

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00096-06 98 01-ЛУ

**СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«ВАЛИДАТА КРИПТОСЕРВЕР» ВЕРСИЯ 4**

Правила пользования

ВАМБ.00096-06 98 01

2020

Аннотация

Настоящий документ содержит описание порядка использования программного комплекса ВАМБ.00096-06 «Средство криптографической защиты информации «Валидата Криптосервер» версия 4» (далее — СКЗИ «Валидата Криптосервер»).

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

Документ предназначен для пользователей, применяющих СКЗИ «Валидата Криптосервер».

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 СКЗИ «ВАЛИДАТА КРИПТОСЕРВЕР» И ЕГО ОСНОВНЫЕ ХАРАКТЕРИСТИКИ	5
1.1 Общие сведения	5
1.2 Состав, реализуемые криптографические преобразования и основные функции СКЗИ «Валидата Криптосервер»	5
1.2.1 Реализуемые криптографические алгоритмы	6
1.2.2 Основные функции СКЗИ «Валидата Криптосервер»	7
1.3 Варианты исполнения СКЗИ «Валидата Криптосервер» и выполняемые нормативные требования	11
1.4 Среда функционирования	12
1.4.1 Общие требования к среде функционирования	12
1.4.2 Минимальные требования к покупным аппаратно-программным средствам	12
1.5 Графические интерфейсы СКЗИ «Валидата Криптосервер»	13
2 КЛЮЧЕВАЯ СИСТЕМА И КЛЮЧЕВЫЕ ДОКУМЕНТЫ	14
2.1 Используемая ключевая система	14
2.2 Управление ключевой системой	14
3 ПОРЯДОК РАСПРОСТРАНЕНИЯ И УЧЁТА СКЗИ «ВАЛИДАТА КРИПТОСЕРВЕР»	16
3.1 Способы передачи и хранения СКЗИ «Валидата Криптосервер»	16
3.2 Поэкземплярный учёт СКЗИ «Валидата Криптосервер»	16
4 ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ СКЗИ «ВАЛИДАТА КРИПТОСЕРВЕР»	17
4.1 Требования по обеспечению безопасности при вводе СКЗИ «Валидата Криптосервер» в эксплуатацию	17
4.1.1 Требования к встраиванию СКЗИ «Валидата Криптосервер» в прикладные системы и к проведению исследований СКЗИ «Валидата Криптосервер»	17
4.1.2 Требования по размещению	18
4.1.3 Требования к персоналу, обеспечивающему функционирование СКЗИ «Валидата Криптосервер»	20
4.1.4 Инициализация и ввод СКЗИ «Валидата Криптосервер» в эксплуатацию	22
4.1.5 Особенности работы с различными ключевыми носителями	22
4.2 Требования по обеспечению безопасности при эксплуатации СКЗИ «Валидата Криптосервер»	23
4.2.1 Общие требования	23
4.2.2 Порядок обеспечения целостности СКЗИ «Валидата Криптосервер»	24
4.2.3 Порядок обеспечения работоспособности СКЗИ «Валидата Криптосервер»	25
4.2.4 Контроль правильности работы ЭВМ	26

4.2.5	Требования к резервному копированию и архивированию данных	26
4.3	Требования по обеспечению безопасности при выводе СКЗИ «Валидата Криптосервер» из эксплуатации и передаче в ремонт	27
5	СВЕДЕНИЯ О СОГЛАСОВАНИИ	29
	ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	30

1 НАЗНАЧЕНИЕ СКЗИ «ВАЛИДАТА КРИПТОСЕРВЕР» И ЕГО ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

1.1 Общие сведения

Программный комплекс (ПК) ВАМБ.00096-06 «Средство криптографической защиты информации «Валидата Криптосервер» версия 4» (далее — СКЗИ «Валидата Криптосервер») предназначен для использования в автоматизированных системах (АС) и ПК эксплуатирующей организации, осуществляющих автоматическое создание и автоматическую проверку электронной подписи (ЭП).

Примечание — В связи с этим требования п. 8 и п. 9 «Требований к средствам ЭП», утверждённых приказом ФСБ России от 27.12.2011 № 796, о визуализации подписываемых и проверяемых данных не применяются к СКЗИ «Валидата Криптосервер».

СКЗИ «Валидата Криптосервер» предназначено для:

- предоставления (в качестве сервера) криптографических функций прикладным серверам, клиентским рабочим местам, обращающимся к нему по протоколу удаленного вызова процедур (DCE RPC);
- контроля целостности, подтверждения авторства, неотрекаемости от авторства и обеспечения конфиденциальности электронных документов, передаваемых в режимах on-line и off-line между клиентскими рабочими местами и центрами обработки информации (ЦОИ) АС и ПК эксплуатирующей организации;
- обеспечения работы криптографического сервера (далее — КС или Криптосервер) в среде операционной системы (ОС) Windows как на одной ЭВМ, так и на нескольких ЭВМ, объединенных в кластер для повышения отказоустойчивости и/или обеспечения балансировки сетевой нагрузки (NLB);
- обеспечения удаленной загрузки ключевой информации в КС;
- использования в качестве инструментария, обеспечивающего проверку работоспособности КС.

СКЗИ «Валидата Криптосервер» функционирует совместно с ПК ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP») и ПК ВАМБ.00077-06 «Валидата Клиент» версия 4».

1.2 Состав, реализуемые криптографические преобразования и основные функции СКЗИ «Валидата Криптосервер»

В состав СКЗИ «Валидата Криптосервер» входят следующие ПК и компоненты:

- ПК ВАМБ.00096-06 12 01 «Криптографический сервер» (далее — КС или криптосервер);

- ПК ВАМБ.00096-06 12 02 «Автоматизированное рабочее место управления криптографическим сервером» (далее — АРМ УКС);
- ПК ВАМБ.00096-06 12 03 «Автоматизированное рабочее место формирования отчётов» (далее — АРМ ФО);
- ВАМБ.00096-06 12 04 «Библиотека прикладного программного интерфейса криптографического сервера для C/C++»;
- ВАМБ.00096-06 12 05 «Конфигурация криптографического сервера» (далее — программа «Конфигурация Криптосервера»);
- ВАМБ.00096-06 12 06 «Монитор криптографического сервера» (далее — программа «Монитор Криптосервера»);
- ВАМБ.00096-06 12 07 «Программа тестирования аппаратно-программных средств криптографического сервера» (далее — ПК «Программа тестирования КС»);
- ВАМБ.00096-06 12 08 «Библиотека прикладного программного интерфейса криптографического сервера для платформ “Java” и “IBM WebSphere Application Server”».

Далее библиотеки прикладного программного интерфейса криптографического сервера для C/C++ и для платформ “Java” и “IBM WebSphere Application Server” будут упоминаться как библиотека ППИ.

1.2.1 Реализуемые криптографические алгоритмы

СКЗИ «Валидата Криптосервер» реализует криптографические алгоритмы согласно следующим стандартам:

- 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 (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);
- 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 и ГОСТ 34.11-2018 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Примечания

1 Для проверки ЭП в СКЗИ «Валидата Криптосервер» 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.

СКЗИ «Валидата Криптосервер» 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 СКЗИ «Валидата Криптосервер» применяется CMS/PKCS#7 формат защищённых (подписанных и зашифрованных) данных.

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

Подробная информация о защите данных с помощью криптографических преобразований приведена в документе ВАМБ.00060-06 31 01 «СКЗИ «Валидата CSP» версия 6. Описание применения».

1.2.2 Основные функции СКЗИ «Валидата Криптосервер»

1.2.2.1 Криптографический сервер

КС обеспечивает выполнение следующих основных функций:

- 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 и файлов в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит. Создание и проверка ЭП CMS сообщений осуществляется в соответствии с Рекомендациями по стандартизации Р 1323565.1.025-2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами»;

- 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 CMS сообщений осуществляются в соответствии с Рекомендациями по стандартизации Р 1323565.1.025-2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами»;

- зашифрование и расшифрование документов в формате CMS в соответ-

ствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью. Зашифрование и расшифрование CMS сообщений осуществляются в соответствии с RFC 4357 и RFC 4490;

- реализация механизма простановки и проверки штампов времени ЭП в соответствии с RFC 3161;
- обновление списка аннулированных сертификатов (САС).

Подробный перечень функций, выполняемых КС, приведен в документе ВАМБ.00096-06 31 01 «СКЗИ «Валидата Криптосервер» версия 4. Описание применения».

1.2.2.2 Библиотека ППИ

Библиотека ППИ обеспечивает обращение к следующим функциям КС:

- зашифрованию и расшифрованию файлов в соответствии с ГОСТ 28147-89 (в режиме гаммирования с обратной связью), и ГОСТ Р 34.12-2015 (блочные шифры «Магма» и «Кузнечик») в режимах гаммирования и выработки имитовставки согласно ГОСТ Р 34.13-2015;
- зашифрованию и расшифрованию блоков памяти в соответствии с ГОСТ 28147-89 (в режиме гаммирования с обратной связью), и ГОСТ Р 34.12-2015 (блочные шифры «Магма» и «Кузнечик») в режимах гаммирования и выработки имитовставки согласно ГОСТ Р 34.13-2015;
- подписи файла в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- подписи области памяти в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- проверке ЭП файла в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- проверке ЭП области памяти в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит;
- удалению подписи;
- выработке хэш-значения для файла в соответствии с ГОСТ Р 34.11-2012 для хэш-значений длиной 256 и 512 бит;
- выработке хэш-значения для области памяти в соответствии с ГОСТ Р 34.11-2012 для хэш-значений длиной 256 и 512 бит;
- выбору и инициализации работы с КС;
- аутентификации при работе КС;
- преобразованию отделенной и совмещенной ЭП;
- выработке случайного числа заданной длины.

1.2.2.3 АРМ УКС

АРМ УКС обеспечивает поддержку функций КС и выполнение следующих основных функций:

- одновременной загрузки в заданную сессию КС как группы сертификатов из одной директории, так и каждого сертификата по отдельности;

- одновременной загрузки в заданную сессию КС как группы САС, так и каждого САС по отдельности;
- одновременной загрузки всех сертификатов и САС в заданную сессию КС (или кластера КС) из указанной папки;
- выгрузки информации о сертификатах и САС из одной криптографической сессии одного узла КС в текстовые файлы с разбиением по издателю;
- загрузки обновлений, полученных из удостоверяющего центра, в КС;
- запоминания последнего пути к папке, из которой выполнялась загрузка сертификатов, САС или обновлений;
- запуска и остановки заданной сессии КС (или кластера КС), за исключением сессии администрирования;
- плановой смены ключей ЭП и сертификатов КС (с АРМ УКС), которая должна осуществляться как на всех КС кластера одновременно, так и по отдельности на каждом КС (или группе КС) из состава кластера (по выбору пользователя);
- фильтрации записей по типу событий протокола событий просматриваемого журнала КС;
- сортировки в диалоговом окне АРМ УКС и экспорта в текстовый файл списка сертификатов, загруженных в заданную сессию КС;
- просмотра состояния узлов кластера КС (только для NLB-кластера);
- ввода (вывода) узла КС в состав кластера (только для NLB-кластера);
- вывода на экран сообщения о невозможности записи события в системный журнал с предложением вызова администратора. Работа АРМ УКС при этом не блокируется;
- удаления из сессии КС (кластера КС) всех сертификатов пользователей (кроме сертификатов Центра сертификации и Центра регистрации), которые аннулированы/прекратили действие на момент выполнения команды;
- просмотра загруженных сертификатов как всего кластера КС, так и отдельных КС из состава кластера, с возможностью фильтрации;
- добавления и удаления IP-адресов компьютеров, которым разрешен доступ к заданной сессии КС (или кластера КС), с возможностью смены данных аутентификации для ранее добавленных IP-адресов;
- отображения сертификатов заданной сессии КС (кластера КС), которые находятся в САС и время аннулирования/прекращения действия которых уже наступило на момент выполнения команды;
- отображения сертификатов заданной сессии КС (кластера КС), срок действия ключа ЭП которых уже истек на момент выполнения команды;
- визуального отображения хода загрузки сертификатов и САС, отображения процента выполнения загрузки, количества загруженных объектов, общего количества загружаемых объектов, времени начала и окончания загрузки;
- сортировки сессий в окне отображения списка сессий (по имени сессии, имени КС, номеру ключа ЭП, имени владельца, путям к справочникам), а также отображения состояния опции «Принудительно кэшировать сертификаты для шифрования при старте сессии» для каждой сессии;

- детализации информации по коду ошибки — по двойному щелчку «мышью» на строке с ошибкой просматриваемого журнала КС или по введенному коду ошибки из меню АРМ УКС;

- при обнаружении ошибки в журнале (полном или ошибок) КС в протокол работы АРМ УКС записывать данный код в поле «Код события». Отображать информационное окно при обнаружении ошибки в журнале КС или при обнаружении изменения состояния NLB-кластера КС (в случае его использования);

- отображения и очистки статистики для заданной сессии КС (кластера КС), для всех сессий КС (кластера КС);

- получения и изменения уровня протоколирования КС (или кластера КС);

- возможности блокирования обработки пользовательских запросов для заданной сессии КС (или кластера КС) с выводом на экран диалогового окна для подтверждения выполняемой операции.

1.2.2.4 АРМ ФО

АРМ ФО функционирует совместно с АРМ УКС и выполняет следующие функции:

- преобразование журнала (полного или ошибок — по выбору пользователя) КС в формат базы данных;

- отображение результата преобразования протокола КС в виде таблицы в главном окне программы;

- разбор, просмотр и анализ преобразованного журнала (полного или ошибок — по выбору пользователя);

- формирование отчёта о выполнении криптографических операций КС за интервал времени до 24 часов по всем пользователям ключевых документов, от имени которых эти операции производились;

- осуществление возможности фильтрации событий в таблице встроенными фильтрами по задаваемому интервалу времени, по задаваемому имени пользователя, по задаваемому наименованию организации и по ошибочным завершениям криптографических функций (каждым фильтром в отдельности и в их комбинациях);

- ввод и запуск на выполнение запроса на языке SQL;

- ограничение импортируемых событий по уровню (порогу) важности события при преобразовании (импорте) протоколов в базу;

- возможность сохранения сформированного отчёта и создаваемых запросов на языке SQL, а также сохранения результатов выполнения SQL-запросов и встроенных фильтров;

- одновременная загрузка журналов (полных или ошибок — по выбору пользователя) со всех узлов кластера КС и предоставление возможности просмотра протоколов на русском языке с возможностью фильтрации.

1.2.2.5 Программа «Конфигурация Криптосервера»

Программа «Конфигурация Криптосервера» выполняет:

- настройку параметров сессий КС;
- настройку параметров DCE RPC;
- настройку параметров протоколирования работы КС.

1.2.2.6 Программа «Монитор Криптосервера»

Программа «Монитор Криптосервера» выполняет:

- отображение состояния сессий криптографического сервера;
- отображение (частичное) настроек сессий криптографического сервера;
- остановку сессий криптографического сервера (за исключением сессии администрирования);
- запуск сессий криптографического сервера (за исключением сессии администрирования).

1.2.2.7 ПК «Программа тестирования КС»

ПК «Программа тестирования КС» обеспечивает:

- тестирование аппаратных компонентов КС без остановки аппаратной платформы КС и без перезагрузки ОС;
- настройку времени начала тестирования;
- контроль целостности программных средств КС.

1.3 Варианты исполнения СКЗИ «Валидата Криптосервер» и выполняемые нормативные требования

СКЗИ «Валидата Криптосервер» имеет два 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.

Используемые совместно с СКЗИ «Валидата Криптосервер» 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 Оба исполнения имеют одну и ту же программную реализацию, не зависящую от применения совместно с СКЗИ «Валидата Криптосервер» сертифицированного СЗИ от НСД.

2 В документации на СКЗИ «Валидата Криптосервер» 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.

СКЗИ «Валидата Криптосервер» удовлетворяет:

– «Специальным требованиям 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;

– «Требованиям к средствам электронной подписи», утверждённым 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;

– «Требованиям 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.

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

СКЗИ «Валидата Криптосервер» функционирует совместно с СЗИ от НСД, перечисленными в документе ВАМБ.00060-06 98 01 «СКЗИ «Валидата CSP» версия 6. Правила пользования».

1.4 Среда функционирования

1.4.1 Общие требования к среде функционирования

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

КС может функционировать как на одной отдельной ЭВМ/виртуальной машине (ВМ), так и на нескольких ЭВМ/ВМ, объединенных в кластер для повышения отказоустойчивости и/или обеспечения балансировки сетевой нагрузки.

СКЗИ «Валидата Криптосервер» функционирует совместно с системами управления базами данных из перечня, приведённого в документе ВАМБ.00077-06 98 01 «Валидата Клиент» версия 4. Правила пользования».

1.4.2 Минимальные требования к покупным аппаратно-программным средствам

ЭВМ, на которых предполагается эксплуатация СКЗИ «Валидата Криптосервер», должны удовлетворять требованиям по защите информации от утечки по

техническим каналам в соответствии с моделью угроз, принятой в АС эксплуатирующей организации.

Минимальные требования к аппаратно-программной среде функционирования СКЗИ «Валидата Криптосервер»:

- персональный компьютер (ЭВМ) с объемом жесткого диска и оперативной памяти, удовлетворяющим минимальным требованиям для установленной на данной ЭВМ версии ОС Microsoft Windows;
- при необходимости — сетевой адаптер и устройство резервного копирования информации на отчуждаемый носитель (например, CD-RW);
- средство защиты информации от несанкционированного доступа (СЗИ от НСД) — при необходимости;
- ОС семейства Windows.

Следует использовать ЭВМ с Intel-совместимым процессором с микроархитектурой Intel Core 2 или более новым, поддерживающим расширения инструкций SSE2, SSE3, SSSE3. Для повышения производительности рекомендуется использовать процессор с поддержкой расширений инструкций SSE4.1, AVX.

Примечания

1 СКЗИ «Валидата Криптосервер» может работать как в 32-битных (x86), так и 64-битных (x64) ОС Windows (выбор производится пользователем при установке СКЗИ «Валидата Криптосервер» на ЭВМ).

2 Необходимость использования СЗИ от НСД при установке и эксплуатации СКЗИ «Валидата Криптосервер» зависит от исполнения СКЗИ «Валидата Криптосервер».

1.5 Графические интерфейсы СКЗИ «Валидата Криптосервер»

СКЗИ «Валидата Криптосервер» предоставляет следующие графические интерфейсы для взаимодействия с пользователем:

- ПК «Автоматизированное рабочее место управления криптографическим сервером»;
- ПК «Автоматизированное рабочее место формирования отчетов»;
- программа «Конфигурация Криптосервера»;
- программа «Монитор Криптосервера».

Подробная информация о порядке работы с перечисленными выше интерфейсами приведена в документах ВАМБ.00096-06 31 01 «СКЗИ «Валидата Криптосервер» версия 4. Описание применения», ВАМБ.00096-06 91 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство по установке и настройке» и ВАМБ.00096-06 95 01 «СКЗИ «Валидата Криптосервер» версия 4. АРМ УКС. АРМ ФО. Руководство администратора».

2 КЛЮЧЕВАЯ СИСТЕМА И КЛЮЧЕВЫЕ ДОКУМЕНТЫ

2.1 Используемая ключевая система

В качестве ключевой системы СКЗИ «Валидата Криптосервер» 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

Для функционирования криптосервера необходимы ключи ЭП (и ключи проверки ЭП) администратора КС, администратора АРМ УКС, ключи пользовательских сессий.

Управление квалифицированными сертификатами ключей проверки ЭП при использовании СКЗИ «Валидата Криптосервер» 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 СКЗИ «Валидата Криптосервер».

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 СКЗИ «Валидата Криптосервер», 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 ВАНБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности» и ВАНБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

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

3 ПОРЯДОК РАСПРОСТРАНЕНИЯ И УЧЁТА СКЗИ «ВАЛИДАТА КРИПТОСЕРВЕР»

3.1 Способы передачи и хранения СКЗИ «Валидата Криптосервер»

Передача дистрибутива СКЗИ «Валидата Криптосервер» 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.00096-06 93 01 «СКЗИ «Валидата Криптосервер» 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 СКЗИ «Валидата Криптосервер»

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

4 ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ СКЗИ «ВАЛИДАТА КРИПТОСЕРВЕР»

4.1 Требования по обеспечению безопасности при вводе СКЗИ «Валидата Криптосервер» в эксплуатацию

4.1.1 Требования к встраиванию СКЗИ «Валидата Криптосервер» в прикладные системы и к проведению исследований СКЗИ «Валидата Криптосервер»

Встраивание СКЗИ «Валидата Криптосервер» в прикладные системы должно выполняться с использованием библиотек прикладного программного интерфейса, входящих в состав СКЗИ «Валидата Криптосервер» или в состав ПК ВАМБ.00136-06 «Средство криптографической защиты информации «Валидата Криптосервер L» версия 6».

При встраивании СКЗИ «Валидата Криптосервер» 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 документации на СКЗИ «Валидата Криптосервер»;
- проверку отсутствия ухудшений инженерно-криптографических свойств СКЗИ «Валидата Криптосервер»;
- проверку выполнения требований к контролю целостности;
- анализ документации прикладного программного обеспечения, использующего СКЗИ «Валидата Криптосервер»;
- проверку программного обеспечения (ПО) BIOS/UEFI ЭВМ, на которой функционирует СКЗИ «Валидата Криптосервер», 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 СКЗИ «Валидата Криптосервер» 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 СКЗИ «Валидата Криптосервер» должен быть обеспечен режим эксплуатации, размещения и хранения технических средств, исключающий несанкционированный доступ к этим техническим средствам. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать сохранность конфиденциальных документов и сведений, включая ключевую информацию.

При размещении технических средств с установленным СКЗИ «Валидата Криптосервер» (исполнение 1):

- должны быть приняты меры по исключению доступа в помещения, в которых размещены технические средства, лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях;
- лица, не находящиеся в списке доступа в помещения, в которых размещены технические средства, должны соответствующим образом сопровождаться и контролироваться.

При размещении технических средств с установленным СКЗИ «Валидата Криптосервер» (исполнение 2):

- должны быть приняты меры по исключению доступа в помещения, в которых размещены технические средства, лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе на этих технических средствах;
- лица, не допущенные к работе на технических средствах, должны соответствующим образом сопровождаться и контролироваться.

При размещении технических средств с установленным СКЗИ «Валидата Криптосервер» необходимо также учитывать требования к организации сетевого взаимодействия, приведенные в документе ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

Размещение и эксплуатация СКЗИ «Валидата Криптосервер» 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 предъявляются.

Технические средства, на которых предполагается эксплуатация СКЗИ «Валидата Криптосервер», 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 СКЗИ «Валидата Криптосервер» 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 СКЗИ «Валидата Криптосервер» приведены в документе ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

Перечень требований к хранению эталонного дистрибутива СКЗИ «Валидата Криптосервер», 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 СКЗИ «Валидата Криптосервер»

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

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

При эксплуатации СКЗИ «Валидата Криптосервер» должны быть определены специалисты, выполняющие следующие роли:

- ответственный за эксплуатацию СКЗИ «Валидата Криптосервер»;
- администратор КС;
- оператор КС (опционально);
- администратор АРМ УКС;
- системный администратор;
- администратор информационной безопасности.

Перечисленный выше персонал также может взаимодействовать с конечными пользователями СКЗИ «Валидата Криптосервер», использующими ключи пользовательских сессий КС.

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

Обязанности ответственного за эксплуатацию СКЗИ «Валидата Криптосервер»

Ответственный за эксплуатацию СКЗИ «Валидата Криптосервер» осуществляет следующие функции:

- организацию безопасной эксплуатации СКЗИ «Валидата Криптосервер»;
- организацию контроля за эксплуатацией СКЗИ «Валидата Криптосервер»;
- формирование, обеспечение безопасного хранения и использования ключа ЭП криптографического сервера (совместно с администратором КС);
- формирование, обеспечение безопасного хранения и использования ключей ЭП администратора АРМ УКС и пользовательских сессий КС (совместно с администратором АРМ УКС);
- руководство персоналом.

Во время отсутствия ответственного за эксплуатацию СКЗИ «Валидата Криптосервер» его обязанности выполняет администратор КС.

Обязанности администратора криптосервера

Администратор КС обеспечивает работу криптосервера. Только администратор КС имеет возможность (с использованием пароля) входа в ОС с функциями администрирования криптосервера с помощью ключа Администратора КС, а также осуществляет контроль за работой криптосервера.

Администратор КС является лицом, ответственным за использование ключа Администратора КС (сессии администрирования) и пароля ОС Windows для администрирования криптосервера, и выполняет работы по плановой смене ключа и пароля Администратора КС.

Запуск и останов криптосервера, текущий контроль целостности программных средств криптосервера могут выполняться как администратором КС, так и другим администратором СКЗИ «Валидата Криптосервер» (согласно распорядительному документу эксплуатирующей организации).

Обязанности оператора КС

Оператор КС осуществляет загрузку ключа оператора КС при запуске АРМ УКС, мониторинг работы КС, просмотр журнала сообщений и ошибок на КС и т.д.

Оператор КС является лицом, ответственным за использование ключей оператора КС.

Наличие оператора КС является опциональным.

Обязанности администратора АРМ УКС

Администратор АРМ УКС осуществляет загрузку ключа администратора АРМ УКС при запуске АРМ УКС, загрузку ключей пользователей в сессии криптосервера, мониторинг работы КС, просмотр журнала сообщений и ошибок на КС, добавление и удаление сертификатов в сессии КС, изменение настроек криптосервера (при совмещении обязанностей с администратором КС) и т.д.

Администратор АРМ УКС является лицом, ответственным за использование ключей администратора АРМ УКС.

Во время отсутствия администратора АРМ УКС его обязанности могут быть возложены на другого администратора СКЗИ «Валидата Криптосервер» (согласно распорядительному документу эксплуатирующей организации).

Обязанности администратора информационной безопасности

Администратор информационной безопасности выполняет следующие функции:

- осуществляет создание инструкций, направленных на обеспечение безопасности функционирования СКЗИ «Валидата Криптосервер», доведение данных инструкций до пользователей и контроль за их соблюдением;
- осуществляет организацию контроля целостности СКЗИ «Валидата Криптосервер»;
- осуществляет управление доступом пользователей к ПО СКЗИ «Валидата Криптосервер» 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 СКЗИ «Валидата Криптосервер» от НСД;
- производит настройку аппаратно-программных и программных средств, обеспечивающих защиту от НСД к СКЗИ «Валидата Криптосервер».

Примечание — Более подробно сведения о функциях, выполняемых администратором информационной безопасности, приведены в документе ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

Обязанности системного администратора

Системный администратор выполняет следующие функции:

- производит установку СКЗИ «Валидата Криптосервер»;
- производит установку аппаратно-программных и программных средств, обеспечивающих защиту от НСД к СКЗИ «Валидата Криптосервер»;
- производит администрирование ОС.

При выполнении своих обязанностей системному администратору необходимо руководствоваться требованиями, приведенными в документах ВАМБ.00096-06 91 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство по установке и настройке», ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности», ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

4.1.4 Инициализация и ввод СКЗИ «Валидата Криптосервер» в эксплуатацию

Установка и первоначальная настройка СКЗИ «Валидата Криптосервер» выполняются в соответствии с документом ВАМБ.00096-06 91 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство по установке и настройке».

Требования по обеспечению безопасности при установке СКЗИ «Валидата Криптосервер» приведены в документе ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

4.1.5 Особенности работы с различными ключевыми носителями

СКЗИ «Валидата Криптосервер» взаимодействует с ключевыми носителями с помощью СКЗИ «Валидата CSP». В связи с этим при работе с СКЗИ «Валидата Криптосервер» 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 СКЗИ «Валидата Криптосервер»

4.2.1 Общие требования

При эксплуатации СКЗИ «Валидата Криптосервер» необходимо принять следующие общие организационные меры:

– право доступа к техническим средствам (ЭВМ) с установленным СКЗИ «Валидата Криптосервер» предоставляется только лицам, изучившим эксплуатационные документы СКЗИ «Валидата Криптосервер», а также другие документы эксплуатирующей организации, созданные на их основе;

– запрещается использование СКЗИ «Валидата Криптосервер» 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.00096-06 93 01 «СКЗИ «Валидата Криптосервер» 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 СКЗИ «Валидата Криптосервер»;
- перечень мер по обеспечению безопасности защищенной связи;
- порядок использования сторонних средств защиты от НСД;
- порядок контроля выполнения требований эксплуатационной документации СКЗИ «Валидата Криптосервер»;
- требования к аутентификации пользователей, в том числе, с использованием парольных механизмов;
- порядок разграничения доступа;

– в случае функционирования СКЗИ «Валидата Криптосервер» 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»;

– установка ПО должна выполняться с лицензионных копий ПО, полученных официально у поставщика;

– запрещается подключение в режиме удаленного рабочего стола к ЭВМ с установленными АРМ УКС и АРМ ФО из состава СКЗИ «Валидата Криптосервер»;

– удаленное подключение к ЭВМ с установленным КС может выполняться только с ЭВМ, на которой установлен АРМ УКС. Для удаленного подключения к КС необходимо использовать средства удаленного доступа, входящие в состав используемой ОС, при этом защита канала должна обеспечиваться с использованием ключей ЭП и сертификатов АРМ УКС и сессии администрирования с помощью сертифицированных средств криптографической защиты соответствующего класса (не ниже КС1 — для исполнения 1, не ниже КС2 — для исполнения

2), поддерживающих работу с данными ключами ЭП и обеспечивающих шифрование и двухстороннюю аутентификацию с использованием протоколов TLS или IPSec. В этом случае сертификаты АРМ УКС (оператора КС или Администратора АРМ УКС) и сессии администрирования дополнительно должны удовлетворять требованиям к сертификатам, которые предъявляет средство криптографической защиты, используемое для защиты канала связи;

- файловые системы ЭВМ с установленным КС, АРМ УКС и АРМ ФО должны содержать только программные средства, необходимые для эксплуатации соответствующих рабочих мест. Запрещается устанавливать, создавать и выполнять на этих рабочих местах посторонние программы;

- запрещается вносить какие-либо изменения в ПО СКЗИ «Валидата Криптосервер».

4.2.2 Порядок обеспечения целостности СКЗИ «Валидата Криптосервер»

При использовании СКЗИ «Валидата Криптосервер» необходимо организовать контроль целостности СКЗИ «Валидата Криптосервер», системного ПО и всех исполняемых файлов, функционирующих совместно с СКЗИ «Валидата Криптосервер», в соответствии с требованиями документа ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

Мероприятия по контролю целостности СКЗИ «Валидата Криптосервер» 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 сред-

ствами 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 данного перечня.

Подробная информация об организации контроля целостности для каждого из перечисленных выше подходов, видов контроля целостности и каждого исполнения СКЗИ «Валидата Криптосервер», 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.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

4.2.3 Порядок обеспечения работоспособности СКЗИ «Валидата Криптосервер»

Проверка корректности работы КС (самотестирование) выполняется программой тестирования аппаратно-программных средств КС. Процедура самотестирования обязательно выполняется один раз при загрузке КС, а затем периодически — через временной интервал, указанный в конфигурации КС. При обнаружении ошибки при проведении самотестирования КС записывает сообщение об этой ошибке в протокол КС и завершает свою работу. Состав тестируемых функций и описание программы приведены в документе ВАМБ.00096-06 92 01 «СКЗИ «Валидата Криптосервер» версия 4. Программа тестирования аппаратно-программных средств криптографического сервера. Руководство пользователя».

СКЗИ «Валидата Криптосервер» регистрирует следующие события:

- запуск КС;
- остановка КС;
- команды управления КС;
- подключение пользовательского процесса к КС;
- выполнение ЭП;
- проверка ЭП;
- выполнение хэширования;
- выполнение шифрования/расшифрования;
- отключение пользовательского процесса;
- события диагностики (при задании в конфигурационном файле).

Создание резервных копий СКЗИ «Валидата Криптосервер» выполняется в

соответствии с п. 4.2.5 настоящего документа.

Порядок действий по восстановлению работоспособности СКЗИ «Валидата Криптосервер» 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.00096-06 93 01 «СКЗИ «Валидата Криптосервер» 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 СКЗИ «Валидата Криптосервер» необходимо с периодом не более 168 часов (7 суток) производить перезагрузку работающей ЭВМ с установленной СКЗИ «Валидата Криптосервер».

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 КС требуют непрерывной работы ЭВМ в течение длительного времени (более 7 суток), допустимо осуществлять перезагрузку ЭВМ с установленным ПО КС 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 ПО КС, системного и прикладного ПО с помощью программы контроля целостности из состава СКЗИ «Валидата CSP» или программы тестирования аппаратно-программных средств криптографического сервера из состава СКЗИ «Валидата Криптосервер»;
- должно быть организовано периодическое, не реже одного раза в сутки, тестирование корректности работы процессора с использованием программы тестирования аппаратно-программных средств криптосервера из состава СКЗИ «Валидата Криптосервер».

4.2.5 Требования к резервному копированию и архивированию данных

В процессе работы СКЗИ «Валидата Криптосервер» необходимо организовать периодическое резервное копирование следующих данных:

- персональный справочник сертификатов, содержащий корневые сертифи-

каты;

- резервная копия (Backup) базы данных КС, содержащей сертификаты и САС.

Подробно организация резервного копирования приведена в документе ВАМБ.00077-06 91 01 «Валидата Клиент» версия 4. Руководство по установке и настройке».

Дополнительно должны быть созданы резервные копии следующих веток реестра ОС Windows, в которых хранятся настройки СКЗИ «Валидата Криптосервер»:

- HKEY_LOCAL_MACHINE\SOFTWARE\Validata;
- HKEY_CURRENT_USER\SOFTWARE\Validata.

Необходимо регулярно архивировать все файлы протокола работы КС за период, прошедший с предыдущего архивирования протоколов.

Период резервного копирования и архивирования данных, а также срок хранения архивов должны быть указаны в эксплуатационной документации АС, в которой применяется СКЗИ «Валидата Криптосервер».

4.3 Требования по обеспечению безопасности при выводе СКЗИ «Валидата Криптосервер» 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 СКЗИ «Валидата Криптосервер» необходимо выполнить подготовку к переходу на новую версию СКЗИ «Валидата Криптосервер», руководствуясь требованиями эксплуатационной документации новой версии СКЗИ «Валидата Криптосервер». После выполнения всех необходимых подготовительных действий (при их наличии) необходимо удалить текущую версию СКЗИ «Валидата Криптосервер».

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 СКЗИ «Валидата Криптосервер» из эксплуатации на одном рабочем месте необходимо выполнить следующие действия:

- с использованием штатных средств СКЗИ «Валидата Криптосервер» удалить ключи ЭП, хранящиеся в реестре ОС Windows (не требуется при переходе на новую версию СКЗИ «Валидата Криптосервер»);

– удалить СКЗИ «Валидата Криптосервер» в соответствии с документом ВАМБ.00096-06 91 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство по установке и настройке».

В случае вывода СКЗИ «Валидата Криптосервер» из эксплуатации на всех рабочих местах эксплуатирующей организации без установки новой версии СКЗИ «Валидата Криптосервер» 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 СКЗИ «Валидата Криптосервер» из эксплуатации на каждом рабочем месте в соответствии с требованиями, приведенными выше;

– вывести из эксплуатации на каждом рабочем месте эксплуатационную документацию СКЗИ «Валидата Криптосервер» (например, путем удаления с ЭВМ). Рекомендуется архивировать журналы (см. документы ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности» и ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности») и формуляр в бумажном виде, который находится в подразделении, ответственном за эксплуатацию СКЗИ «Валидата Криптосервер». Конкретный перечень подлежащих архивированию документов и срок их архивного хранения определяются эксплуатирующей организацией.

Действия, выполняемые с эталонными дистрибутивами, связанные с выводом из эксплуатации СКЗИ «Валидата Криптосервер», определяются эксплуатирующей организацией. В случае уничтожения оптических носителей с эталонными дистрибутивами СКЗИ «Валидата Криптосервер», данные носители должны быть уничтожены (утилизированы) способом, гарантированно исключающим восстановление информации (физическое разрушение, сжигание, разламывание, разрезание и т.п.).

5 СВЕДЕНИЯ О СОГЛАСОВАНИИ

Положения настоящего документа согласованы с ФСБ России.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АС	Автоматизированная система
АРМ УКС	Автоматизированное рабочее место управления криптографического сервера
АРМ ФО	Автоматизированное рабочее место формирования отчётов
ВМ	Виртуальная машина
НСД	Несанкционированный доступ
КС	Криптографический сервер
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
ПК	Программный комплекс
САС	Список аннулированных сертификатов
СЗИ от НСД	Средство защиты информации от несанкционированного доступа
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр
ЦОИ	Центр обработки информации
ЭВМ	Электронно-вычислительная машина
ЭП	Электронная подпись

[illegible][illegible]