

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00077-06 98 01-ЛУ

«ВАЛИДАТА КЛИЕНТ» ВЕРСИЯ 4

Правила пользования

ВАМБ.00077-06 98 01

2020

Аннотация

Настоящий документ содержит описание порядка использования программного комплекса ВАМБ.00077-06 «“Валидата Клиент” версия 4» (далее — ПК «Валидата Клиент»).

Документ содержит описание состава и основных функций ПК «Валидата Клиент», описание ключевой системы, а также требования к обеспечению безопасности на всех этапах использования ПК «Валидата Клиент».

Документ предназначен для пользователей, применяющих ПК «Валидата Клиент».

Настоящий документ составлен в соответствии с технической спецификацией «Информационная технология. Криптографическая защита информации. Состав и содержание правил пользования средств криптографической защиты информации» (ТС 26.2.001-2020) технического комитета по стандартизации «Криптографическая защита информации» (ТК 26).

Содержание

1 НАЗНАЧЕНИЕ ПК «ВАЛИДАТА КЛИЕНТ» И ЕГО ОСНОВНЫЕ ХАРАКТЕРИСТИКИ	5
1.1 Общие сведения	5
1.2 Реализуемые криптографические алгоритмы	5
1.3 Компоненты ПК «Валидата Клиент»	6
1.3.1 ПК «Справочник сертификатов»	7
1.3.2 Утилита командной строки	8
1.3.3 Расширение проводника	8
1.3.4 ПК «Автоматизированный клиент СКЗИ»	8
1.3.5 ПК «Автоматизированный клиент СКЗИ. Сервис»	9
1.3.6 ПК «Автоматизированный клиент СКЗИ. Монитор»	10
1.3.7 ПК «Автоматизированный клиент СКЗИ. Сервис монитор»	10
1.3.8 Библиотека прикладного программного интерфейса	10
1.3.9 Библиотека, реализующая протокол TLS, программа TLSProху и программа STunnel	11
1.4 Варианты исполнения ПК «Валидата Клиент» и выполняемые нормативные требования	12
1.5 Среда функционирования	13
1.6 Графические интерфейсы ПК «Валидата Клиент»	14
2 КЛЮЧЕВАЯ СИСТЕМА И КЛЮЧЕВЫЕ ДОКУМЕНТЫ	15
2.1 Используемая ключевая система	15
2.2 Управление ключевой системой	15
3 ПОРЯДОК РАСПРОСТРАНЕНИЯ И УЧЁТА ПК «ВАЛИДАТА КЛИЕНТ»	17
3.1 Способы передачи и хранения ПК «Валидата Клиент»	17
3.2 Поэкземплярный учёт ПК «Валидата Клиент»	17
4 ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПК «ВАЛИДАТА КЛИЕНТ»	18
4.1 Требования по обеспечению безопасности при вводе ПК «Валидата Клиент» в эксплуатацию	18
4.1.1 Требования к встраиванию ПК «Валидата Клиент» в прикладные системы и к проведению исследований ПК «Валидата Клиент»	18
4.1.2 Требования по размещению	19
4.1.3 Требования к персоналу, обеспечивающему функционирование ПК «Валидата Клиент»	20
4.1.4 Инициализация и ввод ПК «Валидата Клиент» в эксплуатацию	22
4.1.5 Особенности работы с различными ключевыми носителями	22
4.2 Требования по обеспечению безопасности при эксплуатации ПК «Валидата Клиент»	22
4.2.1 Общие требования	22
4.2.2 Порядок обеспечения целостности ПК «Валидата Клиент»	23

4.2.3	Порядок обеспечения работоспособности ПК «Валидата Кли- ент»	24
4.2.4	Контроль правильности работы ЭВМ	25
4.3	Требования по обеспечению безопасности при выводе ПК «Валидата Клиент» из эксплуатации и передаче в ремонт	26

5	СВЕДЕНИЯ О СОГЛАСОВАНИИ	28
----------	--------------------------------	-----------

	ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	29
--	----------------------------	-----------

1 НАЗНАЧЕНИЕ ПК «ВАЛИДАТА КЛИЕНТ» И ЕГО ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

1.1 Общие сведения

Программный комплекс (ПК) ВАМБ.00077-06 «Валидата Клиент» версия 4» (далее — ПК «Валидата Клиент») предназначен для:

- использования в качестве автоматизированного рабочего места клиента удостоверяющего центра (УЦ), в том числе для формирования запросов конечных пользователей в Центр регистрации (ЦР) на создание сертификатов собственных ключей проверки электронной подписи (ЭП), а также запросов на аннулирование/прекращение действия своих сертификатов;
- реализации функций средства ЭП;
- встраивания в прикладные системы (прикладное программное обеспечение) криптографических функций создания и проверки ЭП с использованием сертификатов ключей проверки ЭП;
- встраивания в прикладное программное обеспечение (ПО) криптографических функций шифрования и расшифрования информации с использованием открытых ключей.

1.2 Реализуемые криптографические алгоритмы

ПК «Валидата Клиент» реализует криптографические алгоритмы согласно следующим стандартам:

- ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018) «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
- ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018) «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;
- ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Информационная технология. Криптографическая защита информации. Блочные шифры» (блочные шифры «Магма» и «Кузнечик»);
- ГОСТ Р 34.13-2015 и ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» (блочные шифры «Магма» и «Кузнечик» в режимах простой замены, гаммирования и выработки имитовставки).

Примечания

1 Для проверки ЭП в ПК «Валидата Клиент» реализована поддержка ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

2 Межгосударственные стандарты ГОСТ 34.10-2018, ГОСТ 34.11-2018 и ГОСТ 34.12-2018 определяют криптографические механизмы, совпадающие с криптографическими механизмами, определенными в национальных стандартах ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и ГОСТ Р 34.12-2015 соответственно.

3 Межгосударственный стандарт ГОСТ 34.13-2018 определяет криптографические механизмы, описанные в национальном стандарте ГОСТ Р 34.13-2015, и дополняет их криптографическими механизмами, описанными в Рекомендациях по стандартизации «Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования» (Р 1323565.1.017-2018) и «Режимы работы блочных шифров, реализующие аутентифицированное шифрование» (Р 1323565.1.026-2019).

4 Режим простой замены допускается использовать только для шифрования ключей.

ПК «Валидата Клиент» реализует криптографические преобразования в соответствии с Рекомендациями по стандартизации, указанными в документе ВАМБ.00060-06 98 01 «СКЗИ «Валидата CSP» версия 6. Правила пользования».

В ПК «Валидата Клиент» применяется CMS/PKCS#7 формат защищённых (подписанных и зашифрованных) данных.

Защищаемая информация (текст, видеоизображение и т.д.) представляется в виде бинарной последовательности.

1.3 Компоненты ПК «Валидата Клиент»

ПК «Валидата Клиент» содержит следующие компоненты:

– ПК «Справочник сертификатов», включающий исполняемый модуль командной строки, расширение проводника и программу STunnel. ПК «Справочник сертификатов» предназначен для формирования запросов на создание и аннулирование/прекращение действия сертификатов ключей проверки ЭП, постановки и проверки ЭП электронных документов, а также выполнения операций с базой данных сертификатов (справочниками сертификатов), создаваемой на рабочем месте пользователя, и управления профилями (настройками справочников сертификатов) пользователя;

– ПК «Автоматизированный клиент СКЗИ» (далее — ПК «АК СКЗИ»). ПК «АК СКЗИ» предназначен для автоматизации работы пользователя с криптографическими операциями;

– ПК «Автоматизированный клиент СКЗИ. Сервис» (далее — ПК «АК СКЗИ. Сервис»). ПК «АК СКЗИ. Сервис» предназначен для автоматизации работы пользователя с криптографическими операциями;

– ПК «Автоматизированный клиент СКЗИ. Монитор» (далее — ПК «АК СКЗИ. Монитор»). ПК «АК СКЗИ. Монитор» предназначен для просмотра журналов ПК «АК СКЗИ»;

– ПК «Автоматизированный клиент СКЗИ. Сервис монитор» (далее — ПК «АК СКЗИ. Сервис монитор»). ПК «АК СКЗИ. Сервис монитор» предназначен для

просмотра журналов ПК «АК СКЗИ. Сервис»;

- комплект разработчика прикладного программного обеспечения, включающий библиотеку прикладного программного интерфейса работы с сертификатами ключей для операционной системы (ОС) Windows (для C/C++ и для платформы Microsoft .Net Framework), обеспечивающую возможность встраивания ПК «Валидата Клиент» в прикладное программное обеспечение, и библиотеку, реализующую протокол TLS;

- программа TLSProxy.

ПК «Валидата Клиент» функционирует совместно с ПК ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — криптопровайдер или СКЗИ «Валидата CSP»).

1.3.1 ПК «Справочник сертификатов»

ПК «Справочник сертификатов» обеспечивает:

- формирование защищенного персонального справочника пользователя, содержащего сертификат Центра сертификации (ЦС);

- формирование личных ключей ЭП и ключей проверки ЭП пользователей УЦ с использованием различных ключевых носителей в соответствии с ГОСТ Р 34.10-2012;

- формирование запроса на создание сертификата в формате PKCS#10 с использованием созданного личного ключа ЭП и ключа проверки ЭП;

- передачу запроса в защищенном виде в ЦР;

- создание и проверку ЭП файлов в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;

- добавление и удаление сертификатов, списков аннулированных (отозванных) сертификатов (САС);

- проверку и отображение состояния сертификатов, связанного с окончанием их сроков действия или их аннулированием/прекращением действия;

- формирование и передачу в ЦР сообщения о компрометации ключа пользователя;

- отображение содержания и вывод на печать сертификатов, запросов, САС и сообщений о компрометации;

- обновление САС с использованием сетевого справочника сертификатов;

- восстановление персонального и локального справочника пользователя из резервной копии;

- возможность подключения к терминальному серверу через входящий в состав серверных ОС Windows шлюз терминальных серверов (Terminal Services Gateway);

- возможность подключения в режиме удаленного доступа к терминальным серверам, находящихся под управлением Citrix XenDesktop/XenApp версия 7, по сетевому каналу, защищенному шифрованием и аутентификацией по протоколу TLS. Защита подключения, выполняющегося по протоколу ICA (Independent Computing Architecture), выполняется с помощью входящей в состав ПК «Валидата Клиент» программы STunnel.

Примечание — Под списком аннулированных сертификатов понимается список аннулированных сертификатов и сертификатов, действие которых прекращено, за исключением, возможно, сертификатов, действие которых прекращено по причине истечения срока действия сертификата. Случаи аннулирования и прекращения действия сертификатов устанавливаются удостоверяющим центром.

1.3.2 Утилита командной строки

Утилита командной строки предназначена для осуществления доступа пользователей к криптографическим функциям из режима командной строки ОС Microsoft Windows. Утилита командной строки позволяет осуществлять шифрование/расшифрование информации, формирование/проверку подлинности ЭП, а также простановку/проверку штампов времени ЭП и проверку статуса сертификата. Утилита командной строки использует ПК «Справочник Сертификатов» для управления справочниками сертификатов.

Доступ пользователей к криптографическим функциям осуществляется через вызов утилиты с заданием параметров выполнения из режима командной строки.

1.3.3 Расширение проводника

Программный модуль «Расширение проводника» для ОС Windows встраивается в контекстное меню Проводника. Для работы расширения проводника требуется установленный и настроенный ПК «Справочник сертификатов».

Расширение проводника позволяет выполнять следующие криптографические операции с группами файлов и каталогами через пункт контекстного меню Проводника ОС Windows:

- создание и проверка (с возможностью удаления) ЭП файлов (CMS сообщений) в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- зашифрование и расшифрование файлов в соответствии с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочные шифры «Магма» и «Кузнечик») в режиме гаммирования с возможностью выработки имитовставки;
- зашифрование и расшифрование файлов в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью в соответствии с RFC 4357 и RFC 4490;
- вычисление хэш-функции данных в соответствии с ГОСТ Р 34.11-2012 (для хэш-значений длиной 256 бит).

1.3.4 ПК «Автоматизированный клиент СКЗИ»

ПК «АК СКЗИ» функционирует в качестве приложения, работающего в фоновом режиме.

ПК «АК СКЗИ» позволяет выполнять следующие функции в автоматическом режиме:

- создание и проверка (с возможностью удаления) ЭП файлов (CMS сообщений) в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- зашифрование и расшифрование файлов в соответствии с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочные шифры «Магма» и «Кузнечик») в режиме гаммирования с возможностью выработки имитовставки;
- зашифрование и расшифрование файлов в соответствии с ГОСТ 28147-89 в

режиме гаммирования с обратной связью в соответствии с RFC 4357 и RFC 4490;

- вычисление хэш-функции данных в соответствии с ГОСТ Р 34.11-2012 (для хэш-значений длиной 256 бит);
- реализация механизма простановки и проверки штампов времени ЭП в соответствии с RFC 3161;
- упаковка и распаковка файлов и папок в/из zip- или gzip- архивов;
- перемещение и удаление файлов;
- преобразование файлов в формат и из формата Base64;
- исполнение заданной командной строки с возможностью выбора исполняемого файла и параметров выполнения;
- ведение журнала выполненных операций.

Также ПК «АК СКЗИ» позволяет выполнять следующие функции в ручном режиме:

- настройка профилей, содержащих правила обработки файлов;
- настройка правил обработки файлов, в том числе добавление, редактирование, удаление, временное отключение правил и изменение порядка исполнения правил;
- экспорт правил в файл;
- импорт правил из файла;
- поиск правил по описанию;
- настройка пути записи журнала ПК «АК СКЗИ»;
- настройка списка подписантов.

1.3.5 ПК «Автоматизированный клиент СКЗИ. Сервис»

ПК «АК СКЗИ. Сервис» функционирует в качестве службы ОС Windows.

ПК «АК СКЗИ. Сервис» позволяет выполнять следующие функции в автоматическом режиме:

- создание и проверка (с возможностью удаления) ЭП файлов (CMS сообщений) в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- зашифрование и расшифрование файлов в соответствии с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочные шифры «Магма» и «Кузнечик») в режиме гаммирования с возможностью выработки имитовставки;
- зашифрование и расшифрование файлов в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью в соответствии с RFC 4357 и RFC 4490;
- вычисление хэш-функции данных в соответствии с ГОСТ Р 34.11-2012 (для хэш-значений длиной 256 бит);
- реализация механизма простановки и проверки штампов времени ЭП в соответствии с RFC 3161;
- упаковка и распаковка файлов и папок в/из zip- или gzip- архивов;
- перемещение и удаление файлов;
- преобразование файлов в формат и из формата Base64;
- исполнение заданной командной строки с возможностью выбора исполня-

емого файла и параметров выполнения;

- ведение журнала выполненных операций.

Также ПК «АК СКЗИ. Сервис» позволяет выполнять следующие функции в ручном режиме:

- настройка профилей, содержащих правила обработки файлов;
- настройка правил обработки файлов, в том числе добавление, редактирование, удаление, временное отключение правил и изменение порядка исполнения правил;
- экспорт правил в файл;
- импорт правил из файла;
- поиск правил по описанию;
- настройка пути записи журнала «АК СКЗИ. Сервис»;
- настройка списка подписантов.

1.3.6 ПК «Автоматизированный клиент СКЗИ. Монитор»

ПК «АК СКЗИ. Монитор» выполняет следующие функции:

- просмотр краткого описания событий ПК «АК СКЗИ. Монитор» для каждого профиля ПК «АК СКЗИ», найденного в каталоге журнала;
- просмотр краткого описания ошибок ПК «АК СКЗИ. Монитор» для каждого профиля ПК «АК СКЗИ», найденного в каталоге журнала;
- просмотр подробного описания события/ошибки ПК «АК СКЗИ. Монитор»;
- уведомление о произошедшей ошибке;
- сброс записей журнала.

1.3.7 ПК «Автоматизированный клиент СКЗИ. Сервис монитор»

ПК «АК СКЗИ. Сервис монитор» выполняет следующие функции:

- просмотр краткого описания событий ПК «АК СКЗИ. Сервис монитор» для каждого профиля ПК «АК СКЗИ. Сервис», найденного в каталоге журнала;
- просмотр краткого описания ошибок ПК «АК СКЗИ. Сервис монитор» для каждого профиля ПК «АК СКЗИ. Сервис», найденного в каталоге журнала;
- просмотр подробного описания события/ошибки ПК «АК СКЗИ. Сервис монитор»;
- уведомление о произошедшей ошибке;
- сброс записей журнала.

1.3.8 Библиотека прикладного программного интерфейса

Библиотека прикладного программного интерфейса для работы с сертификатами ключей предназначена для предоставления программного интерфейса для работы с сертификатами и обеспечивает выполнение следующих функций:

- создание (генерация) ключей ЭП длиной 256 и 512 бит, а также соответствующих ключей проверки ЭП длиной 512 и 1024 бита согласно ГОСТ Р 34.10-2012;

- формирование первичного запроса на получение сертификата ключа проверки ЭП в формате PKCS#10;
- формирование непервичного запроса на плановую смену сертификата ключа проверки ЭП в формате PKCS#10+CMS/PKCS#7;
- формирование запроса на аннулирование сертификата ключа проверки ЭП;
- вычисление хэш-функции данных в соответствии с ГОСТ Р 34.11-2012 (для хэш-значений длиной 256 и 512 бит);
- создание и проверка ЭП данных в соответствии с ГОСТ Р 34.10-2012 (для ключей ЭП длиной 256 и 512 бит);
- зашифрование и расшифрование файлов и блоков памяти в соответствии с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочные шифры «Магма» и «Кузнечик») в режиме гаммирования с возможностью выработки имитовставки;
- зашифрование и расшифрование файлов и блоков памяти в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью;
- создание и проверка ЭП файлов и блоков памяти в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- вычисление хэш-функции данных в соответствии с ГОСТ Р 34.11-94 и проверку архивных ЭП в соответствии с ГОСТ Р 34.10-2001;
- реализация протокола безопасности транспортного уровня TLS версии 1.0;
- реализация протокола безопасности транспортного уровня TLS версии 1.2;
- реализация механизма простановки и проверки штампов времени ЭП;
- реализация механизма проверки статуса сертификата.

В состав библиотеки для C/C++ входят следующие файлы:

- zpk1.dll — модуль динамической библиотеки;
- zpk1.lib — модуль библиотеки для линковки с динамической библиотекой;
- vcert1.h — файл с описанием прототипов функций библиотеки;
- vcerterr.h — файл с определениями кодов возврата функций библиотеки.

В состав библиотеки для платформы Microsoft .Net Framework входит модуль динамической библиотеки vcpia2.dll.

1.3.9 Библиотека, реализующая протокол TLS, программа TLSProxy и программа STunnel

Программа STunnel, используя библиотеку, реализующую протокол TLS, позволяет создавать TLS-туннель, обеспечивающий криптографическую защиту произвольного TCP-соединения посредством оборачивания (инкапсуляции) этих данных протоколом TLS.

Программа TLSProxy, которая является аналогом программы STunnel, также предназначена для защиты данных, передаваемых по TCP соединениям, посредством оборачивания (инкапсуляции) этих данных протоколом TLS. В отличие от программы STunnel, программа TLSProxy всегда выполняет двухстороннюю аутентификацию (проверяет цепочку сертификата противоположной стороны), а также имеет возможность фильтровать (блокировать) TLS соединения на ос-

новании данных сертификатов противоположной стороны.

ПК «Валидата Клиент» обеспечивает выполнение следующих функций поддержки протокола TLS:

- создание защищённого канала связи (с обеспечением контроля целостности передаваемой информации) между сервером и клиентом с использованием шифрования информации в соответствии с ГОСТ 28147-89 для протокола TLS 1.0 (согласно RFC 2246);
- создание защищённого канала связи (с обеспечением контроля целостности передаваемой информации) между сервером и клиентом с использованием шифрования информации в соответствии с ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 (блочный шифр «Кузнечик») для протокола TLS 1.2 (согласно RFC 5246);
- аутентификация сервера клиентом посредством вычисления ключа парной связи по способу Диффи-Хеллмана с использованием пар закрытых и открытых ключей, созданных в соответствии с ГОСТ Р 34.10-2012;
- аутентификация клиента сервером посредством вычисления ЭП в соответствии с ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012;
- вычисление расширенного мастер-секрета в соответствии с RFC 7627 для протокола TLS 1.2;
- выполнение безопасного переподключения в соответствии с RFC 5746.

1.4 Варианты исполнения ПК «Валидата Клиент» и выполняемые нормативные требования

ПК «Валидата Клиент» имеет три исполнения:

- исполнение 1, для которого использование средств защиты информации от несанкционированного доступа (СЗИ от НСД), сертифицированных ФСБ России, является рекомендательным;
- исполнение 2, для которого использование СЗИ от НСД, сертифицированных ФСБ России, является обязательным;
- исполнение 3, для которого использование СЗИ от НСД и средств создания замкнутой программной среды, сертифицированных ФСБ России, является обязательным.

Используемые совместно с ПК «Валидата Клиент» СЗИ от НСД должны иметь действующие сертификаты и/или положительные заключения ФСБ России о соответствии требованиям, указанным в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

Примечания

1 Все исполнения имеют одну и ту же программную реализацию, не зависящую от применения совместно с ПК «Валидата Клиент» сертифицированных СЗИ от НСД и средств создания замкнутой программной среды. В связи с этим, применяемые в эксплуатационной документации ПК «Валидата Клиент» обозначения АПК и ПК идентичны.

2 В документации на ПК «Валидата Клиент» термин «Средство защиты от несанкционированного доступа» обозначает исключительно аппаратно-программные и программные модули доверенной загрузки (МДЗ), имеющие

действующие сертификаты и/или положительные заключения ФСБ России.

ПК «Валидата Клиент» удовлетворяет требованиям, изложенным в следующих документах:

– «Требования к средствам электронной подписи», утверждённые приказом ФСБ России от 27.12.2011 № 796:

- для исполнения 1 — по классу КС1 при функционировании в физической и виртуальной среде;
- для исполнения 2 — по классу КС2 при функционировании в физической среде;
- для исполнения 3 — по классу КС3 при функционировании в физической среде;

– «Требования к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну»:

- для исполнения 1 — по классу КС1 при функционировании в физической и виртуальной среде;
- для исполнения 2 — по классу КС2 при функционировании в физической среде;
- для исполнения 3 — по классу КС3 при функционировании в физической среде;

– «Специальные требования к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации» (СТ-Р) по уровню КС_Б.

ПК «Валидата Клиент» поддерживает работу с сертификатами, удовлетворяющими «Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи», утверждённым приказом ФСБ России от 27.12.2011 № 795.

ПК «Валидата Клиент» функционирует совместно с сертифицированными ФСБ России СЗИ от НСД и средствами создания замкнутой программной среды, перечисленными в документе ВАМБ.00060-06 98 01 «СКЗИ «Валидата CSP» версия 6. Правила пользования».

1.5 Среда функционирования

Среда функционирования ПК «Валидата Клиент» определяется требованиями к среде функционирования СКЗИ «Валидата CSP», которые приведены в документе ВАМБ.00060-06 98 01 «СКЗИ «Валидата CSP» версия 6. Правила пользования».

ПК «Валидата Клиент» функционирует совместно со следующими системами управления базами данных:

- Microsoft SQL Server 2016/2017/2019;

- Oracle 11g/12c/18c/19c;
- PostgreSQL/Postgres Pro 9.6/10/11/12/13/14/15/16/17/18.

1.6 Графические интерфейсы ПК «Валидата Клиент»

ПК «Валидата Клиент» предоставляет следующие графические интерфейсы для взаимодействия с пользователем:

- ПК «Справочник сертификатов»;
- ПК «Автоматизированный клиент СКЗИ» и «Автоматизированный клиент СКЗИ. Сервис»;
- ПК «Автоматизированный клиент СКЗИ. Монитор» и «Автоматизированный клиент СКЗИ. Сервис монитор»;
- расширение проводника;
- утилита командной строки.

Подробная информация о порядке работы с перечисленными выше интерфейсами приведена в документе ВАМБ.00077-06 31 01 «“Валидата Клиент” версия 4. Описание применения» и соответствующих руководствах пользователя.

2 КЛЮЧЕВАЯ СИСТЕМА И КЛЮЧЕВЫЕ ДОКУМЕНТЫ

2.1 Используемая ключевая система

В качестве ключевой системы ПК «Валидата Клиент» используется ключевая система, реализованная в СКЗИ «Валидата CSP». Описание ключевой системы приведено в документе ВАМБ.00060-06 98 01 «СКЗИ «Валидата CSP» версия 6. Правила пользования».

Ключевая система СКЗИ «Валидата CSP» является системой с открытым распределением ключей на основе асимметричной криптографии, в которой используется пара асимметричных ключей: открытый ключ (ключ проверки ЭП, открытый ключ шифрования) и закрытый ключ (ключ ЭП, закрытый ключ шифрования).

Сроки действия ключей ЭП и сертификатов ключей проверки ЭП в зависимости от условий эксплуатации приведены в документе ВАМБ.00060-06 98 01 «СКЗИ «Валидата CSP» версия 6. Правила пользования».

2.2 Управление ключевой системой

При работе с ПК «Валидата Клиент» каждый пользователь, обладающий правом подписи (или шифрования), самостоятельно формирует или получает в УЦ личные ключ ЭП (на отчуждаемом носителе) и ключ проверки ЭП (в составе сертификата ключа проверки ЭП, издаваемого УЦ).

Управление квалифицированными сертификатами ключей проверки ЭП при использовании ПК «Валидата Клиент» должно обеспечиваться с использованием средств удостоверяющего центра, имеющих действующий сертификат соответствия (положительное заключение) ФСБ России, а также ключ проверки ЭП в формате, соответствующем рекомендациям по стандартизации Р 1323565.1.023-2022 (утверждены приказом Росстандарта от 09.03.2022 № 123-ст).

Класс средств УЦ, с помощью которых формируется сертификат ключа проверки ЭП, должен быть не ниже класса используемого ПК «Валидата Клиент».

В качестве носителей криптографических ключей должны использоваться носители, указанные в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

Плановая смена ключей ЭП и соответствующих ключей проверки ЭП выполняется в соответствии с требованиями УЦ и документа ВАМБ.00077-06 31 01 ««Валидата Клиент» версия 4. Описание применения».

Владелец ключевой информации должен обеспечить ее сохранность, а также принимать все возможные меры для предотвращения ее потери, раскрытия, модифицирования или несанкционированного использования.

Ответственным за организацию работ по безопасному использованию ПК

«Валидата Клиент», в том числе, ключевой информации, является администратор информационной безопасности.

Порядок обеспечения безопасности ключевой информации, в том числе:

- полномочия и обязанности администратора информационной безопасности;
- организационно-технические меры и средства, необходимые для обеспечения безопасности ключевой информации;
- порядок обращения с ключевыми носителями, включая правила хранения ключевых носителей;
- порядок резервирования ключевой информации;
- порядок уничтожения ключей,

приведен в документах ВАМБ.00077-06 93 01 ««Валидата Клиент» версия 4. Руководство администратора информационной безопасности» и ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

Порядок действий при компрометации ключевой информации определяется документом ВАМБ.00077-06 31 01 ««Валидата Клиент» версия 4. Описание применения» и требованиями УЦ.

3 ПОРЯДОК РАСПРОСТРАНЕНИЯ И УЧЁТА ПК «ВАЛИДАТА КЛИЕНТ»

3.1 Способы передачи и хранения ПК «Валидата Клиент»

Передача дистрибутива ПК «Валидата Клиент» в эксплуатирующую организацию осуществляется на оптическом носителе, не допускающем перезапись информации, или в электронном виде с обеспечением целостности дистрибутива посредством ЭП.

Дистрибутив сопровождается ведомостью машинного носителя записи (ВМНЗ), содержащей информацию о хэш-кодах архивов с программным обеспечением и документацией, вычисленных по алгоритму хэширования согласно ГОСТ Р 34.11-2012 (в формате протокола проверки, формируемого программой контроля целостности).

При получении дистрибутива эксплуатирующая организация осуществляет внешний контроль носителя (проверка маркировки), а также внутренний контроль (проверка комплектности и контроль целостности дистрибутива). Контроль целостности дистрибутива осуществляется в соответствии с документами ВАМБ.00077-06 93 01 ««Валидата Клиент» версия 4. Руководство администратора информационной безопасности», ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности» и ВАМБ.00060-06 92 01 «СКЗИ «Валидата CSP» версия 6. Программа контроля целостности. Руководство пользователя».

Эталонные дистрибутивы с подтвержденной целостностью должны храниться в условиях, исключающих возможность подмены установочных файлов и файлов верификации.

3.2 Поэкземплярный учёт ПК «Валидата Клиент»

ПК «Валидата Клиент» подлежит поэкземплярному учёту с использованием индексов или условных наименований и регистрационных номеров, определяемых ФСБ России.

4 ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПК «ВАЛИДАТА КЛИЕНТ»

4.1 Требования по обеспечению безопасности при вводе ПК «Валидата Клиент» в эксплуатацию

4.1.1 Требования к встраиванию ПК «Валидата Клиент» в прикладные системы и к проведению исследований ПК «Валидата Клиент»

При встраивании ПК «Валидата Клиент» в соответствии с документом ВАМБ.00077-06 33 01 «“Валидата Клиент” версия 4. Руководство программиста» или документом ВАМБ.00077-06 33 02 «“Валидата Клиент” версия 4. Библиотека прикладного программного интерфейса работы с сертификатами для платформы Microsoft .NET Framework. Руководство программиста» в прикладные системы необходимо проводить проверку (оценку) влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, с которыми предполагается его штатное функционирование, на выполнение предъявленных к данному средству требований, в следующих случаях:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнении работ или оказании услуг для государственных нужд;
- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;
- при обработке информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путём использования средств криптографической защиты;
- при обработке информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране её конфиденциальности путём установления необходимости криптографической защиты данной информации.

В остальных случаях указанная проверка носит рекомендательный характер.

В рамках работ по проверке (оценке) влияния необходимо проводить следующие исследования:

- проверку выполнения требований и рекомендаций, указанных в докумен-

тации на ПК «Валидата Клиент»;

- проверку отсутствия ухудшений инженерно-криптографических свойств ПК «Валидата Клиент»;
- проверку выполнения требований к контролю целостности;
- анализ документации прикладного программного обеспечения, использующего ПК «Валидата Клиент»;
- проверку выполнения п. 8 и п. 9 требований к средствам ЭП, утверждённых приказом ФСБ России от 27.12.2011 № 796;
- проверку ПО BIOS/UEFI ЭВМ, на которой функционирует ПК «Валидата Клиент», в соответствии с нормативно-методическими документами ФСБ России в части проведения исследования ПО BIOS/UEFI.

Указанная проверка (оценка) должна проводиться по техническому заданию, согласованному с Центром защиты информации и специальной связи ФСБ России. Проверка должна производиться специализированными организациями, имеющими лицензию ФСБ России на указанный вид деятельности и соответствующую аккредитацию испытательной лаборатории.

При реализации с использованием ПК «Валидата Клиент» криптографических протоколов, обеспечивающих защиту данных, передаваемых по каналам связи, необходима сертификация указанной реализации по требованиям ФСБ России.

4.1.2 Требования по размещению

При эксплуатации, размещении и хранении технических средств с установленным ПК «Валидата Клиент» пользователь должен обеспечить режим эксплуатации, размещения и хранения технических средств, исключающий несанкционированный доступ к этим техническим средствам.

При размещении стационарных ЭВМ с установленным ПК «Валидата Клиент»:

- должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства с установленным ПК «Валидата Клиент», лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях;
- в случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями;
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать сохранность конфиденциальных документов и сведений, включая ключевую информацию, пользователей ПК «Валидата Клиент».

Размещение и эксплуатация ПК «Валидата Клиент» в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

Требования к информативности сигналов линейной передачи и сигналов ПЭМИН (Побочные электромагнитные излучения и наводки) не предъявляют-

ся.

Технические средства, на которых предполагается эксплуатация ПК «Валидата Клиент», должны быть допущены для обработки информации ограниченного доступа по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе по каналу связи (например, СТР-К) с учетом модели угроз, принятой в автоматизированных системах и ПК эксплуатирующей организации. Данное требование не предъявляется в случае эксплуатации ПК «Валидата Клиент» при обработке открытой информации, доступ к которой не ограничивается согласно законодательству Российской Федерации.

Если технические средства аттестованы на соответствие установленным требованиям по защите информации без учета оценки каналов связи, то при их подключении к проводным каналам связи, выходящим за пределы контролируемой территории, необходимо использовать любое из следующих средств:

- волоконно-оптические линии связи;
- оптические развязывающие устройства, устанавливаемые в тракт передачи информации для создания оптоволоконного фрагмента сети;
- сертифицированные средства криптографической защиты информации для передачи информации соответствующего уровня конфиденциальности.

Для технических средств, подключенных к беспроводным каналам связи, для обеспечения защиты информации по уровню КС от утечки по каналу линейной передачи достаточно, чтобы канал связи был реализован в виде радиоканала GSM, GPRS, 3G/4G, WiFi, а также других каналов мобильной или беспроводной связи, работающих в диапазоне частот несущей выше 800 МГц с цифровой модуляцией штатного информационного сигнала.

Требования по защите от НСД к ПК «Валидата Клиент» приведены в документах ВАМБ.00077-06 93 01 «“Валидата Клиент” версия 4. Руководство администратора информационной безопасности» и ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

Перечень требований к хранению эталонного дистрибутива ПК «Валидата Клиент», содержащего, в том числе, эксплуатационную документацию, приведен в документе ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности».

4.1.3 Требования к персоналу, обеспечивающему функционирование ПК «Валидата Клиент»

К установке, эксплуатации и сопровождению ПК «Валидата Клиент» допускаются специалисты, изучившие соответствующие эксплуатационные документы.

Персонал должен знать и строго выполнять правила эксплуатации ПК «Валидата Клиент», изложенные в эксплуатационной документации, а также требования соответствующих руководящих, нормативных, методических и организационно-распорядительных документов.

Помимо пользователей ПК «Валидата Клиент» в обеспечении безопасного функционирования ПК «Валидата Клиент» участвуют администратор информационной безопасности и системный администратор.

Администратор информационной безопасности выполняет следующие функции:

- осуществляет создание инструкций, направленных на обеспечение безопасности функционирования ПК «Валидата Клиент», доведение данных инструкций до пользователей и контроль за их соблюдением;
- осуществляет организацию контроля целостности ПО ПК «Валидата Клиент»;
- осуществляет управление доступом пользователей к ПО и данным, включая установку и периодическую смену паролей;
- при централизованном хранении личных контейнеров с ключевыми носителями (опечатаваемых личной печатью владельца ключей) обеспечивает это централизованное хранение;
- осуществляет определение конкретных настроек операционной системы и её конфигурирование в целях защиты ПК «Валидата Клиент» от НСД;
- производит настройку средств создания замкнутой программной среды;
- производит настройку аппаратно-программных или программных средств, обеспечивающих защиту от НСД к ПК «Валидата Клиент».

Примечание — Более подробно сведения о функциях, выполняемых администратором информационной безопасности, приведены в документе ВАМБ.00077-06 93 01 «“Валидата Клиент” версия 4. Руководство администратора информационной безопасности».

Системный администратор выполняет следующие функции:

- производит установку ПК «Валидата Клиент»;
- производит установку аппаратно-программных или программных средств, обеспечивающих защиту от НСД к ПК «Валидата Клиент»;
- производит установку средств создания замкнутой программной среды;
- производит администрирование операционной системы (ОС).

При выполнении своих обязанностей системному администратору необходимо руководствоваться требованиями, приведенными в документах ВАМБ.00077-06 91 01 «“Валидата Клиент” версия 4. Руководство по установке и настройке», ВАМБ.00077-06 93 01 «“Валидата Клиент” версия 4. Руководство администратора информационной безопасности» и ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

Примечание — Возможно совмещение ролей администратора информационной безопасности и системного администратора.

Процедура назначения и смены персонала всех ролей, а также процедура включения/исключения персонала из ролевой модели определяется эксплуатирующей организацией.

4.1.4 Инициализация и ввод ПК «Валидата Клиент» в эксплуатацию

Установка и первоначальная настройка ПК «Валидата Клиент» выполняются в соответствии с документом ВАМБ.00077-06 91 01 «“Валидата Клиент” версия 4. Руководство по установке и настройке».

Требования по обеспечению безопасности при установке ПК «Валидата Клиент» приведены в документе ВАМБ.00077-06 93 01 «“Валидата Клиент” версия 4. Руководство администратора информационной безопасности».

4.1.5 Особенности работы с различными ключевыми носителями

ПК «Валидата Клиент» взаимодействует с ключевыми носителями с помощью СКЗИ «Валидата CSP». В связи с этим при работе с ПК «Валидата Клиент» необходимо учитывать особенности работы СКЗИ «Валидата CSP» с различными ключевыми носителями, приведенные в документе ВАМБ.00060-06 98 01 «СКЗИ «Валидата CSP» версия 6. Правила пользования».

4.2 Требования по обеспечению безопасности при эксплуатации ПК «Валидата Клиент»

4.2.1 Общие требования

При эксплуатации ПК «Валидата Клиент» следует принять следующие общие организационные меры:

- право доступа к техническим средствам (ЭВМ) с установленным ПК «Валидата Клиент» предоставляется только лицам, изучившим соответствующие эксплуатационные документы ПК «Валидата Клиент», а также другие документы, созданные на их основе;

- запрещается использование ПК «Валидата Клиент» для защиты сведений, составляющих государственную тайну;

- должны быть выполнены требования, изложенные в документах ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности» и ВАМБ.00077-06 93 01 «“Валидата Клиент” версия 4. Руководство администратора информационной безопасности», в том числе требования, определяющие:

- комплекс организационно-технических мероприятий по защите от НСД перед началом и во время работы ПК «Валидата Клиент»;
- перечень мер по обеспечению безопасности защищенной связи;
- порядок использования сторонних средств защиты от НСД;
- порядок контроля выполнения требований эксплуатационной документации ПК «Валидата Клиент»;
- требования к аутентификации пользователей, в том числе, с использованием парольных механизмов;
- порядок разграничения доступа;

- в случае функционирования ПК «Валидата Клиент» в виртуальной среде должны быть выполнены требования, изложенные в документе ВАМБ.00060-06 93 03 «СКЗИ «Валидата CSP» версия 6. Функционирование

в виртуальной среде. Руководство администратора информационной безопасности»;

- на ЭВМ с установленным ПК «Валидата Клиент» должно использоваться только лицензионное ПО фирм-производителей;
- запрещается вносить какие-либо изменения в ПО ПК «Валидата Клиент».

4.2.2 Порядок обеспечения целостности ПК «Валидата Клиент»

При использовании ПК «Валидата Клиент» необходимо организовать контроль целостности ПК «Валидата Клиент», системного ПО и всех исполняемых файлов, функционирующих совместно с ПК «Валидата Клиент», в соответствии с требованиями документа ВАМБ.00077-06 93 01 «“Валидата Клиент” версия 4. Руководство администратора информационной безопасности».

Мероприятия по контролю целостности ПК «Валидата Клиент» должны включать в себя следующие виды работ:

- контроль целостности дистрибутивов;
- первичный контроль — контроль целостности, выполняемый при установке и обновлении ПО;
- текущий (ежедневный) контроль — контроль целостности, выполняемый в процессе работы с ПО (в начале работы, во время работы или по завершении работы) пользователем или уполномоченным контролирующим лицом;
- периодический (регламентный) контроль — контроль целостности, выполняемый администратором информационной безопасности в соответствии с принятым в эксплуатирующей организации регламентом.

В общем случае для контроля целостности допускается применять один из следующих подходов:

- в качестве основного средства контроля целостности используется программа `hashfile.exe`. Целостность программы `hashfile.exe` и эталона верификации при этом обеспечивается либо средствами СЗИ от НСД, либо организационно-техническими мерами, такими как финализированная запись этих объектов на отчуждаемый носитель (CD- или DVD-диск), правила обращения с которым соответствуют правилам обращения с ключевыми носителями;
- в качестве основного средства контроля целостности используется СЗИ от НСД, а программа `hashfile.exe` при необходимости используется в качестве дополнительного средства контроля. Целостность исполняемого файла программы `hashfile.exe` и эталона верификации при этом обеспечивается средствами СЗИ от НСД.

Примечание — Эталон верификации - один из следующих объектов:

- создаваемый программой ***hashfile.exe*** файл, содержащий список файлов, подлежащих контролю целостности, и значение хэш-функции для каждого файла из данного списка;
- ветка реестра ОС Windows, содержащая перечень файлов, подлежащих контролю целостности, и значения хэш-функции для каждого файла из дан-

ного перечня.

Подробная информация об организации контроля целостности для каждого из перечисленных выше подходов, видов контроля целостности и каждого исполнения ПК «Валидата Клиент», а также порядок действий в случае нарушения контроля целостности приведены в документе ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности».

Список объектов, подлежащих контролю целостности, приведен в документе ВАМБ.00077-06 93 01 «“Валидата Клиент” версия 4. Руководство администратора информационной безопасности».

4.2.3 Порядок обеспечения работоспособности ПК «Валидата Клиент»

Проверка работоспособности ПК «Валидата Клиент» обеспечивается контролем целостности его ПО, а также проверкой работоспособности СКЗИ «Валидата CSP».

ПК «Справочник сертификатов» регистрирует следующие события:

- запуск ПК «Справочник сертификатов»;
- завершение работы ПК «Справочник сертификатов»;
- добавление объекта;
- удаление объекта;
- создание резервной копии справочника;
- восстановление справочника из резервной копии;
- формирование ключа ЭП и запроса на соответствующий сертификат ключа проверки ЭП;
- формирование запроса на аннулирование/прекращение действия сертификата;
- загрузка обновлений от ЦС или ЦР;
- установка сертификата пользователя рабочим.

Для каждого типа объекта в журнал дополнительно записывается следующая информация:

- для сертификата и шаблона сертификата: «Имя издателя», «Имя владельца», «Серийный номер», «№ ключа ЭП»;
- для запроса на создание сертификата: «Имя владельца», «№ ключа ЭП»;
- для запроса на аннулирование/прекращение действия сертификата: «Имя владельца», «Серийный номер»,
- для САС: «Имя издателя», «Номер САС», «Количество аннулированных сертификатов».

Создание резервной копии справочников сертификатов ПК «Справочник сертификатов» выполняется в соответствии с документом ВАМБ.00077-06 92 01 «“Валидата Клиент” версия 4. Справочник сертификатов. Руководство пользователя».

Дополнительно должны быть созданы резервные копии следующих веток ре-

естра ОС Windows, в которых хранятся настройки ПК «Валидата Клиент»:

- HKEY_CURRENT_USER\SOFTWARE\Validata.

Порядок действий по восстановлению работоспособности ПК «Валидата Клиент» при сбоях и в случаях нештатных ситуаций приведен в документах ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности» и ВАМБ.00077-06 93 01 «“Валидата Клиент” версия 4. Руководство администратора информационной безопасности». Порядок действий в случае нарушения контроля целостности приведен в документе ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности».

4.2.4 Контроль правильности работы ЭВМ

Для обеспечения контроля правильности работы ЭВМ с установленным ПК «Валидата Клиент» необходимо с периодом не более 168 часов (7 суток) производить перезагрузку работающей ЭВМ с установленным ПК «Валидата Клиент».

При этом перезагрузку работающей ЭВМ необходимо производить с отключением и последующим включением питания ЭВМ с целью выполнения встроенных в постоянное запоминающее устройство ЭВМ тестов проверки работоспособности аппаратных ресурсов. В случае когда после отключения питания ЭВМ дальнейшей работы с данной ЭВМ не требуется, производить перезагрузку не требуется.

Если условия эксплуатации ПК «Валидата Клиент» требуют непрерывной работы ЭВМ в течение длительного времени (более 7 суток), допустимо осуществлять перезагрузку ЭВМ с установленным ПК «Валидата Клиент» с периодом не более одного года при обязательном выполнении следующих условий:

- на ЭВМ должна быть установлена серверная ОС;
- должны использоваться ЭВМ с оперативным запоминающим устройством (ОЗУ) со встроенными средствами, обеспечивающими обнаружение и исправление ошибок памяти при сбоях ОЗУ (как минимум, с контролем четности);
- должен быть организован периодический, не реже одного раза в сутки, контроль целостности ПК «Валидата Клиент», ПК, функционирующих совместно с ПК «Валидата Клиент», системного и прикладного ПО с помощью программы контроля целостности из состава ПК «Валидата Клиент» или программы тестирования аппаратно-программных средств криптографического сервера ВАМБ.00096-06 12 07 (компонент, входящий в состав ПК ВАМБ.00096-06 «Средство криптографической защиты информации «Валидата Криптосервер» версия 4»);
- должно быть организовано периодическое, не реже одного раза в сутки, тестирование корректности работы процессора с использованием программы тестирования аппаратно-программных средств криптосервера ВАМБ.00096-06 12 07.

4.3 Требования по обеспечению безопасности при выводе ПК «Валидата Клиент» из эксплуатации и передаче в ремонт

Ключи ЭП, прекратившие свое действие, уничтожаются порядком, установленным документом ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности», а ключи проверки ЭП (в составе соответствующих сертификатов ключей проверки ЭП) установленным порядком сохраняются в архивах для возможности в последующем выполнения процедуры разбора конфликтных ситуаций.

При обновлении ПК «Валидата Клиент» необходимо выполнить подготовку к переходу на новую версию ПК «Валидата Клиент», руководствуясь требованиями эксплуатационной документации новой версии ПК «Валидата Клиент». После выполнения всех необходимых подготовительных действий (при их наличии) необходимо удалить текущую версию ПК «Валидата Клиент».

Требования к порядку проведения ремонтных и регламентных работ приведены в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

Для вывода ПК «Валидата Клиент» из эксплуатации на одном рабочем месте необходимо выполнить следующие действия:

- с использованием штатных средств СКЗИ «Валидата CSP» удалить ключи ЭП, хранящиеся в реестре ОС Windows (не требуется при переходе на новую версию ПК «Валидата Клиент»);
- удалить ПК «Валидата Клиент» в соответствии с документом ВАМБ.00077-06 91 01 «“Валидата Клиент” версия 4. Руководство по установке и настройке».

В случае вывода ПК «Валидата Клиент» из эксплуатации на всех рабочих местах эксплуатирующей организации без установки новой версии ПК «Валидата Клиент» необходимо выполнить следующие действия:

- прекратить действие ключей ЭП согласно положениям документа ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности» и требованиям УЦ;
- вывести ПК «Валидата Клиент» из эксплуатации на каждом рабочем месте в соответствии с требованиями, приведенными выше;
- вывести из эксплуатации на каждом рабочем месте эксплуатационную документацию ПК «Валидата Клиент» (например, путем удаления с ЭВМ). Рекомендуются архивировать формуляр в бумажном виде, который находится в подразделении, ответственном за эксплуатацию ПК «Валидата Клиент». Конкретный перечень подлежащих архивированию документов и срок их архивного хранения определяются эксплуатирующей организацией.

Действия, выполняемые с эталонными дистрибутивами, связанные с выводом из эксплуатации ПК «Валидата Клиент», определяются эксплуатирующей орга-

низацией. В случае уничтожения оптических носителей с эталонными дистрибутивами ПК «Валидата Клиент», данные носители должны быть уничтожены (утилизированы) способом, гарантировано исключающим восстановление информации (физическое разрушение, сжигание, разламывание, разрезание и т.п.).

5 СВЕДЕНИЯ О СОГЛАСОВАНИИ

Положения настоящего документа согласованы с ФСБ России.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
САС	Список аннулированных сертификатов
СЗИ от НСД	Средство защиты информации от несанкционированного доступа
УЦ	Удостоверяющий центр
ЭВМ	Электронно-вычислительная машина
ЭП	Электронная подпись

[illegible][illegible]