УТВЕРЖДЕН

РБ.ЮСКИ.13001-04 34 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС

«КОМПЛЕКТ АБОНЕНТА АВЕСТ»

AvUCK

Руководство оператора

РБ.ЮСКИ.13001-04 34 01

Листов 18

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

2015

АННОТАЦИЯ

Данный документ содержит руководство оператора программного продукта РБ.ЮСКИ.13001-04 «Программный комплекс «Комплект Абонента АВЕСТ» AvUCK (далее – AvUCK).

В документе содержится информация по установке и использованию программного продукта. А также приведены рекомендуемые меры безопасности, выполнение которых в процессе эксплуатации AvUCK повышает уровень защиты информационных активов оператора и информационной системы.

Изготовителем AvUCK 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. 207-92-34, 207-99-74, факс. 207-91-49.

Интернет-страница: http://www.avest.by.

Электронная почта: welcome@avest.by.

При обнаружении неисправности при эксплуатации AvUCK, необходимо прекратить эксплуатацию AvUCK и связаться с производителем по вышеуказанным телефонам или электронной почте.

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

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

AvUCK функционирует на персональном компьютере конечного субъекта – пользователя (абонента) ИОК и предоставляет пользователю ИОК криптографические сервисы электронной цифровой подписи (далее – ЭЦП) и шифрования, а также сервисы управления криптографическими ключами, сертификатами открытых ключей (далее – СОК) и списками отозванных сертификатов (далее – СОС).

ИОК – это технологическая инфраструктура, сервисы и процедуры, обеспечивающие необходимый уровень доверия и безопасности информационных и коммуникационных систем, использующих криптографические алгоритмы с открытыми ключами.

ИОК обеспечивает сервисы, необходимые для непрерывного управления ключами в распределенной системе, связывает открытые ключи с владельцами соответствующих личных ключей и позволяет пользователям проверять подлинность этих связей.

Цель ИОК состоит в управлении криптографическими ключами, СОК и СОС, посредством которого поддерживается надежная сетевая среда. ИОК позволяет использовать криптографические сервисы шифрования и выработки цифровой подписи согласованно с широким кругом приложений, использующих криптографические алгоритмы с открытыми ключами.

В состав AvUCK входят программные продукты:

1. В качестве программных средств криптографической защиты информации, предоставляющих криптографические сервисы ЭЦП и шифрования:

- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP» AvCSP (РБ.ЮСКИ.08000-03). 32- разрядная версия AvCSP в 32-разрядных версиях ОС; 32- и 64-разрядные версии AvCSP в 64-разрядных версиях ОС;
- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP BEL» AvCSPBEL (РБ.ЮСКИ.12004-02). 32-разрядная версия AvCSPBEL в 32-разрядных версиях ОС; 32- и 64-разрядные версии AvCSPBEL в 64-разрядных версиях ОС;
- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP BIGN» AvCSPBIGN (РБ.ЮСКИ.12005-02) (32-разрядная версия AvCSPBIGN в 32-разрядных версиях ОС; 32- и 64-разрядные

версии AvCSPBIGN в 64-разрядных версиях ОС), использующий криптографические сервисы изделия ИЯТА.467532.003 «Устройства программно-аппаратные электронной цифровой подписи и шифрования AvBign».

2. В качестве программного средства, предоставляющего сервисы управления криптографическими ключами, СОК и СОС:

- программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM (РБ.ЮСКИ.08003-03).

AvUCK обеспечивает выполнение вышеуказанных сервисов в соответствии со следующими нормативными актами и документами:

1) ГОСТ 28147-89 «Системы 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 34.101.17-2012 «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 34.101.18-2009 «Информационные технологии. Синтаксис обмена персональной информацией»;

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

8) СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)»;

9) СТБ 34.101.27-2011 «Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации»;

10) СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности»;

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

12) СТБ 34.101.47-2012 «Информационные технологии и безопасность.

Криптографические алгоритмы генерации псевдослучайных чисел» (раздел 6.2).

13) СТБ 34.101.49-2012 «Информационные технологии и безопасность. Формат карточки открытого ключа»;

14) СТБ П 34.101.50-2012 «Информационные технологии и безопасность. Правила регистрации объектов информационных технологий»;

15) СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов»;

16) Проект Руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа».

Более подробно информация о назначении программных продуктов из состава AvUCK содержится в документах:

- программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM. Руководство оператора (РБ.ЮСКИ.08003-04 34 01);
- программное средство криптографической защиты информации «Криптопровайдер Avest CSP» AvCSP. Руководство оператора (РБ.ЮСКИ.08000-03 34 01);
- программное средство криптографической защиты информации «Криптопровайдер Avest CSP BEL» AvCSPBEL. Руководство оператора (РБ.ЮСКИ.12004-02 34 01);
- программное средство криптографической защиты информации «Криптопровайдер Avest CSP BIGN» AvCSPBIGN. Руководство оператора (РБ.ЮСКИ.12005-02 34 01).

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

AvUCK предназначен для работы на персональном компьютере общего назначения, функционирующим 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 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 R2 Server (x64);
- Windows 10 (x32, x64).

Требуется также наличие установленного Microsoft Internet Explorer версии 6.0 и выше.

Для использования ПК AvPCM в операционных системах Windows XP, Windows 2003, Windows 7, Windows 2008, Windows 8, Windows 8.1, Windows 2012, Windows 10 пользователь должен иметь права «Administrator» либо «PowerUser».

Для установки и работы AvUCK требуется персональный IBM - совместимый компьютер, имеющий оперативную память не менее 128 Мбайт, жесткий диск, содержащий не менее 450 Мбайт свободного пространства, монитор с установленным разрешением не менее чем 800x600 и цветовой палитрой не менее 256 цветов.

Для хранения личных ключей абонентов ИОК AvUCK использует отчуждаемые носители ключевой информации (НКИ).

В качестве отчуждаемого носителя ключевой информации (далее НКИ) AvUCK поддерживает НКИ, указанные в документации на криптопровайдеры, входящие в состав комплекса.

Примечание. Используемые НКИ должны быть зарегистрированы у ЗАО «АВЕСТ» согласно процедуре описанной в Руководстве оператора AvCSP, AvCSPBEL,

AvCSPBIGN.

Более подробно информация об условиях выполнения программных продуктов из состава AvUCK содержится в документах:

- программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM. Руководство оператора (РБ.ЮСКИ.08003-04 34 01);
- программное средство криптографической защиты информации «Криптопровайдер Avest CSP» AvCSP. Руководство оператора (РБ.ЮСКИ.08000-03 34 01);
- программное средство криптографической защиты информации «Криптопровайдер Avest CSP BEL» AvCSPBEL. Руководство оператора (РБ.ЮСКИ.12004-02 34 01);
- программное средство криптографической защиты информации «Криптопровайдер Avest CSP BIGN» AvCSPBIGN. Руководство оператора (РБ.ЮСКИ.12005-02 34 01).

3. УСТАНОВКА И ВЫПОЛНЕНИЕ ПРОГРАММЫ

Функциональность комплекса AvUCK обеспечивается парой продуктов: менеджер сертификатов и криптопровайдер. Поддержка необходимых криптографических алгоритмов в AvUCK обеспечивается использованием одного из криптопровайдеров: AvCSP, AvCSPBEL, AvCSPBIGN.

Стандартной конфигурацией использования AvUCK считается следующая: AvPCM совместно с AvCSPBEL.

Криптопровайдер AvCSP предназначен для обеспечения обратной совместимости и обновления ранних версий криптопровайдера.

Криптопровайдер AvCSPBIGN предназначен для обеспечения повышенных требований защиты информации путем применения в AvUCK аппаратного СКЗИ AvBIGN.

Установка AvUCK заключается в последовательной установке криптопровайдера и затем менеджера сертификатов согласно документации на данные программные продукты.

При необходимости возможна эксплуатация различных типов криптопровайдеров с менеджером сертификатов на одной ПЭВМ. Для этого необходимо установить в различные каталоги отдельный менеджер сертификатов для каждого криптопровайдера.

4. СООБЩЕНИЕ ОПЕРАТОРУ

Программные компоненты AvUCK выдают сообщения оператору путем отображения информации о состоянии программных модулей и содержимого НКИ, выводимой в GUI-интерфейсе.

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.

AvPCM является интерактивным приложением, выполняющимся в среде операционной системы Microsoft Windows. Для выполнения программы необходимо использовать средства, предоставляемые данным семейством операционных систем. Взаимодействие с оператором, осуществляется посредством обращения к пунктам меню и ввода данных в поля диалоговых форм. Сообщения оператору, а также информация об актуальном состоянии базы данных отображается в диалоговых окнах графического пользовательского интерфейса.

Более подробно информация о выводимых сообщений оператору в программных продуктах из состава AvUCK содержится в документах:

- программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM. Руководство оператора (РБ.ЮСКИ.08003-04 34 01);
- программное средство криптографической защиты информации «Криптопровайдер Avest CSP» AvCSP. Руководство оператора (РБ.ЮСКИ.08000-03 34 01);
- программное средство криптографической защиты информации «Криптопровайдер Avest CSP BEL» AvCSPBEL. Руководство оператора (РБ.ЮСКИ.12004-02 34 01);
- программное средство криптографической защиты информации «Криптопровайдер Avest CSP BIGN» AvCSPBIGN. Руководство оператора (РБ.ЮСКИ.12005-02 34 01).

5. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ ПК AVUCK

Программный комплекс AvUCK реализует следующие дополнительные возможности:

1. Криптографические сервисы для выполняемых AvUCK операций предоставляются следующими программными:
   - РБ.ЮСКИ.08000-03 34 01 «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP» AvCSP. Руководство оператора»;
   - РБ.ЮСКИ.12004-02 34 01 «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BEL» AvCSPBEL. Руководство оператора»;
   - РБ.ЮСКИ.12005-02 34 01 «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BIGN» AvCSPBIGN. Руководство оператора»;

   либо программно-аппаратными средствами:
   - ИЯТА.466217.003 «Устройство программно-аппаратное криптографическое AvHSM-Bign»;
   - ИЯТА.467532.003 «Устройства программно-аппаратные электронной цифровой подписи и шифрования «AvBign».
2. Предоставление доступа к сервисам AvUCK приложениям, разработанным на языке Java (см. РБ.ЮСКИ.08014-02 33 01 «Программный комплекс «JCE Provider АВЕСТ» AvJCEProv». Руководство программиста);
3. Использование программы Avest Personal CryptoKit, предоставляющей удобный пользовательский интерфейс для выполнения криптографических операций шифрования данных, их подписи и проверки корректности ЭЦП (см. РБ.ЮСКИ.08034-02 34 01 «Программное средство «AVEST PERSONAL CRYPTOKIT» AvPCK». Руководство оператора).

6. МЕРЫ БЕЗОПАСНОСТИ

Данный раздел содержит рекомендуемые требования обеспечения безопасности поставки, установки и эксплуатации криптопровайдера AvUCK, которым должны следовать потребители в процессе приобретения и использования AvUCK.

Данные требования направлены на достижение следующих целей:

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

6.1. Меры безопасности при поставке

Передача программного обеспечения AvUCK (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.

6.2. 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;

СКЗИ – средство криптографической защиты информации;

СОК – сертификат открытого ключа;

СОС – список отозванных сертификатов;

ЭЦП – электронная цифровая подпись.

Лист регистрации изменений									
Номер листов (страниц)					Всего листов (страниц) в документе	№ документа	Входящий № сопроводи-тельного документа и дата	Подп.	Дата
Изм	Из-ме-нен-ных	Заменен-ных	Новых	Анну-лиро-ванных					