УТВЕРЖДЕН

РБ.ЮСКИ.13001-06 34 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС

«КОМПЛЕКТ АБОНЕНТА АВЕСТ»

AvUCK

Руководство оператора

РБ.ЮСКИ.13001-06 34 01

Листов 24

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

2023

АННОТАЦИЯ

Данный документ содержит руководство оператора программного продукта РБ.ЮСКИ.13001-06 «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-т газеты «Правда», д. 5, пом. 3Н, каб. 7.

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

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

Электронная почта: welcome@avest.by.

При обнаружении неисправности при эксплуатации 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) инфраструктуры открытых ключей (далее - ИОК) и предназначен для предоставления пользователю ИОК криптографических сервисов электронной цифровой подписи (далее – ЭЦП), шифрования, а также сервисов управления криптографическими ключами, сертификатами открытых ключей (далее – СОК) и списками отозванных сертификатов (далее – СОС), контроля целостности, генерации псевдослучайных чисел.

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

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 качестве средств криптографической защиты информации (далее – СКЗИ), предоставляющих криптографические сервисы ЭЦП и шифрования в составе ПК AvUCK используются продукты:

– 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»;

– программный комплекс «JCE Provider АВЕСТ» AvJCEProv (РБ.ЮСКИ.08014-05);

– программное средство «AvConscryptUni» AvConscryptUni (РБ.ЮСКИ.17006-01).

Кроме этого, в качестве СКЗИ, ПК AvUCK может использовать устройство программно-аппаратные криптографические «AvHSM-Bign» (ИЯТА.466217.003).

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

– программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM (РБ.ЮСКИ.08003-06);

– программное средство «Веб плагин AvCMXWebP» (РБ.ЮСКИ.15015-01).

Примечания:

1. Комплект поставки AvUCK определяется по согласованию с потребителем и

определяется параметрами информационной системы потребителя. Минимальный комплект поставки содержит AvCSPBEL и AvPCM, обеспечивающий использование в качестве хранилища СОК и СОС реестр ОС Windows или файловое хранилище.

2. Инсталляционные файлы компонентов AvJCEProv, AvCMXWebP, AvConscryptUni включаются в поставку AvUCK по согласованию с потребителем в зависимости от системной среды информационной системы потребителя и требований к информационной безопасности.

3. Компоненты AvJCEProv, AvConscryptUni интегрируются в информационные системы потребителя с помощью комплекта разработчика (SDK AvUCK), который приобретается отдельно.

AvUCK обеспечивает следующие возможности:

– определение атрибутов пользователя (ввод необходимой информации, определяющей пользователя);

– генерацию личного и открытого ключей, формирование карточки открытого ключа, создание запроса на сертификат;

– подключение (экспорт) личного сертификата, сертификатов других пользователей, атрибутных сертификатов, списка отозванных сертификатов.

AvUCK обеспечивает выполнение криптографических сервисов ЭЦП, шифрования, управления ключами, контроля целостности, управления СОК и СОС абонента ИОК, включая атрибутные сертификаты, 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 34.101.21-2009 «Информационные технологии. Интерфейс обмена информацией с аппаратно-программным носителем криптографической информации (токеном)» (PKCS#11);

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

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

12) СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»;

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

14) СТБ 34.101.65-2014 «Информационные технологии и безопасность. Протокол

защиты транспортного уровня (TLS)»;

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

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

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

18) Проект Руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа» (ПФОК);

19) ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность».

В качестве носителей ключевой информации (далее - НКИ) AvUCK использует защищенные программно-аппаратные USB-ключи AvPass, AvBign, а также устройство AvHSM-Bign, которые удовлетворяют требованиям СТБ 34.101.78-2019 (раздел 11).

Примечания:

1. Алгоритмы, определенные в ГОСТ 28147-89, СТБ 1176.1-99, СТБ 1176.2-99, ПФОК, реализуются в качестве поддержки обратной совместимости с ранее выпущенными версиями AvUCK, эксплуатируемыми в настоящее время. Использование данных алгоритмов определяется конфигурационными файлами, входящими в комплект поставки AvUCK.

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

Более подробная информация о назначении программных продуктов из состава

AvUCK содержится в документах:

– программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM. Руководство оператора (РБ.ЮСКИ.08003-06 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:

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

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

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

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

Кроме того, программные компоненты AvUCK – AvJCEProv и AvConscryptUni – обеспечивают выполнение криптографических алгоритмов и механизмов, определенных в технических нормативно-правовых актах Республики Беларусь, под управлением операционной системы Linux.

AvJCEProv поддерживает работу под ОС SuSE Linux 10 Update 3 и выше, Red Hat Enterprise Linux 4 Update 5 и выше, Ubuntu Server 16.04 и выше для архитектуры Intel

x86, x86-64 и ядром 2.4.x и выше. Необходимо наличие установленного Java Development Kit (далее - JDK) версий 1.8.0.91 и выше.

Программный компонент AvConscryptUni обеспечивает также выполнение криптографических алгоритмов и механизмов, определенных в технических нормативно-правовых актах Республики Беларусь, под управлением операционных систем Android и MacOS (перечень поддерживаемых версий уточняется по запросу).

ВНИМАНИЕ! Для корректной работы криптопровайдеров AvCSP, AvCSPBEL, AvCSPBIGN под управлением операционных систем Windows XP, Windows Server 2003 необходимо перед установкой программного обеспечения установить обновление **KB2836198**, соответствующее разрядности и языку ОС.

ВНИМАНИЕ! На время установки антивирусное программное обеспечение (в том числе встроенное в ОС, например, Windows Defender) рекомендуется отключать, т.к. 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, необходимо добавить инсталляционный файл в исключения антивируса.

Для использования ПК AvPCM в операционных системах Windows пользователь должен иметь права «Administrator» либо «PowerUser».

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

AvUCK предназначен для работы на компьютере (сервере), имеющем следующие

минимальные технические характеристики:

– процессор x86 (x64) с тактовой частотой - не менее 2,5 ГГц;

– объем ОЗУ - не менее 4 Гб;

– жесткий диск, содержащий не менее 8 Гб свободного пространства для стандартной установки ОС;

– монитор с поддержкой VGA или более высокого разрешения;

– манипулятор «мышь» Microsoft или совместимое указывающее устройство,

– свободный USB-порт.

Для хранения личных ключей абонентов ИОК AvUCK использует отчуждаемые 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 ПО, переустановкой (удалением) криптографического ПО (криптопровайдера, персонального менеджера сертификатов и т.д.) необходимо извлечь НКИ из USB-порта компьютера (сервера).

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

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

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

AvCSPBEL, AvCSPBIGN.

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

- программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM. Руководство оператора (РБ.ЮСКИ.08003-06 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);
- программный комплекс «Комплект разработчика AvUCK SDK» (РБ.ЮСКИ.16018-01). Описание».

3. УСТАНОВКА И ВЫПОЛНЕНИЕ ПРОГРАММЫ

Функциональность комплекса AvUCK обеспечивается парой продуктов: менеджер сертификатов (AvPCM) 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 одном компьютере. Для этого необходимо установить в различные каталоги отдельный менеджер сертификатов для каждого криптопровайдера.

4. СООБЩЕНИЯ 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. 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 AvUCK содержится в документах:

- программный комплекс «Персональный менеджер сертификатов АВЕСТ» AvPCM. Руководство оператора (РБ.ЮСКИ.08003-06 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 AVUCK

Программный комплекс AvUCK реализует следующие дополнительные возможности:

1. Криптографические сервисы для выполняемых AvUCK операций предоставляются:

   следующими программными продуктами:

   - 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.08014-05 33 01 «Программный комплекс «JCE Provider АВЕСТ» AvJCEProv». Руководство программиста).
3. Интеграцию криптографических функций в веб-приложения с использованием браузера Internet Explorer.

6. МЕРЫ БЕЗОПАСНОСТИ

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

6.1. 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 AvPCM входит тестовая утилита AvCmUt, позволяющая потребителю самостоятельно вычислить хэш-значения полученных программных компонентов ПО;
- криптопровайдеры AvCSP, AvCSPBEL, AvCSPBIGN, а также программное средство 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», необходимо связаться с сотрудниками ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия https://www.avest.by) и уточнить факт отправки ПО в свой адрес. При подтверждении отправки ПО потребитель должен вышеуказанным способом проконтролировать соответствие версий и целостность полученного ПО. При отсутствии подтверждения от ЗАО «АВЕСТ» факта отправки ПО потребитель должен воздержаться от использования полученного ПО.

6.2. 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, а также аудит событий, связанных с ПО (запуск ПО, чтение-запись файлов и данных ПО, хранящихся на жестком диске компьютера);
- при проведении ремонтных и профилактических работ в отношении компьютера, на котором установлено ПО, должны приниматься организационные меры и использоваться технические средства для исключения несанкционированного доступа к ПО;
- осмотр и ремонт компьютера представителями сторонних организаций проводятся только под наблюдением уполномоченного сотрудника потребителя;

- передача компьютера для ремонта в сторонние организации производится только после демонтажа накопителя информации (накопителя на жестком магнитном диске и/или SSD-диска);
- ремонт накопителя информации, на котором инсталлированы программные компоненты ПО, производится только после уничтожения на нем ПО путем форматирования накопителя информации.

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

1. Сравнить версии и хэш-значения программных компонентов используемого ПО с эталонными. В случае несовпадения сообщить своему руководству, связаться с отделом технической поддержки ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия https://www.avest.by) и действовать в соответствии с рекомендациями сотрудника отдела технической поддержки.
2. Убедиться в работоспособности компьютера, его аппаратных и программных систем.
3. Проанализировать журналы аудита ОС.
4. При необходимости провести процедуру «безопасного восстановления» ПО (см. ниже).
5. В случае невозможности выполнения процедуры безопасного восстановления, прекратить эксплуатацию ПО, связаться с отделом технической поддержки ЗАО «АВЕСТ» (контактная информация расположена на сайте предприятия https://www.avest.by) и действовать в соответствии с рекомендациями сотрудника отдела технической поддержки.

Процедура «безопасного восстановления» ПО заключается в переинсталляции ПО на 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».

5. СОКРАЩЕНИЯ

ИОК – инфраструктура открытых ключей;

НКИ – носитель ключевой информации;

ОС – операционная система;

ПО – программное обеспечение;

СКЗИ – средство криптографической защиты информации;

СОК – сертификат открытого ключа;

СОС – список отозванных сертификатов;

ЭЦП – электронная цифровая подпись;

OCSP (Online Certificate Status Protocol) – онлайновый протокол проверки статуса сертификата, определенный в СТБ 34.101.26;

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

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