

**Средство защиты информации  
«КриптоПро SPR»**

Версия 4.0

**Руководство администратора безопасности  
Установка**

ЖТЯИ.00112-01 90 02

Листов 28



Компания «КРИПТО-ПРО»

2021

Компания «КРИПТО-ПРО», 2019-2021. Все права защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании «КРИПТО-ПРО» этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании «КРИПТО-ПРО».

ООО «КРИПТО-ПРО»

Адрес 127018, г. Москва, ул. Суцеский Вал, дом 18

Телефон +7 (495) 995-4820

e-mail [info@cryptopro.ru](mailto:info@cryptopro.ru)

Web [www.cryptopro.ru](http://www.cryptopro.ru)

## Оглавление

Список сокращений.....	4
1. Введение .....	5
2. Установочный компакт-диск системы.....	6
3. Установка в графическом режиме .....	6
3.1. Установка СКЗИ КристоПро CSP .....	6
3.2. Установка SPR 4.0.....	7
4. Установка в режиме «без окон» .....	12
5. Установка в доменной среде .....	13
6. Методика экспресс-анализа корректности функционирования компонентов СЗИ .....	20
6.1. Предназначение и состав утилиты sprstatus.....	20
6.2. Использование утилиты sprstatus. ....	20
6.3. Проверка работы КристоПро TLS .....	22
6.4. Пересчет контрольных сумм системных библиотек ОС. ....	24
Список литературы .....	28

## Список сокращений

<b>АИС</b>	Автоматизированная информационная система
<b>АРМ</b>	Автоматизированное рабочее место
<b>АС</b>	Автоматизированная система
<b>ЗПС</b>	Замкнутая программная среда
<b>ИС</b>	Информационная система
<b>НСД</b>	Несанкционированный доступ
<b>ОС</b>	Операционная система
<b>ПАК</b>	Программно-аппаратный комплекс
<b>ПКЗИ</b>	Подсистема криптографической защиты информации
<b>ПО</b>	Программное обеспечение
<b>ППО</b>	Прикладное программное обеспечение
<b>СЗИ</b>	Средство или система защиты информации
<b>СКЗИ</b>	Средство криптографической защиты информации
<b>СХКИ</b>	Средство хранения конфиденциальной информации

# 1. Введение

Данное руководство предназначено для администраторов средства защиты информации «КриптоПро SPR» версия 4.0 (сокращенное названия изделия – SPR 4.0). В руководстве содержатся сведения, необходимые администраторам для установки системы защиты, ее обновления, исправления и удаления.

## 2. Установочный компакт-диск системы

Программное обеспечение и эксплуатационная документация SPR 4.0 находится на установочном компакт-диске. Структура каталогов диска представлена в Таб. 1.

**Таб. 1. Структура каталогов дистрибутива SPR 4.0**

Файлы и папки дистрибутива	Описание
Certs	Папка содержит сертификаты соответствия на КристоПро SPR 4.0 и на продукты входящие в его состав.
Editions 1, 2	Папка содержит сертификаты соответствия на СЗИ КристоПро SPR 4.0 (исполнения 1, 2) и на СКЗИ КристоПро CSP 5.0 R2.
Distribs	Папка содержит дистрибутивы SPR 4.0 и продуктов входящих в его состав.
SPR 4.0	Папка содержит дистрибутивы SPR 4.0.
Edition 1 (AK3)	Папка содержит дистрибутивы SPR 4.0 (исполнение 1)
Edition 2 (AK2)	Папка содержит дистрибутивы SPR 4.0 (исполнение 2)
CSP 5.0 R2	Папка содержит дистрибутивы СКЗИ КристоПро CSP 5.0 R2, входящего в состав SPR 4.0 (исполнения 1, 2).
Docs	Папка содержит документацию на SPR 4.0 и на продукты входящие в его состав.
.\SPR	Папка содержит документацию на SPR 4.0.
.\CSP	Папка содержит документацию на CSP 5.0 R2.
ReleaseNotes.pdf	Файл содержит список последних изменений и дополнений SPR 4.0 и продуктов входящих в его состав.

## 3. Установка в графическом режиме

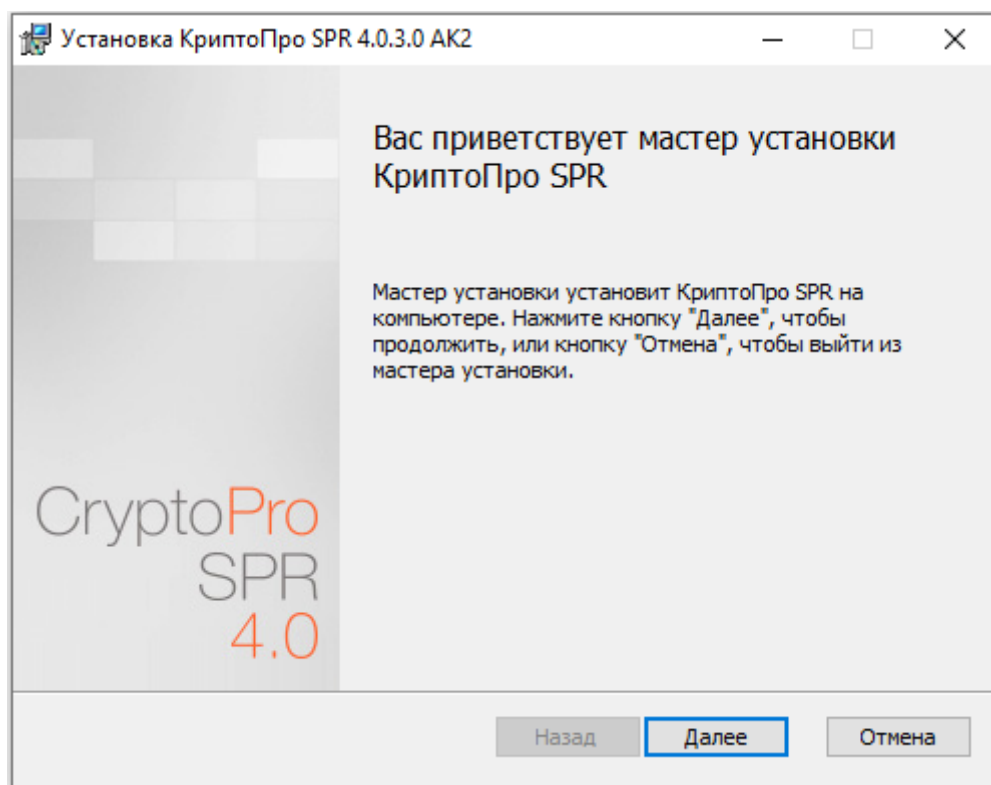
### 3.1. Установка СКЗИ КристоПро CSP

Полная инструкция по установке СКЗИ КристоПро CSP 5.0 R2, необходимого для SPR 4.0 (исполнения 1, 2), приведена в [1] [2].

### 3.2. Установка SPR 4.0

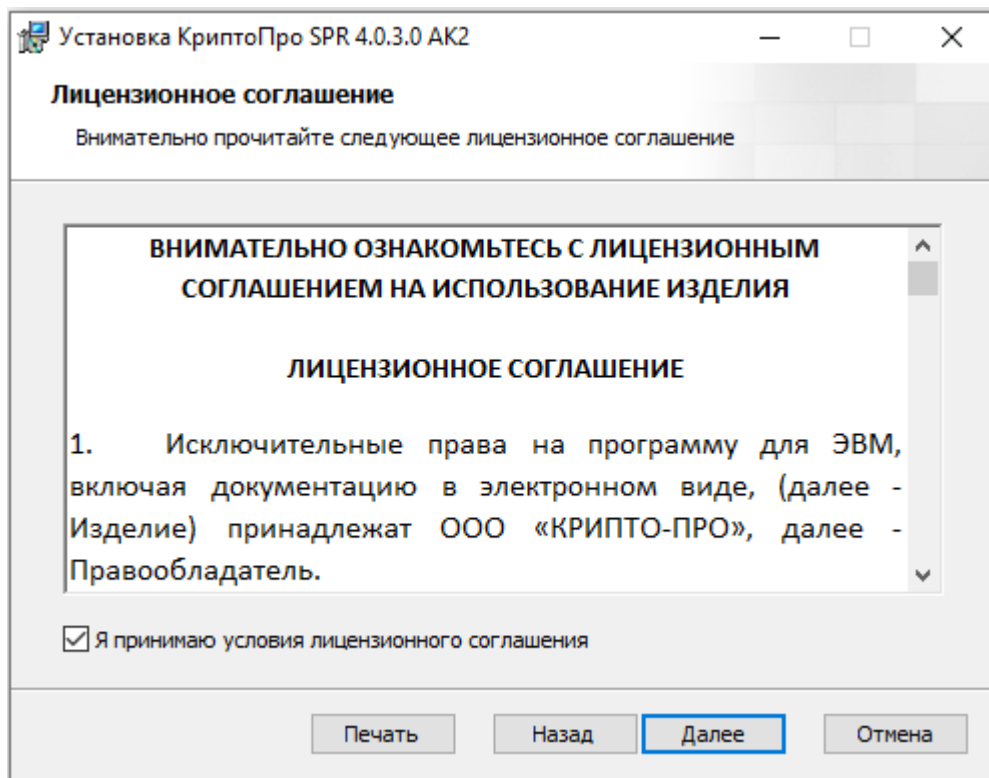
Для установки SPR 4.0 необходимо запустить файл из дистрибутива соответствующий целевой программной платформе (x86 или x64) и необходимому классу СЗИ (АК2 или АК3). После запуска появится окно приветствия (Рис. 1).

**Рис. 1. Окно приветствия установщика SPR 4.0**



После нажатия кнопки «Далее» появится окно с лицензионным соглашением об использовании SPR 4.0 (Рис. 2).

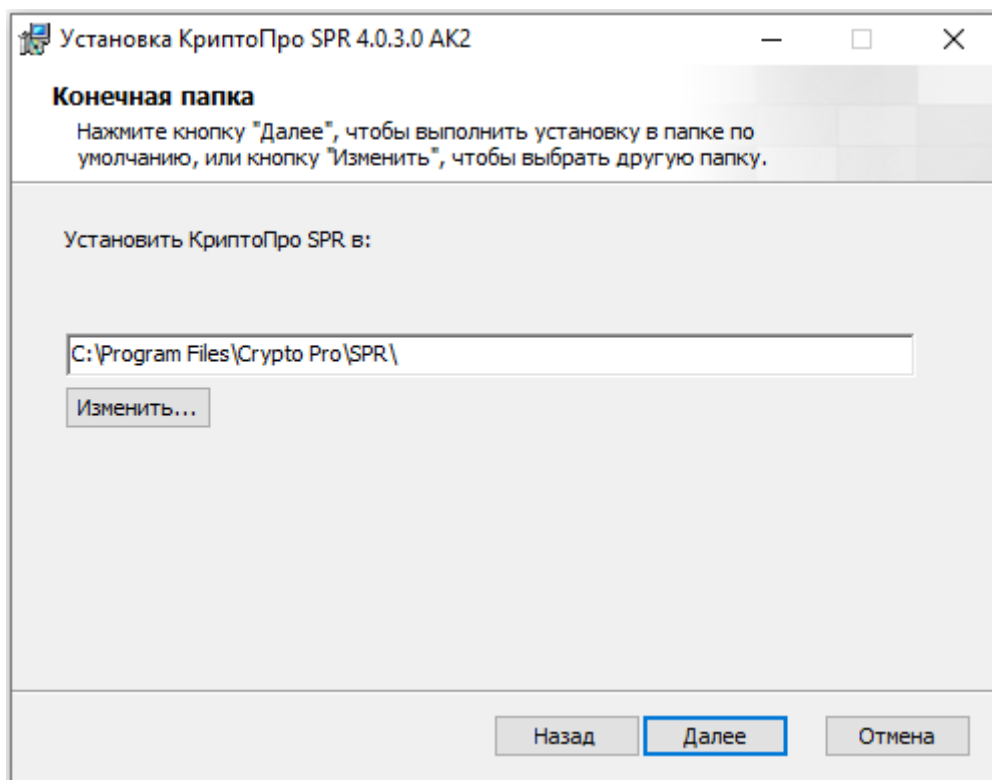
Рис. 2. Окно лицензионного соглашения установщика SPR 4.0



Чтобы продолжить установку, после прочтения лицензионного соглашения с ним нужно согласиться, отметив поле «Я принимаю условия лицензионного соглашения» и нажать «Далее». Появится окно выбора директории, куда будет установлен SPR 4.0 (Рис. 3).

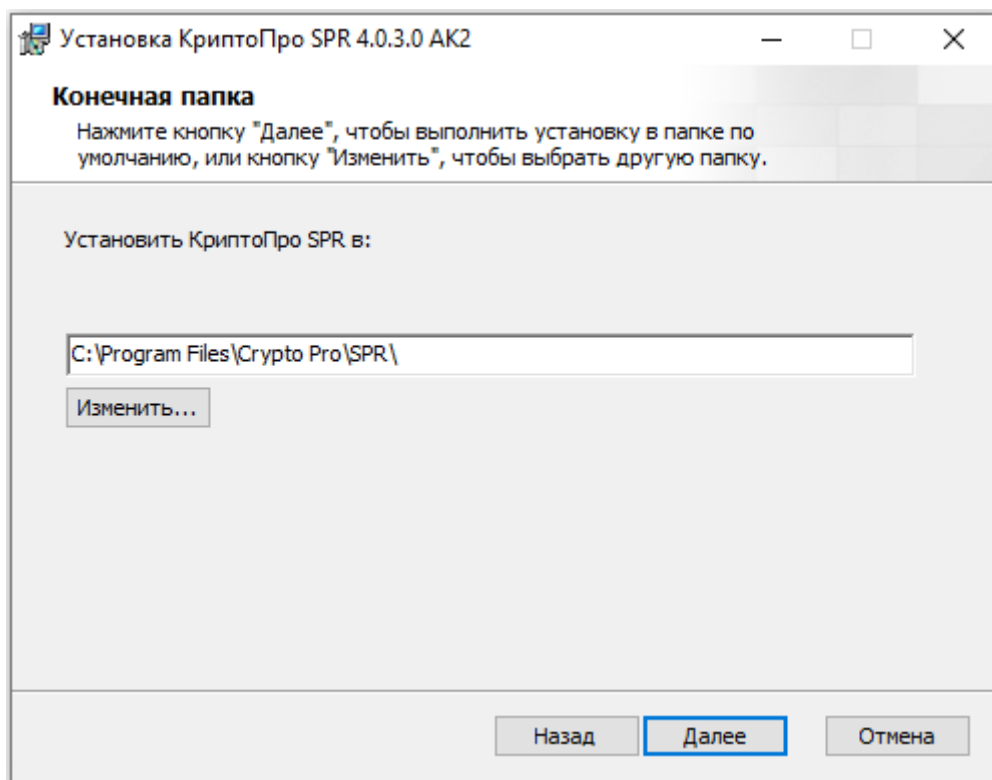


**Рис. 3. Окно выбора папки установки установщика SPR 4.0**



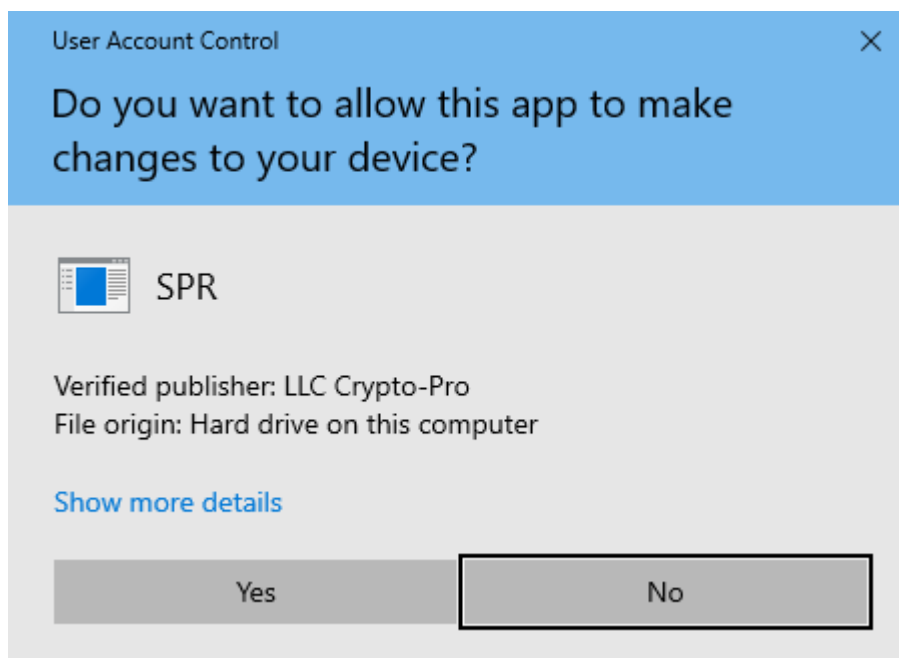
Выбрав директорию установки и нажав «Далее» появится окно подтверждения установки (Рис. 4).

**Рис. 4. Окно подтверждения установки установщика SPR 4.0**



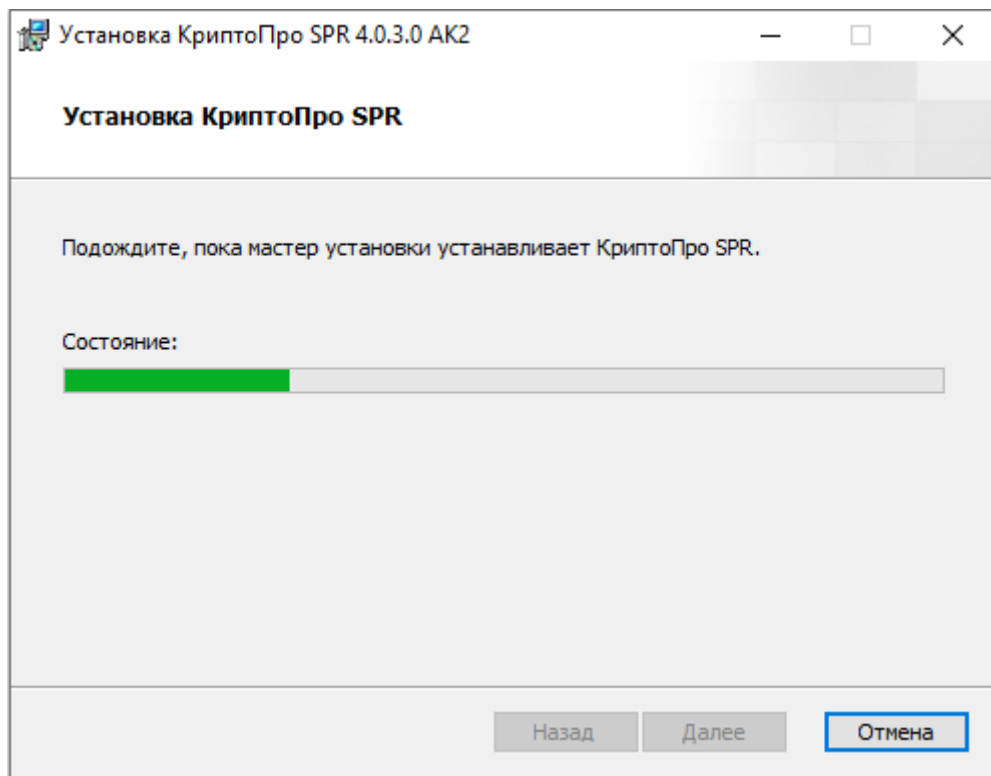
После нажатия кнопки «Установить», если в операционной системе включен контроль учетных записей пользователей, появится окно разрешения установки (Рис. 5).

**Рис. 5. Окно UAC установщика SPR 4.0**



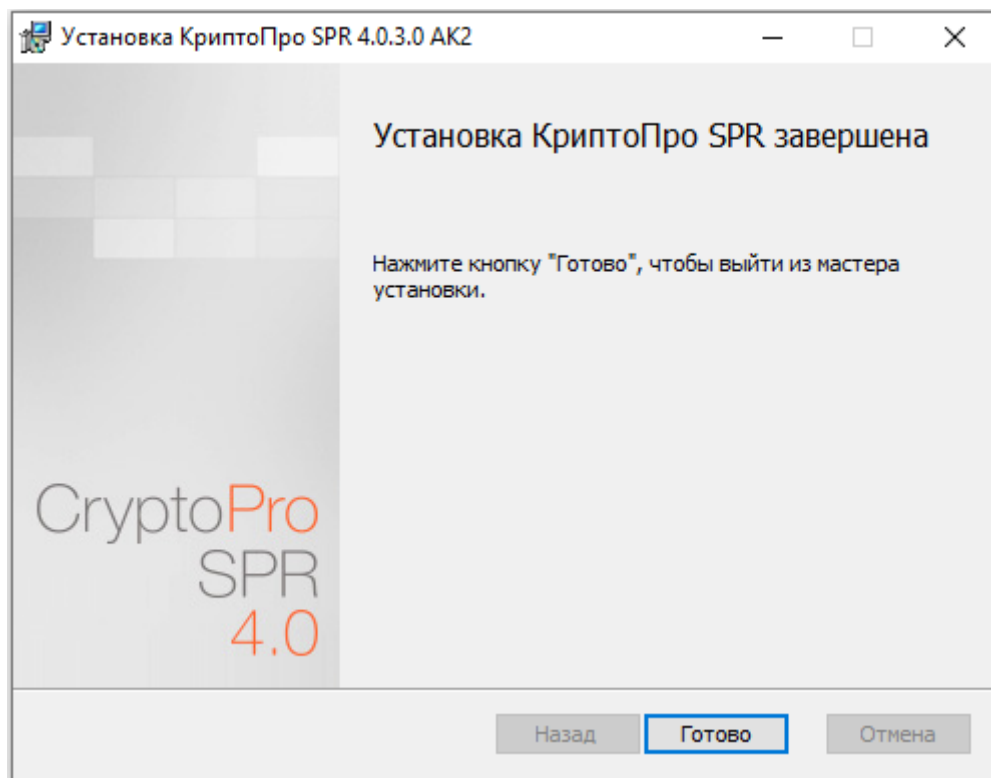
Для продолжения, необходимо разрешить внесение изменений на данном компьютере нажав «Да».

**Рис. 6. Окно прогресса инсталляции установщика SPR 4.0**



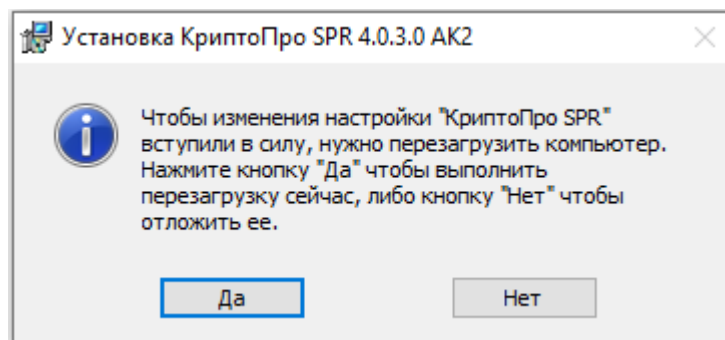
По окончании установки появится окно завершения. В этом окне отображается результат установки, если процесс установки прошел без ошибок, то окно будет как на Рис. 7. Если в процессе установки возникли ошибки, то в окне будет отображена имеющаяся информация о возникших проблемах.

**Рис. 7. Окно завершения инсталляции установщика SPR 4.0**



После нажатия на кнопку «Готово» появится диалог (Рис. 8), предлагающий перезагрузить компьютер.

**Рис. 8. Окно перезагрузки установщика SPR 4.0**



Для завершения установки необходимо перезагрузить компьютер, нажав кнопку «Да».

## **4. Установка в режиме «без окон»**

Для установки в режиме «без окон» (установка не будет видна пользователю) необходимо выполнить следующие команды в консоли CMD, запущенной с правами администратора:

1. Для установки СКЗИ Крипто Про CSP необходимо запустить инсталляционный исполняемый файл CSPSetup-5.0.XXXXXX.exe со следующими ключами:

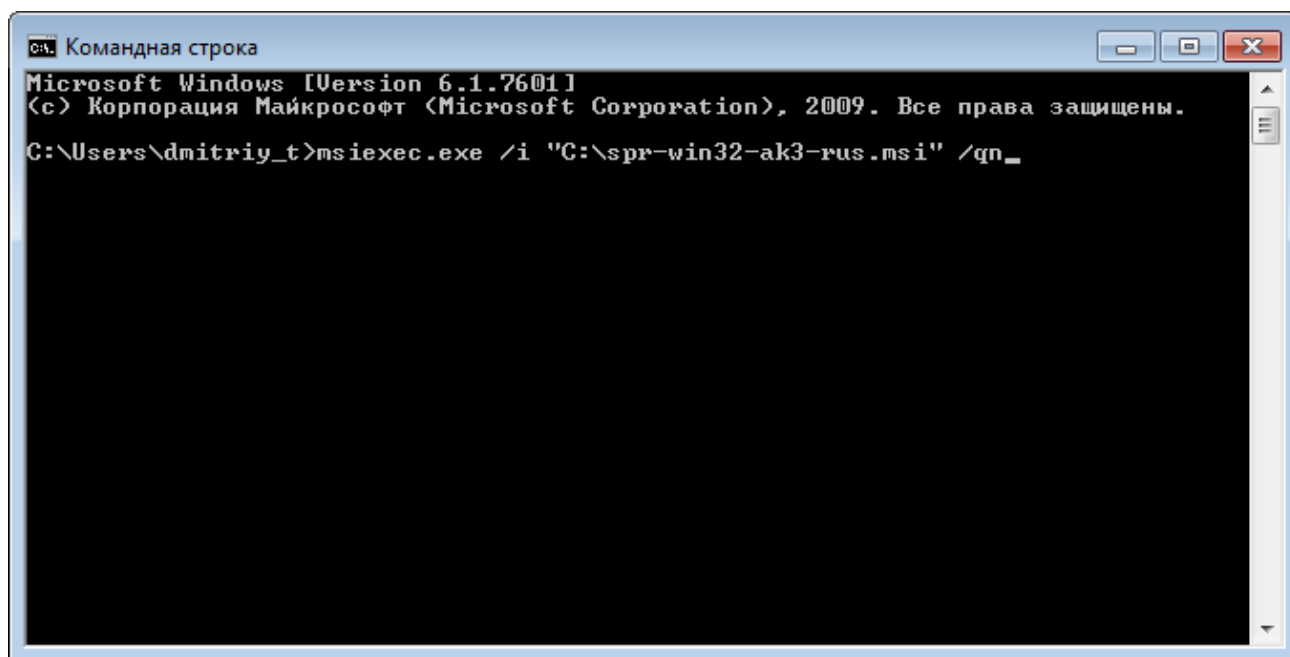
«CSPSetup-5.0.11972.exe -kc kc3 -lang rus -noroot -noreboot -nodlg -silent -args FOREIGN=1 -args DRIVER=1 -args NOREGISTRY=1 -args KCLEVEL=3 -args /qb -args /qn».

2. Для установки SPR 4.0 выполнить:

«msiexec.exe /i "[Полный путь до MSI-файла]\spr-win32-ak3-rus.msi" /qn /norestart».

После завершения установки в фоновом режиме необходимо выполнить перезагрузку компьютера и заполнить поля серийных номеров лицензий для установленного ПО.

**Рис. 9. Пример командной строки запуска установки SPR 4.0 в режиме «без окон»**

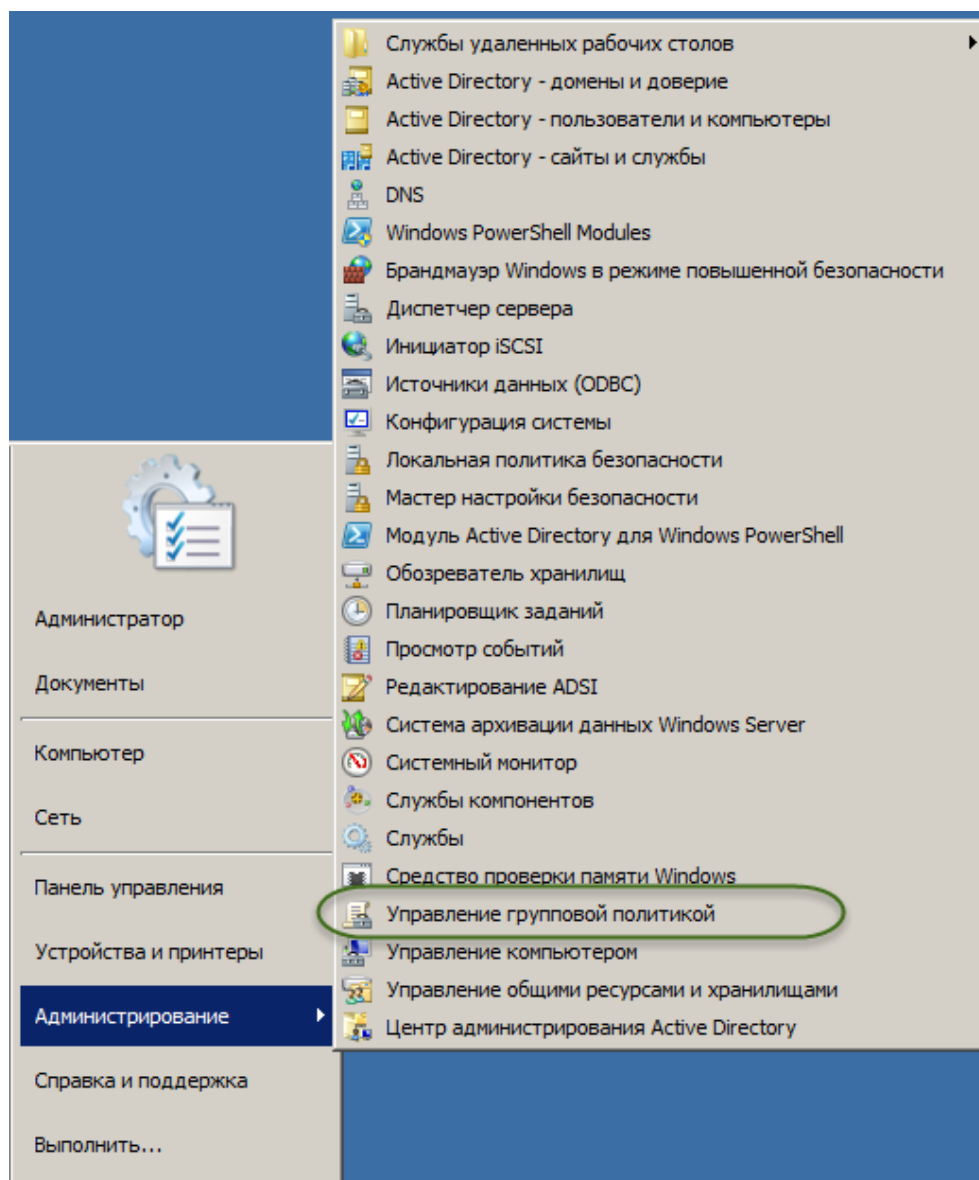


## 5. Установка в доменной среде

Для автоматизации установки в доменной среде можно использовать штатное средство установки ПО с применением механизма доменных политик. Для автоматической установки необходимо создать доступную для всех компьютеров домена, участвующих в установке, общую сетевую папку с правами на чтение, после чего создать несколько объектов групповой политики, соответствующих устанавливаемому компоненту.

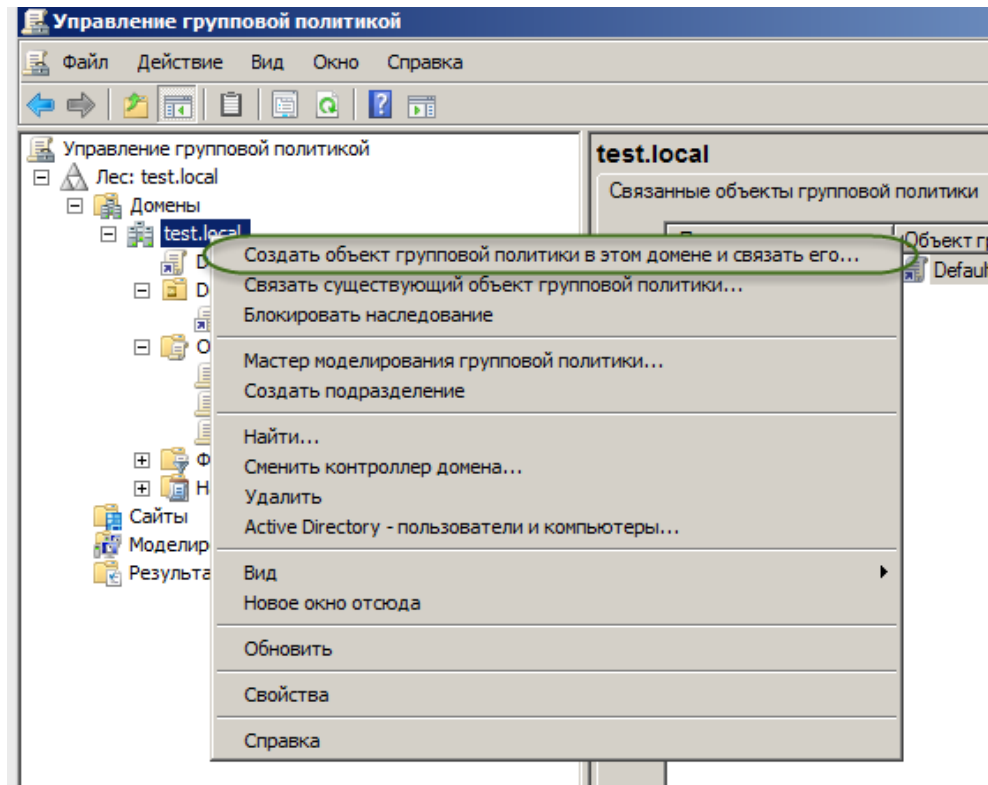
Для создания объекта групповых политик необходимо открыть оснастку «Управление групповой политикой» «Пуск → Администрирование» (Рис. 10).

**Рис. 10. Запуск оснастки управления групповыми политиками**



Необходимо выбрать текущий домен и создать новый объект групповой политики с помощью мастера (Рис. 11).

**Рис. 11. Создание объекта групповой политики**



Выбрав режим редактирования созданного объекта (Рис. 12) необходимо создать пакет для установки требуемого компонента (Конфигурация компьютера → Политики → Конфигурация программ → Установка программ) (Рис. 13 - Рис. 14).

Рис. 12. Редактирование объекта групповой политики

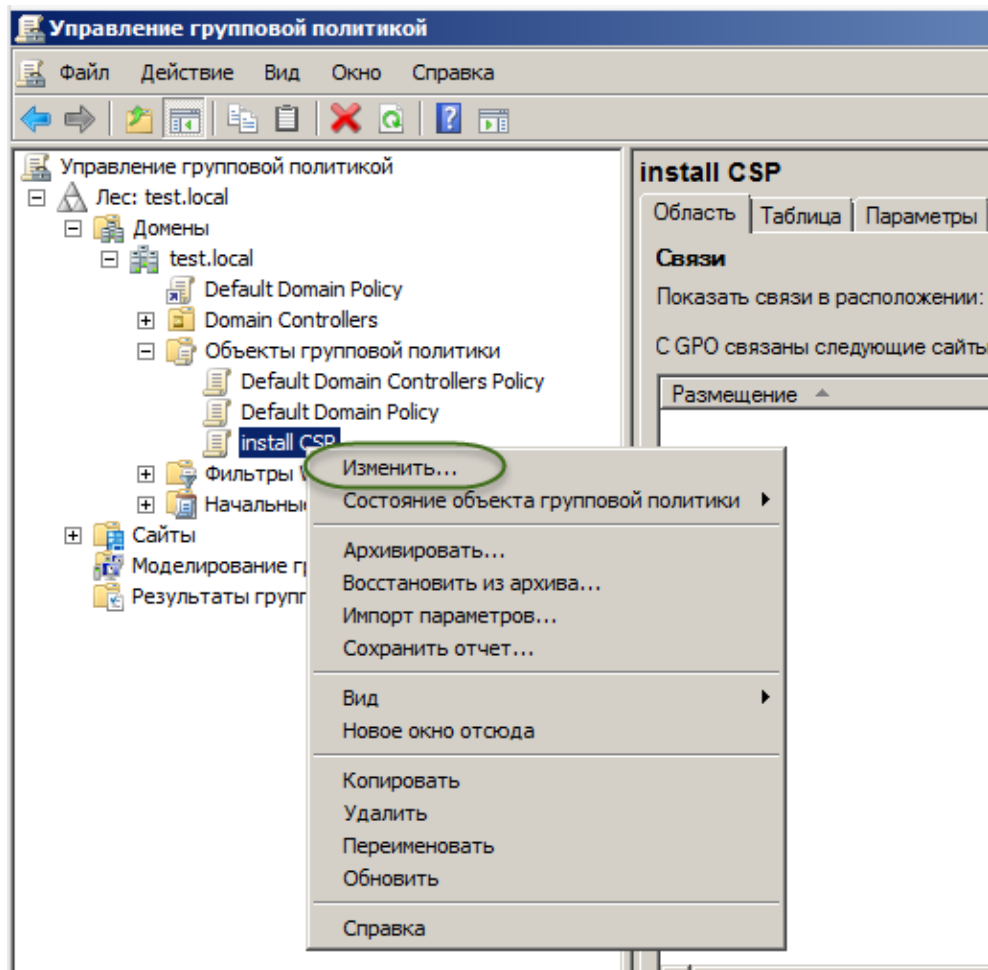




Рис. 13. Создание пакета установки ПО

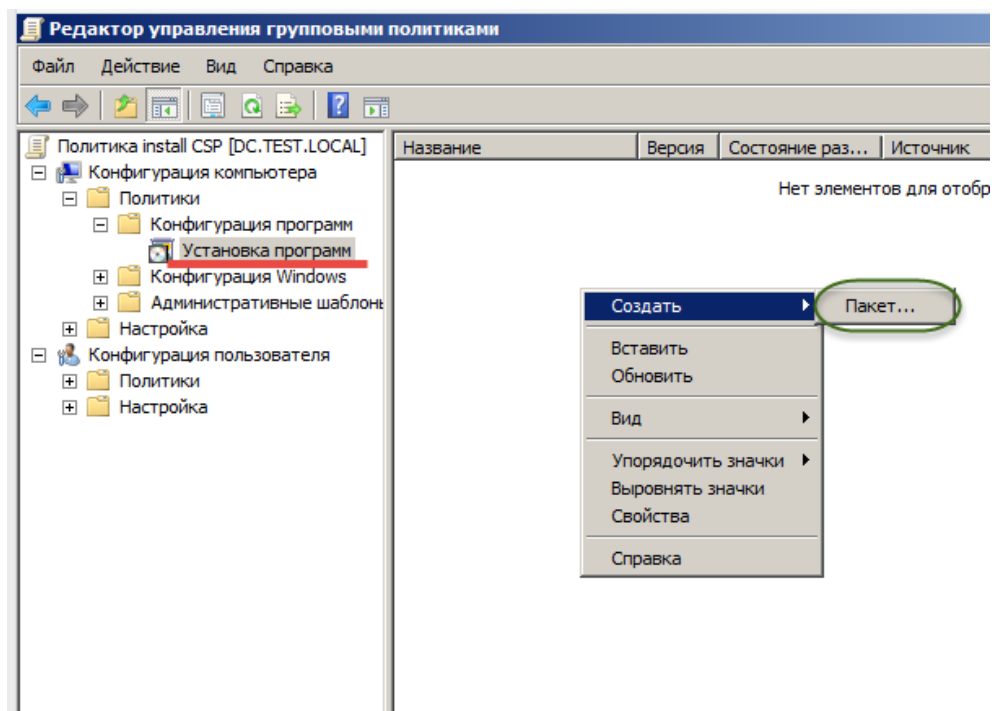
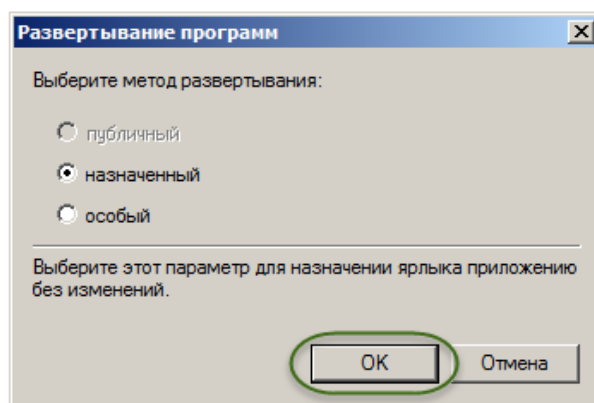


Рис. 14. Выбор типа развертывания ПО



После создания пакета (Рис. 15) необходимо предоставить право на чтение объекта групповой политики для компьютеров, участвующих в установке (Рис. 16).

Рис. 15. Пакет установки ПО

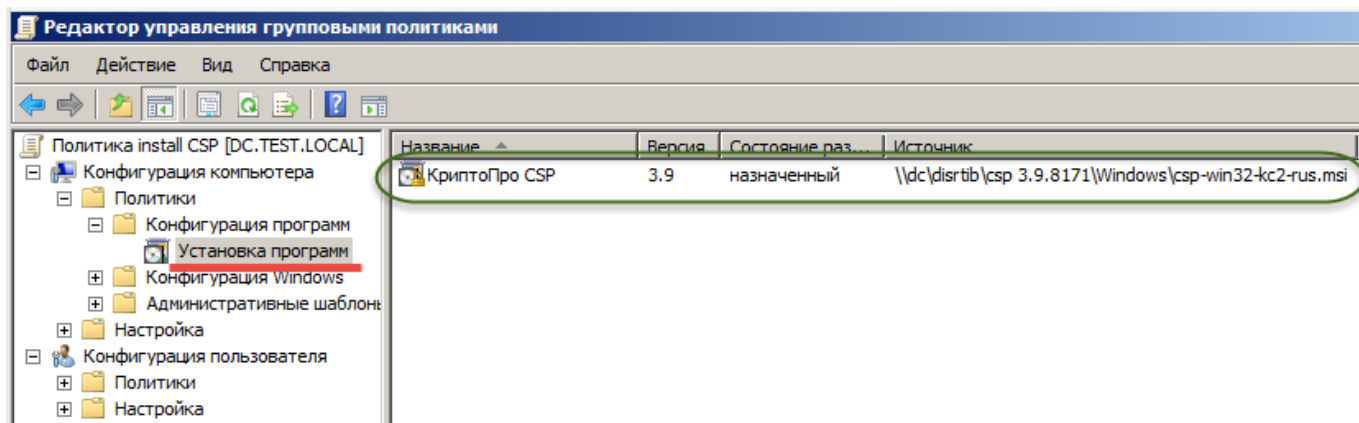
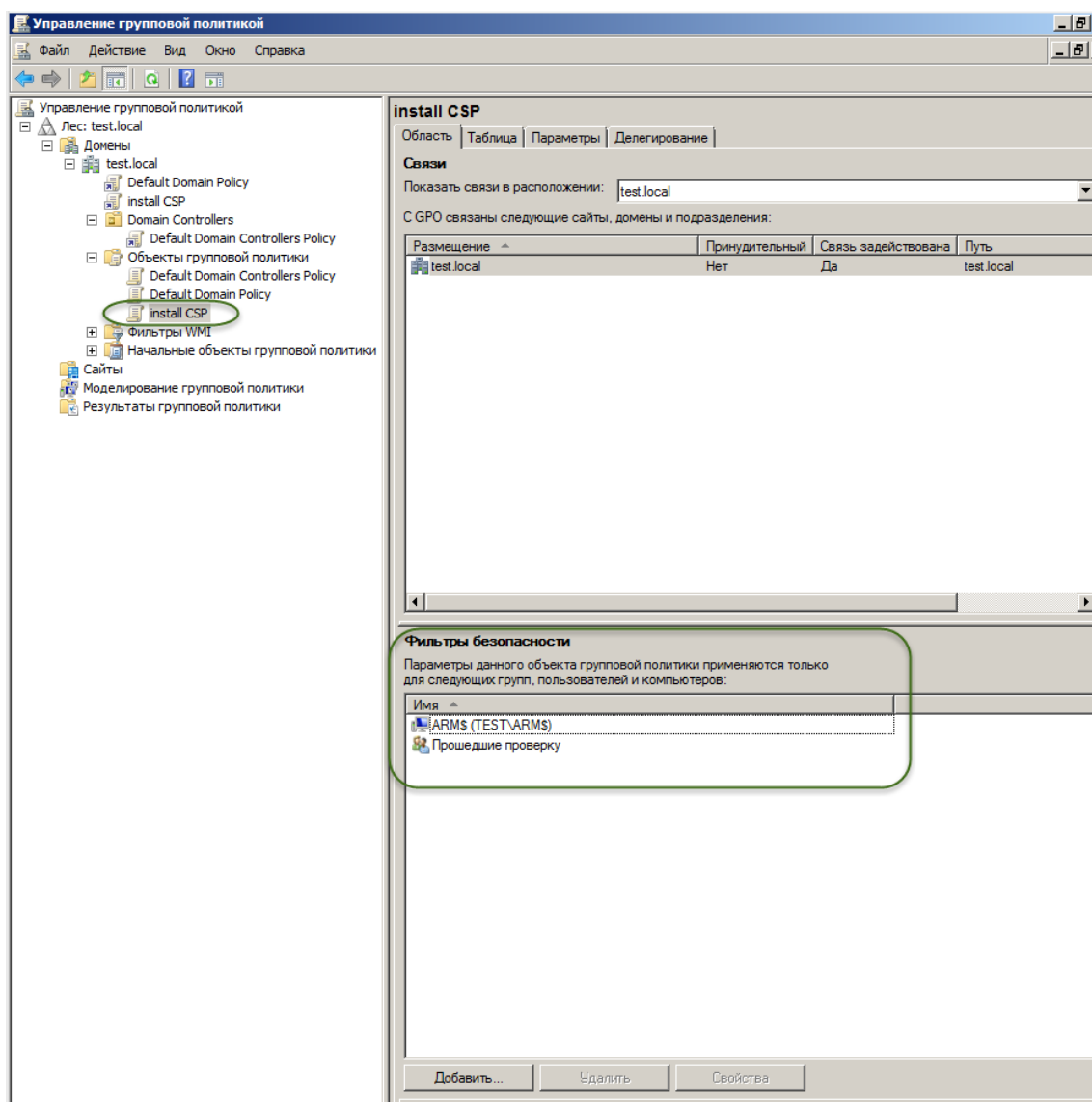
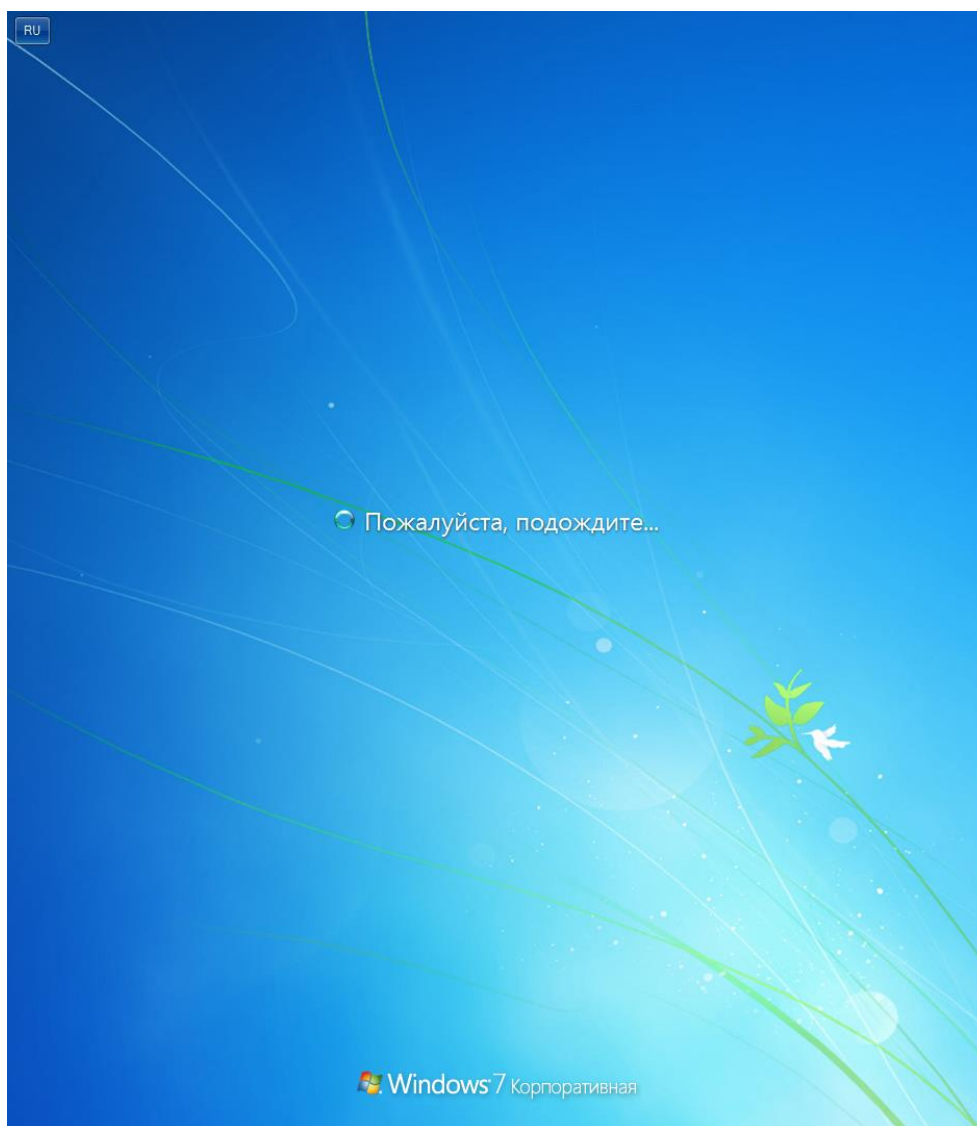


Рис. 16. Управление правами доступа к объекту групповой политики



В процессе очередной перезагрузки объект групповой политик будет применен к компьютеру и произойдет автоматическая установка ПО (Рис. 17).

**Рис. 17. Процесс установки по на пользовательский ПК**



#### **Примечание**

В процессе установки ПО может потребоваться перезагрузка ОС, которая будет выполнена автоматически. До момента полного завершения процесса установки ПО работа пользователя на АРМ будет невозможна.

После установки ПО необходимо зафиксировать серийные номера ПО на АРМ пользователей.

## 6. Методика экспресс-анализа корректности функционирования компонентов СЗИ

Методика экспресс-анализа корректности функционирования компонентов SPR 4.0 предназначена для проверки текущего состояния ряда подсистем СЗИ, включая подсистемы СКЗИ КристоПро CSP.

Основное предназначение экспресс-анализа — это проверка состояния компонентов SPR 4.0 после проведения процедуры обновления ОС Windows.

Экспресс-анализ состоит из двух этапов. На первом этапе с помощью специальной утилиты **sprstatus** проверяется функциональный статус основных программных компонентов SPR 4.0. На втором этапе осуществляется пересчет контрольных сумм системных библиотек СКЗИ.

### 6.1. Предназначение и состав утилиты **sprstatus**.

Утилита **sprstatus** предназначена для автоматизированной проверки функционального состояния основных программных компонентов SPR 4.0, проверки параметров работы тестового HTTPS соединения и генерации отчета о результатах проверки.

В состав утилиты входят файл в формате vbscript (**sprstatus-report.vbs**), командный (batch) файл ОС Windows (**sprstatus.cmd**) и базовый шаблон отчета (**sprstatus-report-template.docx**).

Для генерации отчетов утилита **sprstatus** использует возможности редактора Microsoft Word. Поэтому для получения отчета в виде файла в формате PDF необходимо иметь на компьютере установленный редактор. Имя файла шаблона отчета фиксировано: **sprstatus-report-template.docx**. При необходимости можно изменить содержимое файла шаблона и включить в него любой необходимый текст. Обязательным является наличие в файле шаблона строки **%REPORT%**, на место которой будет скопированы результаты работы утилиты **sprstatus**.

### 6.2. Использование утилиты **sprstatus**.

Для проведения тестирования необходимо выполнить следующие действия:

1. Установите обновление ОС Windows, на совместимость с которым будет проводиться тестирование;
2. Проверьте подключение компьютера к сети Интернет;
3. С помощью командного интерпретатора запустите командный файл **sprstatus.cmd**, который находится в поддиректории **sprstatus** установочной папки SPR 4.0.

Пример успешной работы утилиты приведен на Рис. 18. По результатам тестирования в текущей папке будет сгенерирован файл отчета.

**Рис. 18. Пример работы утилиты sprstatus.**

```
C:\Users\RDUDE>.\work\sprstatus-2.0\sprstatus.cmd
Secure Pack Rus status checking utility (ver. 2.0.1).

Date: 8/9/2020
Time: 10:33:20 PM

Computer Information:
    Computer Name: DESKTOP-SJ5Q7M0

5 Version Information:
    Product Name: Windows 10 Pro
    Release ID: 1909
    Version: 10.0
    Build Number: 18363
    Update Build Revision: 959

1] Checking CryptoPro CSP Installation Status:
    Name: КриптоПро CSP
    Version: 5.0.11319
    IdentifyingNumber: {50F91F80-D397-437C-B0C8-62128DE3B55E}
    CHECK RESULT: OK.

2] Checking CryptoPro CSP Service:
    Name: cpcsp
    State: Running
    Status: OK
    CHECK RESULT: OK.

3] Checking CryptoPro CSP Integrity Driver:
    Name: CProCtrl
    State: Running
    Status: OK
    CHECK RESULT: OK.

4] Checking Secure Pack Rus Installation Status:
    Name: Secure Pack Rus 3.0 AK2
    Version: 3.0.4.3
    IdentifyingNumber: {6B72A778-E760-4BEA-9A3F-EF41A1B5057D}
    CHECK RESULT: OK.

5] Checking Secure Pack Rus Policies Management Service:
    Name: sprpolsvc
    State: Running
    Status: OK
    CHECK RESULT: OK.

6] Checking Microsoft Telemetry Client Service:
    Microsoft Universal Telemetry Client Service does not exist as an installed service.
    CHECK RESULT: OK.

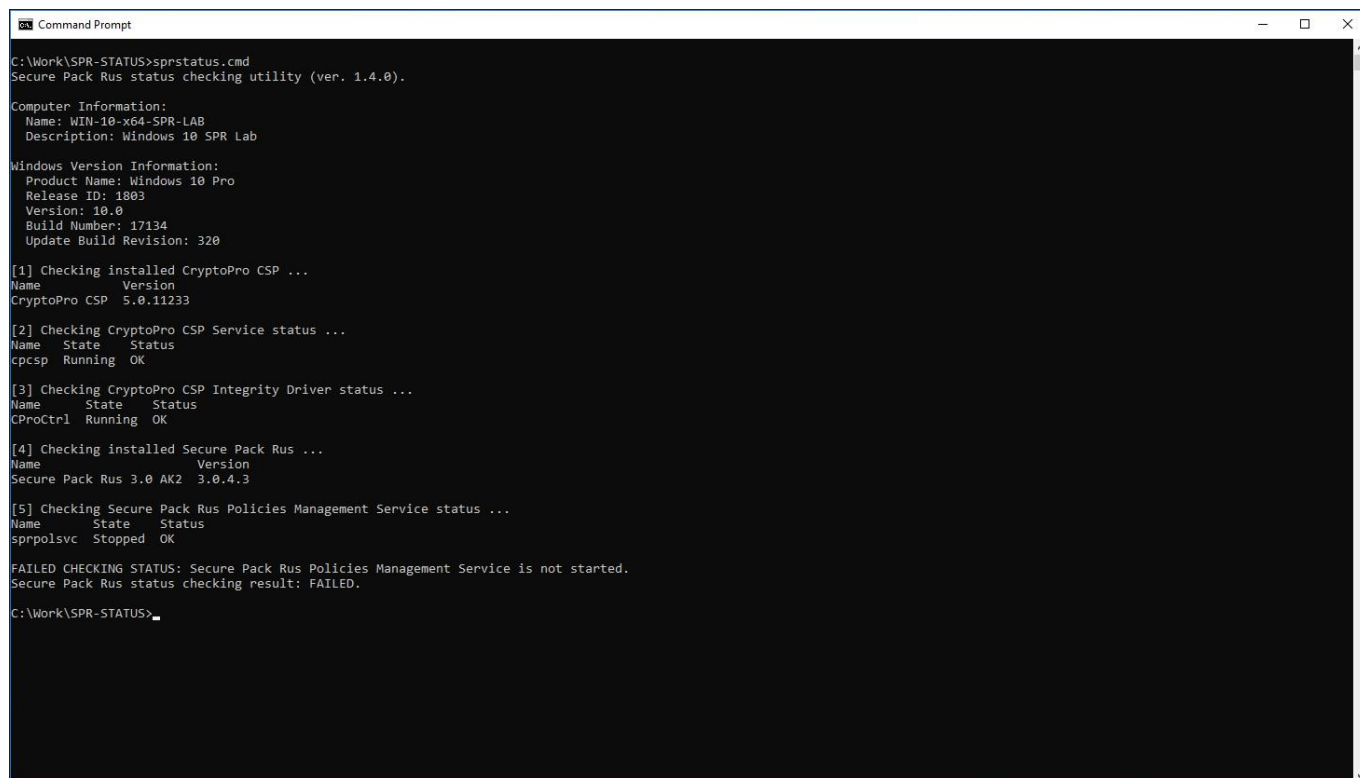
7] Checking CryptoPro HTTPS Connection:
    ssl_protocol: TLSv1.2
    ssl_cipher: GOST2012-GOSTR8912-GOSTR8912 (TLS_GOSTR341112_256_WITH_20147_CNT_IMIT)
    ssl_ciphers: ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES128-SHA:AES128-SHA:AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-SHA384:AES128-SHA384:AES256-SHA:AES128-SHA:0x000a:GOST2012-GOSTR8912-GOSTR8912:GOST2001-GOST89-GOST89
    ssl_client_verify: NONE
    ssl_server_name: tls.cryptopro.ru
    php_random: 1F820DCD18F57CC3
    CHECK RESULT: OK.

SECURE PACK RUS OVERALL STATUS CHECK RESULT: OK.

Report generation:
    The report was successfully generated. Report file name: C:\Users\RDUDE\sprstatus-report-[8-9-2020 10-33-20 PM].pdf
```

Если в результате проверки обнаруживается несоответствие требуемым условиям функционирования какого-либо компонента SPR 4.0, то выдается сообщение об отрицательном результате работы, т.е. о несовместимости установленного обновления и SPR 4.0. Пример такого результата работы приведен на Рис. 19.

Рис. 19. Пример работы утилиты sprstatus.



```
C:\Work\SPR-STATUS>sprstatus.cmd
Secure Pack Rus status checking utility (ver. 1.4.0).

Computer Information:
  Name: WIN-10-x64-SPR-LAB
  Description: Windows 10 SPR Lab

Windows Version Information:
  Product Name: Windows 10 Pro
  Release ID: 1803
  Version: 10.0
  Build Number: 17134
  Update Build Revision: 320

[1] Checking installed CryptoPro CSP ...
Name      Version
CryptoPro CSP  5.0.11233

[2] Checking CryptoPro CSP Service status ...
Name      State      Status
cpcsp     Running   OK

[3] Checking CryptoPro CSP Integrity Driver status ...
Name      State      Status
CProCtrl  Running   OK

[4] Checking installed Secure Pack Rus ...
Name      Version
Secure Pack Rus 3.0 AK2  3.0.4.3

[5] Checking Secure Pack Rus Policies Management Service status ...
Name      State      Status
sprpolsvc Stopped   OK

FAILED CHECKING STATUS: Secure Pack Rus Policies Management Service is not started.
Secure Pack Rus status checking result: FAILED.

C:\Work\SPR-STATUS>
```

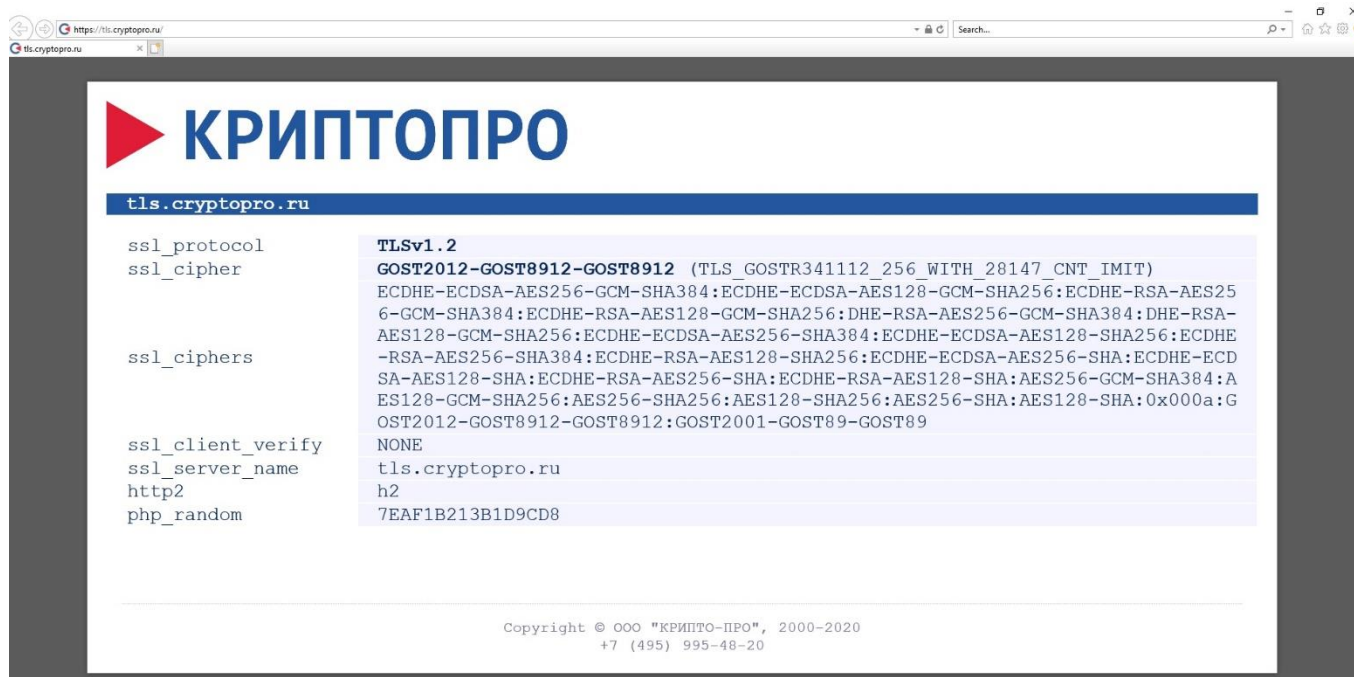
### 6.3. Проверка работы КриптоПро TLS

Утилита **sprstatus** проводит тестирование работы CryptoPro TLS в автоматическом режиме. В случае возникновения необходимости ручной проверки работы криптографической подсистемы СКЗИ КриптоПро CSP необходимо:

1. Подключить исследуемую АРМ к сети Интернет.
2. Воспользовавшись штатным браузером ОС Windows Internet Explorer, войти на специальную страницу сайта компании КриптоПро (<https://tls.cryptopro.ru>).
3. Изучить содержимое отчета о статусе TLS-соединения, установленного между исследуемым АРМ и сайтом КриптоПро (Рис. 20 и Рис. 21).

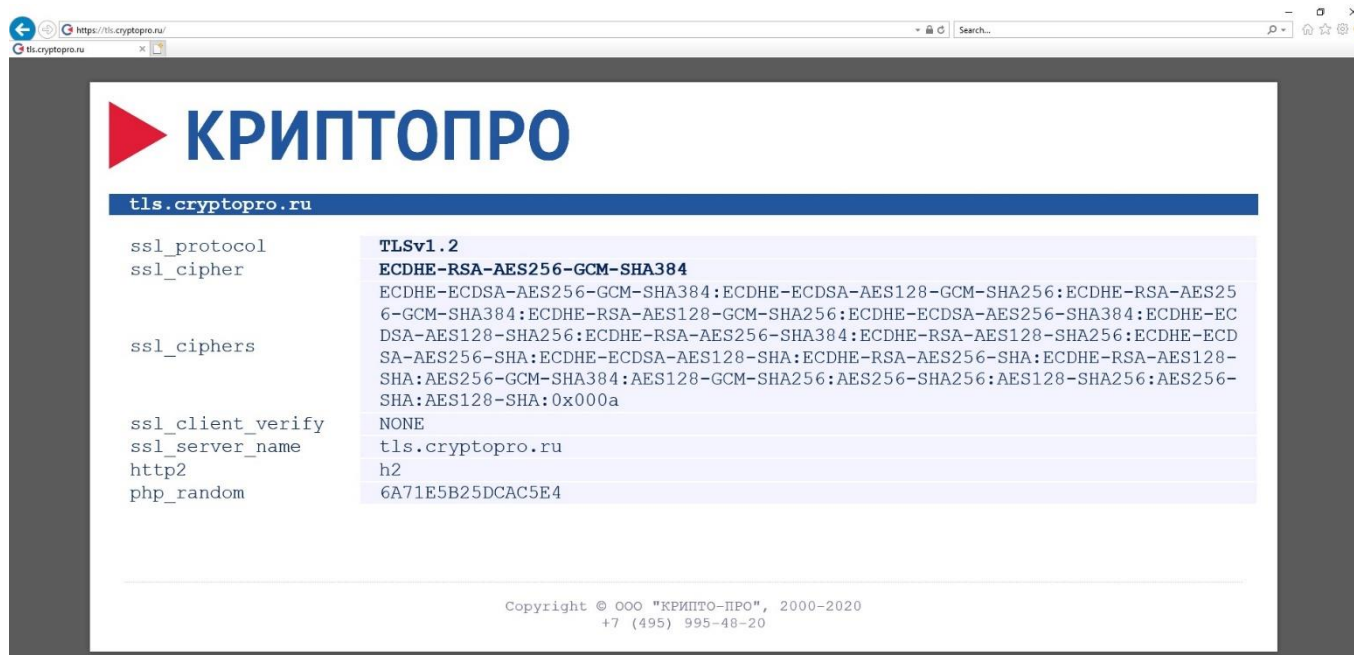
В случае успешного установления защищенного TLS-соединения, использующего сертифицированные криптографические алгоритмы, реализованные в СКЗИ КриптоПро CSP, TLS Cipher Suite (поле `ssl_cipher`) должен иметь значение GOST2012-GOST8912-GOST8912 (TLS\_GOSTR34112\_256\_WITH\_28147\_CNT\_IMIT) (Рис. 20).

Рис. 20. Пример содержимого страницы [tls.cryptopro.ru](https://tls.cryptopro.ru/).



Если установленное TLS-соединение использует другие наборы криптографических алгоритмов (Рис. 21), то это означает некорректное функционирование КриптоПро CSP и общее состояние SPR 4.0 в целом не соответствует требуемому.

Рис. 21. Пример содержимого страницы [tls.cryptopro.ru](https://tls.cryptopro.ru/).



#### **6.4. Пересчет контрольных сумм системных библиотек ОС.**

КриптоПро CSP контролирует целостность некоторых системных библиотек ОС Windows, которые могут быть заменены при установке обновления. Администратору необходимо пересчитать контрольные суммы после установки целевого обновления.

Пересчет контрольных сумм можно осуществить через Панель Управления. На



Рис. 22 показана вкладка «Дополнительно» диалогового окна КриптоПро CSP. Для пересчета контрольных сумм необходимо воспользоваться кнопкой «Пересчитать хеши». Перед пересчетом контрольных сумм администратору необходимо проверить, что повреждены только контрольные суммы следующих системных библиотек (

Рис. 22):

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

Проверку и пересчет контрольных сумм также возможно осуществить с использованием утилиты командной строки **cpverify**.

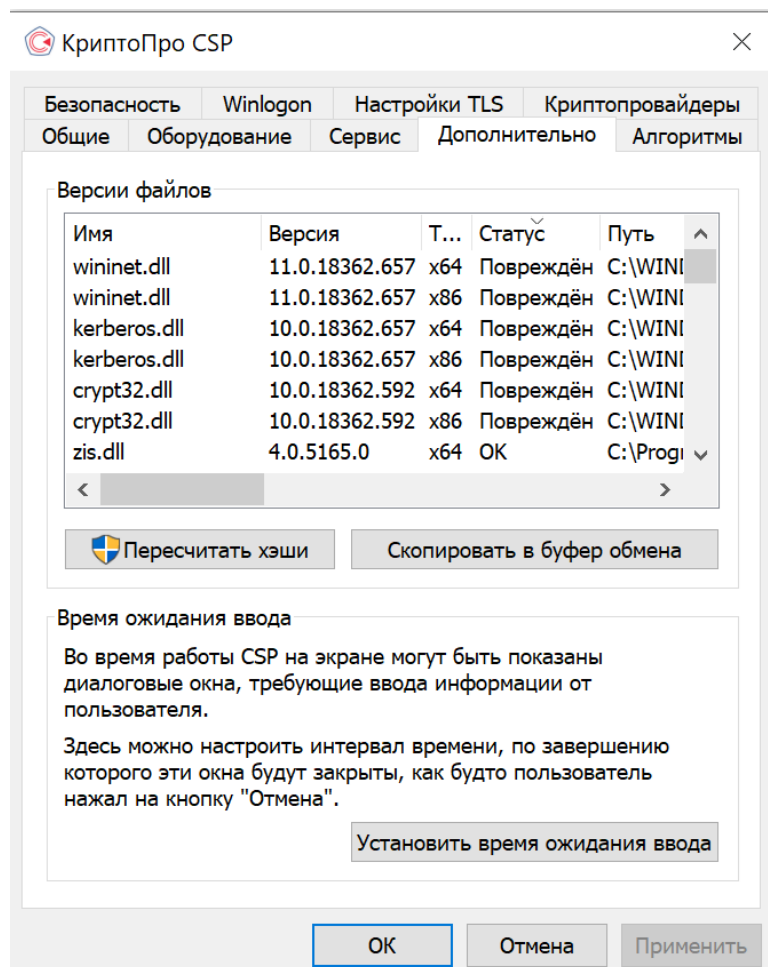
Для проверки целостности контролируемых файлов можно воспользоваться командой:

**start /b /wait cpverify -rv**

Для пересчета контрольных сумм после обновления командой:

**start /b /wait cpverify -rm**

Рис. 22. Диалоговое окно управления пересчетом контрольных сумм системных файлов



## Список литературы

1. Компания "КРИПТО-ПРО". Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows. *Средство криптографической защиты информации «КриптоПро CSP» версия 5.0 R2 2-Base*. ЖТЯИ.00102-02 91 02.
2. —. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows. *Средство криптографической защиты информации «КриптоПро CSP» версия 5.0 R2 3-Base*. ЖТЯИ.00103-02 91 02.
3. —. Формуляр. *Средство защиты информации «КриптоПро SPR» версия 4.0*. ЖТЯИ.00112-01 30 01.
4. —. Описание применения. *Средство защиты информации «КриптоПро SPR» версия 4.0*. ЖТЯИ.00112-01 31 01.
5. —. Руководство администратора безопасности. *Средство защиты информации «КриптоПро SPR» версия 4.0*. ЖТЯИ.00112-01 90 01.
6. —. Руководство администратора безопасности. Установка. *Средство защиты информации «КриптоПро SPR» версия 4.0*. ЖТЯИ.00112-01 90 02.
7. —. Руководство администратора безопасности. Аутентификация. *Средство защиты информации «КриптоПро SPR» версия 4.0*. ЖТЯИ.00112-01 90 03.
8. —. Руководство администратора безопасности. Политики управления приложениями. *Средство защиты информации «КриптоПро SPR» версия 4.0*. ЖТЯИ.00112-01 90 04.
9. —. Руководство администратора безопасности. Аудит. *Средство защиты информации «КриптоПро SPR» версия 4.0*. ЖТЯИ.00112-01 90 05.
10. —. Руководство пользователя. *Средство защиты информации «КриптоПро SPR» версия 4.0*. ЖТЯИ.00112-01 34 01.