УТВЕРЖДЕН

ФДШИ.04198-01 31 01-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СДЗ

Описание применения

ФДШИ.04198-01 31 01

Листов 30

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

2023

Литера $О_1$

АННОТАЦИЯ

В данном документе приведены сведения о назначении, условиях применения, описании задачи, входных и выходных данных ФДШИ.04198-01 «Программное обеспечение СДЗ» (далее – ПО СДЗ) в составе ФДШИ.469535.098 «Аппаратно-программный комплекс «Ребус-СДЗ» (далее – СДЗ), а также руководства администратора и пользователя СДЗ.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ

1.1. Назначение и область применения

ПО СДЗ предназначено для обеспечения доверенной загрузки средства вычислительной техники за счет предотвращения несанкционированного доступа к ресурсам средства вычислительной техники на этапе его загрузки.

ПО СДЗ в составе СДЗ может применяться в качестве элемента системы защиты информации информационных систем, функционирующих на базе средств вычислительной техники, обрабатывающих государственную тайну и (или) конфиденциальную информацию, включая персональные данные.

1.2. Функциональные возможности

ПО СДЗ в составе СДЗ выполняет следующие функции:

- разграничение доступа к управлению СДЗ;
- управление работой СДЗ;
- управление параметрами СДЗ;
- аудит безопасности СДЗ;
- идентификация и аутентификация;
- тестирование СДЗ, контроль целостности программного обеспечения и параметров СДЗ;
- контроль компонентов средств вычислительной техники;
- блокирование загрузки операционной системы средством доверенной загрузки;
- сигнализация СДЗ;
- обеспечение безопасности СДЗ при возникновении сбоев и ошибок в процессе работы;
- обеспечение безопасности после завершения работы СДЗ.

Для выполнения указанных функций ПО СДЗ взаимодействует с аппаратной частью СДЗ – контроллером СДЗ1 «Тверца-5» (далее – контроллер СДЗ).

1.3. Основные характеристики

ПО СДЗ состоит из модулей ПО управления СДЗ и модулей ПО контроллера СДЗ. Модули ПО управления СДЗ находятся на дистрибутивном электронном носителе (ЭН) ФДШИ.469535.098-DE и на SD-карте контроллера СДЗ.

Основные характеристики СДЗ приведены в таблице 1.

Таблица 1 – Основные характеристики СДЗ

Характеристика	Значение
Интерфейс подключения контроллера СДЗ к материнской плате ЭВМ	PCI Express
Поддерживаемые типы слотов PCI Express	x1, x4, x8, x16
Поддерживаемые места установки контроллера СДЗ в ЭВМ	Места для установки полноразмерных плат расширения. Места для установки низкопрофильных плат расширения (low profile)
Максимальное количество регистрируемых в СДЗ пользователей	32
Файловые системы, поддерживаемые контролем целостности файлов	FAT16, FAT32, NTFS, Ext2, Ext3, Ext4
Средний срок службы контроллера СДЗ до предельного состояния	Не менее 10 лет
Допустимый режим эксплуатации	Круглосуточно

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к составу технических средств

2.1.1. Эксплуатация СДЗ (включая ПО СДЗ) возможна только при соблюдении следующих условий:

- применение ЭВМ с архитектурой x86-64;
- наличие в ЭВМ свободного слота PCI Express;
- геометрические размеры корпуса ЭВМ достаточны для установки контроллера СДЗ в соответствующий слот;
- минимальный объем оперативной памяти в ЭВМ –1 Гбайт;
- при необходимости запуска ПО управления СДЗ с CD-диска – наличие в ЭВМ устройства чтения CD/DVD-дисков;
- поддержка монитором и видеоадаптером ЭВМ рабочих разрешений не менее 1024x768 точек при глубине цвета не менее 8 бит;
- наличие у ЭВМ клавиатуры и манипулятора типа «мышь» или совместимого устройства ввода;
- соответствие среды UEFI ЭВМ спецификации Unified Extensible Firmware Interface Specification версии не меньше 2.3.1 и поддержка средой UEFI устройства EFI PCI Option ROM;
- корректная настройка контроллера СДЗ в соответствии с параметрами материнской платы и BIOS ЭВМ;
- корректная настройка параметров BIOS ЭВМ таким образом, чтобы ПО контроллера СДЗ запускалось (в частности, не должен быть отключен запуск ПО с устройств PCI Express и не должна быть активирована функция Security boot) и чтобы корректно функционировала ЭВМ;
- для выполнения двухфакторной аутентификации на контроллере СДЗ с использованием ключей iButton – наличие аппаратных идентификаторов iButton типа DS1991, DS1992, DS1993, DS1995, DS1996;
- для выполнения двухфакторной аутентификации на контроллере СДЗ с использованием USB-ключей – наличие в ЭВМ свободного разъема USB и наличие USB-ключей типа «Рутокен ЭЦП 2.0» (в том числе «Рутокен ЭЦП 2.0 Flash») или JaCarta SF/ГОСТ;
- отсутствие средств перехвата вводимой и выводимой информации в средствах ввода-вывода ЭВМ и в средствах их подключения к ЭВМ.

2.1.2. Функционирование ПО управления СДЗ возможно только при установленном контроллере СДЗ.

2.2. Организационные мероприятия обеспечения безопасности информации

На объекте эксплуатации изделия должен быть выполнен ряд мероприятий, обеспечивающих безопасность эксплуатации СДЗ:

- должен быть назначен администратор СДЗ. Администратор СДЗ должен выполнять настройку параметров СДЗ, управление учетными записями пользователей ЭВМ, просмотр и своевременную очистку журналов регистрации, снятие блокировки контроллера СДЗ, устранение последствий при нарушении безопасности СДЗ и устранение результатов сбоев в процессе работы СДЗ;
- должна быть обеспечена установка корректного времени в СДЗ и ЭВМ;
- должна обеспечиваться защита СДЗ от отключения (обхода) или блокировки;
- должна быть обеспечена физическая защита ЭВМ, доступ к которой контролируется с применением СДЗ;
- подготовка к эксплуатации и эксплуатация СДЗ должны осуществляться в соответствии с эксплуатационной документацией.

2.3. Рекомендации по составу и квалификации обслуживающего персонала

Эксплуатация изделия возможна только при условии наличия на объекте должностного лица, выполняющего роль администратора СДЗ. Данное должностное лицо может также являться администратором безопасности других средств защиты информации. Количество администраторов СДЗ определяется особенностями объекта информатизации.

Администратор СДЗ должен обладать необходимой квалификацией и изучить эксплуатационную документацию на изделие до начала работы с изделием.

2.4. Организация мер безопасности

На объекте эксплуатации должна быть разработана и применена политика назначения и смены паролей пользователей СДЗ. Данная политика должна предусматривать использование безопасных паролей в соответствии с требованиями к паролям в системе защиты информации конкретного объекта эксплуатации. Должна быть предусмотрена процедура периодической смены аутентификационных данных пользователей (паролей пользователей, секретов на аппаратных ключах), а также процедура оперативной смены аутентификационной информации в случаях дискредитации аутентификационных данных пользователей и администраторов СДЗ или потери аппаратных ключей.

2.5. Идентификация режимов работы СДЗ

На ЭВМ с установленным СДЗ может также использоваться средство защиты информации (СрЗИ) от НСД уровня ОС, совместимое с СДЗ. При этом СДЗ может работать автономно (независимо от такого средства) или совместно с ним. Для этого СДЗ поддерживает следующие режимы:

- автономный режим;
- режим совместимости.

При работе в автономном режиме перед началом загрузки рабочей ОС программный интерфейс контроллера СДЗ закрывается. Новый сеанс работы с СДЗ в автономном режиме открыть нельзя. При работе в автономном режиме нельзя выполнять управление СДЗ при помощи ПО управления СДЗ, запущенного с CD-диска. В данном режиме управление СДЗ можно выполнять только из ПО управления СДЗ, запущенного с SD-карты контроллера СДЗ.

При работе в режиме совместимости программный интерфейс контроллера СДЗ продолжает работать после загрузки ОС и позволяет СрЗИ уровня ОС осуществлять взаимодействие с СДЗ. Новый сеанс работы с СДЗ открывается только по запросу (при запуске ПО управления СДЗ и при запуске ПО управления СДЗ из состава СрЗИ уровня ОС с прохождением идентификации и аутентификации администратора СДЗ).

Переключение режимов работы СДЗ выполняется в ПО управления СДЗ.

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Общие положения

СДЗ должно обеспечивать нейтрализацию следующих основных угроз безопасности информации:

- угроза 1 – несанкционированный доступ к информации за счет загрузки нештатной операционной системы и обхода правил разграничения доступа штатной операционной системы и (или) других средств защиты информации, работающих в среде штатной операционной системы;
- угроза 2 – несанкционированная загрузка штатной операционной системы и получение несанкционированного доступа к информации;
- угроза 3 – нарушение целостности программной среды (файлов) средств вычислительной техники и (или) состава компонентов аппаратного обеспечения средств вычислительной техники в информационной системе;
- угроза 4 – нарушение целостности ПО СДЗ;
- угроза 5 – обход нарушителями компонентов СДЗ;
- угроза 6 – несанкционированное изменение конфигурации (параметров) СДЗ;
- угроза 7 – преодоление или обход функций СДЗ, идентификация (аутентификация) за счет недостаточного качества аутентификационной информации;
- угроза 8 – получение остаточной информации СДЗ из памяти СВТ после завершения работы СДЗ;
- угроза 9 – получение доступа к ресурсам СДЗ из программной среды СВТ после завершения работы СДЗ;
- угроза 10 – сбои и ошибки в процессе функционирования СДЗ.

Функции, реализуемые СДЗ, позволяют противостоять данным угрозам. Соответствие угроз безопасности и функций СДЗ приведено в таблице 2.

Таблица 2 – Соответствие угроз безопасности и функций СДЗ

Угроза	Функции СДЗ
Угроза 1	Разграничение доступа к управлению СДЗ. Управление работой СДЗ. Управление параметрами СДЗ. Блокирование загрузки операционной системы средством доверенной загрузки. Обеспечение безопасности после завершения работы СДЗ. Аудит безопасности СДЗ
Угроза 2	Разграничение доступа к управлению СДЗ. Управление работой СДЗ. Управление параметрами СДЗ. Блокирование загрузки операционной системы средством доверенной загрузки. Обеспечение безопасности после завершения работы СДЗ. Аудит безопасности СДЗ
Угроза 3	Разграничение доступа к управлению СДЗ. Контроль компонентов СВТ. Аудит безопасности СДЗ
Угроза 4	Тестирование СДЗ. Аудит безопасности СДЗ
Угроза 5	Разграничение доступа к управлению СДЗ. Блокирование загрузки операционной системы средством доверенной загрузки. Обеспечение безопасности после завершения работы СДЗ. Аудит безопасности СДЗ

Окончание таблицы 2

Угроза	Функции СДЗ
Угроза 6	Разграничение доступа к управлению СДЗ. Управление параметрами СДЗ. Аудит безопасности СДЗ
Угроза 7	Идентификация и аутентификация. Аудит безопасности СДЗ
Угроза 8	Управление параметрами СДЗ. Обеспечение безопасности после завершения работы СДЗ. Аудит безопасности СДЗ
Угроза 9	Управление параметрами СДЗ. Обеспечение безопасности после завершения работы СДЗ. Аудит безопасности СДЗ
Угроза 10	Обеспечение безопасности СДЗ при возникновении сбоев и ошибок в процессе работы. Аудит безопасности СДЗ

Таким образом, для устранения перечисленных выше угроз и, как следствие, обеспечения доверенной загрузки средства вычислительной техники СДЗ позволяет решать следующие задачи:

- разграничение доступа к управлению СДЗ;
- управление работой СДЗ;
- управление параметрами СДЗ;
- аудит безопасности СДЗ;
- идентификация и аутентификация;
- тестирование СДЗ, контроль целостности программного обеспечения и параметров СДЗ;
- контроль компонентов средств вычислительной техники;
- блокирование загрузки операционной системы средством доверенной загрузки;
- сигнализация СДЗ;
- обеспечение безопасности СДЗ при возникновении сбоев и ошибок в процессе работы;
- обеспечение безопасности после завершения работы СДЗ.

3.2. Роли безопасности

В СДЗ предусмотрены две роли пользователей – администратор СДЗ и пользователь СДЗ (пользователь). Роли учетных записей задаются в параметрах учетных записей.

Администратору СДЗ доступны все возможности пользователя СДЗ и дополнительные возможности по управлению СДЗ. Администратор СДЗ имеет возможность запуска ПО управления СДЗ, а также имеет возможность входа в систему, если ЭВМ заблокирована для пользователя.

3.3. Разграничение доступа к СДЗ

Разграничение доступа к СДЗ выполняется СДЗ автоматически на основе ролей безопасности. Администратор СДЗ при создании учетной записи пользователя должен указать для неё одну из ролей (администратор СДЗ или пользователь). В дальнейшем после успешной аутентификации пользователя СДЗ учитывает присвоенную его учётной записи роль для предоставления или блокирования доступа к различным функциям СДЗ.

3.4. Управление работой СДЗ

Управление работой СДЗ осуществляется администратором СДЗ путём управления режимами выполнения функций безопасности СДЗ. Для этого администратор СДЗ в ПО управления СДЗ должен задать параметры запуска СДЗ и параметры работы функций СДЗ. Параметры запуска

СДЗ отвечают за выбор момента запуска СДЗ в процессе запуска ЭВМ. Параметры работы функций СДЗ отвечают за запуск и работу функций СДЗ.

3.5. Управление параметрами СДЗ

К параметрам СДЗ можно отнести все данные, используемые функциями безопасности СДЗ.

Управление параметрами СДЗ осуществляется администратором СДЗ из ПО управления СДЗ. При этом администратору СДЗ доступны для управления следующие параметры СДЗ:

- учетные записи администраторов и пользователей СДЗ (включая аутентификационные данные пользователей, параметры аппаратных ключей пользователей, ограничения на допустимое время работы);
- эталонные данные контроля целостности файлов;
- эталонные данные дерева устройств контроля состава компонентов аппаратного обеспечения.

3.6. Аудит безопасности СДЗ

В ходе работы СДЗ осуществляет регистрацию событий аудита. Регистрируются события с данными о состоянии СДЗ (в том числе события начала работы СДЗ, события самотестирования, события с информацией об ошибках в работе СДЗ и т.п.), события с информацией об успешных и неуспешных событиях входа пользователя в систему, события контроля компонентов средства вычислительной техники. Хранение регистрируемых событий аудита СДЗ осуществляет в отдельных журналах событий:

- журнал контроллера СДЗ;
- журнал контроля целостности файлов;
- журнал контроля состава компонентов аппаратного обеспечения.

Журнал контроллера СДЗ размещается в специальной области энергонезависимой памяти контроллера СДЗ. Журналы контроля целостности файлов и контроля состава компонентов аппаратного обеспечения хранятся на SD-карте контроллера СДЗ. Размер журнала контроллера СДЗ ограничен и позволяет хранить не более 767 записей. Журналы контроля целостности файлов и контроля состава компонентов аппаратного обеспечения ограничены размером поставляемой в комплекте SD-карты.

Администратор СДЗ должен периодически просматривать и анализировать все журналы событий, не допускать переполнения журнала событий. При переполнении журнала осуществляется циклическая перезапись событий, старые записи перезаписываются на новые.

Для обеспечения безопасности при переполнении журналов событий администратор СДЗ может настроить соответствующую блокировку ЭВМ для пользователя.

Работа с журналом событий осуществляется администратором СДЗ из ПО управления СДЗ.

Средства работы с журналами событий обеспечивают их просмотр с возможностью фильтрации данных аудита. Журналы событий могут быть экспортированы для последующей обработки внешними средствами анализа и для обеспечения длительного хранения. При отображении журнала событий происходит упорядочивание событий по порядку регистрации, а не по времени регистрации. Если в процессе работы СДЗ будут изменены дата или время на ЭВМ, то на последовательность вывода событий это не повлияет.

3.7. Идентификация и аутентификация

Идентификация (распознавание) и аутентификация (проверка подлинности) пользователя являются необходимым условием для определения его роли и полномочий и осуществляются при включении или перезагрузке ЭВМ.

Для идентификации пользователя в СДЗ используется алфавитно-цифровой идентификатор, а также (при необходимости) аппаратный ключ.

Для однофакторной аутентификации в СДЗ используются алфавитно-цифровые пароли. СДЗ также предоставляет возможность двухфакторной аутентификации пользователей с использованием аппаратных ключей. Первым фактором в этом случае служит знание пользователем пароля, вторым – наличие у пользователя аппаратного ключа с соответствующими ключевыми данными (секретом).

Если применяются аппаратные ключи iButton, то секрет на ключе хранится в открытом виде; если же используется USB-ключ, то секрет на ключе хранится в памяти ключа, защищенной ПИН-кодом. ПИН-код не выдается пользователю, он хранится в контроллере СДЗ и применяется для получения доступа к USB-ключу без участия пользователя.

В случае предъявления персонального аппаратного ключа, не зарегистрированного в СДЗ:

- вход пользователя в систему запрещается;
- в журнале регистрации событий фиксируется попытка НСД.

В случае ввода пароля, не соответствующего предъявленному идентификатору:

- вход пользователя в систему запрещается;
- счетчик неудачных попыток входа пользователя в систему увеличивается на единицу;
- в журнале регистрации событий фиксируется попытка НСД.

При превышении числа неуспешных попыток идентификации и аутентификации СДЗ блокирует ЭВМ для пользователя.

Подготовка идентификационных и аутентификационных данных пользователей осуществляется администратором СДЗ при создании или изменении учётных записей пользователей. После подготовки или изменения администратор СДЗ сообщает эти данные (и предоставляет аппаратные ключи, при их использовании) соответствующим пользователям.

3.8. Тестирование СДЗ, контроль целостности программного обеспечения и параметров СДЗ

СДЗ проводит самотестирование при своём запуске. Если в процессе самотестирования обнаружены нарушения в работе механизмов СДЗ либо обнаружено нарушение целостности СДЗ, ЭВМ блокируется для пользователя.

Часть тестов выполняется при каждом запуске СДЗ, а часть – по запросу администратора СДЗ. Инициализация тестов, выполняемых по запросу, выполняется администратором СДЗ из ПО управления СДЗ. Эти тесты выполняются однократно при следующем запуске СДЗ. Тесты по запросу необходимо выполнять последовательно, по одному.

На части ЭВМ провести самотестирование контроля состава аппаратных средств невозможно. Это происходит из-за того, что в процессе проведения теста в системе должна проводиться переинициализация USB-устройств, которая не происходит в связи с особенностями работы СДЗ на данной конкретной ЭВМ.

При возникновении проблем с проведением самотестирования контроля состава аппаратных средств, администратор СДЗ должен самостоятельно выполнить проверку работы механизма.

Для проведения тестирования контроля состава аппаратных средств необходимо выполнить следующие действия:

- включить контроль состава аппаратных средств в ПО управления СДЗ;
- перезагрузить ЭВМ для формирования эталонного дерева устройств и сохранить полученное эталонное дерево устройств с использованием ПО управления СДЗ;
- подключить к ЭВМ USB-устройство, перезагрузить ЭВМ;
- выполнить авторизацию, убедиться, что в процессе выполнения контроля состава аппаратных средств обнаружено появление USB-устройства («Обнаружен новый узел дерева аппаратных элементов»).

Тестирование контроля состава аппаратных средств считается выполненным успешно, если в процессе выполнения проверки обнаружено появление USB-устройства.

СДЗ осуществляет контроль целостности ПО СДЗ путём расчёта контрольных сумм модулей СДЗ и проверки их соответствия эталону. Администратор СДЗ может в ПО управления СДЗ просмотреть контрольные суммы модулей СДЗ и верифицировать их, сравнив полученный результат с эталонным значением в ЭД СДЗ.

СДЗ осуществляет контроль целостности данных СДЗ путём расчёта их контрольной суммы. Администратор для контроля целостности данных СДЗ может просмотреть их контрольную сумму, зафиксировать её и периодически проверять её.

3.9. Контроль компонентов средств вычислительной техники

СДЗ обеспечивает контроль компонентов до загрузки ОС с помощью следующих механизмов:

- контроль целостности файлов на ЭВМ;
- контроль состава компонентов аппаратного обеспечения ЭВМ.

СДЗ может контролировать целостность любых файлов на ЭВМ. Рекомендуется применять данный механизм для следующих категорий файлов (определяющих программную среду ЭВМ):

- исполняемые фалы ОС ЭВМ;
- ключевые файлы данных ОС ЭВМ;
- исполняемые файлы средств защиты уровня ОС;
- файлы с данными средств защиты уровня ОС;
- исполняемые файлы функционального ПО ЭВМ.

Для выполнения контроля целостности файлов администратор СДЗ должен при помощи ПО управления СДЗ сформировать список контролируемых файлов и зафиксировать их контрольные суммы. Непосредственно контроль целостности файлов выполняется после идентификации и аутентификации пользователя до загрузки ОС. В случае выявления нарушения целостности контролируемых файлов СДЗ блокирует ЭВМ для пользователя.

Пользователь при входе в систему в случае обнаружения нарушения в контролируемых файлах должен обратиться к администратору СДЗ. Администратор СДЗ в свою очередь должен расследовать причину изменения целостности контролируемых файлов и, при наличии необходимости и возможности, восстановить файлы. Если же изменения файлов допустимы или непреодолимы, необходимо выполнить перерасчет контрольных сумм для фиксации нового корректного состояния программной среды.

Для выполнения контроля состава компонентов аппаратного обеспечения ЭВМ администратор СДЗ должен при помощи ПО управления СДЗ сохранить эталонное дерево устройств и включить механизм контроля. Непосредственно проверка контроля состава компонентов аппаратного обеспечения выполняется после идентификации и аутентификации пользователя до загрузки ОС. В случае выявления нарушения в составе компонентов СДЗ блокирует ЭВМ для пользователя.

Если на ЭВМ штатно предполагается регулярное подключение и отключение отдельных устройств, то для предотвращения ложных срабатываний администратор СДЗ может настроить игнорирование данных устройств. В качестве примера таких устройств могут выступать USB-принтеры (которые не будут определяться в качестве устройств, если они выключены), внешние (штатные) USB-накопители (которые могут быть отключены в момент контроля целостности).

Пользователю необходимо использовать совместно с ЭВМ только штатные устройства, разрешенные к применению. Если пользователь выявил при помощи СДЗ нарушения в составе компонентов аппаратного обеспечения, он должен обратиться к администратору СДЗ.

3.10. Блокирование загрузки операционной системы средством доверенной загрузки

СДЗ обеспечивает блокирование загрузки нештатной ОС и несанкционированной загрузки штатной ОС.

Блокирование загрузки ОС выполняется в следующих случаях:

- при выявлении попыток загрузки нештатной ОС;
- при превышении числа неудачных попыток аутентификации пользователя;
- при нарушении целостности СДЗ;
- при нарушении целостности загружаемой программной среды;
- при нарушении состава аппаратных компонентов;

- при попытках обхода СДЗ;
- при критических типах сбоев и ошибок.

Для обеспечения корректной работы блокировки администратор СДЗ в ПО управления СДЗ должен задать параметры блокировок, настроить параметры сторожевого таймера.

СДЗ блокирует запуск нештатной ОС при выявлении попытки ее загрузки. Блокировка выполняется по-разному в зависимости от момента обнаружения попытки загрузки и от поведения UEFI BIOS материнской платы ЭВМ при блокировке загрузки. В результате блокировки запуска нештатной ОС может быть одна из следующих реакций:

- принудительная загрузка штатной ОС ЭВМ;
- остановка загрузки ОС, при этом на экране может быть отображено сообщение о том, что выявлена попытка загрузки нештатной ОС;
- остановка загрузки ОС, при этом на экране не будет никаких сообщений (данная реакция происходит, если в момент блокировки у СДЗ нет возможности вывести сообщение на экран);
- принудительная перезагрузка ЭВМ.

СДЗ блокирует загрузку любой ОС, если ЭВМ была заблокирована для пользователя (такая блокировка распространяется только на пользователей СДЗ, не являющихся администраторами СДЗ). ЭВМ блокируется для пользователя в следующих случаях:

- если администратор СДЗ настроил блокировку ЭВМ для пользователя при выявлении попытки загрузки нештатной ОС;
- при превышении числа неудачных попыток идентификации и аутентификации пользователя. Допустимое число попыток идентификации и аутентификации устанавливается администратором СДЗ;
- при нарушении целостности СДЗ. Проверка целостности СДЗ проводится в момент самотестирования при инициализации. Администратор СДЗ может отключить блокировку ЭВМ для пользователя, если выявлено нарушение целостности модулей СДЗ на SD-карте;
- при выявлении нарушений целостности программной среды ЭВМ и при выявлении изменений в составе аппаратных средств ЭВМ.

Снять блокировку ЭВМ для пользователя может администратор СДЗ в ПО управления СДЗ.

В качестве средства блокирования загрузки ОС при попытках обхода СДЗ в нём предусмотрены следующие возможности:

- перезагрузка ЭВМ при помощи механизма аварийного сброса по сторожевому таймеру;
- обеспечение запуска СДЗ на ранних стадиях инициализации ЭВМ до запуска средств управления BIOS ЭВМ.

Если злоумышленнику каким-либо образом удастся нарушить взаимодействие ЭВМ и СДЗ и СДЗ не будет корректно запускаться при старте ЭВМ, то при помощи механизма аппаратного сброса по сторожевому таймеру ЭВМ будет перезагружена и злоумышленник не получит доступ к ЭВМ.

После выполнения идентификации и аутентификации СДЗ блокирует клавиатуру и мышь ЭВМ, чтобы злоумышленник не смог повлиять на загрузку ОС (путём настройки параметров BIOS ЭВМ или использования меню BIOS выбора устройства для загрузки).

3.11. Сигнализация СДЗ

СДЗ осуществляет информирование администраторов СДЗ и пользователей о состоянии СДЗ, об ошибках, выявленных при работе СДЗ, и о событиях безопасности с помощью механизма сигнализации.

Пользователю сигнализируется (отображается) следующая краткая информация:

- о блокировке ЭВМ;
- о результатах самотестирования СДЗ;
- о результатах контроля целостности модулей и данных СДЗ;
- о событиях нарушения целостности данных и оборудования ЭВМ.

При попытке ввода неверных идентификационных и аутентификационных данных, а также при попытках входа в систему в недопустимое время пользователю отображается сообщение о

неверном вводе.

Администратору СДЗ дополнительно доступна возможность просмотра расширенной информации сигнализации. Из неё администратор СДЗ может получить информацию о результатах выполнения отдельных тестов СДЗ.

Пользователь и администратор СДЗ должны следить за сигнализацией СДЗ и действовать в соответствии с выдаваемыми указаниями (при их наличии).

3.12. Обеспечение безопасности СДЗ при возникновении сбоев и ошибок в процессе работы

ПО СДЗ обрабатывает ошибки, возникающие в процессе работы. При возникновении разовых некритичных сбоев и ошибок пользователь может попытаться перезагрузить ЭВМ. Если ошибка не пропадает, пользователь должен обратиться к администратору СДЗ.

При обнаружении критичных сбоев и ошибок функционирования СДЗ блокирует доступ пользователя к СДЗ и/или блокирует ЭВМ для пользователя. Пользователь должен в этом случае обратиться к администратору СДЗ. Администратор СДЗ должен выяснить причину сбоя или блокировки ЭВМ для пользователя, устранить причину сбоя, при необходимости произвести восстановление работоспособности СДЗ (восстановить учетные данные пользователей, параметры запуска СДЗ и т.п.). Также при сбое рекомендуется сохранить на внешнем носителе журналы событий и очистить журналы.

Описание возможных сбойных ситуаций при подготовке к использованию и при использовании СДЗ, а также действий, которые необходимо предпринять в случае возникновения таких ситуаций, приведено в разделе 2 документа ФДШИ.469535.098РЭ «Аппаратно-программный комплекс «Ребус-СДЗ». Руководство по эксплуатации».

3.13. Обеспечение безопасности после завершения работы СДЗ

ПО СДЗ обеспечивает безопасность данных СДЗ после завершения работы СДЗ. В ходе и по завершении работы СДЗ автоматически выполняется очистка областей памяти, использовавшихся в процессе работы.

При работе СДЗ в автономном режиме после завершения работы СДЗ (при старте загрузки ОС) выполняется блокировка интерфейса взаимодействия с СДЗ и ресурсы СДЗ становятся недоступны.

При работе СДЗ в режиме совместимости у СДЗ открывается интерфейс взаимодействия, который позволяет средствам защиты информации (СрЗИ) уровня ОС получать доступ к данным СДЗ. Данный режим необходимо включать только для совместного использования СДЗ с СрЗИ уровня ОС, совместимого с СДЗ. При этом администратор должен (с помощью технических и/или организационных мер, в том числе с помощью используемого СрЗИ уровня ОС) следить за составом ПО на ЭВМ и не допускать появления в нём средств, способных получить несанкционированный доступ к управлению СДЗ.

4. РУКОВОДСТВО АДМИНИСТРАТОРА СДЗ

4.1. Функции, доступные администратору СДЗ

Администратор СДЗ должен выполнять все функции по развертыванию, настройке СДЗ и контролю за работой СДЗ и пользователей. Администратор СДЗ должен:

- выполнять установку СДЗ;
- управлять параметрами запуска СДЗ;
- управлять параметрами работы функций безопасности СДЗ;
- управлять учетными записями пользователей СДЗ;
- задавать и периодически менять аутентификационные данные пользователей;
- контролировать корректность работы СДЗ;
- проводить мероприятия по устранению причин и последствий НСД;
- выполнять восстановление работы СДЗ в случаях сбоев и отказов при работе СДЗ;
- контролировать работу пользователей, проводить расследования при выявлении попыток несанкционированного доступа;
- проводить периодический анализ журналов событий с целью выявления нарушений в работе СДЗ и выявления попыток несанкционированного доступа;
- восстанавливать работу СДЗ в случае сбоев и ошибок.

Администратору СДЗ доступны все функции безопасности СДЗ.

4.2. Интерфейсы, доступные администратору СДЗ

Администратору СДЗ доступны следующие интерфейсы СДЗ:

- интерфейс идентификации и аутентификации;
- интерфейс расширенной сигнализации СДЗ;
- интерфейсы приложений ПО управления СДЗ;
- интерфейс аудита СДЗ;
- интерфейс контроля целостности файлов;
- интерфейс контроля состава компонентов аппаратного обеспечения.

Описание интерфейсов СДЗ приводится в документе ФДШИ.04198-01 34 01 «Руководство оператора».

Интерфейс идентификации и аутентификации отображается при запуске СДЗ, а также в ПО управления СДЗ при запуске приложений ПО управления СДЗ. Повторные идентификация и аутентификация необходимы, так как после начала загрузки ПО управления СДЗ сессия работы контроллера завершается.

На экране идентификации и аутентификации всем пользователям СДЗ отображается информация сигнализации. СДЗ сигнализирует о состоянии СДЗ, в том числе о результатах самотестирования и состоянии блокировки ЭВМ. Администратор СДЗ может по запросу получить расширенную информацию сигнализации.

Администратор СДЗ может запустить ПО управления СДЗ. В ПО управления СДЗ администратору доступны интерфейсы следующих приложений:

- управление СДЗ;
- контроль целостности файлов;
- контроль состава компонентов аппаратного обеспечения;
- восстановление заводских настроек;
- расчет контрольных сумм СДЗ.

В процессе работы СДЗ регистрирует события. Администратор СДЗ может просматривать события в приложениях ПО управления СДЗ.

Управление контролем целостности файлов осуществляется в ПО управления СДЗ в средстве контроля целостности файлов. Сам контроль целостности проходит при запуске ЭВМ после идентификации и аутентификации пользователя. В процессе контроля целостности в случае обнаружения нарушения целостности файлов происходит отображение информации о том, целостность какого файла нарушена.

Управление контролем состава компонентов аппаратного обеспечения осуществляется в ПО

управления СДЗ в средстве контроля состава компонентов аппаратного обеспечения. Сам контроль состава компонентов аппаратного обеспечения проходит при запуске ЭВМ после идентификации и аутентификации пользователя. В процессе контроля состава компонентов аппаратного обеспечения в случае обнаружения нарушения состава компонентов аппаратного обеспечения происходит отображение информации о том, какое устройство появилось или пропало.

4.3. Приемка изделия

Перед установкой СДЗ необходимо убедиться в целостности СДЗ. Проверка целостности поставляемого изделия описана в разделе 4 документа ФДШИ.469535.098ФО «Аппаратно-программный комплекс «Ребус-СДЗ». Формуляр».

4.4. Установка и настройка СДЗ

Установка СДЗ выполняется администратором СДЗ на рабочие ЭВМ пользователей. До выполнения установки СДЗ администратор должен выполнить подсчет контрольных сумм модулей СДЗ на дистрибутивном электронном носителе и сверить полученные контрольные суммы с эталонными значениями. В процессе установки администратор должен установить в СДЗ все необходимые настройки контроллера СДЗ для корректного функционирования СДЗ на ЭВМ. Подробное описание установки изделия приведено в разделе 3 ФДШИ.04198-01 34 01 «Руководство оператора».

4.5. Режимы работы СДЗ

СДЗ может работать в одном из следующих режимов:
- автономный режим;
- режим совместимости.

Если включен автономный режим, то перед началом загрузки ОС программный интерфейс контроллера СДЗ будет закрыт, а вместе с ним будет заблокированы механизмы работы с внешними средствами защиты информации уровня ОС. В автономном режиме безопасность СДЗ будет выше, так как вредоносное ПО не сможет получить доступ к СДЗ при помощи программного интерфейса контроллера СДЗ.

Необходимо учитывать, что в автономном режиме ПО управления СДЗ, запущенное с CD-диска, не сможет получить доступ к программному интерфейсу контроллера СДЗ, и в этом случае для управления СДЗ можно использовать только ПО управления, запускаемое с SD-карты контроллера СДЗ.

Если включен режим совместимости, то перед началом загрузки ОС сессия работы с программным интерфейсом контроллера СДЗ закрывается, но программный интерфейс контроллера СДЗ остается открытым. В режиме совместимости средства защиты уровня ОС могут взаимодействовать с контроллером СДЗ. Для обеспечения безопасного взаимодействия средств защиты уровня ОС и контроллера СДЗ, доступ к программному интерфейсу контроллера СДЗ осуществляется только после успешной идентификации и аутентификации администратора СДЗ.

Если на ЭВМ используются средства защиты уровня ОС, которые поддерживают работу с контроллером СДЗ, необходимо включать режим совместимости.

4.6. Управление СДЗ безопасным способом

Администратор должен выполнять периодическое архивирование журнала событий СДЗ и их сохранение на резервном носителе информации, так как журнал ограниченного размера и в случае его переполнения старые записи будут перезаписаны новыми. При возникновении сбоев в работе СДЗ администратор должен выполнить восстановление настроек контроллера и модулей.

Администратор СДЗ должен скопировать дистрибутивный ЭН СДЗ с программным обеспечением и хранить поставляемый диск как эталон, а для эксплуатации использовать копию.

4.7. Контролируемые функции и привилегии

В процессе эксплуатации СДЗ администратор СДЗ должен контролировать работу СДЗ и пользователей СДЗ, в том числе:

- контролировать состав пользователей ЭВМ и не допускать наличия лишних учетных записей пользователей;
- контролировать состав администраторов СДЗ и не допускать наличия роли администратора СДЗ у учетных записей пользователей, которым она не требуется для исполнения их служебных обязанностей;
- периодически менять аутентификационные данные пользователей;
- контролировать журналы событий и периодически их очищать. Переполнение журнала аудита может привести к блокировке работы пользователя на ЭВМ (если настроена блокировка при переполнении журналов событий) либо может привести к потере событий;
- контролировать работу функции самотестирования; при помощи самотестирования могут быть выявлены проблемы в работе СДЗ, что позволит предотвратить нарушение безопасности;
- контролировать работу пользователей на ЭВМ, выяснять причины нарушения безопасности, при необходимости снимать блокировку ЭВМ для пользователя;
- не допускать применения пользователями на рабочих местах нештатных устройств в составе ЭВМ. Применение нештатных устройств приведет к срабатыванию механизма контроля аппаратных средств;
- контролировать состав ПО в рабочей ОС. Особенно важно не допускать появления ПО, позволяющего отлаживать работу устройств, в том числе контроллера СДЗ;
- контролировать, чтобы СДЗ было настроено на работу в автономном режиме, если СДЗ при работе не должно взаимодействовать со средствами защиты информации уровня ОС.

4.8. Управление пользователями

После установки СДЗ администратор может добавить пользователей и других администраторов при необходимости.

Настройка пользователей осуществляется в ПО управления СДЗ в приложении управления СДЗ во вкладке «Пользователи». Описание вкладки «Пользователи» и действий администратора по настройке пользователей приводится в разделе 3 документа ФДШИ.04198-01 34 01 «Руководство оператора».

Идентификатор пользователя не может быть пустым и может содержать не более 49 символов. Возможные параметры пароля задаются с помощью метрики качества и описаны в ФДШИ.04198-01 34 01 «Руководство оператора». Требования к ПИН-коду аппаратного идентификатора определяются в документации на данный аппаратный идентификатор.

4.9. Управление параметрами безопасности

Администратор должен:

- создавать учетные записи пользователей и настраивать для учётных записей аутентификационные данные;
- формировать эталоны для контроля состава компонентов аппаратного обеспечения ЭВМ и контроля целостности файлов;
- задавать параметры запуска СДЗ.

При изменении параметров контроля состава компонентов аппаратного обеспечения текущее дерево устройств сохраняется как эталон. При следующем перезапуске ЭВМ изменения вступят в силу. У администратора есть возможность настроить игнорирование контроля для тех устройств, которые штатно могут быть как подключенными, так и отключенными (например, флеш-накопители).

При первичном создании списка контролируемых файлов, при его изменении либо при

санкционированном изменении контролируемых файлов необходимо пересчитать контрольные суммы файлов. При следующем перезапуске ЭВМ изменения вступят в силу.

Управление параметрами СДЗ осуществляется в ПО управления СДЗ при помощи приложения управления СДЗ. Параметрами, влияющими на безопасность, являются:

- время задержки сторожевого таймера;
- число попыток аутентификации;
- необходимость блокировки клавиатуры и мыши при загрузке ОС;
- необходимость звуковой сигнализации;
- параметр включения/отключения контроля целостности файлов;
- параметр включения/отключения контроля состава компонентов аппаратного обеспечения;
- параметры метрики качества аутентификационных данных;
- параметры порогов блокировки и сигнализации.

Каждый параметр описан подробнее в разделе 3 документа ФДШИ.04198-01 34 01 «Руководство оператора».

4.10. События безопасности

Просмотр событий безопасности доступен только администратору СДЗ. Описание каждого типа событий, относящихся к безопасности, а также событий, связанных с выполнением обязательных функций администрирования, приведено в таблице 3.

Таблица 3 – События, регистрируемые СДЗ

Источник события	Тип события	Дополнительная информация	Результат
Контроллер СДЗ	Блокировка входа пользователя при блокировке ЭВМ для пользователя	<введенный идентификатор, введенный пароль>	Неуспех
Контроллер СДЗ	Пользователю отображена информация о сигналах нарушения безопасности	–	Успех
Контроллер СДЗ	Администратору отображена детализированная информация о сигналах нарушения безопасности	–	Успех
Контроль целостности файлов	Пользователю отображена информация о возможном нарушении безопасности, выявленном при контроле целостности файлов	–	Успех
Контроль состава компонентов аппаратного обеспечения	Пользователю отображена информация о возможном нарушении безопасности, выявленном при контроле состава компонентов аппаратного обеспечения	–	Успех
Контроллер СДЗ. Контроль целостности файлов. Контроль состава компонентов аппаратного обеспечения	Администратору отображена информация о проблеме, возникшей при выполнении самотестирования	<строка с описанием теста>	Успех

Продолжение таблицы 3

Источник события	Тип события	Дополнительная информация	Результат
Контроллер СДЗ	Работа СДЗ начата	<текущая контрольная сумма данных СДЗ, референсная контрольная сумма данных СДЗ, список завершившихся неудачей автоматически запускаемых тестов самотестирования>	Успех – в случае целостности данных и отсутствии завершившихся неудачей тестов самотестирования. Неуспех – в противном случае
Контроллер СДЗ	Работа СДЗ завершена	<информация о точке завершения работы модулей UEFI СДЗ>	Неуспех – в случае блокировки работы СВТ. Успех – в противном случае
Контроллер СДЗ	Сеанс управления СДЗ начат	–	Успех
Контроллер СДЗ	Сеанс управления СДЗ завершен	–	Успех
Контроллер СДЗ. Контроль целостности файлов. Контроль состава компонентов аппаратного обеспечения	Выполнено чтение журнала регистрации событий	–	Успех
Контроллер СДЗ	Целостность записи журнала событий аудита нарушена	<событие в бинарном виде без поля дополнительной информации>	Неуспех
Контроллер СДЗ. Контроль целостности файлов. Контроль состава компонентов аппаратного обеспечения	Журнал событий аудита был очищен	–	Успех
Контроллер СДЗ. Контроль целостности файлов. Контроль состава компонентов аппаратного обеспечения	Целостность журнала событий аудита нарушена	–	Неуспех
Контроллер СДЗ. Контроль целостности файлов. Контроль состава компонентов аппаратного обеспечения	Выполнена сигнализация в связи с переполнением журнала событий аудита	–	Успех
Контроллер СДЗ. Контроль целостности файлов. Контроль состава компонентов аппаратного обеспечения	Выполнена блокировка ЭВМ для пользователя в связи с переполнением журнала событий аудита	–	Неуспех
Контроль целостности файлов	Процедура контроля целостности файлов начата	–	Успех
Контроль целостности файлов	Процедура контроля целостности файлов завершена	–	Успех
Контроль целостности файлов	Раздел с контролируемой файловой системой не найден	Не удалось найти файловую систему с UUID {<UUID файловой системы>}	Неуспех

Продолжение таблицы 3

Источник события	Тип события	Дополнительная информация	Результат
Контроль целостности файлов	Контролируемый объект не найден	Не удалось открыть контролируемый файл '<путь к файлу>' на разделе с UUID {<UUID файловой системы>}	Неуспех
Контроль целостности файлов	Контрольная сумма контролируемого объекта не совпадает с эталонной	Контролируемый файл '<путь к файлу>' на разделе с UUID {<UUID файловой системы>} изменен (ПОСЧИТАНО: <посчитанная контрольная сумма>, ОЖИДАЛОСЬ: <ожидаемая контрольная сумма>)	Неуспех
Контроль целостности файлов	Выполнена очистка данных механизма контроля целостности файлов	УДАЛЕНЫ: <список удаленных файлов> ОШИБКА УДАЛЕНИЯ: <список файлов, которые удалить не удалось>	Неуспех
Контроль целостности файлов	При проведении контроля целостности файлов произошел некритичный сбой	<строка с описанием сбоя>	Неуспех
Контроль целостности файлов	Набор контролируемых объектов файловой системы изменен	Выполнено изменение списка контролируемых объектов для раздела с UUID {<UUID файловой системы>}	Успех
Контроллер СДЗ	Выполнена блокировка ЭВМ для пользователя в связи с превышением максимально допустимого количества попыток аутентификации	<количество попыток аутентификации>	Неуспех
Контроллер СДЗ	Выполнено снятие блокировки ЭВМ для пользователя	–	Успех
Контроллер СДЗ	Изменена метрика качества аутентификационных данных	<тип метрики, старое значение, новое значение>	Успех
ПО управления СДЗ	Попытка сохранения аутентификационных данных, не удовлетворяющих метрике качества	<модификация действия (сохранено, заблокировано), идентификатор изменяемого пользователя, тип значения (пароль ПИН, секрет), значение>	Успех, если администратор принудительно сохранил данные. Неуспех – в противном случае
Контроллер СДЗ	Успешная регистрация пользователя	<идентификатор пользователя>	Успех
Контроллер СДЗ	Пользователь ввел неверный пароль	<идентификатор пользователя, введенный пароль>	Неуспех
Контроллер СДЗ	Введенный пароль имеет истекший срок действия	<идентификатор пользователя, введенный пароль, срок действия введенного пароля>	Неуспех
Контроллер СДЗ	Попытка регистрации в неразрешенный день недели	<идентификатор пользователя, введенный пароль, маска разрешенных пользователю дней недели>	Неуспех
Контроллер СДЗ	Попытка регистрации в неразрешенное время суток	<идентификатор пользователя, введенный пароль, разрешенный для работы временной интервал>	Неуспех

Продолжение таблицы 3

Источник события	Тип события	Дополнительная информация	Результат
Контроллер СДЗ	Применение некорректного аппаратного ключа	Тип аппаратного ключа: <iButton, Rutoken, JaCarta, Esmart>, (дополнительно при вводе неверного идентификатора) некорректный идентификатор пользователя: <идентификатор> (дополнительно при неверном ПИН-коде и секрете) пользователь: <идентификатор> некорректный <ПИН-код> <секрет>	Неуспех
Контроллер СДЗ	Успешная регистрация пользователя	–	Успех
Контроллер СДЗ	Пользователь ввел неверный идентификатор	<введенный идентификатор>	Неуспех
Контроллер СДЗ	Изменено значение таймаута сторожевого таймера	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменено значение максимально допустимого количества попыток аутентификации	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменено значение флага принудительного использования ключей iButton	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменено значение флага принудительного использования USB-ключей	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменено значение флага поддержки ключей iButton	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменено значение флага поддержки USB-ключей	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменено значение флага запуска процедуры контроля целостности файлов	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменено значение флага запуска контроля состава компонентов аппаратного обеспечения	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменён режим функционирования СДЗ	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменено значение флага блокировки ЭВМ для пользователя при обнаружении нарушения целостности UEFI-модулей sd-карты	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменён порог сигнализации для журнала аудита контроллера СДЗ	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменён порог блокировки для журнала аудита контроллера СДЗ	<старое значение, новое значение>	Успех
Контроль целостности файлов	Изменён параметр контроля целостности файлов	<тип настройки, старое значение, новое значение>	Успех

Продолжение таблицы 3

Источник события	Тип события	Дополнительная информация	Результат
Контроль состава компонентов аппаратного обеспечения	Изменён параметр контроля состава компонентов аппаратного обеспечения	<тип настройки, старое значение, новое значение>	Успех
Контроллер СДЗ	Изменён способ запуска ПО управления СДЗ	<старое значение, новое значение>	Успех
Контроллер СДЗ	Изменено значение флага блокировки ЭВМ в случае обнаружения попытки загрузки нештатной ОС	<старое значение, новое значение>	Успех
Контроллер СДЗ	Добавлена учетная запись пользователя	<идентификатор пользователя, лимиты действия паролей, разрешенные время работы и дни недели, роль пользователя>	Успех
Контроллер СДЗ	Изменена учетная запись пользователя	<идентификатор пользователя, старые лимиты действия паролей, старые разрешенные время работы и дни недели, новые лимиты действия паролей, новые разрешенные время работы и дни недели, старая и новая роли пользователя>	Успех
Контроллер СДЗ	Удалена учетная запись пользователя	<идентификатор пользователя, лимиты действия паролей, разрешенные время работы и дни недели, роль пользователя>	Успех
Контроллер СДЗ	Удалены учетные записи всех пользователей	–	Успех
Контроллер СДЗ	Пользователю доведен подготовленный пароль	<идентификатор пользователя, доведенный пароль>	Успех
Контроллер СДЗ	Изменена метрика качества аутентификационных данных	<тип параметра, старое значение, новое значение>	Успех
Контроль состава компонентов аппаратного обеспечения	Попытка сохранения аутентификационных данных, не удовлетворяющих метрике качества	<модификация действия (сохранено, заблокировано), идентификатор изменяемого пользователя, пользователя, тип значения (пароль ПИН, секрет), значение>	Успех, если администратор принудительно сохранил данные. Неуспех – в противном случае
Контроллер СДЗ	Выполнен вручную запускаемый тест самотестирования	<тип теста>	Успех – в случае удачного завершения теста. Неуспех – в противном случае
Контроллер СДЗ	Нарушение целостности модуля СДЗ	<имя модуля>	Неуспех
Контроллер СДЗ	Выполнено восстановление данных пользователей СДЗ после аппаратного сбоя	–	Успех
Контроль целостности файлов	Восстановление настроек механизма контроля целостности файлов	–	Успех

Окончание таблицы 3

Источник события	Тип события	Дополнительная информация	Результат
Контроль состава компонентов аппаратного обеспечения	Восстановление настроек механизма контроля состава компонентов аппаратного обеспечения	–	Успех
Контроллер СДЗ	Выполнена попытка перезагрузки ЭВМ после превышения таймаута сторожевого таймера	–	Успех
Контроллер СДЗ	Выполнена попытка загрузки нештатной операционной системы	<строка с нештатной опцией загрузки>	Неуспех
Контроллер СДЗ	Выполнена блокировка ЭВМ для пользователя в связи с превышением максимально допустимого количества попыток аутентификации	<количество попыток аутентификации>	Неуспех
Контроллер СДЗ	Не удалось выполнить перезагрузку после превышения таймаута сторожевого таймера	–	Неуспех
Контроллер СДЗ	Зафиксирована возможная попытка отладки контроллера СДЗ	–	Неуспех
Контроль состава компонентов аппаратного обеспечения	Процедура контроля состава компонентов аппаратного обеспечения начата	–	Успех
Контроль состава компонентов аппаратного обеспечения	Процедура контроля состава компонентов аппаратного обеспечения завершена	–	Успех – в случае отсутствия ошибок при проведении проверки. Неуспех – в противном случае
Контроль состава компонентов аппаратного обеспечения	Текущее дерево устройств сохранено как эталонное	–	Успех
Контроль состава компонентов аппаратного обеспечения	Файл с эталонным деревом устройств не найден	–	Неуспех
Контроль состава компонентов аппаратного обеспечения	Обнаружен не контролируемый узел дерева устройств	<информация об узле>	Неуспех
Контроль состава компонентов аппаратного обеспечения	Утерян контролируемый узел дерева устройств	<информация об узле>	Неуспех
Контроль состава компонентов аппаратного обеспечения	Контролируемый узел дерева устройств изменился	<старая информация об узле, новая информация об узле>	Неуспех
Контроллер СДЗ	Контроллер СДЗ удалялся из слота ЭВМ	–	Неуспех
Контроллер СДЗ	Расхождение времени ЭВМ и времени контроллера СДЗ превысило максимально допустимое значение	<время ЭВМ, время контроллера СДЗ, максимально допустимое расхождение на момент регистрации события>	Неуспех
Контроль состава компонентов аппаратного обеспечения	При проведении контроля состава компонентов аппаратного обеспечения произошел некритичный сбой	<строка с описанием сбоя>	Неуспех

4.11. Требования безопасности к среде функционирования

4.11.1. Общие требования безопасности к среде функционирования

Требования к среде функционирования СДЗ изложены в разделе 2. Помимо функциональной настройки среды функционирования администратор безопасности должен выполнять её настройку для обеспечения защиты программных модулей и данных СДЗ.

В состав функциональных требований безопасности к среде функционирования СДЗ входят:

- анализ потенциального нарушения;
- тестирование функций безопасности;
- надежные метки времени.

4.11.2. Анализ потенциального нарушения

Нарушитель может попытаться получить доступ к ЭВМ, защищенной СДЗ, путем физического отключения контроллера СДЗ. Для противодействия этому администратор СДЗ должен обеспечить физическую защиту ЭВМ, ограничить доступ посторонних к помещению с ЭВМ. Для выявления попыток нарушения физической целостности ЭВМ администратор СДЗ может выполнять опечатывание корпуса ЭВМ и контролировать целостность печатей.

Нарушитель может попытаться перенастроить параметры BIOS ЭВМ таким образом, чтобы СДЗ не запускалось при инициализации устройств ЭВМ. Для противодействия этому администратор СДЗ должен настроить блокировку ЭВМ при помощи аппаратного сброса по сторожевому таймеру. Для выявления попыток данного нарушения администратор должен контролировать журнал событий контроллера СДЗ. Наличие событий срабатывания сторожевого таймера может быть свидетельством попыток отключения СДЗ при помощи изменения параметров BIOS ЭВМ.

Нарушитель может попытаться получить доступ к ЭВМ, используя нестойкие или дискредитированные аутентификационные данные. Для противодействия этому администратор СДЗ должен формировать для пользователей стойкие пароли, использовать механизм двухфакторной аутентификации, выполнять периодическую смену аутентификационных данных и выполнять смену аутентификационных данных при подозрении в том, что аутентификационные данные дискредитированы. Для выявления попыток данного нарушения администратор СДЗ должен проверять журнал регистрации событий. Свидетельством попыток нарушения могут быть многократные попытки ввода неверных аутентификационных данных, блокировки ЭВМ при превышении числа попыток аутентификации.

Нарушитель может попытаться изменить данные в СДЗ при помощи специального (шпионского) программного обеспечения из рабочей ОС ЭВМ. Для противодействия этому администратор СДЗ должен контролировать состав ПО и состояние средств защиты уровня ОС. Если СДЗ не взаимодействует со средствами защиты уровня ОС, администратору СДЗ необходимо включать режим автономной работы СДЗ. Для выявления попыток данного нарушения администратору необходимо контролировать журнал регистрации событий. Свидетельством попыток данного нарушения может являться наличие событий с информацией об идентификациях и аутентификациях после завершения загрузки ЭВМ.

Администратор СДЗ должен анализировать журнал событий в случае возникновения блокировок ЭВМ для пользователя. Особенно необходимо обращать внимание на те случаи, когда пользователь не может понять причину блокировки ЭВМ, например, если ЭВМ заблокирована в результате превышения числа попыток аутентификации, а пользователь не совершал данных действий.

Корректно настроенное СДЗ позволяет успешно противодействовать нарушителям, а своевременный анализ журналов регистрации позволит выявить попытки получения доступа к ЭВМ.

4.11.3. Тестирование функций безопасности

СДЗ выполняет пакет тестовых программ при каждом запуске и несколько тестов однократно по запросу администратора СДЗ для демонстрации правильности выполнения предположений безопасности. Успешное выполнение тестов в процессе самотестирования подтверждает корректность работы СДЗ на данной ЭВМ.

Описание интерфейса ПО управления СДЗ, в том числе интерфейса управления тестированием, приводится в разделе 3 документа ФДШИ.04198-01 34 01 «Руководство оператора».

4.11.4. Надежные метки времени

Контроллер СДЗ предоставляет надежные метки времени для собственного использования при регистрации событий. Администратор СДЗ должен контролировать корректность времени в контроллере СДЗ и в ЭВМ. Администратор СДЗ должен устанавливать время на внутренних часах в контроллере СДЗ, после установки контроллера в ЭВМ. Время в контроллере СДЗ необходимо устанавливать как при первой установке контроллера СДЗ в ЭВМ, так и после установки контроллера СДЗ после временного изъятия из ЭВМ.

Внутренние часы в контроллере СДЗ идут, только когда контроллер установлен в ЭВМ. В контроллере, который был изъят из ЭВМ, внутренние часы сбрасываются. Если администратор СДЗ не установит время в контроллере СДЗ, то время в контроллере СДЗ будет автоматически восстанавливаться по времени ЭВМ при каждой авторизации пользователя. Если время в контроллере СДЗ не было установлено администратором СДЗ, то контроль времени ЭВМ выполняться не будет.

Описание установки времени в контроллере СДЗ приводится в документе ФДШИ.04198-01 34 01 «Руководство оператора».

При работе с журналом регистрации событий администратору СДЗ необходимо учитывать, что события сохраняются и отображаются в порядке регистрации. Если в результате сбоя в работе ЭВМ произойдет сброс времени, то последовательность событий останется неизменной.

4.11.5. Ограничение и мониторинг скрытых каналов

В СДЗ идентифицированы следующие скрытые каналы:

- функции «Идентификация и аутентификация»;
- функции «Блокирование загрузки операционной системы средством доверенной загрузки»;
- функции «Контроль компонентов средств вычислительной техники».

Данные каналы не представляют существенной угрозы, поскольку:

- могут быть использованы только для локальной передачи информации от одного пользователя другому;
- обладают крайне низкой пропускной способностью и позволяют передавать незначительный объем информации;
- не могут быть использованы для организации передачи данных в автоматическом режиме;
- содержат явные демаскирующие признаки.

Критичные скрытые каналы в СДЗ отсутствуют.

Канал функции «Идентификация и аутентификация» может быть использован двумя злоумышленниками для передачи данных с использованием поля ввода идентификатора пользователя. Демаскирующим признаком канала является наличие посторонней информации (не являющейся идентификатором пользователя) в поле ввода идентификатора. Неявным признаком также может являться наличие событий о начале работы СДЗ с отсутствием последующих событий входа пользователей в систему. Устранение данного канала возможно путём включения обязательного применения аппаратных ключей для идентификации и аутентификации пользователей. При невозможности использования данного механизма администратор СДЗ должен использовать организационные меры – постоянный мониторинг демаскирующих признаков,

организацию и ограничение физического доступа к защищаемой ЭВМ и т.п.

Канал функции «Блокирование загрузки операционной системы средством доверенной загрузки» может быть использован злоумышленниками для передачи единичного сигнала, путем выполнения одним злоумышленником действий, приводящих к блокировке ЭВМ для пользователя, и получением вторым злоумышленником информации о блокировке ЭВМ с экрана ЭВМ. Демаскирующим признаком канала является наличие блокировки. Для ограничения или предотвращения возможности использования канала администратор СДЗ должен использовать организационные меры – постоянный мониторинг демаскирующего признака, оперативное устранение сигнала (блокировки ЭВМ) для предотвращения его получения злоумышленником.

Канал функции «Контроль компонентов средств вычислительной техники» может быть использован злоумышленниками путем модулирования передаваемых данных в событиях нарушения целостности файлов ЭВМ, контролируемых СДЗ, и последующего чтения передаваемой информации с экрана (при сигнализации результатов контроля целостности) другим злоумышленником. Демаскирующим признаком канала является наличие нарушений целостности файлов. Устранение данного канала возможно путём блокирования возможности изменения файлов, контролируемых СДЗ (путём ограничения прав доступа к ним). При невозможности использования данного способа, для ограничения или предотвращения возможности использования канала администратор СДЗ должен использовать организационные меры – постоянный мониторинг демаскирующего признака, оперативное устранение сигналов (сведений об файлах с нарушенной целостностью) для предотвращения его получения злоумышленником.

Администратор СДЗ при создании учетных записей пользователей не должен задавать значение идентификатора пользователя, содержащее защищаемую информацию (например, в идентификаторе пользователя не должен содержаться пароль пользователя), так как защищаемая информация в идентификаторе пользователя может быть прочитана злоумышленником с экрана ЭВМ при вводе. Если для аутентификации пользователей СДЗ используются аппаратные ключи, то идентификатор пользователя автоматически отображается на экране при подключении ключа, и если злоумышленник получит доступ к аппаратному ключу пользователя, то он сможет прочитать идентификатор пользователя просто подключив ключ к ЭВМ.

Администратор СДЗ при настройке контроля целостности файлов должен следить, чтобы в именах контролируемых файлов не содержалась защищаемая информация. В процессе контроля целостности файлов отображаются имена контролируемых файлов, и если в именах фалов будет содержаться защищаемая информация, то она будет отображена на экране.

4.12. Действий после сбоев и ошибок эксплуатации средства

Описание действий при возникновении сбоев и ошибок приводится в разделе 2 документа ФДШИ.469535.098РЭ «Аппаратно-программный комплекс «Ребус-СДЗ». Руководство по эксплуатации».

5. РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

5.1. Функции, доступные пользователю СДЗ

Пользователю СДЗ доступны следующие функции безопасности:

- идентификация и аутентификация;
- контроль компонентов СВТ (контроль целостности файлов, контроль состава компонентов аппаратного обеспечения, в части получения сообщений сигнализации о нарушениях);
- сигнализация средства доверенной загрузки;
- блокирование загрузки операционной системы средством доверенной загрузки.

Пользователь должен пройти идентификацию и аутентификацию для получения доступа к рабочей ОС ЭВМ. Если администратор СДЗ настроил ЭВМ двухфакторные идентификацию и аутентификацию, то пользователю необходимо использовать аппаратный ключ.

После успешных идентификации и аутентификации пользователя автоматически проводится контроль компонентов СВТ, включающий в себя контроль целостности файлов и контроль состава компонентов аппаратного обеспечения (при условии, что данные функции включены администратором СДЗ).

Если СДЗ выявит нарушения в работе СДЗ, попытку запуска нештатной ОС, нарушение целостности файлов или состава компонентов аппаратного обеспечения или если произойдет превышение разрешённого числа попыток аутентификации пользователя, то ЭВМ будет заблокирована для пользователя. В этом случае пользователю необходимо обратиться к администратору СДЗ.

Функция сигнализации информирует пользователя о следующих ситуациях:

- обнаружение нарушений в работе СДЗ;
- неверный ввод идентификационных и аутентификационных данных;
- выявление ошибок при самотестировании СДЗ;
- обнаружение нарушений в целостности ресурсов СВТ;
- блокировка ЭВМ для пользователя.

Пользователь может осуществлять загрузку только штатной ОС ЭВМ; загрузка нештатной ОС с внешнего носителя блокируется средствами СДЗ.

Пользователю СДЗ не доступны функции управления СДЗ в том числе управление параметрами СДЗ и просмотр событий безопасности. Обязанность контролировать параметры безопасности СДЗ возлагается на администратора СДЗ.

5.2. Интерфейсы, доступные пользователю

Пользователю доступны следующие интерфейсы СДЗ:

- интерфейс идентификации и аутентификации;
- интерфейс сигнализации;
- интерфейс контроля целостности файлов;
- интерфейс контроля состава компонентов аппаратного обеспечения.

Интерфейс идентификации и аутентификации отображается пользователю при запуске СДЗ.

Интерфейс сигнализации информирует пользователя о нарушениях безопасности, обнаруженных СДЗ, о результатах самотестирования СДЗ и о том, что ЭВМ заблокирована для пользователя в случае блокировки. Если ЭВМ заблокирована для пользователя, на экране будет выведено соответствующее сообщение. Пользователю доступна только общая часть сообщений сигнализации.

Пользователь может получать информацию о ходе выполнения контроля целостности объектов файловой системы и контроля состава компонентов аппаратного обеспечения ЭВМ.

Подробное описание интерфейсов приведено в разделе 3 документа ФДШИ.04198-01 34 01 «Руководство оператора».

5.3. Обязанности пользователя

Пользователь до начала работы на ЭВМ должен получить от администратора СДЗ идентификатор и пароль, сведения о разрешенных для работы днях недели и времени, а также (при необходимости) аппаратный ключ.

Перед включением ЭВМ пользователь должен проверить физическую целостность корпуса ЭВМ, целостность пломб на корпусе ЭВМ, визуально убедиться в отсутствии нештатных устройств, подключенных к ЭВМ. В случае выявления нарушений пользователь должен обратиться к администратору СДЗ. Если нарушений не выявлено, пользователь может включать ЭВМ.

После включения ЭВМ пользователь должен проконтролировать результаты самотестирования ЭВМ (если они отображаются на экране во время работы BIOS ЭВМ) и уведомить администратора СДЗ в случае обнаружения отрицательных результатов такого самотестирования.

После включения ЭВМ пользователь должен пройти идентификацию и аутентификацию в СДЗ (данная процедура описана в разделе 3 документа ФДШИ.04198-01 34 01 «Руководство оператора»). В случае успешного прохождения процедуры пользователю необходимо дождаться завершения работы контроля целостности файлов и контроля состава компонентов аппаратного обеспечения (если данные механизмы включены администратором СДЗ), после чего будет запущена штатная ОС ЭВМ и пользователь сможет приступить к решению своих задач на ЭВМ. Пользователь не должен вмешиваться в процессы контроля целостности файлов, контроля состава компонентов аппаратного обеспечения, а также в процесс загрузки ОС, не должен нажимать кнопки на клавиатуре либо пытаться изменить режим запуска ОС. До завершения загрузки ОС клавиатура ЭВМ блокируется, а в некоторых случаях нажатие кнопок клавиатуры может привести к перезагрузке ЭВМ.

В ходе работы СДЗ ЭВМ по различным причинам может быть заблокирована для пользователя. В таком случае пользователю необходимо обратиться к администратору СДЗ.

Пользователь также должен обратиться к администратору СДЗ в случае:

- циклических перезагрузок ЭВМ при включении;
- при зависании ЭВМ при запуске;
- если при включении ЭВМ СДЗ не отображает экран идентификации и аутентификации пользователя, а сразу начинается загрузка ОС;
- при выявлении других, не описанных здесь, проблем функционирования СДЗ или ЭВМ.

5.4. Требования безопасности к среде функционирования, относящиеся к пользователю

Требования к среде функционирования СДЗ изложены в разделе 2. Для обеспечения безопасности СДЗ и ЭВМ, на которой применяется СДЗ, пользователь должен:

- эксплуатировать СДЗ и ЭВМ строго в соответствии с их эксплуатационной документацией;
- контролировать результаты самотестирования ЭВМ и СДЗ, и уведомлять администратора СДЗ об отрицательных результатах самотестирования;
- не нарушать физическую целостность корпуса ЭВМ, целостность пломб на корпусе ЭВМ, и уведомлять администратора СДЗ в случае выявления таких ситуаций;
- не подключать к ЭВМ нештатные устройства и уведомлять администратора в случае выявления таких устройств;
- не допускать компрометации своего пароля (путём самостоятельного разглашения, хранения на физическом носителе, предоставления возможности подсмотреть пароль при его наборе и т.п.);
- не допускать утери своего аппаратного ключа (при его использовании);
- своевременно уведомлять администратора СДЗ о появлении сообщений о переполнении журналов аудита СДЗ;
- не осуществлять установку нештатного ПО в ОС ЭВМ, а также уведомлять администратора СДЗ в случае появления нештатного ПО.

6. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными в СДЗ являются:

- идентификаторы, пароли, ПИН-коды и секреты пользователей;
- параметры учетных записей пользователей;
- параметры аппаратных ключей (ПИН-код и секрет);
- параметры запуска контроллера СДЗ;
- параметры работы функций безопасности;
- параметры контроля целостности файлов;
- параметры контроля неизменности состава аппаратных средств;
- параметры реакции СДЗ на возникновения событий нарушения безопасности;
- параметры реакции СДЗ на возникновения сбоев СДЗ.

В качестве выходных данных в СДЗ выступают:

- сообщения СДЗ на действия пользователей;
- сообщения СДЗ на нарушения безопасности;
- сообщения СДЗ в случае возникновения сбоев и отказов;
- журналы аудита СДЗ;
- сохраненные параметры конфигурации СДЗ, сформированные в процессе управления СДЗ;
- отчеты результатов самодиагностики СДЗ;
- контрольные суммы модулей и данных СДЗ.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

НСД – несанкционированный доступ
ОС – операционная система
ПИН – персональный идентификационный номер
ПО – программное обеспечение
СВТ – средство вычислительной техники
СДЗ – средство доверенной загрузки
СрЗИ – средство защиты информации
ЭВМ – электронно-вычислительная машина
ЭД – эксплуатационная документация
ЭН – электронный носитель
ЭЦП – электронная цифровая подпись

Лист регистрации изменений

Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в докум.*	*№ документа*	*Входящий № сопроводительного докум. и дата*	*Подп.*	*Дата*
	изменённых	*заменённых*	*новых*	*аннулированных*					