УТВЕРЖДЕН
ФДШИ.04198-01 34 01-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СДЗ

Руководство оператора

ФДШИ.04198-01 34 01

Листов 57

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

2023

Литера $О_1$

АННОТАЦИЯ

В данном документе описаны действия оператора по практическому использованию ФДШИ.04198-01 «Программное обеспечение СДЗ» (далее по тексту – ПО СДЗ) в составе ФДШИ.469535.098 «Аппаратно-программный комплекс «Ребус-СДЗ» (далее по тексту – СДЗ).

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

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.

1.1. Состав СДЗ

Основными составными частями СДЗ являются:

- ФДШИ.04198-01 «Программное обеспечение СДЗ»;
- ФДШИ.468353.040 «Контроллер СДЗ1 «Тверца-5» (далее по тексту – контроллер СДЗ).

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.

1.2. Функции СДЗ

ПО СДЗ в составе СДЗ выполняет следующие функции:

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

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

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 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 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.

Все функции изделия выполняются до загрузки ОС, требования к общесистемному ПО не предъявляются, и изделие может функционировать с любой ОС, установленной на ЭВМ.

При использовании на ЭВМ специфического оборудования (такого, как дополнительные контроллеры защиты или контроллеры, работающие до загрузки ОС) необходима проверка на возможность совместного функционирования данных устройств с СДЗ.

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.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Общие сведения

ПО СДЗ запускается непосредственно с контроллера СДЗ или с загрузочного дистрибутивного ЭН, установка ПО СДЗ в рабочую ОС не требуется. Описание установки и настройки контроллера СДЗ приведено в документе ФДШИ.469535.098РЭ «Аппаратно-программный комплекс «Ребус-СДЗ». Руководство по эксплуатации».

Запуск ПО контроллера СДЗ происходит автоматически, при включении ЭВМ. Запуск ПО управления СДЗ осуществляется по команде администратора СДЗ.

3.2. Идентификация и аутентификация пользователя

Сразу после включения ЭВМ на мониторе отображается экран идентификации и аутентификации пользователя (рис. 1).

Экран идентификации и аутентификации пользователя

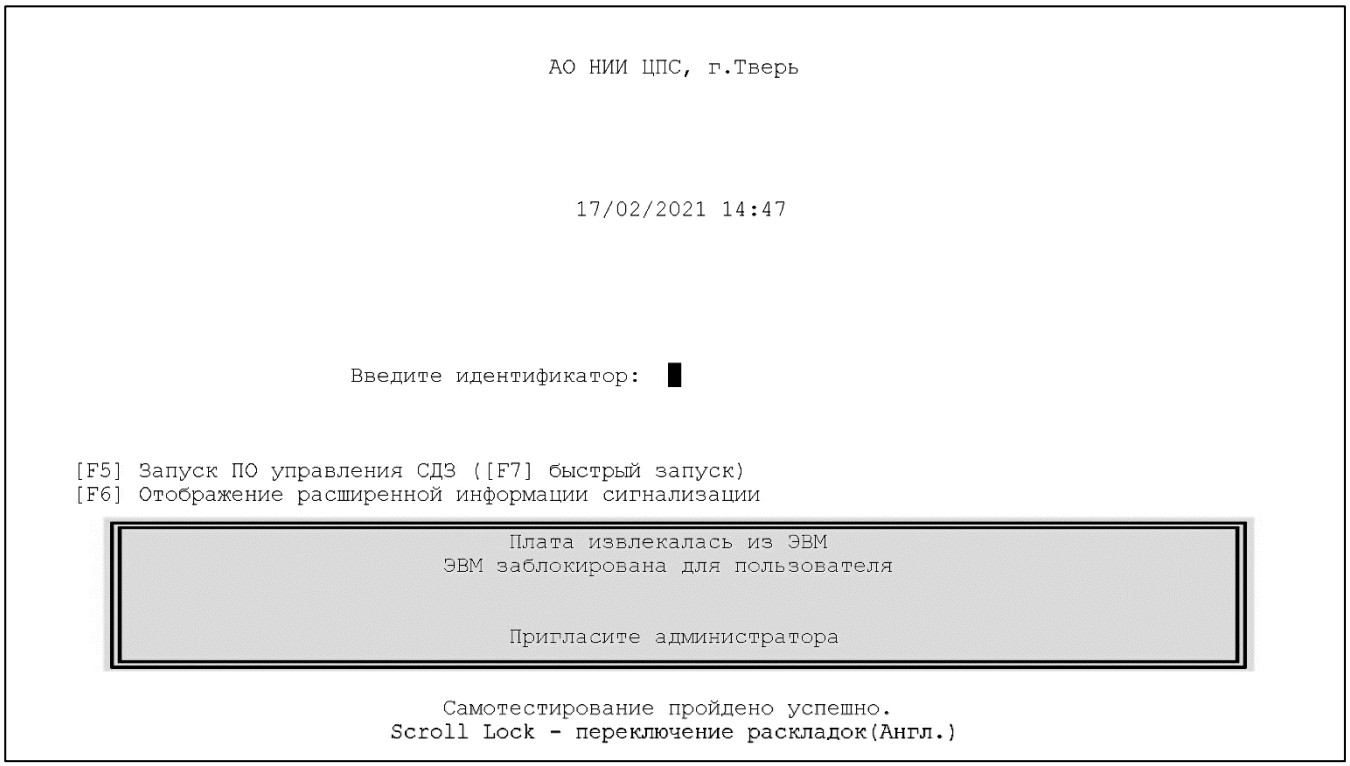


Рис. 1

Экран идентификации и аутентификации пользователя содержит следующие данные:

- текущую дату и время;
- запрос на ввод идентификатора пользователя «Введите идентификатор» либо, если администратором СДЗ настроено обязательное применение аппаратных ключей (двухфакторная аутентификация), запрос «Подключите аппаратный ключ»;
- подсказки «[F5] Запуск ПО управления СДЗ / [F7] быстрый запуск» и «[F6] Отображение расширенной информации сигнализации»;
- при выявлении СДЗ нарушений безопасности – сообщения в рамке на красном фоне: «ЭВМ заблокирована для пользователя», «Пригласите администратора», «Плата извлекалась из ЭВМ» и т.п.;
- сообщение о результате самотестирования: «Самотестирование пройдено успешно» или «Внимание! Самотестирование не пройдено».

Для входа в систему при появлении экрана идентификации и аутентификации пользователь должен выполнить следующие проверки:

- убедиться в корректности отображаемых даты и времени;
- убедиться в наличии сообщения об успешном прохождении самотестирования;
- убедиться в отсутствии сообщений о блокировке ЭВМ для пользователя и о необходимости обратиться к администратору.

В случае выявления несоответствия хотя бы по одному из указанных пунктов пользователь должен незамедлительно обратиться к администратору СДЗ и уведомить о выявленных несоответствиях. Дальнейшая работа пользователя на ЭВМ будет возможна после устранения проблем администратором СДЗ.

При успешном прохождении проверок пользователь должен пройти идентификацию и аутентификацию, используя полученные от администратора СДЗ идентификатор и пароль.

Для идентификации пользователь должен ввести свой идентификатор с помощью клавиатуры (при отображении запроса «Введите идентификатор») либо подключить к ЭВМ свой аппаратный ключ (при отображении запроса «Подключите аппаратный ключ»). Аппаратный ключ типа iButton необходимо подключать к считывателю, подключенному к контроллеру СДЗ. USB-ключ необходимо подключать к USB-порту ЭВМ. При успешном чтении данных с аппаратного ключа идентификатор пользователя, записанный в ключе, отобразится на экране.

Для аутентификации пользователь должен в ответ на запрос ввести свой пароль с помощью клавиатуры.

Примечание. Регистр символов идентификатора и пароля важен и должен верно указываться пользователем при его вводе с клавиатуры.

После предъявления пользователем идентификатора и пароля СДЗ проверит их корректность и соответствие друг другу, срок действия пароля, а также разрешенные пользователю дни недели и время работы.

В случае если введенный пароль пользователя верен, но его срок действия истек и при этом администратором СДЗ для пользователя заранее был подготовлен новый пароль, будет проведена процедура доведения пароля (описанная в 3.4).

В случае неуспешного прохождения проверок пользователю будет отображено соответствующее сообщение, после чего пользователь может повторить попытку идентификации и аутентификации.

Допустимое количество попыток аутентификации ограничено и задается администратором СДЗ. Если пользователь не сможет успешно пройти аутентификацию за это количество попыток, СДЗ заблокирует ЭВМ для пользователя и перезагрузит ЭВМ.

После успешного прохождения идентификации и аутентификации СДЗ проведет контроль целостности файлов (программной среды) и контроль состава компонентов аппаратного обеспечения (если данные механизмы включены администратором СДЗ). Если в ходе этих операций будут выявлены нарушения и администратором СДЗ включена блокировка при нарушении целостности, то СДЗ заблокирует ЭВМ для пользователя.

Если описанные выше проверки пройдут успешно, пользователь будет считаться авторизованным, ему будет разрешена работа на ЭВМ и будет запущена загрузка рабочей ОС ЭВМ. Если же ЭВМ была заблокирована для пользователя, ему для продолжения работы на ЭВМ необходимо будет обратиться к администратору СДЗ.

3.3. Идентификация и аутентификация администратора СДЗ

Процесс идентификации и аутентификации администратора СДЗ в целом идентичен аналогичному процессу для непривилегированного пользователя за исключением следующих моментов:

- блокировка ЭВМ для пользователя на администратора СДЗ не действует. После успешной авторизации администратор СДЗ будет допущен к работе с ЭВМ независимо от наличия или отсутствия такой блокировки;
- администратор СДЗ может инициировать запуск ПО управления СДЗ, нажав клавишу «F5» до или во время ввода идентификатора и пароля. В этом случае около соответствующей

подсказки появится символ, сигнализирующий об активации данной возможности, а после успешной авторизации вместо рабочей ОС будет запущено ПО управления СДЗ;

- администратор СДЗ может инициировать быстрый запуск ПО управления СДЗ, нажав клавишу «F7» до или во время ввода идентификатора и пароля. Быстрый запуск ПО управления СДЗ отличается от обычного тем, что при этом не будут выполнены контроль целостности файлов (программной среды) и контроль состава компонентов аппаратного обеспечения;

- администратор СДЗ может инициировать отображение расширенной информации сигнализации (рис. 2), нажав клавишу «F6» до или во время ввода идентификатора и пароля. В этом случае около соответствующей подсказки появится символ, сигнализирующий об активации данной возможности, а после успешной авторизации будет отображена дополнительная расширенная информация о самотестировании СДЗ и событиях сигнализации;

- если администратор СДЗ предварительно настроил запуск тестов по запросу для самотестирования СДЗ (описание настройки тестов приведено в 3.6.8), после успешного прохождения идентификации и аутентификации эти тесты отработают в соответствии с описанием в 3.11.

Экран отображения расширенной информации сигнализации

```
Тестирование функции разграничения доступа к управлению СДЗ                          |Успешно
Тестирование функции управления работой СДЗ                                          |Успешно
Тестирование функции управления параметрами СДЗ                                      |Успешно
Тестирование функции аудита безопасности средства доверенной загрузки               |Успешно
Тестирование функции идентификации и аутентификации                                  |Успешно
Тестирование функции тестирования средства доверенной загрузки, контроля целостности |Успешно
   программного обеспечения и параметров средства доверенной загрузки               |
Тестирование функции контроля целостности объектов файловой системы СВТ             |Не проводилось
Тестирование функции контроля неизменности состава аппаратных средств СВТ           |Не проводилось
Тестирование функции блокирования загрузки ОС средствами доверенной загрузки       |Не проводилось
Тестирование функции сигнализации средства доверенной загрузки                      |Успешно
Тестирование функции механизма обеспечения безопасного состояния                    |Успешно
Тестирование функции защиты остаточной информации СДЗ                               |Успешно
Тестирование функции защиты интерфейса управления СДЗ                               |Успешно
Тестирование аппаратной части СДЗ                                                    |Успешно
```

Up(Выше), Down(Ниже), Esc(Выход)...

Рис. 2

В случае выявления проблем до или во время идентификации и аутентификации администратор СДЗ должен выявить причины этих проблем и устранить их. Описание возможных проблем и действий администратора СДЗ при их выявлении приведено в документах ФДШИ.04198-01 31 01 «Описание применения» и ФДШИ.469535.098РЭ «Аппаратно-программный комплекс «Ребус-СДЗ». Руководство по эксплуатации».

3.4. Доведение паролей

В СДЗ для пользователя можно заранее задать (подготовить) до пяти паролей. Если срок действия текущего пароля пользователя истек, пользователю дополнительно подготовлен новый пароль (с неистекшим сроком действия) и пользователь знает этот новый пароль, то пользователь может сразу ввести новый пароль при аутентификации.

Если же новый пароль (с неистекшим сроком действия) подготовлен, но пользователь его не знает, то при истечении срока действия текущего пароля и вводе текущего пароля будет запущена процедура доведения пароля: на экране пользователю отобразится новый пароль, и пользователь должен подтвердить вводом нового пароля, что он запомнил новый пароль (рис. 3). После этого пользователь сможет использовать новый пароль для входа в систему.

Доведение пароля

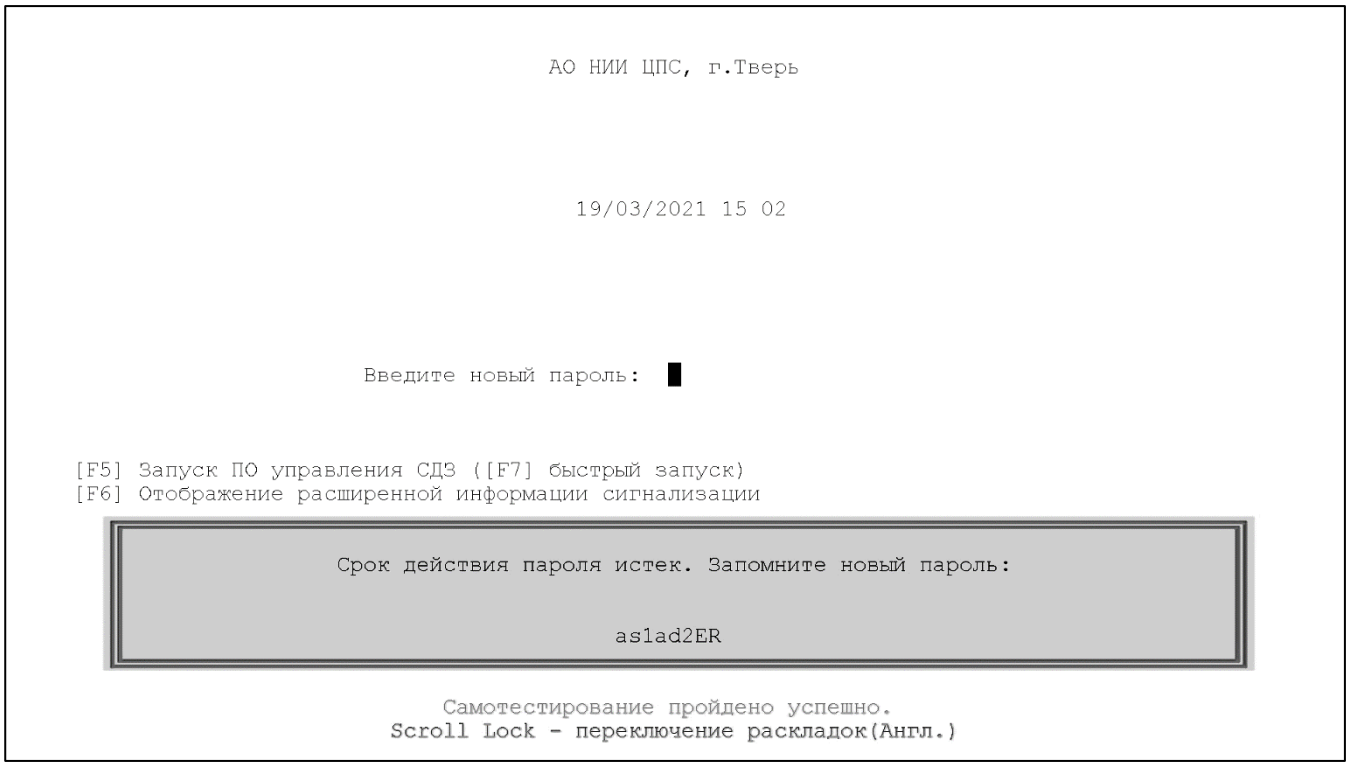


Рис. 3

3.5. ПО управления СДЗ

3.5.1. Запуск ПО управления СДЗ

Управление СДЗ осуществляется администратором СДЗ с помощью ПО управления СДЗ. Непривилегированному пользователю ПО управления СДЗ недоступно.

Запуск ПО управления СДЗ возможен двумя способами:

- из внутренней памяти контроллера СДЗ;
- с загрузочного дистрибутивного электронного носителя (ЭН).

С дистрибутивного ЭН и из внутренней памяти контроллера СДЗ запускается одно и то же графическое приложение ПО управления СДЗ.

Для запуска ПО управления СДЗ из внутренней памяти контроллера СДЗ необходимо при идентификации и аутентификации администратора СДЗ до или во время ввода идентификатора и пароля нажать клавишу «F5» (для обычного запуска) или «F7» (для быстрого запуска – без контроля целостности файлов (программной среды) и контроля состава компонентов аппаратного обеспечения), при этом напротив текста «Запуск ПО управления СДЗ» отобразится символ «*» (рис. 4).

Выбор запуска ПО управления СДЗ

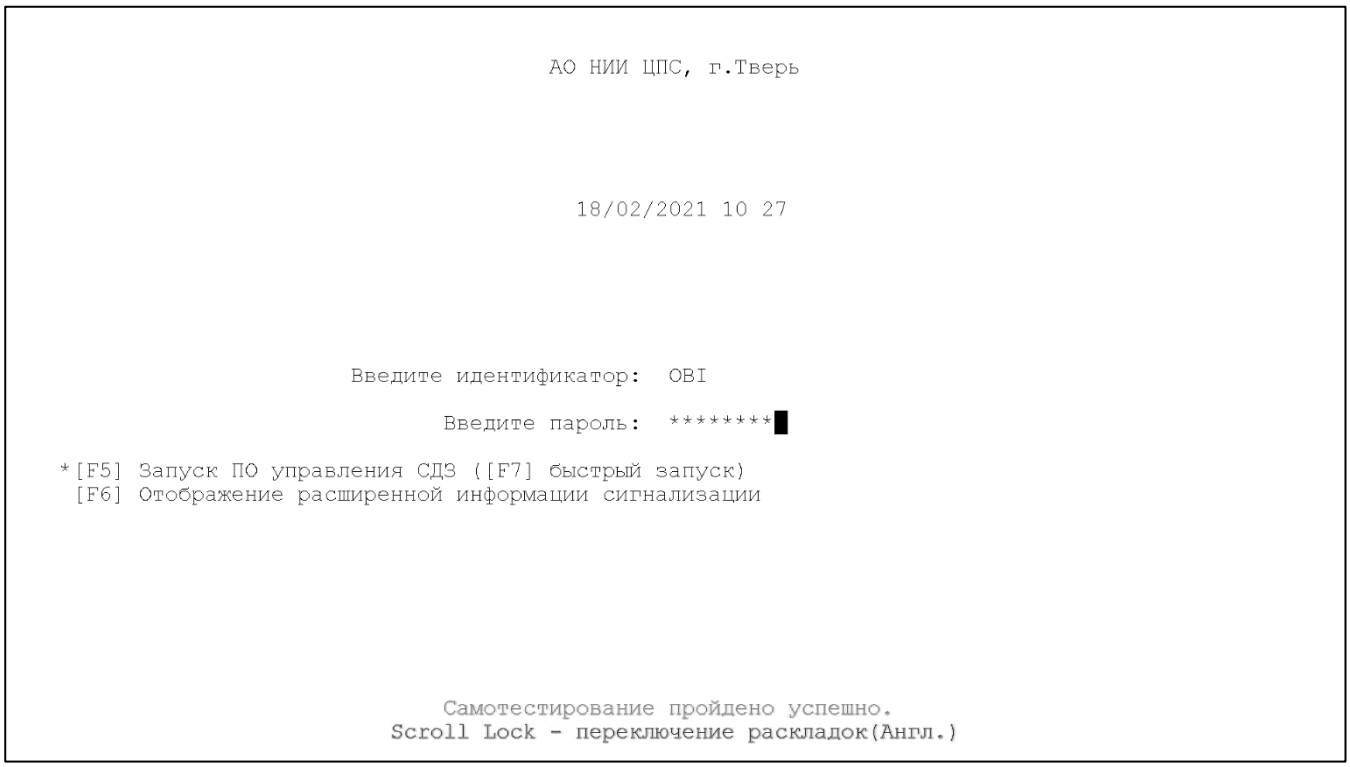


Рис. 4

После успешной авторизации администратора СДЗ вместо запуска рабочей ОС ЭВМ произойдет запуск ПО управления СДЗ (рис. 5).

Главное окно ПО управления СДЗ

Рис. 5

На некоторых типах ЭВМ запуск ПО управления СДЗ из внутренней памяти контроллера СДЗ не может быть выполнен по техническим причинам, в данном случае необходимо пользоваться ПО управления СДЗ с дистрибутивного ЭН. Для запуска с дистрибутивного ЭН необходимо установить его в CD/DVD-привод ЭВМ и обеспечить загрузку с него настройками BIOS ЭВМ или с помощью меню BIOS с выбором устройства для загрузки (обычно данное меню активируется при нажатии в момент включения ЭВМ одной из клавиш «Esc», «F8», «F10» или «F12»; более точную информацию о том, как запустить ЭВМ с загрузочного CD/DVD-диска, можно получить из документации на материнскую плату ЭВМ).

3.5.2. Работа ПО управления СДЗ

При старте ПО управления будет отображено главное меню со следующими пунктами ПО управления СДЗ (см. рис. 5):

- «Управление СДЗ»;
- «Контроль целостности файлов»;
- «Контроль состава компонентов аппаратного обеспечения»;
- «Восстановление заводских настроек»;
- «Расчет контрольных сумм СДЗ».

После выбора любого пункта меню ПО управления СДЗ необходимо ввести идентификатор и пароль администратора СДЗ. Это необходимо для восстановления сессии взаимодействия с контроллером СДЗ.

При использовании ПО управления СДЗ могут возникнуть проблемы с сохранением данных на диски с файловой системой NTFS, когда в качестве рабочей ОС на ЭВМ используется ОС семейства Windows. Данные проблемы связаны с особенностью размонтирования разделов NTFS в указанных ОС. Проблема воспроизводится только при выключении ЭВМ из рабочей ОС, а если рабочая ОС будет отправлена на перезагрузку, и после перезагрузки будет запущено ПО управления СДЗ, то проблем с сохранением данных на разделы NTFS не возникает.

Для устранения проблемы необходимо в Системных параметрах ОС Windows, в разделе «Все элементы панели управления»→«Электропитание»→«Системные параметры» отключить параметр «Включить быстрый запуск» (по умолчанию данный параметр включен). Для активации возможности управления данным параметром необходимо нажать на элемент «Изменение параметров, которые сейчас недоступны».

Получить доступ к необходимому разделу системных параметров ОС Windows можно следующими способами:

- в строке поиска рядом с кнопкой «Пуск» набрать «Панель управления»; открыть в ней «Электропитание»→«Действие кнопки питания» (слева);
- нажать правой кнопкой мышки кнопку «Пуск», выбрать «Управление электропитанием»→«Дополнительные параметры питания» (справа)→«Действие кнопки питания».
- в меню «Пуск» выбрать «Параметры»→«Система»→«Питание и спящий режим»→ «Дополнительные параметры питания»→«Действие кнопки питания» (слева).

3.6. Управление СДЗ

3.6.1. Общая информация

Управление СДЗ предоставляет возможность администратору СДЗ управлять списком пользователей, параметрами запуска СДЗ, параметрами работы функций СДЗ, аппаратными ключами, датой и временем, запускаемыми тестами и выполнять просмотр журналов регистрации событий СДЗ.

Для запуска управления СДЗ необходимо в главном меню ПО управления СДЗ выбрать пункт «Управление СДЗ». Для получения доступа к данным необходимо пройти аутентификацию администратором СДЗ.

После запуска управления СДЗ на экране отображается окно, содержащее следующие вкладки:

- «Пользователи»;
- «Журнал событий (СДЗ)»;
- «Управление контроллером»;
- «Аппаратные ключи»;
- «Дата и время»;
- «Выгрузка драйверов»;
- «Тесты».

Если ЭВМ заблокирована для пользователей, то под заголовком приложения отображается сообщение «Внимание: ЭВМ заблокирована для пользователя!» (рис. 6). Для снятия блокировки администратору СДЗ необходимо нажать кнопку «Снять блокировку». После снятия блокировки сообщение о блокировке пропадает.

Главное окно управления СДЗ

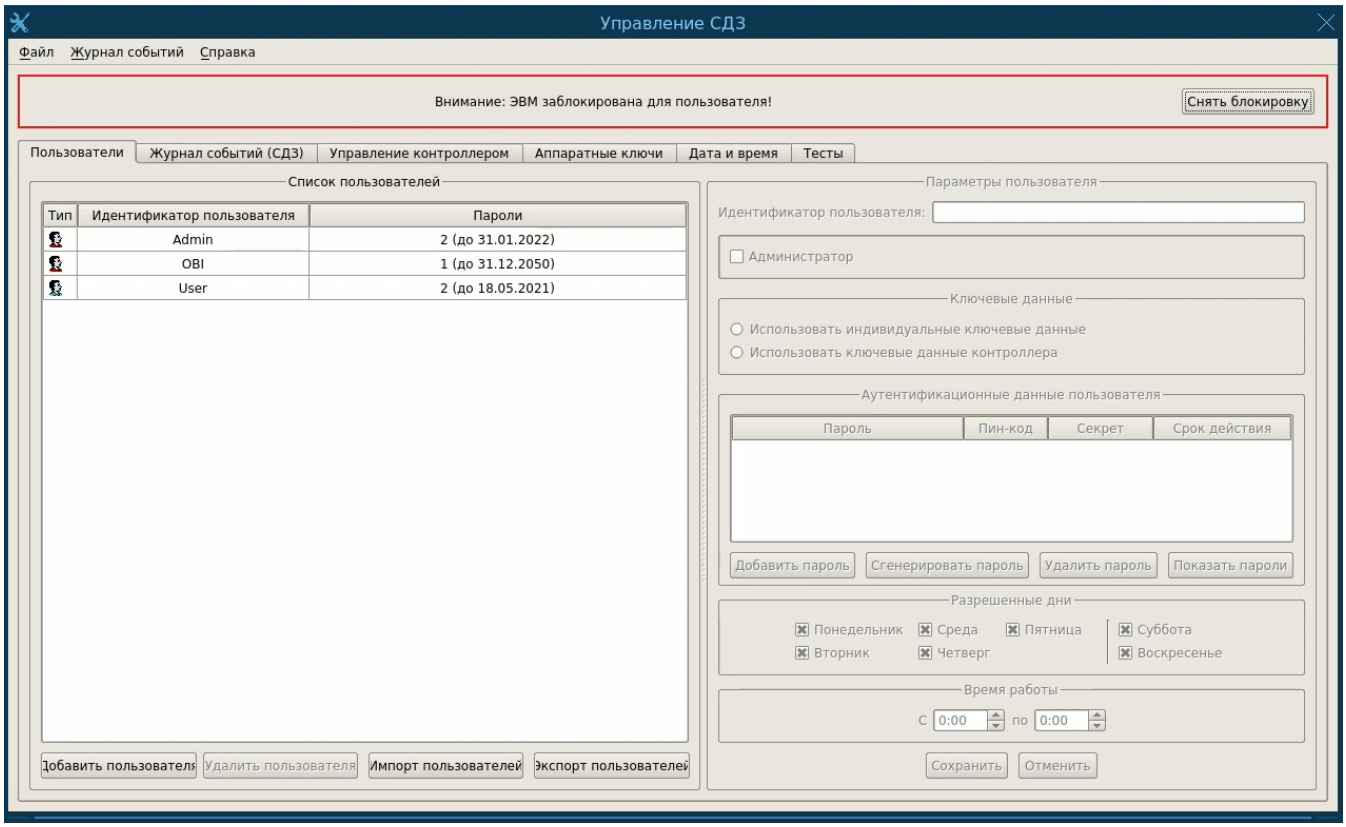


Рис. 6

3.6.2. Вкладка «Пользователи»

Левая панель (группа элементов «Список пользователей») отображает текущий список пользователей, сохраненных в памяти контроллера СДЗ (рис. 7). Каждая строка списка представляет пользователя.

Примечание. Здесь и далее при описании настройки под пользователем понимается учетная запись пользователя. При этом одному и тому же реальному пользователю (человеку) могут соответствовать одна или несколько учетных записей с разными параметрами.

Группа «Список пользователей»

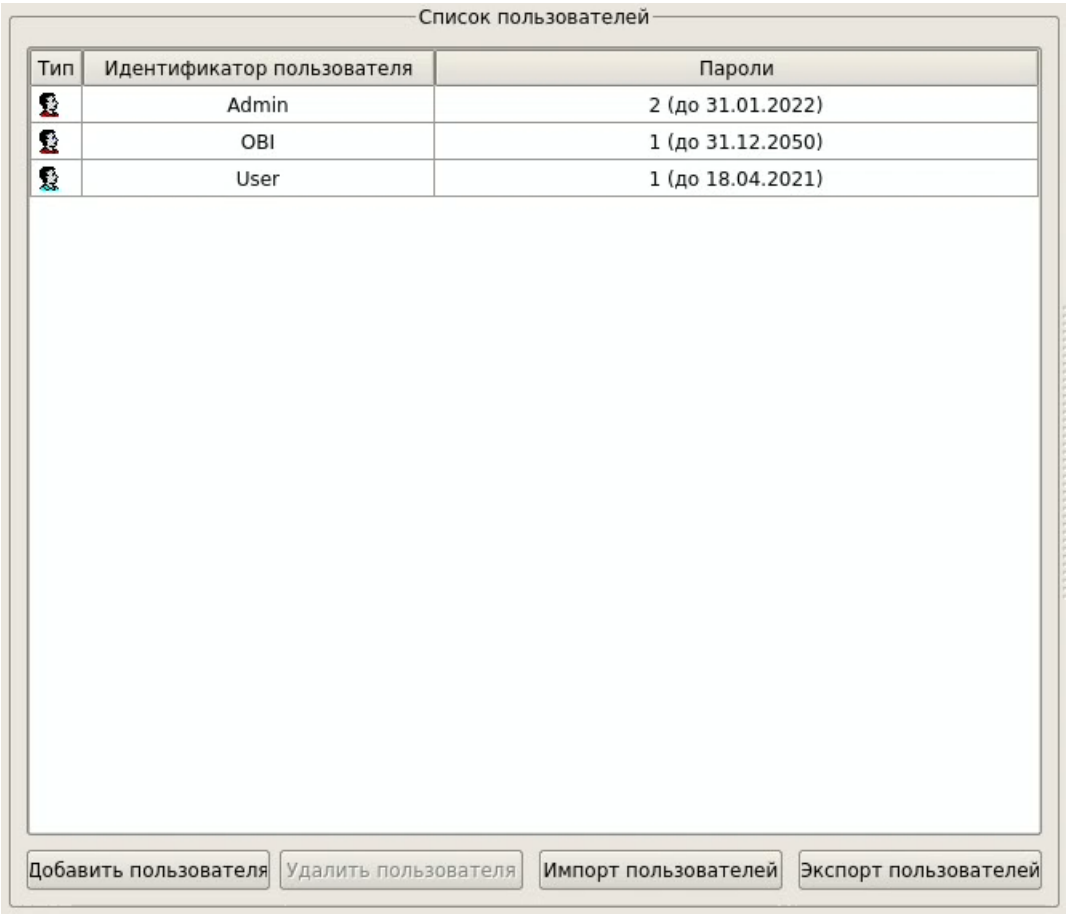


Рис. 7

В колонке «Тип» пиктограммой отображается тип пользователя (синяя пиктограмма обозначает непривилегированного пользователя, красная – администратора СДЗ). В колонке «Идентификатор пользователя» отображается строковый идентификатор пользователя. Колонка «Пароли» содержит указание количества сохраненных паролей и дату истечения последнего из них.

Кнопка «Добавить пользователя» используется для создания нового пользователя. Кнопка «Удалить пользователя» предназначена для удаления выбранного пользователя. Кнопка «Экспорт пользователей» предназначена для сохранения списка пользователей в выбранный файл на носитель. По нажатии кнопки открывается файловый диалог с подключаемыми внешними носителями информации в режиме сохранения данных. Кнопка «Импорт пользователей» используется для добавления пользователей из ранее сохраненного списка. Существующие пользователи будут перезаписаны.

Правая панель отображает параметры учетной записи выбранного в левой панели пользователя либо параметры создаваемой учетной записи пользователя.

Элементы управления группы «Параметры пользователя» позволяют сохранить сделанные изменения на контроллер либо отменить изменения (рис. 8).

Группа «Параметры пользователя»

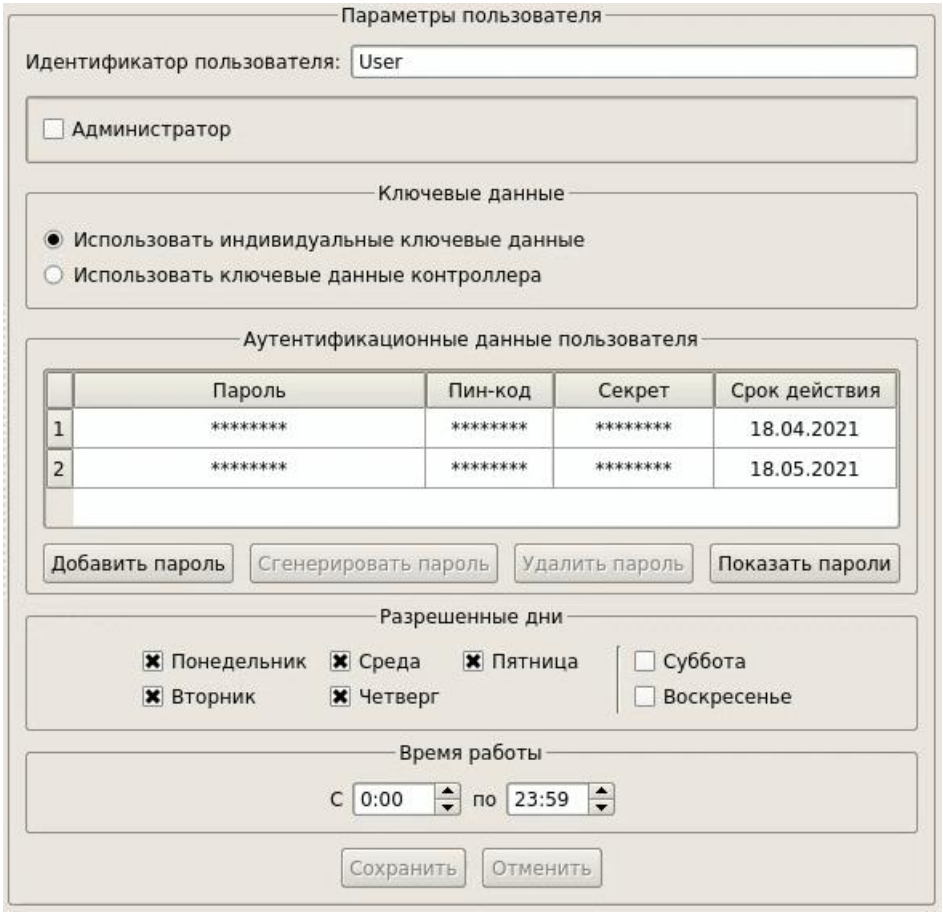


Рис. 8

Поле «Идентификатор пользователя» предназначено для отображения или редактирования строкового идентификатора пользователя. Поле доступно для редактирования только при добавлении пользователя. В случае уже существующего пользователя данное поле не является редактируемым.

Кнопка-флаг «Администратор» позволяет задать роль пользователя. Если флаг установлен, пользователь получает роль администратора СДЗ, в противном случае – роль пользователя (непривилегированного).

Элементы управления группы «Ключевые данные» позволяют выбрать тип используемых при аутентификации данного пользователя ключевых данных (ПИН-кода и секрета аппаратных ключей пользователя). Для каждой учетной записи пользователя можно установить использование индивидуальных ключевых данных или ключевых данных контроллера. Если выбран вариант «Использовать индивидуальные ключевые данные», то при формировании аппаратных ключей будут использоваться данные из таблицы «Аутентификационные данные пользователя». Если выбран пункт «Использовать ключевые данные контроллера», то при формировании аппаратных ключей будут использоваться общие ключевые данные контроллера. Управление ключевыми данными контроллера выполняется во вкладке «Аппаратные ключи».

Таблица «Аутентификационные данные пользователя» содержит набор аутентификационных данных: паролей и их сроков действия, ПИН-кодов, секретов. Не допускается задание двух паролей с одинаковым сроком действия. Допускается задание максимум пяти паролей для учетной записи пользователя.

Если пользователю настроено использование ключевых данных контроллера, то в колонке «ПИН-код» и «Секрет» будут установлены общий для контроллера ПИН-код и секрет, автоматически формируемые из секрета контроллера и данных учетной записи пользователя.

ПИН-код и секрет контроллера задаются во вкладке «Аппаратные ключи» (описание приведено в 3.6.5).

Если пользователю настроено использование индивидуальных ключевых данных, то администратор СДЗ должен задать для каждого пароля ПИН-код и секрет. Активировать режим редактирования ПИН-кода и пароля можно щелчком мыши по соответствующему полю в таблице.

Группа «Разрешенные дни» позволяет задать разрешенные для работы пользователя дни недели.

Группа «Время работы» предназначена для отображения и изменения информации о разрешенном времени работы для пользователя. При установке значений полей «С» и «по» осуществляется контроль ввода непересекающихся интервалов.

Средство управления СДЗ при запуске считывает текущие параметры учетных записей пользователей, хранящиеся во внутренней памяти контроллера, и заполняет таблицу полученными значениями. Для просмотра детальных сведений об отдельном пользователе необходимо выбрать соответствующую строку в списке пользователей. Параметры выбранного пользователя отобразятся в правой панели в режиме редактирования. Для сохранения внесенных изменений необходимо нажать кнопку «Сохранить». При этом автоматически обновится общий список пользователей. Нажатие кнопки «Отменить» отменяет внесенные, но еще не сохраненные изменения.

Для создания нового пользователя необходимо воспользоваться кнопкой «Добавить пользователя». При этом активизируются элементы правой панели, включая идентификатор пользователя. Для добавления пароля нужно нажать на кнопку «Добавить пароль». Пользователю возможно задать 5 паролей. Для изменения срока действия пароля необходимо в таблице «Аутентификационные данные пользователя» в поле «Срок действия» сделать двойной щелчок мышью и затем выбрать срок действия пароля. После установки всех требуемых параметров учетной записи пользователя необходимо нажать кнопку «Сохранить» для записи пользователя в память контроллера. Если идентификатор нового пользователя совпадает с идентификатором одного из уже существующих пользователей, то кнопка «Сохранить» станет неактивной. Нажатие кнопки «Отменить» возвращает фокус ввода в панель всех пользователей, и добавление пользователя не производится.

Если включена проверка метрики качества аутентификационных данных, то при попытке задания некорректных аутентификационных данных поля ввода с данными, не удовлетворяющими метрике качества, будут подкрашены красным цветом.

Если включена блокировка сохранения некорректных аутентификационных данных, то сохранить пользователя с аутентификационными данными, не удовлетворяющими метрике качества, будет нельзя.

Для удаления пользователя необходимо выбрать соответствующую строку в списке пользователей и нажать на кнопку «Удалить пользователя». Появится окно с запросом подтверждения выполняемой операции. Для операции удаления имеет значение тип удаляемого пользователя: так как для работы СДЗ необходима хотя бы одна учетная запись администратора СДЗ, средство управления СДЗ не позволит удалить единственную (последнюю) учетную запись администратора СДЗ. Если данного пользователя все же необходимо удалить, следует заранее создать другую учетную запись администратора СДЗ либо присвоить эту роль одному из уже существующих пользователей.

3.6.3. Вкладка «Журнал событий (СДЗ)»

СДЗ ведет в ходе работы журнал контроллера СДЗ, в который записывает события аудита (кроме событий контроля целостности файлов и контроля состава компонентов аппаратного обеспечения; описания журналов таких событий приведены в 3.7.4 и 3.8.4 соответственно). Записи журнала содержат следующие элементы:

- дата регистрации события;
- время регистрации события;
- идентификатор пользователя;

- тип события;
- результат события;
- дополнительная информация.

Регистрируемые типы событий приводятся в разделе 4 документа ФДШИ.04198-01 31 01 «Описание применения».

Время регистрации событий может быть получено из разных источников: из времени ЭВМ или из внутреннего времени контроллера СДЗ. Администратор СДЗ должен следить за тем, чтобы время на контроллере СДЗ и на ЭВМ было синхронным. Для событий сторожевого таймера («Истекло время ожидания сторожевого таймера» и «Не отработала блокировка по сторожевому таймеру») используется только время из контроллера СДЗ. События, источником времени которых является ЭВМ, при отображении будут подсвечены светло-серым цветом.

При отображении журнала событий упорядочивание событий происходит не по времени, а в порядке их регистрации. Последовательность событий будет сохранена, даже если на ЭВМ в ходе ее работы было изменено время.

Вкладка «Журнал событий (СДЗ)» (рис. 9) предназначена для просмотра администратором СДЗ журнала контроллера СДЗ, а также для работы с архивами журналов. В левой части вкладки расположены элементы управления источниками событий и фильтрами, в правой – таблица с событиями. В группе «Источники событий» можно выбрать источники событий – журнал контроллера СДЗ или архивы.

Вкладка «Журнал событий (СДЗ)»

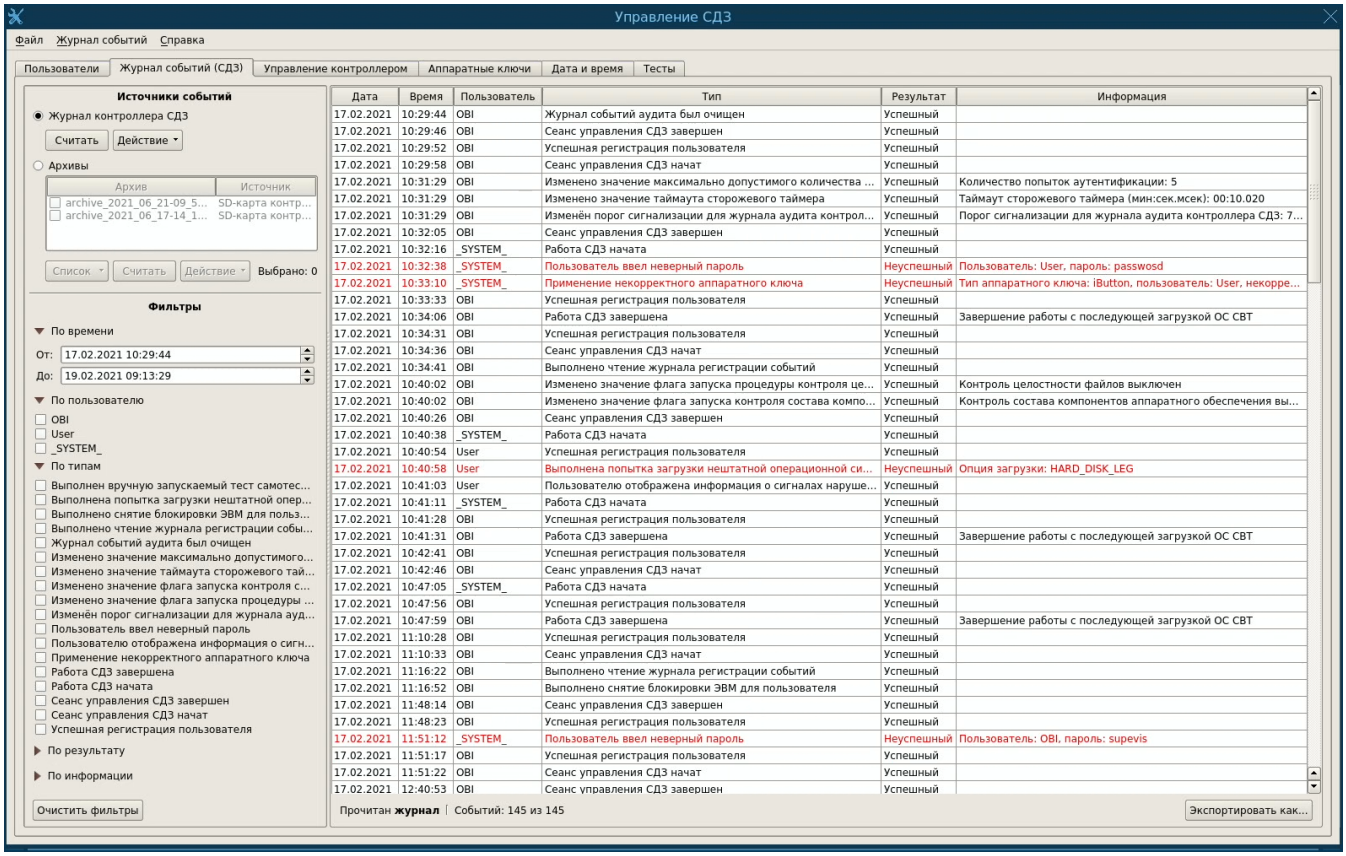


Рис. 9

Для просмотра текущего журнала событий необходимо в качестве источника событий выбрать «Журнал контроллера СДЗ» и нажать кнопку «Считать». Журнал будет считан с контроллера СДЗ и отображен в таблице с событиями.

Кнопка-список «Действие» позволяет администратору СДЗ выполнить следующие действия с журналом контроллера СДЗ:

- просмотр свойств журнала;
- очистка журнала;
- сохранение журнала событий (СДЗ) в качестве архива.

Действие «Показать свойства» позволяет просмотреть свойства текущего журнала, такие как время создания (первого события), размер журнала.

Действие «Очистить журнал» используется для очистки журнала во внутренней памяти контроллера СДЗ. Перед очисткой журнала будет предложено сохранить его как архив. В ходе очистки журнала события будут полностью удалены без возможности восстановления. Факт очистки журнала регистрируется в нем после выполнения очистки.

Действие «Сохранить как архив» используется для сохранения содержимого журнала в виде архива событий. По нажатии кнопки открывается файловый диалог для выбора места сохранения архива (рис. 10). В раскрывающемся списке «Раздел» необходимо выбрать требуемый раздел носителя информации, при этом произойдет его автоматическое монтирование (признаком успешного монтирования является появление структуры раздела в древовидном и табличном представлении). Для разделов Ext2, Ext3, Ext4 можно указать кодировку отображения (например, UTF-8 – для раздела ОС СН «Astra Linux Special Edition», KOI8-R – для раздела ОС МСВС и т.п.); по умолчанию выбрана кодировка UTF-8. Далее в строке имени необходимо указать файл для сохранения данных журнала. Допустимо сразу нажать кнопку «Сохранить», либо задать в строке новое имя файла с расширением .rhv, либо воспользоваться диалогом для указания особого пути размещения файла. При выборе раздела доступен выбор внутренней памяти контроллера, в этом случае данные будут сохранены на SD-карту контроллера СДЗ. Данные, сохраненные на SD-карте контроллера СДЗ, недоступны из ОС ЭВМ.

Файловый диалог

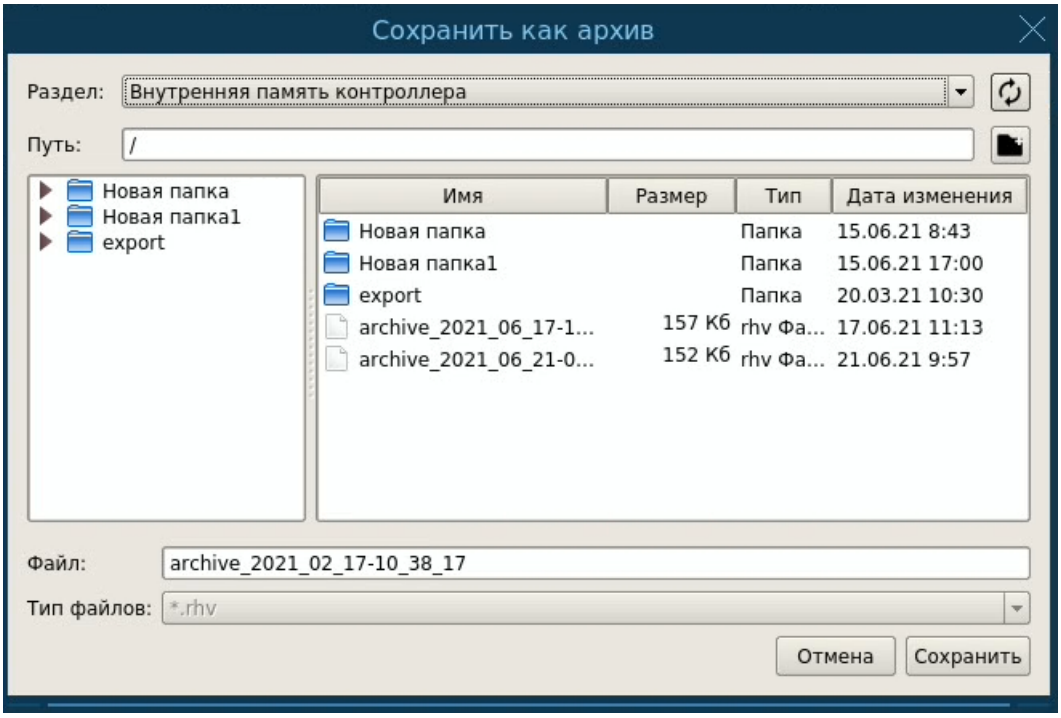


Рис. 10

Архивные журналы могут храниться на контроллере СДЗ (на SD-карте контроллера СДЗ), на внешнем носителе и на жестком диске ЭВМ. Для просмотра архивов событий необходимо в качестве источника событий выбрать «Архивы». При этом в списке архивов для просмотра автоматически отобразятся архивы, ранее сохраненные на SD-карту контроллера СДЗ. При необходимости можно добавить в список архивов нужный архив (или несколько архивов) с внешнего носителя или с жесткого диска ЭВМ. Далее необходимо в списке архивов для просмотра

выбрать один или несколько нужных архивов и нажать кнопку «Считать», расположенную под списком архивов.

Для работы со списком архивов необходимо пользоваться кнопкой-списком «Список», расположенной под списком архивов. Данная кнопка предоставляет возможность управления списком архивов и позволяет выполнить следующие действия:

- добавить архив в список;
- удалить архив из списка;
- выбрать для чтения все архивы;
- снять выделение со всех архивов.

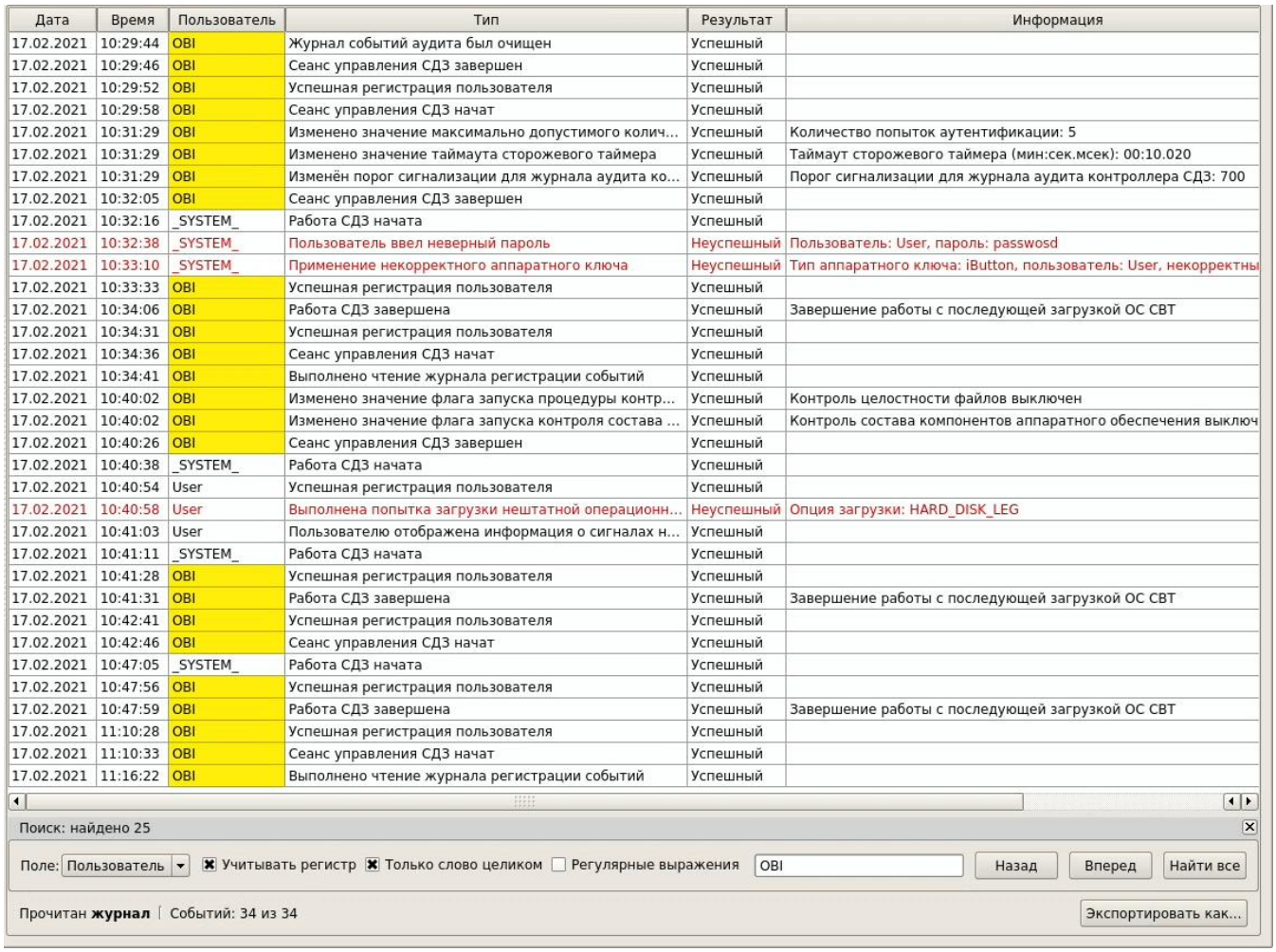
Для выполнения дополнительных действий с архивами необходимо воспользоваться кнопкой-списком «Действие», расположенной под списком архивов. Данная кнопка позволяет выполнить с выделенным в списке архивом следующие действия:

- показать свойства;
- удалить архив;
- копировать архив.

В группе «Фильтры» располагаются элементы управления фильтрацией журнала. Доступны фильтры по времени, по пользователю, типу событий, по результату, а также по информации. Для фильтра по времени нужно выбрать интервал времени, для фильтров по пользователю, типу событий и результату можно указать несколько значений, установив в списке фильтров соответствующие флажки. Для фильтрации по информации можно использовать регулярные выражения. Сразу после изменения значения фильтра в таблице событий будут отображаться события, удовлетворяющие условиям фильтров. Чтобы отменить действие всех фильтров, нужно нажать на кнопку «Очистить фильтры», расположенную под списком фильтров. Если фильтры не заданы, то отобразятся все события журнала контроллера СДЗ.

Чтобы выполнить поиск событий, имеющих определенное время, тип, пользователя, результат и информацию, необходимо в меню «Журнал событий» выбрать пункт «Поиск». Под таблицей с событиями появится окно «Поиск» (рис. 11), в котором можно выбрать поле таблицы, по которому будет осуществляться поиск, указать критерии поиска (учитывать регистр, искать слова только целиком или использовать регулярные выражения) и ввести значение для поиска. Далее необходимо нажать на кнопку «Найти все», все ячейки таблицы с событиями, удовлетворяющими условиям поиска, будут подсвечены. Для перемещения между ячейками можно воспользоваться кнопками «Назад», «Вперед».

Поиск событий в таблице событий



Дата	Время	Пользователь	Тип	Результат	Информация
17.02.2021	10:29:44	OBI	Журнал событий аудита был очищен	Успешный	
17.02.2021	10:29:46	OBI	Сеанс управления СДЗ завершен	Успешный	
17.02.2021	10:29:52	OBI	Успешная регистрация пользователя	Успешный	
17.02.2021	10:29:58	OBI	Сеанс управления СДЗ начат	Успешный	
17.02.2021	10:31:29	OBI	Изменено значение максимально допустимого колич...	Успешный	Количество попыток аутентификации: 5
17.02.2021	10:31:29	OBI	Изменено значение таймаута сторожевого таймера	Успешный	Таймаут сторожевого таймера (мин:сек.мсек): 00:10.020
17.02.2021	10:31:29	OBI	Изменён порог сигнализации для журнала аудита ко...	Успешный	Порог сигнализации для журнала аудита контроллера СДЗ: 700
17.02.2021	10:32:05	OBI	Сеанс управления СДЗ завершен	Успешный	
17.02.2021	10:32:16	_SYSTEM_	Работа СДЗ начата	Успешный	
17.02.2021	10:32:38	_SYSTEM_	Пользователь ввел неверный пароль	Неуспешный	Пользователь: User, пароль: passwosd
17.02.2021	10:33:10	_SYSTEM_	Применение некорректного аппаратного ключа	Неуспешный	Тип аппаратного ключа: iButton, пользователь: User, некорректны
17.02.2021	10:33:33	OBI	Успешная регистрация пользователя	Успешный	
17.02.2021	10:34:06	OBI	Работа СДЗ завершена	Успешный	Завершение работы с последующей загрузкой ОС СВТ
17.02.2021	10:34:31	OBI	Успешная регистрация пользователя	Успешный	
17.02.2021	10:34:36	OBI	Сеанс управления СДЗ начат	Успешный	
17.02.2021	10:34:41	OBI	Выполнено чтение журнала регистрации событий	Успешный	
17.02.2021	10:40:02	OBI	Изменено значение флага запуска процедуры контр...	Успешный	Контроль целостности файлов выключен
17.02.2021	10:40:02	OBI	Изменено значение флага запуска контроля состава ...	Успешный	Контроль состава компонентов аппаратного обеспечения выключ
17.02.2021	10:40:26	OBI	Сеанс управления СДЗ завершен	Успешный	
17.02.2021	10:40:38	_SYSTEM_	Работа СДЗ начата	Успешный	
17.02.2021	10:40:54	User	Успешная регистрация пользователя	Успешный	
17.02.2021	10:40:58	User	Выполнена попытка загрузки нештатной операционн...	Неуспешный	Опция загрузки: HARD_DISK_LEG
17.02.2021	10:41:03	User	Пользователю отображена информация о сигналах н...	Успешный	
17.02.2021	10:41:11	_SYSTEM_	Работа СДЗ начата	Успешный	
17.02.2021	10:41:28	OBI	Успешная регистрация пользователя	Успешный	
17.02.2021	10:41:31	OBI	Работа СДЗ завершена	Успешный	Завершение работы с последующей загрузкой ОС СВТ
17.02.2021	10:42:41	OBI	Успешная регистрация пользователя	Успешный	
17.02.2021	10:42:46	OBI	Сеанс управления СДЗ начат	Успешный	
17.02.2021	10:47:05	_SYSTEM_	Работа СДЗ начата	Успешный	
17.02.2021	10:47:56	OBI	Успешная регистрация пользователя	Успешный	
17.02.2021	10:47:59	OBI	Работа СДЗ завершена	Успешный	Завершение работы с последующей загрузкой ОС СВТ
17.02.2021	11:10:28	OBI	Успешная регистрация пользователя	Успешный	
17.02.2021	11:10:33	OBI	Сеанс управления СДЗ начат	Успешный	
17.02.2021	11:16:22	OBI	Выполнено чтение журнала регистрации событий	Успешный	

Рис. 11

Для удобства просмотра журнала левую часть с фильтрами и архивами можно скрыть, потянув за разделитель и переместив его влево.

Кнопка «Экспортировать как…» предназначена для экспорта выбранных записей журнала в файл в формате XML, HTML или в текстовом формате. При нажатии кнопки открывается файловый диалог с возможностью выбора места сохранения файла и возможностью указания имени файла. Формат экспортируемых данных выбирается в файловом диалоге в поле «Тип файлов»: при выборе типа «*.txt» сохранение происходит в файл в текстовом формате, при выборе типа «*.xml» сохранение происходит в формате XML, при выборе типа «*.html» – в формате HTML. К имени файла автоматически добавляется расширение .xml, .html или .txt.

3.6.4. Вкладка «Управление контроллером»

На вкладке «Управление контроллером» расположены параметры запуска СДЗ и параметры работы функций безопасности СДЗ. Для работы с параметрами в нижней части левой панели расположены кнопки: «Считать», «Сохранить», «Отмена». Соответственно для чтения параметров из внутренней памяти контроллера СДЗ необходимо нажать кнопку «Считать», для сохранения – «Сохранить». Новые значения параметров вступают в силу после перезагрузки ЭВМ. Для отмены измененных, но еще не сохраненных параметров необходимо нажать кнопку «Отменить», при этом во вкладке отобразятся значения параметров, считанные с контроллера СДЗ.

Подробное описание параметров запуска СДЗ приведено в документе ФДШИ.469535.098РЭ «Аппаратно-программный комплекс «Ребус-СДЗ». Руководство по эксплуатации» (раздел 2).

Параметры запуска СДЗ отвечают за инициализацию контроллера СДЗ и запуск ПО СДЗ. К параметрам запуска СДЗ относятся:

- класс и подкласс устройства (класс-код);
- сторожевой таймер;
- консоль;
- блокировка клавиатуры;
- блокировка мыши;
- уровень запуска контроллера;
- способ запуска ПО контроллера СДЗ на ЭВМ;
- способ запуска ПО управления СДЗ;
- звуковая сигнализация;
- запуск UEFI через Legacy.

Параметры работы функций безопасности СДЗ отвечают за работу функций безопасности. К параметрам работы функций безопасности СДЗ относятся:

- число попыток аутентификации;
- режим функционирования СДЗ;
- контроль компонентов СВТ;
- блокировка ЭВМ для пользователя;
- параметры метрики качества аутентификационных данных;
- параметры порогов блокировки и сигнализации для журнала событий контроллера СДЗ.

Параметр «Класс и подкласс устройства (класс-код)» определяет, устройством какого типа представляется в системе контроллер СДЗ. Обычно рекомендуется значение "0x018000", что соответствует типу «устройство хранения». Значение "0xFF0000" («другое устройство PCI») необходимо устанавливать, если ЭВМ не выполняет инициализацию устройств с класс-кодом "0x018000" или если в BIOS ЭВМ есть возможность отключения инициализации устройств с класс-кодом "0x018000". Также возможно задать произвольное значение класс-кода. Рекомендуется задавать стандартные класс-коды например: 0x028000 (сетевое устройство), 0x010400 (RAID-контроллер) и другие. Неверно заданное значение данного параметра чаще всего приводит к невозможности запуска СДЗ при старте ЭВМ.

Рекомендуемое значение данного параметра – «0x018000».

Параметр «Сторожевой таймер» позволяет устанавливать время (порог) срабатывания сторожевого таймера СДЗ. Таймер запускается при включении питания ЭВМ, и если интервал времени от момента включения ЭВМ до момента запуска ПО СДЗ с контроллера превышает заданный порог, автоматически формируется сигнал на аппаратную перезагрузку ЭВМ. При этом в журнале регистрации контроллера СДЗ регистрируются события истечения времени сторожевого таймера. При настройке сторожевого таймера необходимо устанавливать время, немного превышающее время запуска СДЗ, так как слишком малое время сторожевого таймера может привести к постоянным перезагрузкам ЭВМ. Информацию о времени, необходимом для запуска СДЗ, можно получить из поля «Время задержки при последней загрузке». Необходимо учитывать, что время запуска СДЗ может незначительно меняться от запуска к запуску, а также в зависимости от того, происходит включение ЭВМ или перезагрузка.

Значение по умолчанию для данного параметра – 59:59.999, что соответствует максимально возможному значению.

Параметр «Консоль» позволяет задать систему вывода данных на экран, используемую в процессе авторизации пользователя на контроллере СДЗ при запуске ЭВМ. Доступно три вида консолей:

- «Графическая консоль» – основная консоль, применяемая в большинстве случаев;
- «Legacy-консоль» – устаревшая консоль, применяемая на первых ЭВМ с UEFI;
- «Стандартная консоль» – стандартная консоль, применяемая в UEFI, данную консоль необходимо включать на ЭВМ, где не может быть инициализирована графическая консоль.

Рекомендуемое значение данного параметра – «Графическая консоль».

Группа параметров «Блокировка клавиатуры» определяет перечень видов блокировок клавиатуры, используемых в ходе загрузки ЭВМ. Блокировки клавиатуры действуют для непривилегированного пользователя на этапах от завершения аутентификации пользователя до начала загрузки ОС. При их работе нажатия любых клавиш будут блокироваться (игнорироваться, в отдельных случаях – приводить к зависанию или перезагрузке ЭВМ). Доступно несколько видов блокировок («Блокировка 1», «Блокировка 2» и т.п.). Разные блокировки отвечают за блокирование клавиатуры на разных этапах запуска ЭВМ. Блокировки при необходимости могут комбинироваться. Следует учитывать, что отсутствие блокировок клавиатуры может позволить непривилегированному пользователю вмешиваться в процесс загрузки ЭВМ и ОС и ведет к снижению степени защищенности, поэтому отключение блокировок клавиатуры не рекомендуется.

Группа параметров «Блокировка мыши» определяет возможность использования мыши в BIOS ЭВМ. При включении блокировок нажатия на кнопки мыши и попытки перемещения курсора для непривилегированного пользователя будут игнорироваться. Блокировки при необходимости могут комбинироваться. Рекомендуется включать блокировки мыши.

Примечание. Если отключены все блокировки клавиатуры, то блокировки мыши отключаются автоматически, а настройки параметров блокировки мыши игнорируются.

Группа параметров «Уровень запуска контроллера» определяет момент запуска ПО контроллера СДЗ. Чем меньшее значение параметра «Уровень запуска» установлено, тем позже будет запускаться ПО контроллера СДЗ. Включение параметра «Ранний старт» позволяет запускать ПО контроллера СДЗ сразу при инициализации контроллера СДЗ, отключение приводит к тому, что контроллер СДЗ инициализируется, но запуск ПО контроллера СДЗ откладывается на поздние стадии запуска ЭВМ.

Рекомендуемое значение параметра «Ранний старт» – «Включено».

Рекомендуемое значение параметра «Уровень запуска» – «16».

Параметр «Способ запуска ПО контроллера СДЗ на ЭВМ» определяет момент запуска ПО контроллера СДЗ. Параметр может принимать следующие значения:

- «Запуск ПО как сервиса». При таком значении параметра ПО контроллера СДЗ запускается автоматически, как сервис, сразу после его загрузки. Запуск ПО контроллера СДЗ как сервиса является более ранним и предпочтительным для большей части материнских плат;
- «Запуск ПО как драйвера». При таком значении параметра ПО контроллера СДЗ регистрируется в UEFI как драйвер и запускается при обнаружении аппаратной части СДЗ.

В некоторых случаях установка способа запуска ПО контроллера СДЗ на значение «Запуск ПО как сервиса» может привести к тому, что в момент появления на экране запроса на ввод идентификатора и пароля клавиатура ЭВМ может быть еще не проинициализирована, при этом она может не работать либо работать некорректно (например, при нажатии на одну кнопку может вводиться сразу много символов). Проблему с работой клавиатуры можно попытаться исправить, переключив способ запуска ПО контроллера СДЗ на значение «Запуск ПО как драйвера».

Рекомендуемое значение данного параметра – «Запуск ПО как сервиса».

Параметр «Способ запуска ПО управления СДЗ» определяет момент запуска ПО управления СДЗ с SD-карты контроллера СДЗ. Данный параметр не влияет на запуск ПО управления СДЗ с CD-диска. Параметр может принимать следующие значения:

- «Поздний запуск». При такой настройке ПО управления СДЗ запускается непосредственно вместо рабочей ОС ЭВМ. Практически на всех материнских платах на этой стадии среда ЭВМ готова для работы ПО управления СДЗ и среды его функционирования. Однако поздний запуск может использоваться только для ЭВМ с установленной ОС. Если на ЭВМ не установлена ОС, поздний запуск ПО управления СДЗ с SD-карты будет невозможен;
- «Ранний запуск». При такой настройке ПО управления СДЗ запускается сразу после выполнения аутентификации и контроля компонентов средства вычислительной техники. Ранний запуск ПО управления СДЗ происходит до завершения инициализации ЭВМ, из-за чего существует вероятность, что еще не все механизмы, необходимые для работы ПО управления СДЗ, были инициализированы; это может приводить к невозможности запуска ПО управления

СДЗ. Ранний запуск ПО управления может использоваться независимо от наличия на ЭВМ установленной ОС и от того, какой загрузчик ОС (UEFI или Legacy) используется.

Если в процессе настройки контроллера СДЗ будет установлено неверное значение параметра «Способ запуска ПО управления СДЗ», и ПО управления СДЗ не запускается, то можно изменить параметр, запустив ПО управления СДЗ с CD-диска.

Рекомендуемое значение данного параметра – «Ранний запуск».

Параметр «Звуковая сигнализация» определяет необходимость осуществления звуковой сигнализации при неверном вводе идентификационных или аутентификационных данных в ходе регистрации пользователя на контроллере СДЗ. На ЭВМ с UEFI BIOS среда UEFI может не поддерживать звуковые устройства, что может приводить к блокировке или перезагрузке ЭВМ при попытках звуковой сигнализации, в таких случаях звуковую сигнализацию необходимо отключить.

Рекомендуемое значение данного параметра – «Включено».

Параметр «Запуск UEFI через Legacy» определяет порядок запуска UEFI-кода СДЗ. В большинстве случаев на ЭВМ с UEFI BIOS инициализация устройств (в том числе и контроллера СДЗ) выполняется через подсистему UEFI, но на некоторых материнских платах, несмотря на наличие поддержки UEFI, инициализация устройств выполняется через подсистему Legacy. Данный параметр позволяет осуществлять запуск контроллера в UEFI-режиме в процессе инициализации через подсистему Legacy. Отключать данную настройку необходимо только в том случае, если BIOS материнской платы пытается инициализировать контроллер дважды – в UEFI-режиме и в Legacy-режиме, что приводит к блокировке работы контроллера.

Рекомендуемое значение данного параметра – «Включено».

Параметр «Число попыток аутентификации» определяет количество неуспешных попыток аутентификации пользователя до выполнения блокировки ЭВМ для пользователя. Необходимо помнить, что увеличение количества попыток аутентификации пользователя до блокировки повышает вероятность несанкционированного доступа. Значение по умолчанию данного параметра – «3 попытки».

Группа параметров «Контроль компонентов СВТ» включает в себя следующие параметры:

- «Контроль целостности файлов»;
- «Контроль состава компонентов аппаратного обеспечения».

Данные параметры управляют запуском контроля целостности файлов и контроля состава компонентов аппаратного обеспечения при старте ЭВМ. Если данные параметры отключены, то соответствующие механизмы контроля не запускаются. Для работы контроля компонентов СВТ недостаточно включить параметры запуска в управлении контроллером, необходимо выполнить дополнительную настройку параметров соответствующих приложений. Управление контролем целостности файлов выполняется при помощи средства контроля целостности файлов. Управление контролем состава компонентов аппаратного обеспечения выполняется при помощи средства контроля состава компонентов аппаратного обеспечения.

Рекомендуемое значение для каждого параметра – «Включено».

Группа параметров «Блокировка ЭВМ для пользователя» включает в себя следующие параметры:

- Блокировать ЭВМ при обнаружении нарушения целостности UEFI-модулей SD-карты;
- Блокировать ЭВМ в случае обнаружения попытки загрузки нештатной ОС.

При запуске СДЗ проводится контроль целостности модулей СДЗ. Модули, отвечающие за контроль целостности файлов и контроль состава компонентов аппаратного обеспечения, располагаются на SD-карте контроллера СДЗ. С помощью параметра «Блокировать ЭВМ при обнаружении нарушения целостности UEFI-модулей SD-карты» администратор СДЗ может включить или отключить блокировку ЭВМ для пользователя в случае выявления нарушения целостности данных модулей. Рекомендуемое значение параметра – «Включено».

СДЗ при входе в систему пользователя блокирует загрузку нештатной ОС. Если параметр «Блокировать ЭВМ в случае обнаружения попытки загрузки нештатной ОС» установлен, то при выявлении попытки загрузки нештатной ОС ЭВМ будет заблокирована для пользователя; данная блокировка сохранится после перезагрузки ОС. Если блокировка будет выключена, то либо на

ЭВМ будет принудительно загружена штатная ОС, либо пользователь сможет загрузить штатную ОС после устранения причин блокировки. Рекомендуемое значение параметра – «Включено».

Параметр «Режим функционирования СДЗ» определяет, в каком режиме будет работать СДЗ. Можно установить один из двух представленных режимов:

- автономный режим;
- режим совместимости.

Если включен автономный режим, то механизмы работы с внешними средствами защиты информации будут заблокированы, при этом безопасность СДЗ будет выше, так как злоумышленник не сможет получить доступ к СДЗ при помощи интерфейса взаимодействия контроллера СДЗ. В автономном режиме, ПО управления СДЗ, запущенное с CD-диска, не сможет получить доступ к контроллеру СДЗ.

Если включен режим совместимости, то СДЗ сможет взаимодействовать со средствами защиты уровня ОС, совместимыми с СДЗ. Если на ЭВМ используются средства защиты уровня ОС и/или на ЭВМ используется ПО управления СДЗ, запускаемое с CD-диска, то необходимо включить режим совместимости.

Рекомендуемое значение данного параметра – «Режим совместимости».

Группа параметров «Параметры метрики качества аутентификационных данных» определяет необходимые алфавит и длину аутентификационных данных, а также поведение СДЗ при попытке задать аутентификационные данные, не соответствующие заданной метрике качества.

В данной группе параметров выполняется управление следующими параметрами генерации и проверки метрики аутентификационных данных:

- алфавит аутентификационных данных;
- длина аутентификационных данных.

Параметры метрики качества применяются для паролей пользователей, ПИН-кодов и секретов аппаратных ключей.

Рекомендуемые значения для каждого вида аутентификационных данных – алфавит «A-Z,a-z,0-9», длина 8 символов.

Если включен параметр «Проверять метрику качества аутентификационных данных», то при сохранении некорректных аутентификационных данных выводится сообщение с предупреждением. Если дополнительно включен параметр «Блокировать сохранение некорректных аутентификационных данных», то при сохранении некорректных (не соответствующих метрике качества) аутентификационных данных выводится сообщение с уведомлением и блокируется сохранение некорректных данных.

Если у учетной записи пользователя параметру «Ключевые данные» установлено значение «Использовать ключевые данные контроллера», то будет производиться проверка метрики только для пароля.

ВНИМАНИЕ! При смене метрики качества паролей необходимо будет менять все неподходящие аутентификационные данные существующим пользователям и переформировывать индивидуальные ключевые данные пользователей.

Рекомендуемое значение данных параметров – «Включено».

Группа параметров «Параметры порогов блокировки и сигнализации для журнала событий контроллера СДЗ» определяют реакцию СДЗ на переполнение журнала событий контроллера СДЗ.

Максимальный размер журнала событий СДЗ составляет 766 событий. При переполнении журнала самые старые события удаляются, а новые записываются на их место, следовательно, при переполнении журнала событий старые события будут удаляться.

Параметр «Порог сигнализации» определяет количество событий в журнале событий СДЗ, при превышении которого СДЗ будет выдавать соответствующее сообщение администратору СДЗ при помощи расширенной сигнализации СДЗ. Если порогу сигнализации присвоено значение 0, то сигнализация будет отключена. Максимальное значение порога сигнализации – 766 событий.

Параметр «Порог блокировки» определяет количество событий в журнале событий СДЗ, при превышении которого СДЗ заблокирует ЭВМ для пользователя. Если порогу блокировки

присвоено значение 0, то блокировка будет отключена. Максимальное значение порога блокировки – 766 событий.

Не рекомендуется выставлять в качестве пороговых слишком малые значения, так как это может привести к тому, что администратор СДЗ не успеет вовремя обслужить контроллер (сохранить и очистить журнал регистрации контроллера СДЗ). Значение порога сигнализации должно быть меньше значения порога блокировки для того, чтобы сигнализация (оповещение) происходила раньше блокировки.

Рекомендуемое значение данных параметров – «Включено» (значение, отличное от 0).

3.6.5. Вкладка «Аппаратные ключи»

Вкладка «Аппаратные ключи» (рис. 12) служит для подготовки к работе аппаратных ключей (ключей iButton и USB-ключей), управления режимами работы аппаратных ключей, настройки контроллера для работы с аппаратными ключами, записи данных пользователя в аппаратные ключи.

Примечание. Для работы с ключами iButton необходимо подключить считыватель iButton к контроллеру СДЗ до запуска ЭВМ.

Вкладка «Аппаратные ключи»

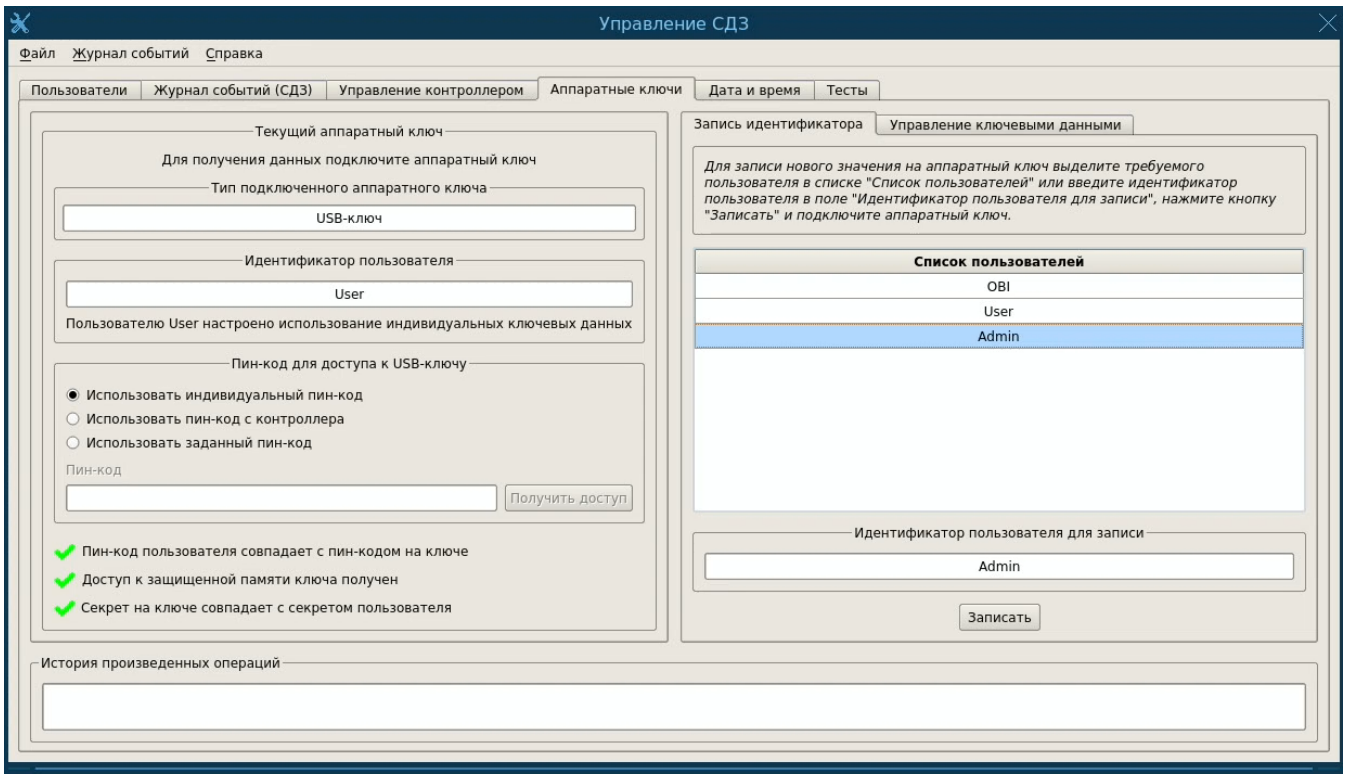


Рис. 12

На правой панели вкладки «Аппаратные ключи» расположена вкладка «Управление ключевыми данными» (рис. 13), при помощи нее производится настройка контроллера СДЗ для работы с аппаратными ключами, а также инициализация и настройка USB-ключей.

Для применения аппаратных ключей необходимо разрешить их использование в группе «Использование аппаратных ключей» на вкладе «Управление ключевыми данными».

Вкладка «Управление ключевыми данными»

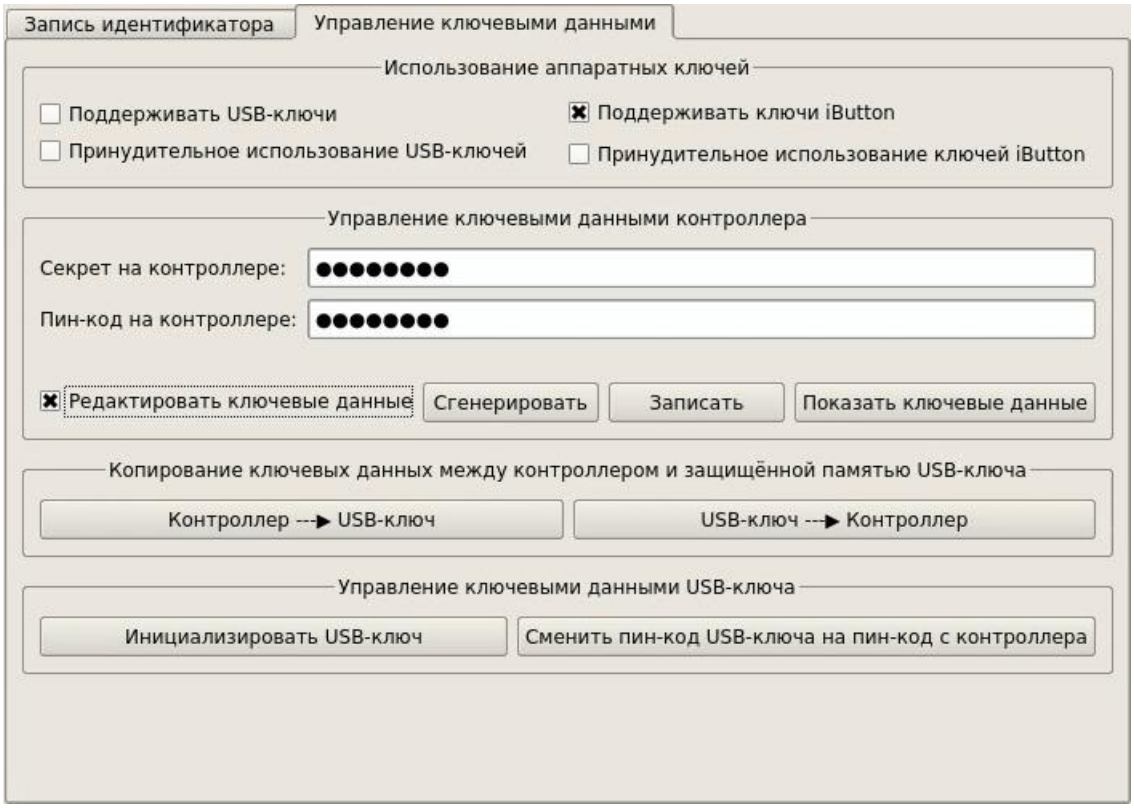


Рис. 13

Для разрешения работы с USB-ключами необходимо включить параметр «Поддерживать USB-ключи». Если поддержка USB-ключей не включена, то при отображении на экране ЭВМ запроса на ввод идентификатора пользователя механизмы работы с USB-ключами работать не будут.

Для разрешения работы с ключами iButton необходимо включить параметр «Поддерживать ключи iButton». Если поддержка ключей iButton не включена, то при отображении на экране ЭВМ запроса на ввод идентификатора пользователя механизмы работы с ключами iButton работать не будут.

В СДЗ аутентификация пользователя проводится по паролю либо по паролю и аппаратному ключу. Если в СДЗ включено принудительное использование аппаратных ключей, то пользователь для идентификации и аутентификации должен использовать аппаратный ключ и пароль.

Для включения принудительного использования аппаратных ключей для идентификации и двухфакторной аутентификации необходимо активировать параметры «Принудительное использование USB-ключей» и/или «Принудительное использование ключей iButton». При этом необходимо иметь в наличии аппаратный ключ iButton и/или USB-ключ с учетной записью администратора.

В группе «Управление ключевыми данными контроллера» задаются общие данные для работы с аппаратными ключами контроллера («Секрет на контроллере» и «ПИН-код на контроллере»). Эти данные используются при формировании ключевых данных для пользователей, для которых настроено использование ключевых данных контроллера.

Перед использованием USB-ключей их необходимо инициализировать. В процессе инициализации происходят формирование внутренней структуры данных и установка ПИН-кода (заданного в поле «ПИН-код на контроллере») для доступа к USB-ключу. Поэтому перед инициализацией необходимо убедиться, что администратор правильно помнит ПИН-код на контроллере (с помощью кнопки «Показать ключевые данные»). Инициализация USB-ключа

производится нажатием на кнопку «Инициализировать USB-ключ». После инициализации на USB-ключ можно записывать учетные данные пользователя.

Для подготовки ключа iButton достаточно записать на него аутентификационные данные пользователя. Данный ключ iButton будет работать на всех ЭВМ, где установлен контроллер СДЗ и в настройках СДЗ присутствуют аналогичные аутентификационные данные пользователя.

Для подготовки USB-ключа необходимо получить к нему доступ по заданному ПИН-коду (после инициализации на USB-ключе установлен ПИН-код контроллера). Способ задания ПИН-кода ключа зависит от того, какого типа учетная запись на него записывается: учетная запись с индивидуальными ключевыми данными или учетная запись с ключевыми данными контроллера. Если для учетной записи пользователя настроено использование индивидуальных ключевых данных, то ключевые данные задаются в параметрах учетной записи пользователя. Если для учетной записи пользователя настроено использование ключевых данных контроллера, то необходимо задать ключевые данные в группе «Управление ключевыми данными контроллера».

При использовании ключевых данных контроллера необходимо, чтобы ПИН-код ключа совпадал с ПИН-кодом контроллера. Для этого необходимо подключить USB-ключ к ЭВМ и нажать кнопку «Сменить ПИН-код USB-ключа на ПИН-код с контроллера».

При использовании общих ключевых данных контроллера ПИН-код и ключевые данные привязывают USB-ключ к конкретному контроллеру СДЗ. Для того чтобы USB-ключ мог использоваться на нескольких ЭВМ с установленным СДЗ, необходимо, чтобы на всех этих ЭВМ были установлены одинаковые настройки ключевых данных контроллера и ПИН-код USB-ключей.

Помимо хранения учетных данных пользователя, на USB-ключе (в защищенной памяти USB-ключа) можно хранить и переносить на СДЗ других ЭВМ ключевые данные контроллера СДЗ. Необходимо понимать, что данные в защищенной памяти USB-ключа – это копия ключевых данных контроллера, а не учетные данные пользователя. Ключевые данные контроллера применяются для настройки контроллеров СДЗ на нескольких ЭВМ с целью обеспечения возможности использования на них одних и тех же аппаратных ключей.

В группе «Управление ключевыми данными контроллера» отображаются ключевые данные, хранящиеся на контроллере, а также кнопки управления редактированием данных и их отображения. Для отображения данных необходимо нажать кнопку «Показать ключевые данные». Для включения возможности редактирования данных необходимо установить галочку «Редактировать данные». Чтобы сохранить ключевые данные на контроллер СДЗ, необходимо нажать кнопку «Записать».

В группе «Копирование ключевых данных между контроллером и защищенной памятью USB-ключа» можно копировать ключевые данные из контроллера в USB-ключ нажатием на кнопку «Контроллер ─►─ USB-ключ» и из USB-ключа на контроллер нажатием на кнопку «USB-ключ ─►─ Контроллер». Данный механизм помогает администратору СДЗ распространить ключевые данные на несколько ЭВМ и этим обеспечить возможность регистрации пользователей на нескольких ЭВМ, используя один USB-ключ.

Запись учетных данных пользователя на аппаратные ключи производится во вкладке «Запись идентификатора». Для записи ключа iButton необходимо на вкладке «Запись идентификатора» выбрать требуемого пользователя в списке «Список пользователей» или ввести идентификатор пользователя в поле «Идентификатор пользователя для записи», нажать кнопку «Записать» и приложить iButton к считывателю. Для записи USB-ключа необходимо предварительно подключить USB-ключ к ЭВМ, при необходимости ввести ПИН-код ключа, убедиться, что доступ к ключу получен, после чего выбрать требуемого пользователя в списке «Список пользователей» или ввести идентификатор пользователя в поле «Идентификатор пользователя для записи», нажать кнопку «Записать». При записи учетных данных пользователя, которого нет в списке, используются ключевые данные контроллера.

В группе «Текущий аппаратный ключ» отображаются данные, записанные на текущем подключенном аппаратном ключе. При использовании ключей iButton для получения данных с ключа достаточно подключить ключ к считывателю. При использовании USB-ключей для получения доступа к секрету, хранящемуся в защищенной памяти, необходимо, чтобы ПИН-код

пользователя на ключе совпадал с ПИН-кодом пользователя, сохраненным на контроллере. Если ПИН-код в аутентификационных данных пользователя или ПИН-код контроллера не совпадает с ПИН-кодом на ключе, администратор СДЗ должен будет ввести ПИН-код ключа с клавиатуры или выбрать другой тип ПИН-кода (индивидуальный или с контроллера).

3.6.6. Вкладка «Дата и время»

Во вкладке «Дата и время» (рис. 14) администратор СДЗ может просмотреть текущие сведения по дате и времени, настроить время на ЭВМ и на контроллере СДЗ, выполнить синхронизацию времени между ЭВМ и контроллером, а также выполнить калибровку часов контроллера СДЗ.

Вкладка «Дата и время»

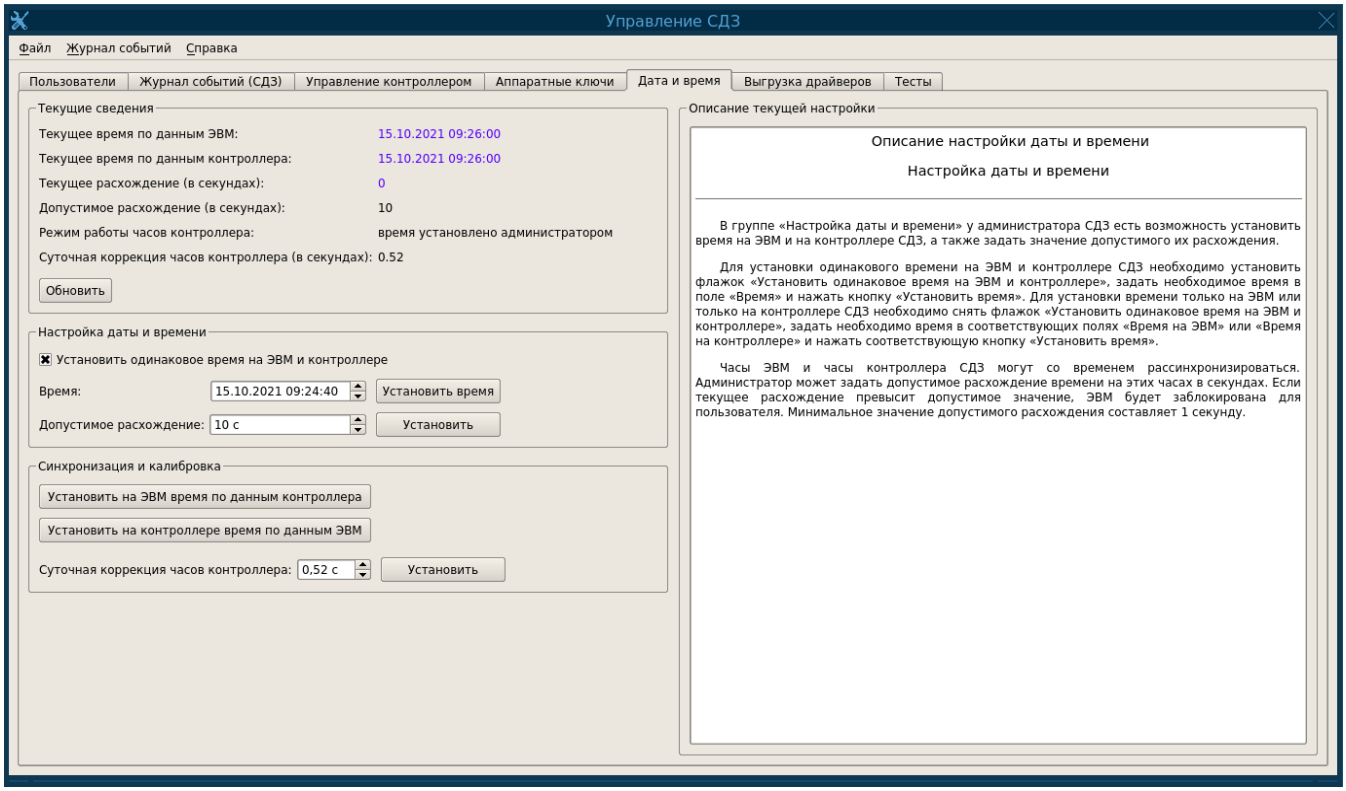


Рис. 14

В группе «Текущие сведения» отображается следующая информация:
- текущее время по данным ЭВМ;
- текущее время по данным контроллера СДЗ;
- текущее расхождение времени на ЭВМ и времени на контроллере СДЗ (в секундах);
- допустимое расхождение времени на ЭВМ и времени на контроллере СДЗ (в секундах);
- режим работы часов контроллера СДЗ;
- суточная коррекция часов контроллера СДЗ (в секундах).

В поле «Режим работы часов контроллера» отображается информация о том, как было установлено время на часах контроллера СДЗ. Режим «время установлено администратором» включается, когда администратор устанавливает время в контроллере СДЗ. В этом случае часы контроллера идут независимо от часов ЭВМ, синхронизация времени по данным ЭВМ не осуществляется. Режим «время восстановлено по времени ЭВМ» автоматически включается после установки контроллера СДЗ в ЭВМ (так как время на контроллере СДЗ в этом случае не установлено). В этом режиме время на контроллере СДЗ автоматически восстанавливается по времени на ЭВМ в ходе аутентификации пользователя.

В группе «Настройка даты и времени» у администратора СДЗ есть возможность установить время на ЭВМ и на контроллере СДЗ, а также задать значение допустимого их расхождения.

Для установки одинакового времени на ЭВМ и контроллере СДЗ необходимо установить флажок «Установить одинаковое время на ЭВМ и контроллере», задать необходимое время в поле «Время» и нажать кнопку «Установить время». Для установки времени только на ЭВМ или только на контроллере СДЗ необходимо снять флажок «Установить одинаковое время на ЭВМ и контроллере», задать время в соответствующих полях «Время на ЭВМ» или «Время на контроллере» и нажать соответствующую кнопку «Установить время».

Часы ЭВМ и часы контроллера СДЗ могут со временем рассинхронизироваться. Администратор может задать допустимое расхождение времени на этих часах в секундах. Если текущее расхождение превысит допустимое значение, ЭВМ будет заблокирована для пользователя. Минимальное значение допустимого расхождения составляет 1 секунду.

В группе «Синхронизация и калибровка» при нажатии кнопки «Установить на ЭВМ время по данным контроллера» или кнопки «Установить на контроллере время по данным ЭВМ» происходит синхронизация часов ЭВМ и контроллера СДЗ в соответствующем направлении. Если в рабочей ОС ЭВМ осуществляется синхронизация времени по внешнему доверенному источнику, то рекомендуется предварительно синхронизировать время в ОС, а потом синхронизировать время контроллера СДЗ по данным времени на ЭВМ.

Если со временем расхождение между часами ЭВМ и контроллера СДЗ увеличивается, то следует настроить калибровку часов контроллера СДЗ. Для этого в группе «Синхронизация и калибровка» необходимо в поле «Коррекция для часов контроллера» установить значение суточной коррекции (в секундах за сутки) и нажать кнопку «Установить». После этого ход часов контроллера СДЗ будет автоматически корректироваться в соответствии с установленным значением.

3.6.7. Вкладка «Выгрузка драйверов»

Для контроля целостности файлов в СДЗ используются драйвера файловых систем NTFS и EXT для среды UEFI. Необходимые драйвера файловых систем входят в состав СДЗ. Однако часто производители материнских плат встраивают драйвера файловых систем в UEFI BIOS. В случае конфликта при работе с драйверами файловых систем у пользователя есть возможность выполнить выгрузку системных драйверов.

Информацию о том, нужно ли выгружать какие-либо драйвера на данной конкретной ЭВМ и какие конкретно, необходимо получить от поставщика оборудования.

Не следует выполнять выгрузку драйвера файловой системы FAT, без него не будет загружаться рабочая ОС ЭВМ и ПО управления СДЗ.

Если в СДЗ ошибочно была настроена выгрузка драйверов, без которых ЭВМ не может запуститься, можно попытаться переставить контроллер СДЗ в другую ЭВМ (с другой моделью материнской платы), где будет другой набор драйверов, и механизм выгрузки драйверов не будет выгружать необходимые драйвера.

3.6.8. Вкладка «Тесты»

При включении ЭВМ СДЗ выполняет самотестирование (проводит набор тестов) для определения возможности выполнения своих функций. В журнал при этом заносится запись о результате прохождения того или иного теста и результат самотестирования. Если в процессе самотестирования обнаружены неисправности и сбои, ЭВМ в нижней части экрана идентификации и аутентификации выводит сообщение о статусе прохождения самотестирования.

Вкладка «Тесты» (рис. 15) предназначена для просмотра результатов самотестирования и для управления тестами, которые выполняются по запросу.

Вкладка «Тесты»

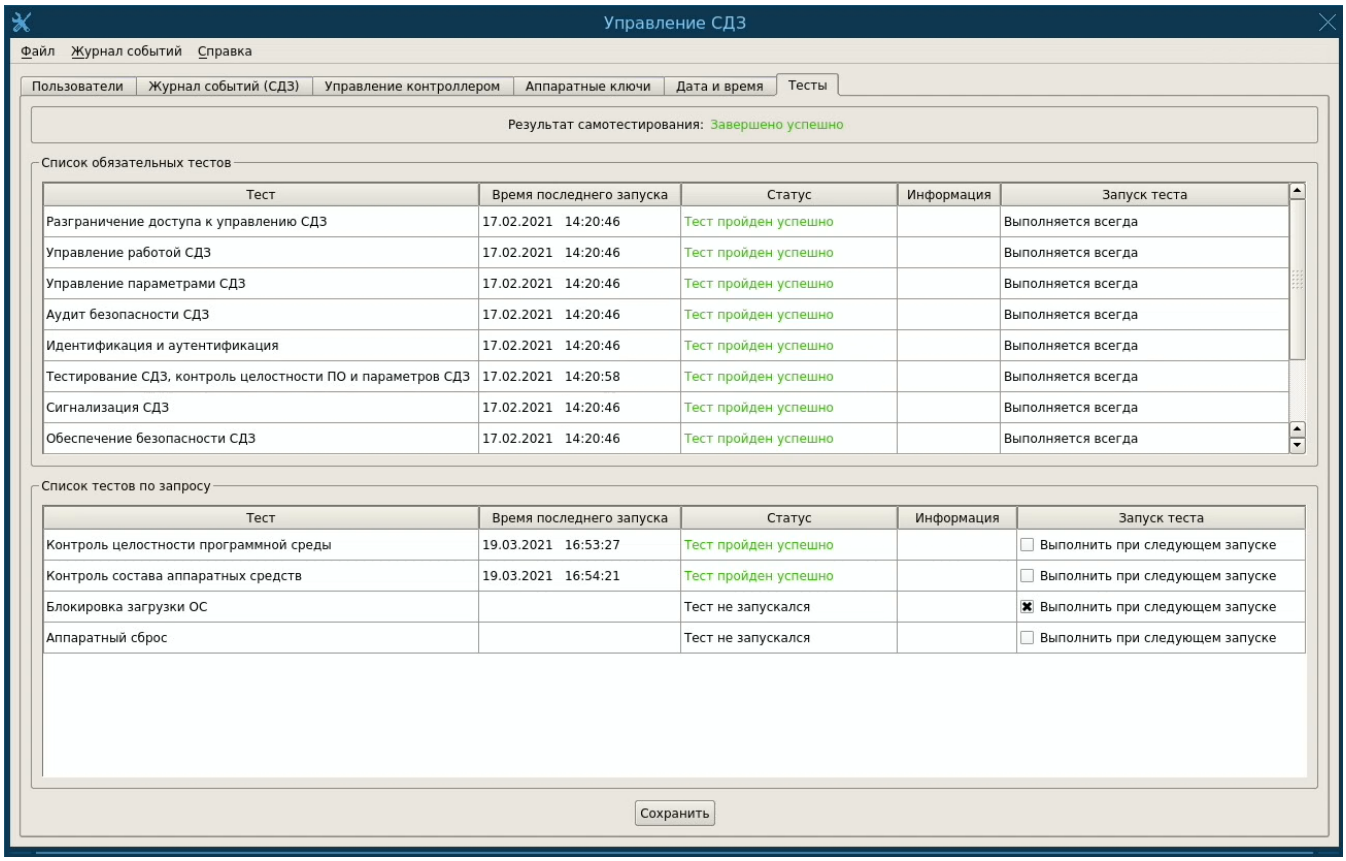


Рис. 15

На вкладке содержатся следующие элементы:

- таблица «Список обязательных тестов» с тестами, которые выполняются всегда и не подлежат настройке. Отображает статусы выполнения тестов, время последнего запуска, а также дополнительную информацию о выполненных тестах. Для каждого такого теста в графе «Запуск теста» отображается «Выполняется всегда»;
- таблица «Список тестов по запросу» с тестами, запуск которых управляется администратором СДЗ. Для запуска конкретного теста необходимо поставить флажок на переключателе в графе «Запуск теста». Для некоторых тестов отображается иконка «⍰», при наведении на которую появится всплывающее окно с вспомогательной информацией для теста;
- кнопка «Сохранить», предназначенная для сохранения установленных параметров запуска тестов.

3.7. Контроль целостности файлов

3.7.1. Общая информация

Механизм контроля целостности файлов предоставляет возможность контролировать целостность файлов на жестком диске ЭВМ и выполняет следующие функции:

- создание и модификация списка контролируемых файлов;
- автоматическая проверка целостности контролируемых файлов до загрузки операционной системы;
- просмотр журнала контроля целостности файлов.

Под контролем целостности при этом понимается проверка соответствия контрольных сумм файлов данным, сохраненным в эталоне.

Примечание. Для использования механизма контроля целостности файлов он должен быть включен в средстве управления СДЗ (описание приведено в 3.6.4).

Средство контроля целостности файлов предназначено для настройки механизма контроля целостности файлов. Для запуска данного средства необходимо в главном меню ПО управления СДЗ выбрать пункт «Контроль целостности файлов». Для получения доступа к данным необходимо пройти аутентификацию администратором СДЗ.

Непосредственно контроль целостности файлов, эталоны для которых были предварительно сохранены, осуществляется СДЗ автоматически, после идентификации и аутентификации пользователя и до загрузки операционной системы.

3.7.2. Настройка параметров

Для управления параметрами контроля целостности файлов необходимо использовать вкладку «Параметры» (рис. 16). В ней доступна настройка параметров самотестирования, журналирования и собственно контроля целостности.

Вкладка «Параметры»

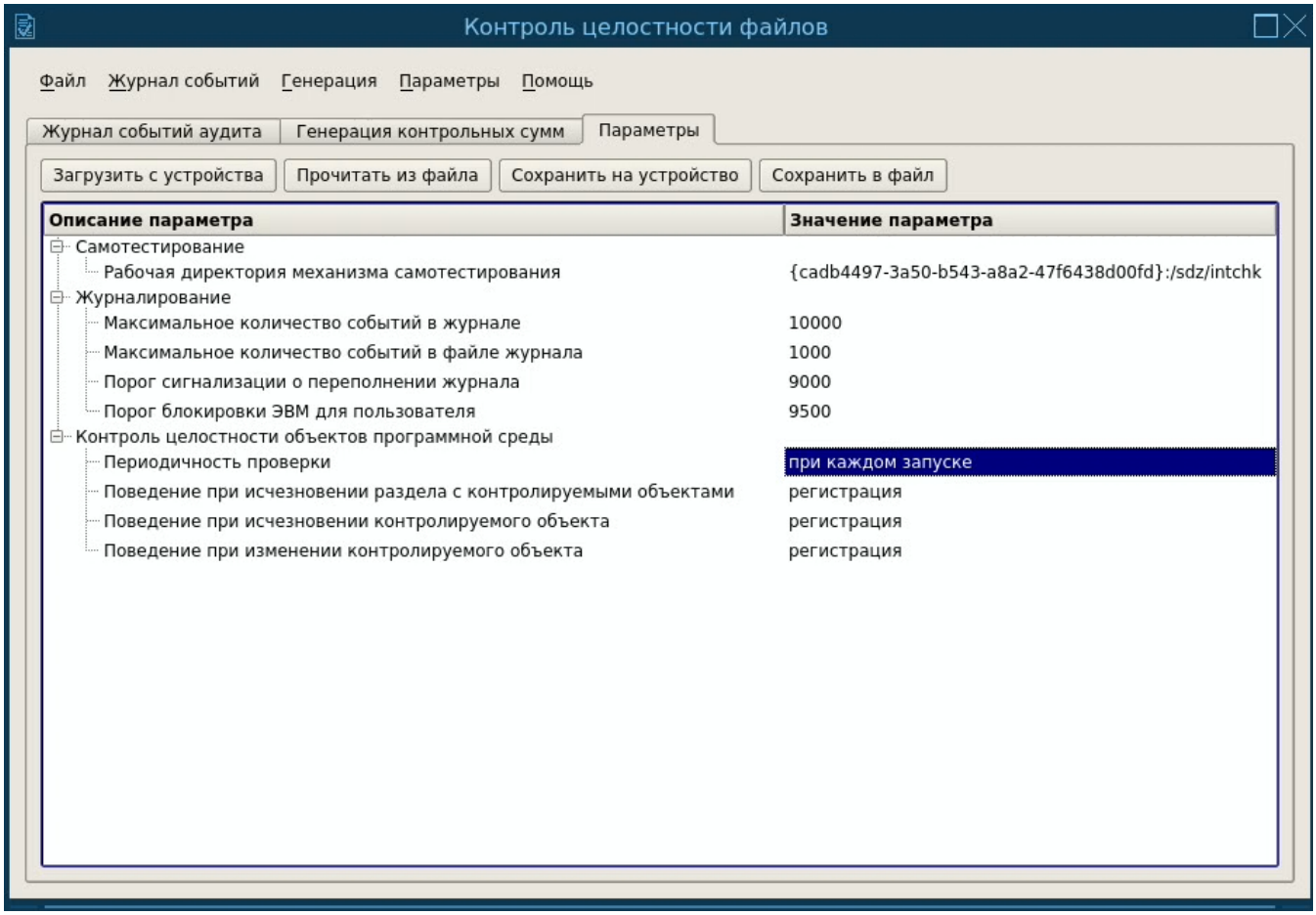


Рис. 16

Параметр «Рабочая директория механизма самотестирования» определяет директорию на одном из разделов ЭВМ, где будут сохранены данные для выполнения самотестирования контроля целостности файлов (программной среды).

Для настройки журналирования доступны следующие параметры:

- «Максимальное количество событий в журнале»;
- «Максимальное количество событий в файле журнала»;
- «Порог сигнализации о переполнении журнала»;

- «Порог блокировки ЭВМ для пользователя».

Журнал контроля целостности файлов хранится в виде нескольких файлов. Параметр «Максимальное количество событий в журнале» определяет максимальное количество событий во всем журнале контроля целостности файлов (во всех его файлах). Параметр «Максимальное количество событий в файле журнала» определяет максимальное количество событий в одном файле журнала. При заполнении одного файла журнала до указанного в параметре значения начинается запись в следующий файл. При достижении размером журналом значения, указанного в параметре «Максимальное количество событий в журнале», самый старый файл журнала удаляется.

Максимальное количество событий в журнале составляет 100000 записей. Журнал разбивается на несколько файлов. Рекомендуется устанавливать максимальное количество событий в файле журнала равным 1000. Данная рекомендация обусловлена тем, что при начале работы контроля целостности файлов выполняется проверка целостности текущего файла журнала. Если задано значение максимального количества событий в файле журнала более 1000, то чтение и контроль целостности текущего файла журнала занимает значительное время и увеличивает общее время запуска СДЗ. Установка значения менее 1000 не дает значительного прироста в скорости запуска СДЗ, но при этом приводит к созданию излишне большого количества файлов.

Параметр «Порог сигнализации о переполнении журнала» определяет количество событий в журнале, после которого будет выполняться сигнализация о переполнении журнала регистрации.

Параметр «Порог блокировки ЭВМ для пользователя» определяет количество событий в журнале, после которого ЭВМ будет блокироваться для пользователя.

Для настройки контроля целостности доступны следующие параметры:

- «Периодичность проверки»;
- «Поведение при исчезновении раздела с контролируемыми объектами»;
- «Поведение при исчезновении контролируемого объекта»;
- «Поведение при изменении контролируемого объекта».

Параметр «Периодичность проверки» определяет период проведения проверок.

Параметр «Поведение при исчезновении раздела с контролируемыми объектами» определяет поведение СДЗ при выявлении исчезновения раздела с контролируемыми объектами.

Параметр «Поведение при исчезновении контролируемого объекта» определяет поведение СДЗ при исчезновении контролируемого объекта.

Параметр «Поведение при изменении контролируемого объекта» определяет поведение СДЗ при выявлении изменения контролируемого объекта.

3.7.3. Подготовка эталона

Для формирования эталона контролируемых файлов необходимо выполнить следующую последовательность действий:

1) запустить средство контроля целостности файлов;
2) перейти на вкладку «Генерация контрольных сумм» (рис. 17);
3) выбрать раздел, файлы в котором необходимо контролировать;
4) добавить в список объекты (конкретные файлы или каталоги со всеми файлами и подкаталогами) для контроля, выбрав их и нажав кнопку ⊕ со всплывающей подсказкой «Добавить выделенные объекты для контроля»;
5) сгенерировать контрольные суммы для объектов данного раздела, нажав кнопку «Применить»;
6) повторить действия, описанные в перечислениях 3) – 5), для других разделов при необходимости.

Вкладка «Генерация контрольных сумм»

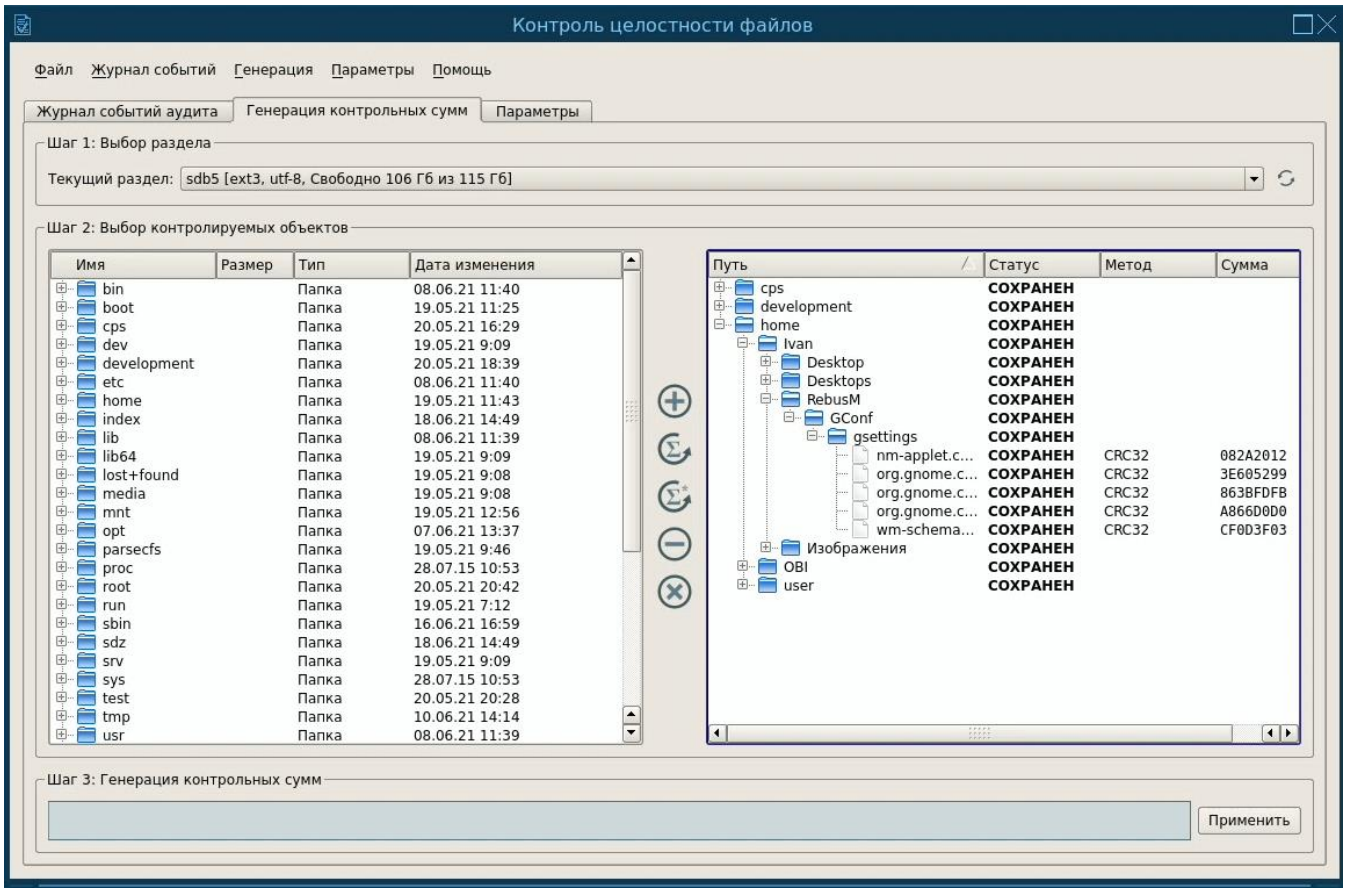


Рис. 17

Для управления списком контролируемых файлов доступны следующие кнопки:

-  – добавить выбранные объекты файловой системы в перечень контролируемых;
-  – очистить перечень контролируемых объектов выбранного раздела;
-  – удалить выделенные объекты из перечня контролируемых объектов;
-  – пересчитать контрольные суммы всех контролируемых объектов;
-  – пересчитать контрольные суммы выделенных объектов.

3.7.4. Журнал событий

Просмотр результатов контроля целостности файлов возможен на вкладке «Журнал событий аудита».

Записи данных журнала содержат следующие элементы:

- дата регистрации события;
- время регистрации события;
- пользователь;
- тип события;
- результат события;
- дополнительная информация.

Регистрируемые типы событий приводятся в разделе 4 документа ФДШИ.04198-01 31 01 «Описание применения».

Вкладка «Журнал событий» предназначена для просмотра администратором СДЗ журнала контроля целостности файлов, а также для работы с архивами журналов. В левой части вкладки расположены элементы управления источниками событий и фильтрами, в правой – таблица с событиями. В группе «Источники событий» можно выбрать источники событий – журнал контроля целостности файлов или архивы.

Для просмотра текущего журнала событий необходимо в качестве источника событий выбрать «Журнал контроля целостности файлов», и нажать кнопку «Считать». Журнал будет считан с контроллера СДЗ и отображен в таблице с событиями.

Кнопка-список «Действие» позволяет администратору СДЗ выполнить следующие действия с журналом:

- просмотр свойств журнала;
- очистка журнала;
- проверка целостности журнала;
- сохранение журнала событий в качестве архива.

Действие «Показать свойства» позволяет просмотреть свойства текущего журнала, такие как время создания (первого события), размер журнала.

Действие «Очистить журнал» используется для очистки журнала и регистрации в журнале события очистки журнала. Перед очисткой журнала будет предложено сохранить его как архив. В ходе очистки журнала события будут полностью удалены без возможности восстановления. Факт очистки журнала регистрируется в нем после выполнения очистки.

Действие «Проверить целостность» используется для проверки целостности журнала. В случае обнаружения нарушения целостности в журнале будет зарегистрировано событие нарушения целостности журнала событий аудита.

Журнал событий контроля целостности файлов хранится в виде нескольких файлов в каталоге. Архив событий также представляет из себя каталог, в который сохранены файлы журнала.

Действие «Сохранить как архив» используется для сохранения содержимого журнала в виде архива событий. По нажатии кнопки открывается файловый диалог для выбора места сохранения архива. В раскрывающемся списке «Раздел» необходимо выбрать требуемый раздел носителя информации, при этом произойдет его автоматическое монтирование (признаком успешного монтирования является появление структуры раздела в древовидном и табличном представлении). Для разделов Ext2, Ext3, Ext4 можно указать кодировку отображения (например, UTF-8 – для раздела ОС СН «Astra Linux Special Edition», KOI8-R – для раздела ОС МСВС и т.п.); по умолчанию выбрана кодировка UTF-8. Далее в строке имени необходимо указать каталог для сохранения данных журнала. При выборе раздела доступен выбор внутренней памяти контроллера, в этом случае данные будут сохранены на SD-карту контроллера СДЗ. Данные, сохраненные на SD-карте контроллера СДЗ, недоступны из ОС ЭВМ.

Архивные журналы могут храниться на контроллере СДЗ (на SD-карте контроллера СДЗ), на внешнем носителе и на жестком диске ЭВМ. Для просмотра архивов событий необходимо в качестве источника событий выбрать «Архивы». При этом в списке архивов для просмотра автоматически отобразятся архивы, ранее сохраненные на SD-карту контроллера СДЗ. При необходимости можно добавить в список архивов нужный архив (или несколько архивов) с внешнего носителя или с жесткого диска ЭВМ. Далее необходимо в списке архивов для просмотра выбрать один или несколько нужных архивов и нажать кнопку «Считать», расположенную под списком архивов.

Для работы со списком архивов необходимо пользоваться кнопкой-списком «Список», расположенной под списком архивов. Данная кнопка-список предоставляет возможность управления списком архивов и позволяет выполнить следующие действия:

- добавить архив в список;
- удалить архив из списка;
- выбрать для чтения все архивы;
- снять выделение со всех архивов.

Для выполнения дополнительных действий с архивами необходимо воспользоваться кнопкой-списком «Действие», расположенной под списком архивов. Данная кнопка-список позволяет выполнить с выделенным в списке архивом следующие действия:

- показать свойства;
- удалить архив;
- копировать архив.

В группе «Фильтры» располагаются элементы управления фильтрацией журнала. Доступны фильтры по времени, по пользователю, типу событий, по результату, а также по информации. Для фильтра по времени нужно выбрать интервал времени, для фильтров по пользователю, типу событий и результату можно указать несколько значений, установив в списке фильтров соответствующие флажки. Для фильтрации по информации можно использовать регулярные выражения. Сразу после изменения значения фильтра в таблице событий будут отображаться события, удовлетворяющие условиям фильтров. Чтобы отменить действие всех фильтров, нужно нажать на кнопку «Очистить фильтры», расположенную под списком фильтров. Если фильтры не заданы, то отобразятся все события журнала.

Чтобы выполнить поиск событий, имеющих определенное время, тип, пользователя, результат и информацию, необходимо в меню «Журнал событий» выбрать пункт «Поиск». Под таблицей с событиями появится окно «Поиск», в котором можно выбрать поле таблицы, по которому будет осуществляться поиск, указать критерии поиска (учитывать регистр, искать слова только целиком или использовать регулярные выражения) и ввести значение для поиска. Далее необходимо нажать на кнопку «Найти все», все ячейки таблицы с событиями, удовлетворяющими условиям поиска, будут подсвечены. Для перемещения между ячейками можно воспользоваться кнопками «Назад», «Вперед».

Для удобства просмотра журнала левую часть с фильтрами и архивами можно скрыть, потянув за разделитель и переместив его влево.

Кнопка «Экспортировать как…» предназначена для экспорта выбранных записей журнала в файл в формате XML, HTML или в текстовом формате. По нажатии кнопки открывается файловый диалог с возможностью выбора места сохранения файла и возможностью указания имени файла. Формат экспортируемых данных выбирается в файловом диалоге в поле «Тип файлов»: при выборе типа «*.txt» сохранение происходит в файл в текстовом формате, при выборе типа «*.xml» сохранение происходит в формате XML, при выборе типа «*.html» – в формате HTML. К имени файла автоматически добавляется расширение .xml, .html или .txt.

3.8. Контроль состава компонентов аппаратного обеспечения

3.8.1. Общая информация

Механизм контроля состава компонентов аппаратного обеспечения предоставляет возможность контролировать неизменность аппаратного состава ЭВМ и выполняет следующие функции:

- создание и модификация списков подконтрольных объектов в интерактивном режиме с формированием эталонного дерева устройств;
- проверка состава компонентов аппаратного обеспечения до загрузки операционной системы;
- просмотр журнала контроля состава компонентов аппаратного обеспечения.

Примечание. Для использования механизма контроля состава компонентов аппаратного обеспечения он должен быть включен в средстве управления СДЗ (описание настройки приведено в 3.6.4).

Средство контроля состава компонентов аппаратного обеспечения из ПО управления СДЗ предназначено для настройки механизма контроля состава компонентов аппаратного обеспечения. Для запуска данного средства необходимо в главном меню ПО управления СДЗ выбрать пункт «Контроль состава компонентов аппаратного обеспечения». Для получения доступа к данным необходимо пройти аутентификацию администратором СДЗ.

Непосредственно контроль состава компонентов аппаратного обеспечения, включенных в эталонное дерево устройств, осуществляется СДЗ автоматически после идентификации и аутентификации пользователя и до загрузки операционной системы.

3.8.2. Настройка параметров

Настройка параметров контроля состава компонентов аппаратного обеспечения заключается в настройке параметров журналирования и, собственно, контроля состава. Для журналирования настраиваются следующие параметры:

- максимальное количество событий в журнале;
- максимальное количество событий в файле журнала;
- порог сигнализации о переполнении журнала;
- порог блокировки ЭВМ для пользователя.

Для контроля состава компонентов аппаратного обеспечения настраиваются следующие параметры:

- периодичность проверки;
- поведение при появлении нового узла;
- поведение при изменении контролируемого узла;
- поведение при исчезновении контролируемого узла.

Для настройки параметров контроля состава компонентов аппаратного обеспечения необходимо использовать вкладку «Параметры».

Максимальное количество событий в журнале составляет 100000 записей. Журнал разбивается на несколько файлов. Рекомендуется устанавливать максимальное количество событий в файле журнала равным 1000. Данная рекомендация обусловлена тем, что при начале работы контроля состава компонентов аппаратного обеспечения выполняется проверка целостности текущего файла журнала. Если задано значение максимального количества событий в файле журнала более 1000, то чтение и контроль целостности текущего файла журнала занимает значительное время и увеличивает общее время запуска СДЗ. Установка значения менее 1000 не дает значительного прироста в скорости запуска СДЗ, но при этом приводит к созданию излишне большого количества файлов.

3.8.3. Подготовка эталона

Для подготовки эталона необходимо предварительно включить запуск контроля состава компонентов аппаратного обеспечения (описание соответствующей настройки приведено в 3.6.4). После включения запуска необходимо перезагрузить ЭВМ и штатно по клавише F5 запустить ПО управления СДЗ.

Примечание. Перезагрузка ЭВМ необходима для формирования текущего дерева устройств при старте СДЗ.

Текущее дерево устройств необходимо сохранить как эталон. Для этого в ПО управления СДЗ, в средстве контроля состава компонентов аппаратного обеспечения, необходимо перейти на вкладку «Контролируемые устройства» (рис. 18). На экране будет отображено дерево устройств. Необходимо выбрать устройства, наличие которых будет проверяться при запуске ЭВМ. Для этого в столбце «Состояние проверки» напротив требуемых устройств необходимо установить флажок. Для выбора всех устройств (или отмены выбора всех устройств) можно нажать кнопку «Выделить все». Для отмены последнего выполненного изменения можно нажать копку «Отменить», а для отмены всех изменений нажать кнопку «Отменить все».

Вкладка «Контролируемые устройства»

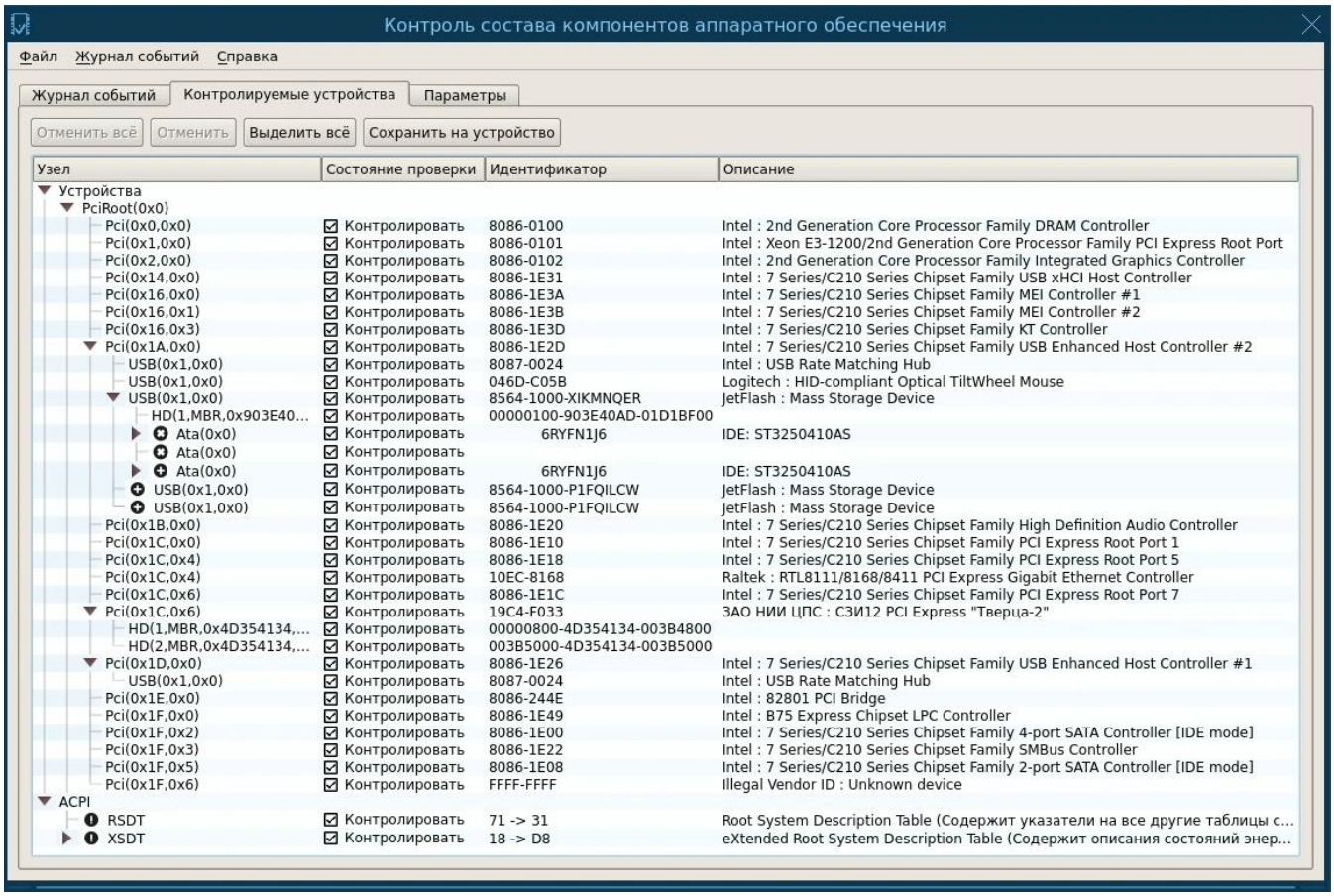


Рис. 18

Если устройство, которое ранее было сохранено в эталоне, отсутствует в ЭВМ, напротив него будет отображена пиктограмма ⊗.

Если в ЭВМ будет обнаружено новое устройство, которого не было в эталоне, напротив него будет отображена пиктограмма ⊕.

Если в ЭВМ устройство будет перемещено из одного места в другое, напротив него будет отображена пиктограмма ❗.

Для сохранения текущего дерева в качестве эталона и сохранения признаков «Контролировать» для всех устройств необходимо сохранить настройки, нажав на кнопку «Сохранить на устройство». После сохранения текущего дерева устройств в СДЗ оно становится эталонным.

На некоторых ЭВМ самопроизвольно изменяются идентификаторы ACPI таблиц, в таких случаях администратору СДЗ необходимо отключить контроль изменяемых устройств. Для отключения контроля устройств, в том числе ACPI таблиц, необходимо снять флажок «Контролировать» в строке с данными устройств, изменения которых необходимо игнорировать.

3.8.4. Журнал событий

Просмотр результатов контроля состава компонентов аппаратного обеспечения возможен на вкладке «Журнал событий».

Записи данных журналов содержат следующие элементы:

- дата регистрации события;
- время регистрации события;
- пользователь;

- тип события;
- результат события;
- дополнительная информация.

Регистрируемые типы событий приводятся в разделе 4 документа ФДШИ.04198-01 31 01 «Описание применения».

Вкладка «Журнал событий» предназначена для просмотра администратором СДЗ журнала состава компонентов аппаратного обеспечения, а также для работы с архивами журналов. Работа с журналом состава компонентов аппаратного обеспечения аналогична работе с журналом контроля целостности файлов (описание работы приведено в 3.7.4).

3.9. Восстановление заводских настроек

Средство восстановления заводских настроек предназначено для восстановления структуры разделов SD-карты контроллера СДЗ. На SD-карте есть два раздела:

- раздел с модулями ПО СДЗ;
- раздел с данными механизмов контроля целостности файлов и контроля состава компонентов аппаратного обеспечения.

Для запуска средства восстановления заводских настроек необходимо в главном меню ПО управления СДЗ выбрать пункт «Восстановление заводских настроек». Для получения доступа необходимо пройти аутентификацию администратором СДЗ. Восстановление выполняется для SD-карты, установленной в контроллер СДЗ.

Для восстановления раздела с модулями ПО СДЗ необходимо запустить ПО управления СДЗ с дистрибутивного электронного носителя (с CD-диска). В ходе восстановления раздела с модулями ПО СДЗ будет полностью очищено содержимое соответствующего раздела SD-карты и будет выполнено копирование модулей с дистрибутивного электронного носителя на SD-карту.

В ходе восстановления структура раздела SD-карты с данными контроля целостности файлов и контроля состава компонентов аппаратного обеспечения будет восстановлена. Восстановление приведет к удалению всех данных контроля целостности файлов и контроля состава компонентов аппаратного обеспечения, включая их журналы событий. Поэтому перед проведением восстановления рекомендуется (при наличии возможности) сохранить журналы событий.

После завершения восстановления данных необходимо заново установить параметры контроля целостности файлов и контроля состава компонентов аппаратного обеспечения, а также сформировать соответствующие эталоны.

Если в контроллере СДЗ заменена SD-карта на новую, или на SD-карте повреждена структура разделов, то необходимо выполнить форматирование SD-карты, а затем выполнить восстановление обоих разделов SD-карты. Для выполнения необходимых действий необходимо запустить ПО управления СДЗ с CD-диска, запустить средство восстановления заводских настроек. Для форматирования SD-карты необходимо нажать кнопку «Форматировать». В ходе форматирования существующие разделы удаляются и создаются новые. После форматирования необходимо восстановить структуру раздела с модулями ПО СДЗ и структуру раздела с данными ПО СДЗ.

3.10. Расчет контрольных сумм СДЗ

Средство расчета контрольных сумм СДЗ предназначено для получения контрольных сумм модулей СДЗ и данных СДЗ. Для запуска данного средства необходимо в главном меню ПО управления СДЗ выбрать пункт «Расчет контрольных сумм СДЗ». Для получения доступа к данным необходимо пройти аутентификацию администратором СДЗ.

Контрольные суммы разнесены по трем таблицам: «Модули ПО управления СДЗ», «Модули ПО контроллера СДЗ» и «Данные СДЗ». В конце первых двух таблиц отображается общая контрольная сумма модулей. В таблице «Данные СДЗ» отображается общая контрольная сумма данных о пользователях и значений параметров СДЗ. Контрольная сумма данных СДЗ не

является постоянной и будет меняться после любого изменения в указанных данных. Контрольная сумма данных СДЗ может применяться администратором СДЗ для отслеживания неизменности данных СДЗ.

Модули ПО управления расположены на дистрибутивном ЭН (CD-диск) и на контроллере СДЗ (на SD-карте контроллера СДЗ). При запуске ПО управления СДЗ с дистрибутивного ЭН в таблице «Модули ПО управления СДЗ» отображается контрольная сумма модулей на дистрибутивном ЭН, тогда как при запуске ПО управления СДЗ с контроллера СДЗ в таблице отображаются контрольные суммы модулей на SD-карте контроллера СДЗ. То, с какого носителя в настоящий момент запущено ПО управления СДЗ, отображается в поле «Тип носителя».

Выведенные на экран рассчитанные контрольные суммы в первых двух таблицах должны соответствовать эталонным контрольным суммам, приведенным в документе ФДШИ.469535.098ФО «Аппаратно-программный комплекс «Ребус-СДЗ». Формуляр».

3.11. Самотестирование СДЗ

3.11.1. Тесты, выполняемые при каждом запуске

При каждом запуске ЭВМ, до отображения экрана идентификации и аутентификации, СДЗ для самотестирования выполняет следующие тесты:

- разграничение доступа к управлению СДЗ;
- управление работой СДЗ;
- управление параметрами СДЗ;
- аудит безопасности СДЗ;
- идентификация и аутентификация;
- тестирование СДЗ, контроль целостности ПО и параметров СДЗ;
- сигнализация СДЗ;
- обеспечение безопасности СДЗ;
- защита остаточной информации СДЗ;
- защита интерфейса управления СДЗ;
- тестирование аппаратной части СДЗ.

При успешном выполнении тестов на экране идентификации и аутентификации отображается сообщение «Самотестирование пройдено успешно». В противном случае отображается сообщение: «Внимание! Самотестирование не пройдено».

Для получения информации о том, какой тест не пройден, администратор может воспользоваться расширенной информацией сигнализации, журналом событий контроллера СДЗ или вкладкой «Тесты» в управлении СДЗ.

3.11.2. Самотестирование контроля целостности файлов

Для выполнения самотестирования контроля целостности файлов необходимо включить тест для данного средства в средстве управления СДЗ на вкладке «Тесты».

Самотестирование данного механизма выполняется перед непосредственным контролем целостности. При этом появится запрос «Инициирован запуск процедуры самотестирования механизма контроля целостности программной среды СВТ. Вы точно желаете ее выполнения? (1 – Да, 2 – Нет) (1, 2)». Для проведения самотестирования необходимо нажать на клавиатуре «1» и затем «Enter» (рис. 19).

Запуск самотестирования механизма контроля целостности программной среды СВТ

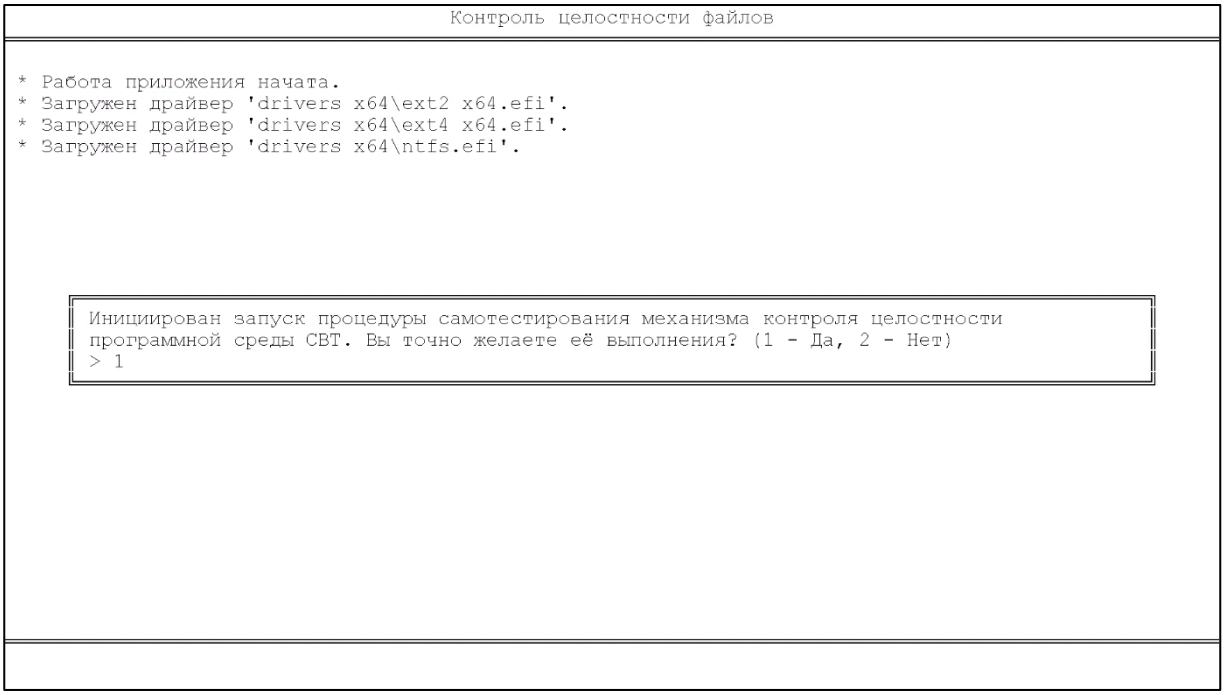


Рис. 19

На экране должен отобразиться результат самотестирования и появиться запрос «Появилось ли сообщение об изменении файла 'self test data damaged.bin' и ошибке доступа к файлу 'self test data deleted.bin'? (1 – Да, 2 – Нет) (1,2)». После чего необходимо ответить «1» или «2» с учетом результата самотестирования (рис. 20).

Результат самотестирования механизма контроля целостности программной среды СВТ

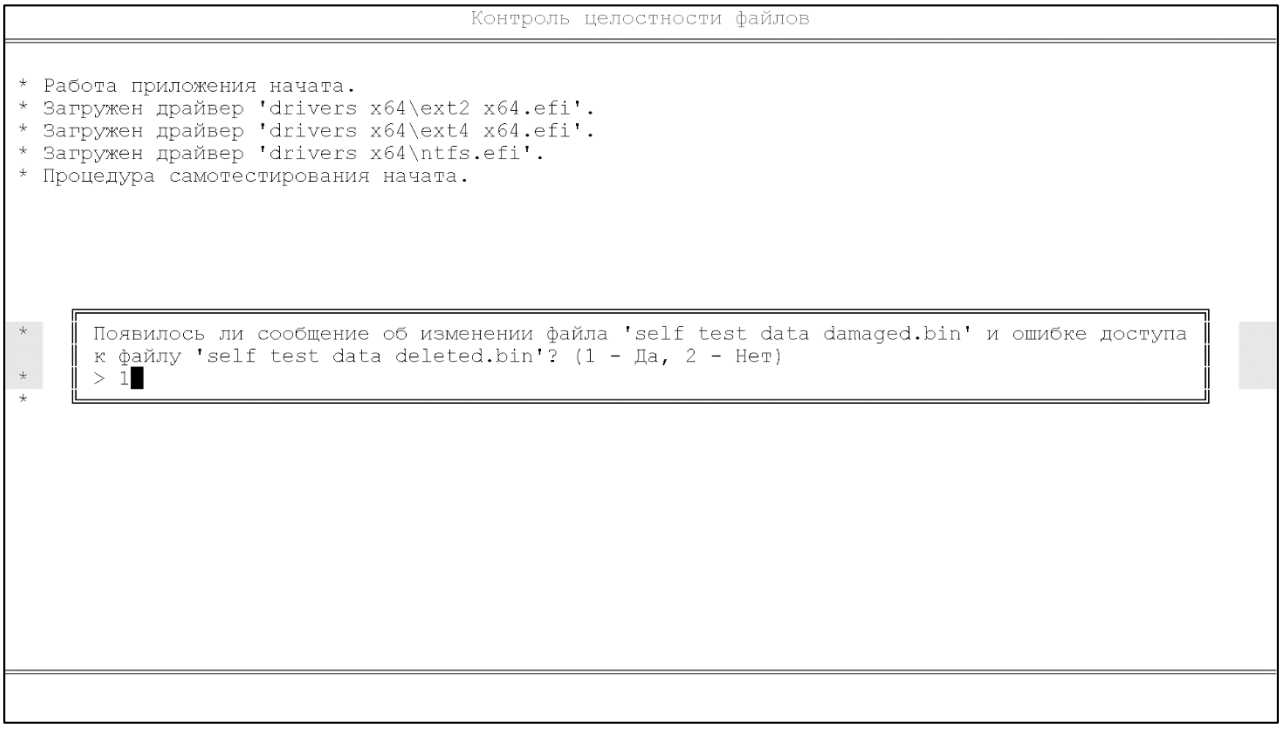


Рис. 20

3.11.3. Самотестирование контроля состава компонентов аппаратного обеспечения

Для выполнения самотестирования контроля состава компонентов аппаратного обеспечения необходимо включить тест для данного средства в средстве управления СДЗ на вкладке «Тесты».

Запуск самотестирования контроля состава компонентов аппаратного обеспечения

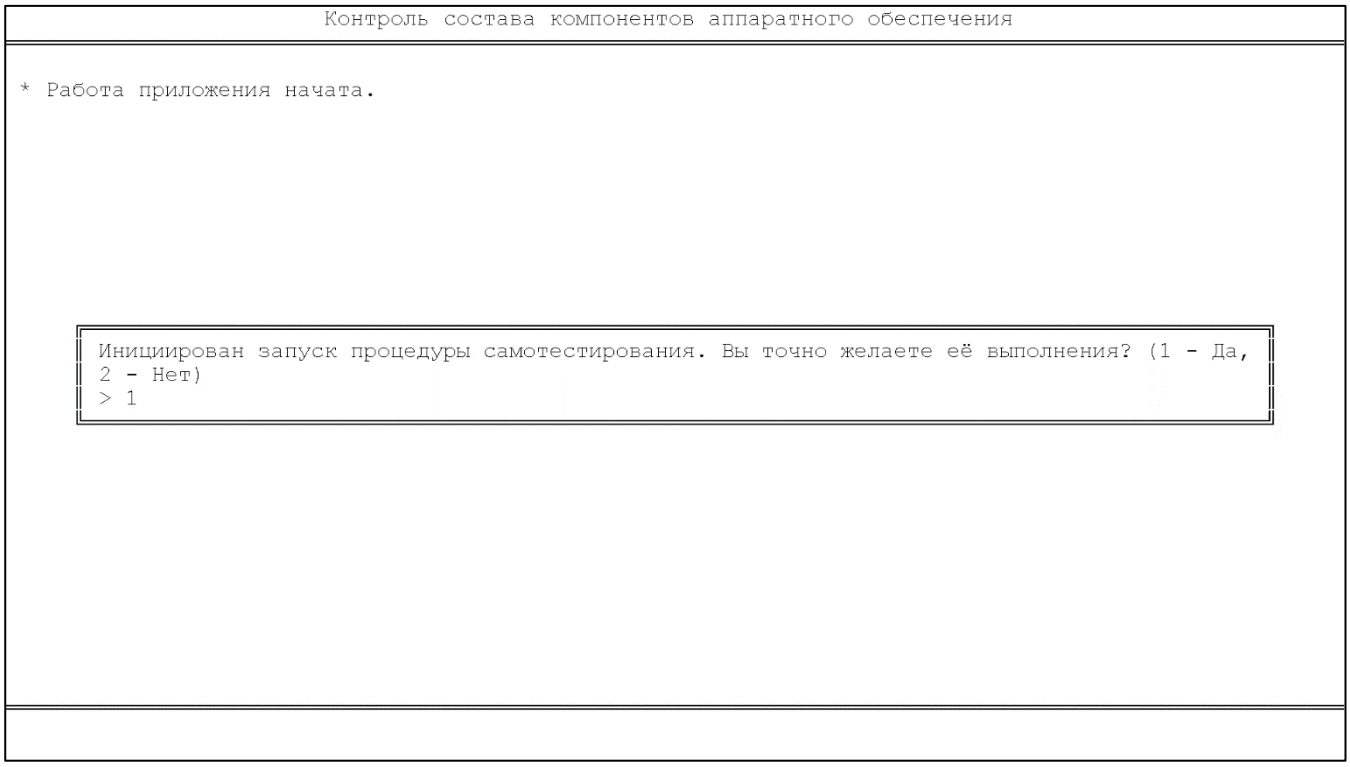


Рис. 21

Самотестирование данного механизма выполняется перед непосредственным контролем целостности. При этом сформируется текущее дерево устройств и появится запрос «Инициирован запуск процедуры самотестирования. Вы точно желаете ее выполнения? (1 – Да, 2 – Нет) (1, 2)». Для проведения самотестирования необходимо нажать на клавиатуре «1» и затем «Enter» (рис. 21). После этих действий появится запрос «Для продолжения тестирования необходимо подключить USB-носитель к USB-порту компьютера. Носитель подключен? (1 – Носитель подключен, 2 – Отмена тестирования) (1, 2)». Необходимо подключить USB-носитель к ЭВМ и нажать клавишу «1». На экране должен отобразиться результат самотестирования и появиться запрос «Появилось ли сообщение об обнаружении нового устройства? (1 – Да, 2 – Нет) (1, 2)». Перед ответом лучше извлечь USB-накопитель (так как иначе он будет добавлен в дерево устройств), после чего необходимо ответить «1» или «2» с учетом результата самотестирования (рис. 22).

Результат самотестирования контроля состава компонентов аппаратного обеспечения

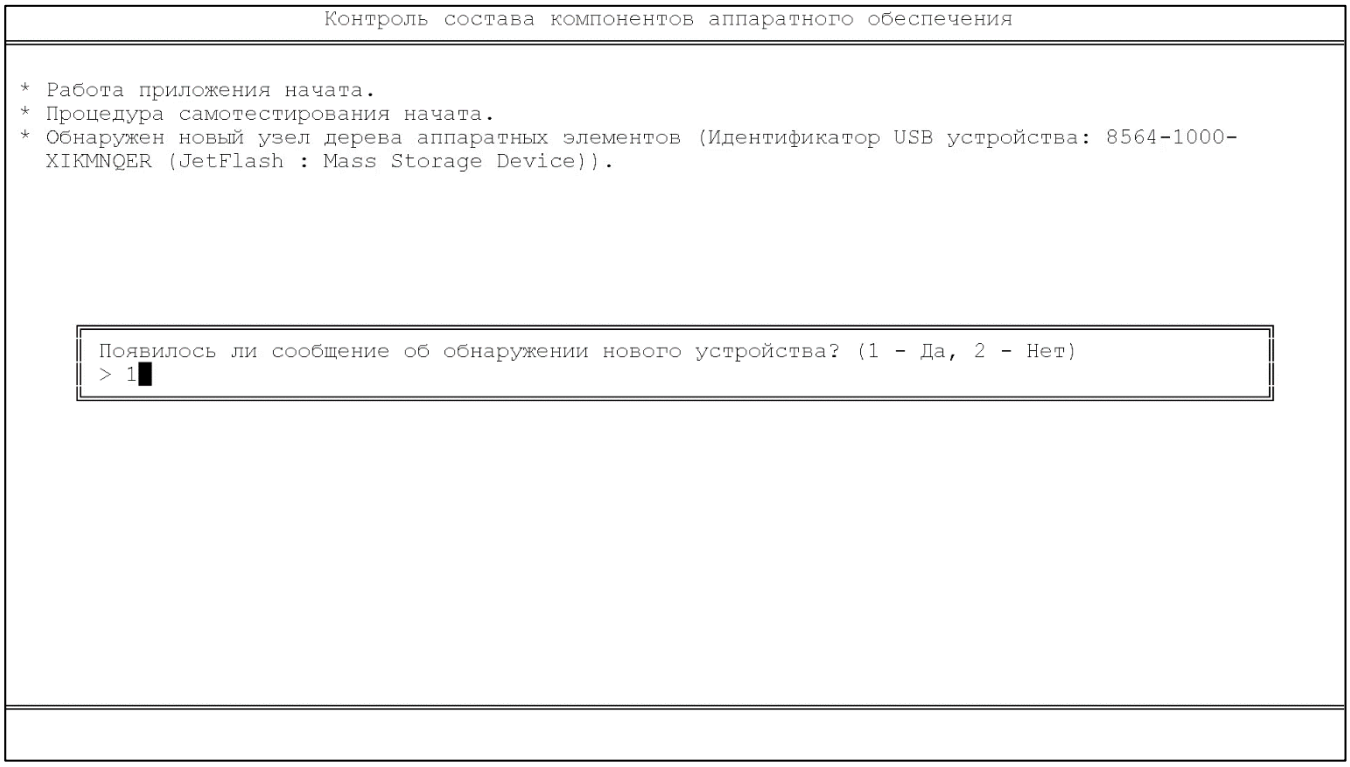


Рис. 22

3.11.4. Самотестирование блокировки загрузки ОС

Для выполнения самотестирования блокировки загрузки ОС необходимо в ПО управления СДЗ в управлении СДЗ включить тест «Блокировка загрузки ОС».

Самотестирование данного механизма выполняется после регистрации администратора безопасности. При этом появится запрос «Инициирован запуск процедуры самотестирования блокировки загрузки ОС. Вы точно желаете ее выполнения? (1 – Да, 2 – Нет)». Для проведения самотестирования необходимо нажать на клавиатуре «1» и затем «Enter». На экране должно отобразиться сообщение «Попытка загрузки нештатной ОС. Пригласите администратора» (рис. 23), примерно через 5 с ЭВМ перезагрузится.

Сообщение о попытке загрузки нештатной ОС

Рис. 23

3.11.5. Самотестирование аппаратного сброса

Для выполнения самотестирования аппаратного сброса необходимо в ПО управления СДЗ в управлении СДЗ включить тест «Аппаратный сброс», и на вкладке «Управление контроллером» настроить параметр «Сторожевой таймер» (например, задать значение сторожевого таймера 20 с).

Самотестирование данного механизма выполняется после регистрации администратора безопасности. При этом появится запрос «Инициирован запуск процедуры самотестирования аппаратного сброса. Вы точно желаете ее выполнения? (1 – Да, 2 – Нет)». Для проведения самотестирования необходимо нажать на клавиатуре «1» и затем «Enter». На экране должно отобразиться сообщение, например: «Осталось 0 мин. 20 сек. до аппаратного сброса» (рис. 24). В случае успешного выполнения теста через заданное время ЭВМ должна перезагрузиться. В случае неуспеха будет выведено сообщение «Тест не пройден» и примерно через 5 с ЭВМ перезагрузится.

Сообщение об оставшемся времени до аппаратного сброса

Рис. 24

4. СООБЩЕНИЯ ОПЕРАТОРУ

Сведения о сообщениях оператору и о действиях оператора при появлении данных сообщений приведены в таблицах 1 – 8.

Таблица 1 – Сообщения оператору, выдаваемые при входе пользователя в систему

Содержание сообщения	Описание сообщения	Действия оператора
Плата извлекалась из ЭВМ	Зафиксировано изъятие контроллера СДЗ из ЭВМ	Сообщение свидетельствует о нарушении безопасности. Возможно ложное срабатывание при разряде элемента питания контроллера СДЗ, в этом случае необходимо заменить элемент питания
ЭВМ заблокирована для пользователя	Выводится при блокировке возможности работы пользователей на ЭВМ средствами СДЗ	Необходимо выяснить причину блокировки, устранить ее причину и снять блокировку
Нарушена целостность модулей/данных СДЗ	При самотестировании выявлено нарушение целостности модулей СДЗ либо данных	При однократном срабатывании перезагрузить ЭВМ. Если после перезагрузки проблема повторяется, то администратору СДЗ необходимо проверить целостность чего нарушена. При нарушении целостности данных сохранить и очистить все журналы событий, восстановить заводские настройки, пересоздать пользователей. При нарушении целостности модулей ПО СДЗ необходимо отправить контроллер СДЗ в ремонт
Неверный ввод или неразрешенное время работы. Повторите ввод	Сообщение выводится при вводе некорректных идентификационных и аутентификационных данных, при попытках входа в систему в недопустимое время или в недопустимый день недели	Ввести корректные идентификационные и аутентификационные данные. Если идентификационные и аутентификационные данные неизвестны, обратиться к администратору для их получения
Самотестирование пройдено успешно	Сообщение отображается, если самотестирование СДЗ выполнено успешно	Никаких действий не требуется

Таблица 2 – Сообщения, выдаваемые при работе со средством управления СДЗ

Содержание сообщения	Описание сообщения	Действия оператора
Запрос статуса блокировки ЭВМ вернул недопустимое значение	При попытке получить статус блокировки произошла ошибка	Повторить попытку после перезагрузки. Если не получится опять, то необходимо обратиться в техническую поддержку

Продолжение таблицы 2

Содержание сообщения	Описание сообщения	Действия оператора
Запрос изменения статуса блокировки ЭВМ вернул недопустимое значение	При попытке снять блокировку произошла ошибка	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если не получится опять, то необходимо обратиться в техническую поддержку
Не удалось прочитать список поддерживаемых контроллером функций. Код ошибки – <код ошибки при взаимодействии с контроллером>	Не удалось прочитать список поддерживаемых контроллером функций. Контроллер не отвечает или поврежден	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если не получится опять, то необходимо обратиться в техническую поддержку
Не удалось найти контроллер. Код ошибки – <код ошибки при взаимодействии с контроллером>	Контроллер отсутствует, или не отвечает, или поврежден	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если не получится опять, то необходимо обратиться в техническую поддержку
Закончить работу с программой управления? Последние значения параметров не будут сохранены	Управление контроллером не было завершено	Необходимо сохранить нужные параметры контроллера и только после этого закрыть средство либо закрыть средство без сохранения изменений, подтвердив данную операцию в диалоговом сообщении
Невозможно прочитать список пользователей контроллера. Код ошибки – <код ошибки при взаимодействии с контроллером>	Контроллер не отвечает или поврежден	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если не получится опять, то необходимо обратиться в техническую поддержку

Продолжение таблицы 2

Содержание сообщения	Описание сообщения	Действия оператора
Контроллер СДЗ не найден. Дальнейшая работа программы невозможна	Контроллер отсутствует, или не отвечает, или поврежден	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если не получится опять, то необходимо обратиться в техническую поддержку
Ошибка открытия сессии. Работа с программой невозможна! Попробуйте запустить ее заново	Возникает при попытке пройти аутентификацию в средстве управления	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если не получится опять выполнить попытку аутентификации, то необходимо обратиться в техническую поддержку
Не удалось прочитать значение принудительного использования электронных идентификаторов. Код ошибки – <код ошибки при взаимодействии с контроллером>	При попытке чтения управляющих значений контроллера возникла ошибка	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если не получится опять получить значения, то необходимо обратиться в техническую поддержку
Не удалось сохранить значение принудительного использования электронных идентификаторов. Код ошибки – <код ошибки при взаимодействии с контроллером>	При попытке записи управляющих значений контроллера возникла ошибка	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если не получится опять сохранить значения, то необходимо обратиться в техническую поддержку
Не удалось прочитать значение принудительного использования USB-ключей. Код ошибки – <код ошибки при взаимодействии с контроллером>	При попытке чтения управляющих значений контроллера возникла ошибка	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если ошибка повторится, то необходимо обратиться в техническую поддержку

Продолжение таблицы 2

Содержание сообщения	Описание сообщения	Действия оператора
Не удалось сохранить значение принудительного использования USB-ключей. Код ошибки – <код ошибки при взаимодействии с контроллером>	При попытке записи управляющих значений контроллера возникла ошибка	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если не получится опять сохранить значения, то необходимо обратиться в техническую поддержку
Не удалось прочитать значение поддержки ключей. Код ошибки – <код ошибки при взаимодействии с контроллером>	При попытке чтения управляющих значений контроллера возникла ошибка	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если ошибка повторится, то необходимо обратиться в техническую поддержку
Не удалось сохранить значение поддержки ключей. Код ошибки – <код ошибки при взаимодействии с контроллером>	При попытке записи управляющих значений контроллера возникла ошибка	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если не получится опять сохранить значения, то необходимо обратиться в техническую поддержку
Не удалось прочитать тип электронного идентификатора. Код ошибки – <код ошибки при взаимодействии с контроллером>	При попытке чтения управляющих значений контроллера возникла ошибка	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления и приложить идентификатор. Если ошибка повторится, то необходимо обратиться в техническую поддержку
Неизвестный тип электронного идентификатора	Подключен неопознанный тип электронного ключа	Подключить разрешенный тип электронного ключа

Продолжение таблицы 2

Содержание сообщения	Описание сообщения	Действия оператора
Ошибка чтения электронного идентификатора. Код возврата – <код ошибки при взаимодействии с контроллером>	При попытке чтения управляющих значений контроллера возникла ошибка	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если ошибка повторится, то необходимо обратиться в техническую поддержку
Не удалось записать идентификатор пользователя – нет доступа к USB-ключу	ПИН-код ключа не совпадает с ПИН-кодом на контроллере	Ввести ПИН-код и нажать кнопку «Получить доступ» либо переинициализовать ключ и записать на него новые данные
Ошибка чтения ключевых данных с контроллера. Код ошибки – <код ошибки при взаимодействии с контроллером>	Ошибка возникает при попытке чтения ключевых данных контроллера	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если ошибка повторится, то необходимо обратиться в техническую поддержку
Данные, считанные с контроллера, содержат недопустимые символы	При чтении данных с контроллера обнаружены нечитаемые символы, или они не соответствуют заданному алфавиту	Необходимо задать корректные данные и сохранить их
Ошибка чтения ключевых данных с USB-ключа. Код ошибки – <код ошибки при работе с ключами>	Коды ошибки при работе с ключами описаны в спецификации по токенам	Ознакомиться со спецификацией, устранить причину ошибки. Воспользоваться официальным ПО для инициализации, а затем повторить попытку
Ошибка записи ключевых данных на USB-ключ. Код ошибки – <код ошибки при работе с ключами>	Коды ошибки при работе с ключами описаны в спецификации по токенам	Ознакомиться со спецификацией, устранить причину ошибки. Воспользоваться официальным ПО для инициализации, а затем повторить попытку
Данные, считанные с USB-ключа, содержат недопустимые символы	При чтении данных с ключа обнаружены нечитаемые символы, или они не соответствуют заданному алфавиту	Необходимо задать корректные данные и сохранить их

Продолжение таблицы 2

Содержание сообщения	Описание сообщения	Действия оператора
Ошибка записи ключевых данных на контроллер. Код ошибки – <код ошибки при взаимодействии с контроллером>	При попытке записи управляющих значений контроллера возникла ошибка	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если ошибка повторится, то необходимо обратиться в техническую поддержку
Введите ПИН-код и секрет. ПИН-код должен состоять из 6 – 8 символов	При сохранении данных было обнаружено, что аутентификационные данные не соответствуют требованиям	Указать ПИН-код и секрет с учетом требований и метрики качества
ПИН-код должен состоять из 6 – 8 символов	При сохранении данных было обнаружено, что аутентификационные данные не соответствуют требованиям	Указать ПИН-код с учетом требований и метрики качества
USB-ключ не может быть инициализирован средствами библиотеки PKCS11. Пожалуйста, воспользуйтесь официальным ПО для инициализации, а затем повторите попытку. Код ошибки – <код ошибки при работе с ключами>	При инициализации устройства возникла непредвиденная ошибка. Предоставляемая библиотека не позволяет выполнять дальнейшую работу с устройством	Воспользоваться официальным ПО для инициализации, а затем повторить попытку
Ошибка инициализации USB-ключа. Код ошибки – <код ошибки при работе с ключами>	Коды ошибки при работе с ключами описаны в спецификации по токенам	Ознакомиться со спецификацией, устранить причину ошибки. Воспользоваться официальным ПО для инициализации, а затем повторить попытку
Ошибка смены ПИН-кода USB-ключа. Код ошибки – <код ошибки при работе с ключами>	Коды ошибки при работе с ключами описаны в спецификации по токенам	Ознакомиться со спецификацией, устранить причину ошибки. Воспользоваться официальным ПО для инициализации, а затем повторить попытку
Введите или выберите идентификатор пользователя	При попытке записать данные на идентификатор не был выбран пользователь из списка	Выбрать идентификатор пользователя из списка

Продолжение таблицы 2

Содержание сообщения	Описание сообщения	Действия оператора
Ошибка чтения списка пользователей. Код ошибки – <код ошибки при взаимодействии с контроллером>	При попытке чтения списка пользователей контроллера возникла ошибка	Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления. Если ошибка повторится, то необходимо обратиться в техническую поддержку
Достигнуто максимальное число пользователей	Количество пользователей ограничено на контроллере	Удалить ненужного пользователя и добавить нового
Ошибка при добавлении пользователя. Код ошибки – <код ошибки при взаимодействии с контроллером>	Коды ошибки при работе с ключами описаны в спецификации по токенам	Ознакомиться со спецификацией, устранить причину ошибки. Воспользоваться официальным ПО для инициализации, а затем повторить попытку
Ошибка при сохранении новых настроек пользователя. Код ошибки – <код ошибки при взаимодействии с контроллером>	При сохранении новых настроек произошла ошибка	Повторить попытку сохранения. Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления и внести изменения. Если ошибка повторится, то необходимо обратиться в техническую поддержку
Не удалось сохранить список выполняемых тестов. Код ошибки – <код ошибки при взаимодействии с контроллером>	При сохранении новых настроек произошла ошибка	Повторить попытку сохранения. Закрыть средство управления, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство управления и внести изменения. Если ошибка повторится, то необходимо обратиться в техническую поддержку
Сохранение списка выполняемых тестов прошло успешно	Список тестов был сохранен, изменения вступят в силу после перезагрузки	Перезагрузить ЭВМ и провести тесты. После отработки тестов посмотреть результаты самотестирования
Операция чтения данных файла <имя файла> завершена с ошибкой. Код ошибки – <код ошибки работы с файловыми операциями>	Возникла ошибка чтения данных с устройства	Выбрать другой файл на устройстве

Продолжение таблицы 2

Содержание сообщения	Описание сообщения	Действия оператора
Обнаружены некорректные настройки: - отсутствует, либо истек пароль, либо его длина меньше 8 символов; - разрешен временной интервал менее 15 минут; - не указано разрешенных дней недели; - часть паролей/ПИН-кодов/секретов не соответствует метрике качества аутентификационных данных, см. вкладку «Управление контроллером». Данные настройки могут заблокировать пользователю «<Имя пользователя>» доступ к станции	Уведомление возникает при попытке сохранить некорректные аутентификационные данные	Изменить аутентификационные данные и разрешенное время работы на корректные. Повторить попытку сохранения

Таблица 3 – Сообщения, выдаваемые при работе со средством контроля состава компонентов аппаратного обеспечения

Содержание сообщения	Описание сообщения	Действия оператора
Контроллер СДЗ не найден. Дальнейшая работа программы невозможна	Сообщение возникает, если контроллер отсутствует, или не отвечает, или поврежден	Закрыть средство контроля состава компонентов аппаратного обеспечения, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство контроля состава компонентов аппаратного обеспечения. Если не получится опять, то необходимо обратиться в техническую поддержку
SD-карта не найдена. Дальнейшая работа программы невозможна	Сообщение возникает, если в контроллере отсутствует или повреждена SD-карта	Убедиться в наличии исправной SD-карты в контроллере
Не удалось получить список устройств от контроллера	Возникла ошибка чтения данных с устройства	Закрыть средство и открыть заново. Восстановить внутреннюю память контроллера при необходимости

Окончание таблицы 3

Содержание сообщения	Описание сообщения	Действия оператора
Не удалось считать настройки с контроллера	Возникла ошибка чтения данных с устройства	Убедиться, что модуль настроен на запуск в средстве управления. Закрыть средство и открыть заново. Восстановить внутреннюю память контроллера при необходимости
Не удалось считать настройки с устройства	Возникла ошибка чтения данных из файла на жестком диске	Закрыть средство и открыть заново, попробовать заново считать настройки из файла. Если проблема повторится, то скорее всего файл с настройками поврежден
Вы действительно хотите сохранить текущее дерево устройств как эталонное? Внимание! Существующее дерево будет удалено!	В ходе работы средство обнаружило новые, измененные или удаленные узлы. Новое дерево будет содержать новые и измененные узлы, а удаленные будут исключены	Подтвердить сохранение дерева устройств. Убедиться, что в журнал регистрации внесено сообщение о сохранении дерева устройств как эталонного
Не удалось сохранить список подконтрольных устройств	При попытке сохранить возникла ошибка	Повторить попытку сохранения устройств
Код ошибки: <код ошибки при работе с файлами>. Не могу открыть файл дерева	При работе с деревом устройств возникла ошибка	Повторить попытку запуска модуля
Настройки успешно сохранены на контроллер	Настройки средства были успешно сохранены и вступят в силу при следующем запуске средства	Закрыть уведомление
Не удалось найти хранилище на контроллере	Во время запуска средства не удалось найти хранилище на внутренней памяти контроллера	Повторить попытку запуска средства. При повторе ошибки восстановить внутреннюю память контроллера
При загрузке параметров произошла ошибка	Возникла ошибка чтения данных с устройства	Будет выполнена попытка восстановления заводских параметров
При восстановлении заводских параметров произошла ошибка	Возникла ошибка при попытке восстановления заводских параметров средства	Повторить попытку запуска средства. При повторе ошибки восстановить внутреннюю память контроллера
Заводские параметры успешно восстановлены	Успешно восстановлены заводские параметры средства	Закрыть уведомление

Таблица 4 – Сообщения, выдаваемые при работе со средством контроля целостности файлов

Содержание сообщения	Описание сообщения	Действия оператора
Контроллер СДЗ не найден. Дальнейшая работа программы невозможна	Сообщение возникает, если контроллер отсутствует, или не отвечает, или поврежден	Закрыть средство контроля целостности файлов, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство контроля целостности файлов. Если не получится опять, то необходимо обратиться в техническую поддержку
Произошла критическая ошибка. Не удалось загрузить параметры контроля целостности файлов. Приложение будет закрыто	Возникла ошибка при загрузке параметров средства	Повторить попытку запуска средства. При повторе ошибки восстановить внутреннюю память контроллера
Произошла критическая ошибка. Произошла ошибка при инициализации механизма самотестирования. Приложение будет закрыто	Возникла ошибка инициализации механизма самотестирования	Повторить попытку запуска средства. При повторе ошибки восстановить внутреннюю память контроллера
Нарушена целостность данных механизма самотестирования. Выполнена попытка восстановления данных. В случае повторения ошибки рекомендуется выполнить переконфигурирование механизма на вкладке «Параметры»	Возникла ошибка при проверке целостности механизма самотестирования	Настроить механизм самотестирования на вкладке «Параметры»
Механизм самотестирования не сконфигурирован либо сконфигурирован неверно. Рекомендуется настроить механизм самотестирования на вкладке «Параметры»	Возникла ошибка при работе механизма самотестирования	Настроить механизм самотестирования на вкладке «Параметры»
При загрузке параметров произошла ошибка	Возникла ошибка чтения данных с устройства	Будет выполнена попытка восстановления заводских параметров
При восстановлении заводских параметров произошла ошибка	Возникла ошибка при попытке восстановления заводских параметров средства	Повторить попытку запуска средства. При повторе ошибки восстановить внутреннюю память контроллера
Заводские параметры успешно восстановлены	Успешно восстановлены заводские параметры средства	Закрыть уведомление

Окончание таблицы 4

Содержание сообщения	Описание сообщения	Действия оператора
При сохранении параметров произошла ошибка	Сообщение возникает, если не удалось сохранить параметры средства на устройство	Повторить попытку запуска средства. При повторе ошибки восстановить внутреннюю память контроллера
Не удалось получить параметры журнала регистрации событий аудита. Будут использованы значения параметров по умолчанию	Возникла ошибка при чтении параметров журнала регистрации событий аудита	При повторе ошибки восстановить внутреннюю память контроллера

Таблица 5 – Сообщения, выдаваемые при работе с файловыми диалогами ПО управления СДЗ

Содержание сообщения	Описание сообщения	Действия оператора
Данный файл содержит недопустимые символы в имени: <имя файла>	Файл содержит нечитаемые символы в своем имени	Необходимо выбрать другой файл или сменить кодировку отображения раздела
Данный файл уже существует: <имя файла> В случае подтверждения он будет перезаписан	Возникает при попытке сохранить в уже существующий файл. Файловый диалог открыт с возможностью перезаписи файлов	Перезаписать выбранный файл или указать новое имя файла
Данный файл уже существует. Вы не можете его перезаписать. Укажите имя нового файла (см. ниже)	Возникает при попытке сохранить в уже существующий файл. Файловый диалог открыт без возможности перезаписи файлов	Указать новое имя файла
Монтирование завершилось ошибкой: <текст ошибки>	Устройство было изъято или повреждено	Необходимо выбрать другое устройство
Уникальная директория для приложения не найдена	Внутренняя память контроллера повреждена	Необходимо восстановить данные на внутренней памяти контроллера
Устройство было извлечено	При обновлении списка разделов устройство не было обнаружено, так как оно было изъято	Выбрать другой раздел в новом списке либо подключить устройство назад
Монтирование раздела в другой кодировке завершилось ошибкой	Возникает при смене кодировки монтирования выбранного раздела	Обновить список разделов и повторить попытку или выбрать другое устройство
Нет доступных устройств. Вставьте устройство	Файловый диалог не нашел ни одного устройства	Подключить устройство хранения данных и обновить список разделов
Вы точно хотите удалить папку со всем ее содержимым?	При выборе в контекстном меню пункта удаления директории необходимо подтвердить операцию	Подтвердить удаление или отменить операцию

Таблица 6 – Сообщения, выдаваемые при работе со средством восстановления заводских настроек

Содержание сообщения	Описание сообщения	Действия оператора
Ошибка открытия сессии. Работа с программой невозможна! Попробуйте запустить ее заново	Возникает при попытке пройти аутентификацию в средстве восстановления заводских настроек	Закрыть средство восстановления заводских настроек, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство. Если опять не получится пройти аутентификацию, то необходимо обратиться в техническую поддержку
Не удалось получить доступ к контроллеру и его внутренней памяти	Во время запуска восстановления настроек не удалось получить доступ к разделам SD-карты контроллера	Повторить попытку запуска средства. При повторе ошибки восстановить внутреннюю память контроллера
Резервные данные не были найдены	Во время запуска восстановления настроек не удалось найти резервные данные	Повторить попытку запуска средства. При повторе ошибки восстановить внутреннюю память контроллера

Таблица 7 – Сообщения, выдаваемые при работе со средством расчета контрольных сумм СДЗ

Содержание сообщения	Описание сообщения	Действия оператора
Неправильный логин или пароль. Осталось попыток: N	При попытке пройти аутентификацию были введены неверные идентификатор пользователя и пароль	Ввести логин и пароль администратора
Ошибка чтения данных контроллера: контроллер не найден	Сообщение возникает, если контроллер отсутствует	Закрыть предупреждение и продолжить работу в режиме без контроллера
Ошибка открытия сессии. Работа с программой невозможна! Попробуйте запустить ее заново	Возникает при попытке пройти аутентификацию в средстве	Закрыть средство, выключить ЭВМ, почистить контакты контроллера, вставить его назад, запустить ПО управления и открыть заново средство. Если опять не получится пройти аутентификацию, то необходимо обратиться в техническую поддержку
Отсутствует список контролируемых файлов	Не удалось найти конфигурационный файл. ПО управления повреждено	Заменить носитель, с которого производился запуск ПО управления, так как носитель поврежден

Окончание таблицы 7

Содержание сообщения	Описание сообщения	Действия оператора
Не удалось найти эталонные контрольные суммы	Не удалось найти конфигурационный файл	Повторить попытку запуска, и если ошибка повторится, то восстановить внутреннюю память контроллера
Ошибка записи контрольных сумм в файл	Не удалось сохранить контрольные суммы на выбранный носитель информации	Выбрать другой носитель информации для записи контрольных сумм

Таблица 8 – Сообщения, выдаваемые при работе с журналами событий аудита

Содержание сообщения	Описание сообщения	Действия оператора
Чтение журнала невозможно: не выбран источник событий	Не выбран источник событий	Выбрать источник событий и повторно запустить чтение журнала
Чтение архивов невозможно: не выбран источник событий	Не выбран источник событий	Выбрать источник событий и повторно запустить чтение архивов
Внимание! Все события в журнале будут удалены. Продолжить?	Будут удалены из журнала все события аудита	Рекомендуется сохранить текущий журнал событий на внешний носитель, а затем выполнить очистку журнала
Очистка журнала не выполнена	Произошла ошибка во время очистки журнала	Перезапустить средство и повторно запустить очистку журнала
Обнаружено нарушение целостности	Журнал событий аудита поврежден	Рекомендуется сохранить текущий журнал событий на внешний носитель, а затем выполнить очистку журнала
Удаление архива невозможно: не выбран архив для удаления	Не выбран архив для удаления	Выбрать архив и повторно запустить удаление
Копирование архива невозможно: не выбран архив для копирования	Не выбран архив для копирования	Выбрать архив и повторно запустить копирование

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

МСВС	–	мобильная система Вооруженных сил
ОС	–	операционная система
ОС СН	–	операционная система специального назначения
ПИН	–	персональный идентификационный номер
ПО	–	программное обеспечение
СВТ	–	средство вычислительной техники
СДЗ	–	средство доверенной загрузки
ЭВМ	–	электронно-вычислительная машина
ЭН	–	электронный носитель
ЭЦП	–	электронная цифровая подпись

Лист регистрации изменений									
Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в докум.*	*№ докумен-та*	*Входящий № сопрово-дительно-го докум. и дата*	*Подп.*	*Да-та*
	изменен-ных	*заменен-ных*	*новых*	*аннули-рован-ных*					