УТВЕРЖДЕН

РБ.ЮСКИ.12004-02 34 01-ЛУ

ПРОГРАММНОЕ СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «КРИПТОПРОВАЙДЕР AvCSPBEL»

AvCSPBEL

Руководство оператора

РБ.ЮСКИ.12004-02 34 01

Листов 32

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

2023

АННОТАЦИЯ

Данный документ содержит руководство оператора РБ.ЮСКИ.12004-02 34 01 «Программное средство криптографической защиты информации «Криптопровайдер AvCSPBEL» AvCSPBEL» (далее – криптопровайдер AvCSPBEL). В документе приведена последовательность действий оператора при установке программного средства, а также тексты сообщений, выдаваемых в ходе установки, описание их содержания и соответствующих действий оператора.

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

Адрес предприятия: 220116, Республика Беларусь, г. Минск, пр. газеты «Правда», д. 5, пом. 3Н., каб. 7.

Тел.: (+375 17) 257-99-74, (+375 17) 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 производителем 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

В операционных системах Windows компании Microsoft возможность выполнения приложениями верхнего уровня криптографических функций обеспечивается специальными программными (программно-аппаратными) модулями – т.н. «поставщиками криптографических услуг» (CSP – Cryptographic Service Provider) 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 криптографических 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) версий 1.0 и 2.0 и Microsoft Crypto API COM (CAPICOM).

Вышеуказанные интерфейсы используются такими стандартными приложениями Microsoft, как Internet Explorer, Outlook Express, Outlook, Internet Information Services и др.

Криптопровайдер, предоставляющий программному обеспечению прикладного уровня криптографические сервисы по интерфейсам CryptoAPI 1.0, 2.0 и CAPICOM 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, а также выработки и проверки цифровой подписи сообщений.

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 и ЭЦП, и др.

Реализованные в криптопровайдере AvCSPBEL криптографические алгоритмы доступны прикладному ПО по интерфейсам CryptoAPI 1.0, 2.0 и CAPICOM в соответствии с их спецификациями компании Microsoft. При этом используются криптографические алгоритмы и протоколы в соответствии с техническими нормативными правовыми актами Республики Беларусь в области криптографической защиты информации:

1) СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования»;

2) СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи» (проверка);

3) СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата»;

4) СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»;

5) СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»;

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

7) СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»;

8) СТБ 34.101.47-2012 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»;

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

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

11) СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых»;

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

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

– генерация криптографических ключей шифрования и ЭЦП и управление данными ключами в течение всего их жизненного цикла;

– генерация псевдослучайных данных;

– симметричное шифрование данных;

– вычисление значения хэш-функции от данных;

– выработка/проверка ЭЦП;

– выработка общего секретного ключа для процедур аутентификации и шифрования данных по асимметричной схеме;

– хранение криптографических ключей и других критичных параметров на отчуждаемых носителях ключевой информации (далее - НКИ) в зашифрованном виде.

При развертывании инфраструктуры открытых ключей с использованием криптопровайдера AvCSPBEL обеспечивается:

– поддержка сертификатов и списков отозванных сертификатов формата X.509;

– поддержка запросов на издание сертификатов открытых ключей формата PKCS#10;

– поддержка криптографических сообщений формата PKCS#7;

– защита Интернет-соединений между Web-сервером и клиентом по протоколу TLS (Transport Layer Security) с использованием аутентификации сторон и шифрования данных (SSP – Security Support Provider);

– поддержка стандарта S/MIME (Secure/Multipurpose Internet Mail Extensions) для криптографической защиты электронной почты.

ПСКЗИ «Криптопровайдер AvCSPBEL» включает компоненты «AvCSPBEL» и «AvCSPBEL Pro», регистрирующиеся в CryptoAPI как Cryptographic Service Provider типов 422 и 423 соответственно. Отличием поведения криптопровайдеров указанных типов является способ вычисления ЭЦП без использования дополнительного хэширования (тип 422) и с использованием (тип 423).

Использование возможностей 422 или 423 типа криптопровайдера прозрачно для пользователя и определяется потребностью прикладного программного обеспечения в использовании сервисов криптопровайдера AvCSPBEL.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

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

- Windows 2008 R1 Server (x32, x64);
- Windows 2008 R2 Server (x64);
- Windows 2012 Server (x64);
- Windows 2012 R2 Server (x64);
- Windows 10 (x32, x64);
- Windows 2016 Server (x64);
- Windows 2019 Server (x64).

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

- Windows 2003 Server (x32, x64) SP2;
- Windows XP SP3 (x32) ;
- Windows 7 (x32, x64);
- Windows 8 (x32, x64);
- Windows 8.1 (x32, x64).

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

ВНИМАНИЕ! Во избежание случайной непреднамеренной потери данных пользователя на НКИ (контейнеров с личными ключами ЭЦП и т.д.) и/или выхода из строя НКИ перед перезагрузкой компьютера (сервера), нештатным завершением работы криптографического ПО, переустановкой (удалением) криптографического ПО (криптопровайдера, персонального менеджера сертификатов и т.д.) необходимо извлечь НКИ из USB-порта компьютера (сервера).

В случае проведения вышеуказанных манипуляций с ПО без извлечения НКИ рекомендуется после завершения данных манипуляций с ПО средствами криптопровайдера AvCSPBEL убедиться в работоспособности НКИ и наличии данных пользователя на НКИ. В случае потери данных или

выхода из строя НКИ необходимо обратиться в техподдержку организации, в которой приобреталось ПО и НКИ.

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

- процессор x86 (x64) с тактовой частотой - не менее 2,5 ГГц;
- объем ОЗУ - не менее 4 Гб;
- жесткий диск, содержащий не менее 8 Гб свободного пространства для стандартной установки ОС;
- монитор с поддержкой VGA или более высокого разрешения;
- манипулятор «мышь» Microsoft или совместимое указывающее устройство,
- свободный USB-порт.

Для использования криптопровайдера AvCSPBEL пользователь должен иметь права «Administrator (Администратор)» либо «Power User (Опытный пользователь)».

В случае использования операционной системы с установленным языком, отличным от русского, необходимо установить в настройках ОС язык для программ, не поддерживающих Юникод – Русский.

ВНИМАНИЕ! Во избежание случайной непреднамеренной потери данных пользователя на НКИ (личных ключей ЭЦП) перед перезагрузкой компьютера (сервера), нештатным завершением криптографического ПО, переустановкой (удалением) криптографического ПО (криптопровайдера, персонального менеджера сертификатов) необходимо извлечь НКИ из USB-порта компьютера (сервера). После перезагрузки компьютера (сервера), переустановки (удаления) средствами криптопровайдера AvCSPBEL убедиться в наличии данных пользователя на НКИ.

В качестве отчуждаемого НКИ криптопровайдер AvCSPBEL поддерживает следующие типы устройств:

- AvToken (в нескольких режимах, см. далее);
- AvPass;
- iButton;
- iKey;
- eToken;

- ruToken;
- смарт-карта Acos3;
- бесконтактная карта MIFARE Std Card 4K.

Устройства AvToken и AvPass предназначены для локального использования оператором совместно с программным продуктом AvCSPBEL входящим в состав комплекта абонента AvUCK. Использование AvToken или AvPass в удалённом сеансе с использованием специализированного ПО для проброса USB-устройств является нештатным использованием. В данном случае не может быть гарантирована надежность работы AvCSPBEL с устройствами, а также конфиденциальность личных ключей.

Примечания:

1. Используемые НКИ должны быть зарегистрированы у ЗАО «АВЕСТ» согласно процедуре, описанной в данном документе.

2. Для корректной работы криптопровайдера AvCSPBEL с НКИ, необходимо до установки на компьютер криптопровайдера AvCSPBEL, установить драйверы для этих НКИ (исключение – AvToken, AvPass и iButton). Необходимые драйвера НКИ, а также инструкции по их установке можно найти на сайтах производителей данных НКИ.

Для работы носителей и сохранения личных ключей на них, предварительно, до установки криптопровайдера, нужно установить драйверы для этих устройств, кроме AvToken, AvPass и iButton:

1) Для того чтобы установить драйвер к носителю Rainbow iKey 1000 нужно с диска с дистрибутивом запустить файл iKeyDrvr.exe, который находится в папке iKey-1000\iKey-driver-3.4.4.103 и далее следовать инструкции программы установки.

2) Для того чтобы установить драйвер к носителю RuToken нужно с диска с дистрибутивом запустить файл SetupDrv.exe который находится в папке ruToken\drivers1.20._18.11.2004 и далее следовать инструкции программы установки.

3) Для запуска установки драйвера к носителю eToken у вас должен быть установлен MS Installer версии не ниже 2.0. Его так же можно найти на диске с дистрибутивом в папке WindowsInstaller\2.0 и далее запустить файл instmsiW.exe и следовать инструкции программы установки.

4) Для того, чтобы установить драйвер к носителю eToken нужно с диска с дистрибутивом запустить файл rte_3.51.17.msi, который находится в папке eToken\redistribution и далее следовать инструкции программы установки.

5) Для того, чтобы установить драйвер к носителю MIFARE нужно с диска с дистрибутивом запустить файл FTDIUNIN.EXE который находится в папке Drivers\FTDI\ и далее следовать инструкции программы установки.

6) Для того, чтобы установить драйвер к носителю ACOS3 нужно с диска с дистрибутивом запустить файл AvAcos setup.exe который находится в папке AvAcosDLL\Output\ и далее следовать инструкции программы установки.

Примечание:

ЗАО «АВЕСТ» гарантирует надежное взаимодействие криптопровайдера AvCSPBEL с НКИ AvPass и AvToken. При использовании НКИ отличных от AvPass и AvToken работа криптопровайдера AvCSPBEL с данными НКИ не гарантируется.

Примечания:

1. Криптопровайдер AvCSPBEL, начиная с версии 5.0 поддерживает работу с НКИ AvToken в режиме **strong**, обеспечивающим повышенные меры безопасности при хранении криптоконтейнера на НКИ.

2. Данный режим доступен при установке криптопровайдера и выборе из отображаемого списка поддерживаемых носителей НКИ «Avest Token strong» (**AvToken strong**).

3. При использовании НКИ AvToken strong криптопровайдер AvCSPBEL обеспечивает уничтожение криптоконтейнера на НКИ после 7 (семи) попыток ввода неправильного пароля на доступ к криптоконтейнеру.

4.Работа оператора AvCSPBEL с устройством AvPass аналогична работе с устройством AvToken. Далее по тексту документа под обозначением AvToken следует понимать устройства AvToken и AvPass.

5.Работа в 64 разрядном AvCSPBEL возможна только с устройствами AvToken и AvPass. С остальными типами носителей можно работать только в 32 разрядном AvCSPBEL.

3. УСТАНОВКА И ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Установка криптопровайдера AvCSPBEL

В зависимости от разрядности операционной системы криптопровайдер AvCSPBEL после установки будет выглядеть по-разному:

- в 32-разрядных операционных системах будет установлен один 32-разрядный криптопровайдер AvCSPBEL в папку по умолчанию «\Program Files\Avest\Avest CSP Bel» (в случае если установочная папка не была изменена на этапе установки);

- в 64-разрядных операционных системах будет установлено два криптопровайдера AvCSPBEL, один 32-разрядный в папку по умолчанию «\Program Files(x86)\Avest\Avest CSP Bel» и еще один 64-разрядный в папку по умолчанию «\Program Files\Avest\Avest CSP Bel»

Действия по установке криптопровайдера:

1) запустить с дистрибутива программу «setupAvCSPBEL6.3.0.8xx.exe»;

2) в первом окне мастера установки содержится описание устанавливаемого продукта, для начала установки программы на компьютер нажмите кнопку «Далее» (см. Рисунок 1 – Заставка мастера установки криптопровайдера).

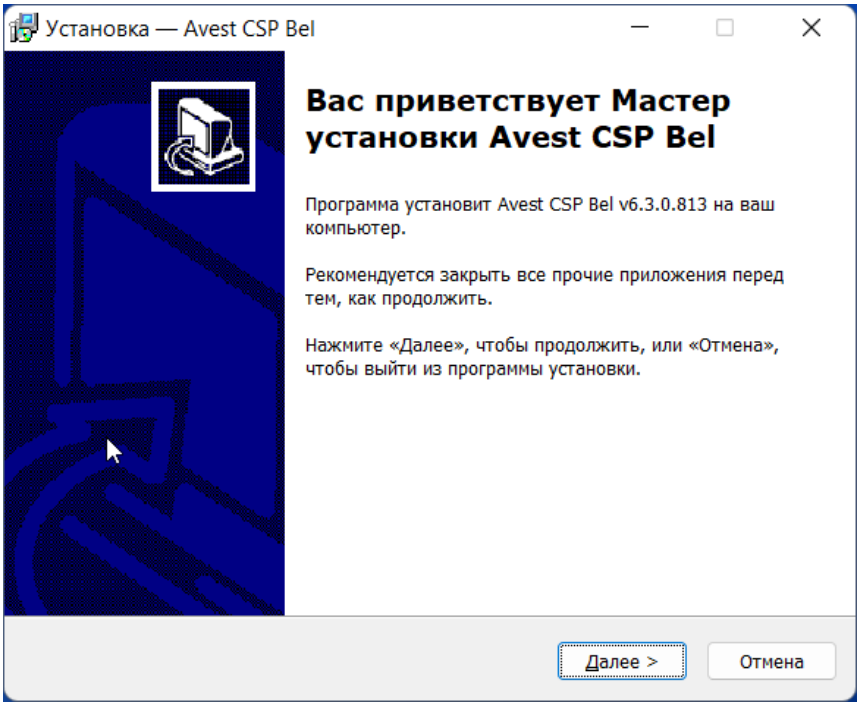

Рисунок 1 – Заставка мастера установки криптопровайдера

Почти все окна программы установки имеют 3 кнопки: «<Назад», «Далее>», «Отмена».

Нажатие на кнопку «<Назад» приводит к возврату к предыдущему окну программы установки.

Нажатие на кнопку «Далее>» позволяет перейти к следующему окну программы установки.

Нажатие на кнопку «Отмена» приведет к выходу из программы установки.

3) После нажатия на кнопку «Далее» будет приведена страница с лицензионным соглашением, условия которого надо изучить и, в случае согласия с лицензионным соглашением, нажать на кнопку «Далее» для продолжения установки.

Если вы не согласны с условиями, указанными в лицензионном соглашении, то нажмите на кнопку «Отмена» для выхода из программы установки.

4) По умолчанию установка программы производится в папку «\Program Files (x86)\Avest\Avest CSP Bel» на системном диске для 32-разрядного криптопровайдера, и в папку «\Program Files\Avest\Avest CSP Bel» для 64-разрядного криптопровайдера (установка одного или двух криптопровайдеров зависит от разрядности ОС, на которой будет устанавливаться криптопровайдер AvCSPBEL).

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

Название папки вы можете указать как вручную, так и при помощи кнопки «Обзор». По умолчанию будет создана папка «Авест» (см. Рисунок 2 - Выбор папки для создания ярлыков в меню «Пуск»).

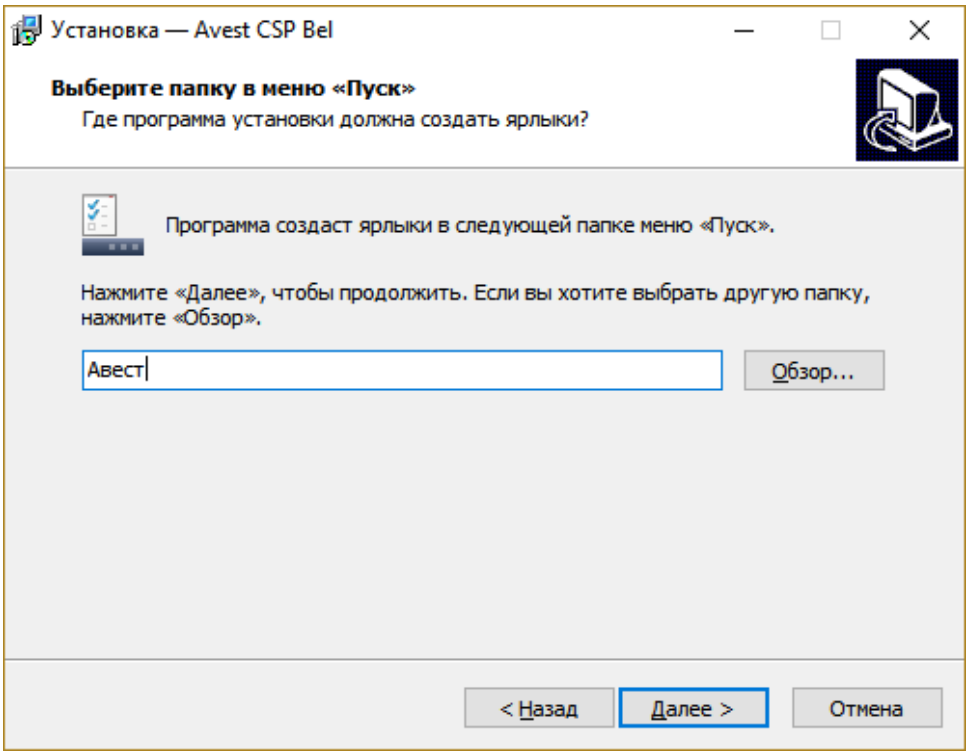

Рисунок 2 - Выбор папки для создания ярлыков в меню «Пуск»

На следующей странице мастера установки предлагается выбрать тип носителя, который будет использоваться для хранения личных ключей по умолчанию, это означает, что при создании личного ключа первым будет предложен этот носитель (см. Рисунок 3 - Выбор используемых носителей).

Чтобы использовать несколько носителей, нужно включить соответствующую опцию. Включенный флажок на любом из носителей в списке означает, что указанный носитель или несколько носителей будут использоваться для хранения личных ключей пользователя, с которым пользователь сможет работать в программном обеспечении.

Так же можно нажать на кнопку «Отметить все», и при работе с ПО, пользователь сможет использовать любой тип носителя, поддерживаемый данным криптопровайдером.

Или нажать кнопку «Снять отметку со всех», тогда будет использоваться один носитель, который выставлен по умолчанию.

Примечание: Работа в 64-разрядном криптопровайдере AvCSPBEL возможна только с устройствами AvToken и AvPass. С остальными типами носителей можно работать только в 32-разрядном AvCSPBEL.

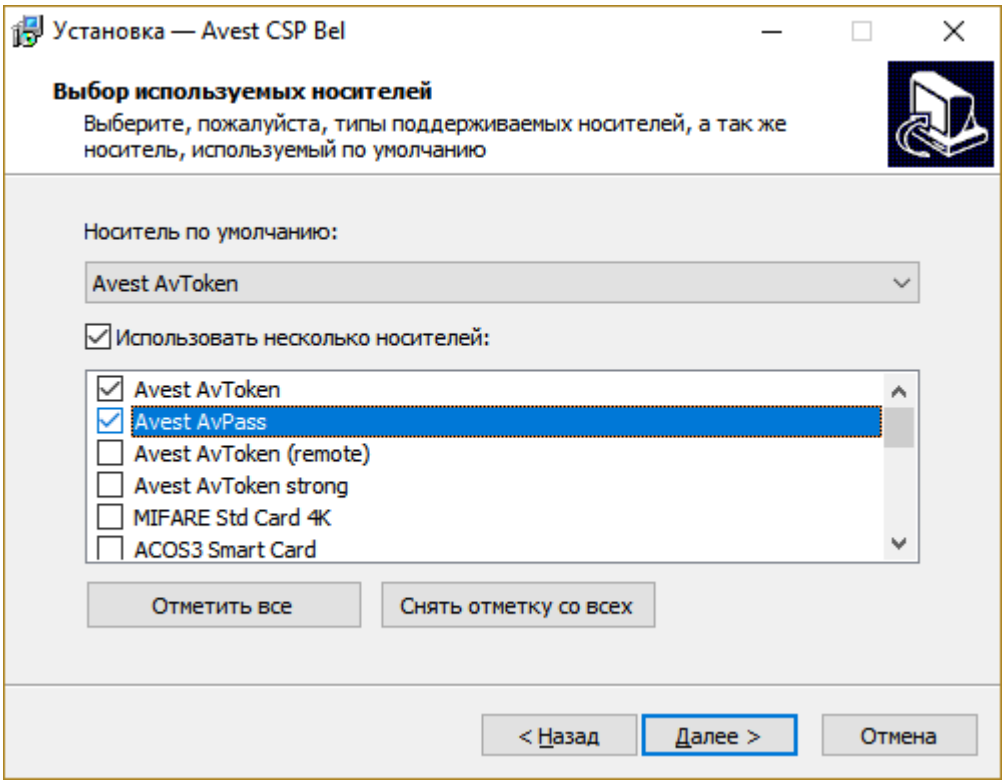

Рисунок 3 - Выбор используемых носителей

6) Теперь всё готово для установки программы на компьютер, о чем сообщает следующее окно мастера установки. В нем отражена информация о последовательности действий пользователя при установке криптопровайдера (описанных выше), (см. Рисунок 4 - Установка криптопровайдера на компьютер). Если пользователь согласен с указанными в данном окне параметрами, то надо нажать кнопку «Установить».

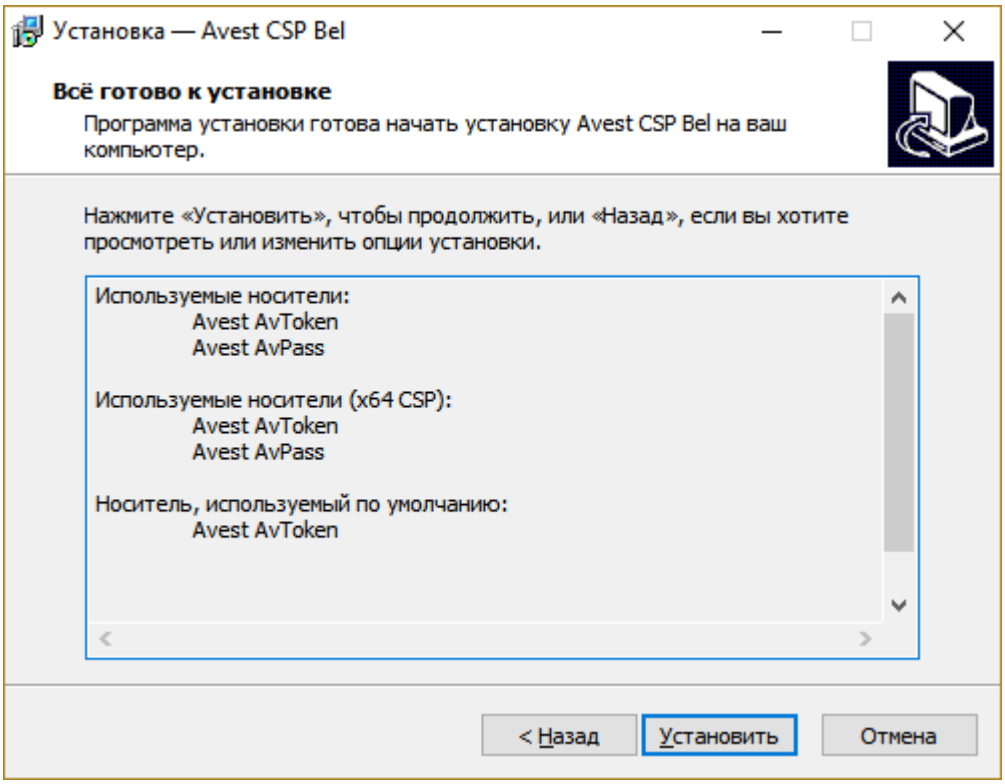

Рисунок 4 - Установка криптопровайдера на компьютер

После этого будет произведена распаковка, копирование файлов и регистрация библиотек на компьютере.

7) Далее необходима регистрация криптопровайдера, для этого нужно некоторое количество случайных данных, необходимо подвигать мышью в пределах следующего появившегося окна. (см. Рисунок 5 - Сбор случайных данных для регистрации криптопровайдера).

Примечание. При повторной инсталляции данное окно появляться не будет.

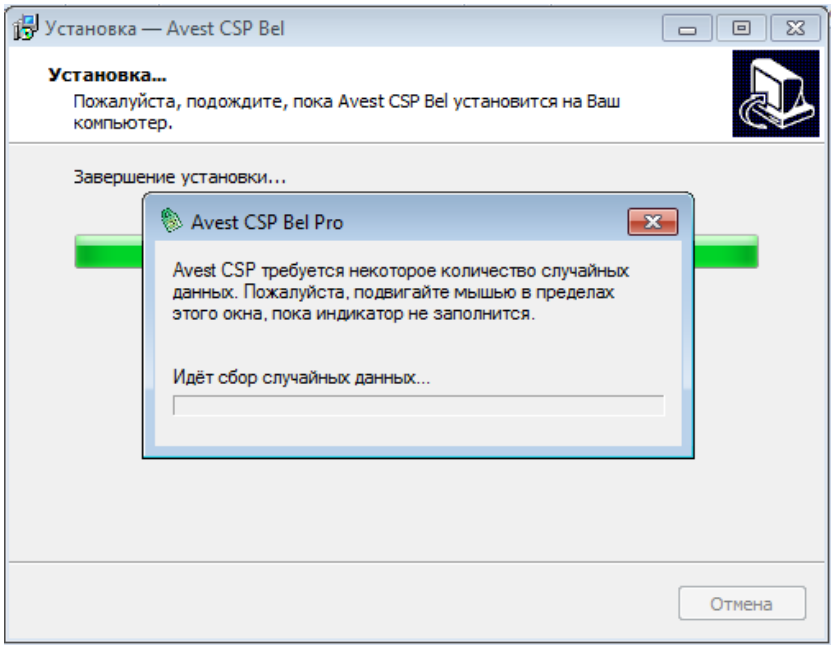

Рисунок 5 - Сбор случайных данных для регистрации криптопровайдера

На этом мастер установки криптопровайдера закончит свою работу, о чем сообщается в последнем окне (см. Рисунок 6 - Завершение установки криптопровайдера). Также необходимо выполнить перезагрузку, если мастер установки предлагает ее сделать.

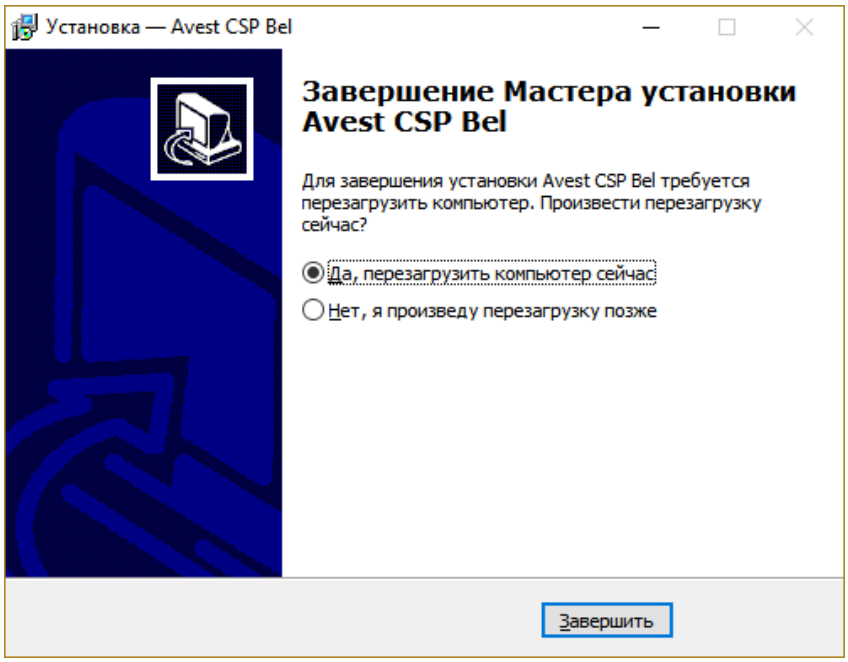

Рисунок 6 - Завершение установки криптопровайдера

После установки криптопровайдера на компьютер с:

- 32-разрядной операционной системой в меню «Пуск» ⇒»Программы»⇒ «Авест» появляется ярлык программы «Avest CSP Bel» (и/или «Avest CSP Bel (admin)»);

- 64-разрядной операционной системой в меню «Пуск» ⇒»Программы»⇒ «Авест» появляются ярлыки 64-разрядной программы «Avest CSP Bel x64» (и/или «Avest CSP Bel x64 (admin)»).и 32-разрядной программы «Avest CSP Bel» (и/или «Avest CSP Bel (admin)»).

3.2. Установка криптопровайдера с использованием командной строки

Программа инсталляции криптопровайдера поддерживает интерфейс командной строки. С его помощью можно задать список используемых носителей и файл-источник энтропии, что позволит инсталлировать криптопровайдер «не интерактивно», без отображения окон «мастера установки».

Для того что бы начать процесс установки криптопровайдера «не интерактивно», без отображения окна мастера установки, нужно запустить с дистрибутива программу «setupAvCSPBel6.3.0.8xx.exe, со следующими параметрами командной строки:

/verysilent - установить криптопровайдер «не интерактивно», т.е. без отображения на экране оконных интерфейсов «мастера установки».

/entropy=”любой файл более 64 байт” – использование указанного файла как источник энтропии, т.е. оператору не надо двигать мышью в пределах окна для сбора случайных данных **(**Рисунок 6 - Сбор случайных данных для регистрация криптопровайдера**)**.

Для того, чтобы задать список используемых носителей, поддержка которых должна быть установлена, (вместо окна выбора носителей см. Рисунок 3 - Выбор используемых носителей) необходимо при запуске инсталлятора указать параметр /devices. Его формат:

/devices=dev1,dev2,dev3

Здесь dev1, dev2 и dev3 – перечень носителей, подлежащих установке.

Можно указать в командной строке как полное имя используемого далее носителя, так и короткое условное обозначение (см. Таблица 1).

Таблица 1

Параметр указания полного имени носителя	Параметр указания короткого имени носителя
Avest Token	avToken
Avest Token Strong	avTokenStrong

Avest AvPass	avPass
"MIFARE Std Card 4K"	"MIFARE Std Card 4K"
Aladdin eToken (считыватель 0)	eToken0
Aladdin eToken (считыватель 1)	eToken1
Rainbow iKey1000/1032	iKey
Aktiv ruToken (считыватель 0)	ruToken0
Aktiv ruToken (считыватель 1)	ruToken1
Dallas TouchMemory (iButton) на COM1	iButton1
Dallas TouchMemory (iButton) на COM2	iButton2
Dallas TouchMemory (iButton) на COM3	iButton3
Dallas TouchMemory (iButton) на COM4	iButton4
ACOS3	acos

Например:

/devices=avToken,iKey,ruToken0,ruToken1,eToken0,eToken1,iButton1,iButton2,iButton3,iButton4

Первый указанный в строке носитель будет использоваться по умолчанию.

3.3. Работа с окном панели управления криптопровайдера

Окно панели управления криптопровайдера состоит из 2 закладок:

- «Носители»;
- «Версия».

На закладке «Носители» (см. Рисунок 7 - Закладка «Носители») отражена информация обо всех используемых носителях, которые поддерживает данный криптопровайдер.

Эта закладка разделена на 2 окна: «Используемые» и «Контейнеры на выбранном носителе».

На данной закладке предусмотрена возможность просмотра носителя личных ключей. Например, выбрав в верхнем окне «Используемые» - AvPass (с соответствующим серийным номером), и нажав на кнопку «Показать/обновить», в нижнем окне «Контейнеры на выбранном устройстве» можно увидеть все контейнеры личных ключей, находящиеся на данном носителе.

Вы также можете управлять контейнерами личных ключей на носителе: удалять, менять пароли, переименовывать ключевые контейнеры, производить контроль носителя.

Примечание: Носители некоторых производителей, например, Aladdin eToken имеют «по умолчанию» собственный пароль (пароль ОС носителя) с возможностью аппаратной блокировки доступа к носителю средствами самого носителя после некоторого количества попыток ввода неправильного пароля (см. документацию производителя). В силу этого все контейнеры на данных носителях личных ключей имеют одинаковый пароль, такой же, как пароль самого носителя, а количество попыток ввода пароля на доступ к контейнеру ограничено параметрами носителя при его форматировании.

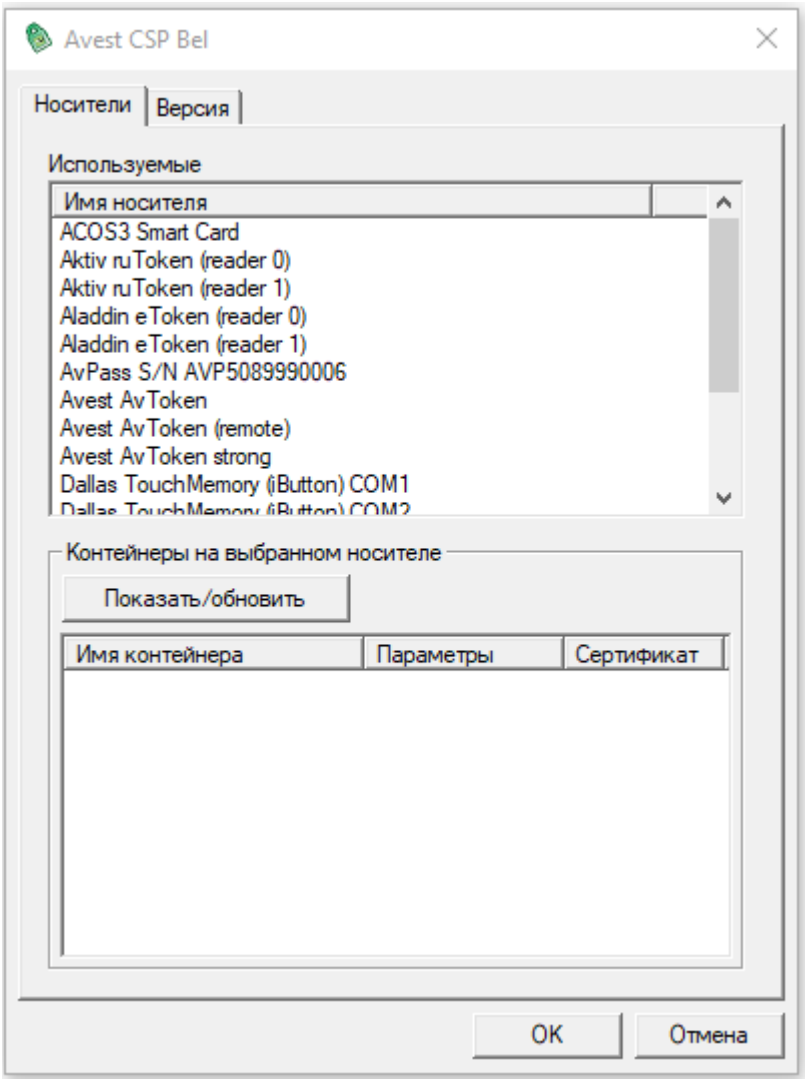

Рисунок 7 - Закладка «Носители»

Для этого надо в окошке «Контейнеры на выбранном носителе» выбрать контейнер личных ключей и щелкнув по нему правой клавишей мыши во всплывающем меню выбрать нужный вам пункт.

Если пользователь не уверен в сохранности своего пароля к контейнеру с личным ключом, то он может сменить его.

Действия по смене пароля к контейнеру с личным ключом:

1) На закладке «Носители» в окне «Контейнеры на выбранном устройстве» выбрать контейнер личного ключа, к которому необходимо сменить пароль;

2) Щелкнув по нему правой клавишей мыши вызвать всплывающее меню, в котором выбрать пункт «Сменить пароль»;

3) В появившемся окне требуется ввести текущий пароль, новый пароль и его подтверждение (см. Рисунок 8 - Смена пароля к контейнеру с личным ключом).

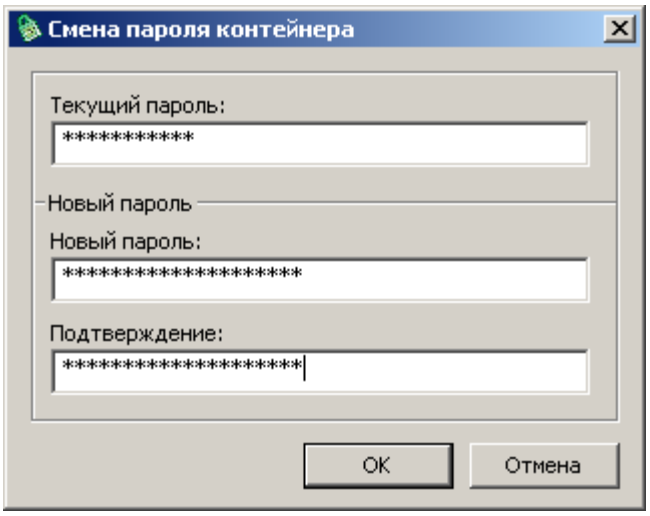

Рисунок 8 - Смена пароля к контейнеру с личным ключом

Примечания:

1. Носитель личных ключей eToken имеет по умолчанию пароль от 1 до 0. Все контейнеры на носителе личных ключей eToken имеют одинаковый пароль, такой же, как пароль самого носителя.

2. Смена пароля к носителю личных ключей eToken должна производиться только с помощью криптопровайдера AvestCSPBel, если при смене пароля будут использоваться аналогичные средства от Aladdin это приведет к невозможности дальнейшего использования данного носителя.

3. Для носителя AvPass смена пароля производится не к отдельному контейнеру, а сразу ко всему носителю.

Для того, чтобы сменить пароль для носителя eToken нужно на закладке «Носители» в окне «Используемые носители» выбрать носитель личного ключа и хранящийся на нем криптоконтейнер, пароль на доступ к которому необходимо сменить.

Щелкнув по нему правой клавишей мыши вызвать всплывающее меню, в котором выбрать пункт «Сменить пароль». В появившемся окне требуется ввести текущий пароль, новый пароль и его подтверждение.

Для того, чтобы переименовать ключевой контейнер нужно на закладке «Носители» в окне «Используемые носители» выбрать носитель личного ключа и хранящийся на нем криптоконтейнер, название которого необходимо изменить.

Необходимо щелкнуть по нему правой клавишей мыши, вызвав контекстное (всплывающее) меню. В нем выбрать пункт «Переименовать». В строке редактирования написать желаемое название криптоконтейнера и подтвердить переименование в появившемся окне.

Если сертификат оператора записан в контейнер с личным ключом, то его можно просмотреть или импортировать.

Включенный пункт всплывающего меню «Контроль носителя» означает, что каждый раз, при обращении к носителю личных ключей оператора, будет проверяться наличие вставленного в считыватель носителя личных ключей оператора.

В верхнем окне «Используемые» закладки «Носители» можно просмотреть информацию о регистрации данного носителя, см. п. 3.4. Регистрация носителя.

3.4. Регистрация носителя

В случае использования неактивированного (незарегистрированного) НКИ необходимо предварительно провести его регистрацию. Для проверки наличия регистрации НКИ необходимо в окне «Используемые» выбрать интересующий вас носитель и щелкнув по нему правой клавишей мыши вызвать всплывающее меню.

Если во всплывающем меню выбран пункт «Информация о регистрации», то появится окно, в котором отражена информация о регистрации носителя (см. Рисунок 9 - Информация о регистрации носителя).

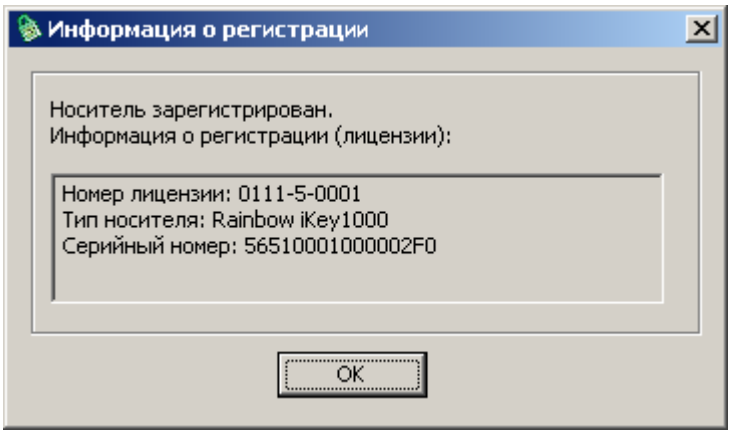

Рисунок 9 - Информация о регистрации носителя

Если носитель не зарегистрирован, то появится окно «Регистрация носителя» (см. Рисунок 10 - Регистрация носителя. Выбор действия).

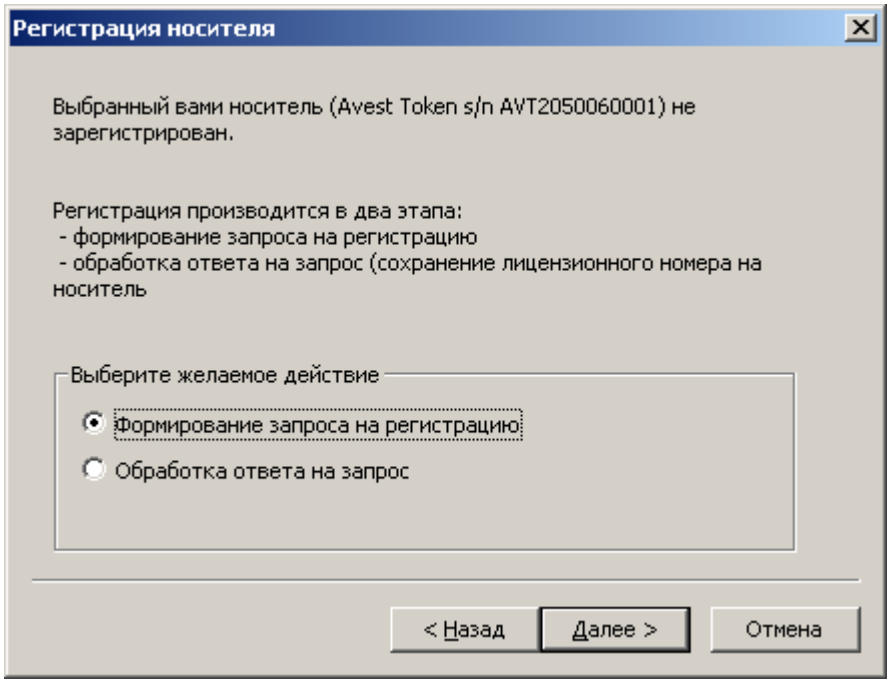

Рисунок 10 - Регистрация носителя. Выбор действия

В этом окне нужно нажать кнопку «Далее». В следующем окне нужно ввести PIN-код, который поставляется вместе с используемым НКИ, и нажать «Далее» (см. Рисунок 11 - Регистрация носителя. Ввод PIN-кода для активации).

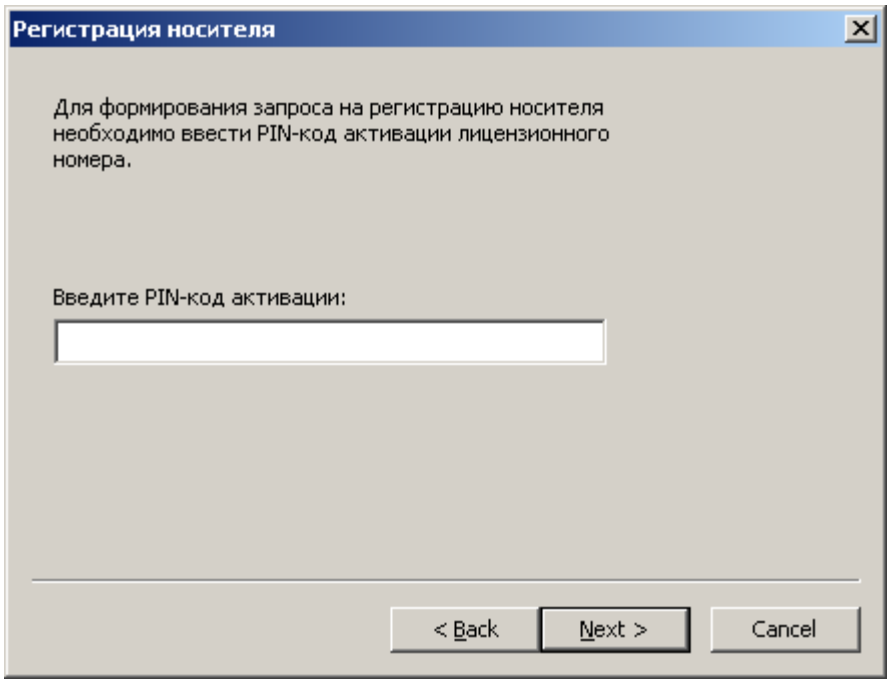

Рисунок 11 - Регистрация носителя. Ввод PIN-кода для активации

Далее появится окно, в котором будет показан ваш запрос на регистрацию (см. Рисунок 12 - Регистрация носителя. Содержание запроса). Этот запрос нужно скопировать и отправить по электронной почте token_reg@avest.by.

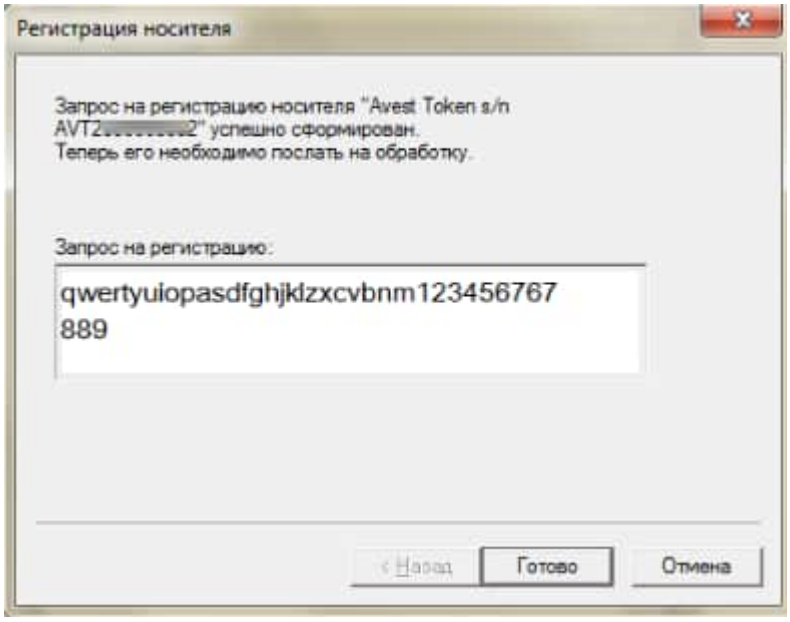

Рисунок 12 - Регистрация носителя. Содержание запроса

После этого на ваш электронный ящик придёт ответ. Нужно открыть окно криптопровайдера, щелкнуть на носителе правой кнопкой мыши, затем выбрать пункт «Информация о регистрации», в появившемся окне «Регистрация носителя» выбрать «Обработка ответа на запрос» и нажать «Далее».

Далее, в появившееся окно, нужно вставить ответ, пришедший по электронной почте и нажать «Завершить».

3.5. Контроль компонентов криптопровайдера AvCSPBEL

Для контроля программных компонентов криптопровайдера AvCSPBEL используются средства контроля, интегрированные в криптопровайдер и доступные оператору с помощью GUI-интерфейса криптопровайдера в закладке «Версия». На данной закладке расположены кнопка «Обновить регистрацию компонентов в системном реестре» и 2 окна: «Информация о продукте» и «Версии компонентов» (см. Рисунок 13 - Закладка «Версия»).

Окно «Информация о продукте» содержит данные о названии и версии криптопровайдера AvCSPBEL, а также контактную информацию разработчика.

Кнопка «Обновить регистрацию компонентов в системном реестре» производит действия по регистрации компонентов криптопровайдера в реестре, аналогичные тем, что выполняются при инсталляции. С её помощью можно восстановить работоспособность криптопровайдера в случае некорректного обновления или удаления связанных с криптопровайдером компонентов.

Окно «Версии компонентов» содержит список основных системных библиотек, а также библиотек, входящих в состав криптопровайдера AvCSPBEL с указанием их версий и контрольных характеристик в виде хэш-значений согласно СТБ 34.101.31-2020.

Данные средства контроля предназначены для контроля версий и целостности программных компонентов криптопровайдера AvCSPBEL оператором путем визуального сравнения хэш-значений, отображаемых в окне, с эталонными значениями.

Эталонные значения могут быть получены путем копирования хэш-значений из данного окна и сохранения в файл сразу после установки криптопровайдера AvCSPBEL с доверенного носителя, либо по запросу у разработчика криптопровайдера AvCSPBEL, либо на сайте разработчика криптопровайдера AvCSPBEL.

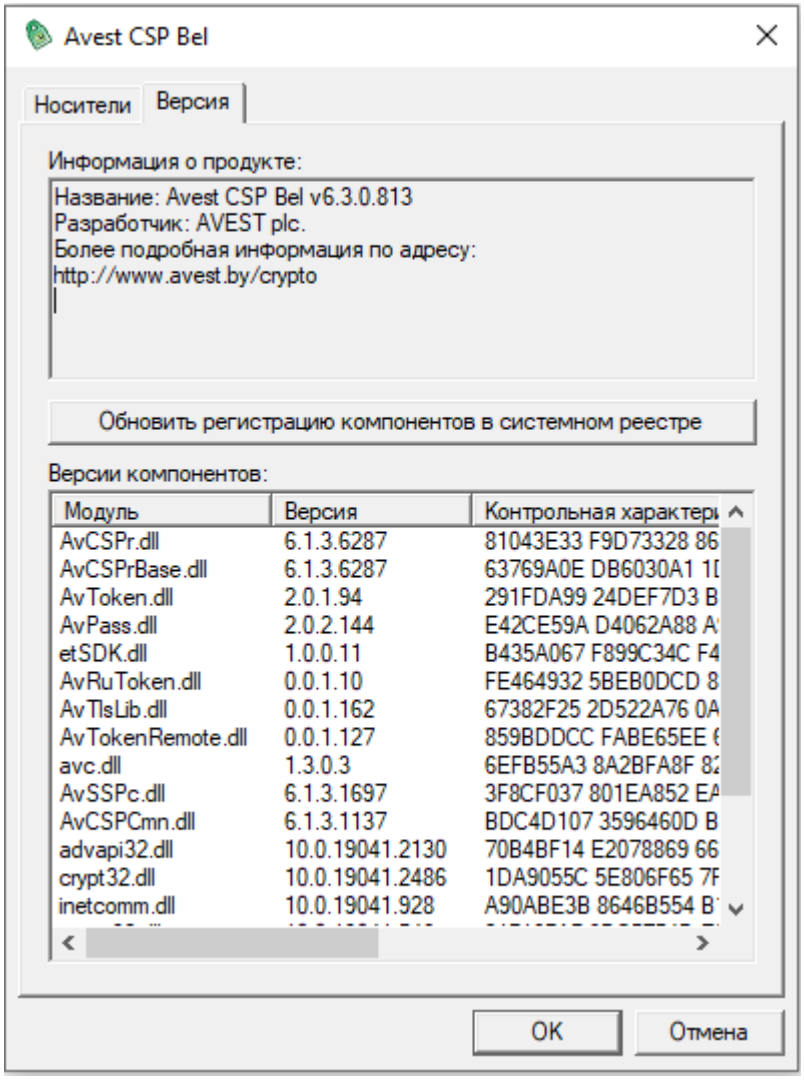

Рисунок 13 - Закладка «Версия»

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.

4. 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.

Данные требования направлены на достижение следующих целей:

– предупреждение нарушений целостности и подлинности программных компонентов криптопровайдера AvCSPBEL;

– обеспечение защиты криптографических ключей и данных потребителя от компрометации;

– обеспечение надежного функционирования криптопровайдера AvCSPBEL.

4.1. Меры безопасности при поставке

Передача программного обеспечения криптопровайдера AvCSPBEL (далее - 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», необходимо 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.

4.2. 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 эталонные хэш-значения 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 на доступ к данным на НКИ должен храниться в тайне. Запрещается сообщать кому-либо значение пароля. При смене сотрудника, работающего с НКИ, новый сотрудник в первую очередь должен сменить пароль на доступ 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 инсталлированы программные компоненты ПО, производится только после уничтожения на нем ПО путем форматирования накопителя информации.

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 «АВЕСТ» (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 аудита ОС;
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».

5. СОКРАЩЕНИЯ

НКИ – носитель ключевой информации;

ОС – операционная система;

ПО – программное обеспечение;

ПСКЗИ – программное средство криптографической защиты информации;

СКЗИ – средство криптографической защиты информации;

ЭЦП – электронная цифровая подпись;

TLS (Transport Layer Security) – протокол защиты транспортного уровня, определенный в СТБ 34.101.65.

Лист регистрации изменений									
Номер листов (страниц)					Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм	Измененных	Замененных	Новых	Аннулированных					