

УТВЕРЖДЕН
РБ.ЮСКИ.13001-07 34 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС
«КОМПЛЕКТ АБОНЕНТА АВЕСТ»

AvUSK

Руководство оператора

РБ.ЮСКИ.13001-07 34 01

Листов 29

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

АННОТАЦИЯ

Данный документ содержит руководство оператора программного продукта «Программный комплекс «Комплект Абонента АВЕСТ» (AvUSK)» (РБ.ЮСКИ.13001-07) (далее – ПК AvUSK).

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

Изготовителем ПК AvUSK является белорусское предприятие «Закрытое акционерное общество «АВЕСТ» (ЗАО «АВЕСТ»).

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

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

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

Электронная почта: welcome@avest.by.

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

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

СОДЕРЖАНИЕ

1. Назначение программы	4
2. Условия выполнения программы	9
3. Перечень сервисов, доступных оператору	12
4. Входные и выходные данные	14
5. Установка и выполнение программы.....	17
6. Сообщения оператору.....	18
7. Меры безопасности.....	19
7.1. Меры безопасности при поставке	19
7.2. Меры безопасности при установке и эксплуатации.....	20
8. Перечень сокращений.....	26
9. Ссылки.....	27

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

ПК AvUSCK является программным средством криптографической защиты информации (СКЗИ) и предназначен для использования в качестве компонента подсистемы безопасности информационных систем, в которых взаимодействующие стороны являются субъектами инфраструктуры открытых ключей (ИОК).

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, сертификатами открытых ключей (СОК) и списками отозванных сертификатов (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.

ПК AvUSCK обеспечивает выполнение требований 2-го уровня безопасности, установленных в СТБ 34.101.27-2022.

Согласно Перечню государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утвержденному приказом ОАЦ от 12.03.2020 № 77 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 28.12.2022 № 207), ПК AvUSCK является средством:

- предварительного шифрования;
- линейного шифрования;
- выработки электронной цифровой подписи;
- проверки электронной цифровой подписи;
- выработки личного и открытого ключей;
- контроля целостности.

ПК AvUCK включает в себя следующие программные продукты (компоненты):

- «Программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM» (РБ.ЮСКИ.08003-07) (далее – ПК AvPCM);
- «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BEL» AvCSPBEL» (РБ.ЮСКИ.12004-03) (далее – криптопровайдер AvCSPBEL);
- «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BIGN» AvCSPBIGN» (РБ.ЮСКИ.12005-03) (далее – криптопровайдер AvCSPBIGN);
- «Программное средство «Веб плагин AvCMXWebP» AvCMXWebP» (РБ.ЮСКИ.15015-02) (далее – ПС AvCMXWebP).

Данные компоненты, в свою очередь, состоят из внутренних компонентов, обеспечивающих их требующуюся функциональность.

Примечания.

1. Комплект поставки AvUCK определяется по согласованию с потребителем и определяется параметрами информационной системы потребителя. Минимальный комплект поставки содержит ПК AvPCM (хранилище сертификатов в реестре операционной системы (ОС) Windows) и криптопровайдер AvCSPBEL/AvCSPBIGN.

2. ПС AvCMXWebP включается в поставку ПК AvUCK по согласованию с потребителем в зависимости от системной среды информационной системы потребителя и требований к информационной безопасности.

ПК AvUCK предназначен для функционирования на персональном компьютере либо сервере (далее – компьютере) с целью предоставления взаимодействующей стороне (пользователю) криптографических сервисов электронной цифровой подписи (ЭЦП), шифрования, контроля целостности, генерации псевдослучайных чисел, а также сервисов управления криптографическими ключами, СОК и СОС.

Также ПК AvUCK реализует клиентские части протоколов TLS и OCSP при взаимодействии с соответствующими серверными программными продуктами.

Пользователем, использующим сервисы ПК AvUCK, может являться как пользователь – оператор компьютера, так и пользователь – автоматизированный сервис информационной системы.

ПК AvUCK предназначен для использования по следующим основным направлениям:

- использование в качестве программного СКЗИ конечного пользователя – потребителя различных информационных сервисов (в частности, ГосСУОК);
- использование в составе SDK (software development kit) – комплекта разработчика для создания на его базе компонентов подсистемы безопасности автоматизированных информационных систем широкого круга назначения;
- использование в качестве эталонного и контрольного программного СКЗИ при проведении испытаний и исследований различного рода, а также при проведении работ по аттестации систем защиты информационных систем.

ПК AvUCK предоставляет пользователю следующие основные функции:

- выработка и проверка ЭЦП;
- генерация личных и открытых ключей ЭЦП и шифрования;
- создание запроса на получение сертификата;

- использование СОК и СОС;
- предварительное и линейное шифрование;
- использование алгоритмов хэширования;
- генерация псевдослучайных чисел;
- проверка действительности СОК по протоколу OCSP;
- использование атрибутных сертификатов;
- использование протокола TLS;
- поддержка синтаксиса криптографических сообщений.

При использовании ПК AvUCK в качестве компонента системы защиты информации информационной системы, аттестуемой в соответствии с приказами Оперативно-аналитического центра при Президенте Республики Беларусь и иными нормативными правовыми актами Республики Беларусь, в качестве механизмов безопасности, реализуемых ПК AvUCK, следует учитывать лишь те, ТНПА для которых приведены в сертификате соответствия требованиям ТР 2013/027/BY.

Криптографические сервисы для выполняемых ПК AvUCK операций предоставляются:

- криптопровайдерами AvCSPBEL/AvCSPBIGN;
- программно-аппаратным СКЗИ «Устройства программно-аппаратные электронной цифровой подписи и шифрования «AvBign» (ИЯТА.467532.003) (далее – НКИ AvBign).

Сервисы управления криптографическими ключами, СОК и СОС предоставляются ПК AvPCM.

Интеграция криптографических функций в веб-приложения с использованием браузеров Internet Explorer и Microsoft Edge в режиме Internet Explorer предоставляется программным продуктом ПС AvCMXWebP.

В качестве носителей ключевой информации в ПК AvUCK используются USB-устройства AvPass, AvBign.

Более подробная информация о назначении программных продуктов из состава ПК AvUSK содержится в документах:

- «Программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM. Руководство оператора» (РБ.ЮСКИ.08003-07 34 01);
- «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BEL» AvCSPBEL. Руководство оператора» (РБ.ЮСКИ.12004-03 34 01);
- «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BIGN» AvCSPBIGN. Руководство оператора» (РБ.ЮСКИ.12005-03 34 01);
- «Программное средство «Веб плагин AvCMXWebP». Руководство оператора» (РБ.ЮСКИ.15015-02 34 01).

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

ПК AvUCK функционирует под управлением одной из следующих ОС:

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

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

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

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

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

Для использования ПК AvUCK в ОС Windows пользователь должен иметь права «Administrator».

Для интеграции криптографических функций в веб-приложения с использованием ПС AvCMXWebP требуется наличие установленного браузера Internet Explorer версии 10.0 и выше и/или браузера Microsoft Edge, имеющего возможность работать в режиме Internet Explorer.

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

ПК AvUSCK предназначен для работы на компьютере (сервере), имеющем следующие минимальные технические характеристики:

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

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

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 программного обеспечения, переустановкой (удалением) криптографического программного обеспечения (криптопровайдера, персонального менеджера сертификатов и т.д.) нужно извлечь НКИ из USB-порта компьютера (сервера).

В случае проведения вышеуказанных манипуляций с программным

обеспечением без извлечения НКИ рекомендуется после завершения данных манипуляций с программным обеспечением средствами криптопровайдера AvCSPBEL/AvCSPBIGN убедиться в работоспособности НКИ и наличии данных пользователя на НКИ. В случае потери данных или выхода из строя НКИ нужно обратиться в техподдержку организации, в которой приобреталось программное обеспечение и НКИ.

В качестве отчуждаемого НКИ ПК AvUCK поддерживает НКИ, указанные в документации на криптопровайдеры, входящие в состав ПК AvUCK.

Примечание. Используемые НКИ должны быть зарегистрированы в ЗАО «АВЕСТ» согласно процедуре, описанной в Руководстве оператора криптопровайдера AvCSPBEL/AvCSPBIGN.

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

- «Программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM. Руководство оператора» (РБ.ЮСКИ.08003-07 34 01);
- «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BEL» AvCSPBEL. Руководство оператора» (РБ.ЮСКИ.12004-03 34 01);
- «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BIGN» AvCSPBIGN. Руководство оператора» (РБ.ЮСКИ.12005-03 34 01);
- «Программное средство «Веб плагин AvCMXWebP». Руководство оператора» (РБ.ЮСКИ.15015-02 34 01).

3. ПЕРЕЧЕНЬ СЕРВИСОВ, ДОСТУПНЫХ ОПЕРАТОРУ

Работа с ПК AvUCK предполагает одну роль оператора `Role.User`, которая совмещает роли «Администратор» и «Пользователь». Оператор роли `Role.User` (далее – пользователь ПК AvUCK, пользователь) является пользователем операционной системы компьютера, на который установлен ПК AvUCK.

Сервисы, реализуемые ПК AvUCK, делятся на внутренние и внешние. Внутренние сервисы используются внешними сервисами (или запускаются автоматически), не доступны пользователю ПК AvUCK в явном виде. Внешние сервисы доступны пользователю ПК AvUCK в явном виде.

ПК AvUCK предоставляет пользователю внешние сервисы, приведенные в таблице 3.1.

Таблица 3.1 – Внешние сервисы, предоставляемые ПК AvUCK пользователю.

Сервис	Описание сервиса
<code>Service.Version</code>	Вывод номера версии
<code>Service.State</code>	Вывод текущего состояния СКЗИ
<code>Service.SelfTest</code>	Самотестирование по внешней команде
<code>Service.ViewProperty</code>	Вывод контрольных характеристик файлов программ СКЗИ
<code>Service.Hash</code>	Вычисление значения хэш-функции
<code>Service.CertReq</code>	Создание запроса на получение сертификата
<code>Service.SignCMS</code>	Формирование подписанных данных
<code>Service.SignCMSVerify</code>	Проверка подписанных данных
<code>Service.Auth.AvPass</code>	Аутентификация пользователя ПК AvUCK перед НКИ AvPass
<code>Service.Auth.AvBign</code>	Аутентификация пользователя ПК AvUCK перед НКИ AvBign

Service.ChangePassword.AvPass	Смена пароля к НКИ AvPass
Service.ChangePassword.AvBign	Смена пароля к НКИ AvBign
Service.TLSUsage	Передача данных по TLS-соединению
Service.Envelope.Create	Формирование конвертованных данных
Service.Envelope.Parse	Разбор конвертованных данных

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входные и выходные данные, их параметры, поддерживаемые компонентами ПК AvUSK, определяются реализуемыми криптографическими алгоритмами, протоколами и форматами на основе требований ТНПА Республики Беларусь:

- шифрование данных по алгоритмам, определенным в СТБ 34.101.31;
- расшифрование данных по алгоритмам, определённым в ГОСТ 28147-89;
- выработка/проверка ЭЦП по алгоритмам, определенным в СТБ 34.101.45;
- проверка ЭЦП по алгоритму, определенному в СТБ 1176.2-99;
- вычисление значения хэш-функции по алгоритмам, определенным в СТБ 34.101.31, СТБ 1176.1-99;
- генерация псевдослучайных чисел по алгоритму, определенному в СТБ 34.101.47;
- генерация личных и открытых ключей ЭЦП для алгоритмов СТБ 34.101.45 и ключей шифрования для алгоритмов СТБ 34.101.31;
- формирование запроса на получение сертификата к удостоверяющему центру согласно СТБ 34.101.17 с учётом СТБ 34.101.78;
- реализация онлайнового протокола проверки статуса сертификата (OCSP) согласно СТБ 34.101.26 с учётом СТБ 34.101.78;
- поддержка СОК и СОС согласно СТБ 34.101.19 с учётом СТБ 34.101.78;
- поддержка АС согласно СТБ 34.101.67;
- поддержка идентификаторов объектов информационных технологий согласно СТБ 34.101.50;
- поддержка синтаксиса криптографических сообщений согласно СТБ 34.101.23 с учётом СТБ 34.101.78;
- реализация протокола TLS согласно СТБ 34.101.65.

Также ПК AvUSK обеспечивает:

- поддержку стандарта S/MIME (Secure/Multipurpose Internet Mail Extensions) для криптографической защиты электронной почты;
- использование открытых стандартизированных криптографических интерфейсов: Microsoft Cryptographic Application Programming Interface (CryptoAPI) версий 1.0 и 2.0 для взаимодействия с криптопровайдером AvCSPBEL/ AvCSPBIGN;
- использование реестра сертификатов, размещенного в локальной файловой системе, сетевой базе данных, хранилищах Microsoft Crypto API (системный реестр Windows) или в LDAP-хранилище;
- хранение списка доверенных корневых удостоверяющих центров с контролем целостности в случае использования файлового хранилища СОК и СОС;
- использование реестра сертификатов УЦ и РЦ ИОК;
- информирование пользователя об ошибке при некорректных действиях пользователя или сбоях компонентов программного комплекса;
- визуализацию сертификата для просмотра атрибутов его владельца и назначения сертификата;
- проверку действительности СОК и СОС;
- ведение журнала работы ПК AvPCM с обеспечением контроля целостности файла журнала.

Кроме того, ПК AvUSK поддерживает в качестве входных данных – данные по настройке параметров работы программы, а в качестве выходных данных – данные, выводимые в журналы работы программных компонентов, и сообщения оператору о функционировании программы и возникающих ошибках (при их наличии).

Более подробная информация о входных и выходных данных, а также о настройках программных продуктов из состава ПК AvUSK содержится в документах:

- «Программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM. Руководство оператора» (РБ.ЮСКИ.08003-07 34 01);
- «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BEL» AvCSPBEL. Руководство оператора» (РБ.ЮСКИ.12004-03 34 01);
- «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BIGN» AvCSPBIGN. Руководство оператора» (РБ.ЮСКИ.12005-03 34 01);
- «Программное средство «Веб плагин AvCMXWebP». Руководство оператора» (РБ.ЮСКИ.15015-02 34 01).

5. УСТАНОВКА И ВЫПОЛНЕНИЕ ПРОГРАММЫ

Функциональность ПК AvUCK обеспечивается менеджером сертификатов (ПК AvPCM) и криптопровайдером AvCSPBEL/AvCSPBIGN. Поддержка необходимых криптографических алгоритмов в ПК AvUCK обеспечивается использованием одного из криптопровайдеров AvCSPBEL/AvCSPBIGN.

Стандартной конфигурацией использования ПК AvUCK считается использование ПК AvPCM совместно с криптопровайдером AvCSPBEL.

Криптопровайдер AvCSPBIGN предназначен для обеспечения повышенных требований защиты информации путем применения в ПК AvUCK в качестве носителя ключевой информации USB-устройства AvBign.

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

При необходимости возможна эксплуатация различных типов криптопровайдеров с менеджером сертификатов на одном компьютере. Для этого нужно установить в различные папки отдельный менеджер сертификатов для каждого криптопровайдера.

6. СООБЩЕНИЯ ОПЕРАТОРУ

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

В состав ПК AvUSCK входят интерактивные приложения, выполняющиеся в среде ОС Microsoft Windows. 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 подробная информация о выводимых сообщениях оператору в программных продуктах из состава ПК AvUSCK содержится в документах:

- «Программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM. Руководство оператора» (РБ.ЮСКИ.08003-07 34 01);
- «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BEL» AvCSPBEL. Руководство оператора» (РБ.ЮСКИ.12004-03 34 01);
- «Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BIGN» AvCSPBIGN. Руководство оператора» (РБ.ЮСКИ.12005-03 34 01).

7. МЕРЫ БЕЗОПАСНОСТИ

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

Данные требования направлены на достижение следующих целей:

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

7.1. Меры безопасности при поставке

Передача ПО потребителю может осуществляться следующими способами:

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

Во всех данных случаях для защиты от несанкционированной модификации ПО в процессе доставки ПО потребителю 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»;

- в состав ПК AvPCM входит тестовая утилита AvCmUt, позволяющая потребителю самостоятельно вычислить хэш-значения полученных программных компонентов ПО;

- криптопровайдеры AvCSPBEL/AvCSPBIGN, а также ПК AvPCM обеспечивают в своих GUI-интерфейсах отображение используемых версий программных продуктов.

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

7.2. Меры безопасности при установке и эксплуатации

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

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

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

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

– после установки ПО отчуждаемый носитель (компакт-диск) с эталонным установочным файлом ПО и список эталонных хэш-значений программных компонентов 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. Пароль ОС Windows пользователя ПК AvUCK на доступ к компьютеру должен соответствовать требованиям, определяемым политикой безопасности потребителя, а также следующим минимальным требованиям:

– минимальная длина пароля – 8 символов;

– в пароль должны включаться как цифровые, так и буквенные символы в различных регистрах;

– при смене пароля новое значение должно не совпадать со старым;

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

- осмотр и ремонт компьютера представителями сторонних организаций проводятся только под наблюдением уполномоченного сотрудника потребителя;
- передача компьютера для ремонта в сторонние организации производится только после демонтажа накопителя информации (накопителя на жестком магнитном диске и/или SSD-диска);
- ремонт накопителя информации, на котором установлены программные компоненты ПО, производится только после уничтожения на нем ПО путем форматирования накопителя информации.

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

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

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

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

Периодичность проведения анализа и предпринимаемые действия при обнаружении таких предупреждений определяются политикой безопасности потребителя. При этом при обнаружении предупреждения об отсутствии источника

случайности RDRAND генерировать личные ключи пользователя ПК AvUCK средствами ПС AvCSPBEL запрещено до устранения причины предупреждения (например, путём замены процессора).

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

1. Сравнить версии и хэш-значения программных компонентов используемого ПО с эталонными. В случае несовпадения сообщить своему руководству, связаться с отделом технической поддержки ЗАО «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 событий ОС Windows.

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

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

Процедура «безопасного восстановления» ПО заключается в переинсталляции ПО на компьютер с носителя (компакт-диска) 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».

8. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ГосСУОК	– Государственная система управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь
ИОК	– инфраструктура открытых ключей
НКИ	– носитель ключевой информации
ОЗУ	– оперативное запоминающее устройство
ОС	– операционная система
ПК	– программный комплекс
ПС	– программное средство
СКЗИ	– средство криптографической защиты информации
СОК	– сертификат открытого ключа
СОС	– список отозванных сертификатов
ТНПА	– технический нормативный правовой акт
ЭЦП	– электронная цифровая подпись
OCSP	– (Online Certificate Status Protocol) онлайн-протокол проверки статуса сертификата
TLS	– (Transport Layer Security) протокол защиты транспортного уровня

9. ССЫЛКИ

1. СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования».
2. СТБ 1176.2-99 «Информационная технология. Защита информации. Процедура выработки и проверки электронной цифровой подписи».
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 34.101.26-2012 «Информационные технологии и безопасность. Онлайн-протокол проверки статуса сертификата (OCSP)».
7. СТБ 34.101.27-2022 «Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности».
8. СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности».
9. СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых».
10. СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел».
11. СТБ 34.101.50-2019 «Информационные технологии и безопасность. Правила регистрации объектов информационных технологий».
12. СТБ 34.101.65-2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)».

13. СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых».
14. СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутивных сертификатов».
15. СТБ 34.101.77-2020 «Информационные технологии и безопасность. Криптографические алгоритмы на основе sponge-функции».
16. СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей».
17. ТР 2013/027/ВУ «Информационные технологии. Средства защиты информации. Информационная безопасность».
18. ГОСТ 28147-89 «Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
19. Программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM. Руководство оператора (РБ.ЮСКИ.08003-07 34 01).
20. Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BEL» AvCSPBEL. Руководство оператора (РБ.ЮСКИ.12004-03 34 01).
21. Программное средство криптографической защиты информации «Криптопровайдер Avest CSP BIGN» AvCSPBIGN. Руководство оператора (РБ.ЮСКИ.12005-03 34 01).
22. Программное средство «Веб плагин AvCMXWebP». Руководство оператора (РБ.ЮСКИ.15015-02 34 01).

