

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-06-ЛУ

**СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«ВАЛИДАТА CSP» ВЕРСИЯ 6**

Руководство администратора информационной безопасности

ВАМБ.00060-06 93 01

2020

Аннотация

Данный документ содержит основные правила, связанные с эксплуатацией программного комплекса (ПК) ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP»), в том числе следующие рекомендации:

- рекомендации по эксплуатации технических средств с установленным СКЗИ «Валидата CSP»;
- рекомендации по размещению технических средств с установленным СКЗИ «Валидата CSP»;
- рекомендации по применению средств защиты информации от несанкционированного доступа;
- рекомендации по ведению журналов;
- рекомендации по обеспечению информационной безопасности.

Указанные в настоящем руководстве требования являются общими как для СКЗИ «Валидата CSP», так и для ПК, функционирующих совместно с СКЗИ «Валидата CSP». Каждое требование, предъявляемое к условиям эксплуатации СКЗИ «Валидата CSP», либо предъявляется к функционирующим совместно с ним ПК без изменений (в этом случае оно не указывается в перечне требований к соответствующему ПК), либо ужесточается (в этом случае в перечне требований к соответствующему ПК приводится уточнённая формулировка). Требования к ПК, функционирующим совместно с СКЗИ «Валидата CSP», могут содержать дополнительные требования, не входящие в настоящее руководство. Перечень требований для каждого ПК, функционирующего совместно с СКЗИ «Валидата CSP», приведён в руководстве Администратора информационной безопасности соответствующего ПК.

Данный документ предназначен для администраторов информационной безопасности и системных администраторов и может служить руководством для разработки инструкций администраторам информационной безопасности и пользователям, эксплуатирующим СКЗИ «Валидата CSP». Перед чтением настоящего руководства необходимо ознакомиться с эксплуатационными документами СКЗИ «Валидата CSP», приведёнными в документе ВАМБ.00060-06 20 01 «СКЗИ «Валидата CSP» версия 6. Ведомость эксплуатационных документов».

Содержание

1 ВВЕДЕНИЕ	5
2 ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРОПРИЯТИЯ	6
2.1 Общие требования	6
2.2 Правила обращения с ключевой информацией и ключевыми носителями	6
2.2.1 Правила хранения ключевых носителей	7
2.2.2 Контроль срока действия ключей	7
2.2.3 Уничтожение ключей	7
2.2.4 Компрометация ключей	8
2.2.5 Использование устройств HSM	9
2.3 Требования по защите от НСД при эксплуатации СКЗИ «Валидата CSP»	9
2.3.1 Требования по размещению технических средств	10
2.3.2 Требования по установке программного обеспечения на ЭВМ .	10
2.3.3 Настройка ЭВМ для работы с СКЗИ «Валидата CSP»	11
2.3.4 Эксплуатация ЭВМ с установленным СКЗИ «Валидата CSP» . .	13
2.3.5 Требования к аутентификации пользователей	15
2.3.6 Требования к использованию программных средств защиты информации	15
2.4 Требования к антивирусной защите	16
2.5 Требования к межсетевым экранам	17
2.6 Требования по обеспечению безопасности подключения к сетям связи	17
2.6.1 Требования по обеспечению безопасности подключения к сетям общего пользования	17
2.6.2 Требования по обеспечению безопасности подключения к се- тям связи для ОС, поддержка которых прекращена	18
2.7 Парольная защита ЭВМ	18
2.8 Требования к порядку проведения ремонтных и регламентных работ	19
2.9 Требования к отключению функций телеметрии в ОС Windows 10, Windows Server 2016 и Windows Server 2019	20
2.10 Применение СЗИ от НСД	21
2.11 Установка и настройка средств создания замкнутой программной среды	21
3 КОНТРОЛЬ ЦЕЛОСТНОСТИ ПО	22
3.1 Перечень модулей СКЗИ «Валидата CSP», подлежащих контролю целостности	22
3.2 Перечень модулей системного ПО, подлежащих контролю целостности	24
3.3 Перечень модулей ПО средств виртуализации, подлежащих контролю целостности	25

4	КОНТРОЛЬ ПРАВИЛЬНОСТИ РАБОТЫ ЭВМ	26
5	РЕЖИМ НЕШТАТНОЙ СИТУАЦИИ	27
6	ВЕДЕНИЕ ЖУРНАЛОВ	29
7	ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ ВЫПОЛНЕНИЯ РАБОТ	30
	ПРИЛОЖЕНИЕ А. ПРИМЕР НАСТРОЕК ОС WINDOWS ДЛЯ ЗАЩИТЫ ОТ НСД	31
	ПРИЛОЖЕНИЕ Б. ФОРМЫ ЖУРНАЛОВ	33
	ПРИЛОЖЕНИЕ В. РЕКОМЕНДУЕМАЯ ФОРМА АКТА УНИЧТОЖЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ	34
	ПРИЛОЖЕНИЕ Г. АКТ ГОТОВНОСТИ К РАБОТЕ	35
	ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	37

1 ВВЕДЕНИЕ

В организации, эксплуатирующей программный комплекс (ПК) ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP»), должен быть назначен ответственный за организацию работ по безопасному использованию СКЗИ «Валидата CSP» (далее — Администратор информационной безопасности).

Примечание — При необходимости функции Администратора информационной безопасности могут быть возложены на нескольких сотрудников или на подразделение.

На Администратора информационной безопасности возлагается:

- создание инструкций, направленных на обеспечение безопасности функционирования СКЗИ «Валидата CSP», доведение данных инструкций до пользователей и контроль за их соблюдением;
- контроль соблюдения описанных в настоящем руководстве требований;
- контроль выполнения всех вводимых на технологическом участке организационно-технических мер защиты рабочих мест с установленным СКЗИ «Валидата CSP» от несанкционированного доступа (НСД);
- администрирование программно-аппаратных и программных средств защиты информации от НСД (СЗИ от НСД) на рабочих местах с установленным СКЗИ «Валидата CSP»;
- контроль выполнения работ по проверке целостности СКЗИ «Валидата CSP»;
- управление доступом пользователей к программному обеспечению (ПО) и данным, включая установку и периодическую смену паролей;
- определение конкретных настроек ОС и её конфигурирование в целях защиты СКЗИ «Валидата CSP» от НСД в соответствии с положениями настоящего документа (пример настроек приведён в приложении А).

2 ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРОПРИЯТИЯ

2.1 Общие требования

При эксплуатации СКЗИ «Валидата CSP» следует принять следующие общие организационные меры:

- право доступа к техническим средствам (далее — ЭВМ) с установленным СКЗИ «Валидата CSP» предоставляется только лицам, изучившим соответствующие эксплуатационные документы СКЗИ «Валидата CSP», а также другие документы, созданные на их основе;
- запрещается использование СКЗИ «Валидата CSP» для защиты сведений, составляющих государственную тайну;
- в случае функционирования СКЗИ «Валидата CSP» 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»;
- должны соблюдаться требования по контролю целостности ПО, изложенные в разделе 3 настоящего документа;
- на ЭВМ с установленным СКЗИ «Валидата CSP» должно использоваться только лицензионное ПО фирм-производителей;
- запрещается вносить какие-либо изменения в ПО СКЗИ «Валидата CSP».

2.2 Правила обращения с ключевой информацией и ключевыми носителями

В качестве носителей ключевой информации в СКЗИ «Валидата CSP» могут использоваться только ключевые носители, приведённые в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр». Хранение ключей электронной подписи (ЭП) в реестре ОС Windows допустимо только при условии распространения на ЭВМ требований по хранению ключевых носителей.

При работе с ключевой информацией следует руководствоваться следующими требованиями:

- ключевая информация является конфиденциальной;
- запрещается оставлять без контроля носители ключевой информации;
- запрещается осуществлять несанкционированное Администратором информационной безопасности копирование ключевых носителей;
- копирование ключевой информации выполняется (при необходимости) только средствами устройства Hardware Security Module (только для ключей, хранящихся в устройстве HSM) или с помощью программы конфигурации СКЗИ «Валидата CSP»;
- запрещается разглашать ключевую информацию или передавать ключе-

вые носители лицам, к ним не допущенным, выводить ключевую информацию на экран, принтер и иные средства отображения информации;

- запрещается записывать на ключевые носители постороннюю информацию;

- запрещается использовать носители ключевой информации в режимах, не предусмотренных эксплуатационной документацией СКЗИ «Валидата CSP»;

- ключевая информация должна уничтожаться порядком, изложенным в п. 2.2.3 настоящего документа.

2.2.1 Правила хранения ключевых носителей

Ключевые носители необходимо хранить способом, исключающим несанкционированный доступ к этим ключевым носителям. В случае централизованного хранения ключевых носителей ответственность за хранение ключевых носителей пользователей несёт Администратор информационной безопасности, иначе пользователь лично несёт ответственность за хранение своих ключевых носителей.

В случае невозможности отчуждения ключевого носителя с ключевой информацией от ЭВМ организационно-техническими мероприятиями должен быть исключён доступ неуполномоченных лиц к этой ЭВМ.

2.2.2 Контроль срока действия ключей

Сроки действия ключей и сертификатов приведены в документе ВАМБ.00060-06 31 01 «СКЗИ «Валидата CSP» версия 6. Описание применения».

Для обеспечения непрерывной работы СКЗИ «Валидата CSP» с системой управления сертификатами следует в соответствии с эксплуатационной документацией СКЗИ «Валидата CSP» и ПК, функционирующих совместно с СКЗИ «Валидата CSP», а также с требованиями эксплуатирующей организации сформировать комплекс организационных мер по обращению с ключами и сертификатами (создание резервных копий ключей, соблюдение сроков действия, выведение из действия, плановая и внеплановая смена, действия в условиях компрометации ключей и др.) и организовать контроль их выполнения.

2.2.3 Уничтожение ключей

Выведенные из действия (после плановой смены или компрометации) ключи ЭП подлежат уничтожению (удалению). Уничтожение ключей должно выполняться комиссионно.

Удаление ключей, хранящихся в устройстве HSM, выполняется в соответствии с эксплуатационной документацией используемого устройства HSM.

Удаление ключей, хранящихся на всех остальных типах ключевых носителей, поддерживаемых СКЗИ «Валидата CSP», выполняется с использованием программы конфигурации СКЗИ «Валидата CSP» согласно процедуре, описанной в документе ВАМБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора».

Ключевые носители, ключевая информация с которых была удалена указанным выше способом, могут быть использованы в дальнейшей работе без ограни-

чений.

При выходе ключевых носителей из строя или при наступлении событий, требующих уничтожения ключевых носителей, они должны быть уничтожены (утилизированы) способом, гарантировано исключающим восстановление ключевой информации (физическое разрушение, сжигание, разламывание, разрезание и т.п.).

При уничтожении ключевой информации составляется Акт уничтожения ключевой информации и производится соответствующая запись в «Журнал учёта ключевой информации». Рекомендуемая форма журнала приведена в приложении Б. Рекомендуемая форма Акта приведена в приложении В.

2.2.4 Компрометация ключей

Компрометацией ключей называется событие, приводящее к утрате доверия к тому, что используемые ключи обеспечивают безопасность информации.

К основным событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие события:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключей ЭП;
- возникновение подозрений на утечку информации или её искажение в системе конфиденциальной связи;
- нарушение печати на сейфе (или на упаковке), в котором хранятся ключевые носители;
- случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что выход из строя произошёл в результате несанкционированных действий злоумышленника).

Различают два вида компрометации ключей ЭП: явную и неявную. Первые четыре события, приведённые выше, должны трактоваться как явная компрометация ключей. Остальные события требуют специального рассмотрения в каждом конкретном случае.

При наступлении любого из перечисленных выше событий (связанных как с явной, так и с неявной компрометацией) пользователь должен немедленно прекратить связь с другими пользователями с использованием скомпрометированного ключа (или ключей). Пользователь (или Администратор информационной безопасности) должен немедленно известить о компрометации ключей пользователя Удостоверяющий центр (УЦ), выдавший соответствующие сертификаты ключей проверки ЭП.

По факту компрометации ключа (за исключением увольнения сотрудников, имевших доступ к ключевой информации) должно быть проведено служебное расследование силами специально созданной для этого комиссии. Целью расследования должно быть принятие мер, исключающих такую компрометацию в будущем. В случае неявной компрометации данная комиссия дополнительно

выдает заключение о том, могла ли критичная информация о ключе попасть к нарушителю.

В случае явной компрометации следует вывести из действия скомпрометированные ключи и незамедлительно приступить к восстановлению защищённой связи (получению новых ключей) установленным порядком.

Аналогичные действия следует предпринять в случае неявной компрометации, если не представляется возможным выдать заключение достаточно быстро (за время, на которое допустимо прекращение связи). Вместе с тем работу комиссии следует продолжить до получения окончательных выводов.

Выведенные из действия скомпрометированные ключи после проведения служебного расследования уничтожаются порядком, изложенным в п. 2.2.3 настоящего документа.

2.2.5 Использование устройств HSM

В случае использования устройства HSM для генерации и хранения ключей ЭП, а также для создания ЭП, для обеспечения информационной безопасности необходимо в дополнение к требованиям, изложенным в настоящем документе, руководствоваться положениями, приведёнными в эксплуатационной документации используемого устройства HSM.

В случае подключения устройства HSM к компонентам СКЗИ «Валидата CSP» с использованием незащищенного канала необходимо обеспечить защиту данного канала следующими организационно-техническими мерами:

- устройство HSM и все подключаемые к нему компоненты СКЗИ «Валидата CSP» должны располагаться в одной серверной стойке, находящейся в охраняемом помещении;
- компоненты СКЗИ «Валидата CSP» должны подключаться к устройству HSM посредством выделенного сетевого сегмента;
- не допускается подключение к указанному сетевому сегменту оборудования, не расположенного в этой стойке, а также выход указанного сетевого сегмента за пределы данной стойки;
- доступ в помещение без сопровождения должен иметь только персонал, допущенный к работе на технических средствах с установленными компонентами СКЗИ «Валидата CSP», расположенных в данном помещении.

2.3 Требования по защите от НСД при эксплуатации СКЗИ «Валидата CSP»

Защита ПО и аппаратного обеспечения от НСД при установке и использовании СКЗИ «Валидата CSP» является составной частью общей задачи обеспечения безопасности информации в автоматизированных системах и ПК эксплуатирующей организации. Для обеспечения защиты информации от НСД необходимо выполнение целого ряда мер, включающих организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление соответствующих правил для персонала, администраторов информационной безопасности и пользователей СКЗИ «Валидата CSP». Защита СКЗИ «Валидата CSP» от НСД в автоматизированных системах и ПК

эксплуатирующей организации должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования СКЗИ «Валидата CSP», в том числе при проведении ремонтных работ.

Защита информации от НСД должна предусматривать контроль эффективности СЗИ от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или Администратором информационной безопасности.

2.3.1 Требования по размещению технических средств

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

При размещении стационарных ЭВМ с установленным СКЗИ «Валидата CSP»:

- должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства с установленным СКЗИ «Валидата CSP», 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 СКЗИ «Валидата CSP».

2.3.2 Требования по установке программного обеспечения на ЭВМ

К установке СКЗИ «Валидата CSP», системного и специального ПО допускаются лица, изучившие соответствующую эксплуатационную документацию.

2.3.2.1 Установка СКЗИ «Валидата CSP»

Установка СКЗИ «Валидата CSP» на ЭВМ должна выполняться с передаточного носителя, поставляемого в виде оптического диска или в электронном виде. Поставляемые в электронном виде передаточные носители в обязательном порядке должны быть защищены ЭП.

Перед установкой СКЗИ «Валидата CSP» с передаточного носителя, полученного в виде оптического диска, должна быть выполнена проверка целостности файлов на передаточном носителе с использованием программы контроля целостности.

Перед установкой СКЗИ «Валидата CSP» с передаточного носителя, полученного в электронном виде, должна быть проверена ЭП данного передаточного носителя с использованием СКЗИ «Валидата CSP» или иного сертифицированного средства ЭП.

Администратор информационной безопасности должен заблаговременно обеспечить загрузку на ЭВМ, на которой выполняется проверка ЭП полученного в электронном виде передаточного носителя, актуальных сертификатов и списков аннулированных сертификатов, необходимых для проверки ЭП.

2.3.2.2 Установка системного и специального ПО

При установке системного и специального ПО следует соблюдать следующие требования:

- установка ПО должна выполняться с лицензионных копий ПО, полученных официально у поставщика;
- на ЭВМ должна быть установлена только одна ОС (в случае работы в виртуальной среде — только одна родительская (host) ОС);
- не должны использоваться нестандартные, изменённые или отладочные версии ОС;
- оборудование, на которое устанавливается СКЗИ «Валидата CSP», не должно создавать угрозу безопасности ОС. Недопустимо использовать нестандартные аппаратные средства, имеющие возможность влиять на нормальный ход работы компьютера или ОС;
- запрещается устанавливать средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано Администратором информационной безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти ЭВМ и приложений, использующих СКЗИ «Валидата CSP», а также для просмотра кода и памяти ЭВМ и приложений, использующих СКЗИ «Валидата CSP», в процессе обработки СКЗИ «Валидата CSP» защищаемой информации и/или при загруженной ключевой информации;
- ПО, устанавливаемое на ЭВМ, не должно содержать возможностей, позволяющих:
 - модифицировать содержимое произвольных областей памяти;
 - модифицировать собственный код и код других подпрограмм;
 - модифицировать память, выделенную для других подпрограмм;
 - передавать управление в область собственных данных и данных других подпрограмм;
 - несанкционировано модифицировать файлы, содержащие исполняемые коды при их хранении на жёстком диске;
 - повышать предоставленные привилегии;
 - модифицировать настройки ОС;
 - использовать не документированные фирмой-разработчиком функции ОС;
- правом установки и настройки ОС должен обладать системный администратор, но только под контролем Администратора информационной безопасности.

2.3.3 Настройка ЭВМ для работы с СКЗИ «Валидата CSP»

Администратор информационной безопасности должен сконфигурировать ОС, в среде которой планируется использовать СКЗИ «Валидата CSP», и осуществлять периодический контроль выполненных настроек в соответствии со следующими требованиями:

– настройки для работы прикладного ПО не должны противоречить настройкам для работы с СКЗИ «Валидата CSP» и не должны понижать безопасность СКЗИ «Валидата CSP» и защищаемой им информации;

– должна быть исключена возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;

– в BIOS/UEFI ЭВМ должны быть заданы установки, исключающие возможность загрузки ОС, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-R и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ЭВМ с BIOS/UEFI, исключающими возможность отключения сетевой загрузки ОС;

– средствами BIOS/UEFI должна быть исключена возможность отключения пользователями ISA и PCI устройств при использовании СЗИ от НСД, устанавливаемых в ISA и PCI разъем;

– необходимо предусмотреть меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части ЭВМ (например, путем опечатывания системного блока и разъемов ЭВМ);

– режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;

– всем пользователям и группам, зарегистрированным в ОС, должны быть назначены минимально возможные для выполнения служебных обязанностей права;

– все неиспользуемые ресурсы системы должны быть отключены (протоколы, сервисы и т.п.);

– необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

- системному реестру;
- файлам и каталогам;
- временным файлам;
- журналам системы;
- файлам подкачки;
- кэшируемой информации (паролям и т.п.);
- отладочной информации;

– необходимо организовать затирание (по окончании сеанса работы СКЗИ «Валидата CSP») файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ «Валидата CSP»;

– необходимо отключить функции телеметрии в ОС Windows 10, Windows Server 2016 и Windows Server 2019 в соответствии с требованиями, изложенными в подразделе 2.9;

– необходимо отключить механизм дополнительной защиты Local Security Authority (LSA) RunAsPPL в ОС Windows, поскольку данный механизм несовместим с реализованной в СКЗИ «Валидата CSP» защитой исполняемых модулей посредством ЭП;

Примечание — Подробная информация об отключении данного механизма приведена в статье по ссылке <https://docs.microsoft.com/ru-ru/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection>.

– необходимо регулярно в соответствии с нормативными документами и указаниями эксплуатирующей организации устанавливать пакеты обновления безопасности ОС, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам информационной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС. Рекомендуется иметь эталонные ЭВМ для проверки влияния поступающих обновлений ОС на функционирование операционной системы, СКЗИ «Валидата CSP» и ПК, функционирующих совместно с СКЗИ «Валидата CSP». При наличии негативного влияния обновлений ОС на функционирование операционной системы, СКЗИ «Валидата CSP» и ПК, функционирующих совместно с СКЗИ «Валидата CSP», устанавливать данное обновление на ЭВМ пользователей не рекомендуется;

– в случае подключения ЭВМ к сетям общего пользования (СОП) необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

В случае необходимости управления, администрирования и модификации ОС и её настроек с ЭВМ, отличной от ЭВМ с установленным СКЗИ «Валидата CSP» (далее — удаленная ЭВМ), должны выполняться следующие требования:

– не допускается обращаться к функциям, связанным с использованием СКЗИ «Валидата CSP» и/или управлением ключевой информацией СКЗИ «Валидата CSP»;

– должна обеспечиваться защита канала типа «точка-точка» между удаленной ЭВМ и ЭВМ с установленным СКЗИ «Валидата CSP» с использованием сертифицированных СКЗИ соответствующего класса (не ниже KC1 — для исполнения 1, не ниже KC2 — для исполнения 2, не ниже KC3 — для исполнения 3), обеспечивающих шифрование и двустороннюю аутентификацию с использованием протоколов TLS или IPSec.

2.3.4 Эксплуатация ЭВМ с установленным СКЗИ «Валидата CSP»

Правила обращения с ключевыми носителями (в том числе учёта и хранения) и эксплуатации ЭВМ с установленным СКЗИ «Валидата CSP» регламентируются отдельной инструкцией, разрабатываемой в эксплуатирующей организации на основе эксплуатационной документации СКЗИ «Валидата CSP», а также нормативных и организационно-распорядительных документов эксплуатирующей организации.

При эксплуатации СКЗИ «Валидата CSP» должны соблюдаться следующие требования:

– необходимо разработать и применить политику назначения и смены паро-

лей (для входа в ОС, BIOS/UEFI и т.д.), использовать фильтры паролей в соответствии с правилами, указанными в подразделе 2.7 настоящего документа;

- пароль для входа в BIOS/UEFI должен быть известен только системному администратору и быть отличным от пароля системного администратора для входа в ОС;

- запрещается оставлять включенные вычислительные средства, на которых эксплуатируется СКЗИ «Валидата CSP», без принятия мер ограничения доступа к их использованию (например, включение парольной заставки);

- запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ «Валидата CSP», после ввода ключевой информации либо иной информации ограниченного доступа;

- должны соблюдаться правила обращения с ключевыми носителями, изложенные в подразделе 2.2 настоящего документа;

- в случае использования персональных идентификаторов программно-аппаратных СЗИ от НСД правила обращения с ключевыми носителями и ключевой информацией, изложенные в подразделе 2.2 настоящего документа, распространяются на данные персональные идентификаторы;

- должна быть исключена возможность работы на ЭВМ с установленным СКЗИ «Валидата CSP», если во время её начальной загрузки не проходят встроенные тесты, а также если имеются сбои или отказы в работе СЗИ от НСД;

- должны соблюдаться правила подключения к сетям связи, изложенные в подразделе 2.6 настоящего документа;

- должны соблюдаться правила аутентификации пользователей, изложенные в п. 2.3.5 настоящего документа;

- должны соблюдаться требования по контролю правильности работы аппаратных средств, изложенные в разделе 4;

- необходимо организовать и использовать систему аудита, организовать регулярный анализ результатов аудита. При этом анализ содержания системных журналов и протоколов регистрации работы СЗИ от НСД должен выполняться Администратором информационной безопасности с периодом не более 30 дней;

- периодически Администратором информационной безопасности должны контролироваться сохранность оборудования и целостность печатей на ЭВМ;

- необходимо исключить одновременную работу в ОС с работающим СКЗИ «Валидата CSP» и загруженной ключевой информацией нескольких пользователей в случае, когда невозможно организационно-техническими мерами исключить доступ пользователя к ключевой информации других пользователей;

- запрещается снятие задач с выполнения при помощи выключения питания ЭВМ или нажатия на кнопку «RESET» на системном блоке (для выхода из работы необходимо применять штатные процедуры, принятые в соответствующей ОС);

- запрещается несанкционированное вскрытие системных блоков и работа при нарушении целостности печатей (на системных блоках).

Кроме того, должно быть запрещено несанкционированное Администратором информационной безопасности подключение к ЭВМ с установленным

СКЗИ «Валидата CSP» в режиме удаленного рабочего стола. Санкционированное Администратором информационной безопасности подключение в режиме удаленного рабочего стола допускается только для пользователей, не имеющих прав локального администратора, и должно выполняться одним из следующих способов:

- удаленный доступ к терминальным серверам из состава ОС Windows Server (Microsoft Terminal Services) по протоколу RDP (Remote Desktop Protocol) с защитой передаваемой информации шифрованием и аутентификацией путем использования сертифицированной реализации протокола TLS или IPsec;
- удаленный доступ к терминальным серверам из состава ОС Windows Server (Microsoft Terminal Services) через входящий в состав ОС Windows Server шлюз терминальных серверов (Terminal Services Gateway) протоколу RDP с защитой передаваемой информации шифрованием и аутентификацией путем использования сертифицированной реализации протокола TLS или IPsec;
- удаленный доступ к терминальным серверам, находящихся под управлением Citrix XenDesktop/XenApp версия 7, по протоколу ICA (Independent Computing Architecture) по сетевому каналу, защищенному шифрованием и аутентификацией путем использования сертифицированной реализации протокола TLS или IPsec.

Пользователи должны своевременно ставить Администратора информационной безопасности в известность обо всех инцидентах и подозрительных случаях, произошедших при работе на ЭВМ с установленным СКЗИ «Валидата CSP».

В случаях обнаружения «посторонних» программ, нарушения целостности ПО ЭВМ либо выявления факта повреждения печатей на системных блоках работа на данной ЭВМ должна быть прекращена. По выявленным фактам проводится служебное расследование комиссией, в состав которой рекомендуется включать представителей службы информатизации и службы безопасности и защиты информации эксплуатирующей организации. При необходимости к работе комиссии могут быть привлечены представители ФСБ России и организации-разработчика.

Комиссия проводит работы по анализу причин и формирует предложения по ликвидации негативных последствий выявленных нарушений.

2.3.5 Требования к аутентификации пользователей

При встраивании СКЗИ «Валидата CSP» в прикладное ПО аутентификация субъектов должна осуществляться до начала выполнения первого программного модуля. Кроме того, при встраивании СКЗИ «Валидата CSP» (исполнение 2 или исполнение 3) аутентификация субъектов должна выполняться до загрузки ОС. При отрицательном результате аутентификации работа ПО СКЗИ «Валидата CSP» должна быть заблокирована.

2.3.6 Требования к использованию программных средств защиты информации

Для реализации отдельных требований по защите от НСД, перечисленных в п. 2.3.3 и п. 2.3.4 настоящего раздела, допускается использовать программные

средства защиты информации, соответствующие требованиям к СЗИ, приведенным в таблице ниже (Таблица 1). Конкретный перечень требований по защите от НСД, обеспечиваемых использованием программного СЗИ, определяется администратором информационной безопасности, исходя из возможностей и конкретных настроек выбранного СЗИ.

Примечание — Упоминаемые в настоящем разделе программные СЗИ не обеспечивают выполнение мер по информационной безопасности, для которых эксплуатационной документацией СКЗИ «Валидата CSP» предписано использование сертифицированных ФСБ России СЗИ от НСД (аппаратно-программных и программных модулей доверенной загрузки), в частности, доверенной загрузки ЭВМ и контроля целостности ПО.

Таблица 1 – Требования к используемым программным СЗИ для СКЗИ «Валидата CSP»

Исполнение СКЗИ «Валидата CSP»	Требования к используемым СЗИ			
	Сертифицированные ФСБ России СЗИ		Сертифицированные ФСТЭК России СЗИ	
	Класс защиты	Централизованное управление	Класс защиты	Централизованное управление
Исполнение 1	Не ниже АК2	Определяется эксплуатационной документацией на СЗИ	Не ниже 4 класса по уровню доверия и не ниже 5го класса защищенности средств вычислительной техники	Должно быть санкционированно администратором информационной безопасности. Если каналы связи между компонентами СЗИ, реализующими централизованное управление, и защищаемыми ЭВМ выходят за границы контролируемой зоны, должна быть обеспечена защита каналов связи между контролируемыми зонами с использованием сертифицированных ФСБ России СКЗИ класса не ниже КС1.
Исполнение 2				Не допускается
Исполнение 3	Не ниже АК3		Использование не допускается	

2.4 Требования к антивирусной защите

При создании информационной системы, защищаемой с использованием шифровальных (криптографических) средств, необходимость применения анти-

вирусных средств в создаваемой информационной системе определяется на основании модели угроз и нарушителя для данной системы. Если такая необходимость определена, должны применяться антивирусные средства, одобренные федеральным органом исполнительной власти, ответственным за обеспечение информационной безопасности в создаваемой информационной системе.

2.5 Требования к межсетевым экранам

В случае необходимости применения межсетевого экрана (МЭ) в создаваемой информационной системе должен использоваться МЭ, имеющий подтверждение соответствия требованиям ФСБ России к устройствам типа МЭ, установленным для 4-го класса, или МЭ аналогичного класса защиты, одобренный федеральным органом исполнительной власти, ответственным за обеспечение информационной безопасности в создаваемой информационной системе.

2.6 Требования по обеспечению безопасности подключения к сетям связи

Для передачи информации, поступающей от СКЗИ «Валидата CSP» и в СКЗИ «Валидата CSP», допускается использование выходящих за пределы контролируемой зоны каналов связи, относящихся к корпоративной сети и оснащённых СЗИ от НСД (межсетевыми экранами).

В иных случаях с целью исключения возможности несанкционированного доступа к системным ресурсам используемой операционной системы, к программному обеспечению, в окружении которого функционируют СКЗИ «Валидата CSP» и ПК, функционирующие совместно с СКЗИ «Валидата CSP», и к компонентам этих ПК со стороны используемых сетей связи рекомендуется использовать дополнительные методы и средства защиты (например, использование межсетевых экранов, организация VPN-сетей и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.

2.6.1 Требования по обеспечению безопасности подключения к сетям общего пользования

Допускается подключение к СОП при выполнении следующих требований:

- эксплуатирующей организацией должен быть определён порядок подключения ЭВМ с установленным СКЗИ «Валидата CSP» к СОП;
- при подключении ЭВМ с установленным СКЗИ «Валидата CSP» к СОП должна быть обеспечена безопасность защищённой связи;
- ответственным за безопасность работы ЭВМ с установленным СКЗИ «Валидата CSP» по СОП должен быть Администратор информационной безопасности;
- должен быть разработан типовой регламент защищённой связи, включающий:
 - политику безопасности защищённой связи;
 - состав программных средств, обеспечивающих защиту информации, передаваемых по СОП;

- перечень допустимых беспроводных соединений (Wi-Fi, Bluetooth и т.п.);
- перечень допустимых сетевых протоколов и процедуру контроля за их использованием;

- перечень и порядок применения программных средств, обеспечивающих защиту СКЗИ «Валидата CSP» и ПК, функционирующих совместно с СКЗИ «Валидата CSP», от несанкционированного доступа к нему потенциального нарушителя через СОП;

- порядок обновления программных средств;
- процедуру контроля целостности ПО СКЗИ «Валидата CSP», ПК, функционирующих совместно с СКЗИ «Валидата CSP», системного ПО и всех исполняемых файлов, функционирующих совместно с СКЗИ «Валидата CSP»;
- систему и средства антивирусной защиты;

– политика безопасности должна определять организационно-технические меры (возможно, дополнительные к предусмотренным правилами пользования ЭВМ с установленным СКЗИ «Валидата CSP»), обеспечивающие безопасность работы ЭВМ с установленным СКЗИ «Валидата CSP» по СОП;

– политика безопасности должна предусматривать соблюдение правил пользования ЭВМ с установленным СКЗИ «Валидата CSP»;

– при проведении исследований по оценке влияния прикладной системы на выполнение предъявленных к СКЗИ «Валидата CSP» и к ПК, функционирующих совместно с СКЗИ «Валидата CSP», требований необходимо оценивать возможность негативного влияния на функционирование указанных ПК нарушителя, использующего возможности СОП.

2.6.2 Требования по обеспечению безопасности подключения к сетям связи для ОС, поддержка которых прекращена

Если СКЗИ «Валидата CSP» функционирует в ОС, поддержка которой прекращена производителем, допускается подключение ЭВМ с установленным СКЗИ «Валидата CSP» только к корпоративным сетям связи. При этом допускается подключение ЭВМ с установленным СКЗИ «Валидата CSP» к корпоративным сетям связи, выходящим за пределы контролируемой зоны, только при выполнении следующих условий:

– на ЭВМ должны использоваться средства антивирусной защиты, удовлетворяющие требованиям п 2.4;

– для защиты от НСД должен использоваться МЭ, удовлетворяющий требованиям п. 2.5 настоящего документа;

– сетевые соединения, выходящие за пределы контролируемой зоны, должны быть защищены с использованием средств криптографической защиты информации, сертифицированных ФСБ России по классу не ниже класса используемого СКЗИ «Валидата CSP», либо быть выделенными.

2.7 Парольная защита ЭВМ

При использовании парольных механизмов на ЭВМ с установленным СКЗИ «Валидата CSP» необходимо разработать и применить политику назначе-

ния и смены паролей (для входа в ОС, BIOS/UEFI и т.д.), руководствуясь соответствующими нормативными документами эксплуатирующей организации и изложенными ниже правилами:

- не должен использоваться один пароль для различных целей (вход в ОС, вход в BIOS/UEFI, при шифровании на пароле и т.д.);
- пароль должен быть периодически изменяющийся, из не менее чем 8 символов при мощности алфавита не менее 36;
- период действия пароля не должен превышать 6 месяцев;
- максимальное число неудачных попыток ввода пароля должно быть не более 10;
- следует использовать в качестве пароля комбинацию знаков, смысл последовательности которых трудно определить;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.), в том числе:
 - имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, адрес места жительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе,
 - один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов,
 - комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567» или «1йфячыц2» и т. п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.

2.8 Требования к порядку проведения ремонтных и регламентных работ

Вскрытие системных блоков для проведения ремонта или технического обслуживания аппаратных средств должно осуществляться в присутствии представителя подразделения информационной безопасности или Администратора информационной безопасности при наличии письменного разрешения на вскрытие от руководителя подразделения информационной безопасности.

В случае ремонта ЭВМ или жёсткого диска за пределами контролируемой зоны или работниками, не допущенными к хранящейся на ЭВМ информации, вся хранящаяся на жёстком диске информация, относящаяся к СКЗИ «Валидата CSP» и ПК, функционирующим совместно с СКЗИ «Валидата CSP», должна быть гарантировано уничтожена до передачи диска в ремонт, например, путем четырехкратной перезаписи памяти

жесткого диска случайными данными. Допускается передача в ремонт ЭВМ без удаления указанной информации с жёсткого диска при условии его изъятия из ЭВМ и хранения на время ремонта у Администратора информационной безопасности.

Мелкий ремонт ЭВМ или дискового накопителя (выполняемый в пределах контролируемой зоны) возможен без удаления информации, но только под наблюдением Администратора информационной безопасности.

Повторное использование жёстких дисков после ремонта возможно после гарантированного удаления информации либо в составе ранее использовавшихся рабочих мест с СКЗИ «Валидата CSP», либо в других системах, территориально располагающихся в пределах контролируемой зоны.

При невозможности удаления информации или ремонта жёсткого диска требуется его физическое уничтожение.

2.9 Требования к отключению функций телеметрии в ОС Windows 10, Windows Server 2016 и Windows Server 2019

Для отключения функций телеметрии в ОС Windows 10, Windows Server 2016 и Windows Server 2019 необходимо выполнить следующие действия:

а) проверить наличие и статус сервиса DiagTrack (Панель управления → Система и безопасность → Администрирование → Службы). Если данный сервис запущен, необходимо остановить его;

б) с использованием программы regedit (Пуск → Выполнить → regedit) удалить запись регистрации сервиса DiagTrack из реестра в разделе HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services. В данном разделе необходимо найти и удалить папку DiagTrack;

в) удалить подготовленные к отправке данные, которые сохраняются в файлах с расширением *.rbs, хранящихся в директории %ProgramData%\Microsoft\Diagnosis. Необходимо удалить все файлы с расширением *.rbs. При возникновении проблем с удалением данных файлов необходимо в свойствах на вкладке «Безопасность» разрешить полный доступ к файлу, а затем удалить его;

г) остановить автоматическую (AutoLogger) ETW сессию AutoLogger-DiagTrack-Listener, которую DiagTrack активирует в процессе своей остановки;

д) удалить файл, в котором автоматическая (AutoLogger) ETW сессия AutoLogger-DiagTrack-Listener сохраняла собранные данные.

Путь к данному файлу хранится в реестровой записи AutoLogger-DiagTrack-Listener в значении FileName. Конфигурации автоматических (AutoLogger) ETW сессий находятся в ключе реестра HKLM\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger. Конфигурация целевой сессии хранится в данном ключе под записью AutoLogger-DiagTrack-Listener.

Собранные данные сохраняются в файл %ProgramData%\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-DiagTrack-Listener.etl;

е) удалить запись регистрации конфигурации автоматической (AutoLogger) ETW сессии AutoLogger-DiagTrack-Listener из реестра;

ж) перечисленные выше действия необходимо выполнять после каждого кумулятивного обновления, поскольку данные обновления практически являются полной переустановкой ОС и удаленные сервисы восстанавливаются.

2.10 Применение СЗИ от НСД

В случае использования СЗИ от НСД совместно с СКЗИ «Валидата CSP», СЗИ от НСД должно обеспечивать:

- идентификацию и проверку подлинности субъектов доступа к ресурсам ЭВМ;
- контроль целостности программных средств;
- регистрацию действий пользователей;
- формирование случайного числа и выдачу его в вызывающую программу (для модификаций с аппаратным датчиком случайных чисел).

Установка и настройка СЗИ от НСД выполняется согласно руководствам по установке и настройке соответствующих СЗИ от НСД.

2.11 Установка и настройка средств создания замкнутой программной среды

Совместно с СКЗИ «Валидата CSP» (исполнение 3), в целях обеспечения защиты по классу КСЗ, должны использоваться только средства создания замкнутой программной среды из перечня, приведенного в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

Установка и настройка средств создания замкнутой программной среды выполняется согласно руководствам по установке и настройке соответствующих средств создания замкнутой программной среды.

3 КОНТРОЛЬ ЦЕЛОСТНОСТИ ПО

При использовании СКЗИ «Валидата CSP» необходимо организовать контроль целостности СКЗИ «Валидата CSP», системного ПО и всех исполняемых файлов, функционирующих совместно с СКЗИ «Валидата CSP», в соответствии с требованиями документа ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности».

В настоящем разделе приведены списки модулей СКЗИ «Валидата CSP», системного ПО и ПО средств виртуализации, подлежащих контролю целостности. Для ПК, функционирующих совместно с СКЗИ «Валидата CSP», перечень файлов, подлежащих контролю целостности, приведён в эксплуатационной документации соответствующих ПК.

3.1 Перечень модулей СКЗИ «Валидата CSP», подлежащих контролю целостности

Ниже приведён список файлов, входящих в СКЗИ «Валидата CSP» и требующих контроля целостности:

- **%windir%\system32\vdcnng.dll** — разделяемая библиотека CNG провайдера. Для криптографических операций использует разделяемую библиотеку vdcsp.dll. Регистрируется в ОС Windows как провайдер CNG;
- **%ProgramFiles%\Validata\VDCSP\vdcsp.dll** — разделяемая библиотека CSP провайдера. Содержит процедуры криптографических преобразований по ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015, Диффи-Хеллмана, генерации датчика случайных чисел (ДСЧ);
- **%windir%\system32\drivers\vdcrydrv.sys** — криптографический драйвер. Содержит процедуры криптографических преобразований по ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015, генерации ДСЧ. Используется для инициализации программных ДСЧ процессов ОС;
- **%ProgramFiles%\Validata\VDCSP\vdcspe.dll** — внешняя разделяемая библиотека CSP провайдера. Содержит все точки входа в CSP (функции CPXXX) и ссылки в разделяемую библиотеку vdcsp.dll. Подписывается Microsoft и регистрируется в ОС Windows как провайдер CSP;
- **%ProgramFiles%\Validata\VDCSP\testcsp.exe** — тестовая утилита CSP. Позволяет выполнить операции вычисления и проверки ЭП, зашифрования и расшифрования файлов из командной строки, а также другие операции;
- **%ProgramFiles%\Validata\VDCSP\gips.exe** — графический интерфейс пользователя сервисов. Предназначен для вывода на экран некоторых диалоговых окон СКЗИ «Валидата CSP» от процессов, запущенных как сервис (служба) с правами системной учётной записи в ОС Windows 10;
- **%ProgramFiles%\Validata\VDCSP\vdcsp_cfg.exe** — программа конфигурации CSP. Позволяет настроить конфигурационные параметры, подключаемые модули (считыватели и ДСЧ), выполнять операции с ключами ЭП и шифрования

(копирование, удаление, смена пароля);

- **%ProgramFiles%\Validata\VDCSP\vdtoken.exe** — утилита загрузки инициализационной последовательности ДСЧ функционального ключевого носителя (ФКН). Позволяет инициализировать ДСЧ ФКН «Валидата vdToken» и «Валидата vdToken» версия 2.0;
- **%ProgramFiles%\Validata\VDCSP\vdkeys.dll** — разделяемая библиотека управления подключаемыми модулями;
- **%ProgramFiles%\Validata\VDCSP\vdkeys02.dll** — подключаемый модуль считывателя с носителя «Съемный диск»;
- **%ProgramFiles%\Validata\VDCSP\vdkeys03.dll** — подключаемый модуль считывателя СЗИ от НСД «Соболь»;
- **%ProgramFiles%\Validata\VDCSP\vdkeys04.dll** — подключаемый модуль считывателя программно-аппаратного комплекса (ПАК) «Аккорд-АМДЗ»;
- **%ProgramFiles%\Validata\VDCSP\vdkeys06.dll** — подключаемый модуль считывателя «Реестр»;
- **%ProgramFiles%\Validata\VDCSP\vdkeys07.dll** — подключаемый модуль считывателя ruToken;
- **%ProgramFiles%\Validata\VDCSP\vdkeys11.dll** — подключаемый модуль считывателя eToken;
- **%ProgramFiles%\Validata\VDCSP\vdkeys13.dll** — подключаемый модуль считывателя JaCarta;
- **%ProgramFiles%\Validata\VDCSP\vdkeys16.dll** — подключаемый модуль считывателя ФКН «Валидата vdToken» и «Валидата vdToken» версия 2.0, предназначенный для работы с ключами, хранящимися в ФКН в неизвлекаемом режиме;
- **%ProgramFiles%\Validata\VDCSP\vdkeys17.dll** — подключаемый модуль считывателя «Валидата vdToken» и «Валидата vdToken» версия 2.0, предназначенный для работы с ключами, хранящимися в ФКН в извлекаемом режиме;
- **%ProgramFiles%\Validata\VDCSP\vdkeys21.dll** — подключаемый модуль считывателя Dallas;
- **%ProgramFiles%\Validata\VDCSP\vdkeys23.dll** — подключаемый модуль считывателя Secret Net;
- **%ProgramFiles%\Validata\VDCSP\vdkeys43.dll** — библиотека поддержки считывателя ПАКМ «КриптоПро HSM»;
- **%ProgramFiles%\Validata\VDCSP\vdkeys44.dll** — библиотека поддержки считывателя ПАК «ViPNet HSM»;
- **%ProgramFiles%\Validata\VDCSP\vdkeys45.dll** — библиотека поддержки считывателя ПАМБ «vdHSM»;
- **%ProgramFiles%\Validata\VDCSP\vdRand01.dll** — подключаемый модуль биологического ДСЧ;
- **%ProgramFiles%\Validata\VDCSP\vdRand03.dll** — подключаемый модуль ДСЧ СЗИ от НСД «Соболь»;
- **%ProgramFiles%\Validata\VDCSP\vdRand04.dll** — подключаемый модуль

ДСЧ СЗИ от НСД «Аккорд-АМД3»;

- **%ProgramFiles%\Validata\VDCSP\vdRand16.dll** — подключаемый модуль ДСЧ ФКН «Валидата vdToken» и ФКН «Валидата vdToken» версия 2.0;
- **%ProgramFiles%\Validata\VDCSP\vdTls_mon.exe** — программа монитора TLS. Позволяет включить использование Программного модуля поддержки TLS для клиентского ПО;
- **%windir%\system32\drivers\vdmondrr.sys** — драйвер монитора процессов ОС. Отвечает за загрузку разделяемых библиотек модификаций для исправления библиотек ОС;
- **%windir%\system32\vdmondll.dll** — разделяемая библиотека монитора процессов ОС. Отвечает за загрузку разделяемых библиотек модификаций для исправления библиотек ОС;
- **%windir%\system32\vdTokenpkcs11.dll** — разделяемая библиотека управления аутентификационными данными СЗИ от НСД;
- **%ProgramFiles%\Validata\VDCSP\vdcr32hk.dll** — разделяемая библиотека модификаций для CRYPT32.DLL;
- **%ProgramFiles%\Validata\VDCSP\vdcrsphk.dll** — разделяемая библиотека модификаций для CRYPTSP.DLL;
- **%ProgramFiles%\Validata\VDCSP\vdkerbhk.dll** — разделяемая библиотека модификаций для KERBEROS.DLL;
- **%ProgramFiles%\Validata\VDCSP\vdincmhk.dll** — разделяемая библиотека модификаций для INETCOMM.DLL;
- **%ProgramFiles%\Validata\VDCSP\vdmlcmhk.dll** — разделяемая библиотека модификаций для MAILCOMM.DLL;
- **%ProgramFiles%\Validata\VDCSP\vdolmmhk.dll** — разделяемая библиотека модификаций для OUTLMIME.DLL;
- **%ProgramFiles%\Validata\VDCSP\vdschnhk.dll** — разделяемая библиотека модификаций для SCHANNEL.DLL;
- **%ProgramFiles%\Validata\VDCSP\vdsg32hk.dll** — разделяемая библиотека модификаций для MSSIGN32.DLL.

При использовании СКЗИ «Валидата CSP» на 64-битной ОС Windows к указанному списку файлов должны быть добавлены 32-битные версии исполняемых модулей, находящиеся в каталогах %ProgramFiles(x86)%\Validata\VDCSP и %windir%\sysWOW64\.

При встраивании СКЗИ «Валидата CSP» в системы обработки информации прикладное ПО, осуществляющее обращение к функциям СКЗИ «Валидата CSP», должно быть включено в список контроля целостности.

3.2 Перечень модулей системного ПО, подлежащих контролю целостности

В Таблице 2 для каждой поддерживаемой ОС указано имя соответствующего файла с расширением *.hsh, находящегося на передаточном носителе и содер-

жащего перечень файлов ПО данной ОС, подлежащих контролю целостности.

Таблица 2 – Списки файлов с перечнем модулей системного ПО для поддерживаемых ОС

Операционная система	Имя файла, содержащего перечень файлов системного ПО
Windows 10 x86	Windows 10 x86.hsh
Windows 10 x64	Windows 10 x64.hsh
Windows Server 2016	Windows Server 2016.hsh
Windows Server 2019	Windows Server 2019.hsh

3.3 Перечень модулей ПО средств виртуализации, подлежащих контролю целостности

В Таблице 3 для каждого разрешенного к использованию средства виртуализации указано имя соответствующего файла с расширением *.hsh, находящегося на передаточном носителе и содержащего перечень файлов ПО указанного средства виртуализации, подлежащих контролю целостности.

Примечание — В списках контроля целостности ПО средств виртуализации приведен полный перечень модулей ПО данных средств, подлежащих контролю целостности. В зависимости от устанавливаемых компонент средств виртуализации фактический перечень модулей ПО может содержать меньшее количество файлов, чем указано в соответствующем списке контроля целостности. В этом случае необходимо скорректировать список контроля целостности, исключив из него отсутствующие файлы.

Таблица 3 – Список файлов контроля целостности ПО средств виртуализации

Средство виртуализации	Имя файла, содержащего перечень файлов ПО средства виртуализации
VMWare ESXi 6.5	VMWare-ESXi-6.5.hsh
VMWare ESXi 6.7	VMWare-ESXi-6.7.hsh
VMWare ESXi 7.0	VMWare-ESXi-7.0.hsh
Windows Server 2016 + Hyper-V	Windows Server 2016 + Hyper-V.hsh
Windows Server 2019 + Hyper-V	Windows Server 2019 + Hyper-V.hsh

4 КОНТРОЛЬ ПРАВИЛЬНОСТИ РАБОТЫ ЭВМ

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

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.

В случае, когда условия эксплуатации СКЗИ «Валидата CSP» требуют непрерывной работы ЭВМ в течение длительного времени (более 7 суток), необходимо принять во внимание, что СКЗИ «Валидата CSP» может использоваться только в качестве криптопровайдера в составе сертифицированных функционально законченных СКЗИ (далее — ФЗ СКЗИ) с высокоуровневым криптографическим интерфейсом.

Правила пользования ФЗ СКЗИ, использующих СКЗИ «Валидата CSP», должны содержать требования, при выполнении которых допускается выполнять перезагрузку ЭВМ (с целью проверки правильности работы ЭВМ) с периодом, большим 7 суток. При отсутствии таких требований или при невозможности их выполнения перезагрузку работающей ЭВМ с установленным СКЗИ «Валидата CSP» необходимо производить с периодом не более 168 часов (7 суток).

5 РЕЖИМ НЕШТАТНОЙ СИТУАЦИИ

Ниже (Таблица 4) приведён основной перечень нештатных ситуаций и рекомендуемые действия в случае их возникновения.

Администратор информационной безопасности на основании указанных рекомендаций и в соответствии с требованиями эксплуатирующей организации должен разработать инструкцию по действиям в нештатных ситуациях. Администратор информационной безопасности должен довести данную инструкцию до сведения каждого пользователя, эксплуатирующего СКЗИ «Валидата CSP».

Таблица 4 – Действия в нештатных ситуациях

Нештатная ситуация	Предпринимаемые действия
Эвакуация, угроза нападения, взрыва и т.п., стихийные бедствия, аварии общего характера	<p>1. Остановить все ЭВМ. Персонал, имеющий доступ к ключам, обязан опечатать и сдать все имеющиеся у него в наличии ключевые носители и личные идентификаторы лицу, ответственному за хранение ключевых носителей или лицу его заменяющему (см. п. 2.2.1 настоящего документа, далее — ответственный). Ответственный упаковывает все ключевые носители информации (в том числе и резервные) в опечатываемый контейнер, который выносится в безопасное помещение или здание до окончания действия нештатной ситуации и восстановления нормальной работы аппаратных и программных средств.</p> <p>2. В случае наступления события, повлекшего за собой долговременный выход из строя аппаратных средств СКЗИ «Валидата CSP», ответственный должен организовать уничтожение всех ключевых носителей, находящихся в контейнере, согласно п. 2.2.3 настоящего документа, а также установленным порядком оповещает об этом УЦ, выпустивший соответствующие сертификаты ключей проверки ЭП.</p>
Компрометация ключа ЭП	При компрометации ключа пользователя он должен немедленно прекратить связь по сети с другими пользователями. Пользователь (или администратор информационной безопасности организации) должен немедленно известить УЦ о компрометации ключей пользователя. Подробные действия в случае компрометации ключа пользователя описаны в п. 2.2.4 настоящего документа.
Отказы и сбои в работе технических средств с установленным СКЗИ «Валидата CSP»	При отказах и сбоях в работе СКЗИ «Валидата CSP» необходимо остановить работу, по возможности локализовать неисправность и в дальнейшем произвести ремонт в установленном порядке и, при необходимости, переустановку СКЗИ «Валидата CSP».

Нештатная ситуация	Предпринимаемые действия
Отказы и сбои в работе программных средств вследствие не выявленных ранее ошибок в ПО	При отказах и сбоях в работе программных средств вследствие не выявленных ранее ошибок в ПО необходимо остановить работу, локализовать по возможности причину отказов и сбоев и предпринять меры для устранения причин, вызывающих отказы и сбои. По возможности, для устранения причин, вызывающих отказы и сбои, рекомендуется привлекать разработчика данного ПО или его представителя.
Отказы в работе программных средств вследствие случайного или умышленного их повреждения	При отказах в работе программных средств вследствие случайного или умышленного их повреждения Администратор информационной безопасности обязан провести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке.
Отказы в работе программных средств вследствие ошибок пользователя	При отказах в работе программных средств вследствие ошибок пользователя он сообщает о данном факте Администратору информационной безопасности. Администратор информационной безопасности даёт соответствующие указания обслуживающему персоналу по восстановлению правильной работы программных средств в установленном порядке.
Выход из строя первого личного ключевого носителя	Необходимо сообщить по телефону в УЦ о факте выхода из строя личного ключевого носителя и обеспечить его доставку в УЦ для выяснения причин выхода из строя. Для работы используется второй личный ключевой носитель.
Выход из строя второго личного ключевого носителя (при условии, что первый тоже вышел из строя)	Пользователь, у которого вышли из строя оба личных ключевых носителя, является в УЦ для повторной регистрации (без изменения данных регистрации).
Отказы и сбои в работе СЗИ от НСД	При отказах и сбоях в работе СЗИ от НСД необходимо произвести замену вышедшего из строя оборудования на исправное.
Утеря личного идентификатора Touch-Memory и смарт-карты	Утеря указанных идентификаторов равносильна компрометации ключевых документов.

6 ВЕДЕНИЕ ЖУРНАЛОВ

При эксплуатации СКЗИ «Валидата CSP» необходимо вести следующие журналы:

а) **«Журнал учёта ключевой информации»**, в котором фиксируют факты движения ключевой информации, в том числе изготовление и уничтожение ключевой информации (включая резервные копии, при их наличии). В журнале указывают:

- учетный (порядковый) номер ключевого носителя, содержащего ключевую информацию, по данному журналу;
- идентификатор ключевого носителя;
- идентификатор ключа ЭП;
- фамилия, инициалы и подпись сотрудника, изготовившего (получившего) ключевую информацию;
- дата изготовления (получения) ключевой информации;
- вид ключевой информации, содержащейся на носителе;
- срок действия ключей (если он определён);
- сведения о передаче (возврате) носителя;
- дата и причина вывода из действия ключа.

Рекомендуемые формы журналов приведены в приложении Б.

На основании рекомендованных форм журналов и в соответствии с требованиями нормативных документов эксплуатирующая организация должна разработать и утвердить номенклатуру и формы журналов, инструкцию по ведению журналов, назначить ответственных за ведение и сохранность журналов и довести указанную информацию до каждого ответственного за ведение журналов.

7 ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ ВЫПОЛНЕНИЯ РАБОТ

После реализации рекомендаций, перечисленных в настоящем документе, и требований нормативных документов эксплуатирующей организации по обеспечению безопасности информации оформляется Акт готовности к работе.

Рекомендуемая форма Акта приведена в приложении Г.

ПРИЛОЖЕНИЕ А

(справочное)

ПРИМЕР НАСТРОЕК ОС WINDOWS ДЛЯ ЗАЩИТЫ ОТ НСД

Для обеспечения защиты от НСД в ОС Windows выполняются следующие действия:

1) регистрация в системе пользователей, обладающих правами локального администратора, на которых возлагается обязанность конфигурировать ОС Windows и ЭВМ, на которую она установлена, а также настраивать её безопасность;

2) разработка и применение политики назначения и смены паролей;

3) включение парольных фильтров, определяющих требования к сложности паролей;

4) выбор надежного пароля входа в систему для локального администратора, удовлетворяющего требованиям раздела 2.7 настоящего документа, с периодом смены пароля не более 30 дней, и доступом к паролю только для системного администратора;

5) включение блокировки компьютера заставкой (screen saver), защищённой паролем;

6) назначение локальным администратором минимально необходимых для нормальной работы прав всем пользователям, зарегистрированным в ОС Windows, в соответствии с политикой безопасности, при которой каждый пользователь, не являющийся локальным администратором, может просматривать и редактировать только свои установки в рамках прав доступа, назначенных ему локальным администратором;

7) установка на всех жёстких дисках файловой системы NTFS и установка на компьютере только одной ОС Windows (при этом не используются нестандартные, измененные или отладочные версии ОС Windows такие, например, как Debug/Checked Build);

8) ограничение доступа пользователей к системному реестру в соответствии с принятой в организации политикой безопасности;

9) исключение возможности удалённого редактирования системного реестра;

10) отключение учетной записи для гостевого входа (Guest);

11) отказ от использования режима автоматического входа пользователя в операционную систему при ее загрузке;

12) отключение сетевых протоколов, которые не используются на данной ЭВМ;

13) закрытие доступа к не используемым сетевым портам;

14) удаление всех общих ресурсов на ЭВМ (в том числе, и создаваемых по умолчанию при установке ОС Windows), которые не используются. Задание прав доступа к используемым общим ресурсам в соответствии с политикой безопасности, принятой в организации;

15) отключение режима отображения окна всех зарегистрированных на ЭВМ пользователей и быстрого переключения пользователей (ОС Windows);

- 16) исключение возможности удалённого администрирования ЭВМ (ОС Windows);
- 17) ввод ограничения количества неудачных попыток входа в систему в соответствии с политикой безопасности, принятой в организации и данным документом (не более 10);
- 18) использование системы аудита в соответствии с политикой безопасности, принятой в организации, регулярный анализ результатов аудита;
- 19) принятие одного из трех вариантов обработки заполненных журналов аудита: ***Overwrite Events As Needed, Overwrite Events Older Than X Days*** или ***Do Not Overwrite Events***, в максимальной степени обеспечивающих эффективность аудита в конкретных условиях эксплуатации;
- 20) регулярный просмотр сообщений в журнале событий Event Viewer;
- 21) установка прав доступа на все директории, содержащие системные файлы Windows, СКЗИ «Валидата CSP» и всех ПК, функционирующих совместно с СКЗИ «Валидата CSP», запрещающие запись всем пользователям, кроме Администратора (Administrator), Создателя/Владельца (Creator/Owner) и Системы (System);
- 22) отключение возможности создания аварийного дампа оперативной памяти, так как он может содержать криптографически опасную информацию;
- 23) очистка файла подкачки при перезагрузке путём внесения на ЭВМ следующих изменений в системный реестр: установка в ключе HKLM\System\CurrentControlSet\Control\SessionManager\MemoryManagment параметра ClearPageFileAtShutdown (REG_DWORD) со значением «1»;
- 24) установка обновлений фирмы Microsoft, направленных на защиту от сетевых вирусов, на всех ЭВМ с ОС Windows;
- 25) выключение Autorun для CD-ROM (для каждого пользователя в отдельности) в реестре.

(справочное)
ФОРМЫ ЖУРНАЛОВ

[illegible]

ПРИЛОЖЕНИЕ В

(справочное) РЕКОМЕНДУЕМАЯ ФОРМА АКТА УНИЧТОЖЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ

<Наименование подразделения>

АКТ

УТВЕРЖДАЮ

<должность руководителя структурного подразделения>

уничтожения ключевой информации
от ДД.ММ.20____ №

<подпись> <инициалы, фамилия>

“ ____ ” _____ 20__ г.

Мы, нижеподписавшиеся:

1) Администратор информационной безопасности <наименование подразделения> <инициалы, фамилия> ,

2) Владелец ключевых документов <должность, инициалы, фамилия> ,
составили настоящий Акт о том, что <дата> произвели уничтожение ключевой информации, содержащейся на следующих ключевых носителях СКЗИ «Валидата CSP»:

№ п.п.	Идентификатор ключевого носителя	Идентификатор ключа	Оригинал/Копия
1	<уникальный идентификатор носителя>	<уникальный идентификатор ключа>	Оригинал
...	...		
n	<уникальный идентификатор носителя>	<уникальный идентификатор ключа>	Рабочая копия 1

Уничтожение ключевой информации произведено средствами СКЗИ «Валидата CSP».

Уничтожение ключевой информации проведено в связи с < указать причину: истечение срока действия, плановая смена ключей, смена должностных обязанностей владельца ключевых документов и т.д. >.

Настоящий акт составлен в двух экземплярах, которые хранятся:

экз. № 1 в <наименование подразделения> ,

экз. № 2 в <подразделение безопасности> .

Подписи:

<подпись> <дата> / фамилия, инициалы администратора информационной безопасности /

<подпись> <дата> / должность, фамилия, инициалы владельца ключевых документов /

ПРИЛОЖЕНИЕ Г**(справочное)
АКТ ГОТОВНОСТИ К РАБОТЕ****УТВЕРЖДАЮ**_____
(должность)_____
(наименование учреждения)<подпись> <инициалы, фамилия>
М.П.**АКТ****готовности к работе** _____ **с**
(наименование учреждения)_____
(наименование изделий)

“ ____ ” _____ 20__ г.

Комиссия в составе председателя _____ и членов
(должность) (фамилия, инициалы)
комиссии, назначенная _____, составила настоящий акт о
том, что помещение пользователя, размещение _____,
(оборудование)
хранилища ключевых документов, охрана помещений и подготовленность
сотрудников к обслуживанию _____ соответствует:
(оборудование)

(ГОСТ, инструкция, руководящие документы, правила пользования и т.п.)
Комиссия отмечает, что установка и настройка ПО вы-
шеупомянутых изделий проведены в соответствии с

(название инструкции)
Вывод: объект _____ отвечает требованиям _____
(название объекта) (название инструкции)
по обеспечению безопасности связи и может быть введен в действие.

Председатель

(подпись)_____
(Инициалы, фамилия)

Члены комиссии

(подпись)_____
(Инициалы, фамилия)

(подпись)

(Инициалы, фамилия)

(подпись)

(Инициалы, фамилия)

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

НСД	Несанкционированный доступ
ОС	Операционная система (Operating System)
ПК	Программный комплекс
ПО	Программное обеспечение
СЗИ от НСД	Средство защиты информации от несанкционированного доступа
СКЗИ	Средство криптографической защиты информации
СОП	Сети общего пользования
УЦ	Удостоверяющий центр
ЭВМ	Электронно-вычислительная машина
ЭП	Электронная подпись (Digital Signature)

[illegible][illegible]