УТВЕРЖДЕН

РБ.ЮСКИ.08000-02 34 01-ЛУ

ПРОГРАММНОЕ СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «КРИПТОПРОВАЙДЕР Avest CSP»

AvCSP

ver. 6.1.0.699

Руководство оператора

РБ.ЮСКИ.08000-02 34 01

Листов 34

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

2013

АННОТАЦИЯ

Данный документ содержит руководство оператора РБ.ЮСКИ.08000-02 «Программное средство криптографической защиты информации «криптопровайдер Avest CSP» ver. 6.1.0.699 (далее – криптопровайдер AvCSP). В документе содержится информация и приведена последовательность действий оператора при установке программного средства. А также приведены тексты сообщений, выдаваемых в ходе установки, описание их содержания и соответствующих действий оператора.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

В операционных системах Windows компании Microsoft возможность выполнения приложениям 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 осуществления универсальности доступа приложений к криптографических сервисам и независимости вызова криптографических функций от реализации криптографических алгоритмов и их типов, ОС Windows содержит 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 AvCSP 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:

– ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

– СТБ 1176.1–99 «Информационная технология. Защита информации. Процедура хэширования»;

– СТБ 1176.2–99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи»;

– проект РД РБ «Банковские технологии. Протоколы формирования общего ключа»;

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

– СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности» (хэширование).

Криптопровайдер AvCSP 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 AvCSP 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 Avest CSP» включает компоненты «Avest CSP» и «Avest CSP Base», регистрирующиеся в CryptoAPI как Cryptographic Service Provider типов 420 и 421 соответственно. Отличием поведения криптопровайдеров указанных типов является способ вычисления ЭЦП согласно СТБ 1176.2-99 – без использования дополнительного хэширования (тип 420) и с использованием (тип 421).

Использование возможностей 420 или 421 типа криптопровайдера прозрачно для пользователя и определяется потребностью прикладного программного обеспечения в использовании сервисов криптопровайдера AvCSP.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Криптопровайдер AvCSP предназначен для работы на ПЭВМ (ЭВМ), функционирующей под управлением одной из следующих ОС MS Windows:

- Windows 2003 Server (x32, x64) SP1 или выше;
- Windows XP SP3 (x32);
- Windows XP SP2 (x64);
- Windows Vista SP1/SP2 (x32, x64);
- Windows 7 (x32, x64);
- Windows 8 (x32, x64);
- Windows 8.1 (x32, x64);
- Windows 2008 R1 Server (x32, x64);
- Windows 2008 R2 Server (x64);
- Windows 2012 Server (x64);
- Windows 2012 R1 Server (x64)

2.2. Криптопровайдер AvCSP предназначен для работы на ПЭВМ (ЭВМ), имеющей следующие минимальные технические характеристики:

- процессор 486DX с тактовой частотой - не менее 66 МГц;
- объем ОЗУ - не менее 16 Мбайт;
- жесткий диск, содержащий не менее 195 Мбайт свободного пространства для стандартной установки ОС;
- монитор с поддержкой VGA или более высокого разрешения;
- манипулятор «мышь» Microsoft или совместимое указывающее устройство.

Для использования криптопровайдера AvCSP с функциями Microsoft CryptoAPI 1.0, 2.0 и CAPICOM требуется наличие установленного Microsoft Internet Explorer версии 6.0 и выше.

2.3. В качестве отчуждаемого носителя ключевой информации (далее НКИ) криптопровайдер AvCSP поддерживает следующие типы устройств:

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

- iButton;
- iKey;
- eToken;
- ruToken;
- смарт-карта Acos3;
- бесконтактная карта MIFARE Std 4K;
- дискета.

Примечания:

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

2. Для корректной работы криптопровайдера AvCSP с НКИ, необходимо до установки на ПЭВМ (ЭВМ) криптопровайдера AvCSP, 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.

2.4. 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.

Примечания:

1. Криптопровайдер AvCSP, 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 AvCSP обеспечивает уничтожение криптоконтейнера на НКИ после 7 (семи) попыток ввода неправильного пароля на доступ к криптоконтейнеру.

4. Криптопровайдер AvCSP поддерживает работу с НКИ AvToken в режиме **remote**, обеспечивающим взаимодействие криптопровайдера с НКИ, подключенным к другой ПЭВМ.

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

6. AvToken Remote используется, если нет возможности работать с AvCSP непосредственно на ПЭВМ и существует возможность подключения к удалённому рабочему столу с помощью стандартных средств ОС Windows.

7. Работа с AvToken Remote доступна при наличии:
   - на рабочем месте оператора - установленного и настроенного криптопровайдера AvCSP с поддержкой AvToken Remote;
   - на удаленном рабочем столе - установленного ПО AvToken Server (поставляется отдельно по согласованию с потребителями) и подключенного AvToken.

8. Работа с носителем AvToken в режиме remote осуществляется с использованием незащищённого канала связи (сети Ethernet), поэтому использование НКИ в этом режиме должно осуществляться с соблюдением организационно-технических мер, препятствующих

несанкционированному доступу к каналу связи, использующимся для обмена данными с AvToken Remote.

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

10. Работа в 64-разрядном AvCSP возможна только с устройствами AvToken и AvPass. С остальными типами носителей можно работать только в 32-разрядном AvCSP.

3. УСТАНОВКА И ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Установка криптопровайдера Avest CSP

В зависимости от битности операционной системы криптопровайдер Avest CSP после установки будет выглядеть по-разному:

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

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

Действия по установке криптопровайдера:

1) Запустить с дистрибутива программу «setupAvCSP6.1.0.699.exe;

2) В первом окне мастера установки содержится описание устанавливаемого продукта, для начала установки программы на компьютер нажмите кнопку «Далее» (см. Рис. 1).

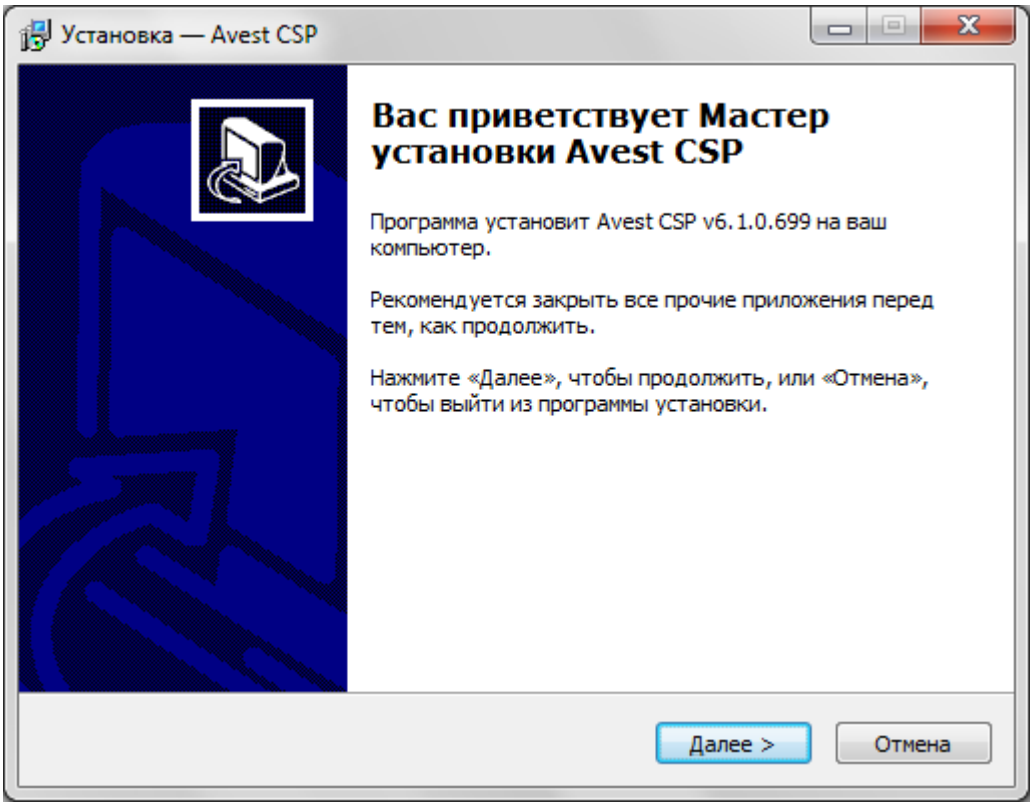

Рисунок 1 – Заставка мастера установки криптопровайдера

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) После этого надо определить основной каталог, в котором будут расположены устанавливаемые компоненты, и нажать кнопку «Далее». По умолчанию установка программы производится в каталог «\Program Files(x86)\Avest\ Avest CSP» на системном диске для 32 разрядного криптопровайдера и в каталог «\Program Files\Avest\ Avest CSP» для 64 разрядного криптопровайдера. (см. Рис. 2).

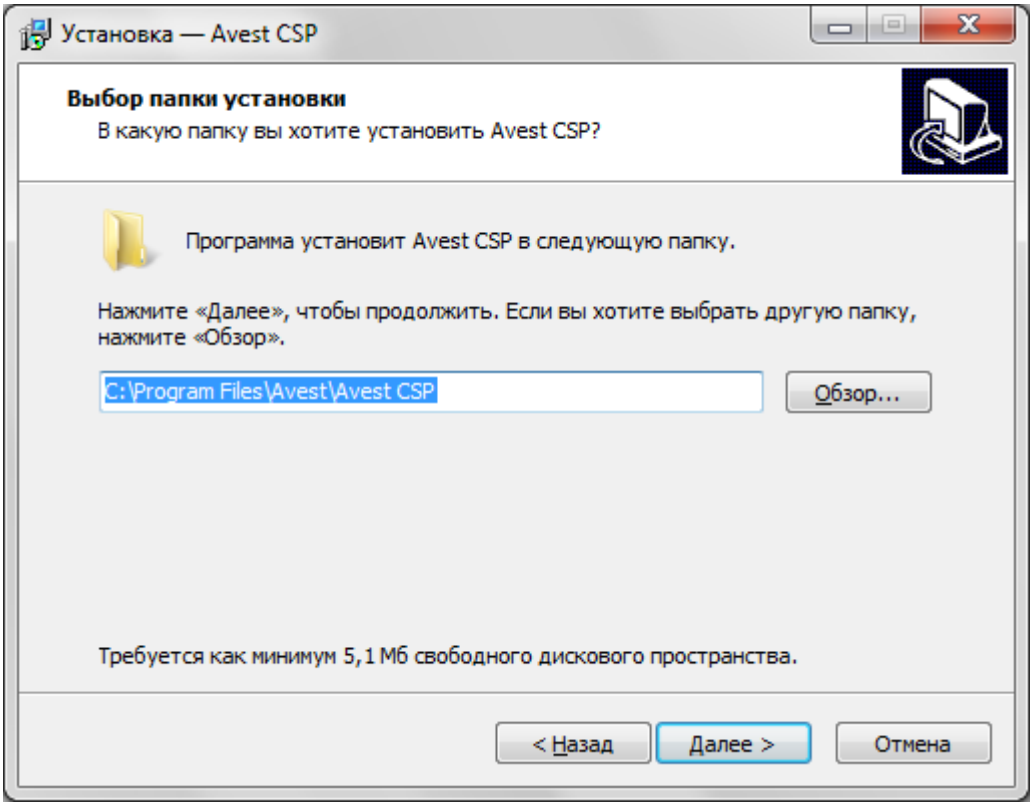

Рисунок 2 –Выбор каталога установки

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

Название папки Вы можете указать как вручную, так и при помощи кнопки «Обзор». По умолчанию будет создана папка «Авест» (См. Рис.3).

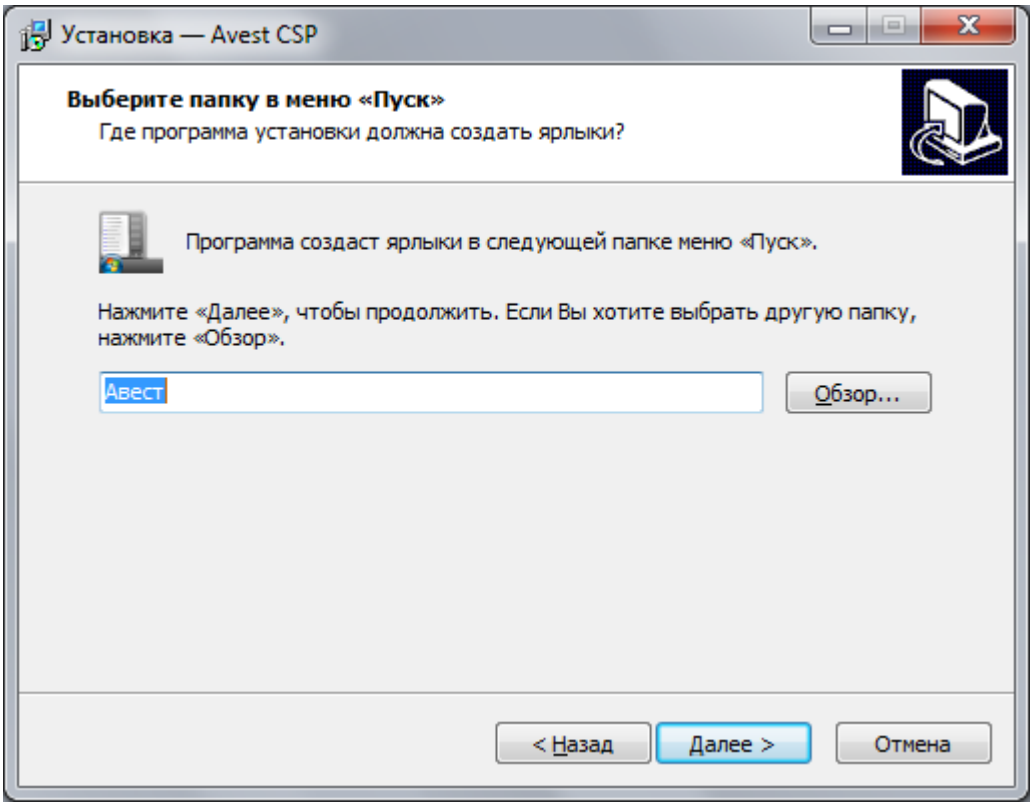

Рисунок 3 - Выбор папки для создания ярлыков в меню «Пуск»

6) На следующей странице мастера установки предлагается выбрать тип носителя, который будет использоваться для хранения личных ключей по умолчанию (Это значит что при создании личного ключа первым будет предложен этот носитель) (См. Рис. 4).

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 Avest CSP возможна только с устройствами AvToken и AvPass. С остальными типами носителей можно работать только в 32-разрядном Avest CSP.

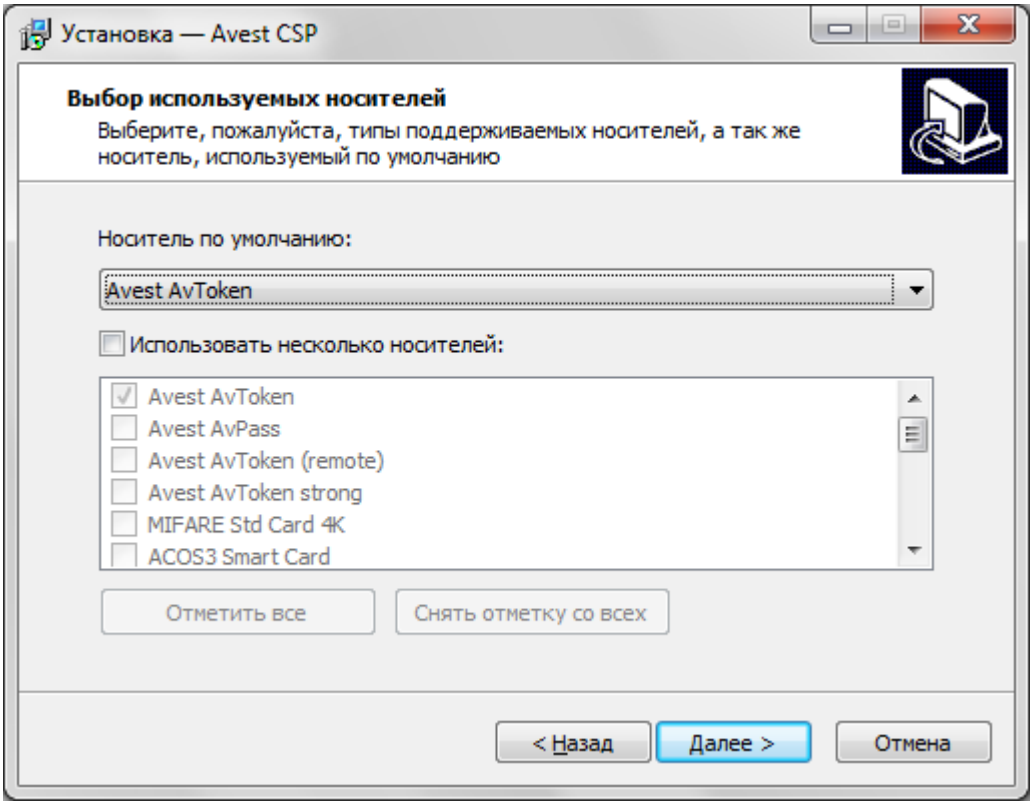

Рисунок 4 - Выбор носителя личных ключей по умолчанию.

7) 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. Рис. 5). Если пользователь согласен с указанными в данном окне параметрами, то надо нажать кнопку «Установить».

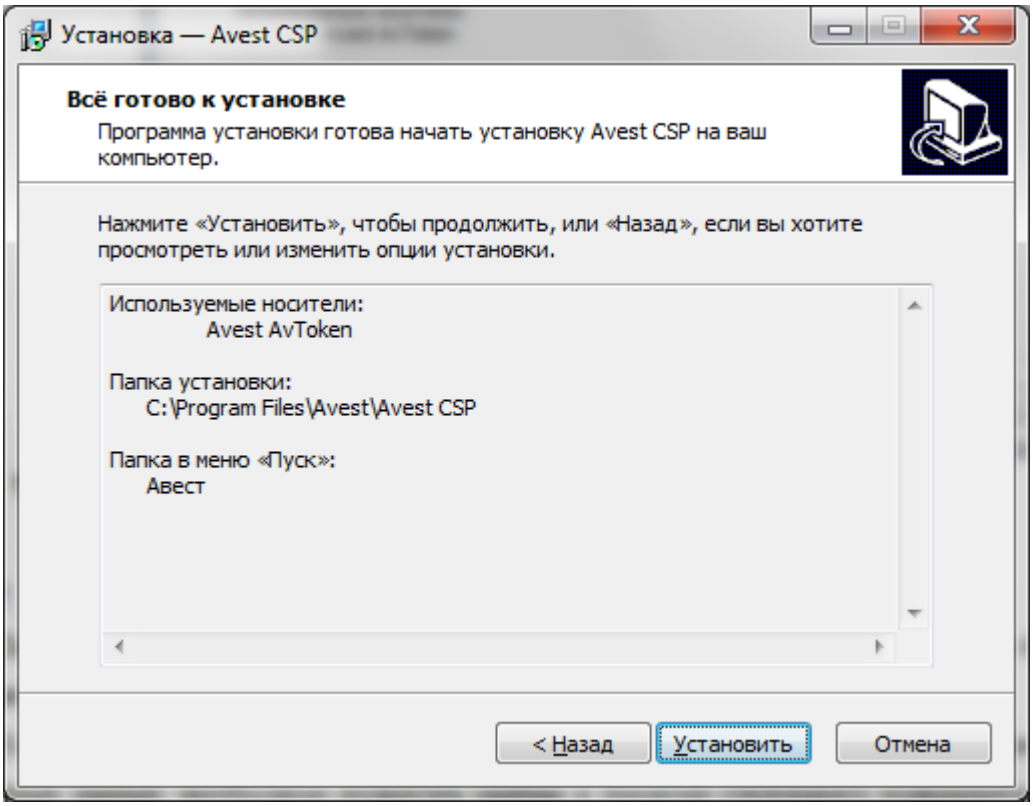

Рисунок 5 - Установка криптопровайдера на компьютер

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

8) Далее необходима регистрация криптопровайдера, для этого нужно некоторое количество случайных данных, необходимо подвигать мышью в пределах следующего появившегося окна. (См. Рис. 6) .

Примечание. При повторной инсталляции данное окно появляться не будет.

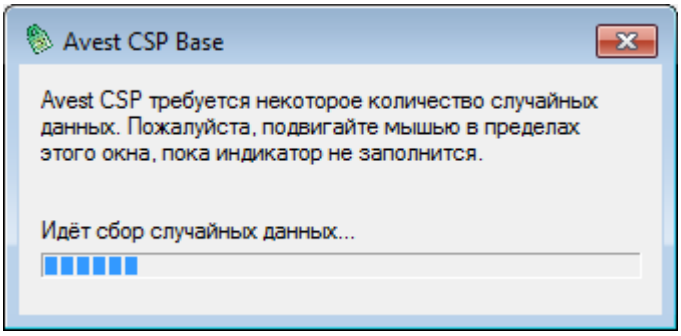

Рисунок 6 - Сбор случайных данных для регистрация криптопровайдера

На этом мастер установки криптопровайдера закончит свою работу, о чем сообщается в последнем окне (См. Рис. 7).

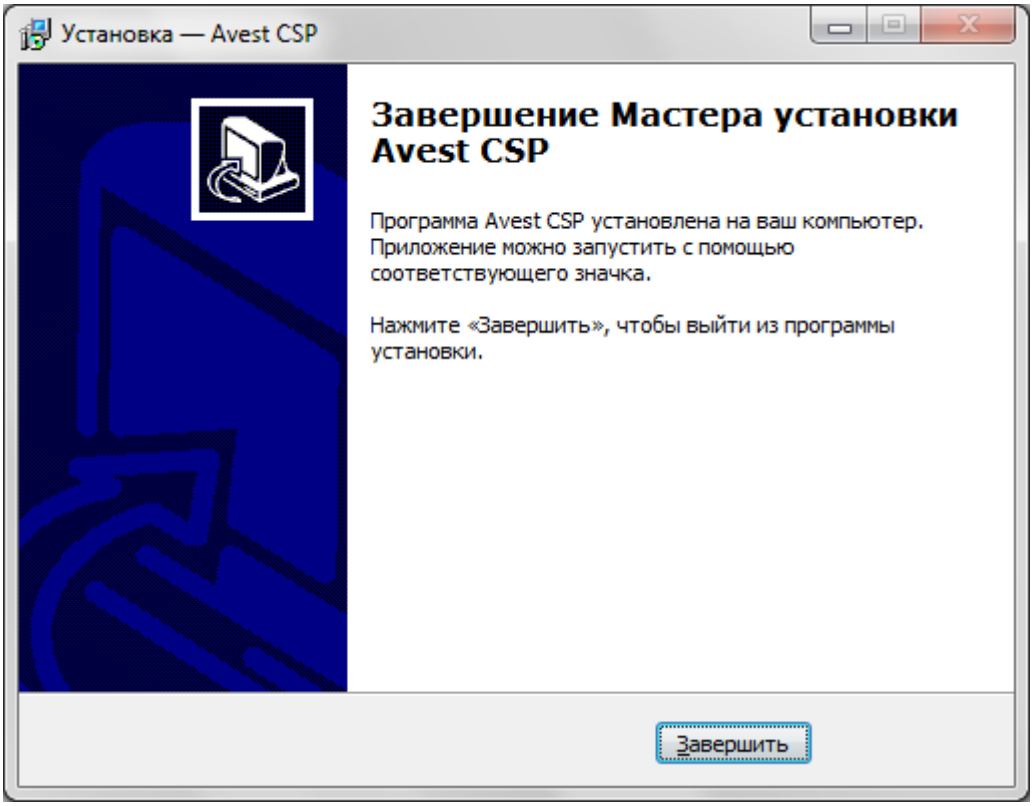

Рисунок 7 - Завершение установки криптопровайдера

После установки криптопровайдера на компьютер с:

- 32 разрядной операционной системой в меню «Пуск» ⇒»Программы»⇒ «Авест» появляется ярлык программы «Avest CSP».

- 64 разрядной операционной системой в меню «Пуск» ⇒»Программы»⇒ «Авест» появляются ярлыки 64 разрядной программы «Avest CSP x64» и 32 разрядной программы «Avest CSP»

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 «тихо», без отображения окна мастера, нужно запустить с дистрибутива программу «setupAvCSP6.1.0.699.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” – использует указанный файл 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. Рис. 4) 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, например:

Таблица 1.

Параметр указания полного имени носителя	Параметр указания короткого имени носителя
Avest Token	avToken
Avest Token Remote	avTokenRemote
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
Диск A	floppy
ACOS3	acos

Например:

/devices=avToken,iKey,"MIFARE Std Card 4K",ruToken0,ruToken1,eToken0,eToken1,iButton1,iButton2, iButton3,iButton4,floppy

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. Рис. 8) отражена информация обо всех используемых носителях, которые поддерживает данный криптопровайдер.

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

На данной закладке предусмотрена возможность просмотра носителя личных ключей. Например, выбрав в верхнем окошке «Используемые носители» - Dallas TouchMemory (iButton) на COM2, и нажав на кнопку «Показать/обновить», в нижнем окошке «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

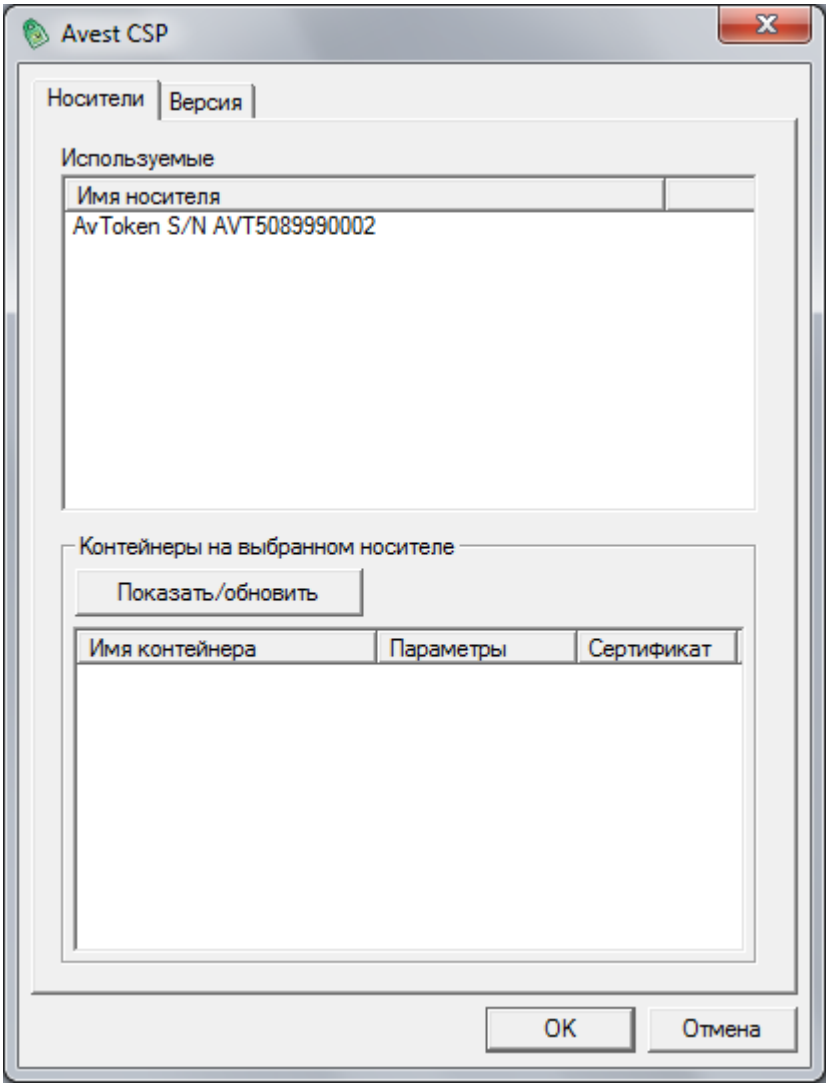

Рисунок 8 - Закладка «Носители»

Для этого надо в окошке «Контейнеры на выбранном устройстве» 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 окошке требуется ввести текущий пароль, новый пароль и его подтверждение (см. Рис. 9).

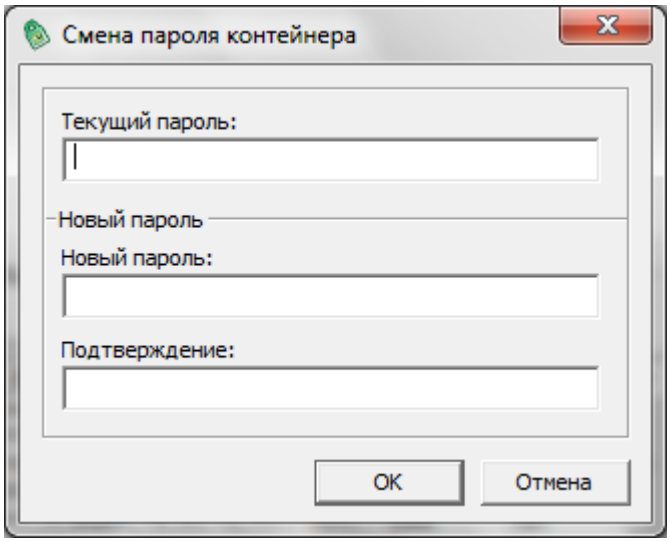

Рисунок 9 - Смена пароля к контейнеру с личным ключом

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 AvestCSP, 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 окошке 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 личного ключа, 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 носители» закладки «Носители» можно просмотреть информацию о регистрации данного носителя.

3.4. Регистрация носителя

Для регистрации носителя необходимо в окне «Используемые носители» 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 окошко, в котором отражена информация о регистрации носителя (см. Рис.10).

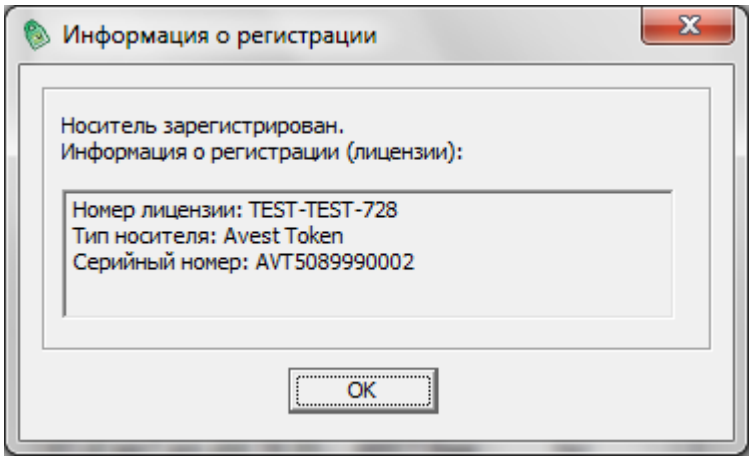

Рисунок 10 - Информация о регистрации носителя

Если носитель не зарегистрирован, то появится окно «регистрация носителя»

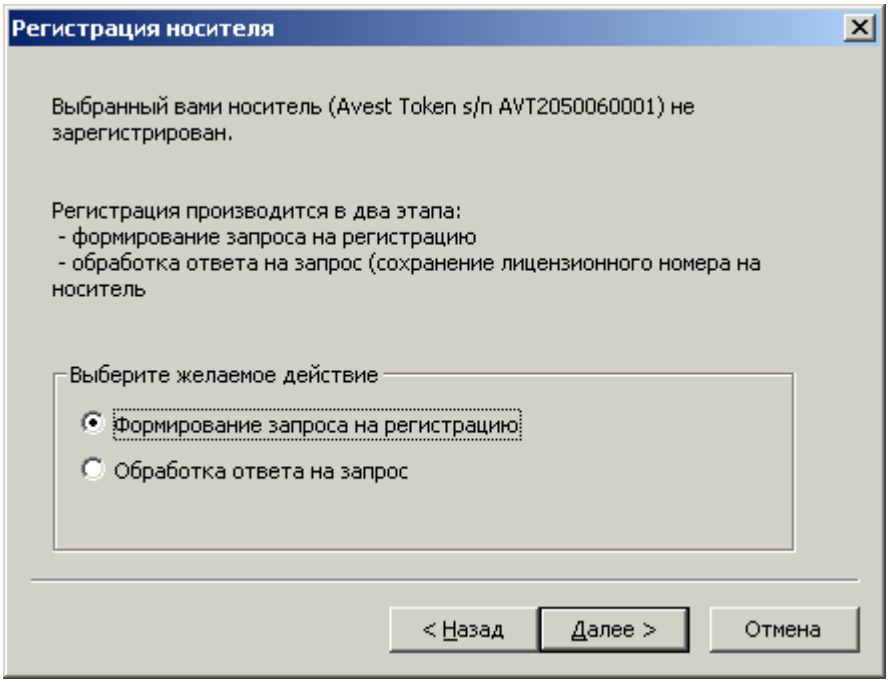

Рисунок 11 - Регистрация носителя. Выбор действия.

В этом окне нужно нажать кнопку «Next». В следующем окне нужно ввести PIN-код, который поставляется вместе с криптопровайдером «Авест», и нажать «Next».

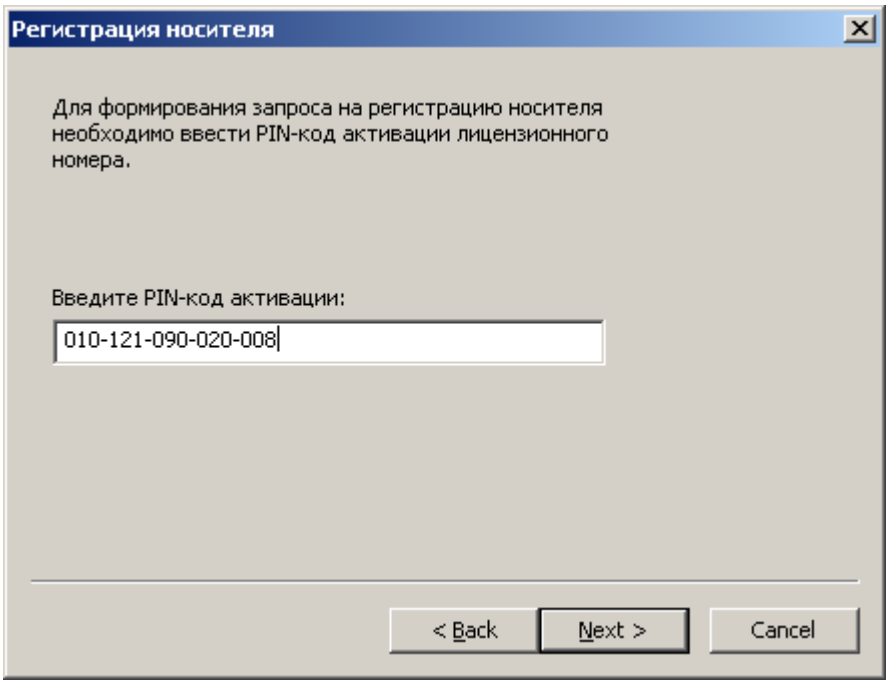

Рисунок 12 - Регистрация носителя. Ввод PIN-кода для активации.

Далее появится окно, в котором будет показан ваш запрос на регистрацию. Этот запрос нужно скопировать и отправить по электронной почте **token_reg@avest.by**.

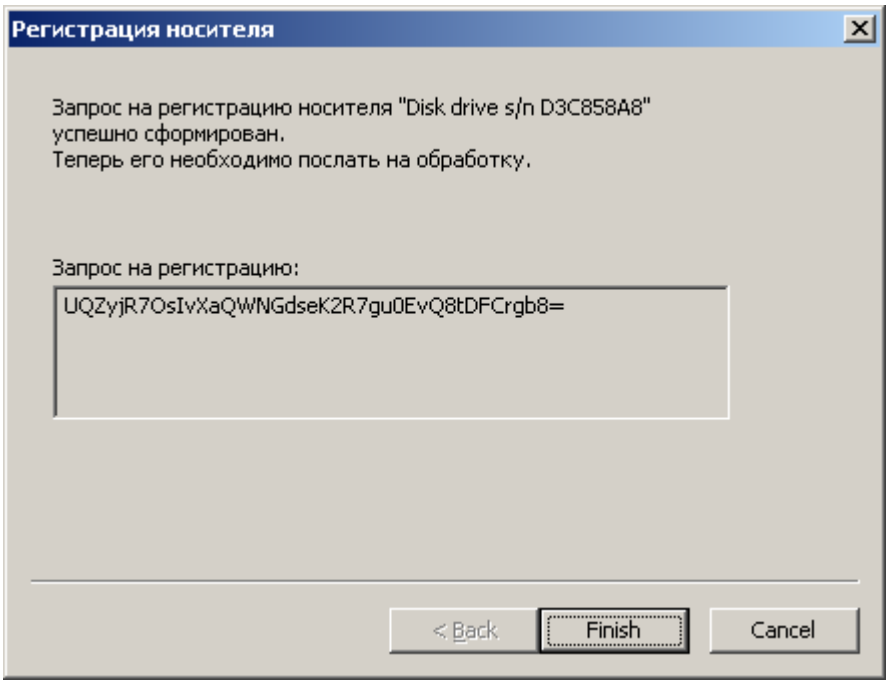

Рисунок 13 - Регистрация носителя. Содержание запроса.

После этого на электронный ящик придёт ответ. Нужно открыть окно криптопровайдера, щелкнуть на носителе правой кнопкой мыши, затем выбрать пункт «информация о регистрации» и

появится окно «регистрация носителя», в котором нужно выбрать «обработка ответа на запрос» и нажать «Next»

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

3.5. Контроль криптопровайдера AvCSP

Для контроля целостности программных компонентов криптопровайдера AvCSP и тестирования реализованных криптоалгоритмов оператором используется утилита AvTestCSP.exe. Данная утилита включается в поставку с криптопровайдером по согласованию с заказчиком.

Данная утилита предназначена для использования оператором криптопровайдера AvCSP с целью тестирования правильности функционирования криптографических компонентов криптопровайдера и контроля целостности программных модулей криптопровайдера AvCSP. Пример работы данной утилиты изображен на рис. 14.

Для работы утилиты AvTestCSP.exe ее необходимо поместить в папку по пути установки криптопровайдера. Запуск утилиты производится из командной строки, результаты работы выводятся на экран, а также в файл (при использовании перенаправления стандартного вывода в файл).

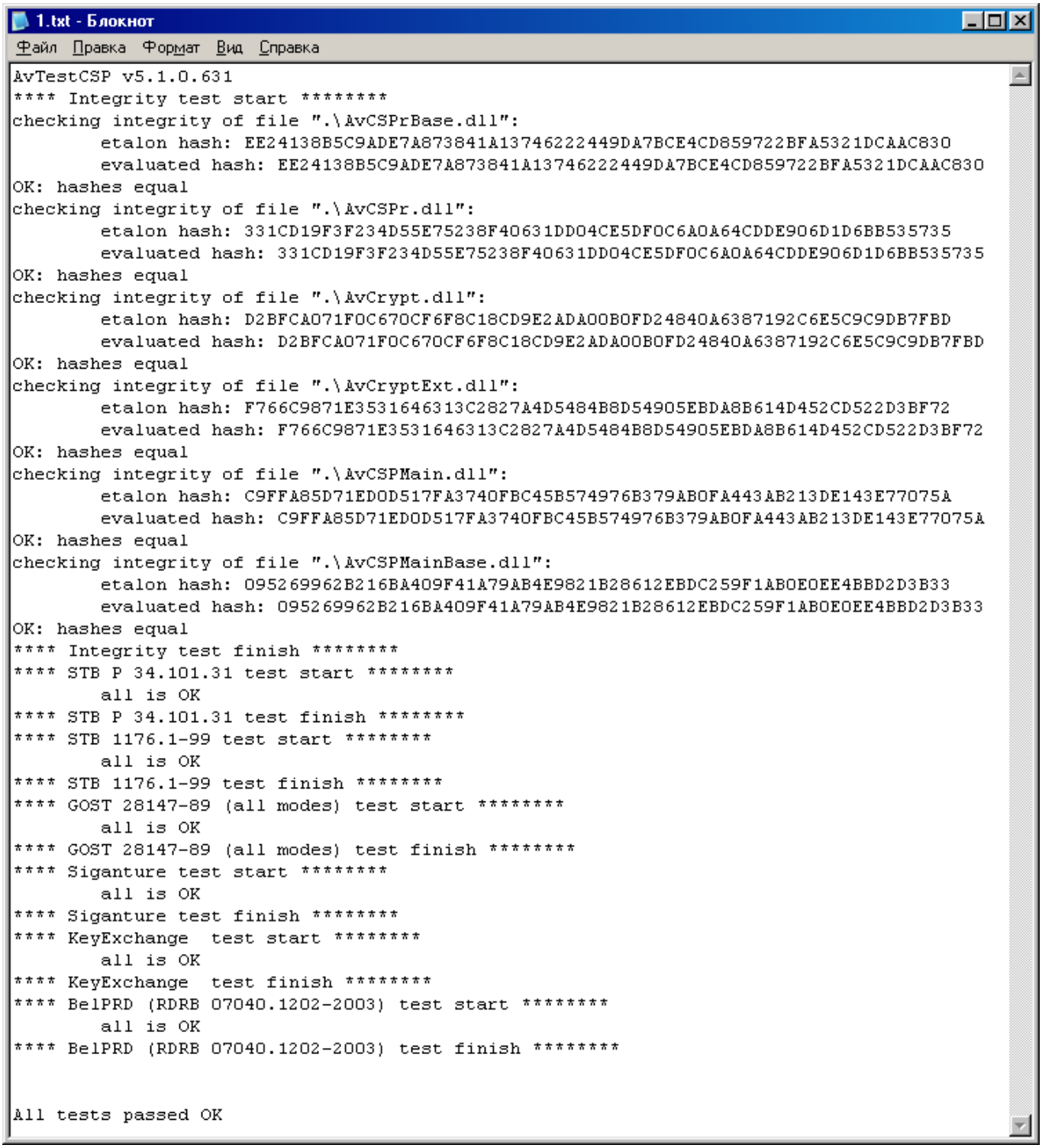

Рисунок 14 - Результаты работы утилиты AvTestCSP.exe

Оператор может воспользоваться данной утилитой в ситуации, когда необходимо убедиться в работоспособности криптопровайдера, а также в любой другой момент времени.

Для вспомогательного контроля программных компонентов криптопровайдера AvCSP используются средства контроля интегрированные в криптопровайдер и доступные оператору с помощью GUI-интерфейса криптопровайдера в закладке «Версия». Данная закладка состоит из кнопки «Обновление регистрации компонентов системном реестре» и 2 окон: «Информация о продукте» и «Версии компонентов».(см. Рис. 15).

Окно «информация о продукте» содержит данные о названии и версии криптопровайдера AvCSP, 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 той или иной прикладной СКЗИ.

Окно «Версии компонентов» содержит список основных системных библиотек, а также библиотек, входящих в состав криптопровайдера AvCSP с указанием их версий и контрольных характеристик в виде хэш-значений согласно СТБ 1176.1-99 со стартовым вектором хэширования в шестнадцатеричном виде – AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA (32 байта).

Данные средства контроля дополняют возможности утилиты AvTestCSP.exe и предназначены для контроля версий и целостности программных компонентов криптопровайдера AvCSP 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 AvCSP с доверенного носителя, средствами утилиты AvTestCSP.exe, либо по запросу у разработчика криптопровайдера AvCSP.

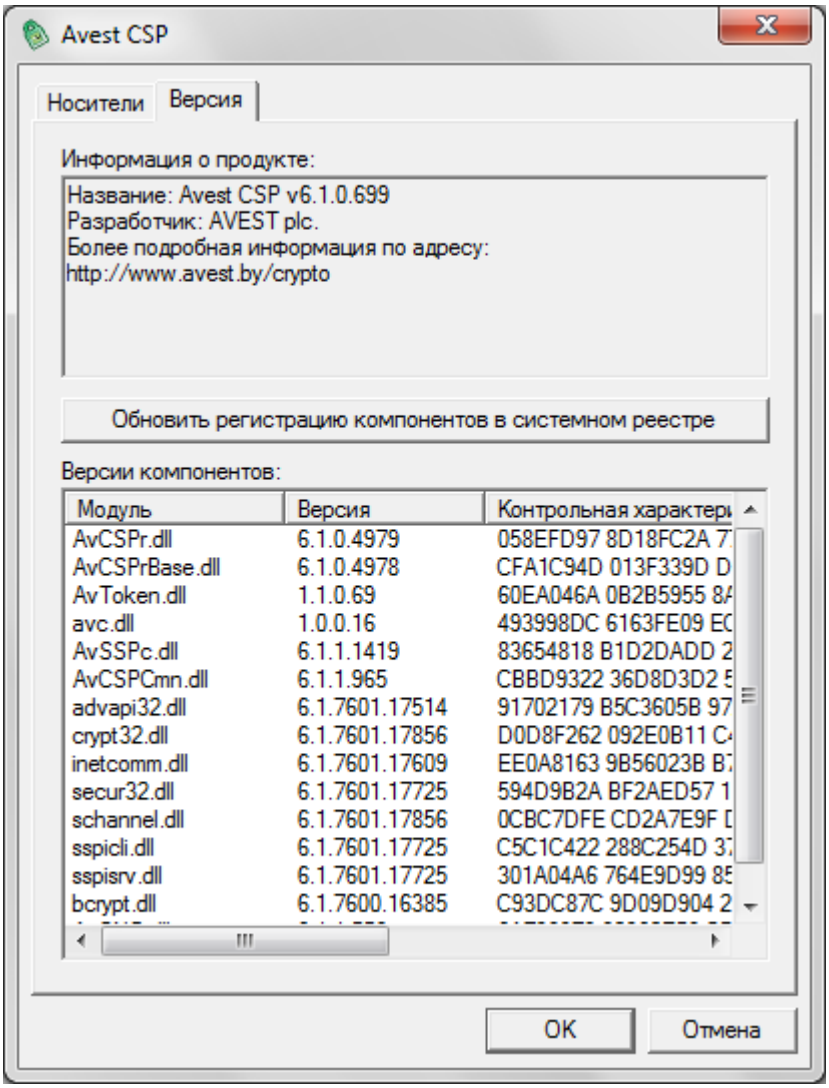

Рисунок 15 - Закладка «Версия»

3.6. Сообщение оператору

Криптопровайдер AvCSP 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 AvCSP, которым должны следовать потребители в процессе приобретения и использования криптопровайдера AvCSP.

Данные требования направлены на достижение следующих целей:

– предупреждение нарушений целостности и подлинности программных компонентов криптопровайдера AvCSP;

– обеспечение защиты криптографических ключей и данных потребителя от компрометации;

– обеспечение надежного функционирования криптопровайдера AvCSP.

4.1. Меры безопасности при поставке

Передача программного обеспечения криптопровайдера AvCSP (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;

– 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 РБ 1176.1-99 «Информационная технология. Защита информации. Процедура хэширования»;

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

– ПО содержит механизмы, указанные в данном документе позволяющие потребителю контролировать версии и текущие 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 http://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 ПЭВМ 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 согласно процедуре указанной в предыдущем разделе данного документа;

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

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

– после установки ПО, отчуждаемый носитель (компакт-диск CD-R) с эталонным установочным файлом ПО и эталонные хэш-значения программных компонентов (см. п. 3.5) должны быть помещены в безопасное хранилище, доступ к которому должен иметь только уполномоченный персонал потребителя.

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

– сотрудник, эксплуатирующий ПО должен быть предупрежден о гражданской, правовой и финансовой 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» или в иных случаях;

– для эксплуатации ПО должна использоваться, по возможности, выделенная ПЭВМ с установленным на ней лицензионным системным и прикладным программным обеспечением и только необходимым по технологии использования ПО в информационной системе потребителя;

– ПЭВМ предназначенная для эксплуатации ПО должна быть защищена от «закладок», «компьютерных вирусов», несанкционированного изменения системного и прикладного программного обеспечения;

– любое изменение (реконфигурирование, дополнение и т.д.) системного и прикладного программного обеспечения ПЭВМ 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 ПЭВМ с установленным ПО должен быть ограничен и разрешен только уполномоченным на работу с ПО сотрудникам потребителя;

– средствами ОС MS Windows 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 жестком диске ПЭВМ);

– при проведении ремонтных и профилактических работ ПЭВМ, на которой установлено ПО должны приниматься организационные меры и использоваться технические средства для исключения несанкционированного доступа к ПО;

– осмотр и ремонт ПЭВМ представителями сторонних организаций проводятся только под наблюдением уполномоченного сотрудника потребителя;

– передача ПЭВМ для ремонта в сторонние организации производится только после демонтажа накопителя на жестком магнитном диске (НЖМД);

– ремонт НЖМД, на котором инсталлированы программные компоненты ПО, производится только после уничтожения на нем ПО путем форматирования НЖМД.

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 поддержки ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия http://www.avest.by) и действовать в соответствии с рекомендациями сотрудника отдела поддержки;
2. Убедиться в работоспособности ПЭВМ, ее 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 поддержки ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия http://www.avest.by) и действовать в соответствии с рекомендациями сотрудника отдела поддержки.

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

Примечания:

1. Взаимодействие с отделом 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, получившей 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».

5. СОКРАЩЕНИЯ

НКИ – носитель ключевой информации;

ОС – операционная система;

ПО – программное обеспечение;

ПЭВМ – персональная электронная вычислительная машина;

ЭЦП – электронная цифровая подпись.

Лист регистрации изменений									
Номер листов (страниц)					Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
Изм	Изменен-ных	Заменен-ных	Новых	Аннулиро-ванных					