

УТВЕРЖДЕН
РБ.ЮСКИ.12004-03 34 01-ЛУ

ПРОГРАММНОЕ СРЕДСТВО
КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«КРИПТОПРОВАЙДЕР Avest CSP BEL»

AvCSPBEL

Руководство оператора

РБ.ЮСКИ.12004-03 34 01

Листов 64

Инв.№ подл.	Подп. и дата	Взам. инв.№	Инв.№ дубл	Подп. и дата

РБ.ЮСКИ.12004-03 34 01

АННОТАЦИЯ

Данный документ содержит руководство оператора программного продукта «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BEL» AvCSPBEL» (РБ.ЮСКИ.12004-03) (далее – криптопровайдер AvCSPBEL, ПС AvCSPBEL).

В документе содержится информация по назначению и условиям выполнения программного продукта. Описана последовательность действий оператора при установке, выполнении и удалении программного продукта, приведены тексты сообщений, формируемых криптопровайдером AvCSPBEL, с пояснением их содержания и описанием рекомендуемых действий оператора. Приведены рекомендуемые меры безопасности, выполнение которых в процессе эксплуатации криптопровайдера AvCSPBEL повышает уровень защиты информационных активов оператора и информационной системы.

Изготовителем криптопровайдера AvCSPBEL является белорусское предприятие «Закрытое акционерное общество «АВЕСТ» (ЗАО «АВЕСТ»).

Адрес предприятия: 220083, Республика Беларусь, г. Минск, пр-т Газеты Правда, д. 5, пом. 3Н, каб. 7.

Тел.: +375(17) 257-99-74, 318-92-34, факс: +375(17) 303-91-49.

Интернет-страница: <https://www.avest.by>.

Электронная почта: welcome@avest.by.

При обнаружении неисправности при эксплуатации криптопровайдера AvCSPBEL необходимо прекратить эксплуатацию криптопровайдера AvCSPBEL и связаться с разработчиком по вышеуказанным телефонам или электронной почте.

Гарантийный срок, обязательства изготовителя, дата изготовления криптопровайдера AvCSPBEL указываются в лицензионном договоре при поставке криптопровайдера AvCSPBEL в соответствии с законодательством Республики Беларусь.

СОДЕРЖАНИЕ

1. Назначение программы	4
2. Условия выполнения программы.....	8
3. Установка и выполнение программы	11
3.1. Установка криптопровайдера AvCSPBEL.....	11
3.2. Установка криптопровайдера AvCSPBEL в неинтерактивном режиме (с использованием командной строки).....	20
3.3. Работа с окном управления криптопровайдером AvCSPBEL	20
3.3.1. Вкладка «Носители».....	21
3.3.2. Вкладка «Версия»	33
3.4. Регистрация НКИ	33
3.5. Контроль компонентов криптопровайдера AvCSPBEL.....	38
3.6. Сообщения оператору.....	43
4. Удаление программы.....	50
5. Меры безопасности.....	55
5.1. Меры безопасности при поставке	55
5.2. Меры безопасности при установке и эксплуатации.....	56
6. Перечень сокращений	61
7. Ссылки	62

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

В операционных системах (ОС) Windows компании Microsoft возможность выполнения приложениями верхнего уровня криптографических функций обеспечивается специальными программными (программно-аппаратными) модулями – т.н. «поставщиками криптографических служб» – Cryptographic Service Provider (CSP) или «криптопровайдерами».

Помимо криптопровайдеров компании Microsoft, установленных в ОС Windows по умолчанию, имеется возможность интегрировать в данную ОС криптопровайдеры сторонних разработчиков, в частности, с целью использования криптографических алгоритмов согласно ТНПА Республики Беларусь.

Для обеспечения универсальности доступа приложений к криптографическим сервисам и независимости вызова криптографических функций от реализации криптографических алгоритмов и их типов, ОС Windows поддерживает открытые стандартизированные криптографические интерфейсы: Microsoft Cryptographic Application Programming Interface (CryptoAPI) и SSPI-интерфейс.

Вышеуказанные интерфейсы используются такими стандартными приложениями Microsoft как Internet Explorer, Outlook Express, Outlook, Internet Information Services и др., а также поддерживаются в Microsoft Edge, имеющем возможность работать в режиме Internet Explorer.

Криптопровайдер, предоставляющий программному обеспечению (ПО) прикладного уровня криптографические сервисы по интерфейсам CryptoAPI, обеспечивает выполнение следующих основных классов базовых функций:

- функции управления криптопровайдерами и контекстами криптопровайдеров;
- функции создания, конфигурирования, уничтожения криптографических ключей, а также обмена ключами;
- функции, реализующие операции зашифрования, расшифрования и вычисления имитовставки с использованием симметричных ключей;
- функции, используемые для вычисления значений хэш-функций;

– функции, используемые для выработки и проверки электронной цифровой подписи (ЭЦП).

Кроме этого, криптопровайдер с поддержкой вышеуказанных криптографических интерфейсов предоставляет прикладному уровню возможность работы с функциями, реализующими «инфраструктуру открытых ключей» (ИОК) или Public Key Infrastructure (PKI): управление и работа с сертификатами формата X.509, списками и хранилищами сертификатов, работа с открытыми ключами и их идентификаторами, работа с криптографическими сообщениями формата PKCS#7, работа с функциями шифрования, ЭЦП и др.

Реализованные в криптопровайдере AvCSPBEL криптографические алгоритмы доступны прикладному ПО по интерфейсам CryptoAPI и SSPI-интерфейсу для поставщика поддержки безопасности (SSP) Schannel (для построения защищенных TLS-соединений) в соответствии с их спецификациями компании Microsoft. При этом используются криптографические алгоритмы и протоколы в соответствии с ТНПА Республики Беларусь в области криптографической защиты информации:

- 1) ГОСТ 28147-89 «Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
- 2) СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования»;
- 3) СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи»;
- 4) СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности»;
- 5) СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»;
- 6) СТБ 34.101.47-2012 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»;

7) СТБ 34.101.50-2019 «Информационные технологии и безопасность. Правила регистрации объектов информационных технологий»;

8) СТБ 34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)».

Криптопровайдер AvCSPBEL предоставляет прикладному программному обеспечению следующий набор механизмов и процедур защиты активов информационных систем:

- генерация личных и открытых ключей ЭЦП и шифрования и управление данными ключами в течение всего их жизненного цикла;
- генерация псевдослучайных чисел;
- симметричное шифрование данных;
- вычисление значения хэш-функции от данных;
- выработка и проверка ЭЦП;
- выработка общего секретного ключа для процедур аутентификации и шифрования данных по асимметричной схеме;
- хранение криптографических ключей на отчуждаемых носителях ключевой информации (НКИ) в зашифрованном виде.

При разворачивании ИОК с использованием криптопровайдера AvCSPBEL обеспечивается:

- поддержка сертификатов открытых ключей (СОК) и списков отозванных сертификатов (СОС) согласно СТБ 34.101.19 с учетом СТБ 34.101.78;
- поддержка запросов на получение СОК согласно СТБ 34.101.17 с учетом СТБ 34.101.78;
- поддержка синтаксиса криптографических сообщений согласно СТБ 34.101.23 с учетом СТБ 34.101.78;
- реализация онлайн-протокола проверки статуса сертификата (OCSP) согласно СТБ 34.101.26 с учетом СТБ 34.101.78;

РБ.ЮСКИ.12004-03 34 01

- поддержка атрибутивных сертификатов согласно СТБ 34.101.67;
- защита Интернет-соединений между Web-сервером и клиентом по протоколу Transport Layer Security (TLS) согласно СТБ 34.101.65;
- поддержка стандарта S/MIME (Secure/Multipurpose Internet Mail Extensions) для криптографической защиты электронной почты.

При установке криптопровайдера AvCSPBEL в системном реестре ОС Windows регистрируется криптопровайдер типа 423.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

Криптопровайдер AvCSPBEL предназначен для работы на компьютере общего назначения, функционирующем под управлением одной из следующих ОС:

- Windows 11 (x64);
- Windows 2016 Server (x64);
- Windows 2019 Server (x64);
- Windows 2022 Server (x64);
- Windows 2025 Server (x64).

Примечание. Допускается работа криптопровайдера AvCSPBEL в среде следующих ОС Windows, которые сняты с поддержки компании Microsoft:

- Windows 7 (x32, x64);
- Windows 8 (x32, x64);
- Windows 8.1 (x32, x64);
- Windows 10 (x32, x64);
- Windows 2008 R2 Server (x64).
- Windows 2012 Server (x64);
- Windows 2012 R2 Server (x64).

В случае использования вышеуказанных ОС, снятых с поддержки компании Microsoft, устойчивая работа криптопровайдера AvCSPBEL не гарантируется.

ВНИМАНИЕ! На время установки антивирусное программное обеспечение (в том числе встроенное в ОС, например, Windows Defender) рекомендуется отключать, так как некоторые антивирусные программы могут препятствовать записи значений в реестр Windows и установке компонентов программ в системные папки. Если отключение антивирусного программного обеспечения не приводит к желаемому результату, то нужно добавить инсталляционный файл в исключения антивируса.

Для использования криптопровайдера AvCSPBEL пользователь должен иметь

права «Administrator (Администратор)»).

Криптопровайдер AvCSPBEL предназначен для работы на компьютере, имеющем следующие минимальные технические характеристики:

- процессор x86 (x64) с тактовой частотой – не менее 2,5 ГГц;
- объем оперативного запоминающего устройства (ОЗУ) – не менее 4 Гбайт;
- жесткий диск (накопитель информации), содержащий не менее 8 Гбайт свободного пространства для стандартной установки ОС;
- монитор с разрешением 1024x768 или более высокого разрешения;
- манипулятор «мышь» или совместимое указывающее устройство, клавиатура;
- свободный USB-порт при необходимости подключения USB-токена.

В случае использования операционной системы с установленным языком, отличным от русского, для корректного отображения символов в криптопровайдере AvCSPBEL нужно установить в настройках ОС язык для программ, не поддерживающих Юникод – Русский.

В качестве отчуждаемого НКИ криптопровайдер AvCSPBEL поддерживает «Устройство программно-аппаратное хранения информации «AvPass» (далее – НКИ AvPass).

НКИ AvPass предназначен для локального использования пользователем совместно с программным продуктом криптопровайдером AvCSPBEL, входящим в состав программного продукта «Программный комплекс «Комплект Абонента АВЕСТ» (AvUCK)» (РБ.ЮСКИ.13001-07) (далее – ПК AvUCK).

Использование НКИ AvPass в удалённом сеансе с использованием специализированного ПО для проброса USB-устройств является нештатным использованием. В данном случае не может быть гарантирована надежность работы криптопровайдера AvCSPBEL с устройствами, а также конфиденциальность личных ключей.

Используемый НКИ AvPass должен быть зарегистрирован в ЗАО «АВЕСТ»

согласно процедуре, описанной в данном документе (см. п. 3.4. Регистрация НКИ).

Внимание! Во избежание случайной непреднамеренной потери данных пользователя на НКИ (личных ключей, СОК) перед перезагрузкой компьютера, нештатным завершением криптографического ПО, переустановкой (удалением) криптографического ПО (криптопровайдера, персонального менеджера сертификатов) нужно извлечь НКИ из USB-порта компьютера.

В случае проведения вышеуказанных манипуляций с ПО без извлечения НКИ рекомендуется после их завершения средствами криптопровайдера AvCSPBEL убедиться в работоспособности НКИ и наличии данных пользователя на НКИ. В случае потери данных или выхода из строя НКИ нужно обратиться в техподдержку организации, в которой приобреталось ПО и НКИ.

3. УСТАНОВКА И ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Установка криптопровайдера AvCSPBEL

Структура папок установки криптопровайдера AvCSPBEL зависит от разрядности операционной системы:

- в 32-разрядной ОС устанавливается один 32-разрядный криптопровайдер AvCSPBEL в папку %ProgramFiles%\Avest\Avest CSP Bel;
- в 64-разрядной ОС устанавливаются два криптопровайдера AvCSPBEL:
 - 32-разрядный – в папку %ProgramFiles(x86)%\Avest\Avest CSP Bel;
 - 64-разрядный – в папку %ProgramFiles%\Avest\Avest CSP Bel.

Кроме того, при установке часть компонентов криптопровайдера AvCSPBEL размещается в системных папках общего доступа, выбор которых также зависит от разрядности ОС:

- в 32-разрядной ОС: %CommonProgramFiles%\Avest;
- в 64-разрядной ОС:
 - для 32-битных компонентов: %CommonProgramFiles(x86)%\Avest;
 - для 64-битных компонентов: %CommonProgramFiles%\Avest.

Все перечисленные пути установки и системные папки общего доступа жёстко заданы и не подлежат изменению.

Действия по установке криптопровайдера AvCSPBEL:

1) Запустить установочный файл «setupAvCSPBelX.X.X.XXX.exe». Если появится окно контроля учетных записей с запросом разрешения программе/приложению вносить изменения на компьютере/устройстве, нажать кнопку «Да».

2) В первом окне мастера установки содержится краткое описание устанавливаемого продукта. Нажать кнопку «Далее>» для начала установки или «Отмена» – чтобы выйти из программы установки (см. Рисунок 1 – Заставка мастера установки Avest CSP BEL).

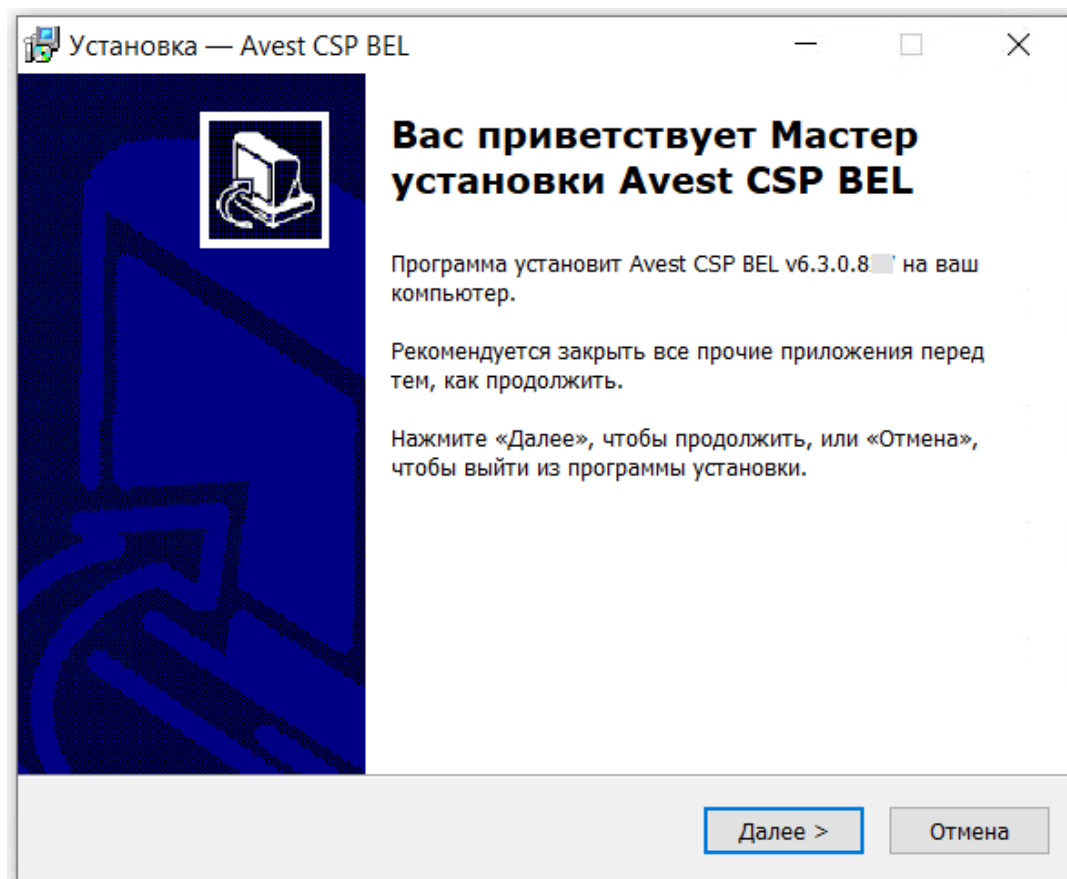


Рисунок 1 – Заставка мастера установки Avest CSP BEL

3) После нажатия на кнопку «Далее>» откроется окно с лицензионным соглашением. Нужно внимательно ознакомиться с его условиями (см. Рисунок 2– Лицензионное соглашение).

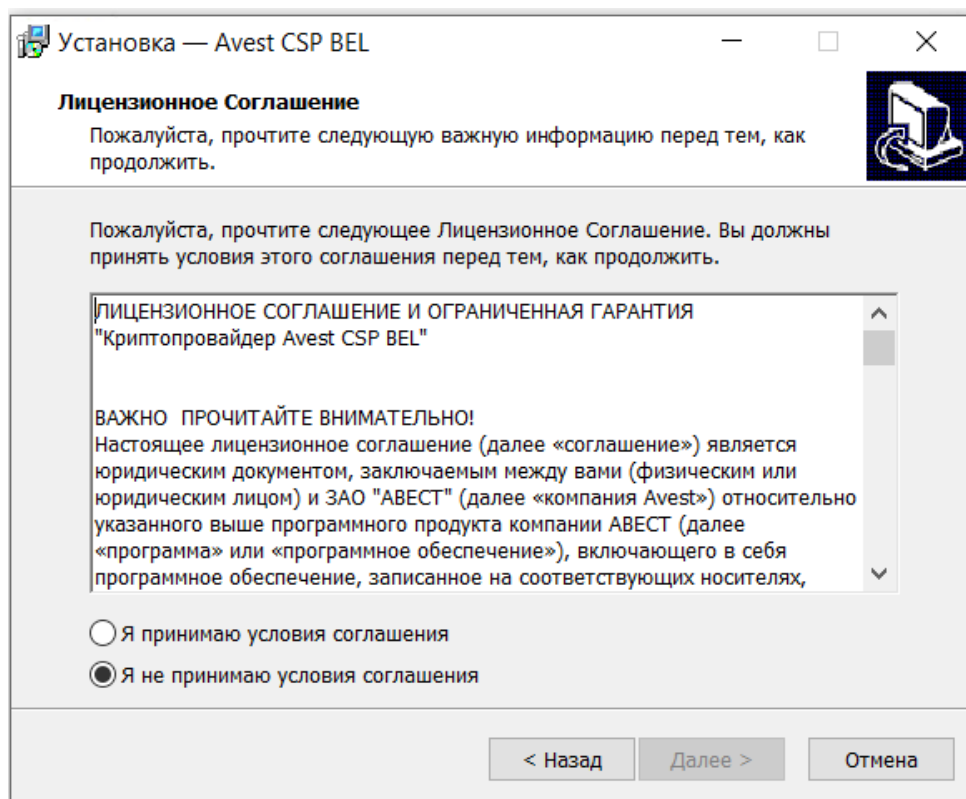


Рисунок 2– Лицензионное соглашение

Для продолжения установки криптопровайдера AvCSPBEL необходимо установить переключатель на пункт «Я принимаю условия соглашения» и нажать кнопку «Далее>». Для возврата к предыдущему окну надо нажать кнопку «<Назад». Если условия лицензионного соглашения не принимаются, то надо нажать кнопку «Отмена» для выхода из программы установки.

4) Следующим шагом установки является выбор папки в меню «Пуск», в которой будут созданы ярлыки быстрого запуска программы.

По умолчанию будет создана папка «Авест» (см. Рисунок 3 – Выбор папки для создания ярлыков в меню «Пуск»).

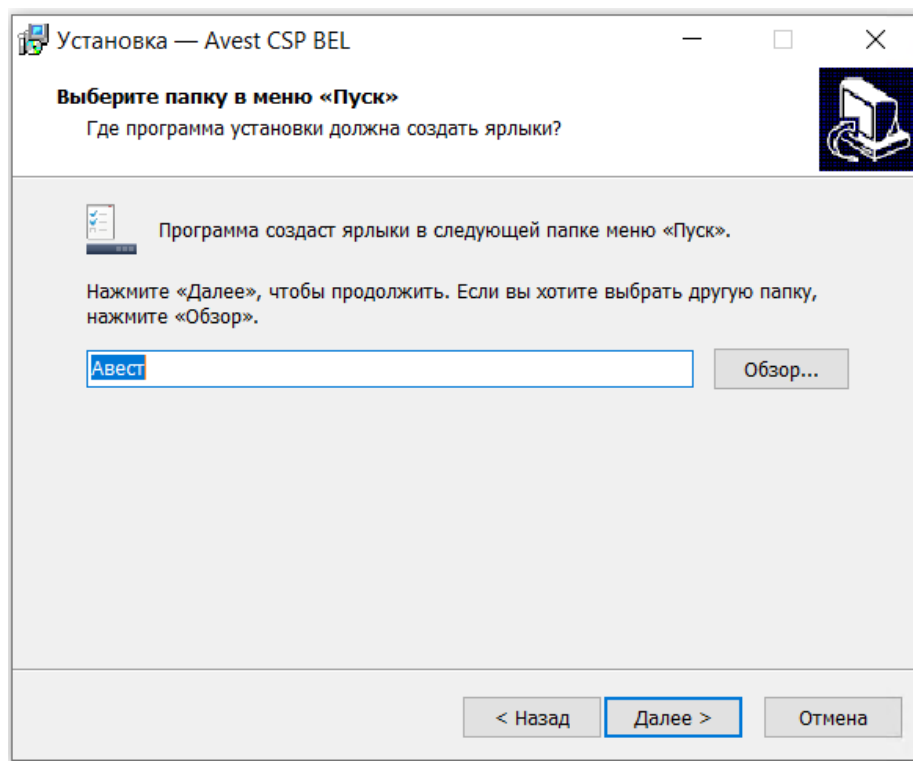


Рисунок 3 – Выбор папки для создания ярлыков в меню «Пуск»

Название папки можно изменить: указать вручную или выбрать при помощи кнопки «Обзор».

После выбора папки чтобы продолжить установку необходимо нажать кнопку «Далее>». Для возврата к предыдущему окну нажать кнопку «<Назад». Если нужно выйти из программы, нажать «Отмена».

5) После нажатия на кнопку «Далее>» мастер установки Avest CSP BEL отобразит окно готовности к установке (см. Рисунок 4 – Установка криптопровайдера AvCSPBEL на компьютер). Чтобы начать установку, необходимо нажать кнопку «Установить». Для возврата к предыдущему окну следует нажать кнопку «<Назад», для выхода из программы установки – нажать кнопку «Отмена».

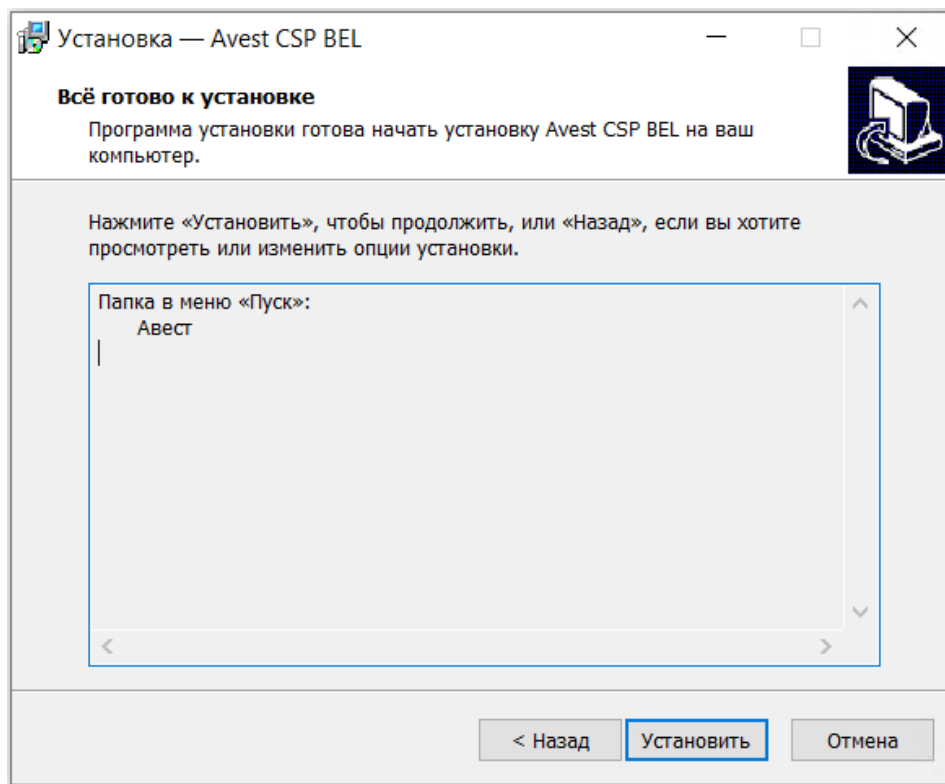


Рисунок 4 – Установка криптопровайдера AvCSPBEL на компьютер

После нажатия кнопки «Установить» будет произведена распаковка, копирование файлов и регистрация библиотек на компьютере.

Примечание. Если в процессе установки будут открыты приложения, которые используют файлы криптопровайдера AvCSPBEL, то программа при подготовке к установке предложит автоматически закрыть эти приложения (см. Рисунок 5 – Подготовка к установке). Чтобы выполнить установку криптопровайдера AvCSPBEL корректно, необходимо установить переключатель на пункт «Автоматически закрыть эти приложения» и нажать кнопку «Далее>». Для возврата к предыдущему окну следует нажать кнопку «<Назад», для выхода из программы установки – нажать кнопку «Отмена».

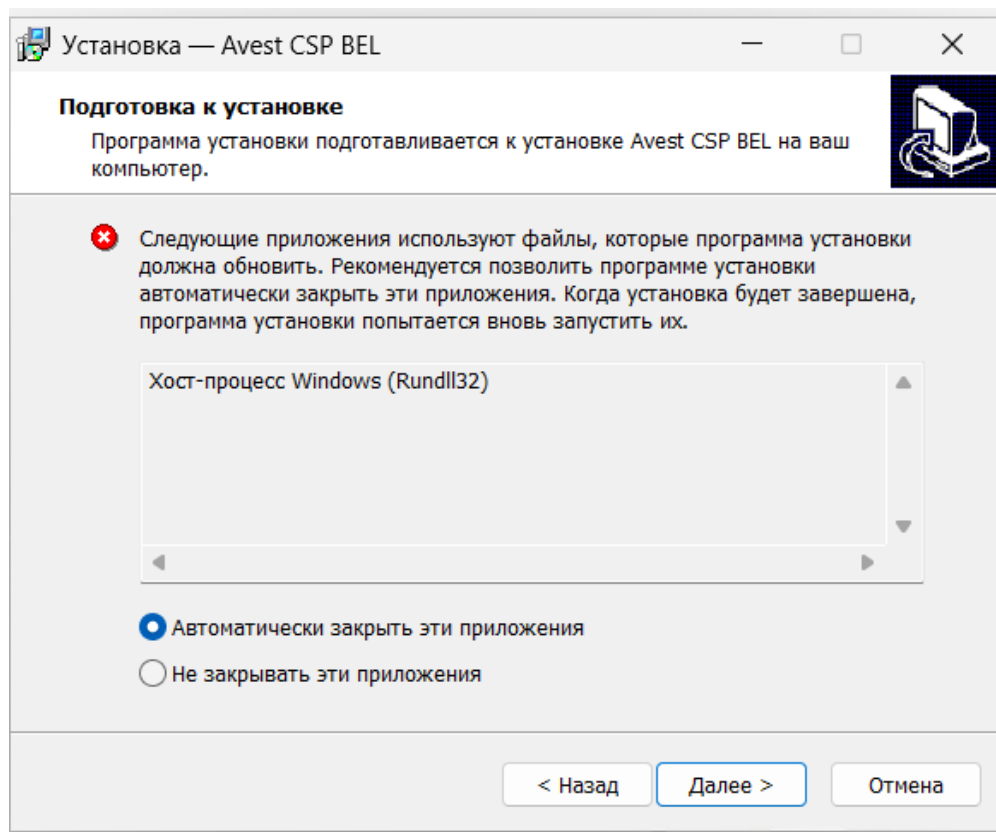


Рисунок 5 – Подготовка к установке

6) Если установка производится на компьютер, на котором криптопровайдер ранее не был установлен, то при выполнении установки появится окно сбора случайных данных (см. Рисунок 6 – Сбор случайных данных). Для регистрации криптопровайдера AvCSPBEL в системе нужно подвигать мышью в пределах этого окна, пока индикатор прогресса полностью не заполнится.

Примечание. При повторной инсталляции криптопровайдера AvCSPBEL данное окно появляться не будет.

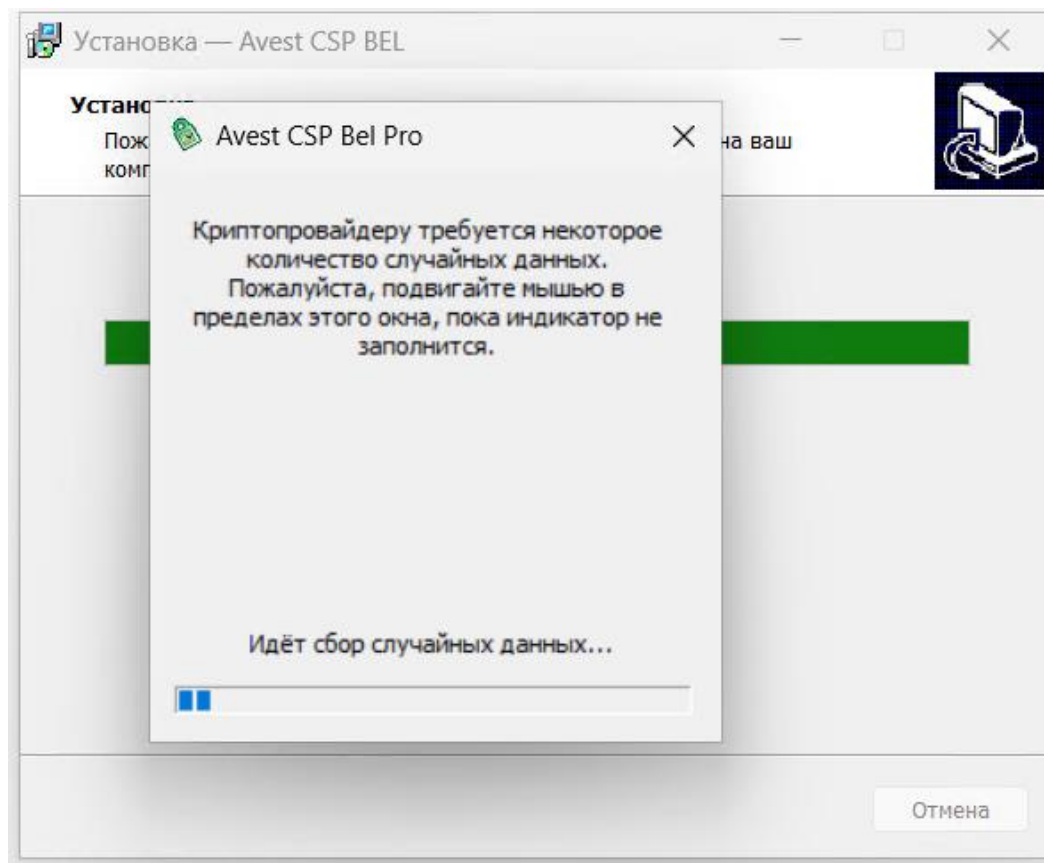


Рисунок 6 – Сбор случайных данных

7) После завершения установки дождаться появления финального окна мастера установки Avest CSP BEL (см. Рисунок 7 – Завершение установки криптопровайдера AvCSPBEL), в котором нужно нажать кнопку «Завершить».

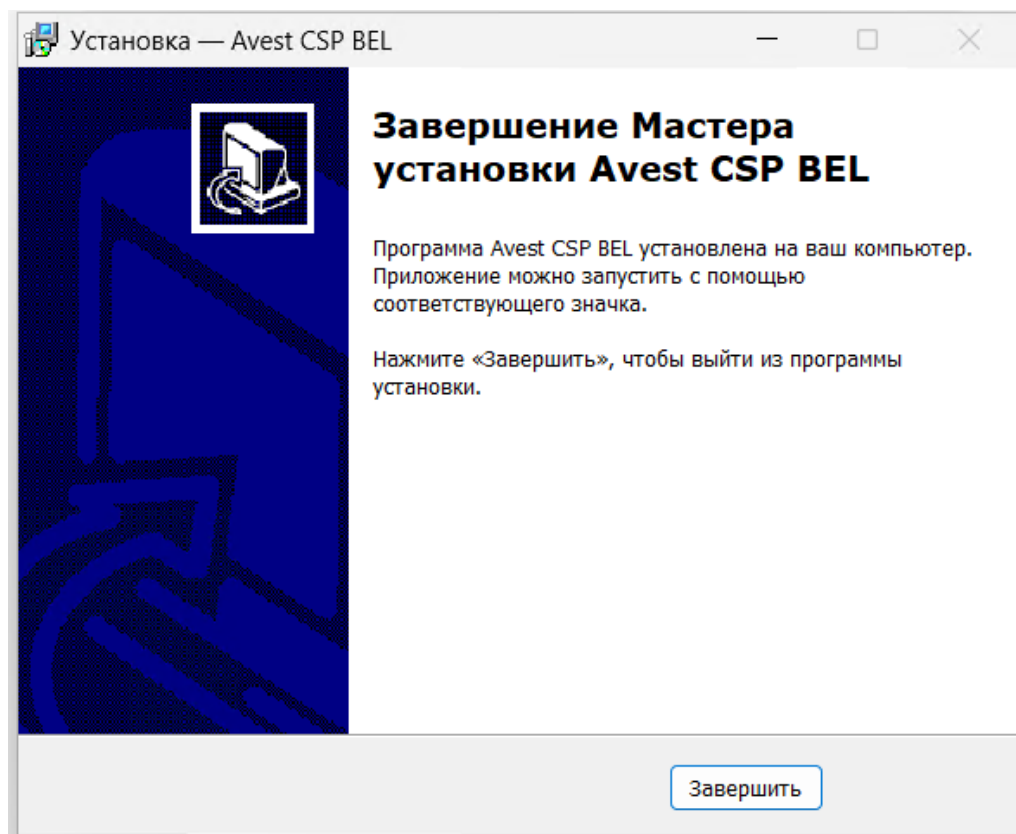


Рисунок 7 – Завершение установки криптопровайдера AvCSPBEL

При этом, если в окне отображается предложение о перезагрузке компьютера (см. Рисунок 8 – Требуется перезагрузка), необходимо установить переключатель в положение «Да, я произведу перезагрузку сейчас». В этом случае перезагрузка будет выполнена автоматически.

Если предложение о перезагрузке отсутствует, перезагрузку компьютера необходимо выполнить вручную.

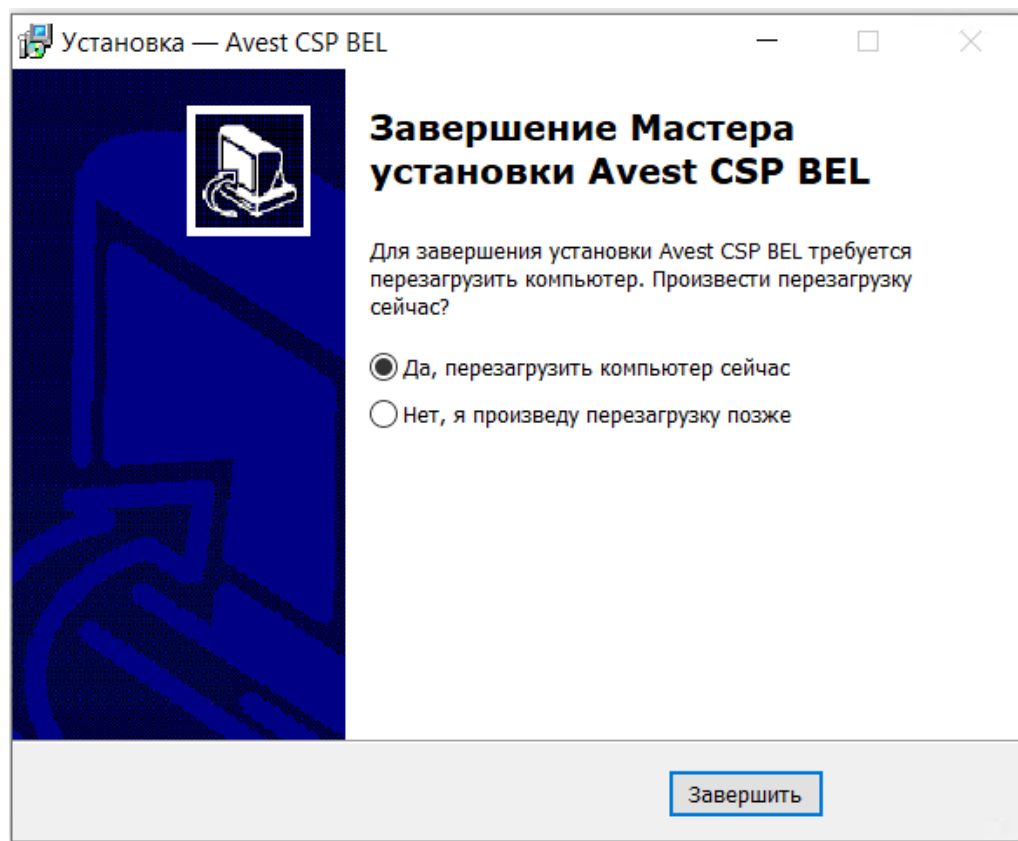


Рисунок 8 – Требуется перезагрузка

После установки криптопровайдера ярлыки размещаются в меню:

«Пуск»⇒»Программы»⇒«Авест».

Примечание. «Авест» – название папки по умолчанию. Если на этапе выбора папки в меню «Пуск» оно не было изменено, ярлыки криптопровайдера AvCSPBEL будут созданы именно в этой папке.

Состав ярлыков криптопровайдера AvCSPBEL в папке «Авест» зависит от разрядности операционной системы:

- в 32-разрядной ОС создаются ярлыки «Avest CSP BEL» и/или «Avest CSP BEL (admin)»;
- в 64-разрядной ОС создаются ярлыки как для 32-, так и для 64-разрядной версии программы:
 - ярлыки 32-разрядной программы: «Avest CSP BEL» и/или «Avest CSP BEL (admin)»;

– ярлыки 64-разрядной программы: «Avest CSP BEL x64» и/или «Avest CSP BEL x64 (admin)».

3.2. Установка криптопровайдера AvCSPBEL в неинтерактивном режиме (с использованием командной строки)

Программа установки криптопровайдера AvCSPBEL поддерживает использование параметров командной строки, что позволяет указывать файл-источник случайных данных и выполнять установку в неинтерактивном режиме без отображения окон мастера установки.

Для того чтобы начать процесс установки криптопровайдера AvCSPBEL неинтерактивно, нужно запустить установочный файл криптопровайдера «setupAvCSPBelX.X.X.XXX.exe в командной строке со следующими параметрами:

- /verysilent – установить криптопровайдер неинтерактивно, т.е. без отображения оконных интерфейсов мастера установки Avest CSP BEL;
- /entropy="любой файл более 64 байт" – использование указанного файла в качестве источника случайных данных. В случае указания данного параметра окно для сбора случайных данных не появится (см. Рисунок 6 – Сбор случайных данных).

Пример команды:

```
setupAvCSPBel6.3.0.835.exe /verysilent /entropy=entropy_file_sample
```

3.3. Работа с окном управления криптопровайдером AvCSPBEL

Окно управления криптопровайдером AvCSPBEL запускается через ярлык программы в меню «Пуск»⇒»Программы», в папке, указанной на соответствующем шаге установки (по умолчанию – «Авест»). Описание шага выбора папки в меню «Пуск», а также перечень создаваемых ярлыков приведены в п. 3.1. Установка криптопровайдера AvCSPBEL.

Окно управления состоит из 2 вкладок:

- Вкладка «Носители»;

- Вкладка «Версия».

3.3.1. Вкладка «Носители»

Вкладка «Носители» предназначена для отображения информации обо всех подключенных к компьютеру НКИ AvPass.

На вкладке «Носители» (см. Рисунок 9 – Вкладка «Носители») представлены следующие элементы:

- поле «Используемые носители» – отображает серийные номера всех подключенных НКИ AvPass;
- кнопка «Самотестирование криптопровайдера» – осуществляет контроль целостности и тестирование работоспособности компонентов криптопровайдера AvCSPBEL;
- поле «Контейнеры на выбранном носителе» – отображает контейнеры с личными ключами на выбранном НКИ AvPass.

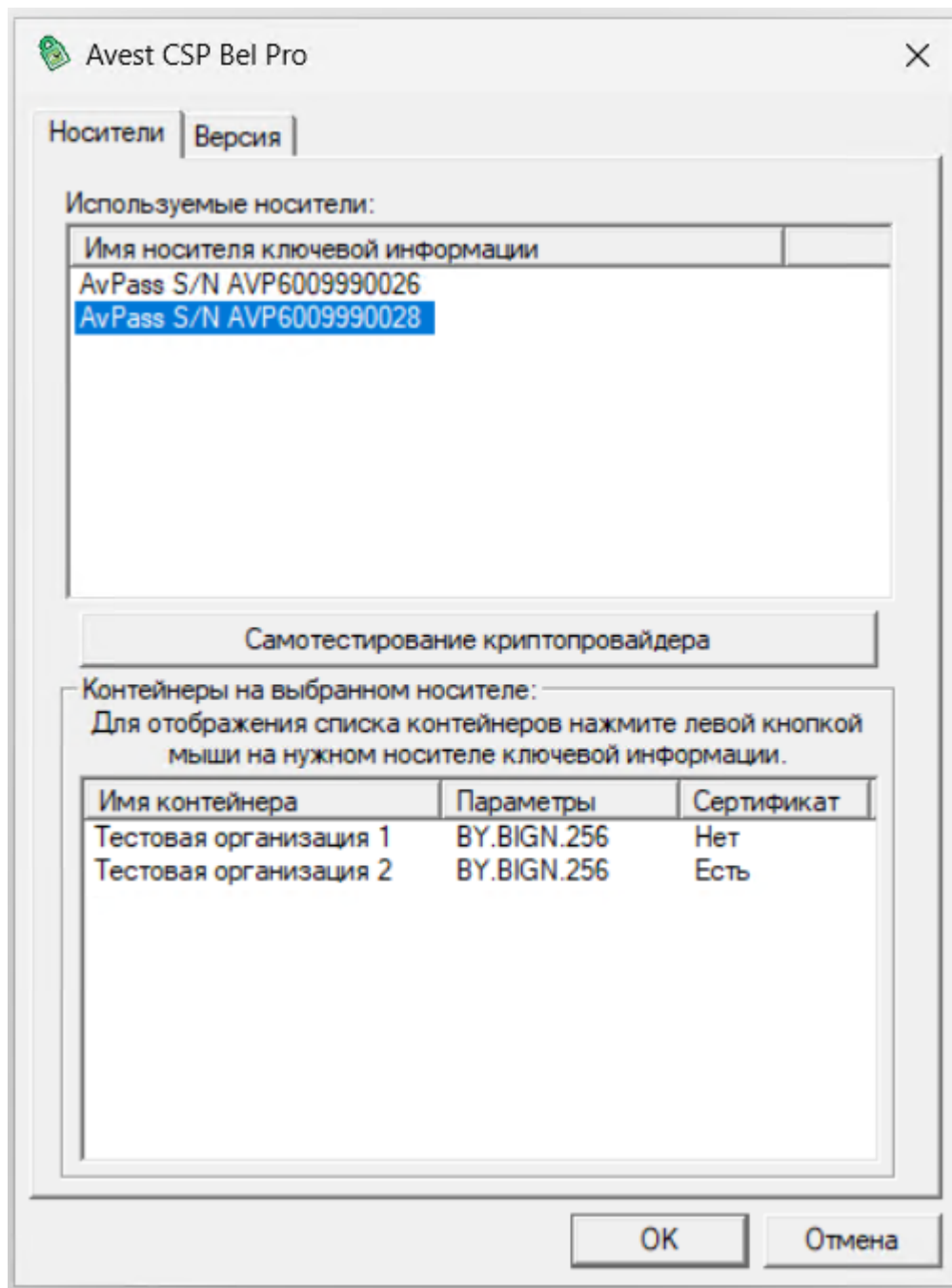


Рисунок 9 – Вкладка «Носители»

На вкладке «Носители» доступны следующие операции:

- Просмотр контейнеров с личными ключами на НКИ;
- Смена пароля для доступа к НКИ;
- Просмотр информации о регистрации НКИ. Регистрация НКИ;
- Удаление контейнера с личным ключом;

- Переименование контейнера с личным ключом;
- Просмотр сертификата в контейнере с личным ключом;
- Управление режимом контроля НКИ;
- Контроль целостности и тестирование работоспособности компонентов криптопровайдера AvCSPBEL.

Ниже приведено описание этих операций и последовательность действий оператора для их выполнения.

Просмотр контейнеров с личными ключами на НКИ

Для просмотра контейнеров с личными ключами на НКИ нужно на вкладке «Носители» в верхнем поле «Используемые» щелкнуть левой клавишей мыши по требуемому НКИ.

В результате в нижнем поле «Контейнеры на выбранном носителе» отобразятся все контейнеры личных ключей на этом НКИ.

Поле «Контейнеры на выбранном носителе» содержит следующую информацию (см. Рисунок 9 – Вкладка «Носители»):

- «Имя контейнера»;
- «Параметры» – параметры алгоритма ЭЦП личного ключа;
- «Сертификат» – наличие или отсутствие сертификата в контейнере.

Смена пароля для доступа к НКИ

Если есть подозрение, что текущий пароль для доступа к НКИ может быть скомпрометирован, рекомендуется его сменить.

Порядок действий по смене пароля для доступа к НКИ:

1. На вкладке «Носители» в верхнем поле «Используемые» щелкнуть правой клавишей мыши по НКИ AvPass, для которого требуется сменить пароль для доступа к НКИ, и вызвать контекстное меню (см. Рисунок 10 – Вызов контекстного меню в поле «Используемые»).

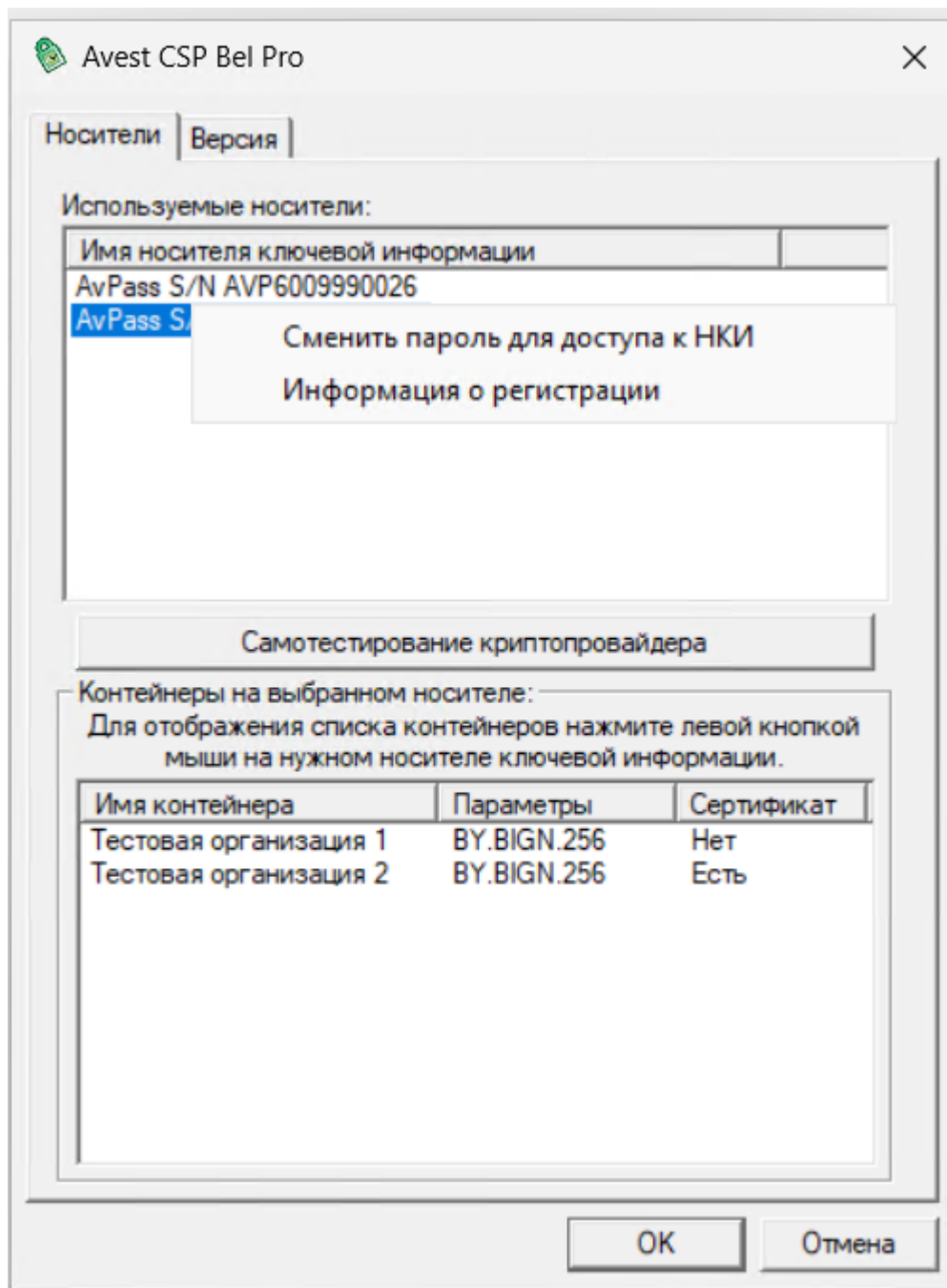
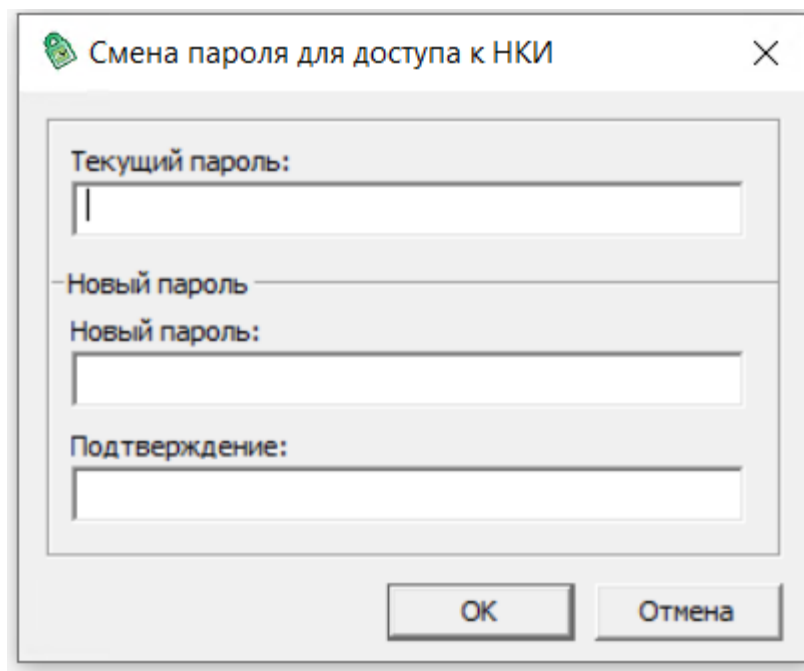


Рисунок 10 – Вызов контекстного меню в поле «Используемые»

2. В контекстном меню выбрать пункт «Сменить пароль для доступа к НКИ».
3. В открывшемся окне «Смена пароля для доступа к НКИ» ввести:
 - текущий пароль для доступа к НКИ,
 - новый пароль для доступа к НКИ,

- подтверждение нового пароля для доступа к НКИ (см. Рисунок 11 – Смена пароля для доступа к НКИ).



The image shows a standard Windows-style dialog box with the title 'Смена пароля для доступа к НКИ' (Change password for access to NKI). It features a close button (X) in the top right corner. The main area contains three text input fields with labels: 'Текущий пароль:' (Current password), 'Новый пароль:' (New password), and 'Подтверждение:' (Confirmation). The 'Новый пароль:' label is positioned above the second input field. At the bottom of the dialog, there are two buttons: 'ОК' (OK) and 'Отмена' (Cancel).

Рисунок 11 – Смена пароля для доступа к НКИ

Требования к сложности нового пароля для доступа к НКИ:

1. минимальная длина – 8 символов;
2. не должен совпадать с текущим паролем для доступа к НКИ;
3. должен содержать как минимум:
 - одну цифру (0-9);
 - одну строчную букву (латиницы или кириллицы);
 - одну заглавную букву (латиницы или кириллицы).

Примечание. В целях воспрепятствования подбору пароля для доступа к НКИ без знания его верного значения, реализована временная задержка при вводе значения пароля для доступа к НКИ.

Внимание! Пароль для доступа к НКИ нигде не сохраняется. Ответственность за сохранность пароля для доступа к НКИ несет владелец личного ключа. При утере пароля для доступа к НКИ выполнение криптографических операций с данным НКИ

невозможно. Требуется переинициализация НКИ, что приведет к полной утрате записанных на нём данных.

Примечание. Операция смены пароля для доступа к НКИ фиксируется в журнале событий Windows.

Если операция выполнена в 32-разрядной версии программы, то сообщение имеет следующий вид:

AvCSPBEL x86. Произведена смена пароля на НКИ.

Если операция выполнена в 64-разрядной версии программы, то сообщение имеет следующий вид:

AvCSPBEL x64. Произведена смена пароля на НКИ.

Для просмотра события нужно перейти по пути:

«Просмотр событий» → «Журналы Windows» → «Приложение»

и найти соответствующую запись с источником AVEST.CSP.

Просмотр информации о регистрации НКИ. Регистрация НКИ

Действия по просмотру информации о регистрации НКИ, а также его регистрации подробно описаны в п. 3.4. Регистрация НКИ.

Удаление контейнера с личным ключом

Порядок действий по удалению контейнера с личным ключом:

1. На вкладке «Носители» в верхнем поле «Используемые» щелкнуть левой клавишей мыши по требуемому НКИ AvPass.

2. В нижнем поле «Контейнеры на выбранном носителе» щелкнуть правой клавишей мыши по контейнеру с личным ключом, который нужно удалить, и вызвать контекстное меню (см. Рисунок 12 – Вызов контекстного меню в поле «Контейнеры на выбранном носителе»).

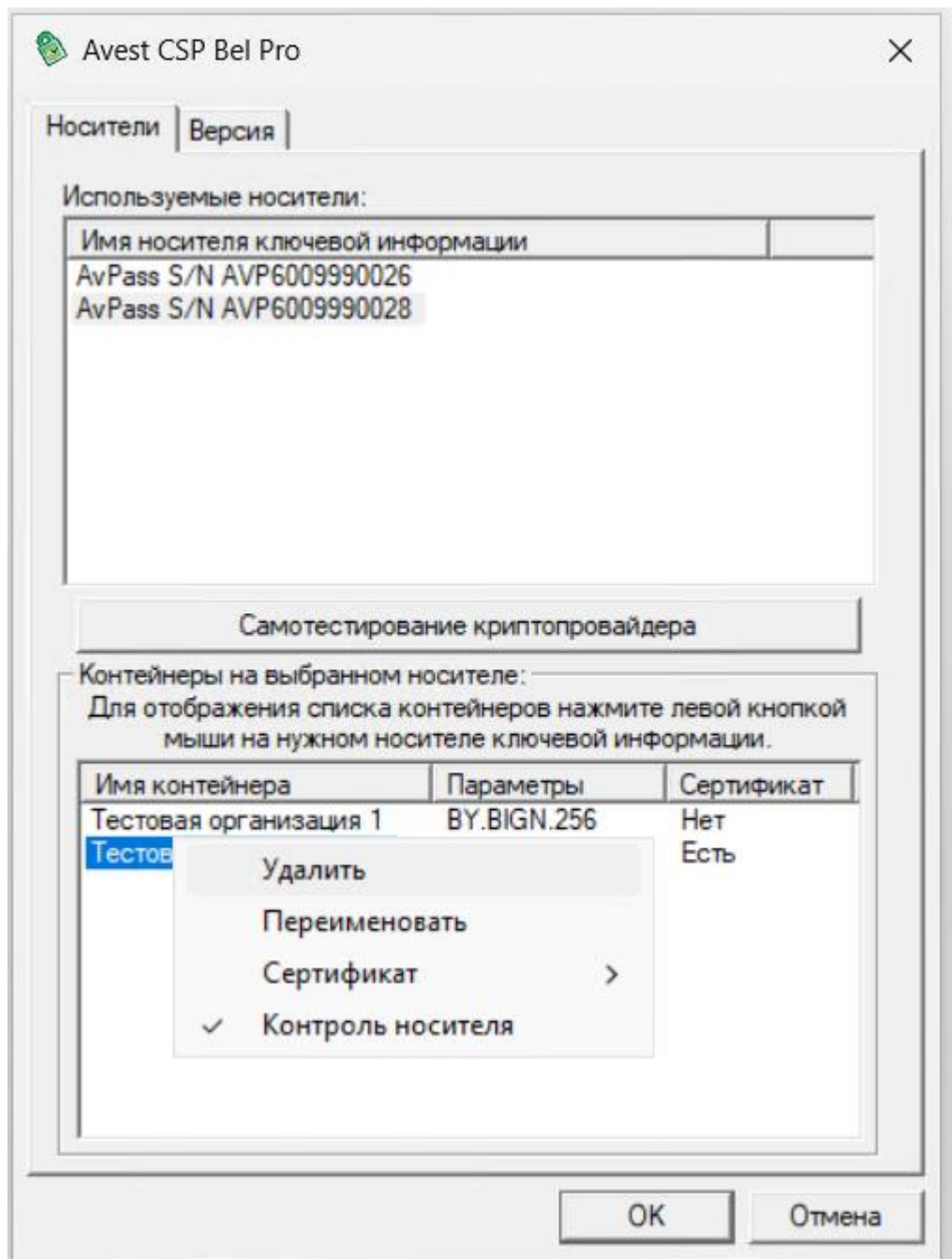


Рисунок 12 – Вызов контекстного меню в поле «Контейнеры на выбранном носителе»

4. В контекстном меню выбрать пункт «Удалить».

5. Подтвердить удаление, нажав «Да» в появившемся окне «Подтверждение» (см.

Рисунок 13 – Подтверждение удаления контейнера).

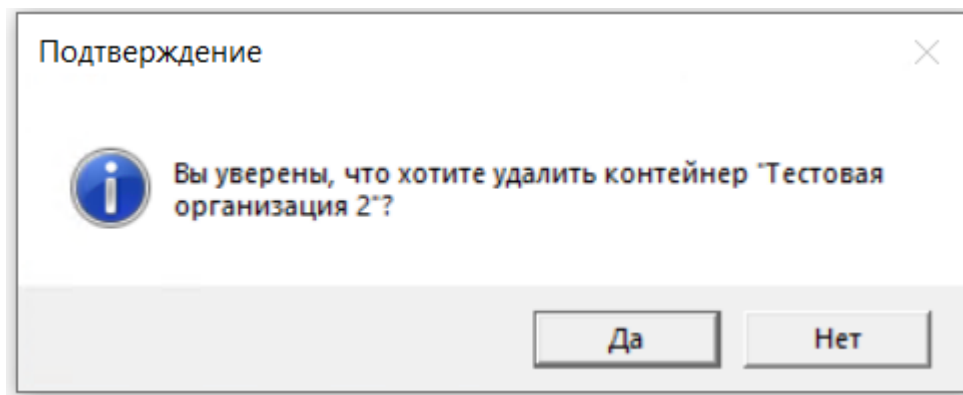


Рисунок 13 – Подтверждение удаления контейнера

6. В появившемся окне «Пароль» ввести пароль для доступа к НКИ и нажать «ОК» (см. Рисунок 14 – Окно ввода пароля для доступа к НКИ для подтверждения удаления контейнера).

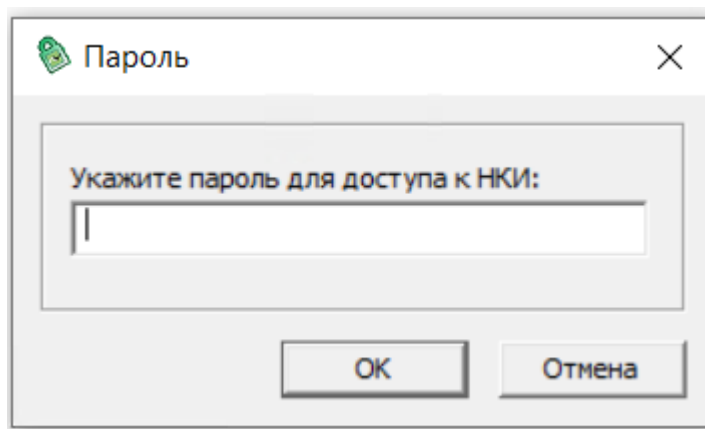


Рисунок 14 – Окно ввода пароля для доступа к НКИ для подтверждения удаления контейнера

Внимание! Удаление контейнера с личным ключом – необратимая операция. Восстановление невозможно. После удаления контейнера с личным ключом выполнение криптографических операций с данным личным ключом невозможно.

Примечание. Операция удаления контейнера на НКИ фиксируется в журнале событий Windows.

Если операция выполнена в 32-разрядной версии программы, то сообщение имеет следующий вид:

AvCSPBEL x86. "Имя контейнера" был удален.

Если операция выполнена в 64-разрядной версии программы, то сообщение имеет следующий вид:

AvCSPBEL x64. "Имя контейнера" был удален.

Для просмотра события нужно перейти по пути:

«Просмотр событий» → «Журналы Windows» → «Приложение»

и найти соответствующую запись с источником AVEST.CSP.

Переименование контейнера с личным ключом

Порядок действий по переименованию контейнера с личным ключом:

1. На вкладке «Носители» в верхнем поле «Используемые» щелкнуть левой клавишей мыши по требуемому НКИ AvPass.

2. В нижнем поле «Контейнеры на выбранном носителе» щелкнуть правой клавишей мыши по контейнеру с личным ключом, имя которого нужно изменить, и вызвать контекстное меню (см. Рисунок 12 – Вызов контекстного меню в поле «Контейнеры на выбранном носителе»).

3. В контекстном меню выбрать пункт «Переименовать».

4. Ввести новое имя контейнера в строку редактирования, после того как имя станет доступным для изменения.

5. Подтвердить переименование контейнера, нажав «Да» в появившемся окне «Переименование контейнера» (см. Рисунок 15 – Подтверждение переименования контейнера).

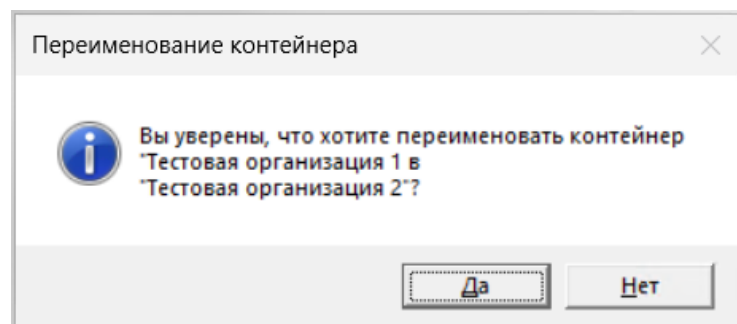


Рисунок 15 – Подтверждение переименования контейнера

7. В появившемся окне «Пароль» ввести пароль для доступа к НКИ и нажать «ОК» (см. Рисунок 16 – Окно ввода пароля для доступа к НКИ для подтверждения переименования контейнера).

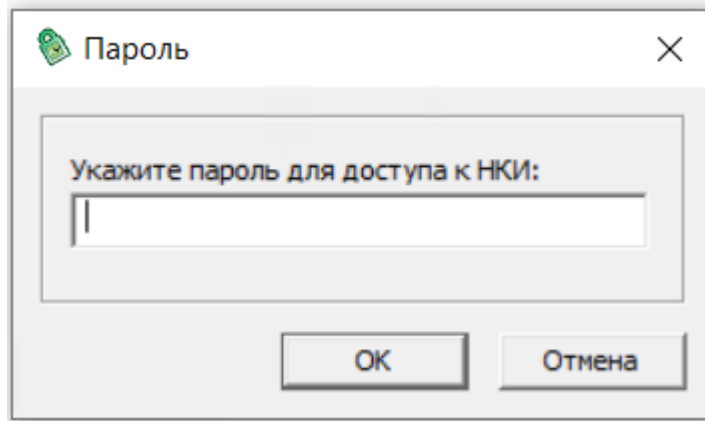


Рисунок 16 – Окно ввода пароля для доступа к НКИ для подтверждения переименования контейнера

Примечание. Операция переименования контейнера на НКИ фиксируется в журнале событий Windows.

Если операция выполнена в 32-разрядной версии программы, то сообщение имеет следующий вид:

AvCSPBEL x86. Название контейнера "Имя контейнера" было изменено на "Имя контейнера".

Если операция выполнена в 64-разрядной версии программы, то сообщение имеет следующий вид:

AvCSPBEL x64. Название контейнера "Имя контейнера" было изменено на "Имя контейнера".

Для просмотра события нужно перейти по пути:

«Просмотр событий» → «Журналы Windows» → «Приложение»

и найти соответствующую запись с источником AVEST.CSP.

Просмотр сертификата в контейнере с личным ключом

Порядок действий по просмотру сертификата в контейнере с личным ключом:

1. На вкладке «Носители» в верхнем поле «Используемые» щелкнуть левой клавишей мыши по требуемому НКИ AvPass.

2. В нижнем поле «Контейнеры на выбранном носителе» щелкнуть правой клавишей мыши по контейнеру с личным ключом, чей сертификат нужно просмотреть (для данного контейнера в колонке «Сертификат» должно быть указано значение «Есть»), и вызвать контекстное меню (см. Рисунок 12 – Вызов контекстного меню в поле «Контейнеры на выбранном носителе»).

3. В контекстном меню выбрать пункт «Сертификат», подпункт «Просмотреть».

4. Откроется окно просмотра сертификата, записанного в контейнер (см. Рисунок 17 – Окно просмотра сертификата).

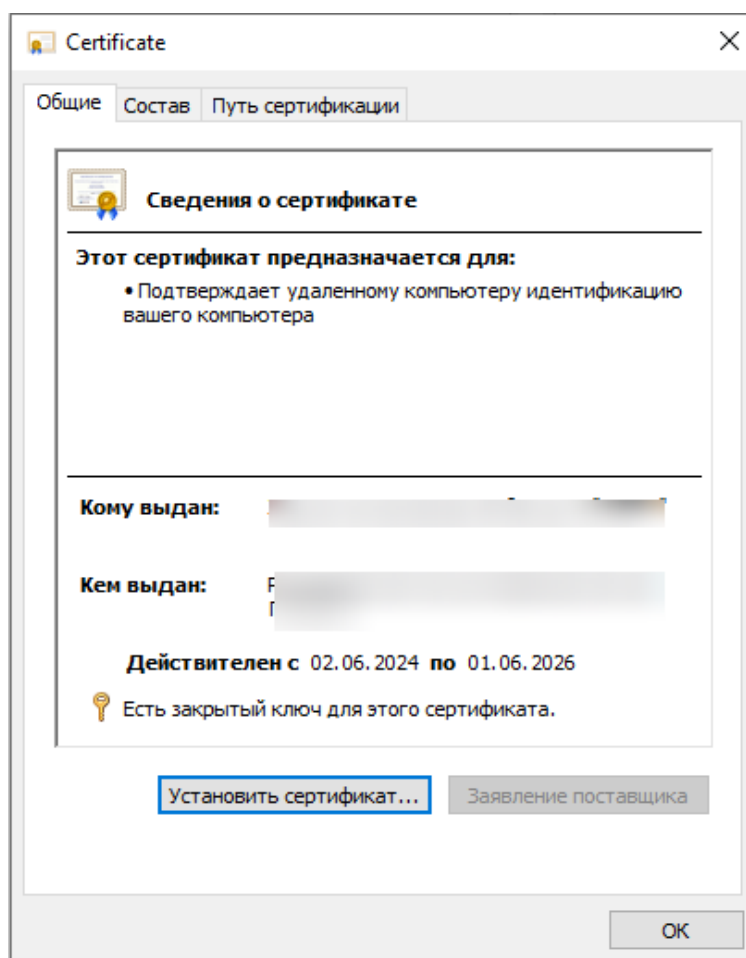


Рисунок 17 – Окно просмотра сертификата

Управление режимом контроля НКИ

Опция «Контроль носителя» включает проверку наличия вставленного НКИ при каждом обращении к нему. Если опция отключена, проверка не выполняется в течение времени действия кэширования пароля для доступа к НКИ.

По умолчанию контроль НКИ включен.

Порядок действий по управлению контролем НКИ:

1. На вкладке «Носители» в верхнем поле «Используемые» щелкнуть левой клавишей мыши по требуемому НКИ AvPass.

2. В нижнем поле «Контейнеры на выбранном носителе» щелкнуть правой клавишей мыши по контейнеру с личным ключом, чей контроль нужно проверить, и вызвать контекстное меню (см. Рисунок 12 – Вызов контекстного меню в поле «Контейнеры на выбранном носителе»).

3. В контекстном меню пункт «Контроль носителя» будет отмечен галочкой, если данная опция включена. Для отключения нужно снять галочку.

Внимание! Отключение контроля носителя снижает уровень безопасности при эксплуатации НКИ.

Контроль целостности и тестирование работоспособности компонентов криптопровайдера AvCSPBEL

Кнопка «Самотестирование» позволяет осуществить контроль целостности и тестирование работоспособности компонентов криптопровайдера AvCSPBEL.

После нажатия кнопки «Самотестирование» должно появиться окно «Информация» с сообщением: «Самотестирование прошло успешно» (см. Рисунок 18 – Самотестирование прошло успешно).

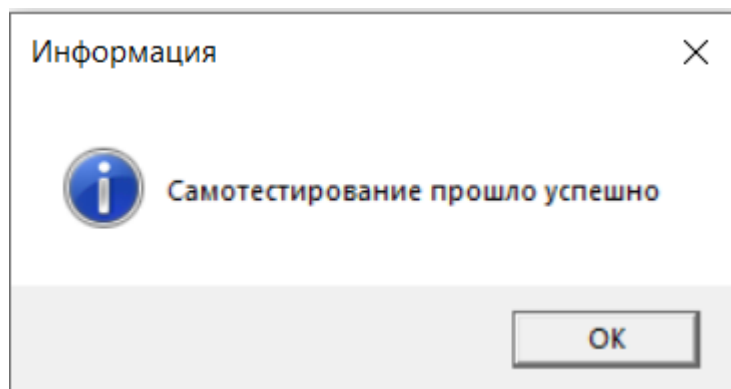


Рисунок 18 – Самотестирование прошло успешно

3.3.2. Вкладка «Версия»

Назначение вкладки «Версия» – контроль компонентов криптопровайдера AvCSPBEL. Подробнее см. п. 3.5. Контроль компонентов криптопровайдера AvCSPBEL.

3.4. Регистрация НКИ

При использовании неактивированного (незарегистрированного) НКИ нужно предварительно выполнить его регистрацию.

Порядок действия для проверки наличия регистрации НКИ:

1. На вкладке «Носители» в верхнем поле «Используемые» щелкнуть правой клавишей мыши по НКИ AvPass, для которого требуется проверить наличие регистрации, и вызвать контекстное меню (см. Рисунок 10 – Вызов контекстного меню в поле «Используемые»).

2. В контекстном меню выбрать пункт «Информация о регистрации».

Если НКИ **зарегистрирован**, то откроется окно «Информация о регистрации», в котором будут указаны:

- номер лицензии,
- тип НКИ,
- серийный номер (см. Рисунок 19 – Информация о регистрации НКИ).

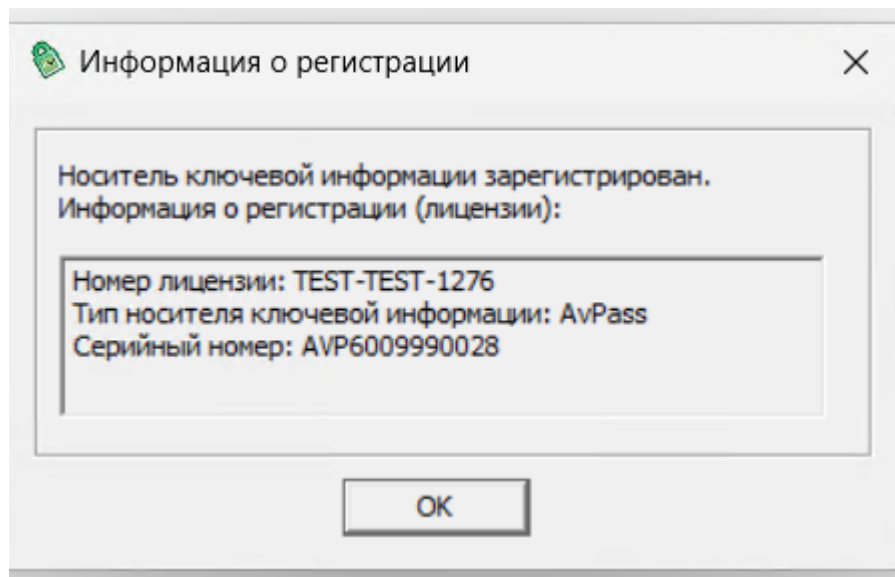


Рисунок 19 – Информация о регистрации НКИ

Если НКИ **не зарегистрирован**, то откроется окно «Регистрация носителя» (см. Рисунок 20 – Регистрация НКИ. Выбор действия).

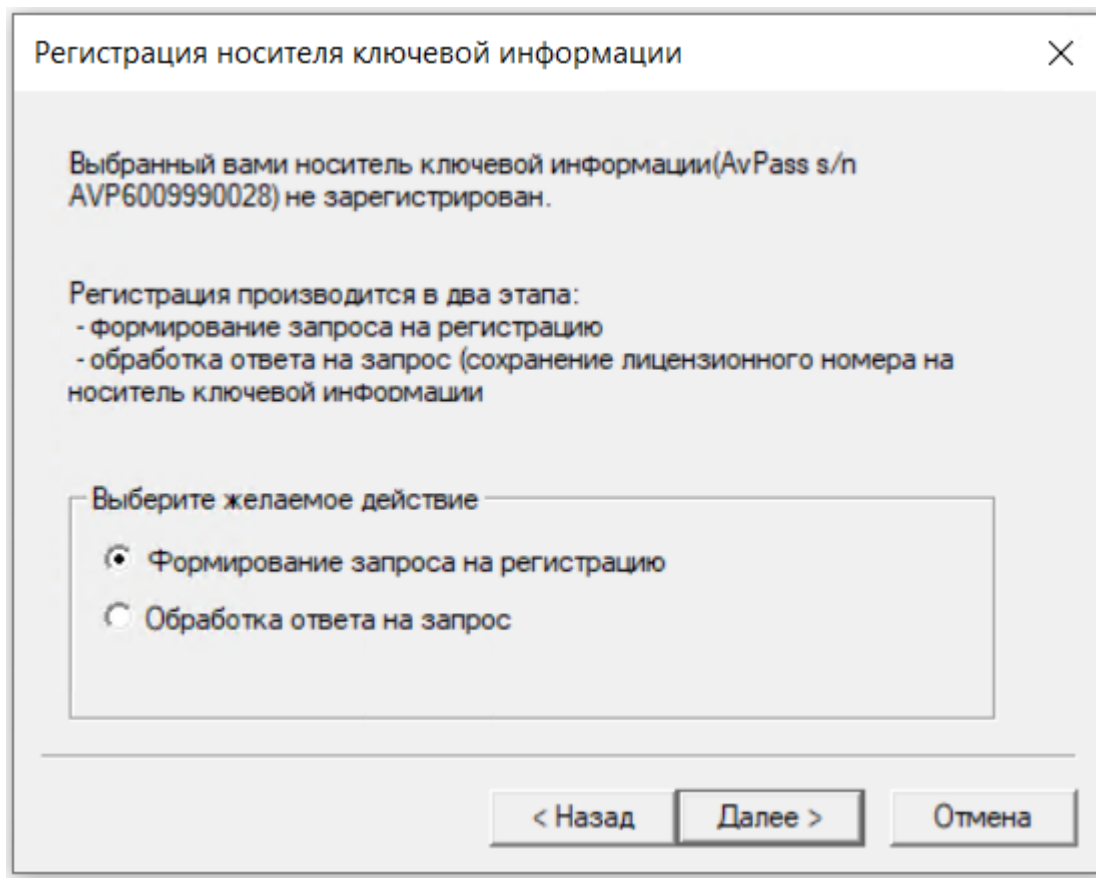


Рисунок 20 – Регистрация НКИ. Выбор действия

Порядок действий по регистрации незарегистрированного НКИ:

1. В окне «Регистрация носителя ключевой информации» установить переключатель на пункт «Формирование запроса на регистрацию» и нажать кнопку «Далее>» (см. Рисунок 20 – Регистрация НКИ. Выбор действия).

2. В следующем окне ввести PIN-код активации, который поставляется вместе с используемым НКИ, и нажать кнопку «Далее>» (см. Рисунок 21 – Регистрация НКИ. Ввод PIN-кода активации).

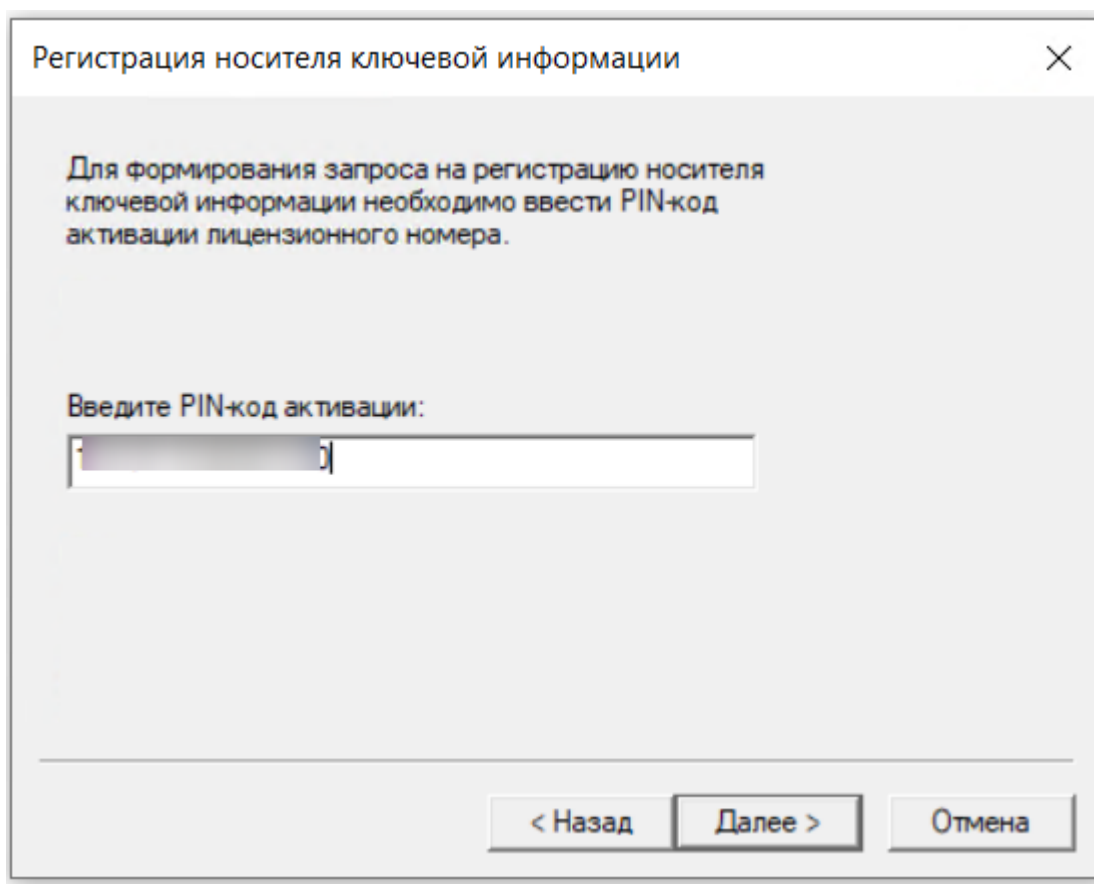


Рисунок 21 – Регистрация НКИ. Ввод PIN-кода активации

3. Далее появится окно, в котором будет показан ваш запрос на регистрацию (см. Рисунок 22 – Регистрация НКИ. Содержание запроса). Этот запрос нужно скопировать и отправить по электронной почте **token_reg@avest.by**.

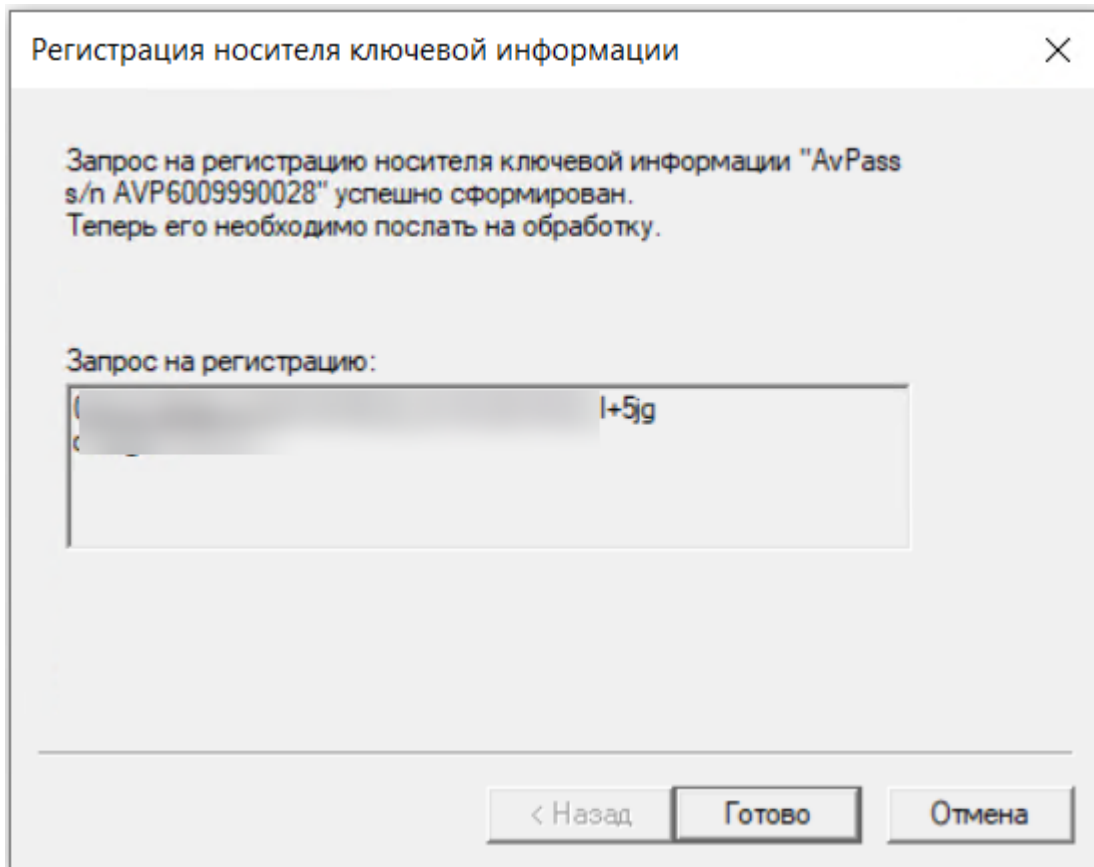


Рисунок 22 – Регистрация НКИ. Содержание запроса

4. Нажать кнопку «Готово» для закрытия окна «Регистрация носителя ключевой информации».

5. Дождаться получения ответа на email. Пример ответа:

```
QwJrUZmaNxckTTTAhtfV3ZBcYx7LnOdP/psID8cTyyygXAMfwA  
l6yZkeG1W0pRoUn2Gfffffffffffffr7MuEjbrCd2rFwLqa5Wq  
YPhTsVzI9ltMeyF6OEam0GzVcY5U9rnXpQ==
```

Скопировать полученный ответ.

6. В окне управления криптопровайдером на вкладке «Носители» в верхнем поле «Используемые» щелкнуть правой клавишей мыши по НКИ AvPass, который нужно зарегистрировать, и вызвать контекстное меню (см. Рисунок 10 – Вызов контекстного меню в поле «Используемые»).

7. В контекстном меню выбрать пункт «Информация о регистрации».

8. В появившемся окне «Регистрация носителя ключевой информации» (см. Рисунок 20 – Регистрация НКИ. Выбор действия) установить переключатель на пункт «Обработка ответа на запрос» и нажать кнопку «Далее>».

9. Далее в появившемся окне вставить полученный по электронной почте ответ и нажать кнопку «Готово» (см. Рисунок 23 – Регистрация НКИ. Ввод ответа на запрос).

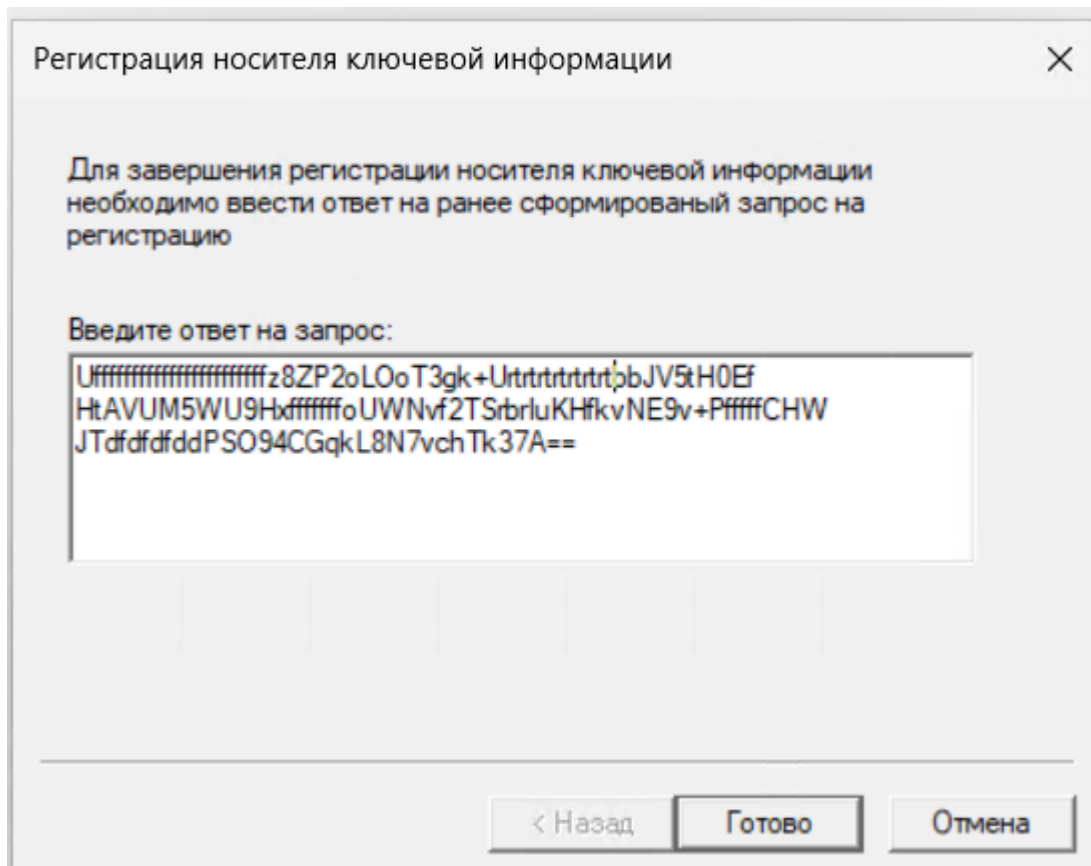


Рисунок 23 – Регистрация НКИ. Ввод ответа на запрос

8. В появившемся окне «Пароль» ввести пароль для доступа к НКИ и нажать «ОК» (см. Рисунок 24 – Регистрация НКИ. Окно ввода пароля для доступа к НКИ для подтверждения регистрации).

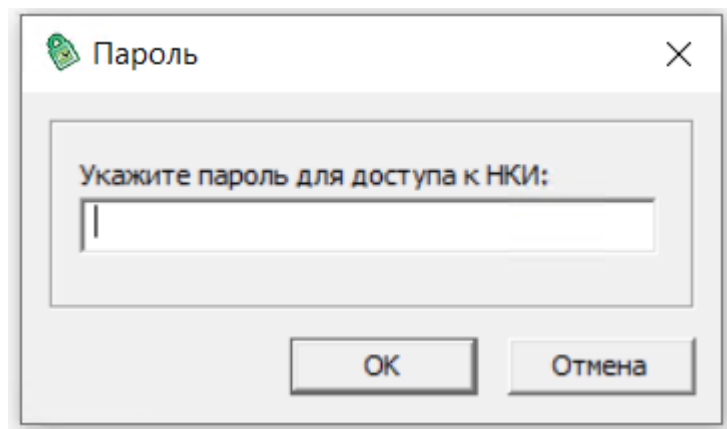


Рисунок 24 – Регистрация НКИ. Окно ввода пароля для доступа к НКИ для подтверждения регистрации

9. В случае успешной регистрации ответ должен быть «Носитель успешно зарегистрирован», нажать «ОК» (см. Рисунок 25 – Регистрация НКИ. Носитель ключевой информации успешно зарегистрирован).

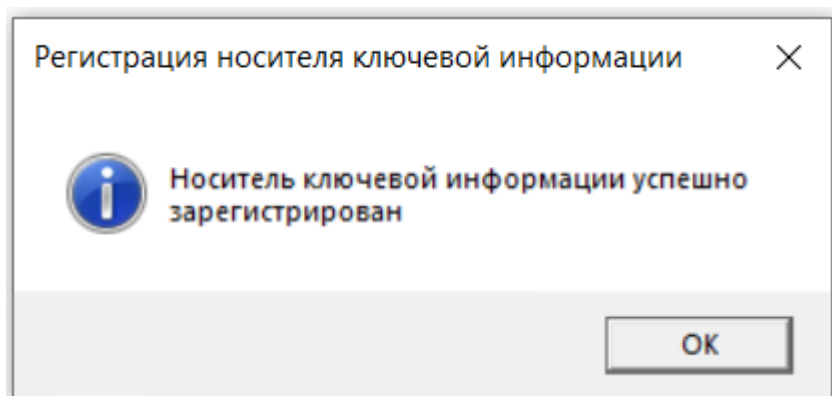


Рисунок 25 – Регистрация НКИ. Носитель ключевой информации успешно зарегистрирован

3.5. Контроль компонентов криптопровайдера AvCSPBEL

Для контроля программных компонентов криптопровайдера AvCSPBEL используются встроенные средства, доступные на вкладке «Версия» в окне управления криптопровайдером.

На вкладке «Версия» (см. Рисунок 26 – Вкладка «Версия») представлены следующие элементы (подробное описание приведено ниже):

- Поле «Информация о продукте»;
- Кнопка «Обновить регистрацию компонентов в системном реестре»;
- Поле «Версии компонентов».

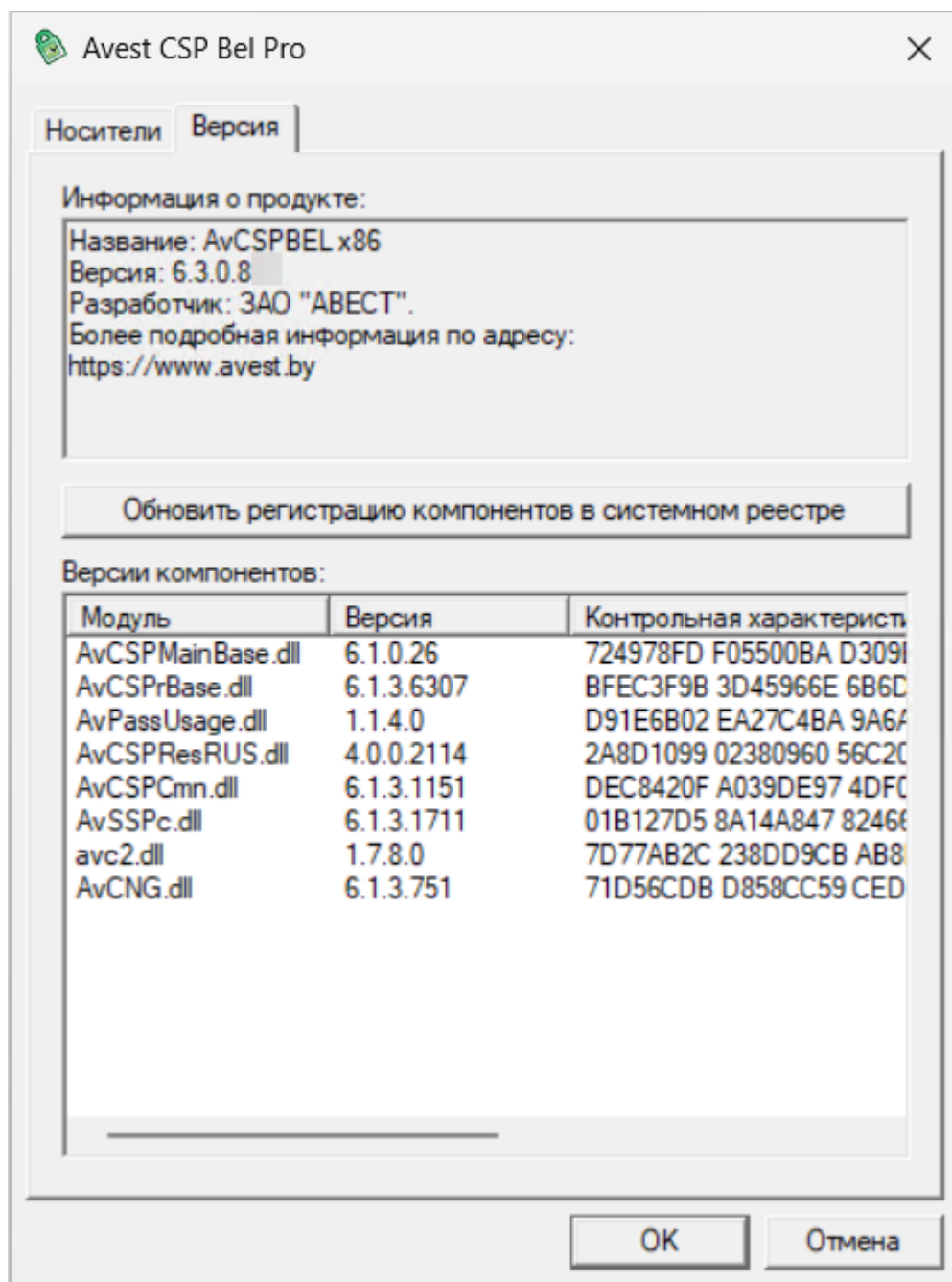


Рисунок 26 – Вкладка «Версия»

Поле «Информация о продукте»

Поле отображает название продукта, номер версии и сведения о разработчике.

Кнопка «Обновить регистрацию компонентов в системном реестре»

Кнопка «Обновить регистрацию компонентов в системном реестре» позволяет зарегистрировать или восстановить регистрацию компонентов в системном реестре Windows. Операция аналогична процессу регистрации компонентов при установке криптопровайдера AvCSPBEL и может быть использована для восстановления работоспособности криптопровайдера AvCSPBEL в случае некорректного обновления или удаления его компонентов.

После нажатия кнопки «Обновить регистрацию компонентов в системном реестре» должно появиться окно «Информация» с сообщением: «Регистрация компонентов завершена успешно» (см. Рисунок 27 – Регистрация компонентов завершена успешно).

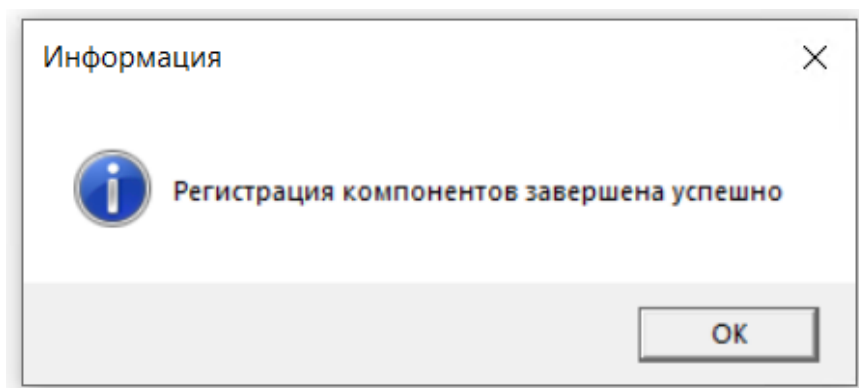


Рисунок 27 – Регистрация компонентов завершена успешно

Поле «Версии компонентов»

Поле содержит информацию о версиях и целостности компонентов криптопровайдера AvCSPBEL.

Поле состоит из трех колонок:

1. «Модуль» – список основных криптографических системных библиотек и библиотек криптопровайдера AvCSPBEL;
2. «Версия» – версия каждой библиотеки;
3. «Контрольная характеристика» – хэш-значение криптографической библиотеки согласно СТБ 34.101.31-2020.

Оператор проверяет целостность компонентов, сравнивая отображаемые хэш-значения с эталонными.

Эталонные значения можно получить тремя способами.

Способ 1.

Скопировать значения в окне управления криптопровайдером сразу после установки криптопровайдера AvCSPBEL с доверенного носителя.

1. Нажать правой клавишей мыши в области поля «Версии компонентов» вкладки «Версия» окна управления криптопровайдером.

2. В контекстном меню выбрать «Скопировать в буфер обмена» (см. Рисунок 28 – Скопировать в буфер обмена).

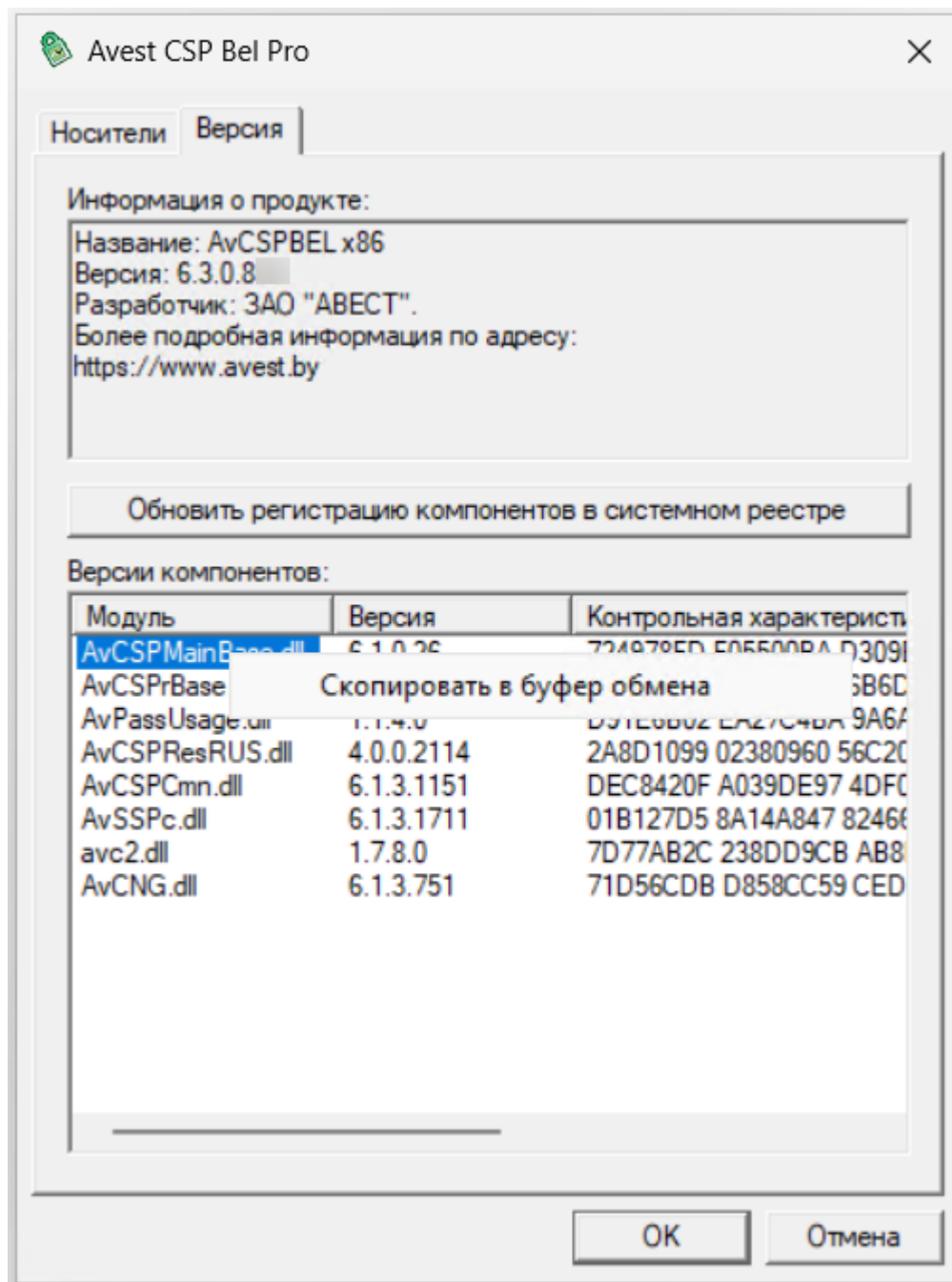


Рисунок 28 – Скопировать в буфер обмена

3. Сохранить скопированные данные (модули, версии, хэш-значения) в файл.

Способ 2.

Запросить эталонные значения у разработчика криптопровайдера AvCSPBEL – компании ЗАО «АВЕСТ».

Способ 3.

Просмотреть файл контрольных характеристик.

Файл контрольных характеристик 32-разрядного криптопровайдера AvCSPBEL:
%ProgramFiles(x86)%\Avest\Avest CSP Bel\avcspbel_x86.int

Файл контрольных характеристик 64-разрядного криптопровайдера AvCSPBEL:
%ProgramFiles%\Avest\Avest CSP Bel\avcspbel_x64.int

3.6. Сообщения оператору

Криптопровайдер AvCSPBEL выдает сообщения оператору путем отображения информации о состоянии программных модулей и содержимого НКИ, выводимой в GUI-интерфейсе программы.

При возникновении ошибок сообщения оператору выдаются в среде GUI-интерфейса путем вывода окна с информацией об ошибке. При взаимодействии с прикладным ПО сообщения вызывающему программному обеспечению возвращаются в виде кодов возврата MS CryptoAPI.

Ниже приведены примеры типичных ошибок, отображаемых в GUI, с возможными причинами и рекомендуемыми действиями:

1. Указанный носитель ключевой информации отсутствует в считывателе (см. Рисунок 29 – Ошибка. Указанный носитель ключевой информации отсутствует в считывателе).

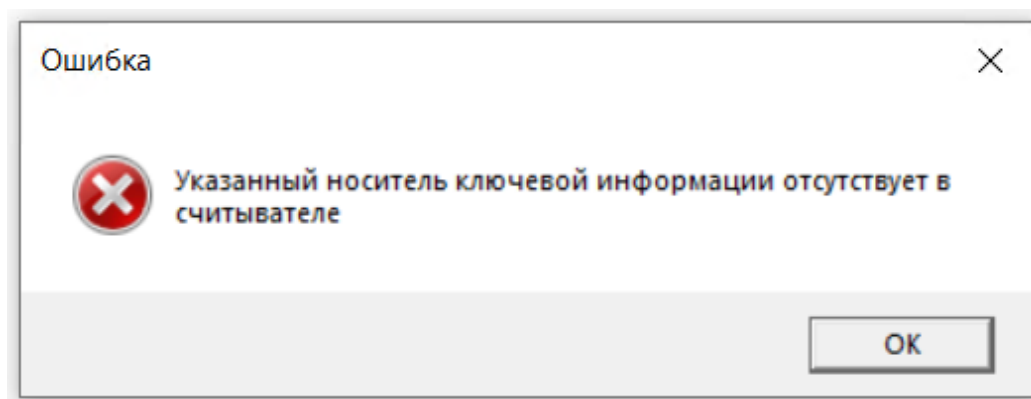


Рисунок 29 – Ошибка. Указанный носитель ключевой информации отсутствует в считывателе

Причина: НКИ, к которому идет обращение, не определён в ОС или физически не подключён.

Решение: установить НКИ в рабочий USB-порт или переподключить НКИ.

2. Пароль для доступа к НКИ неверен (см. Рисунок 30 – Ошибка. Пароль для доступа к НКИ неверен).

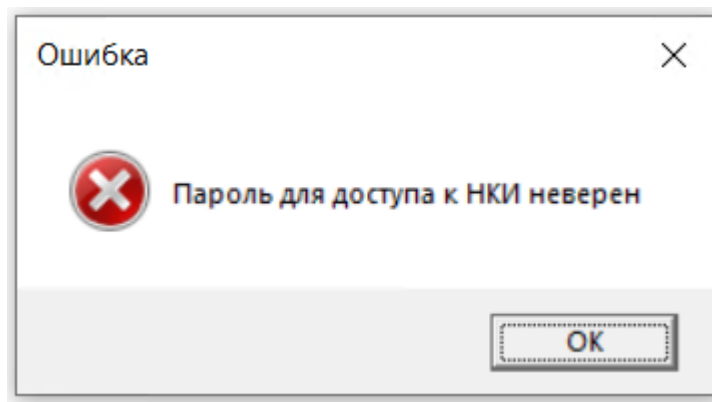


Рисунок 30 – Ошибка. Пароль для доступа к НКИ неверен

Причина: введен неправильный пароль для доступа к НКИ.

Решение: ввести корректный пароль для доступа к НКИ.

3. Ошибки при смене пароля для доступа к НКИ, возникающие при нарушении требований к сложности нового пароля для доступа к НКИ:

- Длина пароля для доступа к НКИ менее 8 символов (см. Рисунок 31 – Ошибка. Пароль для доступа к НКИ должен иметь длину не менее 8 символов).

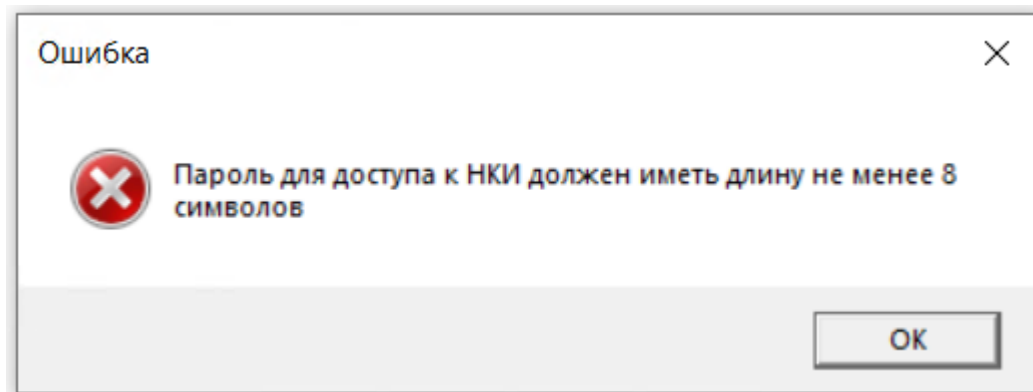


Рисунок 31 – Ошибка. Пароль для доступа к НКИ должен иметь длину не менее 8
символов

Решение: задать новый пароль для доступа к НКИ длиной не менее 8 символов.

- Пароль для доступа к НКИ не должен совпадать с текущим паролем для доступа к НКИ (см. Рисунок 32 – Ошибка. Новый пароль для доступа к НКИ не должен совпадать с текущим паролем для доступа к НКИ).

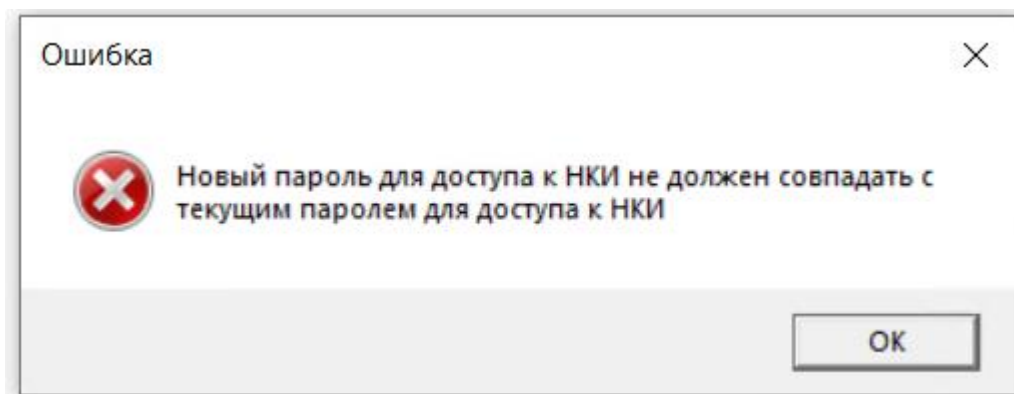


Рисунок 32 – Ошибка. Новый пароль для доступа к НКИ не должен совпадать с текущим паролем для доступа к НКИ

Решение: задать новый пароль для доступа к НКИ, отличающийся от текущего.

- Пароль для доступа к НКИ не содержит обязательных символов (см. Рисунок 33 – Ошибка. Новый пароль для доступа к НКИ должен содержать...).

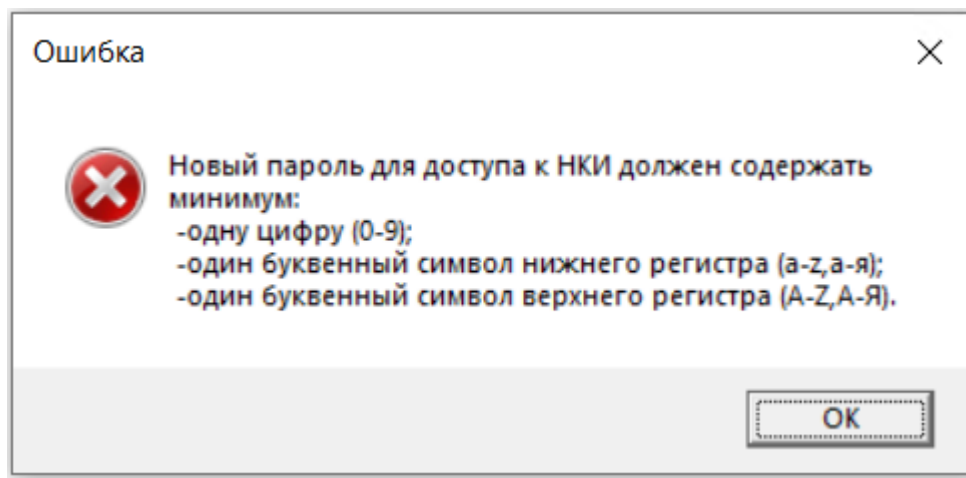


Рисунок 33 – Ошибка. Новый пароль для доступа к НКИ должен содержать...

Решение: задать новый пароль для доступа к НКИ, удовлетворяющий требованиям безопасности, который содержит как минимум:

- одну цифру (0-9);

- одну строчную букву (латиницы или кириллицы);
- одну заглавную букву (латиницы или кириллицы).

4. Ошибки при регистрации НКИ:

- Некорректный PIN-код активации (см. Рисунок 34 – Ошибка. Некорректный PIN-код).

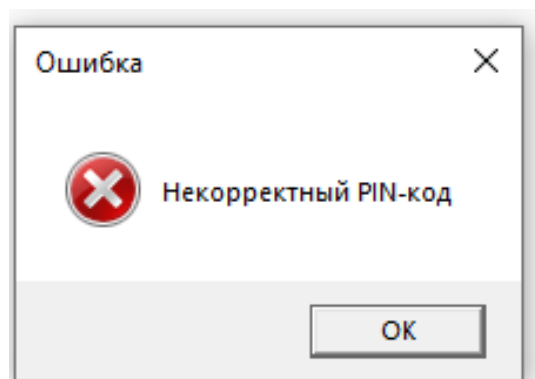


Рисунок 34 – Ошибка. Некорректный PIN-код

Причина: формат PIN-кода активации не соответствует требованиям.

Решение: ввести верный PIN-код активации, полученный с НКИ.

- Лицензионные данные некорректны (см. Рисунок 35 – Ошибка. Область данных слишком мала, Рисунок 36 – Ошибка. Плохой ключ, Рисунок 37 – Ошибка. Недопустимые данные).

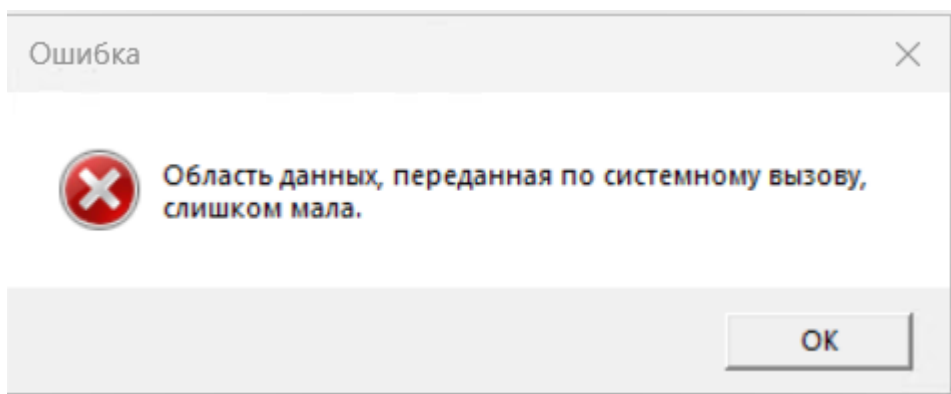


Рисунок 35 – Ошибка. Область данных слишком мала

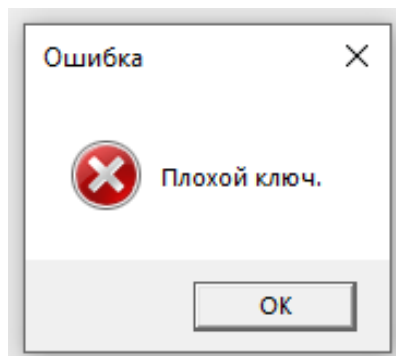


Рисунок 36 – Ошибка. Плохой ключ

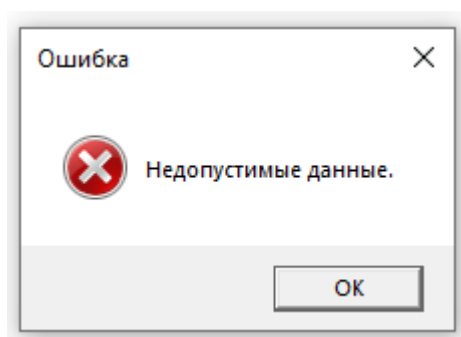


Рисунок 37 – Ошибка. Недопустимые данные

Причина: неверный формат введенных лицензионных данных.

Решение: использовать данные, полученные в ответ на лицензионный запрос.

- Лицензионные данные предназначены для другого НКИ (см. Рисунок 38 – Ошибка. Введенные лицензионные данные предназначены для другого НКИ).

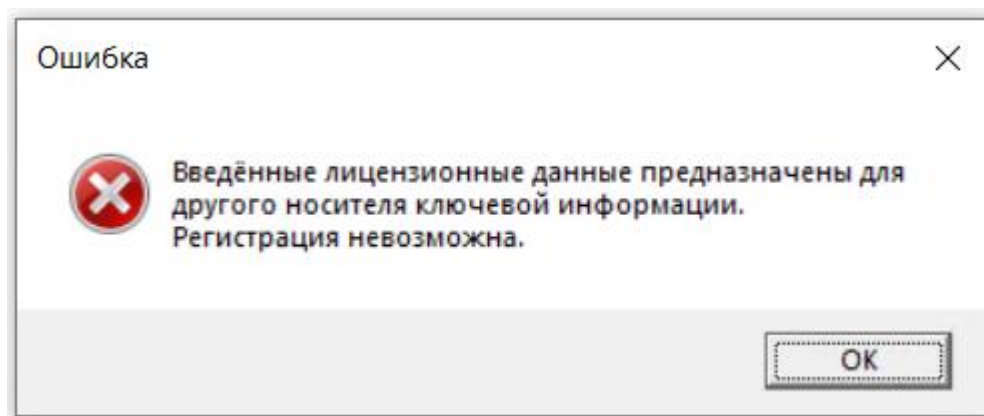


Рисунок 38 – Ошибка. Введенные лицензионные данные предназначены для другого НКИ

Причина: введены лицензионные данные для другого НКИ.

Решение: использовать данные, полученные в ответ на лицензионный запрос для данного НКИ.

5. Ошибка «Отказано в доступе» при нажатии на кнопку «Обновить регистрацию компонентов в системном реестре» (см. Рисунок 39 – Ошибка. Отказано в доступе).

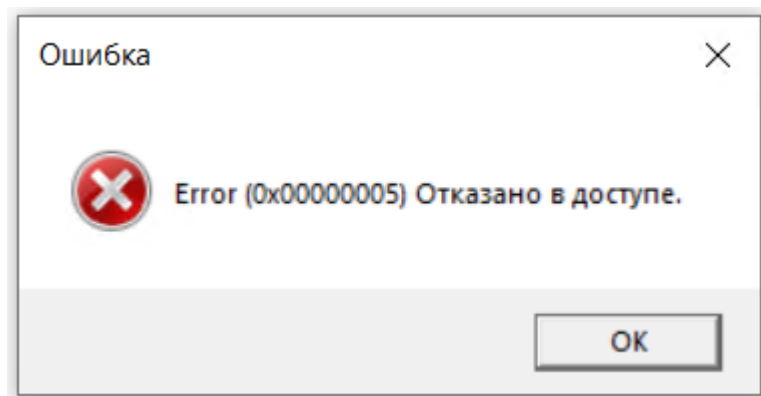


Рисунок 39 – Ошибка. Отказано в доступе

Причины:

- У пользователя недостаточно прав для выполнения операции.
- Операция блокируется антивирусным ПО.

Решение:

- Запустить программу от имени пользователя с правами на изменение реестра.
- Временно отключить или настроить антивирусное ПО.

6. Ошибки проверки целостности и работоспособности компонентов криптопровайдера AvCSPBEL.

Ошибки возникают при запуске программы или нажатии кнопки «Самотестирование»:

- «Ошибка при проверке целостности файлов» (см. Рисунок 40 – Ошибка. Ошибка при проверке целостности файлов).

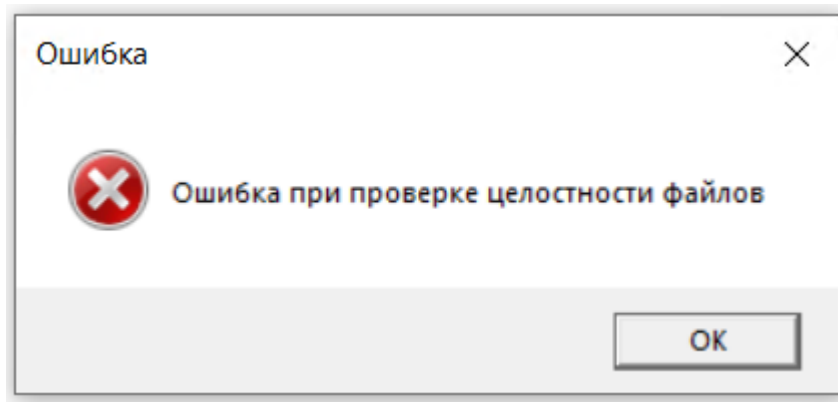


Рисунок 40 – Ошибка. Ошибка при проверке целостности файлов

- «Ошибка самотестирования» (см. Рисунок 41 – Ошибка. Ошибка самотестирования).

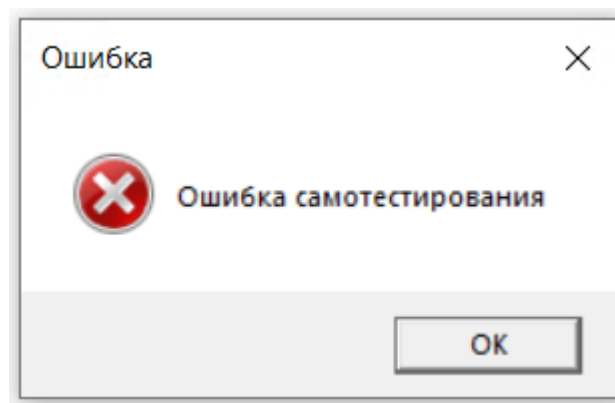


Рисунок 41 – Ошибка. Ошибка самотестирования

Причины:

- Компоненты криптопровайдера AvCSPBEL повреждены/удалены/подменены.
- Доступ к компонентам криптопровайдера AvCSPBEL заблокирован.

Решение:

- Полностью удалить установленный криптопровайдер AvCSPBEL и все его компоненты (см. п. 4. Удаление программы).
- Перезагрузить компьютер.
- Установить криптопровайдер AvCSPBEL с дистрибутива, полученного из надежного источника (см. п. 5.2. Меры безопасности при установке и эксплуатации).

4. УДАЛЕНИЕ ПРОГРАММЫ

Существует два способа удаления криптопровайдера AvCSPBEL:

- 1) С использованием стандартных средств операционной системы. Конкретные действия зависят от версии ОС Windows.
- 2) С помощью файла unins000.exe из папки, в которую был установлен криптопровайдер AvCSPBEL.

1 способ. Удаление средствами операционной системы

В ОС Windows 7, Windows 2008 R2 Server:

- 1) Выбрать из основного меню Windows: «Пуск» – «Панель управления» – «Программы и компоненты» (или «Программы»/«Удаление программы»).
- 2) В окне «Удаление или изменение программы» в списке программ выбрать «Avest CSP BEL vX.X.X.XXX», щелкнуть по нему правой клавишей мыши, нажать кнопку «Удалить».
- 3) В окне подтверждения решения об удалении нажать кнопку «Да».
- 4) Если появится окно «Удалить совместно используемый файл?», то надо нажать кнопку «Да для Всех».
- 5) После завершения удаления появится окно с сообщением об удалении программы Avest CSP BEL с компьютера, в котором необходимо нажать кнопку «ОК» и выполнить перезагрузку компьютера вручную.

Либо появится окно «Деинсталляция – Avest CSP BEL. Выполнить перезагрузку сейчас?», в котором необходимо нажать кнопку «Да» для перезагрузки компьютера.

В ОС Windows 8, Windows 2012 Server:

- 1) Навести курсор мыши на левый нижний угол рабочего стола до появления кнопки «Пуск», щелкнуть по ней правой клавишей мыши, в контекстном меню выбрать «Программы и компоненты».

2) В окне «Удаление или изменение программы» в списке программ выбрать «Avest CSP BEL vX.X.X.XXX», щелкнуть по нему правой клавишей мыши, нажать кнопку «Удалить».

3) Если появится окно контроля учетных записей с запросом разрешения программе/приложению вносить изменения на компьютере/устройстве, то надо нажать кнопку «Да».

4) В окне подтверждения решения об удалении нажать кнопку «Да».

5) Если появится окно «Удалить совместно используемый файл?», то надо нажать кнопку «Да для Всех».

6) После завершения удаления появится окно с сообщением об удалении программы Avest CSP BEL с компьютера, в котором необходимо нажать кнопку «ОК» и выполнить перезагрузку компьютера вручную.

Либо появится окно «Деинсталляция – Avest CSP BEL. Выполнить перезагрузку сейчас?», в котором необходимо нажать кнопку «Да» для перезагрузки компьютера.

В ОС Windows 8.1, Windows 2012 R2 Server, Windows 2016 Server:

1) Щелкнуть по кнопке «Пуск» правой клавишей мыши, выбрать «Программы и компоненты».

2) В окне «Удаление или изменение программы» в списке программ выбрать «Avest CSP BEL vX.X.X.XXX», щелкнуть по нему правой клавишей мыши, нажать кнопку «Удалить».

3) В окне подтверждения решения об удалении нажать кнопку «Да».

4) Если появится окно «Удалить совместно используемый файл?», то надо нажать кнопку «Да для Всех».

5) После завершения удаления появится окно с сообщением об удалении программы Avest CSP BEL с компьютера, в котором необходимо нажать кнопку «ОК» и выполнить перезагрузку компьютера вручную.

РБ.ЮСКИ.12004-03 34 01

Либо появится окно «Деинсталляция – Avest CSP BEL. Выполнить перезагрузку сейчас?», в котором необходимо нажать кнопку «Да» для перезагрузки компьютера.

В ОС Windows 10, Windows 2019 Server, Windows 2022 Server:

1) Щелкнуть по кнопке «Пуск» правой клавишей мыши, выбрать «Приложения и возможности».

2) В окне «Приложения и возможности» в списке приложений выбрать и нажать на «Avest CSP BEL vX.X.X.XXX».

3) Нажать кнопку «Удалить».

4) Появится окно «Это приложение и все его данные будут удалены.», нажать кнопку «Удалить».

5) Если появится окно контроля учетных записей с запросом разрешения программе/приложению вносить изменения на компьютере/устройстве, то надо нажать кнопку «Да».

6) В окне подтверждения решения об удалении нажать кнопку «Да».

7) Если появится окно «Удалить совместно используемый файл?», то надо нажать кнопку «Да для Всех».

8) После завершения удаления появится окно с сообщением об удалении программы Avest CSP BEL с компьютера, в котором необходимо нажать кнопку «ОК» и выполнить перезагрузку компьютера вручную.

Либо появится окно «Деинсталляция – Avest CSP BEL. Выполнить перезагрузку сейчас?», в котором необходимо нажать кнопку «Да» для перезагрузки компьютера.

В ОС Windows 11, Windows 2025 Server:

1) Щелкнуть по кнопке «Пуск» правой клавишей мыши, выбрать «Установленные приложения».

2) В окне «Установленные приложения» в списке приложений выбрать «Avest CSP BEL vX.X.X.XXX», нажать на 3 точки сбоку рядом с ним, нажать «Удалить».

3) Появится окно «Это приложение и все его данные будут удалены.», нажать кнопку «Удалить».

4) Если появится окно контроля учетных записей с запросом разрешения программе/приложению вносить изменения на компьютере/устройстве, то надо нажать кнопку «Да».

5) В окне подтверждения решения об удалении нажать кнопку «Да».

6) Если появится окно «Удалить совместно используемый файл?», то надо нажать кнопку «Да для Всех».

7) После завершения удаления появится окно с сообщением об удалении программы Avest CSP BEL с компьютера, в котором необходимо нажать кнопку «ОК» и выполнить перезагрузку компьютера вручную.

Либо появится окно «Деинсталляция – Avest CSP BEL. Выполнить перезагрузку сейчас?», в котором необходимо нажать кнопку «Да» для перезагрузки компьютера.

2 способ. Удаление с помощью файла unins000.exe.

1) Открыть папку установки криптопровайдера AvCSPBEL. В зависимости от типа установки это может быть:

- в 32-разрядной ОС папка %ProgramFiles%\Avest\Avest CSP Bel;
- в 64-разрядной ОС папка %ProgramFiles(x86)%\Avest\Avest CSP Bel.

2) Запустить файл unins000.exe.

3) Если появится окно контроля учетных записей с запросом разрешения программе/приложению вносить изменения на компьютере/устройстве, то надо нажать кнопку «Да».

4) В окне подтверждения решения об удалении нажать кнопку «Да».

5) Если появится окно «Удалить совместно используемый файл?», то надо нажать кнопку «Да для Всех».

6) После завершения удаления появится окно с сообщением об удалении программы Avest CSP BEL с компьютера, в котором необходимо нажать кнопку «ОК» и выполнить перезагрузку компьютера вручную.

Либо появится окно «Деинсталляция – Avest CSP BEL. Выполнить перезагрузку сейчас?», в котором необходимо нажать кнопку «Да» для перезагрузки компьютера.

5. МЕРЫ БЕЗОПАСНОСТИ

Данный раздел содержит рекомендуемые требования обеспечения безопасности поставки, установки и эксплуатации криптопровайдера AvCSPBEL, которым должны следовать потребители в процессе приобретения и использования криптопровайдера AvCSPBEL (далее – ПО).

Данные требования направлены на достижение следующих целей:

- предупреждение нарушений целостности и подлинности программных компонентов ПО;
- обеспечение защиты криптографических ключей и данных потребителя от компрометации;
- обеспечение надежного функционирования ПО.

5.1. Меры безопасности при поставке

Передача ПО потребителю может осуществляться следующими способами:

- передача потребителю компакт-диска с записанным ПО;
- запись ПО на носитель потребителя при очной явке уполномоченного лица на предприятие (ЗАО «АВЕСТ»);
- пересылка по электронной почте (допускается в отдельных случаях, при тестовой эксплуатации ПО, либо при необходимости обновления ПО).

Во всех данных случаях для защиты от несанкционированной модификации ПО в процессе доставки ПО до потребителя применяются следующие меры безопасности:

- представитель потребителя в процессе получения ПО взаимодействует с конкретным сотрудником ЗАО «АВЕСТ», уполномоченным на передачу ПО, при этом представитель потребителя документально подтверждает свои полномочия;
- по согласованию с потребителем ЗАО «АВЕСТ» предоставляет перечень программных компонентов ПО с указанием эталонных значений версий и контрольных характеристик в виде хэш-значений, выработанных от файлов программных компонентов в соответствии со стандартом Республики Беларусь

СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности»;

- по согласованию с потребителем ЗАО «АВЕСТ» предоставляет, при необходимости, потребителю тестовую утилиту AvCmUt, позволяющую тому самостоятельно вычислить хэш-значения полученных программных компонентов ПО;

- ПО обеспечивает в своем GUI-интерфейсе отображение используемой версии программного продукта и контрольные хэш-значения программных компонентов ПО.

При получении потребителем ПО, в случае, когда он не запрашивал его у ЗАО «АВЕСТ», нужно связаться с сотрудниками ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия <https://www.avest.by>) и уточнить факт отправки ПО в свой адрес. При подтверждении отправки ПО, потребитель должен вышеуказанным способом проконтролировать соответствие версий и целостность полученного ПО. При отсутствии подтверждения от ЗАО «АВЕСТ» факта отправки ПО, потребитель должен воздержаться от использования полученного ПО.

5.2. Меры безопасности при установке и эксплуатации

Установка ПО на компьютер потребителя должна производиться в соответствии с данным руководством. При этом должны быть обеспечены следующие условия:

- перед установкой должна быть произведена проверка хэш-значения установочного файла ПО с хэш-значениями, указанными в сертификате соответствия на ПО, с помощью программного обеспечения по расчету хэш-значений, полученных потребителями из доверенного источника;

- установка ПО должна производиться уполномоченным сотрудником потребителя, ознакомленным с данным документом и выполняющим обязанности администратора;

- на компьютере, предназначенном для установки ПО, должны отсутствовать вредоносные программы («компьютерные вирусы», «резиденты», «отладчики», «клавиатурные шпионы» и т.д.);

– после установки ПО отчуждаемый носитель (компакт-диск) с эталонным установочным файлом ПО и список эталонных хэш-значений программных компонентов (см. п. 3.5. Контроль компонентов криптопровайдера AvCSPBEL) должны быть помещены в безопасное хранилище, доступ к которому должен иметь только уполномоченный персонал потребителя.

Эксплуатация ПО на компьютере потребителя должна производиться в соответствии с данным руководством. При этом должны быть обеспечены следующие условия:

– сотрудник, эксплуатирующий ПО, должен быть предупрежден об ответственности, возлагаемой на него при использовании ПО в информационных системах электронного документооборота, обеспечивающих средствами ПО электронную цифровую подпись в соответствии с Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи» или в иных случаях;

– для эксплуатации ПО должен использоваться, по возможности, выделенный компьютер с установленным на нем лицензионным системным и прикладным программным обеспечением и только необходимым по технологии использования ПО в информационной системе потребителя;

– компьютер, предназначенный для эксплуатации ПО, должен быть защищен от «закладок», «компьютерных вирусов», несанкционированного изменения системного и прикладного программного обеспечения;

– любое изменение (реконфигурирование, дополнение и т.д.) системного и прикладного программного обеспечения компьютера должно быть согласовано с уполномоченным сотрудником потребителя, выполняющим обязанности администратора;

– сотрудник потребителя, эксплуатирующий ПО должен изучить данный документ;

- НКИ, содержащие личные ключи ЭЦП и шифрования, в отсутствие работы с ними должны храниться в надежном хранилище, доступ к которому имеют только уполномоченные сотрудники потребителя. Пароль для доступа к НКИ должен храниться в тайне. Запрещается сообщать кому-либо значение пароля для доступа к НКИ. При смене сотрудника, работающего с НКИ, новый сотрудник в первую очередь должен сменить пароль для доступа к НКИ и хранить его в дальнейшем в тайне;
- в процессе эксплуатации запрещается передавать НКИ, содержащие личные ключи ЭЦП и шифрования, посторонним лицам, оставлять НКИ без присмотра;
- ответственность за сохранность НКИ и содержащихся на нем данных несет сотрудник потребителя, работающий с НКИ;
- доступ к компьютеру с установленным ПО должен быть ограничен и разрешен только уполномоченным на работу с ПО сотрудникам потребителя;
- средствами ОС должна быть обеспечена аутентификация пользователя при запуске ОС, а также аудит событий, связанных с ПО (запуск ПО, чтение-запись файлов и данных ПО, хранящихся на носителе информации компьютера);
- при проведении ремонтных и профилактических работ в отношении компьютера, на котором установлено ПО, должны приниматься организационные меры и использоваться технические средства для исключения несанкционированного доступа к ПО;
- осмотр и ремонт компьютера представителями сторонних организаций проводятся только под наблюдением уполномоченного сотрудника потребителя;
- передача компьютера для ремонта в сторонние организации производится только после демонтажа накопителя информации (накопителя на жестком магнитном диске и/или SSD-диска);
- ремонт накопителя информации, на котором установлены программные компоненты ПО, производится только после уничтожения на нем ПО путем форматирования накопителя информации.

Для обеспечения высокого качества генерируемых криптографических ключей используемая аппаратная платформа должна располагать источником случайности RDRAND. При отсутствии источника случайности RDRAND генерация личного ключа пользователя ПК AvUCK средствами ПС AvCSPBEL запрещается.

Примечание. Инструкция RDRAND доступна в процессорах Intel, начиная с архитектуры Ivy Bridge (с 2012 года), а в процессорах AMD — начиная с модели Ryzen (с 2017 года).

После установки ПО, в комплекте поставки которого содержится ПС AvCSPBEL, необходимо произвести запуск ПС AvCSPBEL. После запуска необходимо убедиться в том, что на экран не было выведено информационное сообщение о том, что источник случайности RDRAND отсутствует. При наличии такого информационного сообщения пользователю ПК AvUCK запрещается генерировать личные ключи пользователя ПК AvUCK средствами ПС AvCSPBEL при работе на данном компьютере.

Периодически необходимо анализировать системный журнал ОС Windows на наличие предупреждений об отсутствии и/или неисправности источника случайности RDRAND.

Периодичность проведения анализа и предпринимаемые действия при обнаружении таких предупреждений определяются политикой безопасности потребителя. При этом при обнаружении предупреждения об отсутствии источника случайности RDRAND генерировать личные ключи пользователя ПК AvUCK средствами ПС AvCSPBEL запрещено до устранения причины предупреждения (например, путём замены процессора).

В случае возникновения ошибок или сбоев в работе ПО уполномоченный сотрудник потребителя, выполняющий роль администратора, должен:

1. Сравнить версии и хэш-значения программных компонентов используемого ПО с эталонными. В случае несовпадения сообщить своему руководству, связаться с отделом технической поддержки ЗАО «АБЕСТ» (контактная информация расположена

на сайте предприятия <https://www.avest.by>) и действовать в соответствии с рекомендациями сотрудника отдела технической поддержки.

2. Убедиться в работоспособности компьютера, его аппаратных и программных систем.

3. Проанализировать журналы событий ОС Windows.

4. При необходимости провести процедуру «безопасного восстановления» ПО (см. ниже).

5. В случае невозможности выполнения процедуры безопасного восстановления, прекратить эксплуатацию ПО, связаться с отделом технической поддержки ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия <https://www.avest.by>) и действовать в соответствии с рекомендациями сотрудника отдела технической поддержки.

Процедура «безопасного восстановления» ПО заключается в переинсталляции ПО на компьютере с носителя (компакт-диск) с эталонным установочным файлом ПО. При этом рекомендуется предварительно проверить работоспособность компьютера без установленного на нем ПО.

Примечания.

1. Взаимодействие с отделом технической поддержки ЗАО «АВЕСТ» по вопросам эксплуатации программного обеспечения ЗАО «АВЕСТ» возможно при условии заключения потребителем договора с ЗАО «АВЕСТ» на сопровождение программных продуктов ЗАО «АВЕСТ».

2. Потребитель, получивший программное обеспечение ЗАО «АВЕСТ» на законных основаниях от третьей стороны, по вопросам эксплуатации программного обеспечения ЗАО «АВЕСТ» должен обращаться в организацию-поставщика программного обеспечения ЗАО «АВЕСТ», если иное не определено в договоре между организацией-поставщиком и ЗАО «АВЕСТ».

6. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ИОК	– инфраструктура открытых ключей
НКИ	– носитель ключевой информации
ОЗУ	– оперативное запоминающее устройство
ОС	– операционная система
ПО	– программное обеспечение
СКЗИ	– средство криптографической защиты информации
СОК	– сертификат открытого ключа
СОС	– список отозванных сертификатов
ТНПА	– технический нормативный правовой акт
ЭЦП	– электронная цифровая подпись
CryptoAPI	– (Microsoft Cryptographic Application Programming Interface) криптографический программный интерфейс Microsoft для приложений
CSP	– (Cryptographic Service Provider) поставщик криптографических служб
GUI	– (Graphical User Interface) графический пользовательский интерфейс
PKI	– (Public Key Infrastructure) инфраструктура открытых ключей
S/MIME	– (Secure/Multipurpose Internet Mail Extensions) безопасные/многоцелевые расширения интернет-почты
SSP	– (Security Support Provider) поставщик поддержки безопасности
TLS	– (Transport Layer Security) протокол защиты транспортного уровня

7. ССЫЛКИ

1. ГОСТ 28147-89 «Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
2. СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования».
3. СТБ 1176.2-99 «Информационная технология. Защита информации. Процедура выработки и проверки электронной цифровой подписи».
4. СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата».
5. СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей».
6. СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений».
7. СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайн-протокол проверки статуса сертификата (OCSP)».
8. СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности».
9. СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых».
10. СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел».
11. СТБ 34.101.50-2019 «Информационные технологии и безопасность. Правила регистрации объектов информационных технологий».
12. СТБ 34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)».

РБ.ЮСКИ.12004-03 34 01

13. СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутивных сертификатов».

14. СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей».

15. ТР 2013/027/ВУ «Информационные технологии. Средства защиты информации. Информационная безопасность».

[illegible][illegible]