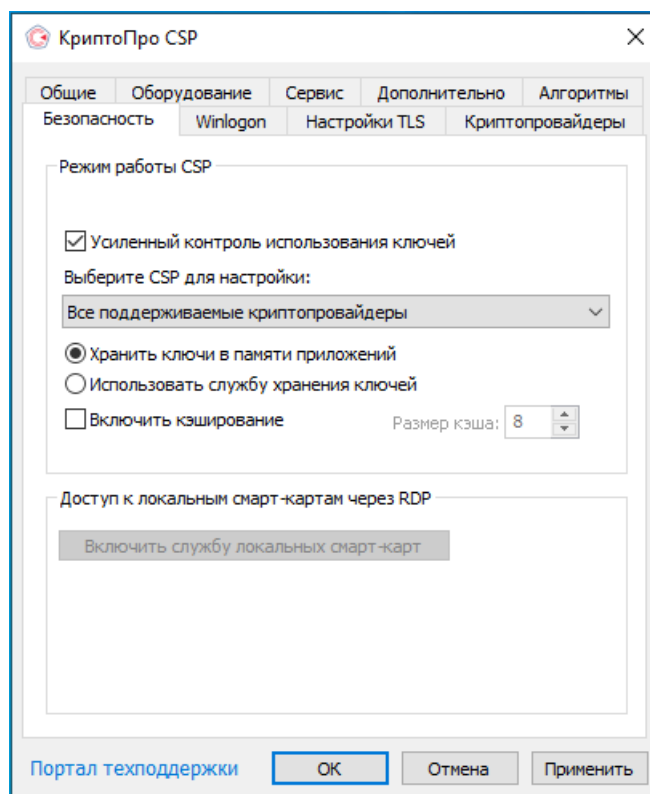


Рисунок 28. Включение режима усиленного контроля использования ключей в контрольной панели КриптоПро CSP

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 создается при установке СКЗИ. После успешного завершения установки 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 Доступ к локальным смарт-картам через RDP

Служба локальных смарт-карт позволяет получить доступ по RDP к смарт-картам, подключенным на удаленном компьютере. Данный режим может быть включен при установке СКЗИ, либо через контрольную панель КриптоПро CSP, вкладка «Безопасность» (см. [рис. 29](#)). Включение/отключение режима через контрольную панель потребует прав администратора. После установки необходимо произвести перезагрузку компьютера.



Примечание. При таком использовании ключевого носителя необходимо учитывать требования, приведенные в п. 3.8 документа ЖТЯИ.00101-03 95 01. Правила пользования, в части запрета оставления без контроля вычислительных средств с установленным СКЗИ после ввода ключевой информации и несения персональной ответственности пользователем за хранение личных ключевых носителей.



Примечание. Доступ к локальным смарт-картам через RDP возможен только в случае выключения режима усиленного контроля использования ключей (в соответствии с разделом 1 ЖТЯИ.00101-03 95 01. Правила пользования отключение режима усиленного контроля использования ключей может производиться только в целях тестирования).

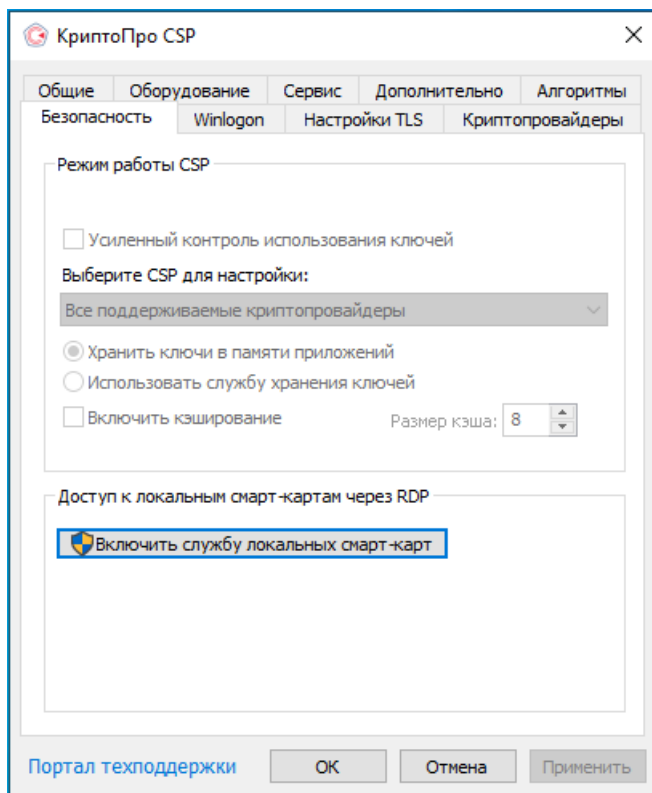


Рисунок 29. Включение службы локальных смарт-карт

4.3 Очистка кэша контейнеров закрытых ключей и кэша паролей при блокировке рабочей станции

По умолчанию при блокировке рабочей станции кэш контейнеров закрытых ключей и кэш паролей не очищается. Для использования функции очистки кэша контейнеров и паролей при блокировке ПК необходимо включить службу хранения ключей, режимы кэширования и работы без подключенного токена (в соответствии с разделом 2.6 ЖТЯИ.00101-03 92 01. Инструкция по использованию. Windows) и службу очистки кэша, добавив параметры реестра **ServiceClearContainerCache** для контейнеров и **ServiceClearPasswordCache** для паролей со значением «1» в ветку HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Crypto Pro\Cryptography\CurrentVersion\Parameters.

Очистка кэша будет производиться в случаях:

- блокировки и разблокировки ПК (только очистка кэша контейнеров);
- перехода ПК в спящий режим;
- переключения между пользователями;
- выхода из системы и последующего входа в неё пользователя;
- перезагрузки ПК.

Кэш контейнеров закрытых ключей сохранится при перезапуске Инструментов КриптоПро (cptools) или восстановлении настроек по умолчанию (см. вкладку **Настройки**).

Кэш паролей сохранится при перезапуске Инструментов КриптоПро (cptools), использовании функции **Удалить сохранённые пароли** (см. вкладку **Настройки**) или разблокировании Windows.



Примечание. Сброс кэша паролей в случае, если контейнер закеширован, нецелесообразен, так как кэшированный контейнер не имеет защиты в виде пароля.

4.4 Отключение функций телеметрии на ОС Windows 10/11/Server 2016/Server 2019/Server 2022



Примечание. Отключение функций телеметрии является обязательным условием эксплуатации СКЗИ под управлением ОС Windows 10/11/Server 2016/Server 2019/Server 2022.

Для отключения функций телеметрии на ОС Windows необходимо выполнить следующие действия:

1) Проверить наличие и статус сервиса DiagTrack («Функциональные возможности для подключенных пользователей и телеметрия») (Панель управления → Система и безопасность → Администрирование → Службы).

2) Если сервис запущен, то остановить его.

3) Удалить запись регистрации сервиса DiagTrack («Функциональные возможности для подключенных пользователей и телеметрия») 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.

Это действие можно выполнить командой `xperf -stop AutoLogger-DiagTrack-Listener`.

6) Удалить файл (если он существует), 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 %systemroot%\System32\LogFiles\WMI\AutoLogger-Diagtrack-Listener.etl.

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



Примечание. В Windows 11 данные сохраняются в файл Diagtrack-Listener.etl

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

4.5 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 (см. [рис. 30](#)) или с помощью модуля контроля целостности `cpverify`, выполнив команду:

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

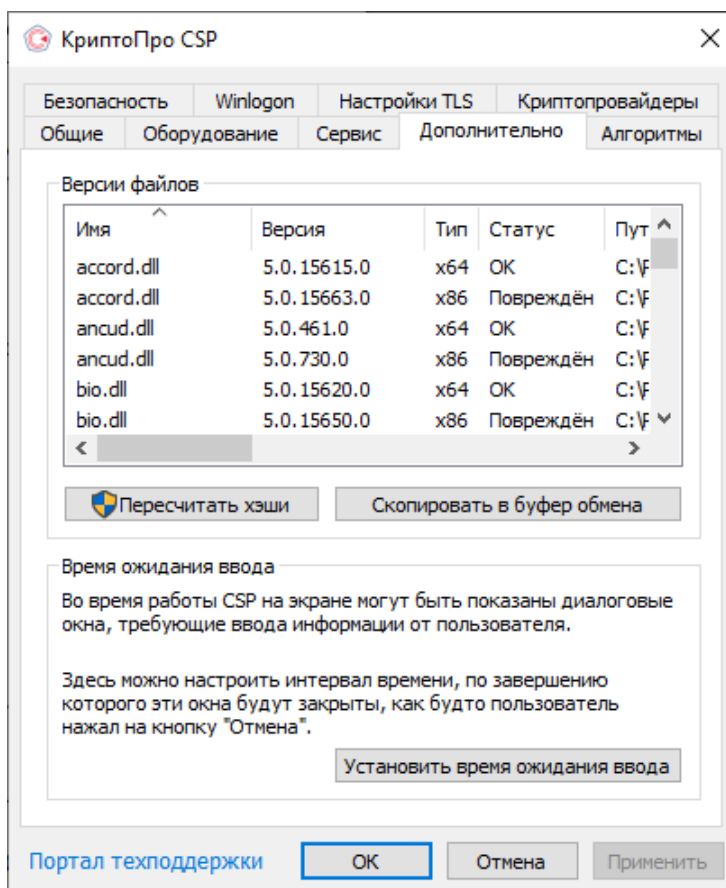


Рисунок 30. Вкладка «Дополнительно» панели управления КриптоПро CSP

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

- crypt32.dll
- cryptsp.dll
- inetcomm.dll
- kerberos.dll
- schannel.dll
- wininet.dll



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

4.6 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 групповой политики введите `gpedit.msc` в поиске Windows. 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. 31](#)).

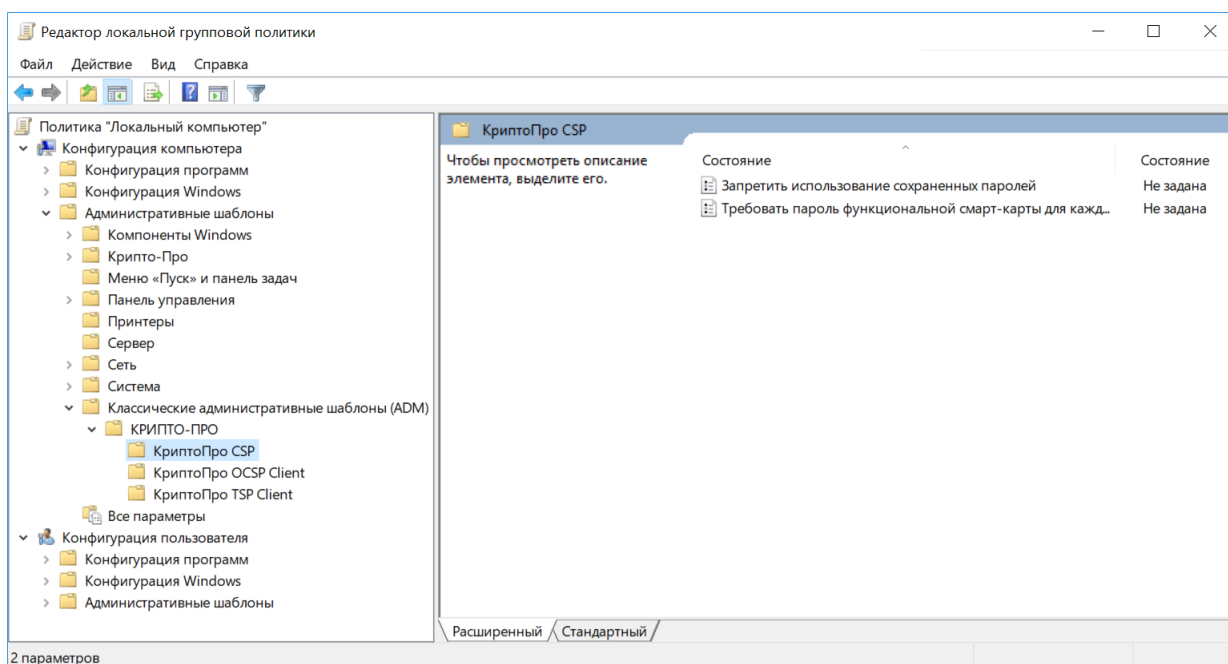


Рисунок 31. Параметры групповой политики для СКЗИ КриптоПро CSP

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

4.6.1 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. 32](#)).

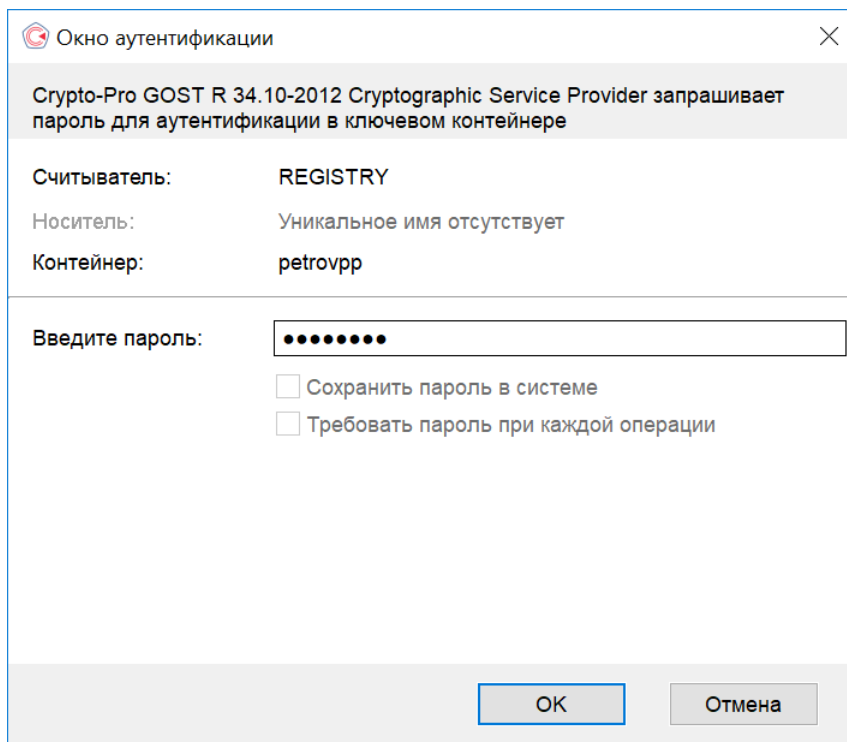


Рисунок 32. Окно аутентификации в контейнере в случае запрета использования сохраненных паролей

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

4.6.2 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. 33](#));
- 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. 33](#)).

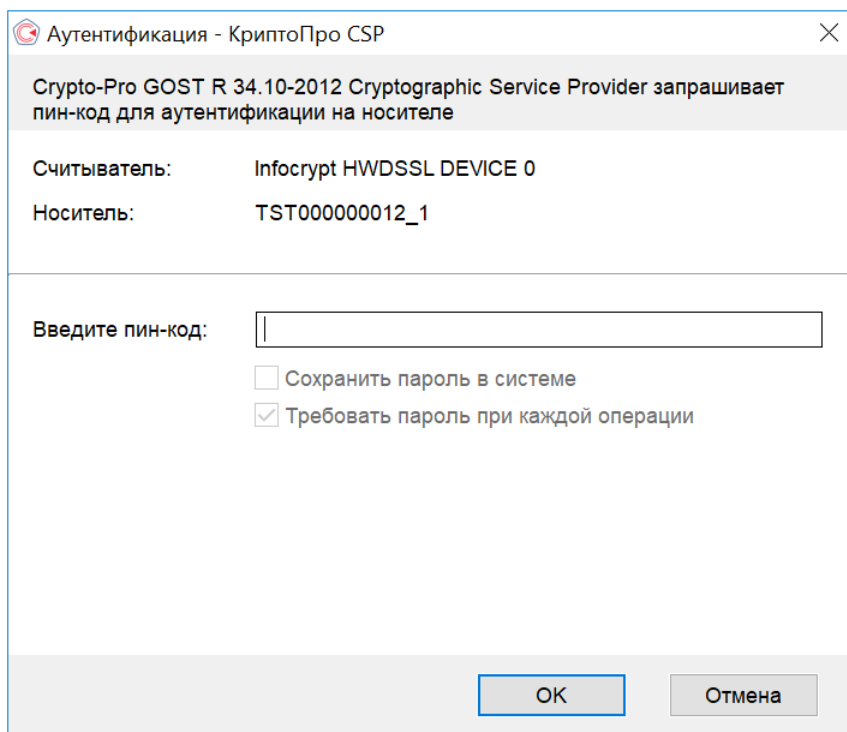


Рисунок 33. Окно аутентификации на носителе в случае запрета сохранения пароля носителя

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.

4.7 Настройка использования Microsoft Edge в режиме интеграции с Internet Explorer

СКЗИ КриптоПро CSP можно эксплуатировать с Microsoft Edge без проведения исследований по оценке влияния только при использовании веб-браузера Microsoft Edge в режиме интеграции с Internet Explorer (Internet Explorer mode).

Для настройки функционирования Microsoft Edge в режиме интеграции с Internet Explorer необходимо выполнить следующие действия:

- 1) Включить режим Internet Explorer (например, с помощью групповой политики, параметров реестра, edge://flags или параметров командной строки);
- 2) Настроить перенаправление сайтов с Microsoft Edge в режим Internet Explorer.

Пример включения интеграции с Internet Explorer с помощью групповой политики:

- 1) скачать и установить (подробнее см. [инструкцию](#)) актуальный [шаблон политик Microsoft Edge](#) (кнопка GET POLICY FILES);
- 2) открыть редактор групповых политик (для запуска редактора групповой политики введите gpedit.msc в поиске Windows или откройте его в качестве оснастки консоли управления MMC (подробнее см. [открытие локальной групповой политики](#));
- 3) в папке Конфигурация компьютера (Конфигурация пользователя) ⇒ Административные шаблоны ⇒ Классические административные шаблоны (ADM) ⇒ Microsoft Edge (см. [рис. 34](#)) открыть параметр **Настройка интеграции с Internet Explorer**;

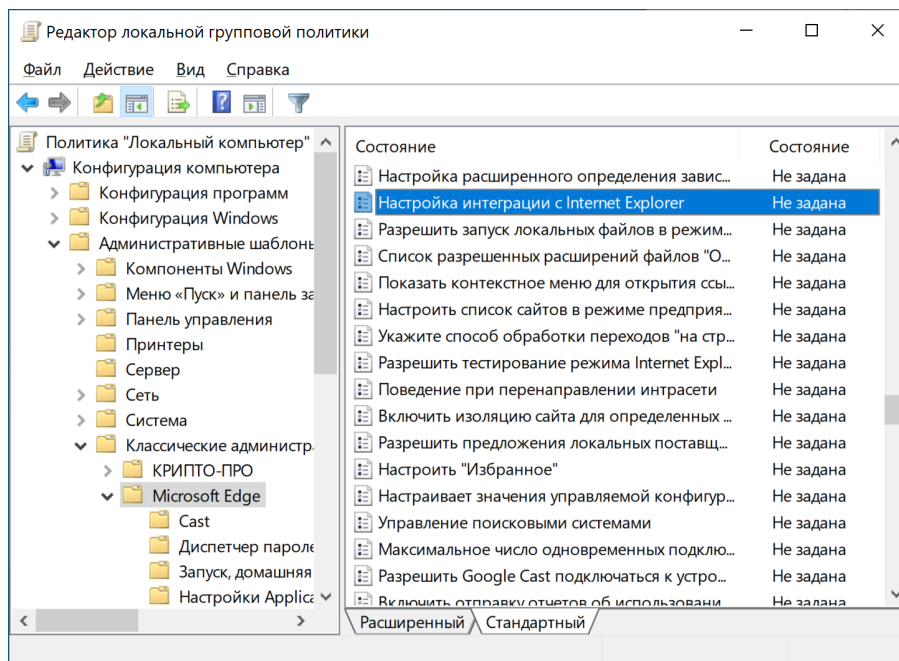


Рисунок 34. Параметры групповой политики Microsoft Edge

4) установить значение **Включено** и в разделе Параметры выбрать из раскрывающегося списка значение **Режим Internet Explorer** (см. рис. 35).

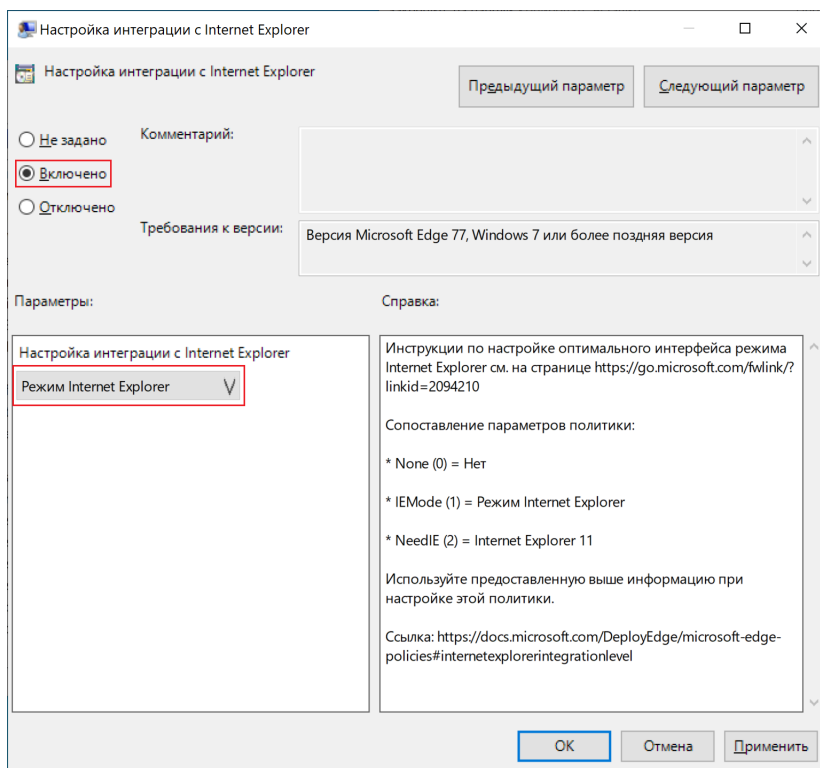


Рисунок 35. Настройка интеграции с Internet Explorer

5) нажать **ОК** или **Применить**, чтобы сохранить этот параметр политики.



Примечание. Аналогичные настройки политик возможно выполнить с помощью установки значения параметра **InternetExplorerIntegrationLevel** ветки реестра **HKEY_LOCAL_MACHINE (HKEY_CURRENT_USER) \Software\Policies\Microsoft\Edge (REG_DWORD)** в значение 1.

После этого необходимо настроить список сайтов, которые должны открываться в режиме Internet Explorer, например, с помощью одной из следующих групповых политик:

- **Использовать список веб-сайтов IE в режиме предприятия** (папка Конфигурация компьютера (Конфигурация пользователя) ⇒ Административные шаблоны ⇒ Компоненты Windows ⇒ Internet Explorer);
- **Настроить список сайтов в режиме предприятия** (папка Конфигурация компьютера (Конфигурация пользователя) ⇒ Административные шаблоны ⇒ Microsoft Edge);
- **Отправить все сайты интрасети в Internet Explorer** (папка Конфигурация компьютера (Конфигурация пользователя) ⇒ Административные шаблоны ⇒ Microsoft Edge).

Подробная инструкция по настройке политик для режима Internet Explorer приведена на [сайте Microsoft](#).



Примечание.

Аналогичные настройки политик возможно выполнить с помощью установки значения параметра **SiteList** веток реестра **HKEY_LOCAL_MACHINE (HKEY_CURRENT_USER) \Software\Policies\Microsoft\Internet Explorer\Main\EnterpriseMode** и **HKEY_LOCAL_MACHINE (HKEY_CURRENT_USER) \Software\Policies\Microsoft\MicrosoftEdge\Main\EnterpriseMode** (перенаправление только сайтов из списка), параметра **SendIntranetTrafficToInternetExplorer** ветки реестра **HKEY_LOCAL_MACHINE (HKEY_CURRENT_USER) \Software\Policies\Microsoft\MicrosoftEdge\Main** (перенаправление всех сайтов интрасети)

4.8 Настройка клиентского компонента КриптоПро HSM

4.8.1 Устанавливаемые криптопровайдеры

В процессе установки дистрибутива в Реестре ОС Windows регистрируются следующие криптопровайдеры:

- Crypto-Pro HSM CSP (тип 75);
- Crypto-Pro HSM Svc CSP (тип 75);
- Crypto-Pro HSM RSA CSP (тип 1);
- Crypto-Pro HSM RSA Svc CSP (тип 1);
- Crypto-Pro GOST R 34.10-2001 HSM CSP (тип 75);
- Crypto-Pro GOST R 34.10-2012 HSM CSP (тип 80);
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP (тип 81);
- Crypto-Pro GOST R 34.10-2001 HSM Svc CSP (тип 75);
- Crypto-Pro GOST R 34.10-2012 HSM Svc CSP (тип 80);
- Crypto-Pro GOST R 34.10-2012 Strong HSM Svc CSP (тип 81).

В самом ПАКМ «КриптоПро HSM» зарегистрирован расширенный набор имен криптопровайдеров, которые при необходимости могут быть использованы для доступа к криптографическим функциям ПАКМ. В этом случае в ОС Windows они должны быть зарегистрированы вручную. Полный список возможных имен криптопровайдеров приведен ниже:

- Crypto-Pro GOST R 34.10-2012 HSM CSP[01-04] (тип 80);
- Crypto-Pro GOST R 34.10-2012 HSM Svc CSP (тип 80);
- Crypto-Pro GOST R 34.10-2012 HSM 1.0 CSP[01-04] (тип 80);
- Crypto-Pro GOST R 34.10-2012 HSM 1.0 Svc CSP (тип 80);

- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP[01-04] (тип 81);
- Crypto-Pro GOST R 34.10-2012 Strong HSM Svc CSP (тип 81);
- Crypto-Pro GOST R 34.10-2012 Strong HSM 1.0 CSP[01-04] (тип 81);
- Crypto-Pro GOST R 34.10-2012 Strong HSM 1.0 Svc CSP (тип 81) ;
- Crypto-Pro ECDSA and AES HSM CSP[01-04] (тип 16);
- Crypto-Pro ECDSA and AES HSM Svc CSP (тип 16);
- Crypto-Pro ECDSA and AES HSM 1.0 Svc CSP (тип 16);
- Crypto-Pro ECDSA and AES HSM 1.0 CSP[01-04] (тип 16);
- Crypto-Pro Enhanced RSA and AES HSM CSP[01-04] (тип 24);
- Crypto-Pro Enhanced RSA and AES HSM Svc CSP (тип 24);
- Crypto-Pro Enhanced RSA and AES HSM 1.0 CSP[01-04] (тип 24);
- Crypto-Pro Enhanced RSA and AES HSM 1.0 Svc CSP (тип 24);
- Crypto-Pro Curve25519 and AES HSM CSP (тип 32);
- Crypto-Pro Curve25519 and AES HSM Svc CSP (тип 32);
- Crypto-Pro Curve25519 and AES HSM 1.0 CSP[01-04] (тип 32);
- Crypto-Pro Curve25519 and AES HSM 1.0 Svc CSP (тип 32);
- Crypto-Pro HSM RSA CSP[01-08] (тип 1);
- Crypto-Pro HSM RSA Svc CSP (тип 1);
- Crypto-Pro RSA HSM CSP (тип 1);
- Crypto-Pro RSA HSM Svc CSP (тип 1);
- Crypto-Pro RSA HSM 1.0 CSP[01-04] (тип 1);
- Crypto-Pro RSA HSM 1.0 Svc CSP (тип 1);
- Crypto-Pro HSM CSP[01-08] (тип 75);
- Crypto-Pro HSM Svc CSP (тип 75);
- Crypto-Pro GOST R 34.10-2001 HSM CSP (тип 75);
- Crypto-Pro GOST R 34.10-2001 HSM Svc CSP (тип 75);
- Crypto-Pro GOST R 34.10-2001 HSM 1.0 CSP (тип 75);
- Crypto-Pro GOST R 34.10-2001 HSM 1.0 Svc CSP (тип 75);
- Crypto-Pro HSM 1.0 CSP[01-04] (тип 75);
- Crypto-Pro HSM 1.0 Svc CSP[01-04] (тип 75).



Примечание. Криптопровайдеры, поддерживающие алгоритмы RSA/ECDSA/AES, не допускается использовать для защиты информации, отличной от тестовых данных.

Для генерации и хранения ключей используется внутренний считыватель ПАКМ с именем «HSMDB». Его отличительной особенностью является то, что все закрытые ключи/ключи ЭП шифруются на ключах шифрования ПАКМ (подробнее см. раздел 6 ЖТЯИ.00096-03 91 01. Руководство администратора безопасности из состава эксплуатационной документации на ПАКМ «КриптоПро HSM»).

В приведенном выше списке криптопровайдеров встречаются имена с суффиксами вида «...[01-04]» или «...[01-08]». Это означает, что кроме основного имени, например, Crypto-Pro GOST R 34.10-2012 HSM CSP зарезервировано ещё несколько синонимов имени данного криптопровайдера, например, Crypto-Pro GOST R 34.10-2012 HSM CSP 01, Crypto-Pro GOST R 34.10-2012 HSM CSP 02 и т.д. Они служат для создания высокопроизводительных систем повышенной надежности — пулов из ПАКМ. На серверах, использующих СКЗИ «КриптоПро HSM», можно зарегистрировать эти имена таким образом, что при обращении к криптопровайдерам с подобными именами запросы будут направляться на конкретный ПАКМ, связанный с данным именем криптопровайдера. Таким образом, управляя в прикладном ПО именами криптопровайдеров, по сути производится манипуляция IP-адресами, по которым будут направляться CryptoAPI запросы, разных клонов «КриптоПро HSM». При необходимости эти имена криптопровайдеров на устройствах доступа должны

быть зарегистрированы вручную. Данные имена имеют вид:

Для 80 типа:

- Crypto-Pro GOST R 34.10-2012 HSM CSP 01;
- Crypto-Pro GOST R 34.10-2012 HSM CSP 02;
- Crypto-Pro GOST R 34.10-2012 HSM CSP 03;
- Crypto-Pro GOST R 34.10-2012 HSM CSP 04.

Для 81 типа:

- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 01;
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 02;
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 03;
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 04.

Для 16 типа:

- Crypto-Pro ECDSA and AES HSM CSP 01;
- Crypto-Pro ECDSA and AES HSM CSP 02;
- Crypto-Pro ECDSA and AES HSM CSP 03;
- Crypto-Pro ECDSA and AES HSM CSP 04.

Для 24 типа:

- Crypto-Pro Enhanced RSA and AES HSM CSP 01;
- Crypto-Pro Enhanced RSA and AES HSM CSP 02;
- Crypto-Pro Enhanced RSA and AES HSM CSP 03;
- Crypto-Pro Enhanced RSA and AES HSM CSP 04.

Криптопровайдеры с именами, включающими лексему «Svc», отличается от криптопровайдеров без её наличия тем, что их использование позволяет выводить запросы на ввод pin-кодов для ключей пользователей не на «рабочий стол» рабочей станции пользователя, а на LCD панель ПАКМ. Кроме этого они позволяют организовать обмен между сервером и ПАКМ по более производительному нешифрованному каналу, при условии осуществления однозначной двусторонней аутентификации «сервер↔ПАКМ», нахождении сервера и ПАКМ в одной контролируемой зоне и условии, что используется специальный сертификат ключа доступа, включающий расширение (EKU) «1.2.643.2.2.34.22».

Такие криптопровайдеры используются в основном в серверных конфигурациях серверами приложений, работающими в фоновом режиме и не имеющими консоли для вывода сообщений и/или запроса pin-кодов. Они реализованы в виде отдельного сервиса ОС Windows, запускаемого при загрузке ОС.

Криптопровайдеры с именами, включающими лексему «HSM 1.0», отличаются от криптопровайдеров без её наличия тем, что ключевые контейнеры используют считыватель «HSM» вместо «HSMDB».

Считыватель «HSMDB» — это внутренняя память (флеш-диск) ПАКМ, которая защищается ключами шифрования ПАКМ, т.е. все ключи, сформированные на считывателе «HSMDB», автоматически шифруются. А так как ключи шифрования ПАКМ защищены на разделенном по схеме 3 из 5-ти ключе активации ПАКМ, то все ключи, созданные на считывателе «HSMDB», невозможно открыть без активации ПАКМ (активации разделенного «ключа активации ПАКМ»). При этом ключевые контейнеры хранятся во внутренней Базе данных ПАКМ и могут реплицироваться подсистемой горячего резервирования в другой ПАКМ.

Считыватель «HSM» — это также внутренняя память (флеш-диск) ПАКМ, которая защищается ключами шифрования ПАКМ также, как и для считывателя «HSMDB». Но ключевые контейнеры хранятся не в БД, а в виде файлов ОС и не могут реплицироваться подсистемой горячего резервирования в другой ПАКМ. Для резервирования таких ключевых контейнеров может быть применено только клонирование ПАКМ (холодное

резервирование).

Криптопровайдеры 75-го типа Crypto-Pro GOST R 34.10-2001 HSM CSP (синоним имени Crypto-Pro HSM CSP) реализуют:

- выполнение функции проверки электронной подписи (ЭП) согласно ГОСТ Р 34.10-2001, возможность вычисления хэш-функции согласно ГОСТ Р 34.11-94;
- возможность шифрования и имитозащиты согласно ГОСТ 28147-89.

Для хранения ключей используется внутренний считыватель ПАКМ с именем «HSMDB».

Алгоритмы подписи данного криптопровайдера выводятся из обращения, используются только для проверки ЭП, и расшифрования ранее созданных криптографических сообщений. Для формирования новых криптографических сообщений используйте более новые алгоритмы и соответствующие криптопровайдеры.

Криптопровайдеры 80 и 81 типа Crypto-Pro GOST R 34.10-2012 HSM CSP и Crypto-Pro GOST R 34.10-2012 Strong HSM CSP (и их синонимы) реализуют:

- выполнение функций создания и проверки электронной подписи (ЭП) согласно ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), вычисление хэш-функции согласно ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018);
- возможность шифрования и имитозащиты согласно ГОСТ 28147 89, ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018).

На настоящий момент криптопровайдеры 80-го типа являются основными и используются для всех служебных ключей ПАКМ «КриптоПро HSM».

Помимо криптопровайдеров, реализующих алгоритмы ГОСТ, в ПАКМ «КриптоПро HSM» устанавливаются криптопровайдеры, реализующие зарубежные алгоритмы.

Криптопровайдеры 1-го типа Crypto-Pro HSM RSA CSP и Crypto-Pro HSM RSA Svc CSP (тип 1) устаревшей реализации (wine) оставлены для совместимости с предыдущими версиями. Не рекомендуется их использовать в новых приложениях. Следует использовать более новую реализацию — криптопровайдер Crypto-Pro RSA HSM CSP (и его синонимы). Они реализуют алгоритмы электронной подписи RSA:

- генерацию ключевых пар с размером открытого ключа до 16K;
- формирование и проверку ЭП (RSA);
- вычисление значения хэш-функции с использованием алгоритмов SHA1, SHA256, SHA384, MD5;
- генерацию симметричных ключей DES, 3DES, 3DES_112;
- шифрование/расшифрование по указанным алгоритмам.

При необходимости использования зарубежных алгоритмов рекомендуется использовать более современные их модификации, которые реализуются криптопровайдерами 16-го, 24 и 32 типов: «...ECDSA and AES...», «...Enhanced RSA and AES...» и «...Curve25519 and AES...».

Все необходимые криптопровайдеры должны быть зарегистрированы на ПЭВМ, использующих криптографические сервисы.

Обычному пользователю не следует использовать криптопровайдеры «...Svc...». ПО «Клиент КриптоПро HSM» не позволяет работать с данными провайдерами, если в сертификате ключа доступа к ПАКМ нет соответствующего расширения.

Администраторам серверов при использовании ПАКМ «КриптоПро HSM» с такими сервисами как Microsoft CA, «КриптоПро УЦ», Microsoft IIS и другими, реализованными в виде служб ОС Windows, необходимо использовать криптопровайдеры «...Svc...». Клиентская часть таких провайдеров (на машине клиента ПАКМ «КриптоПро HSM») реализована в виде службы ОС Windows, которая запускается в момент загрузки ОС и может обслуживать криптографические запросы других служб, даже если никто из

пользователей не открыл Windows-сессию.

Клиентская часть обычных провайдеров (без лексемы «Svc» в имени) реализована в виде пользовательского приложения, которое грузится в момент входа пользователя, и отображается в виде иконки в системном трее. Таким образом, если на ПЭВМ с установленным ПО «Клиент КриптоПро HSM» нет активной Windows-сессии (ни одного «залогиненного» пользователя), то никто не сможет обслужить криптографические запросы, обращенные к обычным криптопровайдерам.

Администраторам серверов следует с осторожностью относиться к установке криптопровайдеров «КриптоПро HSM» в качестве «провайдеров по умолчанию» в ОС Windows. Некоторые системные сервисы ОС Windows перечисляют установленные типы криптопровайдеров и реализуемые ими алгоритмы путем обращения к этим криптопровайдерам. При этом, если «КриптоПро HSM» выключен в данный момент, не активирован, или в считывателе отсутствует ключ доступа к ПАКМ, то может наблюдаться эффект зависания ОС. Рекомендуется для «провайдеров по умолчанию» использовать криптопровайдеры с локальной реализацией криптоалгоритмов. Сервера приложений, которым необходимо использовать криптопровайдеры «КриптоПро HSM», должны всегда явно обращаться по именам криптопровайдеров (HSM), а не по типам, вне зависимости от значений, указанных в ветках реестра «Провайдеры по умолчанию» (Default Provider Types).

Обращения к криптопровайдерам, работающим с ПАКМ через сервис, могут быть сделаны только пользователями с учетными именами SYSTEM (LocalSystem), пользователями, входящими в группу локальных администраторов компьютера или в группу «Привилегированные пользователи КриптоПро HSM». Группу «Привилегированных пользователей КриптоПро HSM» можно создать вручную и добавить туда, например, учетные имена, под которыми исполняются сервисные приложения (например, пул приложений .NET под управлением Microsoft IIS). Эти же правила действуют при обращении пользователей к любым криптопровайдерам ПАКМ через системный трей, при использовании специального флага в вызовах интерфейса CryptoAPI — CRYPT_MACHINE_KEYSET.

Процесс установки дистрибутива ПО «Клиент КриптоПро HSM» не изменяет значение провайдера по умолчанию для 1-го типа. Как правило, в ОС Windows им является криптопровайдер «Microsoft Strong Cryptographic Provider».

4.8.2 Дополнительные настройки параметров клиента ПАКМ

Для более тонкой настройки работы с криптопровайдерами существует ряд параметров, которые нельзя изменить, используя штатные оконные средства панели управления криптопровайдером.

Данные параметры по умолчанию не прописываются в реестре Windows и имеют значения по умолчанию, указанные в табл. 1. Для изменения значения параметра необходимо вручную добавить ключ с именем параметра и его новое значение типа «DWORD» в реестр Windows в ветку HKLM\SOFTWARE\[WOW6432Node\]Crypto Pro\Cryptography\CurrentVersion\HSM\.

Таблица 1. Описание и значения параметров криптопровайдеров

Параметр	Имя параметра в реестре	Значение по умолчанию
Адрес HSM (IP-адрес или DNS-имя)	Channel	—
Месторасположение ключа доступа (имя считывателя или полное имя контейнера в реестре)	Reader	—

Таймаут ожидания ответа от HSM (в секундах) ¹	RPCTimeout	15 секунд — для обычных (не сервисных) криптопровайдеров 60 секунд — для сервисных («...Svc...») криптопровайдеров
Разрешить использование канала «K2s» (отключить шифрование в канале «K2» для увеличения производительности) ²	WithoutEnc	0 (используется канал «K2»)
Запретить удаление контейнеров ключей (через оснастку «КриптоПро HSM» консоли управления КриптоПро PKI)	DisableDeleteContainer	0
Запретить установку сертификатов в контейнер ключей (через оснастку «КриптоПро HSM» консоли управления КриптоПро PKI)	DisableInstallCertificate	0
Запретить просмотр сертификата в контейнере ключей (через оснастку «КриптоПро HSM» консоли управления КриптоПро PKI)	DisableViewCertificate	0
Запретить изменение пароля на контейнер ключей (через оснастку «КриптоПро HSM» консоли управления КриптоПро PKI)	DisableChangePassword	0
Максимальное количество соединений с HSM ³	Pool_max_connection	20
Начальное количество соединений с HSM ³	Init_pool_size	1 Должно быть $\leq$ Pool_max_connection
Количество попыток найти свободное соединение с HSM ³	Connection_pool_max_retry	40
Таймаут ожидания очереди на отправку запросов к HSM (в секундах)	SENDTimeout	15



1. Увеличенный таймаут RPCTimeout для сервисных криптопровайдеров объясняется тем, что pin-коды на контейнеры ключей, хранящихся в ПАКМ для данного криптопровайдера, запрашиваются с LCD панели ПАКМ. Это может быть довольно длительная процедура, особенно если дополнительно запрашивается подтверждение ввода pin-кода. Pin-коды для контейнеров ключей, сформированных для провайдера Crypto-Pro HSM CSP, запрашиваются на рабочем столе пользователя, и данная процедура не входит в интервал ожидания ответа от ПАКМ.

При очень высокой загрузке ПАКМ криптографическими запросами пользователей и серверов приложений время отклика ПАКМ может существенно возрастать, особенно если используется полное журналирование криптографических запросов (событий подписи, шифрования, расшифрования...) в журнале аудита ПАКМ.

2. Значение параметра «WithoutEnc» может быть изменено на значение «1» только при использовании специального сертификата ключа доступа к ПАКМ, включающего расширение «Администратор сервера»; как правило используется криптопровайдером Crypto-Pro HSM Svc CSP.

Для использования канала «K2s» также необходимо произвести соответствующую настройку внутри ПАКМ «КриптоПро HSM» (см. опцию «Enable K2s» в п. «Просмотр и изменение параметров ПАКМ» документа ЖТЯИ.00096-03 90 01. КриптоПро HSM. Инструкция по использованию), позволяющую работу (запускающую слушатель на специальный порт 1503) по нешифрованному каналу. При этом TLS аутентификация проходит обычным образом.

Для отключения шифрования в канале «K2» (использование канала «K2s»), необходимо обеспечить выполнение следующих условий:

- сервер и ПАКМ должны находиться в одной серверной стойке;
- для работы по нешифрованному каналу должен использоваться отдельный сетевой интерфейс ПАКМ.

3. ПО «Клиент КриптоПро HSM» является многопоточным приложением и позволяет создавать пул соединений с ПАКМ «КриптоПро HSM» для обеспечения большей производительности. Эти готовые соединения могут быть использованы приложениями пользователя, серверами приложений для доступа к HSM одновременно и без длительного процесса начальной установки соединений. Соединения устанавливаются каждым экземпляром ПО «Клиент КриптоПро HSM» (hsmtray, сервисом crcpsphclm).

По умолчанию используется пул из 20 возможных соединений с предварительной установкой 1-го соединения. Последующие соединения будут устанавливаться по мере необходимости. Если какое-либо приложение/поток подаст запрос к ПАКМ, но при этом все открытые соединения заняты обработкой запросов от других приложений/потоков, то ПО «Клиент КриптоПро HSM» установит новое соединение, если общее количество не превышает заданного максимального количества соединений («Pool_max_connection»). Если используются все возможные соединения, то ПО «Клиент КриптоПро HSM» будет пытаться несколько раз (в зависимости от значения параметра «Connection_pool_max_retry») получить освобождающееся соединение из пула. Начальное количество устанавливаемых соединений с ПАКМ при запуске службы crcpsphclm или при подключении hsmtray можно изменить, установив соответствующее значение параметра «Init_pool_size».

Указанные выше параметры также могут быть переопределены групповой политикой.

Для редактирования групповой политики используется специальный административный шаблон (см. [рис. 36](#)).

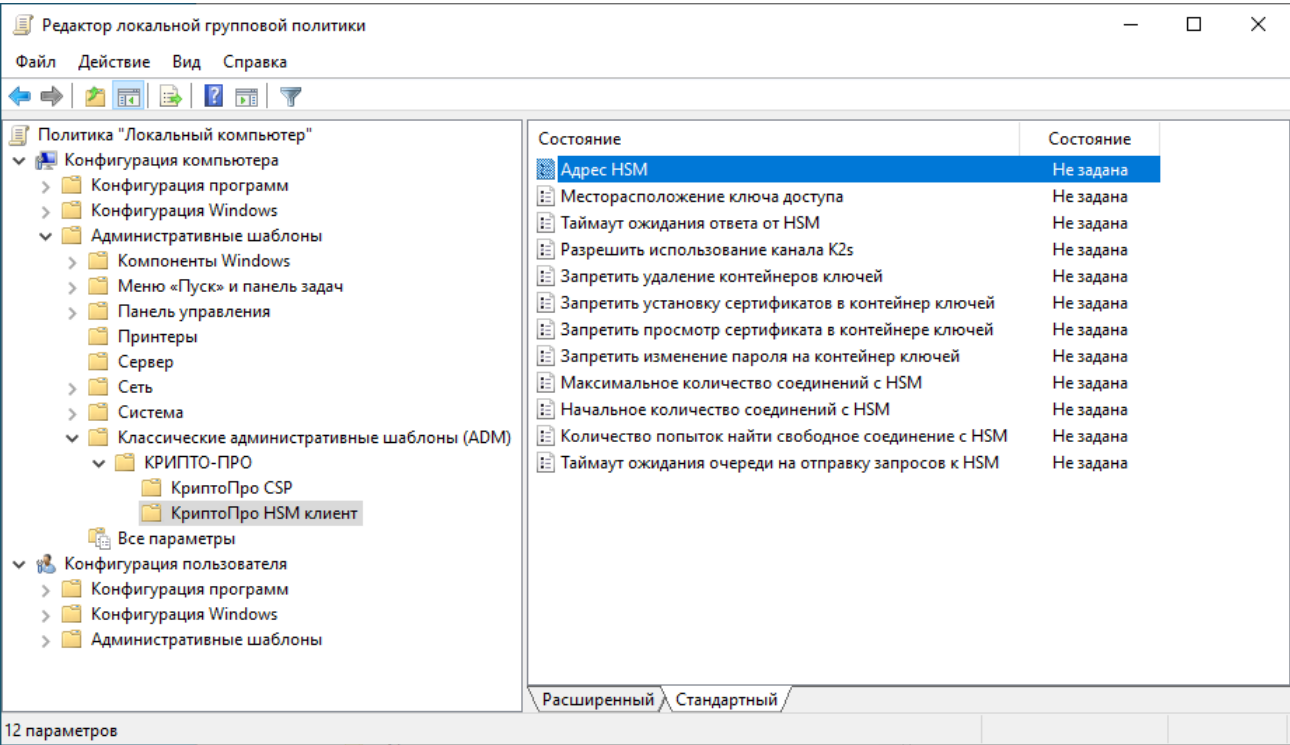


Рисунок 36. Административный шаблон «КриптоПро HSM клиент»

Для доступа к указанной политике используйте команду gpedit /32.

Значения переменных групповой политики хранятся в ветке реестра Windows Software\[WOW6432Node\]Policies\Crypto-Pro\HSM и имеют преимущество (если установлены) перед теми, которые хранятся в ветке SOFTWARE\[WOW6432Node\]Crypto Pro\Cryptography\CurrentVersion\HSM.

4.8.3 Настройка конфигурации с несколькими ПАКМ

ПО «Клиент КриптоПро HSM» поддерживает возможность одновременной работы пользователя с одной рабочей станции сразу с несколькими экземплярами ПАКМ «КриптоПро HSM». Данные ПАКМ могут быть как клонами друг друга, например, в целях повышения производительности систем или отказоустойчивости, так и различными по наборам ключевой информации и вариантам использования.

В конечном итоге, с точки зрения программного интерфейса MS CryptoAPI, выбор приложения для работы с тем или иным ПАКМ сводится к выбору соответствующего имени криптопровайдера.

Существующий графический интерфейс пользователя (GUI) по настройке параметров ПО «Клиент КриптоПро HSM» прописывает значения параметров подключения к ПАКМ в реестре Windows в ветках:

- HKLM\SOFTWARE\[Wow6432Node\]Crypto Pro\Cryptography\CurrentVersion\HSM
- HKLM\SOFTWARE\[Wow6432Node\]Policy\Crypto Pro\Cryptography\CurrentVersion\HSM

(аналогично, но настраиваемое как групповая политика)

Далее будет указываться только один вариант корня данной ветки.

Если в системе присутствует только один ПАКМ, то этой ветки реестра достаточно для нормального функционирования сервисов ПО «Клиент КриптоПро HSM».

Если в конфигурации системы присутствует несколько ПАКМ, то параметры, указанные в ветке реестра HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM, используются как

параметры по умолчанию, наследуемые всеми ПАКМ.

Для указания, что в системе используется несколько ПАКМ (более одного), необходимо прописать их идентификаторы в виде ключей ветки Реестра HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\HSMIDs.

Например:

- HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\HSMIDs\HSM1
- HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\HSMIDs\HSM2
- HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\HSMIDs\HSM3

Для каждого HSM можно указать соответствующие значения параметров точно (включая IP-адрес и имя считывателя/контейнера ключа доступа к ПАКМ).

Использование нескольких описаний с одними и теми же параметрами может увеличить производительность сервера (распараллелить обращения нескольких процессов к одному и тому же ПАКМ).

На каждый ПАКМ может быть запущено несколько сервисов ПО «Клиент КриптоПро HSM», а также системных треев. При подключении к ПАКМ через GUI системного трея пользователю будет выдаваться меню из набора идентификаторов ПАКМ (ключей ветки HKLM\SOFTWARE\CryptoPro\Cryptography\CurrentVersion\HSM\HSMIDs) для выбора, к какому ПАКМ осуществить подключение данного экземпляра трея (см. [рис. 37](#)).

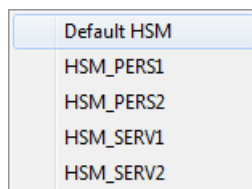


Рисунок 37. Меню идентификаторов ПАКМ «КриптоПро HSM»

Таким образом, если у пользователя нет необходимости в одновременной работе с несколькими ПАКМ, то может быть запущен только один экземпляр системного трея. Пользователь может завершить работу с одним ПАКМ, потом подключиться к другому, выбрав из меню идентификаторов соответствующий ПАКМ.

Главным условием запуска нескольких сервисов и системных треев ПО «Клиент КриптоПро HSM» одновременно является использование разных имен «слушателей» — RPC (Remote Procedure Call) точек подключений (RPC Endpoint).

Для указания имени «RPC точки подключения» используется:

- Флаг «-e» с последующим именем в командной строке запуска трея (например, `hsmtray -e "My endpoint 1 %d"`);
- Параметр «CP Service Name» в ключе реестра Windows, описывающем запускаемый сервис.

При установке ПО «Клиент КриптоПро HSM» прописываются

- один сервис `srcsphclm` для работы с ПАКМ в фоновых режимах (без обязательного наличия Logon сессии пользователя), которому соответствуют ветки реестра:
 - HKLM\SYSTEM\CurrentControlSet\services\cpcspchlm,
 - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost (см. документацию на svchost)
- запуск одного системного трея при входе пользователя в систему, которому соответствуют ветки реестра:
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

При этом параметры, указывающие имена «RPC точек подключения», нигде не прописываются. По умолчанию используются следующие имена (зафиксированы в коде программы):

- "CryptoPro HSM Client Service LM" — для сервиса;
- "CryptoPro HSM Client Service %d" — для троя.

Если в имени точки подключения последние 2 символа %d, то они будут заменены при старте троя/сервиса номером LOGON сессии пользователя (или 0 — для сервиса).

Для запуска ещё одного экземпляра троя необходимо в командной строке его запуска указать уникальное значения опции «-е».

Чтобы запустить ещё один экземпляр сервиса, необходимо добавить его описание в систему (см. документацию на svchost), а также в его описании в реестре добавить строковый параметр «CP Service Name» и указать там уникальное значение имени RPC точки подключения. Для указания, к какому экземпляру ПАКМ данный экземпляр сервиса должен подключаться, необходимо там же добавить строковый параметр «HSMID» и указать значение идентификатора ПАКМ, например, «HSM3» (без кавычек), т.е. одно из тех имен, которые прописывались в ветке HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\HSMIDs.

При запуске системного троя в командной строке также можно указать, с каким именно HSMID данный трей должен работать. Для этого используется параметр «-m» с последующим значением идентификатора ПАКМ, например, «-m HSM3». В этом случае данный трей не будет видеть других идентификаторов ПАКМ, прописанных в реестре, и, фактически, будет «закреплен» за конкретным ПАКМ. Это позволяет запускать несколько системных треев при автозагрузке с заранее определенной администратором конфигурацией.

Библиотеки криптопровайдеров КриптоПро для подключения к криптографическим сервисам используют значение параметра «CP Service Name» как имя «RPC точки подключения». Данный параметр прописывается в ключе, описывающем конкретное имя криптопровайдера (см. HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\<имя_криптопровайдера>).

Таким образом, если необходимо использовать несколько криптографических сервисов, каждый из которых прослушивает RPC с использованием уникальных имен «RPC точек подключений», необходимо зарегистрировать дополнительные имена криптопровайдеров, у которых прописать значения этих точек подключений.

При этом, если приложению необходимо обратиться к определенному ПАКМ, оно должно обратиться к определенному сервису/трею по согласованной «точке подключения», а фактически использовать для этого правильное имя криптопровайдера.

Т.к. в ПАКМ «КриптоПро HSM» набор зарегистрированных имен криптопровайдеров строго определен заранее в момент его изготовления и не может быть расширен в процессе эксплуатации, ПО сервисов/трея «Клиента КриптоПро HSM» в таких случаях пытается сделать замену имени криптопровайдера, транслируя в ПАКМ уже правильное имя.

В имени криптопровайдера, переданном приложением сервису/трею, выполняется поиск подстроки «Проху», и, если такое имя находится, то для определения криптопровайдера в этом имени отсекается часть, начинающаяся с «Проху». Например, в ПАКМ «КриптоПро HSM» и в ОС Windows есть зарегистрированный провайдер с именем Crypto-Pro HSM CSP. Для того, чтобы использовать еще один сервис с дополнительной точкой подключения, можно зарегистрировать дополнительное имя криптопровайдера с именем Crypto-Pro HSM CSPProху HSM1, Crypto-Pro HSM CSPProху HSM2 и т.п. В ПАКМ сервис будет передавать строку Crypto-Pro HSM CSP.

Кроме этого в ПАКМ «КриптоПро HSM» для целей создания кластеров из ПАКМ добавлено по 8 дополнительных имен криптопровайдеров для 1-го и 75-го типов, по 4 дополнительных имени для 80, 81, 16

и 24 типов криптопровайдеров. Данные имена имеют вид:

Для 75 и 1 типа:

- Crypto-Pro HSM CSP NN;
- Crypto-Pro HSM RSA CSP NN, где NN — номера от 1 до 8 с лидирующим нулем (т.е. в виде «01», ..., «08»).

Для 80 типа:

- Crypto-Pro GOST R 34.10-2012 HSM CSP 01;
- Crypto-Pro GOST R 34.10-2012 HSM CSP 02;
- Crypto-Pro GOST R 34.10-2012 HSM CSP 03;
- Crypto-Pro GOST R 34.10-2012 HSM CSP 04.

Для 81 типа:

- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 01;
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 02;
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 03;
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 04.

Для 16 типа:

- Crypto-Pro ECDSA and AES HSM CSP 01;
- Crypto-Pro ECDSA and AES HSM CSP 02;
- Crypto-Pro ECDSA and AES HSM CSP 03;
- Crypto-Pro ECDSA and AES HSM CSP 04.

Для 24 типа:

- Crypto-Pro Enhanced RSA and AES HSM CSP 01;
- Crypto-Pro Enhanced RSA and AES HSM CSP 02;
- Crypto-Pro Enhanced RSA and AES HSM CSP 03;
- Crypto-Pro Enhanced RSA and AES HSM CSP 04.

Таким образом, если количество синхронизируемых ПАКМ не превышает указанного числа криптопровайдеров нужного типа, рекомендуется использовать указанные выше имена, зарегистрированные внутри ПАКМ «КриптоПро HSM». Если количество синхронизируемых ПАКМ более восьми или четырех (в зависимости от типа), в дополнение можно использовать произвольные имена, полученные из зарегистрированных имен с добавлением суффиксов «Proху...».

При использовании имен с суффиксом «Proху...» не рекомендуется использовать в прикладном ПО вызовы `CryptGetProvParam (... , PP_NAME, ...)` с последующим использованием возвращаемого данным методом имени криптопровайдера в том же ПО. Возвращаемое таким образом имя будет отличаться от начального, используемого при открытии контекста, в нем уже будет отсутствовать суффикс «Proху...». Следующий вызов открытия контекста с новым именем может быть перенаправлен в другой ПАКМ.

4.8.3.1 Пример настройки конфигурации

Список (HSMIDs) зарегистрированных ПАКМ приведен на [рис. 38](#).

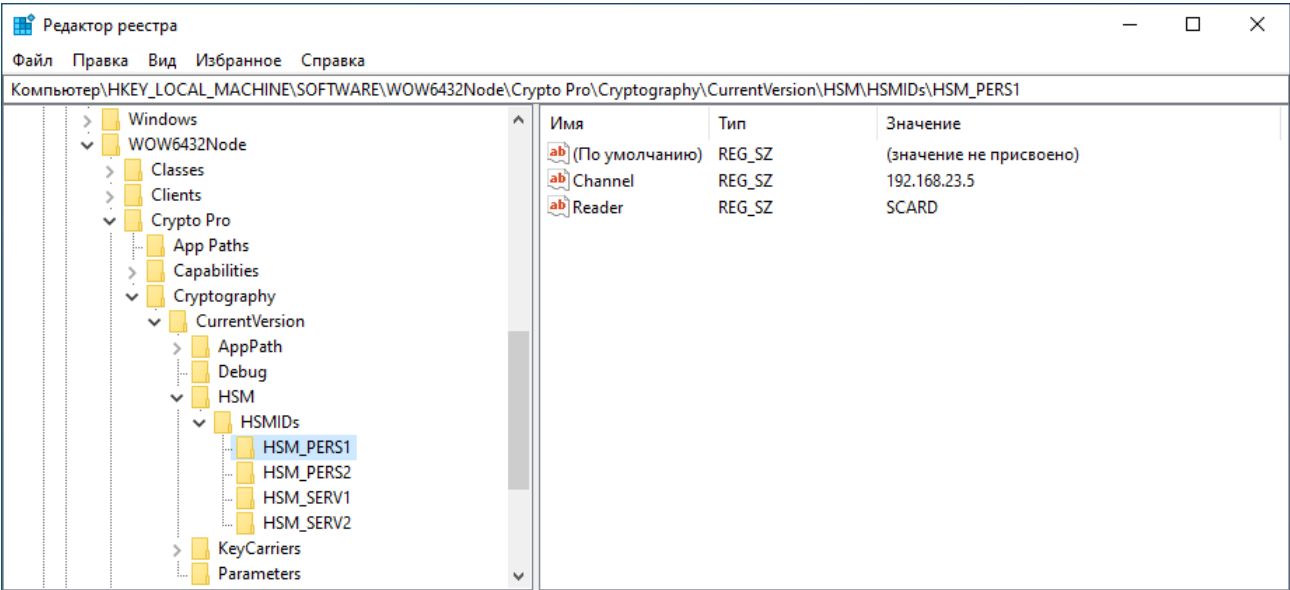


Рисунок 38. Список зарегистрированных ПАКМ

Описание дополнительных имен криптопровайдеров (по одной паре 75-го и 1-го типа для каждого ПАКМ, зарегистрированного в ключе HSMIDs) приведено на [рис. 39](#).

Регистрацию дополнительных имен криптопровайдеров удобно выполнять путем экспорта описаний существующих криптопровайдеров, например, Crypto-Pro HSM CSP и Crypto-Pro HSM RSA CSP, в файлы «.reg», изменением в этих файлах имен криптопровайдеров и параметров с именем «CP Service Name» (значение «RPC точки подключения»), и запуском этих обновленных файлов из оболочки Windows Explorer.

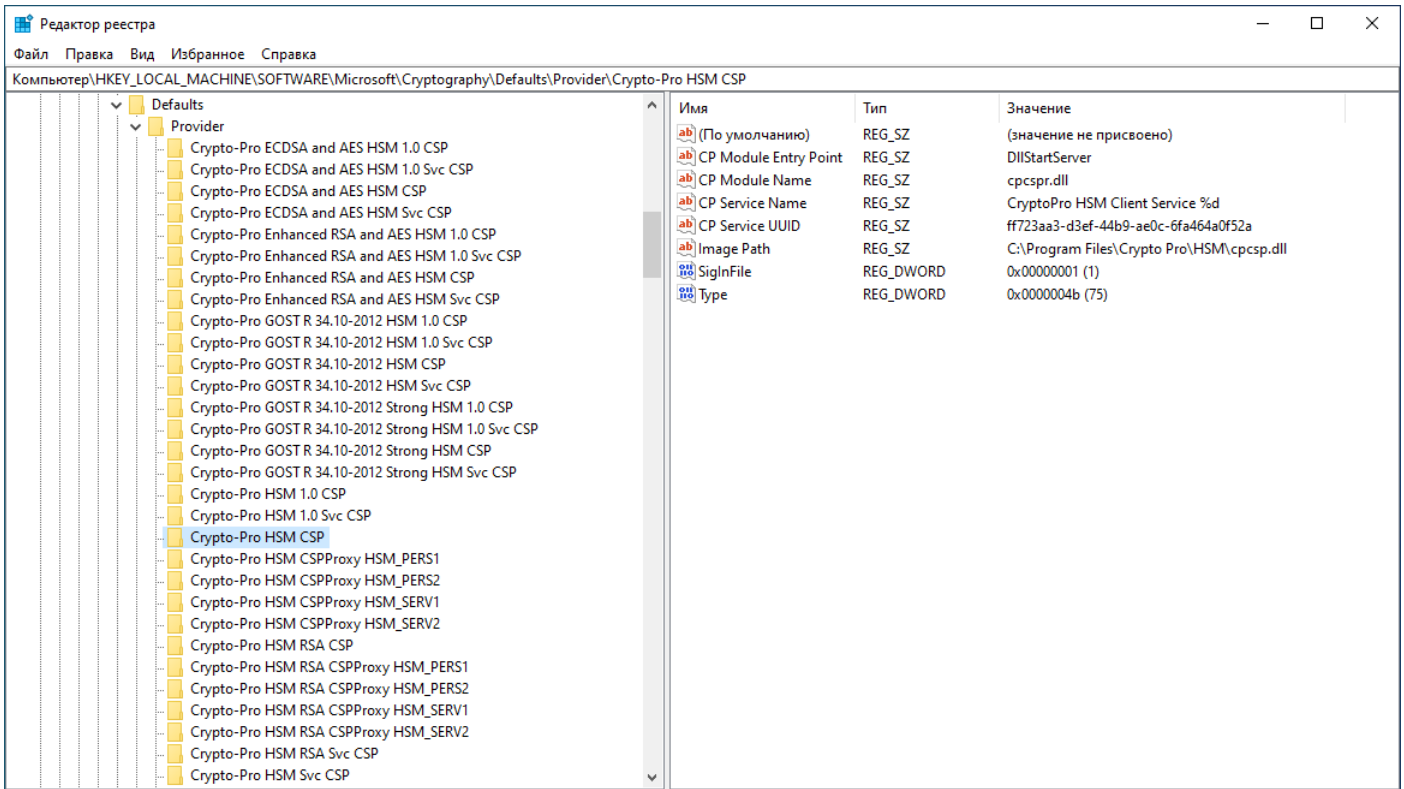


Рисунок 39. Дополнительные имена криптопровайдеров

При этом значение параметров «CP Service Name» для каждой пары ГОСТ и RSA криптопровайдеров должны быть одинаковы, т.е. один системный трей будет подключаться к одному ПАКМ, который обрабатывает запросы и для ГОСТ, и для RSA криптопровайдера (см. [рис. 40](#), [рис. 41](#), [рис. 42](#) и [рис. 43](#)).

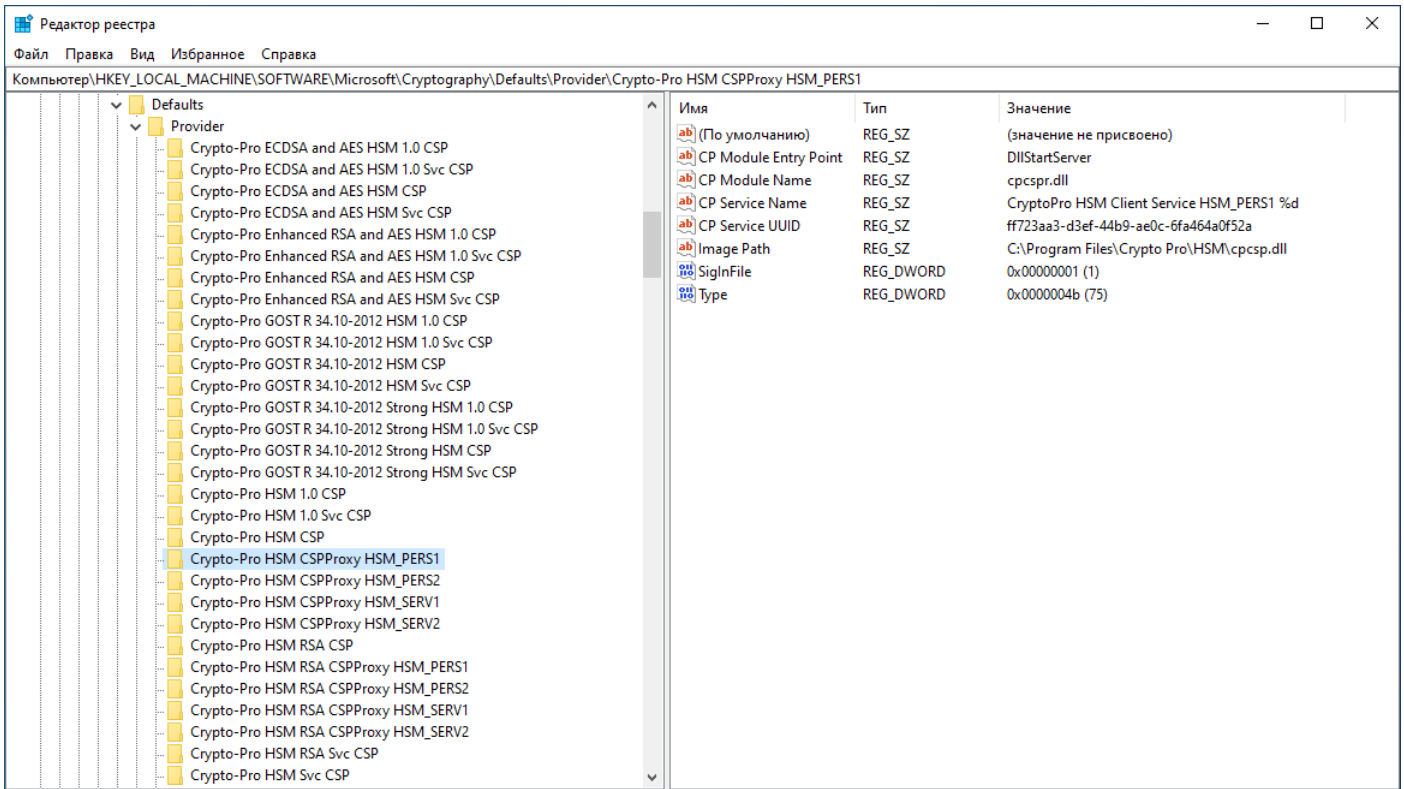


Рисунок 40. Параметры криптопровайдера Crypto-Pro HSM CSPPProxy HSM_PERS1

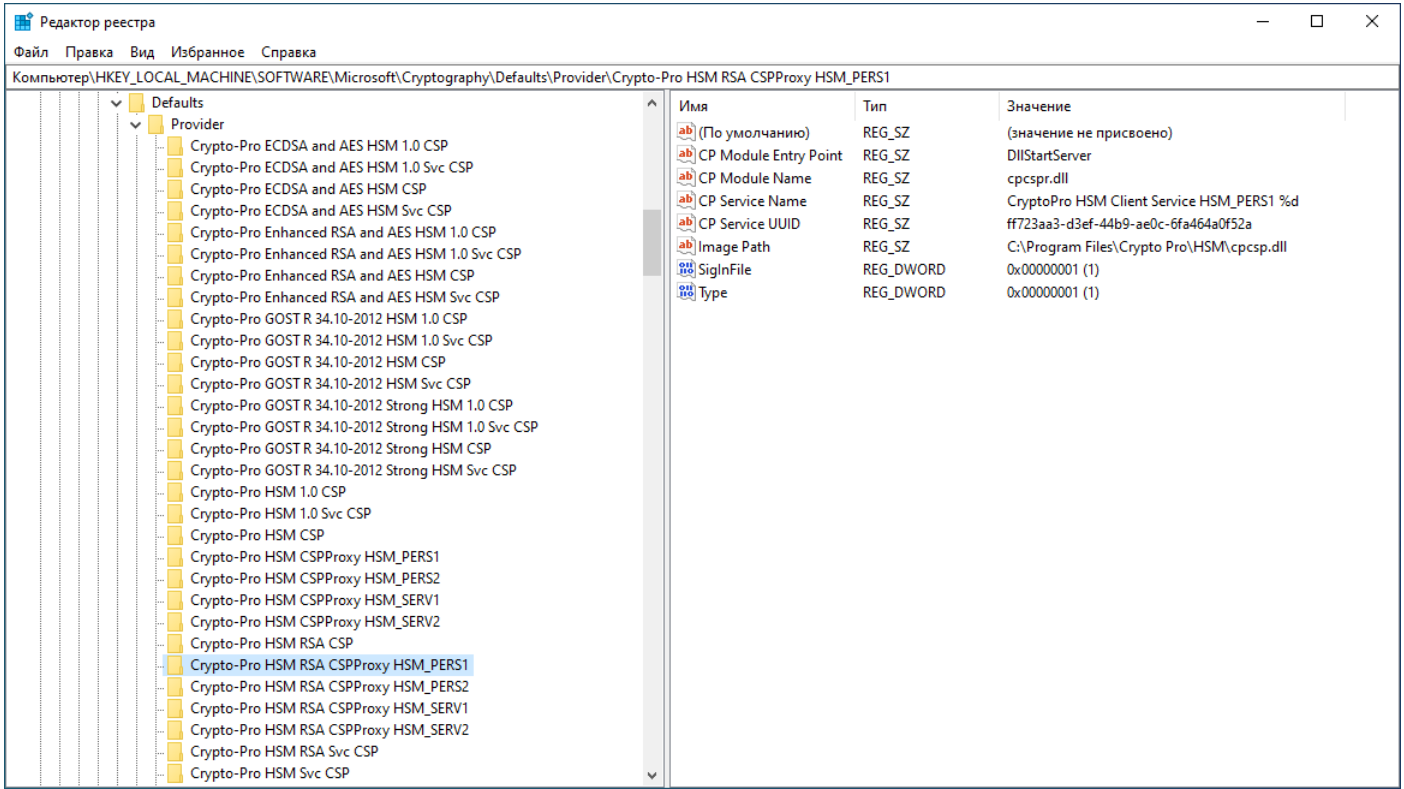


Рисунок 41. Параметры криптопровайдера Crypto-Pro HSM RSA CSPProxy HSM_PERS1

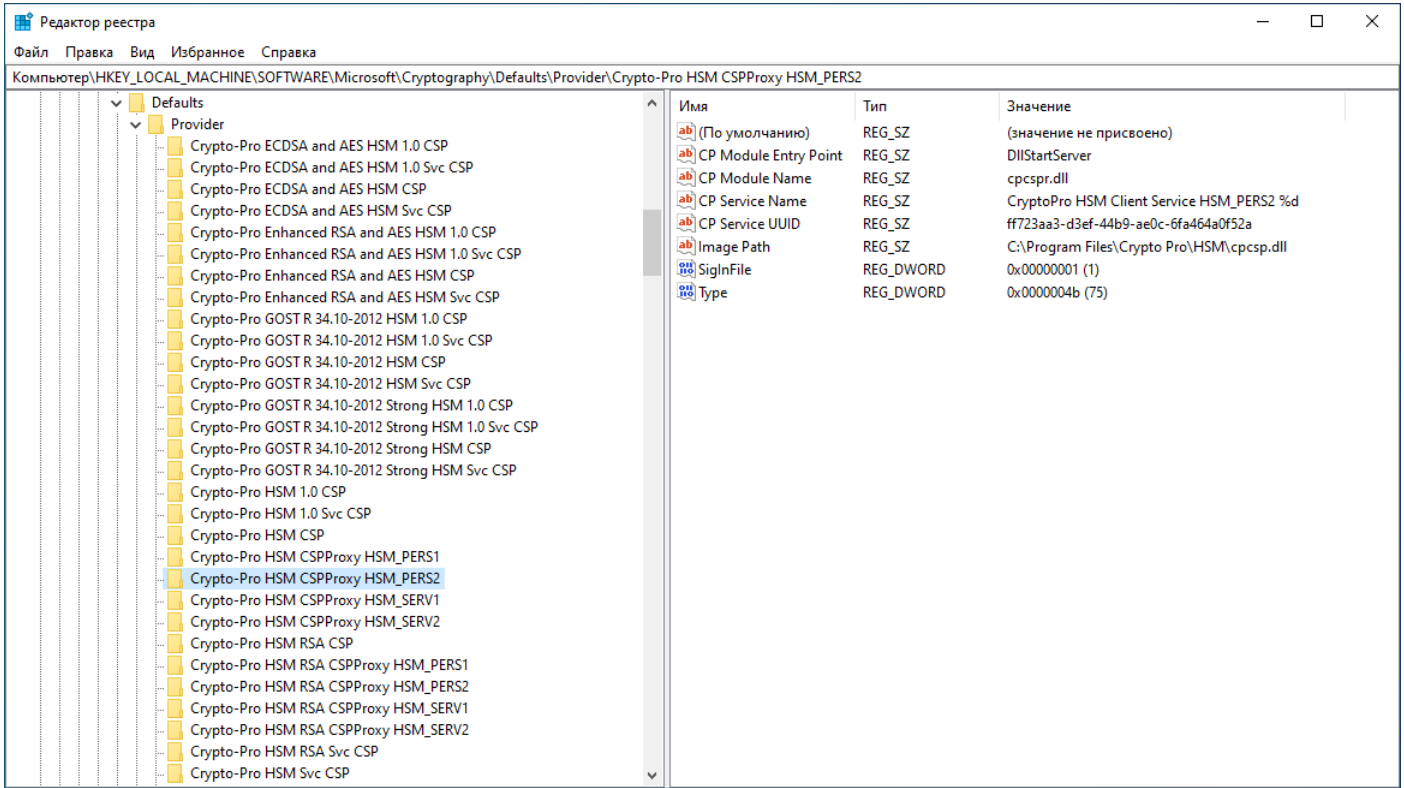


Рисунок 42. Параметры криптопровайдера Crypto-Pro HSM CSPProxy HSM_PERS2

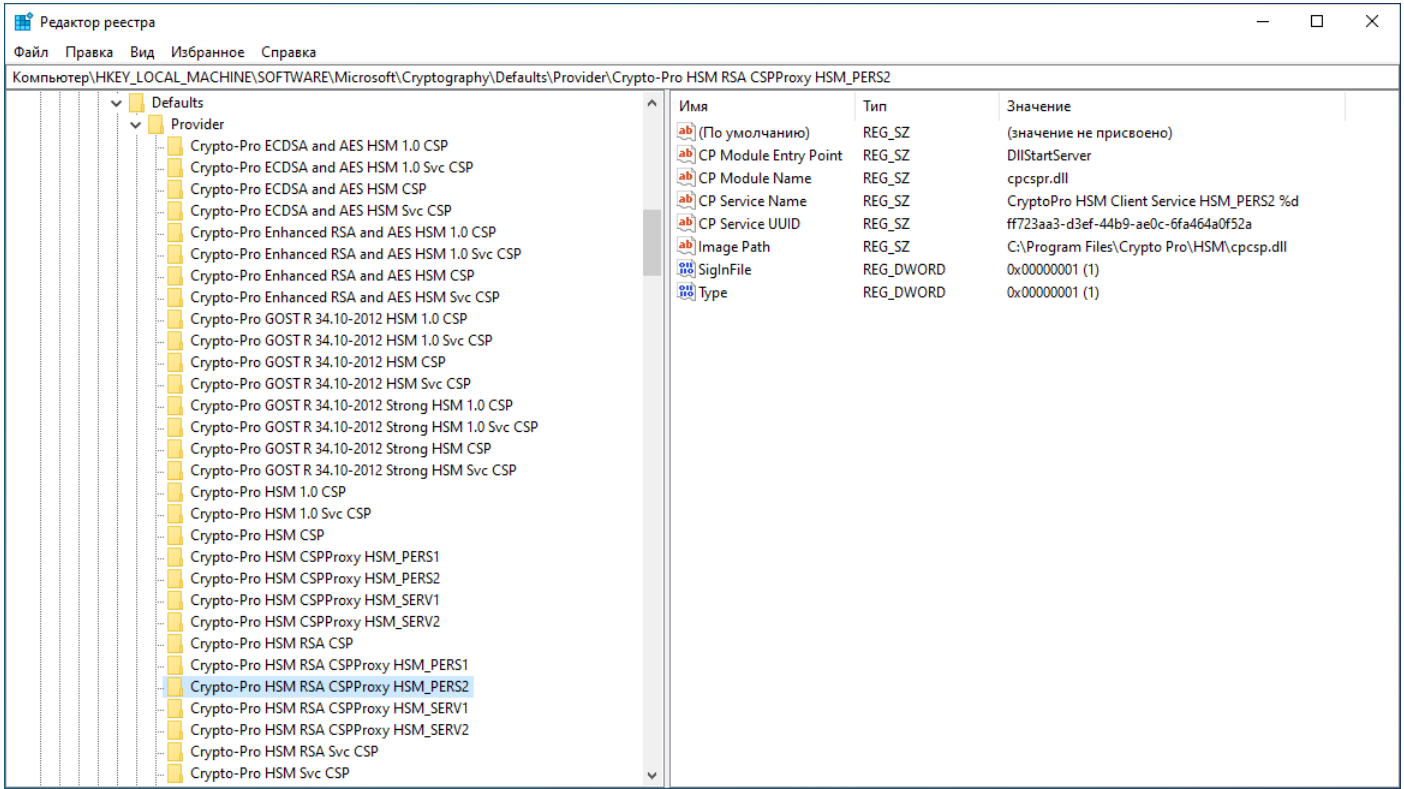


Рисунок 43. Параметры криптопровайдера Crypto-Pro HSM RSA CSPPProxy HSM_PERS2

Если в использовании RSA алгоритмов нет необходимости, то прописывать соответствующие имена криптопровайдеров не нужно.

5 Состав и назначение компонент ПО СКЗИ

5.1 Дистрибутив

Дистрибутив СКЗИ поставляется в виде пакета «Windows Installer» — файла `csp-<название_архитектуры>-<язык>.msi` (например, `csp-x64-rus.msi`). При запуске файл установщика разворачивает структуры данных дистрибутива во временный каталог и проводит установку ПО СКЗИ.

5.2 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 (HKLM)` — 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. 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 типа `DWORD`, равный требуемому числу дескрипторов, но не более 1048576.

5.3 Базовые модули СКЗИ

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

Следующие базовые модули входят в состав ПО СКЗИ:

<code>crverify.exe</code>	модуль предназначен для контроля целостности дистрибутива (см. Приложение 1 документа ЖТЯИ.00101-03 95 01. Правила пользования) при установке и использовании ПО СКЗИ КриптоПро CSP на компьютере пользователя
<code>crpanel.cpl</code>	модуль обеспечивает возможность управления пользователем конфигурацией ПО СКЗИ, а также содержит возможности регистрации установленного ПО и получения пользователем дополнительной информации

wipefile.exe	модуль используется для удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях (см. Приложение 1 документа ЖТЯИ.00101-03 95 01. Правила пользования)
cptools.exe	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)
certmgr.exe	приложение командной строки и используется для управления сертификатами, списками отзыва сертификатов и хранилищами
cryptsp.exe	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)
stunnel.exe	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.exe	приложение для создания TLS-туннеля с интерфейсом msspi, позволяющее организовывать соединения с поддержкой криптографических алгоритмов ГОСТ
stunnel_msspi_cli.exe	приложение для создания TLS-туннеля
cpcurl.dll	динамическая библиотека, предназначенная для передачи данных с синтаксисом URL (с поддержкой ГОСТ TLS)
cadcs.dll	динамическая библиотека, предназначенная для взаимодействия с CADES
npcades.dll	динамическая библиотека NPAPI для работы КриптоПро ЭЦП Browser plug-in

5.4 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.00101-03 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.).

Список модулей настройки подсистемы программной СФ ОС Windows и их описание приведено в [табл. 4](#).

Таблица 4. Модули настройки подсистемы программной СФ ОС Windows и их описание

Модуль	Описание модуля
cpext.dll	Зарегистрированная в системном реестре Windows динамическая библиотека (DLL) расширения CryptoAPI 2.0, обеспечивающая: • 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.
CProCtrl.sys	Модуль инициализации для ОС Windows, реализованный в виде драйвера. 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).
cpenroll.dll	Модуль, обеспечивающий настройку клиента служб регистрации.
cpmail.dll	Модуль, обеспечивающий настройку Internet Mail Messaging API.
cprastls.dll	Модуль, обеспечивающий исправление функционирования функционирования служб удаленного доступа (RAS).
cpxml5.dll	Модуль, обеспечивающий исправление функционирования служб обработки данных MSXML5.
cpcrypt.dll	Модуль настройки для системного DLL crypt32.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.
cpintco.dll	Модуль настройки для системного DLL inetcomm.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.
cpcertocm.dll	Модуль настройки для системного DLL certocm.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.

cpwinet.dll	Модуль настройки для системного DLL wininet.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.
cpadvai.dll	Модуль настройки для системного DLL advapi32.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.
cpkrb.dll	Модуль настройки для системного DLL kerberos.dll. Загружается в виртуальное адресное пространство процессов, использующих модуль kerberos.dll, и обеспечивает эмуляцию поддержки криптопровайдером стандарта Triple DES.
cpschan.dll	Модуль настройки TLS. Загружается в виртуальное адресное пространство процесса Internet Explorer/Microsoft Edge, если он использует TLS. Модуль позволяет использовать алгоритмы «КриптоПро TLS» в Internet Explorer/Microsoft Edge.
cpXML.dll	Модуль настройки XML. Загружается в виртуальное адресное пространство процессов, использующих XML, и позволяющий применять алгоритмы СКЗИ для подписи XML.
cpkdc.dll	Модуль настройки контроллера домена. Загружается в виртуальное адресное пространство процессов доменной аутентификации на контроллере домена и обеспечивает возможность использования для проверки подписи алгоритмов, реализуемых СКЗИ.
Модули настройки MS Office	
cpMSO.dll	Модуль, загружаемый в виртуальное адресное пространство процессов MS Word и MS Excell и позволяющий подписывать документы с помощью алгоритмов СКЗИ.
cpExSec.dll	Модуль, загружаемый в виртуальное адресное пространство процесса MS Outlook, и настраивающий его для правильной работы с СКЗИ.

5.5 Модули подсистемы программной СФ СКЗИ

Список модулей подсистемы программной среды функционирования криптосредства и их описание приведено в [табл. 5](#).

Таблица 5. Модули подсистемы программной СФ СКЗИ и их описание

Модуль	Описание модуля
--------	-----------------

cpui.dll	Модуль поддержки пользовательского интерфейса КриптоПро CSP.
cprevchk.dll	Модуль, обеспечивающий проверку сертификата на отзыв.
cppkcs11.dll	Модуль поддержки PKCS#11.
capi10.dll, capi20.dll	Модули управления сертификатами открытых ключей и обеспечения выполнения криптографических запросов на уровне интерфейсов CryptoAPI 1.0 и CryptoAPI 2.0 соответственно.
cpconfig.exe	Утилита командной строки для конфигурирования СКЗИ (работа с конфигурационным файлом).
genkpim.exe	Утилита командной строки для выработки внешней гаммы.
csptest.exe	Утилита командной строки для тестирования и проверки работоспособности СКЗИ.
cpsspi.dll	Модуль поддержки интерфейса SSPI и эмуляции LSA для работы с КриптоПро TLS.
CProDspr.dll	Модуль поддержки диспетчера контроля загрузки КриптоПро CSP.
hvisdef.dll	Модуль поддержки базового визуализатора КриптоПро CSP.
cpeng.dll	Модуль поддержки CNG в КриптоПро CSP.
cpsuprt.dll	Модуль поддержки общих функций доступа к различным устройствам хранения ключевой информации.
cpocard.dll	Модуль поддержки доступа к локальным смарт-картам по RDP.
cpasp.dll	Интерфейсная библиотека, реализующая стандартный интерфейс криптопровайдера, соответствующий спецификации Microsoft Cryptographic Service Provider, и обеспечивающая данный интерфейс для обычных приложений через криптографический сервис по RPC, или для привилегированных приложений (имеющих право доступа к устройствам носителей ключевого контейнера) — непосредственно.
Реализация криптопровайдера в форме сервиса хранения ключей	
cpaspr.dll	Интерфейсная библиотека, обеспечивающая возможность обращения обычных приложений к сервису криптографических функций по протоколу RPC.
Реализация криптопровайдера в форме подгружаемых библиотек	
cpaspi.dll	Интерфейс, реализующий целевые функции криптографической защиты информации для cpaspr.dll в варианте функционирования ПО СКЗИ без использования cpaspr.dll.
Реализация криптопровайдера в форме драйвера ядра ОС	

cpdrvlib.sys	Интерфейс, реализующий 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.
Реализация криптопровайдера в форме модуля ядра ОС	
cpksp.dll	Модуль, реализующий криптографические функции КриптоПро CSP для использования в режиме ядра. Если эта служба остановлена, на данном компьютере будет недоступна криптография КриптоПро CSP в режиме ядра. Если эта служба отключена, любые службы, которые явно зависят от нее, не могут быть запущены.
Интерфейсные модули ДСЧ	
accord.dll	Модуль поддержки ДСЧ АМДЗ "Аккорд".
ancud.dll	Модуль поддержки ДСЧ производства АНКАД.
bio.dll	Модуль поддержки БиоДСЧ.
crypton.dll	Модуль поддержки ДСЧ АПМДЗ "КРИПТОН-ЗАМОК".
dsrf.dll	Модуль поддержки ДСЧ ДСДР.
maxim.dll	Модуль поддержки ДСЧ АПМДЗ "МАКСИМ-М1".
sable.dll	Модуль поддержки ДСЧ электронного замка "Соболь".
vityaz.dll	Модуль поддержки ДСЧ АПМДЗ "Витязь А".
Панель управления ресурсами СКЗИ КриптоПро CSP	
cpanel.cpl	Модуль управления ресурсами СКЗИ КриптоПро CSP через панель управления. 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 панелью управления КриптоПро CSP приводится в документе ЖТЯИ.00101-03 92 01. Инструкция по использованию. Windows.
Интерфейсные модули устройств хранения ключевой информации	
accord.dll	Модуль поддержки считывателя АМДЗ "Аккорд".

cpfkс.dll	Модуль поддержки токенов и смарт-карт с поддержкой SESPАKE.
cloud.dll	Модуль поддержки облачного токена.
cryptoki.dll	Модуль поддержки доступа к ключам ФКН через интерфейс PKCS#11.
ds199x.dll	Модуль поддержки носителей Dallas Touch Memory (iButton).
edoc.dll	Модуль поддержки платформы eDoc (УЛГ).
emv.dll	Модуль поддержки смарт-карт Gemalto (EMV).
esmarttoken.dll	Модуль поддержки смарт-карт и токенов ESMART Token.
esmarttokengost.dll	Модуль поддержки смарт-карт и токенов ESMART Token ГОСТ.
fat12.dll	Модуль поддержки съемных дисков и разделов HDD/SDD.
infocrypt.dll	Модуль поддержки токенов InfoCrypt.
inpaspot.dll	Модуль поддержки смарт-карт Alioth.
jacarta.dll	Модуль поддержки токенов и смарт-карт JaCarta.
kst.dll	Модуль поддержки смарт-карт MorphoKST.
mskey.dll	Модуль поддержки токенов Multisoft MS_Key.
novacard.dll	Модуль поддержки смарт-карт Novacard.
pcsc.dll	Модуль поддержки базового считывателя носителей, поддерживающих интерфейс PC/SC.
reg.dll	Модуль поддержки системного реестра.
ric.dll	Модуль поддержки смарт-карт Оскар и Форос (Магистра).
rosan.dll	Модуль поддержки смарт-карт Rosan.
rutoken.dll	Модуль поддержки смарт-карт и токенов Рутокен.
sable.dll	Модуль поддержки считывателя электронного замка "Соболь".
safenet.dll	Модуль поддержки смарт-карт и токенов Gemalto и SafeNet.

5.6 Модули КриптоПро ЭЦП Browser plug-in

Список модулей КриптоПро ЭЦП Browser plug-in в составе КриптоПро CSP и их описание приведено в [табл. 6](#).

Таблица 6. Модули КриптоПро ЭЦП Browser plug-in и их описание

Модуль	Описание модуля
cplib.dll	Модуль поддержки работы с общеиспользуемыми типами.
mydss.dll	Модуль поддержки взаимодействия с DSS.
nmcades.exe	Модуль хоста Chrome Native Messaging для КриптоПро ЭЦП Browser plug-in.
xades.dll	Модуль поддержки внешнего интерфейса усовершенствованной ЭЦП для языка C (XAdES).
cadescm.dll, cadescm_enrollctrl.exe	Модули поддержки внешнего интерфейса усовершенствованной ЭЦП.
cplicmgt.dll	Модуль поддержки управления лицензиями продуктов компании «КРИПТО-ПРО».
pkimgmt.dll	Модуль поддержки управления продуктами компании «КРИПТО-ПРО».
pkiv validator.dll	Модуль проверки корректности различных условий для объектов PKI.
capicom.dll	COM-модуль для защиты приложений.
Модули взаимодействия с ASN.1 структурами	
asn1.dll	Модуль поддержки функций кодирования (декодирования) высокоуровневых структур ASN.1 в машинно-независимое представление.
asn1bercpp.dll	Модуль поддержки функций кодирования (декодирования) структур ASN.1 в BER/DER.
asn1rtcpp.dll	Модуль поддержки работы со структурами ASN.1.
asn1xercpp.dll	Модуль поддержки функций кодирования (декодирования) структур ASN.1 в XER.
cpasn1.dll	Модуль внешнего интерфейса для работы со структурами ASN.1.
Модули поддержки OCSP	
ocsp.dll	Модуль поддержки внешнего интерфейса протокола OCSP.
ocspcli.dll	Модуль поддержки интерфейса клиентских приложений (C++) протокола OCSP.
ocspview.exe	Приложение для просмотра OCSP-запросов и OCSP-ответов.
Библиотеки поддержки TSP	
tsp.dll	Модуль поддержки внешнего интерфейса протокола TSP.
tspcli.dll	Модуль поддержки интерфейса клиентских приложений (C++) протокола TSP.

tsppview.exe	Приложение для просмотра запросов на штамп времени и штампов времени.
--------------	---

5.7 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`, `cpssspap.dll` — при установке модуля аутентификации, поддерживающего аутентификацию в домене, `cpsspcore.dll`, `ssp.dll` — без возможности доменной аутентификации.

5.7.1 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 → Algorithm → 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.

5.8 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 `сapi20/сapi10`. При этом не требуется установка (инсталляция) криптопровайдера.

6 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.

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»).

7 Требования по криптографической защите

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

Контролем целостности должны быть охвачены указанные ниже файлы.



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

В случае нарушения целостности системных библиотек в результате обновления операционной системы необходимо пересчитать их контрольные суммы в соответствии с [разд. 4.5](#).

Windows 32-bit

```
\Program Files\Common Files\Crypto Pro\AppCompat\cpadvai.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpcertocm.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpcrypt.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\AppCompat\cpintco.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpkdc.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\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
\Program Files\Common Files\Crypto Pro\AppCompat\cpwinet.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpxml5.dll
\Program Files\Common Files\Crypto Pro\Shared\cadescom.dll
\Program Files\Common Files\Crypto Pro\Shared\cadescom_enrollctrl.exe
\Program Files\Common Files\Crypto Pro\Shared\cpext.dll
\Program Files\Common Files\Crypto Pro\Shared\cplicmgt.dll
\Program Files\Common Files\Crypto Pro\Shared\cptools.exe
\Program Files\Common Files\Crypto Pro\Shared\ocspview.exe
\Program Files\Common Files\Crypto Pro\Shared\pkimgmt.dll
\Program Files\Common Files\Crypto Pro\Shared\pkivalidator.dll
\Program Files\Common Files\Crypto Pro\Shared\tspview.exe
\Program Files\Crypto Pro\CSP\accord.dll
\Program Files\Crypto Pro\CSP\ancud.dll
\Program Files\Crypto Pro\CSP\bio.dll
\Program Files\Crypto Pro\CSP\certmgr.exe
\Program Files\Crypto Pro\CSP\cloud.dll
\Program Files\Crypto Pro\CSP\cpanel.cpl
\Program Files\Crypto Pro\CSP\cpcsp.dll
\Program Files\Crypto Pro\CSP\cpcspi.dll
\Program Files\Crypto Pro\CSP\cpcspr.dll
\Program Files\Crypto Pro\CSP\cpdrvlib.sys
```

\Program Files\Crypto Pro\CSP\cpfkcs.dll
\Program Files\Crypto Pro\CSP\cpksp.sys
\Program Files\Crypto Pro\CSP\cppkcs11.dll
\Program Files\Crypto Pro\CSP\cprevchk.dll
\Program Files\Crypto Pro\CSP\CProCtrl.sys
\Program Files\Crypto Pro\CSP\CProDspr.dll
\Program Files\Crypto Pro\CSP\cpscard.dll
\Program Files\Crypto Pro\CSP\cpsspi.dll
\Program Files\Crypto Pro\CSP\cpsuprt.dll
\Program Files\Crypto Pro\CSP\cpui.dll
\Program Files\Crypto Pro\CSP\cpverify.exe
\Program Files\Crypto Pro\CSP\cryptoki.dll
\Program Files\Crypto Pro\CSP\crypton.dll
\Program Files\Crypto Pro\CSP\csptest.exe
\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
\Program Files\Crypto Pro\CSP\hvisdef.dll
\Program Files\Crypto Pro\CSP\infocrypt.dll
\Program Files\Crypto Pro\CSP\inpaspot.dll
\Program Files\Crypto Pro\CSP\jacarta.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\oauth2client.exe
\Program Files\Crypto Pro\CSP\pcsc.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
\Program Files\Crypto Pro\CSP\usbccid.sys
\Program Files\Crypto Pro\CSP\vityaz.dll
\Program Files\Crypto Pro\CSP\wipefile.exe
\Program Files\Crypto Pro\CADES Browser Plug-in\asn1.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\asn1bercpp.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\asn1rtcpp.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\asn1xercpp.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\cades.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\cpasn1.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\cplib.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\mydss.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\nmcades.exe

\Program Files\Crypto Pro\CADES Browser Plug-in\npcades.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\ocsp.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\ocspcli.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\tsp.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\tspcli.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\xades.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\asn1.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\asn1bercpp.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\asn1rtcpp.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\asn1xercpp.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\bio.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\capi10.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\capi20.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\cpasn1.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\cpconfig.exe
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\cpcspi.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\cpplib.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\cpsuprt.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\cpui.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\dsrf.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\fat12.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\jacarta.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\pcsc.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\rutoken.dll
\Program Files\Crypto Pro\CADES Browser Plug-in\Mini CSP\safenet.dll
\Windows\system32\cpcng.dll
\Windows\system32\cpssl.dll
\Windows\system32\cpsspap.dll
\Windows\system32\crypt32.dll
\Windows\system32\cryptsp.dll
\Windows\system32\inetcomm.dll
\Windows\system32\kerberos.dll
\Windows\system32\schannel.dll
\Windows\system32\sspicli.dll
\Windows\system32\wininet.dll
\Windows\system32\winscard.dll



Примечание. Для ОС Windows Server 2008 под контролем целостности вместо библиотек cryptsp.dll и ssPICLI.dll находятся библиотеки \Windows\system32\advapi32.dll и \Windows\system32\secur32.dll.



Примечание. При использовании модулей (приложений) cryptsp и stunnel их исполняемые файлы также должны быть поставлены под контроль целостности (с использованием утилиты cerverify, подробнее см. Приложение 1 ЖТЯИ.00101-03 95 01. Правила пользования) с указанием пути их расположения, выбранного Администратором безопасности при установке.

Windows 64-bit

```
\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
\Program Files\Common Files\Crypto Pro\AppCompat\cpcrypt.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpcrypt.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\AppCompat\cpintco.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpintco.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpkdc.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpkdc.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 (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\Common Files\Crypto Pro\AppCompat\cpschan.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpschan.dll
\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
\Program Files\Common Files\Crypto Pro\Shared\cadescom.dll
\Program Files (x86)\Common Files\Crypto Pro\Shared\cadescom.dll
\Program Files\Common Files\Crypto Pro\Shared\cadescom_enrollctrl.exe
\Program Files (x86)\Common Files\Crypto Pro\Shared\cadescom_enrollctrl.exe
\Program Files\Common Files\Crypto Pro\Shared\cpext.dll
\Program Files (x86)\Common Files\Crypto Pro\Shared\cpext.dll
\Program Files\Common Files\Crypto Pro\Shared\cplicgmt.dll
\Program Files (x86)\Common Files\Crypto Pro\Shared\cplicgmt.dll
\Program Files (x86)\Common Files\Crypto Pro\Shared\cptools.exe
\Program Files (x86)\Common Files\Crypto Pro\Shared\ocspview.exe
\Program Files\Common Files\Crypto Pro\Shared\pkimgmt.dll
\Program Files (x86)\Common Files\Crypto Pro\Shared\pkimgmt.dll
\Program Files\Common Files\Crypto Pro\Shared\pkivalidator.dll
\Program Files (x86)\Common Files\Crypto Pro\Shared\pkivalidator.dll
\Program Files (x86)\Common Files\Crypto Pro\Shared\tspview.exe
\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
```

\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\Crypto Pro\CSP\cpanel.cpl
\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\Crypto Pro\CSP\cpcspr.dll
\Program Files (x86)\Crypto Pro\CSP\cpcspr.dll
\Program Files\Crypto Pro\CSP\cpdrvlib.sys
\Program Files (x86)\Crypto Pro\CSP\cpdrvlib.sys
\Program Files\Crypto Pro\CSP\cpfkcdll.dll
\Program Files (x86)\Crypto Pro\CSP\cpfkcdll.dll
\Program Files\Crypto Pro\CSP\cpksp.sys
\Program Files (x86)\Crypto Pro\CSP\cpksp.sys
\Program Files\Crypto Pro\CSP\cppkcs11.dll
\Program Files (x86)\Crypto Pro\CSP\cppkcs11.dll
\Program Files\Crypto Pro\CSP\cprevchk.dll
\Program Files (x86)\Crypto Pro\CSP\cprevchk.dll
\Program Files\Crypto Pro\CSP\CProCtrl.sys
\Program Files (x86)\Crypto Pro\CSP\CProCtrl.sys
\Program Files\Crypto Pro\CSP\CProDspr.dll
\Program Files (x86)\Crypto Pro\CSP\CProDspr.dll
\Program Files\Crypto Pro\CSP\cpscard.dll
\Program Files (x86)\Crypto Pro\CSP\cpscard.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\Crypto Pro\CSP\cpui.dll
\Program Files (x86)\Crypto Pro\CSP\cpui.dll
\Program Files (x86)\Crypto Pro\CSP\cpverify.exe
\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
\Program Files\Crypto Pro\CSP\csptest.exe
\Program Files (x86)\Crypto Pro\CSP\csptest.exe
\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
\Program Files\Crypto Pro\CSP\hvisdef.dll
\Program Files (x86)\Crypto Pro\CSP\hvisdef.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
\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 (x86)\Crypto Pro\CSP\oauth2client.exe
\Program Files\Crypto Pro\CSP\pcsc.dll
\Program Files (x86)\Crypto Pro\CSP\pcsc.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
\Program Files (x86)\Crypto Pro\CSP\usbccid.sys
\Program Files\Crypto Pro\CSP\vityaz.dll
\Program Files (x86)\Crypto Pro\CSP\vityaz.dll
\Program Files (x86)\Crypto Pro\CSP\wipefile.exe
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\asn1.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\asn1bercpp.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\asn1rtcpp.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\asn1xercpp.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\cades.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\cpasn1.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\cplib.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\mydss.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\nmcades.exe
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\npcades.dll

\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\ocsp.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\ocspcli.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\tsp.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\tspcli.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\xades.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\asn1.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\asn1.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\asn1bercpp.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\asn1bercpp.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\asn1rtcpp.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\asn1rtcpp.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\asn1xercpp.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\asn1xercpp.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\bio.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\bio.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\capi10.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\capi10.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\capi20.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\capi20.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpasn1.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpasn1.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpconfig.exe
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpconfig.exe
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpspi.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpspi.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpplib.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpplib.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpsuprt.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpsuprt.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpui.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\cpui.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\dsrf.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\dsrf.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\fat12.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\fat12.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\jacarta.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\jacarta.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\pcsc.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\pcsc.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\rutoken.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\rutoken.dll
\Program Files\Crypto Pro\CAdES Browser Plug-in\Mini CSP\safenet.dll
\Program Files (x86)\Crypto Pro\CAdES Browser Plug-in\Mini CSP\safenet.dll
\Windows\system32\cpcng.dll
\Windows\SysWOW64\cpcng.dll
\Windows\system32\cpssl.dll
\Windows\SysWOW64\cpssl.dll
\Windows\system32\cpsspap.dll
\Windows\SysWOW64\cpsspap.dll
\Windows\system32\crypt32.dll

\Windows\SysWOW64\crypt32.dll
\Windows\system32\cryptsp.dll
\Windows\SysWOW64\cryptsp.dll
\Windows\system32\inetcomm.dll
\Windows\SysWOW64\inetcomm.dll
\Windows\system32\kerberos.dll
\Windows\SysWOW64\kerberos.dll
\Windows\system32\schannel.dll
\Windows\SysWOW64\schannel.dll
\Windows\system32\sspicli.dll
\Windows\SysWOW64\sspicli.dll
\Windows\system32\wininet.dll
\Windows\SysWOW64\wininet.dll
\Windows\system32\winscard.dll
\Windows\SysWOW64\winscard.dll



Примечание. Для ОС Windows Server 2008 под контролем целостности вместо библиотек cryptsp.dll и spicli.dll находятся библиотеки:

- \Windows\system32\advapi32.dll,
- \Windows\SysWOW64\advapi32.dll,
- \Windows\system32\secur32.dll,
- \Windows\SysWOW64\secur32.dll.



Примечание. При использовании модулей (приложений) cryptsp и stunnel их исполняемые файлы также должны быть поставлены под контроль целостности (с использованием утилиты crverify, подробнее см. Приложение 1 ЖТЯИ.00101-03 95 01. Правила пользования) с указанием пути их расположения, выбранного Администратором безопасности при установке.

8 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 раздела 4 ЖТЯИ.00101-03 95 01. Правила пользования.

Приложение А

Управление протоколированием

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
cap10	CryptoAPI 1.0
cap120	CryptoAPI 2.0
cloud	облачный провайдер
cng	CNG
cpext	расширения CryptoAPI
cryptoki	поддержка PKCS#11
csp	ядро CSP
cspi	интерфейс CSP
cspr	интерфейс CSP в режиме службы (RPC)
pcsc	считыватели смарт-карт PC/SC
ssp	TLS
support	считыватели ключевой информации

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 0xXX0YY0ZZ. 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:

```
ssp = 0x0100003f // выводить только критические ошибки в EventLog и всю трассировочную  
информацию в DbgView модуля поддержки TLS
```

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

Таблица Б2. 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 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:

```
ssp_fmt = 0x00000042 - выводить значение GetLastError и номер нитки для модуля поддержки TLS
```

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.

Включение аудита SSP

Управление протоколированием КриптоПро SSPI в журнале событий Windows (EventLog) осуществляется с помощью параметра **EventLogging** (DWORD) ветки реестра HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL.

Значением параметра является шестнадцатеричное число (сумма чисел), соответствующее уровням выводимых событий (см. [табл. Б4](#)).

Таблица Б4. Уровни протоколирования Schannel

0x00	логирование отключено
0x01	сообщения об ошибках
0x02	предупреждения
0x03	предупреждения и сообщения об ошибках
0x04	информационные сообщения и успешные события
0x05	информационные сообщения, успешные события и сообщения об ошибках
0x06	информационные сообщения, успешные события и предупреждения
0x07	все события



Примечание. Для применения настроек необходима перезагрузка компьютера.

Лист регистрации изменений

[illegible]