



АКЦИОНЕРНОЕ ОБЩЕСТВО
«Аладдин Р.Д.»

УТВЕРЖДЕН
RU.АЛДЕ.02.13.022-02 94 01

СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ
«TRUSTED SECURITY MODULE»
ДЛЯ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА
«ДОВЕРЕННАЯ ПЛАТФОРМА» НА БАЗЕ
ARM-ПРОЦЕССОРОВ

Руководство пользователя по эксплуатации

RU.АЛДЕ.02.13.022-02 94 01

Листов 102

2020

| | | | | |
|--------------|----------------|--------------|--------------|----------------|
| Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата |
| | | | | |

СОДЕРЖАНИЕ

| | | |
|--------|--|----|
| 1. | Общие сведения..... | 8 |
| 1.1. | Обозначение и наименование..... | 8 |
| 1.2. | Назначение СДЗ «TSM» | 8 |
| 1.3. | Основные возможности и функции СДЗ «TSM» | 9 |
| 1.4. | Состав программных компонентов СДЗ «TSM»..... | 12 |
| 2. | Условия применения..... | 13 |
| 2.1. | Общие положения | 13 |
| 2.2. | Особенности приемки и реализации функций безопасности среды функционирования СДЗ «TSM» | 14 |
| 2.2.1. | Особенности приемки СДЗ «TSM»..... | 14 |
| 2.2.2. | Особенности реализации функций безопасности среды функционирования СДЗ «TSM»..... | 17 |
| 3. | Безопасная установка и настройки СДЗ «TSM» | 19 |
| 3.1. | Правила безопасной работы администратора СДЗ | 19 |
| 3.2. | Правила безопасной работы пользователя | 19 |
| 3.3. | Разграничение ролей пользователей в СДЗ «TSM» | 20 |
| 3.4. | Функции администратора | 20 |
| 3.5. | Описание логической структуры СДЗ «TSM»..... | 21 |
| 3.6. | Этап инициализации данных СДЗ «TSM» | 22 |
| 3.7. | Этап идентификации и аутентификации пользователя | 24 |
| 3.8. | Администрирование СДЗ..... | 24 |
| 3.9. | Контроль целостности разделов файловой системы..... | 25 |
| 4. | Вход на защищенное средство вычислительной техники..... | 28 |
| 4.1. | Ситуации, возникающие при входе в СВТ..... | 32 |
| 4.2. | Разблокировка доступа к СДЗ..... | 34 |
| 5. | Администрирование СДЗ «TSM» | 37 |
| 5.1. | Описание пункта меню «Контроль» | 39 |
| 5.1.1. | Описание подпункта меню «Области» | 39 |
| 5.1.2. | Описание подпункта меню «Разделы» | 40 |
| 5.1.3. | Описание подпункта меню «Файлы ОС» | 44 |
| 5.1.4. | Описание подпункта меню «Файлы СДЗ» | 45 |
| 5.2. | Описание пункта основного меню «Тестирование» | 46 |
| 5.2.1. | Описание подпункта меню «Системное» | 47 |

| | |
|--|-----|
| 5.2.2. Описание подпункта меню «ФБО» | 48 |
| 5.3. Описание пункта меню «Пользователи» | 49 |
| 5.3.1. Управление учетными записями пользователей | 49 |
| 5.3.2. Создание учетной записи | 51 |
| 5.3.3. Удаление учетной записи пользователя | 52 |
| 5.3.4. Смена пароля пользователя | 53 |
| 5.3.5. Продление действия пароля пользователя | 55 |
| 5.3.6. Привязка токена к учетной записи пользователя | 56 |
| 5.3.7. Наделение пользователя правами администратора | 56 |
| 5.3.8. Управление доступом пользователя к разделам ЗН | 57 |
| 5.3.9. Блокировка и разблокировка пользователя | 58 |
| 5.3.10. Сообщения, возникающие при управлении учетной записью пользователя | 60 |
| 5.4. Описание пункта меню «Действия» | 62 |
| 5.5. Регистрация и аудит | 64 |
| 5.5.1. Описание пункта меню «Журнал аудита» | 64 |
| 5.5.2. Механизм фильтрации записей в журнале аудита | 66 |
| 5.5.3. Аудит безопасности | 68 |
| 5.6. Описание пункта меню «Обновление» | 70 |
| 5.6.1. Описание подпункта меню «СДЗ «TSM»» | 70 |
| 5.6.2. Описание подпункта меню «Резервные копии» | 72 |
| 5.6.3. Описание подпункта меню «Файловые системы» | 78 |
| 5.6.4. Описание подпункта меню «Таблица разделов» | 80 |
| 5.7. Описание пункта меню «Настройки» | 83 |
| 5.7.1. Описание подпункта меню «Аутентификация» | 83 |
| 5.7.2. Описание подпункта меню «Дата и время» | 89 |
| 5.7.3. Описание подпункта меню «Файлы ОС» | 90 |
| 5.7.4. Описание подпункта меню «Восстановление» | 92 |
| 5.7.5. Описание подпункта меню «Управление» | 94 |
| 5.7.6. Описание подпункта меню «Разное» | 98 |
| 6. Выход из графического интерфейса администрирования СДЗ «TSM» | 100 |
| ПРИЛОЖЕНИЕ А | 101 |
| ПРИЛОЖЕНИЕ Б | 105 |

СОКРАЩЕНИЯ

| | |
|-----------|---|
| ВКЛ | Включить |
| ВЫКЛ | Выключить |
| ЗН | Загрузочный носитель |
| КС | Контрольная сумма |
| ОЗУ | Оперативное запоминающее устройство |
| ОО | Оцениваемый образец |
| ОС | Операционная система |
| ПЗУ | Постоянное запоминающее устройство |
| ПО | Программное обеспечение |
| СВТ | Средство вычислительной техники |
| СДЗ | Средство доверенной загрузки |
| СДЗ «TSM» | Средство доверенной загрузки «Trusted Security Module» |
| СПО | Системное программное обеспечение |
| ФБО | Функции безопасности объекта оценки |
| ФС | Файловая система |
| eMMC | Embedded Multimedia Memory Card – мультимедийная карта памяти, монтируемая на печатную плату. Эквивалентная SD-карте по функциям |
| FAT | File Allocation Table — файловая система, широко применяемая в ОС Windows |
| HDMI | High Definition Multimedia Interface — мультимедиа-интерфейс высокой четкости, цифровой интерфейс для подключения мониторов и телевизоров |
| MBR | Master Boot Record - Главная загрузочная запись |
| RO | Read only – режим доступа «только для чтения» |
| RW | Read write – режим доступа «чтение и запись» |
| SD | Secure Digital Memory Card |
| TEE | Trusted Execution Environment – «Доверенная среда исполнения» |
| USB | Universal Serial Bus — «Универсальная последовательная шина» |

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

| | |
|------------------------------|---|
| Аудит | Независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям и предоставляет результаты в виде рекомендаций |
| Аутентификация | Проверка подлинности предъявленного пользователем идентификатора |
| Графический интерфейс | Система средств для взаимодействия пользователя с компьютером, основанная на представлении всех доступных пользователю системных объектов и функций в виде графических компонентов экрана (окон, значков, меню, кнопок, списков и т. п.). |
| Двухфакторная аутентификация | Метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов |
| Идентификация | Процесс распознавания субъекта в компьютерной системе или на веб-ресурсе при помощи анализа его идентификатора |
| Инициализация | Создание, активация, подготовка к работе, определение параметров. Приведение программы или устройства в состояние готовности к использованию |
| Контроль целостности | Процесс означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение |
| Контрольная сумма | Некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении. |
| Логин | Имя учётной записи пользователя в компьютерной системе |
| Несанкционированный доступ | Доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации |

| | |
|----------------------|--|
| Операционная система | Комплекс программ, обеспечивающий управление аппаратными средствами компьютера, организующий работу с файлами и выполнение прикладных программ, осуществляющий ввод и вывод данных. |
| Специальная область | Область данных или кода ФБО СДЗ «TSM» |
| Токен | Компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удалённого доступа к информационным ресурсам и т. д. |
| Трастлет | Приложение, работающее в доверенной среде исполнения |
| Файловая система | Компонент операционной системы, реализующий структурированное хранение данных на носителях информации в виде файлов и каталогов, и предоставляющий доступ к этим данным для ОС и приложений. |
| Чек-бокс | Элемент графического пользовательского интерфейса, позволяющий пользователю управлять параметром с двумя состояниями — включено и выключено. |
| Ядро ОС | Центральная часть операционной системы (ОС), обеспечивающая приложениям координированный доступ к ресурсам компьютера, таким как процессорное время, память, внешнее аппаратное обеспечение, внешнее устройство ввода и вывода информации. |
| ARM-процессор | Микропроцессор основанный на ядре ARM |
| Ethernet | Доминирующая технология проводных локальных сетей |
| USB-порт | Последовательный интерфейс для подключения периферийных устройств к вычислительной технике |

АННОТАЦИЯ

Данное руководство предназначено для всех пользователей, отвечающих за администрирование и эксплуатацию средства доверенной загрузки «TRUSTED SECURITY MODULE» для программно-аппаратного комплекса «Доверенная платформа» на базе ARM-процессоров (далее по тексту СДЗ «TSM»).

В настоящем руководстве приведены сведения об эксплуатации СДЗ «TSM», дано подробное описание графического интерфейса администрирования СДЗ «TSM», представлены сведения о конфигурировании параметров СДЗ и пользователей.

1.ОБЩИЕ СВЕДЕНИЯ

1.1. Обозначение и наименование

Полное наименование программного изделия: Средство доверенной загрузки «TRUSTED SECURITY MODULE» для программно-аппаратного комплекса «Доверенная платформа» на базе ARM-процессоров.

Краткое наименование программного изделия: СДЗ «TSM».

Обозначение изделия: RU.АЛДЕ.02.13.022-01 94 01.

Разработчик и изготовитель: ЗАО «Аладдин Р.Д.».

Юридический адрес: 129226, г. Москва, ул. Докукина, дом 16.

Почтовый адрес: 129226, г. Москва, ул. Докукина, дом 16 строение 1.

Телефоны: +7 (495) 223-0001, +7 (495) 988-4640.

Факс: +7 (495) 646-0882.

1.2. Назначение СДЗ «TSM»

Средство доверенной загрузки «Trusted Security Module» для программно-аппаратного комплекса «Доверенная платформа» на базе ARM-процессоров предназначено для управления доступом пользователей¹ к процессу загрузки операционной системы средств вычислительной техники и обеспечивает невозможность подключения нарушителя в разрыв между загрузчиком, средством доверенной загрузки и штатной операционной системой средств вычислительной техники для осуществления несанкционированного доступа.

Средство доверенной загрузки «Trusted Security Module» применяется как элемент систем защиты информации автоматизированных (информационных) систем. Средство доверенной загрузки используется в составе средств вычислительной техники совместно с другими средствами защиты информации для предотвращения несанкционированного доступа к информации в автоматизированных (информационных) системах.

Средство доверенной загрузки «Trusted Security Module» соответствует 2 классу защиты и обеспечивает выполнение требований к функциям безопасности, установ-

¹ Пользователь – физическое лицо, являющееся сотрудником (работником) владельца программного средства, которое на законных основаниях (правомерно) по разрешению (поручению) владельца непосредственно эксплуатирует программное средство.

ленных нормативным документом «Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам доверенной загрузки)»² и методическим документом «ИТ.СДЗ.УБ2.ПЗ Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты»³.

Средство доверенной загрузки «Trusted Security Module» может применяться при обработке информации, содержащей сведения со степенью секретности «совершенно секретно», и использоваться при реализации требований по защите информации от несанкционированного доступа для автоматизированных систем классов защищенности 1Б, 2А, 3А⁴.

Средство доверенной загрузки «Trusted Security Module» может применяться:

- при реализации мер защиты в государственных информационных системах до 1 класса защищенности включительно;
- при обеспечении до 1-го уровня защищенности персональных данных, включительно, при их обработке в информационных системах персональных данных;
- при реализации мер защиты в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1 класса защищенности включительно.

1.3. Основные возможности и функции СДЗ «TSM»

СДЗ «TSM» предназначено для защиты СВТ от следующих угроз безопасности информации:

- 1) Несанкционированного доступа к информации при загрузке нештатной ОС, в обход правил разграничения доступа штатной ОС и (или) других

² Нормативный документ утвержден приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 27.09.2013 г. № 119дсп.

³ Методический документ утвержден Федеральной службой по техническому и экспортному контролю Российской Федерации 30.12.2013 г. и введен в действие с 30.12.2014.

⁴ За исключением автоматизированных систем классов защищенности 2А, 3А, в которых обрабатывается информация, содержащая сведения со степенью секретности «особой важности».

СЗИ, работающих в среде штатной ОС;

- 2) Несанкционированной загрузки штатной ОС и получение несанкционированного доступа к информационным ресурсам;
 - 3) Нарушения целостности программной среды СБТ и (или) состава компонентов аппаратного обеспечения СБТ в информационной системе;
 - 4) Нарушения целостности ПО СДЗ «TSM»;
 - 5) Отключения и (или) обхода нарушителями СДЗ «TSM»;
 - 6) Несанкционированного изменения конфигурации (параметров) СДЗ «TSM»;
 - 7) Преодоления или обхода функций СДЗ «TSM» идентификация (аутентификация) за счет недостаточного качества аутентификационной информации;
 - 8) Получения остаточной информации СДЗ «TSM» из памяти СБТ после завершения работы СДЗ «TSM»;
 - 9) Получения доступа к ресурсам СДЗ «TSM» из программной среды СБТ после завершения работы средства доверенной загрузки;
 - 10) Отключения (обход) или блокирования базовой системы ввода-вывода.
- СДЗ «TSM» реализует следующие функции безопасности:

- 1) Аудит безопасности, обеспечивает:
 - регистрацию и учет выполнения функций безопасности объекта оценки;
 - сигнализацию о событиях, связанных с нарушением безопасности;
 - выполнение действий в случае обнаружения возможного нарушения безопасности.
- 2) Идентификация и аутентификация, обеспечивает:
 - идентификацию и аутентификацию пользователей до выполнения ими любых действий;
 - идентификацию и аутентификацию уполномоченных пользователей с ролью «администратор» до выполнения ими любых действий, выполняемых при посредничестве функций безопасности объекта оценки;
 - применение различных механизмов аутентификации;
 - проверку аутентификационной информации на соответствие установленным критериям;

- защиту обратной связи с пользователем во время его аутентификации;
- обработку отказов аутентификации.

3) Доверенная загрузка, обеспечивает:

- контроль целостности данных функций безопасности объекта оценки;
- контроль целостности загрузочных модулей (выполняемого кода) объекта оценки;
- самопроверку исправности (самотестирование) функций безопасности объекта оценки;
- контроль целостности программных средств и компонентов технического (аппаратного) обеспечения средства вычислительной техники;
- очистка остаточной информации объекта оценки до завершения его работы;
- загрузка штатной операционной системы, если идентификация и аутентификация пользователя, контроль целостности и самопроверка дали положительный результат и отсутствуют попытки загрузки нештатной операционной системы и критичные сбои или ошибки в функционировании объекта оценки;
- блокировка загрузки операционной системы, если идентификация и аутентификация пользователя, контроль целостности и самопроверка объекта оценки не дали положительного результата, выполнена попытка загрузки нештатной операционной системы или при функционировании объекта оценки возникли критичные сбои или ошибки.

4) Управление работой и параметрами, обеспечивает:

- управление доступом к интерфейсам управления функциями безопасности объекта оценки на основе ролей;
- управление режимами выполнения функций безопасности объекта оценки со стороны уполномоченного пользователя с ролью «администратор»;
- управление данными и ограничениями данных функций безопасности объекта оценки со стороны уполномоченного пользователя с ролью «администратор».

1.4. Состав программных компонентов СДЗ «TSM»

СДЗ «TSM» включает в себя следующие программные компоненты:

- 1) **СПО «Доверенный загрузчик»** - осуществляет, инициализацию периферии микропроцессора в соответствии с параметрами аппаратной платформы. Является первой программной в цепочки доверенной загрузки СВТ. Основная функция - доверенная загрузка СПО «Компонент СДЗ»;
- 2) **СПО «Компонент СДЗ»** - осуществляет защиту СВТ от угроз безопасности и реализует функциональные возможности, перечисленные в п. 1.3 данного руководства пользователя по эксплуатации;
- 3) **Параметры аппаратной платформы** – набор данных, хранящихся в защищенной области, на загрузочном носителе (SD или EMMC) СВТ, требуемые для корректной инициализации СВТ. Используются СПО «Доверенный загрузчик» и СПО «Компонент СДЗ».

Также стоит отметить, что СДЗ «TSM» работает совместно с:

- 1) **СПО «Доверенная среда исполнения»**, которая осуществляет контроль доступа ОС и программ пользователя к ресурсам СВТ через использование технологии ARM TrustZone. Основные функции - осуществление невозможности действий, направленных на нарушение физической целостности СВТ, предоставление среды исполнения и интерфейса для удаленного управления и обновления СДЗ «TSM»;
- 2) **Трастлет удаленного управления компонентом СДЗ и предоставления доверенного канала** - служит для обеспечения доверенного канала при удаленном управлении ОО и взаимодействии с другими средствами защиты информации и доверенного маршрута при взаимодействии с уполномоченным объектом.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Общие положения

СДЗ «TSM» может применяться на мобильных устройствах, а также на разнообразных контроллерах – сетевых, для техпроцессов, миникомпьютеров, POS-терминалов, разработанных на архитектуре ARM. СДЗ «TSM» поставляется в предустановленном виде, как ПО интегрированное в аппаратуру заказчика.

СДЗ «TSM» может функционировать, как на автономных СБТ, так и на СБТ в составе локальной вычислительной сети.

Для функционирования компонентов СДЗ «TSM» требуются СБТ, обладающие следующими аппаратными и программными требованиями:

1) Аппаратные требования:

- Наличие SD/microSD или eMMC;
- Наличие разъема/интерфейса USB 2.0 (тип A/B);
- Дисплей с сенсорным экраном или HDMI (для подключения дисплея) + USB-мышь;
- Сетевой интерфейс (для обеспечения процедур обновления СДЗ «TSM»).
- Микропроцессор – ARM-процессоры серии i.MX6 производства NXP Semiconductors N.V.: i.MX6 Solo, i.MX6 DualLite, i.MX6 Dual, i.MX6 Quad;
- Объем ОЗУ – от 128 Мбайт до 4 Гбайт;
- Объем ПЗУ – от 32 Мбайт до 160 Мбайт

2) Программные требования

СДЗ «TSM» предназначена для доверенной загрузки ОС следующих типов unix-подобных ОС общего назначения: Linux (Debian, Ubuntu, Astra Linux и др.), Android, Sailfish, Tizen.

СДЗ применяется с любыми типами ФС на устройстве-носителе (внешняя SD-карта или встроенная микросхема eMMC) с которого загружается.

Примечание. СДЗ «TSM» может встраиваться в уже работающие системы, поддерживающие MBR разбиение диска на разделы, наделяя их дополнительными возможностями по обеспечению информационной безопасности.

2.2. Особенности приемки и реализации функций безопасности среды функционирования СДЗ «TSM»

2.2.1. Особенности приемки СДЗ «TSM»

Конструктивные особенности СДЗ «TSM», как средства доверенной загрузки уровня базовой системы ввода-вывода, обуславливают необходимость его генерации с использованием специализированного технологического оснащения в порядке, определенном документированными технологическими процедурами изготовителя (производителя).

СДЗ «TSM» поставляется владельцу программного средства как программа в составе программно-аппаратного комплекса «Доверенная платформа» в порядке, определенном документом «RU.АЛДЕ.02.13.022-01 91 01 Средство доверенной загрузки «Trusted Security Module» для программно-аппаратного комплекса «Доверенная платформа» на базе ARM-процессоров. Поставка и эксплуатация. Обнаружение модификации. Руководство». Самостоятельная установка СДЗ «TSM» на средства вычислительной техники пользователем (владельцем программного средства) не предусмотрена. Программа в составе программно-аппаратного комплекса «Доверенная платформа» идентична программе на носителе оптической записи из комплекта поставки. Идентичность средства доверенной загрузки обеспечивается изготовителем (производителем) при генерации с использованием специализированного технологического оснащения в порядке, определенном документированными технологическими процедурами.

Каждый единичный СДЗ «TSM» маркируется номером программного средства предприятия и знаком соответствия системы сертификации средств защиты информации по требованиям безопасности информации (рег. № РОСС RU.0001.01БИ00). Способ маркировки зависит от количества изделий в поставке.

При приемке единичных образцов СДЗ «TSM» необходимо проверить:

– наличие номера программного средства предприятия, который указывается:

1) в эксплуатационном документе «RU.АЛДЕ.02.13.022-02 30 01 Средство доверенной загрузки «Trusted Security Module» для программно-аппаратного комплекса «Доверенная платформа» на базе ARM-процессоров. Формуляр. Приложение 1. Свидетельство о приемке, упаковке и маркировке». Номер программного средства предприятия должен быть приведен в разделе «2 Общие сведения» и в разделе «7 Свидетельство об упаковке и маркировке»;

2) на корпусе программно-аппаратного комплекса «Доверенная платформа». Номер программного средства предприятия должен обозначаться штрих-кодом типа Data matrix на самоклеящейся этикетке (Рисунок 1);

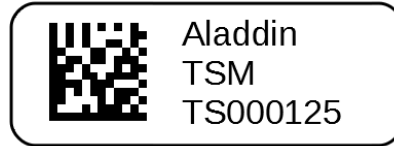


Рисунок 1 – Общий вид самоклеящейся этикетки со штрих-кодом, содержащим номер программного средства предприятия

3) на креплении носителя оптической записи в индивидуальной упаковке средства доверенной загрузки. Номер программного средства предприятия должен обозначаться штрих-кодом типа Data matrix на самоклеящейся этикетке (Рисунок 1).

– наличие знака соответствия системы сертификации средств защиты информации по требованиям безопасности информации должен быть размещен в эксплуатационном документе «RU.АЛДЕ.02.13.022-01 30 01 Средство доверенной загрузки «Trusted Security Module» для программно-аппаратного комплекса «Доверенная платформа» на базе ARM-процессоров. Формуляр» в разделе «7 Свидетельство об упаковке и маркировке».

При приемке партии единичных образцов изделия для каждого единичного образца необходимо проверить:

– номер программного средства предприятия, который указывается:

1) в эксплуатационном документе «RU.АЛДЕ.02.13.022-01 30 01-02 Средство доверенной загрузки «Trusted Security Module» для программно-аппаратного комплекса «Доверенная платформа» на базе ARM-процессоров. Формуляр. Приложение» в графе «Номер программного средства предприятия»;

2) на корпусе программно-аппаратного комплекса «Доверенная платформа» каждого единичного образца СДЗ «TSM». Номер программного средства предприятия должен обозначаться штрих-кодом типа Data matrix на самоклеящейся этикетке (Рисунок 1).

– знак соответствия системы сертификации средств защиты информации по требованиям безопасности информации должен быть размещен на корпусе программно-аппаратного комплекса «Доверенная платформа» каждого единичного образца СДЗ «TSM».

При поставке партии единичных образцов изделий соотношение между номером программного средства предприятия и знаком соответствия системы сертификации средств защиты информации по требованиям безопасности информации фиксируется в документе «RU.АЛДЕ.02.13.022-01 30 01-02 Средство доверенной загрузки «Trusted Security Module» для программно-аппаратного комплекса «Доверенная платформа» на базе ARM-процессоров. Формуляр. Приложение» в графах «Номер программного средства предприятия» и «Номер знака соответствия системы сертификации средств защиты информации по требованиям безопасности информации».

При приемке партии единичных образцов изделий необходимо проверить номер партии, который указывается на креплении носителя оптической записи в индивидуальной упаковке СДЗ «TSM». Данный номер партии также указывается в документе «RU.АЛДЕ.02.13.022-01 30 01-02 Доверенная платформа» на базе ARM-процессоров. Формуляр. Приложение» в графе «Примечание».

При приемке особое внимание необходимо обратить внимание на отсутствие следов нарушений в нанесении знака соответствия системы сертификации средств защиты информации по требованиям безопасности информации.

Первый запуск СДЗ «TSM» во время приемки должен выполняться в соответствии с разделом» 3.6 Этап инициализации данных СДЗ «TSM» настоящего документа.

Если при поставке средства доверенной загрузки возникнет необходимость его проверки как программы на носителе оптической записи, то контроль целостность можно выполнить с использованием программы «ФИКС» версии 2.0.2⁵ (Сертификат соответствия на № 1548 от 15.01.2008 г., техническая поддержка до 15.01.2025 г.) путем расчета контрольных сумм файлов на носителе оптической записи и сравнением их со значениями, указанными в документе «RU.АЛДЕ.02.13.022-01 30 01 Средство доверенной загрузки «Trusted Security Module» для программно-аппаратного комплекса «Доверенная платформа» на базе ARM-процессоров. Формуляр». Значения контрольных сумм, полученные при расчете должны совпасть со значениями указанными в документе.

⁵ Программное средство «ФИКС» не входит в комплект поставки средства доверенной загрузки.

2.2.2. Особенности реализации функций безопасности среды функционирования СДЗ «TSM»

Средой функционирования для средства доверенной загрузки «Trusted Security Module» является программно-аппаратный комплекс «Доверенная платформа», который используется в составе средств вычислительной техники. Программно-аппаратный комплекс «Доверенная платформа» функционирует на базе следующих ARM-процессоров серии i.MX6 производства NXP Semiconductors N.V:

- i.MX6 Solo;
- i.MX6 DualLite;
- i.MX6 Dual;
- i.MX6 Quad.

Дополнительно программно-аппаратный комплекс «Доверенная платформа» должен иметь в своем составе:

- оперативное запоминающее устройство объемом от 128 Мбайт до 4 Гбайт;
- постоянное запоминающее устройство от 32 Мбайт до 160 Мбайт;
- машинный носитель информации (карты памяти SD/microSD или eMMC);
- интерфейс HDMI для подключения дисплея или дисплей с сенсорным экраном;
- часы реального времени, которые подключены к встроенному элементу электрического питания;
- интерфейс проводной локальной вычислительной сети (технология Ethernet⁶) и/или интерфейс беспроводной локальной вычислительной сети (технология Wi-Fi⁷) и/или интерфейс беспроводной высокоскоростной передачи данных сети подвижной радиотелефонной связи 3 или 4 поколения (3G/4G)⁸.



Примечание – Возможность использования интерфейса беспроводной локальной вычислительной сети и интерфейса беспроводной высокоскоростной передачи данных в автоматизированных (информационных) системах (и, соответственно, необходимость их наличия в средствах вычислительной техники), должна определяться в соответствии с нормативными правовыми актами и нормативными документами.

Для подключения токена, используемого при аутентификации пользователя, программно-аппаратный комплекс «Доверенная платформа» должен включать USB-интерфейс, как минимум, соответствующий спецификации «Universal Serial Bus Specification Revision 2.0».

⁶ Технология Ethernet определяется семейством стандартов IEEE 802.3.

⁷ Технология Wi-Fi определяется семейством стандартов IEEE 802.11.

⁸ Технология беспроводной высокоскоростной передачи данных определяется рекомендациями ITU-R серии М и техническими спецификациями 3GPP TS Rel.9 и 3GPP TS Rel.11.

В среде функционирования во время работы средства доверенной загрузки не содержится других системных, системных управляющих или прикладных программ. Настройка функций безопасности среды функционирования не требуется.

3. БЕЗОПАСНАЯ УСТАНОВКА И НАСТРОЙКИ СДЗ «TSM»

При работе с СДЗ «TSM» должны быть приняты организационные (организационно-технические) меры, исключая неконтролируемый доступ посторонних лиц к СВТ пользователя в нерабочее время, а также в рабочее время при отсутствии пользователя.

3.1. Правила безопасной работы администратора СДЗ

Администратор СДЗ должен работать в соответствии с документом «Средство доверенной загрузки «Trusted security module» для программно-аппаратного комплекса «Доверенная платформа» на базе ARM-процессоров. Руководство пользователя по эксплуатации» (данное руководство) и, прежде всего, ознакомиться с ним.

Администратор СДЗ обязан соблюдать следующие правила:

- 1) При первичном входе в графический интерфейс администрирования СДЗ «TSM», пользователю с ролью администратор СДЗ, рекомендуется заменить установленный в нем пароль для защиты доступа;
- 2) Осуществлять своевременную смену пароля в соответствии с политикой безопасности организации;
- 3) При вводе пароля исключать возможности визуального просмотра его набора другими лицами;
- 4) На случай утери пароля администратора либо токена и невозможности доступа к учетной записи администратора, рекомендуется задать код разблокировки. Код разблокировки хранить в защищенном месте и не использовать без крайней необходимости;
- 5) При наличии токена у администратора СДЗ, не передавать его другим лицам, а также не оставлять его без присмотра. Попадание токена в чужие руки несет опасность его компрометации;
- 6) При утере токена следует немедленно присвоить новый токен учетной записи администратора СДЗ;
- 7) Беречь токен от механических повреждений.

3.2. Правила безопасной работы пользователя

Пользователь обязан соблюдать следующие правила:

- 1) При первичной аутентификации пользователя, рекомендуется заменить

- установленный пароль для защиты доступа к компьютеру, при условии, если администратор СДЗ включил данную функцию для пользователя;
- 2) Осуществлять своевременную замену пароля своей учетной записи в соответствии с политикой безопасности организации, при условии, если администратор СДЗ включил данную функцию для пользователя;
 - 3) При вводе пароля исключать возможность визуального просмотра его набора другими лицами;
 - 4) При наличии токена у пользователя, не передавать его другим лицам, а также не оставлять его без присмотра. Попадание токена в чужие руки несет опасность его компрометации;
 - 5) При утере токена немедленно сообщить об этом администратору;
 - 6) Беречь токен от механических повреждений.

3.3. Разграничение ролей пользователей в СДЗ «TSM»

В СДЗ «TSM» полномочия на эксплуатацию и администрирование определяется ролью пользователя.

В зависимости от представленных полномочий, каждый пользователь может быть отнесен к одной из двух ролей:

- 7) «Администратор СДЗ» – пользователь, наделенный всеми правами на администрирование СДЗ «TSM»;
- 8) «Пользователь» – пользователь, допущенный к пользованию СВТ и не обладающий правами по управлению СДЗ «TSM».

3.4. Функции администратора

В общем случае, администратор СДЗ в рамках своих полномочий должен выполнять следующие функции:

- 9) Управление регистрацией учётных записей пользователя: создание и удаление учетных записей;
- 10) Изменение параметров учетной записи пользователей;
- 11) Работа с журналом аудита на предмет выявления возможных нарушений безопасности;
- 12) Управление работой пользователей;
- 13) Мониторинг и управление параметрами контроля целостности.

14) Настройка параметров СДЗ «TSM», обеспечивающие корректную и безопасную работу.

3.5. Описание логической структуры СДЗ «TSM»

Реализуя функции безопасности, СДЗ «TSM» обеспечивает последовательное выполнение следующих этапов работы:

- 1) Запуск;
- 2) Инициализации данных СДЗ «TSM»;
- 3) Идентификация и аутентификация пользователя:
 - Аутентификация пользователя;
 - Аутентификация администратора;
- 4) Администрирование СДЗ;
- 5) Контроль целостности разделов ЗН;
- 6) Загрузка ОС.

Взаимодействие этапов показано на рисунке 2.

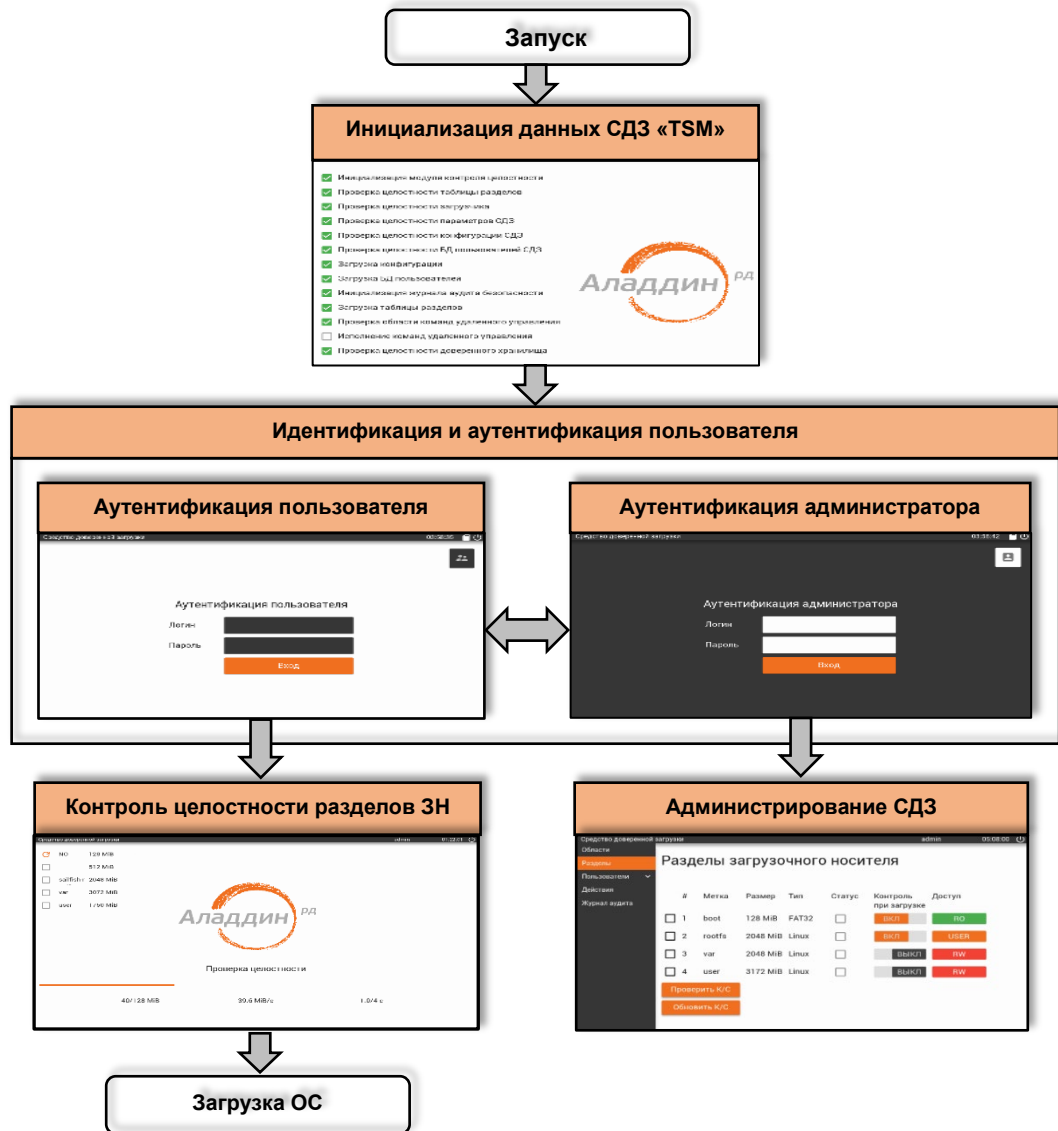


Рисунок 2 - Алгоритм работы СДЗ «TSM»

3.6. Этап инициализации данных СДЗ «TSM»

Этап инициализации данных СДЗ «TSM» осуществляется при запуске СВТ и обеспечивает самотестирование СДЗ, в том числе проверку контроля целостности специальных областей.

При выполнении контроля целостности используется метод сравнения, для этого последовательно считываются все секторы специальных областей, далее по ним рассчитывается КС и проверяются на соответствие с сохраненной на ЗН.

Для подсчета контрольных сумм специальных областей используется алгоритм ГОСТ Р 34.11-2004.

Если инициализация выполнена успешно, пользователю предоставляется возможность пройти авторизацию в новом окне.

В случае, если при инициализации данных КС не совпали, СДЗ информирует пользователя о том, что проверка целостности не пройдена и дальнейший вход возможен только пользователю с ролью администратора СДЗ.

Последовательность и название выполняемых проверок на этапе инициализации данных СДЗ «TSM», а также возможный исход при ошибке представлен в таблице 1.

Таблица 1 – Выполняемые проверки при инициализации данных СДЗ «TSM»

| № п/п | Название проверки | Возможный исход при ошибке |
|-------|--|--------------------------------|
| 1 | Инициализация журнала аудита безопасности | Аварийное выключение |
| 2 | Инициализация модуля контроля целостности | Аварийное выключение |
| 3 | Проверка идентичности платформы | Аварийное выключение |
| 4 | Проверка целостности таблицы разделов (специальная область В0) | Вход только администратора СДЗ |
| 5 | Проверка целостности загрузчика (специальная область В1) | Вход только администратора СДЗ |
| 6 | Проверка целостности параметров СДЗ (специальная область В2) | Вход только администратора СДЗ |
| 7 | Проверка целостности конфигурации СДЗ (специальная область В3) | Вход только администратора СДЗ |
| 8 | Проверка целостности БД пользователей СДЗ (специальная область В4) | Вход только администратора СДЗ |
| 9 | Загрузка конфигурации | Вход только администратора СДЗ |
| 10 | Загрузка БД пользователей | Аварийное выключение |
| 11 | Контроль переполнения журнала аудита безопасности | Вход только администратора СДЗ |
| 12 | Тестирование аппаратного обеспечения | Вход только администратора СДЗ |
| 13 | Загрузка таблицы разделов | Аварийное выключение |
| 14 | Проверка области команд удаленного управления | Пропуск и дальнейшая загрузка |
| 15 | Исполнение команд удаленного управления (специальная область В8) | Вход только администратора СДЗ |
| 16 | Проверка целостности доверенного хранилища | Вход только администратора СДЗ |

3.7. Этап идентификации и аутентификации пользователя

Этап идентификации и аутентификации осуществляется после успешной инициализации данных СДЗ «TSM» и выполняет авторизацию пользователя СДЗ «TSM».

В зависимости от настройки параметров учетной записи пользователя (см. п. 5.3.6), идентификация и аутентификация выполняется:

- 1) «По имени и паролю» - предусматривает вход пользователя в систему путем ввода логина (имени) и пароля.
- 2) «Двухфакторная» - предусматривает ввод логина и пароля, а также предъявление токена.

Примечание. Для аутентификации в СДЗ «TSM» применяются токены на базе JaCarta.

Процесс идентификации и аутентификации осуществляется через:

- 1) Интерфейс аутентификации пользователя – позволяет любому пользователю, учтенному в СДЗ «TSM», включая администратора СДЗ выполнить загрузку ОС;
- 2) Интерфейс аутентификации администратора – позволяет осуществить вход в графический интерфейс администратора СДЗ «TSM», предусматривающий полное управление всеми функциями и параметрами СДЗ.

В СДЗ «TSM» предусмотрена возможность переключения между интерфейсами аутентификации пользователя и администратора.

В случае положительной идентификации и аутентификации происходит вход пользователя для дальнейшей работы с СБТ, которая соответствует роли пользователя или администратора в СДЗ.

Примечание. При идентификации и аутентификации пользователя в СДЗ «TSM» предусмотрены ограничения при неудачных попытках ввода пароля (см. п. 5.7.1).

3.8. Администрирование СДЗ

Этап администрирования выполняется после успешной аутентификации администратора и предусматривает выполнение следующих функций:

- 1) Контроля целостности специальных областей разделов ЗН;
- 2) Настройки параметров механизма защиты СДЗ «TSM», а также учетных

записей пользователей;

- 3) Контроля выполняемых пользователями действий с целью предотвращения нарушений информационной безопасности.

Выполнение данных функций осуществляется из графического интерфейса администрирования СДЗ «TSM» (см. разд. 4.2).

3.9. Контроль целостности разделов файловой системы

Контроль целостности разделов ЗН выполняется перед загрузкой ОС и предназначен для обеспечения целостности разделов носителя данных с целью исключить возможность загрузки СВТ в случае нештатного изменения разделов ЗН.

Для проведения контроля целостности разделов ЗН используется метод сравнения, для этого последовательно считываются все кластеры (блоки секторов) раздела с ЗН, после чего по ним рассчитываются контрольные суммы. Далее происходит сравнение полученных контрольных сумм с сохраненными на ЗН.

Для подсчета контрольных сумм используются алгоритмы CRC32, хэш ГОСТ Р 34.11-2012, хэш UMAC – 32, - 64, - 128, хэш SHA 256.

В зависимости от того, как выполнено разбиение ЗН, количество и состав разделов ЗН может быть различен (см. Приложение А) и может состоять из следующих объектов, приведенных в таблице 2.

Таблица 2 – Объекты загрузочного носителя

| Объект загрузочного носителя | Описание |
|------------------------------|--|
| Раздел Sys | Это системный раздел СДЗ TSM, на нем хранятся исполняемые файлы СДЗ. Он должен быть первым разделом на ЗН и необходим для работы СДЗ. Форматируется в FAT/FAT32. Раздел SYS не должен быть доступен из ОС ни на чтение, ни на запись |

| | |
|-----------------------|---|
| Раздел RootFS | Это корневая файловая система ОС Linux. Содержит все дерево каталогов (/etc, /lib, /usr и так далее) и большинство или все файлы ОС. В минималистичном сценарии RootFS – единственный раздел с ОС и всеми файлами, включая данные пользователей, и настраивается как Read/Write. В более сложном варианте установки на RootFS сохраняются только исполняемые файлы и библиотеки, а данные пользователей и изменяемые файлы переносятся в другие разделы. В этом случае RootFS может быть Read-Only и это дает преимущество в защищенности |
| Раздел Boot | Содержит файлы для загрузки ОС. СДЗ TSM берет из раздела Boot образ ядра Linux и файл Device Tree. Раздел Boot может отсутствовать, тогда файлы ОС размещаются на Rootfs |
| Файлы для загрузки ОС | Ядро Linux и Device Tree. Могут быть размещены на разделе Boot или Rootfs. Если они размещаются на разделе RootFS, раздел Boot не нужен |
| Раздел Var | Содержит изменяемые файлы, которые в Linux обычно располагаются в каталогах /var и /tmp. Используется при сложном разбиении Linux на Read-Only и Read-Write разделы. Не обязателен для загрузки ОС через TSM |
| Раздел User | Содержит файлы пользователей, которые в Linux обычно располагаются в каталогах /home. Используется при сложном разбиении Linux на Read-Only и Read-Write разделы. Не обязателен для загрузки ОС через TSM. Может быть несколько таких разделов – для разных пользователей |
| Раздел Update | Раздел обновлений. На этом разделе СДЗ TSM может искать обновления, загруженные во время работы ОС. Раздел Update может отсутствовать, тогда обновления могут располагаться в каталоге на другом разделе, например, Var |
| Обновления | Могут располагаться в каталоге на разделе Update или на другом разделе |
| Раздел Swap | Раздел подкачки. Может использоваться или не использоваться. Для систем, работающих с eMMC, его использование не рекомендуется, т.к. интенсивное |

| | |
|-----------------|--|
| | использование подкачки быстро выработает ресурс eMMC. Для работы TSM не требуется |
| Раздел Recovery | Раздел с маленькой ОС восстановления. По сути это минимальный Rootfs, построенный по принципу “все в одном”. Загрузка с rootfs позволяет провести операции по восстановлению разделов основной ОС, выполнить глубокое обновление или провести анализ неисправностей, когда основная ОС не может быть загружена. Запуск с ОС восстановления поддерживается СДЗ TSM напрямую, однако эта функция является отключаемой. Поэтому для работы СДЗ TSM наличие этого раздела не принципиально. Раздел должен включать в себя всю ФС, включая файлы ядра и Device Tree |

Примечание. Количество, состав и порядок разбиение ЗН на разделы зависит от инсталляционного комплекта ОС.

Так же, осуществляется контроль целостности разделов перед загрузкой ОС, при условии, если администратор включил раздел в список проверки целостности.

Целостность раздела ЗН считается нарушенной, если при выполнении контроля целостности разделов ЗН не все контрольные суммы совпали. В данном случае на экран выводится сообщение о нарушении целостности, и дальнейшая загрузка ОС становится невозможна. Для устранения ошибки необходимо вмешательство администратора.

При условии отсутствия ошибок контроля целостности разделов ЗН производится загрузка ОС.

4. ВХОД НА ЗАЩИЩЕННОЕ СРЕДСТВО ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Загрузка СБТ с установленной СДЗ «TSM» начинается с появления экран инициализации данных СДЗ «TSM», информирующий пользователя о результатах проверки данных СДЗ. Внешний вид экрана с результатами инициализации данных СДЗ «TSM» представлен на рисунке 3.

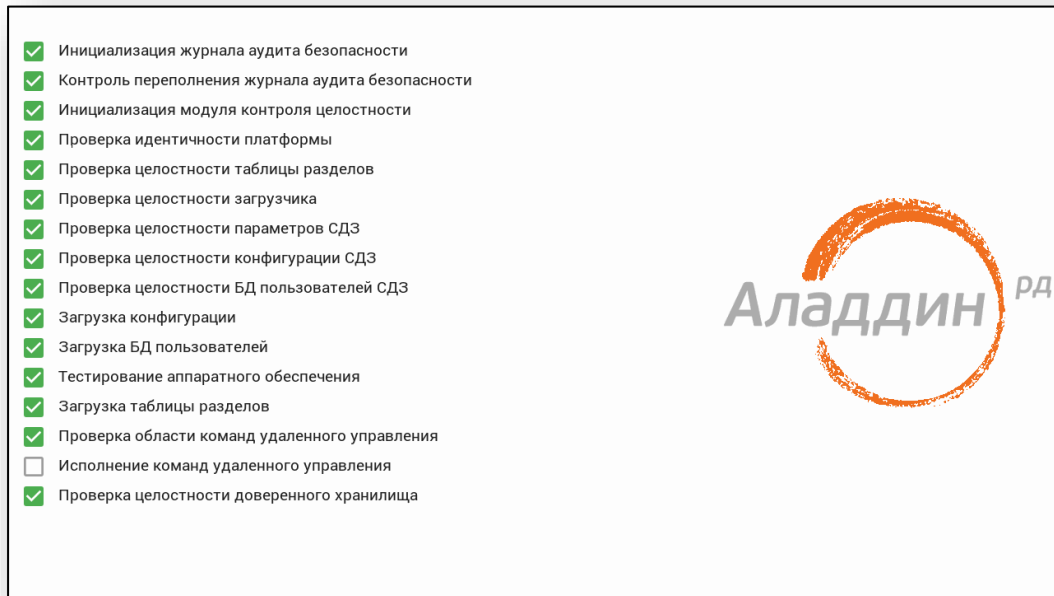


Рисунок 3 - Процесс инициализации данных СДЗ «TSM»

Если в процессе инициализации данных СДЗ «TSM» возникла ошибка, то на экране появляется сообщение, информирующее об обнаружении критической ошибки, и предлагается дальнейшая загрузка СБТ только через графический интерфейс администрирования СДЗ «TSM», в ином случае будет выведено сообщение об автоматическом отключении.

Критическая ошибка проверки целостности данных обозначается восклицательным знаком в круге с красным фоном на соответствующем этапе проверки. Пример обозначения критической ошибки представлен на рисунке .

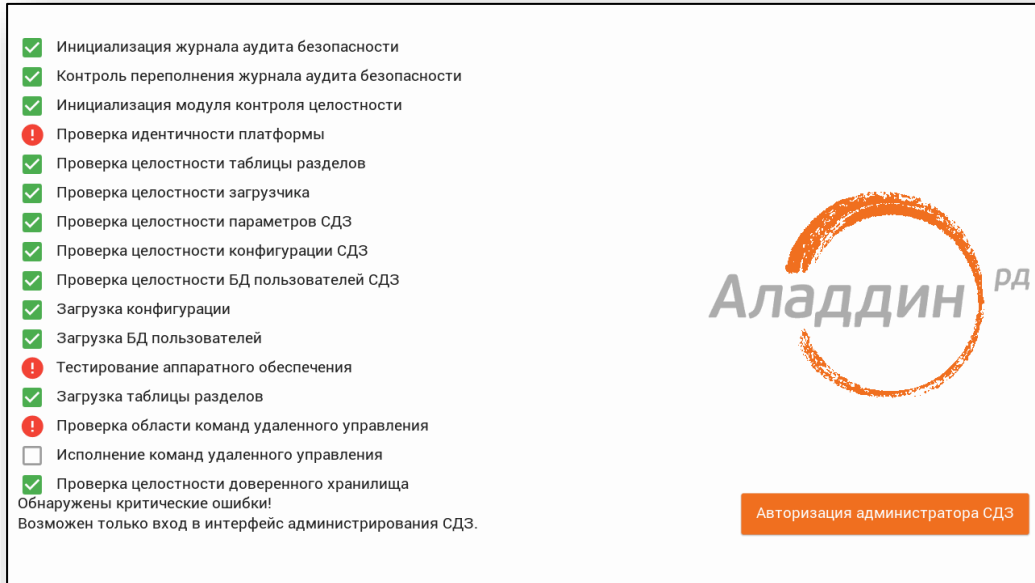


Рисунок 4 - Обнаружение критической ошибки

В случае успешной инициализации данных СДЗ «TSM» на экране появляется диалоговое окно аутентификации пользователя, позволяющее как обычному пользователю, так и пользователю с ролью администратора СДЗ перейти к загрузке ОС (см. рисунок 5).

Примечание. Аутентификационные параметры администратора СДЗ при первом входе: логин - admin, пароль – admin.

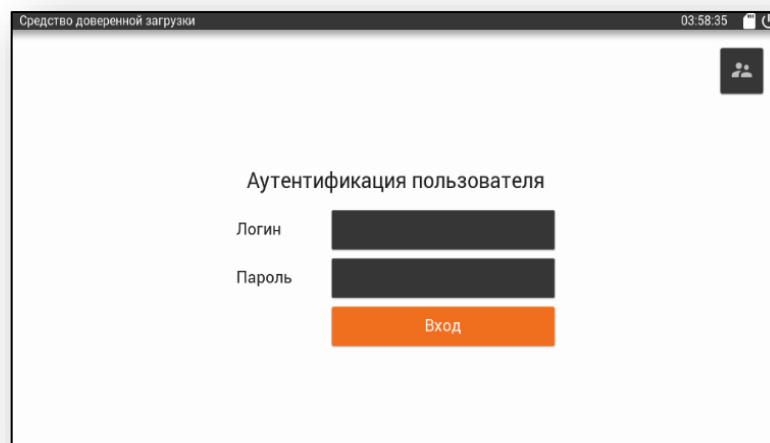



Рисунок 5 - Аутентификация пользователя

При необходимости входа в графический интерфейс администрирования СДЗ «TSM» пользователь СВТ с ролью администратора СДЗ должен переключиться

в режим аутентификации администратора. Для этого в верхнем правом углу экрана нужно нажать кнопку , после чего появится диалоговое окно аутентификации администратора (см. рисунок 6).

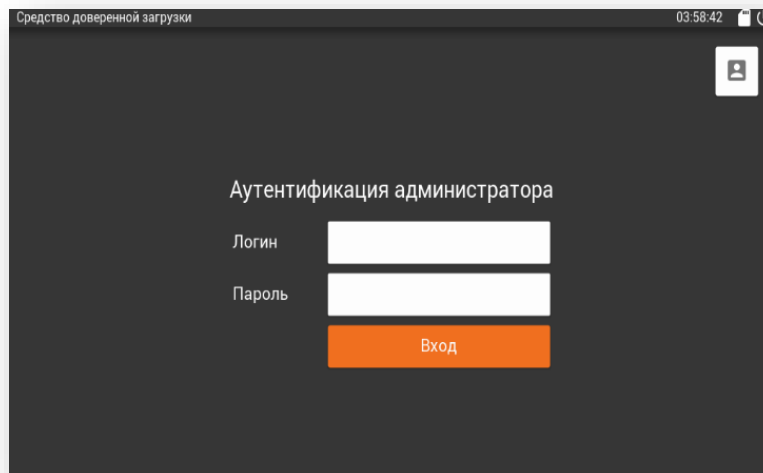




Рисунок 6 – Аутентификация администратора

Для возврата в диалоговое окно аутентификации пользователя следует нажать кнопку , также расположенную в верхнем правом углу экрана.

После выбора режима входа, необходимо ввести логин и пароль учетной записи пользователя СДЗ, после нажать кнопку .

Примечание. При вводе пароля на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «•» (точка). Также следует помнить, что строчные и прописные буквы в пароле различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.

Если логин и пароль были введены неправильно, на экран выводится соответствующее сообщение (см. подраздел 4.1). Пользователь может осуществить повторный ввод данных. При превышении количества неудачных попыток аутентификации осуществляется блокировка СВТ (см. п. 5.7.1).

В случае если для учетной записи установлено требование двухфакторной аутентификации, то после успешного ввода логина и пароля на экран выводится сообщение о предъявлении пользователем СДЗ токена (см. рисунок 7).

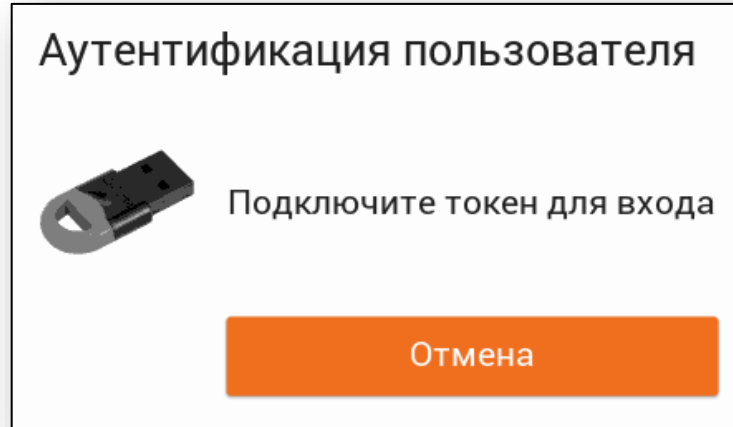


Рисунок 7 – Сообщения о необходимости предъявления токена

Далее происходит загрузка ОС или графического интерфейса администрирования СДЗ «TSM», в зависимости от выбранного режима аутентификации.

Если администратор СДЗ настроил контроль целостности, указав подвергаемый контролю разделы ЗН (см. п. 5.1.2), то на экран перед загрузкой ОС будет выводиться контроль целостности указанных разделов ЗН (см. рисунок 8).

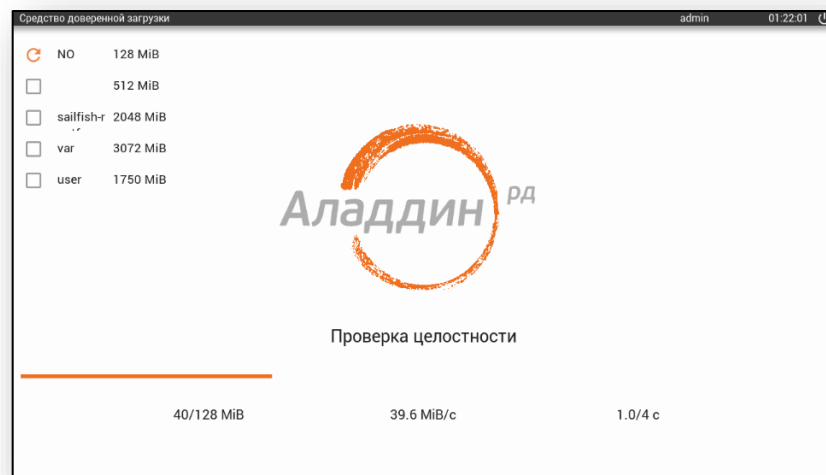


Рисунок 8 – Проверка целостности

При успешном прохождении данного процесса продолжится загрузка ОС.

4.1. Ситуации, возникающие при входе в СВТ

При нарушении правил входа система защиты СДЗ прерывает процедуру входа. Ниже в таблице 3 приведены сообщения защиты при неверных действиях пользователей или сбоях при входе.

Таблица 3 – Список сообщений возникшие при входе в СВТ

| № п/п | Этап | Выводимые сообщения об ошибке | Причина | Действие пользователя |
|-------|--|--|---|--|
| 1 | Процесс инициализации данных СДЗ «TSM» | Обнаружены критические ошибки! Возможен только вход в интерфейс администрирования СДЗ | Обнаружено нарушение целостности в одной из специальных областей | Необходимо выключить СВТ и обратиться к администратору СДЗ для устранения ошибки |
| 2 | Процесс аутентификация | Неверное имя пользователя | Указанное имя пользователя отсутствует в базе данных системы и/или введен неправильный пароль | Проверьте состояние переключателя регистра клавиатуры (верхний/нижний) и переключателя раскладки клавиатуры (рус./лат.). Если допущена ошибка при вводе, повторите ввод имени и пароля. Если вы забыли свой пароль, обратитесь за помощью к администратору СДЗ |
| 3 | | Неверный логин и пароль | | |
| 4 | | Недопустимый пароль | | |
| 5 | | Неверный пароль | | |
| 6 | | Пользователь заблокирован | | |

| | | | | |
|----|--|---|---|---|
| 7 | | Пользователь без прав администратора | Попытка запуска графического интерфейса администрирования СДЗ «TSM» пользователем, не обладающим ролью администратора. Сообщение носит предупреждающий характер | Проверить правильность выбора режима аутентификации (пользователь/администратор) |
| 8 | | Истек срок действия пароля | При входе в СДЗ указан пароль, срок действия которого истек | Обратиться к администратору СДЗ для смены пароля |
| 9 | | Нужен токен для аутентификации | Токен отсутствует в USB-порту | В этом случае необходимо предъявить токен для аутентификации |
| 10 | | Неверный (чужой, неисправный) токен | При входе в СДЗ предъявлен токен, не принадлежащий входящему пользователю или токен испорчен | Предъявить верный токен. Если токен верный, но ошибка устойчиво повторяется, обратитесь за помощью к администратору СДЗ |
| 11 | Процесс контроля целостности разделов ЗН | Ошибка целостности ФС, загрузка ОС не будет выполнена | Нарушена целостность системных данных или пользовательских данных, в результате повреждения информации или ее изменения | Необходимо выключить СВТ и обратиться к администратору СДЗ для устранения ошибки |

4.2. Разблокировка доступа к СДЗ

В ряде случаев доступ к управлению СДЗ может быть утрачен:

- Забыт пароль администратора;
- Утерян токен, используемый для доступа;
- Учетная запись администратора удалена другим пользователем с правами администратора;
- Учетная запись администратора заблокирована;
- Прошел срок действия пароля администратора;
- Неизвестен логин администратора.

В любом из этих случаев восстановление доступа к устройству может быть крайне затруднено либо невозможно. Чтобы избежать таких ситуаций в процессе нормальной эксплуатации, в СДЗ предусмотрена возможность задания кода разблокировки.

Код разблокировки – это пароль длиной от 24 символов и более, который используется вместо пароля администратора для получения доступа к учетной записи администратора СДЗ несмотря на все вышеперечисленные факторы.

Правильный механизм использования кода разблокировки:

- Администратор использует любое средство создание надежных случайных паролей и создает пароль длиной 24 или более символов. Пароль должен соответствовать настроенным в СДЗ политикам безопасности паролей.
- Пароль распечатывается и хранится в сейфе соответствующего класса защищенности (по классу информации, которая обрабатывается в СВТ).
- Можно иметь разные коды разблокировки для каждого устройства, или один код на несколько устройств. При этом, не рекомендуется назначать одинаковые коды разблокировки для устройств, используемых в разных структурных подразделениях, в разных условиях, при работе с разными данными.
- При инициализации устройства администратор безопасности вводит код разблокировки в интерфейсе “Настройки → Аутентификация”.
- Код разблокировки хранится в сейфе и не используется без крайней необходимости.

Порядок разблокировки устройства:

- Включить устройство, попробовать авторизоваться с использованием логина и пароля администратора, если они известны. Если это удалось, процесс разблокировки не нужен.
- Перейти в режим “Аутентификация администратора”.
- Оставить поле “Логин” пустым.
- В поле “Пароль” ввести код разблокировки.
- Нажать кнопку “Вход”.

В процессе разблокировки СДЗ предпримет следующие действия:

- Убедится, что поле “Логин” пусто. Если поле “Логин” заполнено, будет выполнена стандартная процедура аутентификации пользователя;
- Проверит введенный код разблокировки. Если код неверный, будет выдана ошибка “Неверное имя пользователя”, как при неудачной идентификации, и разблокировка не будет произведена.
- Найдет в БД пользователей первого пользователя с правами администратора. Если такого пользователя нет, то создаст пользователя с правами администратора.
- Выполнит вход в интерфейс администрирования СДЗ от имени, найденного или созданного пользователя, несмотря на возможные блокировки.

После входа в интерфейс администрирования СДЗ с использованием кода разблокировки администратор должен самостоятельно перенастроить учетную запись администратора:

- Задать пароль;
- Задать срок действия пароля;
- Если нужно, подключить токен.

Если этого не сделать, учетная запись не будет доступна при следующем входе.

После разблокировки администратор также должен проанализировать настройки СДЗ и журнал событий аудита безопасности.

Примечание. В СВТ АС и ИС и автоматических устройствах на базе СВТ, использующих для восстановления работоспособного состояния СДЗ «TSM» его же встроенные механизмы, должна отсутствовать необходимость обязательного использования усиленной (с использованием и пароля и

токена) аутентификации пользователей СДЗ «TSM» и в составе пользователей СДЗ «TSM» должно быть не более одного пользователя, которому назначена роль «Администратор».

При невозможности выполнения данного условия код разблокировки не должен быть задан, а ранее заданный код разблокировки должен быть сброшен (см. п.7.7.1 ниже).

5. АДМИНИСТРИРОВАНИЕ СДЗ «TSM»

Администрирование выполняется с помощью графического интерфейса администрирования СДЗ «TSM». Запуск интерфейса осуществляется после аутентификации администратора, как указано в разделе 4.

Графический интерфейс администратора позволяет управлять параметрами настройки СДЗ «TSM», работой пользователя, параметрами безопасности и аудита событий, происходящих в СДЗ, просматривать журнал событий.

Внешний вид главного окна графического интерфейса администрирования СДЗ «TSM» представлен на рисунке и содержит следующие рабочие области:

- 1) Заголовок окна, содержащий имя учетной записи администратора СДЗ, текущее время, индикатор наличия в устройстве внешних носителей и кнопку выключения СВТ;
- 2) Основное меню, содержащее следующие пункты: «Контроль», «Тестирование», «Пользователи», «Действия», «Журнал аудита», «Обновление», «Настройки»;
- 3) Рабочую область пункта меню, содержащую списки параметров настройки и элементы управления ими.

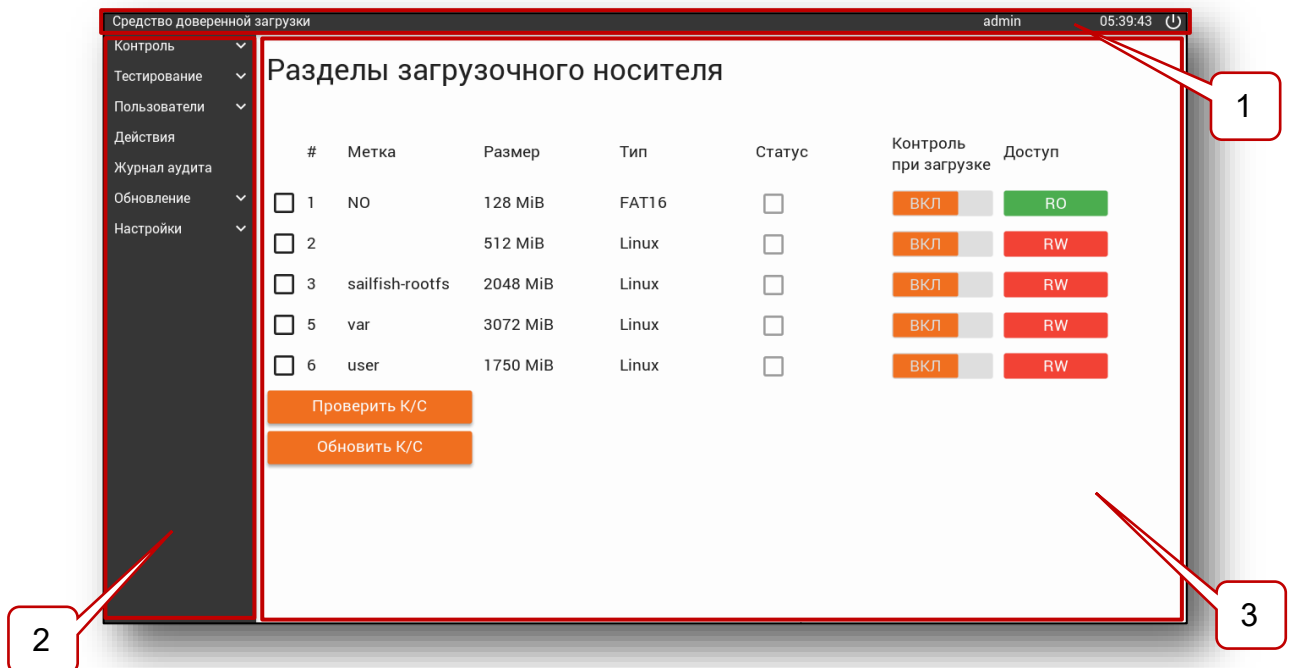


Рисунок 9 - Общий вид графического интерфейса СДЗ «TSM»

Пункты основного меню имеют следующее предназначение:

- 1) Пункт **«Контроль»** предназначен для:
 - мониторинга состояния целостности специальных областей, разделов ЗН, а также объектов ОС и СДЗ «TSM»;
 - штатного пересчёта КС специальных областей, разделов ЗН, объектов ОС и СДЗ «TSM»;
- 2) Пункт **«Тестирование»** предназначен для проведения проверок, которые выполняются в рамках тестирования системных средств и ФБО;
- 3) Пункт **«Пользователи»** предназначен для:
 - создания и удаления учетной записи пользователя;
 - выполнение настройки параметров учетной записи пользователя
- 4) Пункт **«Действия»** предназначен для:
 - загрузки ОС;
 - загрузки ОС восстановления;
 - сохранения конфигурации СДЗ и параметров пользователя;
 - выгрузки журнала аудита на SD;
 - очистки журнала аудита;
- 5) Пункт **«Журнал аудита»** предназначен для:
 - просмотра журнала аудита;
 - сортировки событий;
 - фильтрации событий;
 - аудита безопасности;
- 6) Пункт **«Обновление»** предназначен для:
 - Обновления и восстановление СДЗ;
 - установки, восстановления и обновления ОС;
 - создание и изменения таблицы разделов ЗН;
- 7) Пункт **«Настройки»** предназначен для:
 - настройки аутентификации и качества пароля;
 - установки даты и времени в СДЗ «TSM»;
 - установка расположения разделов и путей к файлам основной ОС и вспомогательной ОС восстановления, с которых они будут загружаться, а также разделу загрузки файлов обновления.

5.1. Описание пункта меню «Контроль»

При выборе пункта основного меню «Контроль», ниже, располагаются подпункты меню:

- 1) «Области»;
- 2) «Разделы»;
- 3) «Файлы ОС»;
- 4) «Файлы СДЗ»

Данные подпункты меню предназначены для выполнения мониторинга и управления контролем целостности специальных областей, разделов ЗН и объектов ОС, а также проведения проверки в рамках тестирования аппаратных средств. Более подробное описание подпунктов меню представлено ниже.

5.1.1. Описание подпункта меню «Области»

При выборе пункта основного меню «Контроль» и перехода в подпункт «Области», на экран выводится интерфейс с отображением состояния всех специальных областей (см. рисунок 10).

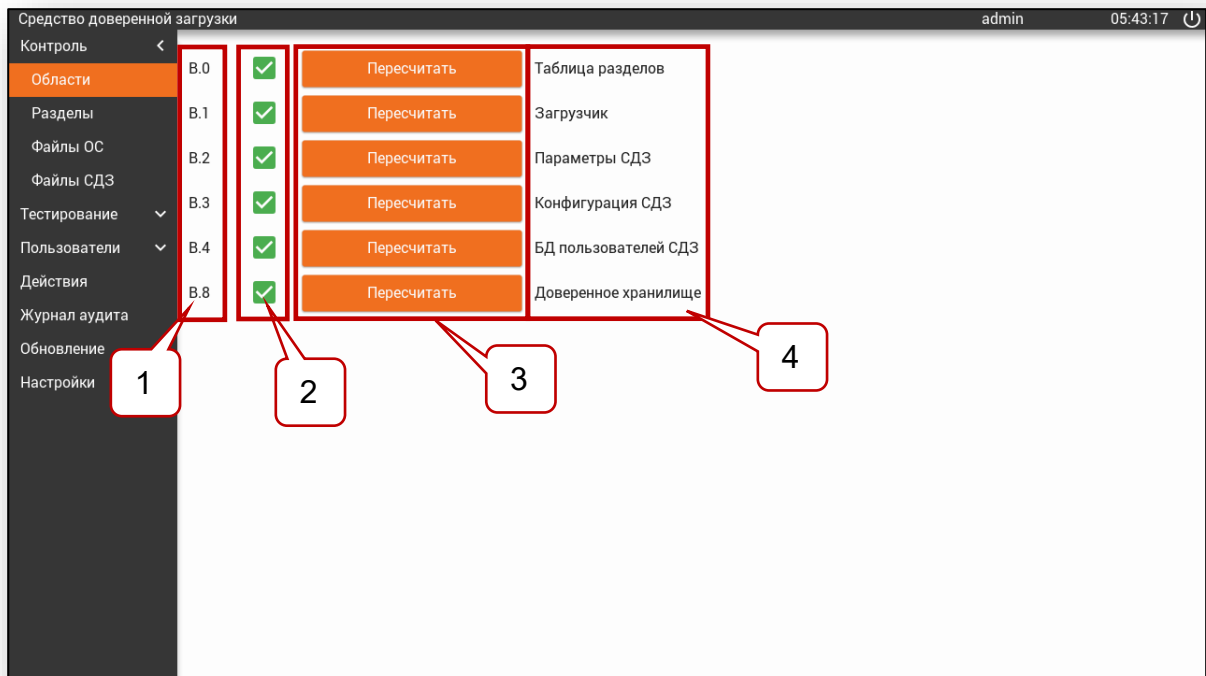


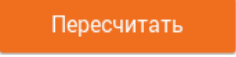


Рисунок 10 - Общий вид пункта «Области»

Описание элементов интерфейса представлено в таблице 4.

Таблица 4 - Элементы интерфейса «Области»

| № п\п | Элемент интерфейса | Описание |
|-------|--|---|
| 1 | Надпись «В.Н», где N – число обозначающее номер области | Краткое обозначение спец. области |
| 2 | Индикатор статуса целостности |  – означает целостность области;  – целостность области нарушена |
| 3 | Кнопка  | При нажатии на кнопку запускается процедура пересчета контрольных сумм соответствующей специальной области |
| 4 | Словесное описание специальной зоны | - |

Данный интерфейс позволяет администратору СДЗ получить информацию о состоянии целостности специальных областей и в случае ее нарушения осуществить пересчет КС.

Пересчет КС специальных областей следует осуществлять, в случае если причины, приведшие к нарушению целостности, поняты и контролируются администратором СДЗ.

Таким образом, для запуска пересчета КС следует выбрать специальную область, целостность которой была нарушена, после чего нажать кнопку



5.1.2. Описание подпункта меню «Разделы»

Для мониторинга и управления разделами ЗН выберите пункт основного меню **«Контроль»** и перейдите в подпункт **«Разделы»**. На экран появится интерфейс с отображением информации о всех разделах ЗН, а также элементы управления ими (см. рисунок 11).

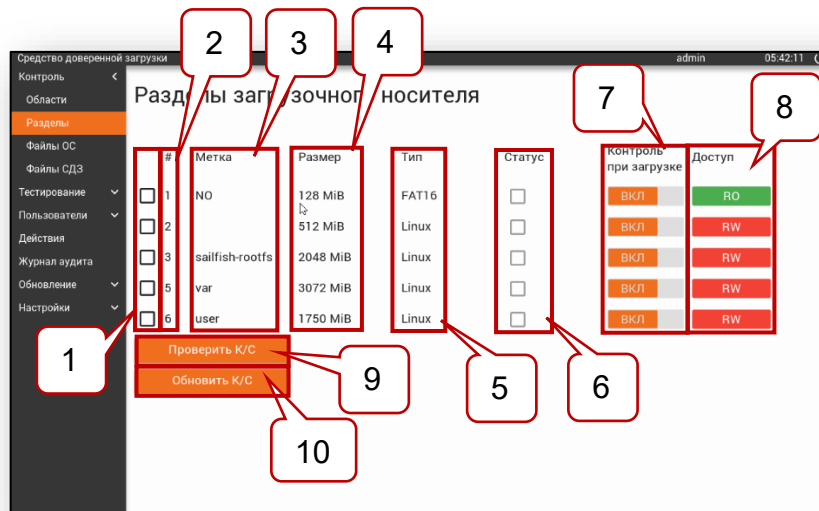




Рисунок 11 – Общий вид интерфейса «Разделы»

Описание элементов интерфейса представлено в таблице 5.

Таблица 5 – Элементы интерфейса «Разделы»

| № | Элемент интерфейса | Описание |
|---|---------------------------|---|
| 1 | «Чек-бокс» выбора раздела | Если выбран, то над данным разделом будет произведена операция проверки или обновления контрольных сумм |
| 2 | # - номер раздела | Порядковый номер раздела, как его учитывает СДЗ |
| 3 | Метка | Метка раздела |
| 4 | Размер | Размер раздела |
| 5 | Тип | Тип файловой системы раздела |
| 6 | Статус | Статус раздела, показывающий целостность раздела после проверки целостности или обновления контрольных сумм. Принимаемы значения: <input checked="" type="checkbox"/> - целостность раздела не нарушена; <input type="checkbox"/> - целостностью раздела нарушена. |
| 7 | Контроль при загрузке | Переключатель, принимающий значения: <input checked="" type="checkbox"/> ВКЛ – проверка целостности раздела при загрузке ОС; <input type="checkbox"/> ВЫКЛ – контроль целостности раздела при загрузке ОС не производится |

| 8 | Доступ | Доступ ОС (пользователя ОС) к разделу. Принимаемые значения: <table border="1" data-bbox="676 293 1422 667"> <thead> <tr> <th data-bbox="676 293 868 342">Значение</th> <th data-bbox="868 293 1422 342">Описание</th> </tr> </thead> <tbody> <tr> <td data-bbox="676 342 868 398">OFF</td> <td data-bbox="868 342 1422 398">Нет доступа</td> </tr> <tr> <td data-bbox="676 398 868 454">RO</td> <td data-bbox="868 398 1422 454">Только чтение</td> </tr> <tr> <td data-bbox="676 454 868 510">RW</td> <td data-bbox="868 454 1422 510">Чтение и запись</td> </tr> <tr> <td data-bbox="676 510 868 667">USER</td> <td data-bbox="868 510 1422 667">Доступ к разделу задается через интерфейс управления учетными записями пользователя</td> </tr> </tbody> </table> | Значение | Описание | OFF | Нет доступа | RO | Только чтение | RW | Чтение и запись | USER | Доступ к разделу задается через интерфейс управления учетными записями пользователя |
|----------|--|---|----------|----------|-----|-------------|----|---------------|----|-----------------|------|---|
| Значение | Описание | | | | | | | | | | | |
| OFF | Нет доступа | | | | | | | | | | | |
| RO | Только чтение | | | | | | | | | | | |
| RW | Чтение и запись | | | | | | | | | | | |
| USER | Доступ к разделу задается через интерфейс управления учетными записями пользователя | | | | | | | | | | | |
| 9 | Кнопка  | При нажатии на кнопку запускается процедура проверки контрольных сумм выбранного раздела ЗН | | | | | | | | | | |
| 10 | Кнопка  | При нажатии на кнопку запускается процедура обновления контрольных сумм выбранного раздела ЗН | | | | | | | | | | |


Данный графический интерфейс позволяет администратору выполнять следующие действия:

- 1) Установку контроля целостности разделов ЗН перед загрузкой ОС;
- 2) Установку прав доступа к разделам ЗН;
- 3) Контроль целостности разделов ЗН.

Установка контроля целостности раздела ЗН перед загрузкой ОС позволяет производить автоматическую проверку разделов ЗН перед выполнением загрузки ОС, для этого администратору СДЗ необходимо выполнить следующее:





- 1) В графическом интерфейсе выбрать необходимый раздел ЗН;
- 2) Установить переключатель **«Контроль при загрузке»** в положение



Установка переключателя в положение  означает, что перед загрузкой ОС будет выводиться экран (см. рисунок 8) отображающий процесс проверки целостности выбранных разделов ЗН.

Установка прав доступа к разделам ЗН позволяет контролировать действия, которые пользователь или процессы могут выполнять над объектами (файлами и другими компьютерными ресурсами) разделов ЗН. Возможно установить единое значение прав доступа к разделам ЗН, как для всех пользователей СДЗ «TSM», так и для каждого пользователя индивидуально, для этого следует выполнить:

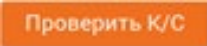
- 1) В графическом интерфейсе выбрать необходимые разделы;
- 2) Напротив, нужного раздела ЗН в столбце **«Доступ»** выбрать тип доступа из списка:

-  – всем пользователям запрещен доступ к разделу ЗН (установлен по умолчанию);
-  – позволяет всем пользователям доступ к разделу ЗН в режиме просмотра;
-  – позволяет всем пользователям доступ к разделу ЗН в режиме просмотра и редактирования;
-  – данный пункт позволяет администратору индивидуально настраивать доступ к разделу ЗН для каждого пользователя (настройка доступа к разделу задается через интерфейс управления учетными записями пользователя (см. п. 5.3.1)).



Внимание. Для корректной и безопасной настройки параметров прав доступа к разделам ЗН в **Приложении А** приведены примеры значений параметров данной настройки.

Кроме автоматического контроля целостности разделов ЗН перед загрузкой ОС, также возможен контроль целостности разделов ЗН по команде администратора, для этого выполняются следующие действия:

- 1) В графическом интерфейсе выбрать необходимый раздел ЗН и отметить его флажком;
- 2) Нажать кнопку .

Система сверит все значения контрольных сумм выбранных разделов со значениями, сохраненными на ЗН и в столбце «Статус» появится значок, соответствующий значению целостности:




- целостность не нарушена;



- целостность нарушена.

В случае если целостность раздела нарушена (по причине несанкционированного доступа, повреждения ЗН или в результате обновления были изменены объекты ЗН) необходимо выполнить обновление КС раздела ЗН.

Для пересчета значения КС выбранных разделов ЗН нажмите кнопку .

5.1.3. Описание подпункта меню «Файлы ОС»

Для выполнения мониторинга контроля целостности объектов ОС, выберите пункт основного меню «**Контроль**» и перейдите в подпункт «**Файлы ОС**», на экран выводится интерфейс с отображением состояния файла ядра ОС и файла параметров ядра ОС (см. рисунок 12).

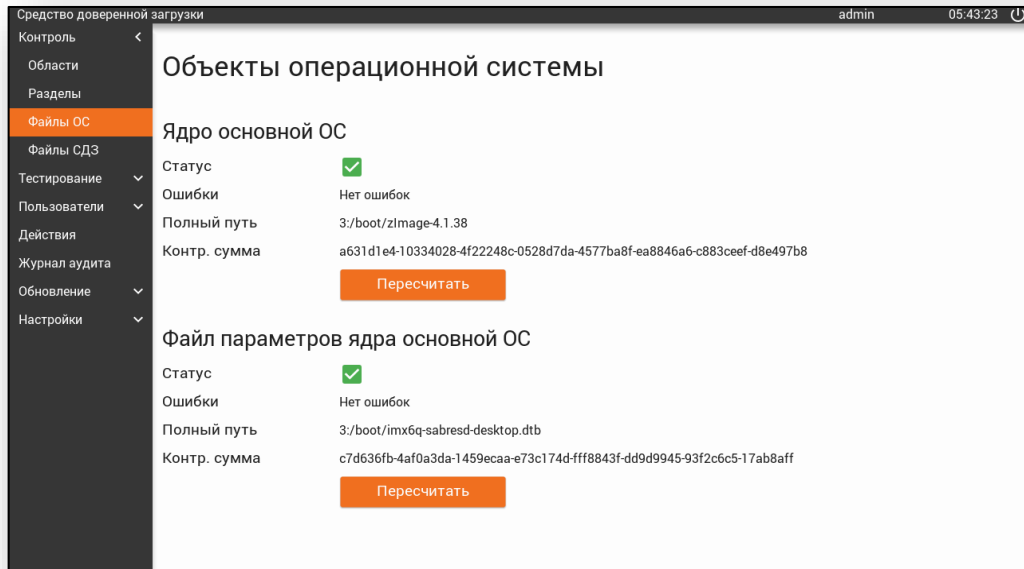


Рисунок 12 - Объекты операционной системы

Описание элементов интерфейса представлено в таблице 6.

Таблица 6 – Элементы интерфейса «Объекты ОС»

| № п/п | Значение | Описание | | | | | | |
|-------------|-------------------------|---|-------------|----------|--|-------------------------|--|----------------------|
| 1 | Статус | Статус объекта ОС, показывающий целостность файла ядра ОС и его файла параметров после проверки. Принимаемые значения: <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>Обозначение</th> <th>Описание</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"></td> <td>Целостность не нарушена</td> </tr> <tr> <td style="text-align: center;"></td> <td>Целостность нарушена</td> </tr> </tbody> </table> | Обозначение | Описание | | Целостность не нарушена | | Целостность нарушена |
| Обозначение | Описание | | | | | | | |
| | Целостность не нарушена | | | | | | | |
| | Целостность нарушена | | | | | | | |
| 2 | Ошибка | Указывает наименование выявленной ошибки | | | | | | |
| 3 | Полный путь | Показывает путь к контролируемому объекту ОС | | | | | | |
| 4 | Контрольная сумма | Контрольная сумма файлов ядра ОС и его параметров | | | | | | |

В случае если целостность одного из объектов ОС нарушена и причиной нарушения целостности является обновление объектов ОС, то требуется запустить пересчет КС для поврежденного объекта ОС, для этого нажмите **Пересчитать**, в ином случае администратор СДЗ «TSM» должен обратиться в службу безопасности своей организации.

5.1.4. Описание подпункта меню «Файлы СДЗ»

Для выполнения мониторинга и контроля целостности объектов СДЗ «TSM», выберите пункт основного меню **«Контроль»** и перейдите в подпункт **«Файлы СДЗ»**, на экран выводится интерфейс с отображением информации о следующих объектах СДЗ «TSM» (см. рисунок 13):

- Образ СДЗ – результат проверки наличия файла-образа СДЗ на ЗН;
- Образ ТЕЕ – результат проверки контроля целостности файла-образа ТЕЕ.

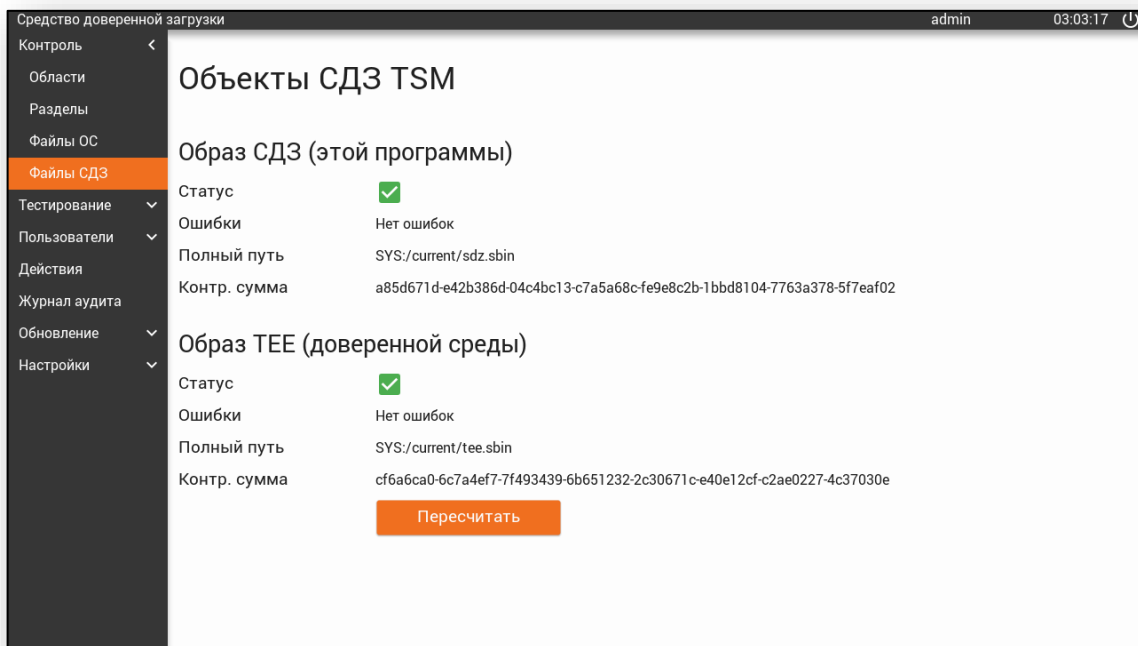



Рисунок 13 - Объекты СДЗ

Описание элементов интерфейса представлено в таблице 7.

Таблица 7 - Информация об объектах СДЗ «TSM»

| № п/п | Значение | Описание | | | | | | |
|---|-------------------------|---|-------------|----------|---|-------------------------|---|----------------------|
| 1 | Статус | Статус объекта СДЗ «TSM», показывающий целостность образа СДЗ и ТЕЕ. Принимаемые значения: <table border="1" data-bbox="732 479 1402 707"> <thead> <tr> <th>Обозначение</th> <th>Описание</th> </tr> </thead> <tbody> <tr> <td></td> <td>Целостность не нарушена</td> </tr> <tr> <td></td> <td>Целостность нарушена</td> </tr> </tbody> </table> | Обозначение | Описание |  | Целостность не нарушена |  | Целостность нарушена |
| Обозначение | Описание | | | | | | | |
|  | Целостность не нарушена | | | | | | | |
|  | Целостность нарушена | | | | | | | |
| 2 | Ошибка | Указывает наименование выявленной ошибки | | | | | | |
| 3 | Полный путь | Показывает путь к контролируемому объекту СДЗ «TSM» | | | | | | |
| 4 | Контрольная сумма | Контрольная сумма образа СДЗ и ТЕЕ | | | | | | |

Если объекты СДЗ «TSM» изменены или удалены, то при проверке, целостность объекта считается нарушена и в поле статус появится соответствующий знак .

В случае если целостность **файла-образа СЗД** нарушена, то это означает, что файл-образ СДЗ отсутствует в указанном месте ЗН. Причиной данной ситуации может явиться сбой при выполнении процесса обновления СДЗ «TSM».

Установить целостность данного объекта СДЗ возможно двумя способами:

1. Повторно выполнив обновление СДЗ (см. п. 5.6.1);
2. Выполнив восстановление СДЗ к предыдущей версии или к заводским настройкам (см. п. 5.6.2.).

В случае нарушение целостности **файла-образа ТЕЕ**, выполняется пересчет КС, при условии, что причина, приведшая к нарушению целостности известна администратору СДЗ.

Для выполнения пересчета КС файла-образа ТЕЕ нажмите кнопку



5.2. Описание пункта основного меню «Тестирование»

В СДЗ «TSM» предусмотрена возможность мониторинга и тестирования по команде администратора СДЗ системной части и функциональной безопасности объекта оценки, которая предназначена для проверки корректной и безопасной работы.

5.2.1. Описание подпункта меню «Системное»

Тестирование осуществляется при помощи пункта основного меню «Тестирование». Для начала тестирования системной части СДЗ необходимо выбрать подпункт «Системное». При этом появляется интерфейс (см. рисунок 14) со списком всех проверок, которые могут быть выполнены в рамках данного тестирования.

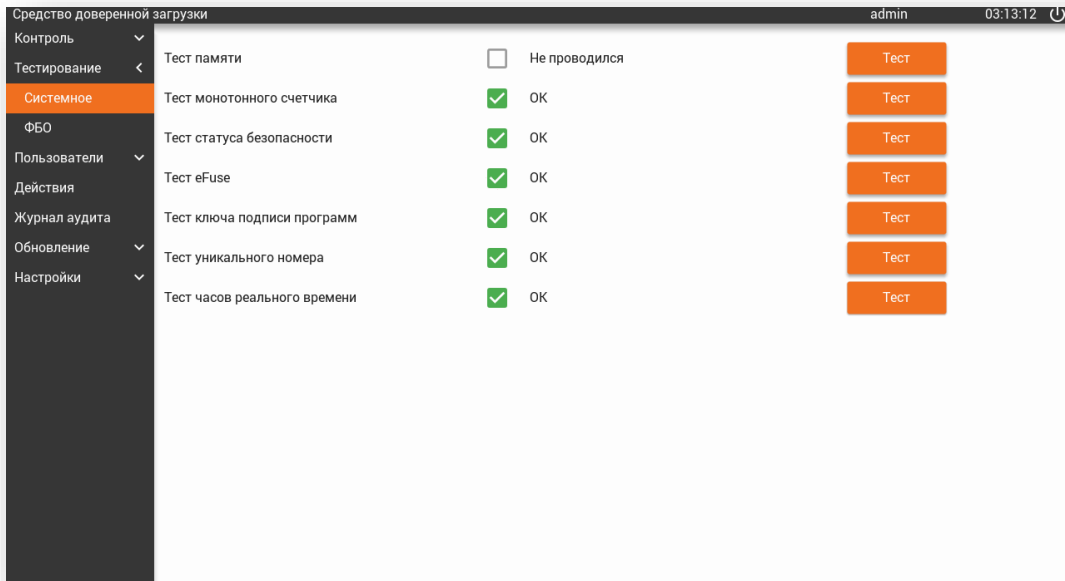






Рисунок 14 - Интерфейс тестирования системной части СДЗ

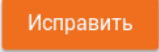
В случае необходимости выполнения тестирования, выберите требуемый пункт проверки и напротив него нажмите кнопку .

По завершения тестирования в интерфейсе будет выведен результат проверки. Возможные результаты проверок приведены в таблице 8.

Таблица 8 - Результаты проверки тестирования

| № п\п | Статус | Результат | Описание |
|-------|---|---------------|--|
| 1 |  | ОК | Проверка по данному пункту выполнена успешно |
| 2 |  | Не выполнено | Проверка была не выполнена |
| 3 |  | Не проверялся | Проверка по данному пункту не проводилась |

После чего, в случае если некоторые пункты тестирования не прошли проверку,

такие как «Тест монотонного счетчика» и «Тест часов реального времени», выполняется их исправление, для этого следует нажать на появившуюся напротив пункта кнопку .

5.2.2. Описание подпункта меню «ФБО»

Тестирование осуществляется при помощи пункта основного меню «Тестирование». Для начала тестирования ФБО необходимо выбрать подпункт «ФБО». При этом появляется интерфейс (см. рисунок 15) со списком всех проверок, которые могут быть выполнены в рамках данного тестирования.

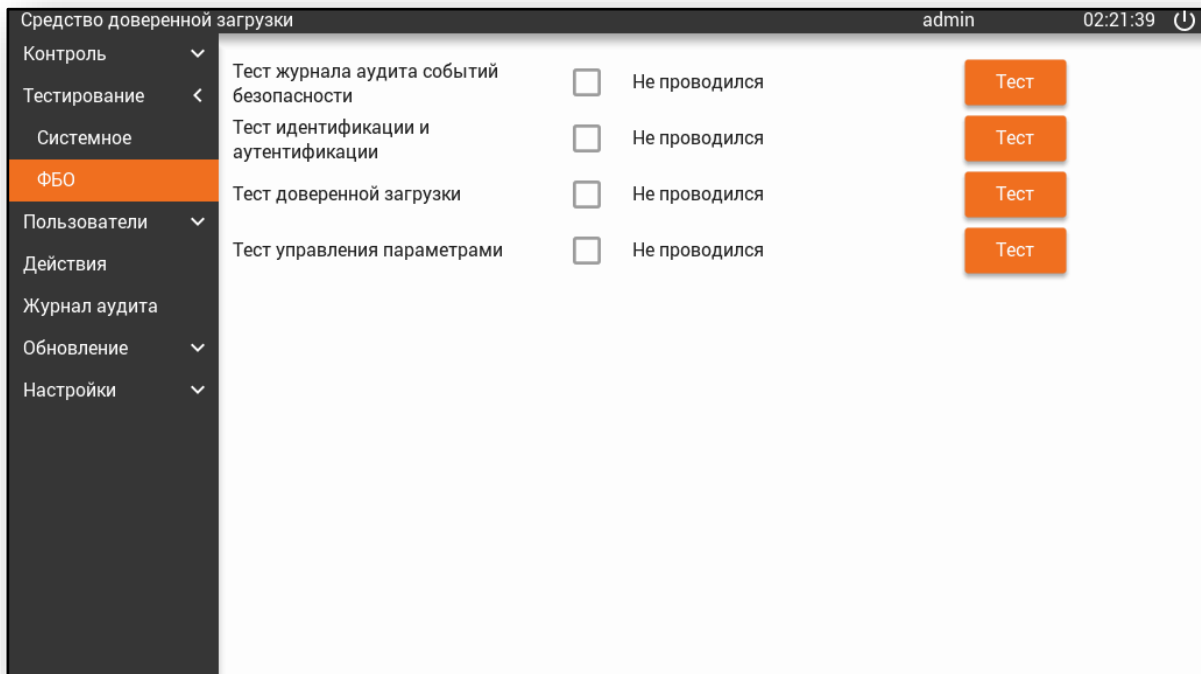






Рисунок 15- Интерфейс тестирования ФБО

В случае необходимости выполнения тестирования, выберите требуемый пункт проверки и напротив него нажмите кнопку .

По завершения тестирования в интерфейсе будет выведен результат проверки. Возможные результаты проверок приведены в таблице 9.

Таблица 9 - Результаты проверки тестирования

| № п\п | Статус | Результат | Описание |
|-------|---|---------------|--|
| 1 |  | ОК | Проверка по данному пункту выполнена успешно |
| 2 |  | Не выполнено | Проверка была не выполнена |
| 3 |  | Не проверялся | Проверка по данному пункту не проводилась |

5.3. Описание пункта меню «Пользователи»

5.3.1. Управление учетными записями пользователей

Для просмотра и редактирования свойств пользователя необходимо войти в графический интерфейс администрирования СДЗ «TSM» и выбрать пункт основного меню **«Пользователи»**, на экране, под пунктом меню, появится список учетных записей пользователей (см. рисунок 16).

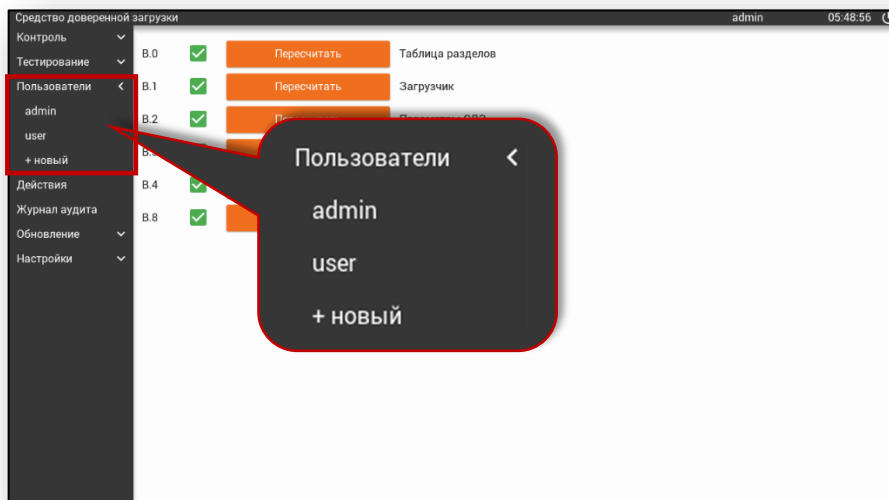


Рисунок 16 - Список учетных записей пользователей

После выбора учетной записи в списке пользователей на экран выводится интерфейс управления учетной записью пользователя с параметрами настройки, которые разбиты на следующие группы:

- 1) **Информация о пользователе.** Позволяет выполнять удаление учетной записи пользователя, а также позволяет указать дополнительные (необязательные для заполнения) сведения;
- 2) **Роль.** Позволяет наделять учетную запись пользователя правами

администратора;

- 3) **Пароль.** Позволяет выполнять смену пароля, продление его действия и привязку токена к учетной записи пользователя;
- 4) **Доступ к разделам.** Позволяет выполнять индивидуальные настройки разграничения доступа пользователя к разделам ЗН, при условии, если выполнены соответствующие настройки (см. п. 5.1.2)
- 5) **Блокировка.** Позволяет выполнять блокировку или разблокировку учетной записи пользователя.

Внешний вид данного интерфейса представлен на рисунке 17.

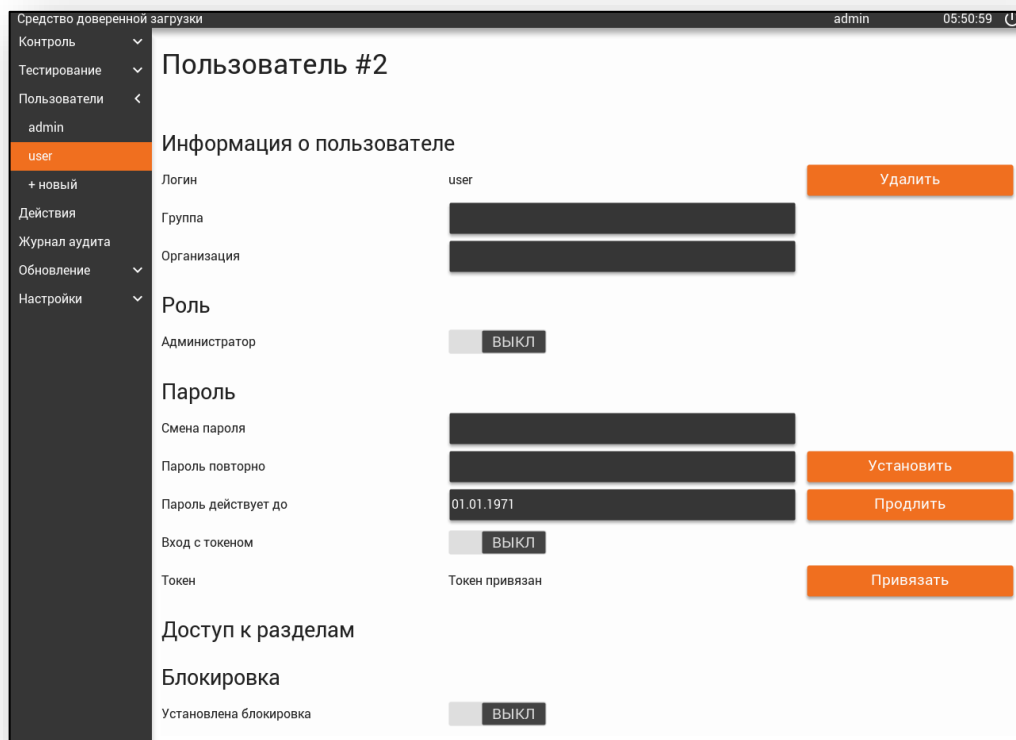


Рисунок 17 - Интерфейс управления учетной записью пользователя

Примечание:

- 1) При редактировании учетных записей пользователей невозможно изменять логин (имя пользователя).
- 2) Обычные пользователи, допущенные к работе на защищенном СВТ, не должны иметь роль «Администратор СДЗ».
- 3) Для текущей учетной записи отключены функции удаления и настройки роли. Таким образом, текущий администратор не может лишиться себя роли «Администратор» или удалить свою учетную запись.

5.3.2. Создание учетной записи

Для создания новой учетной записи пользователя в СДЗ «TSM» необходимо выбрать пункт основного меню **«Пользователи»** и в появившемся списке учетных записей выбрать **«+ новый»** (см. рисунок 18).

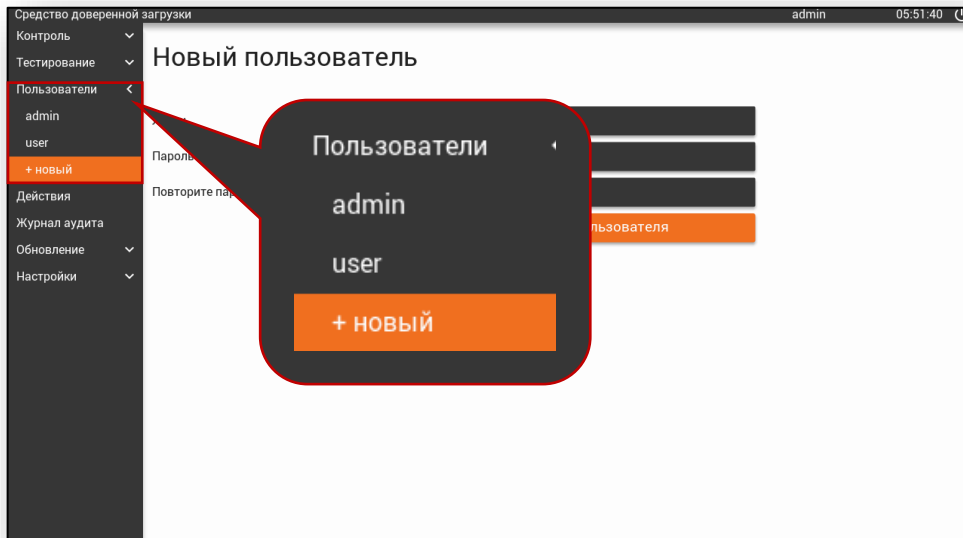
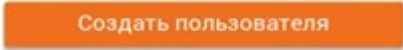


Рисунок 18 - Создания нового пользователя

Далее, в появившемся интерфейсе «Новый пользователь» (см. рисунок 19) выполнить следующие действия:

- 1) В поле **«Логин»** ввести имя нового пользователя;
- 2) В поле **«Пароль»** ввести пароль, отвечающий установленным требованиям сложности пароля (см. п. 5.7.1), а в поле **«Пароль повторно»** ввести значение нового пароля еще раз;


Рисунок 19 - Параметры создания нового пользователя

3) Для сохранения введенных параметров нажать кнопку .

После нажатия кнопки выводится интерфейс управления учетной записью пользователя, в котором выполняются необходимые настройки, смотри рисунок 17.

Примечание. В СДЗ «TSM» ограничено количество создаваемых учетных записей пользователей, администратору СДЗ позволяет создать 8 учетных записи.

5.3.3. Удаление учетной записи пользователя

Для удаления пользователя выберите пункт основного меню «**Пользователи**» и выберите его имя в списке учетных записей, нажмите кнопку  в интерфейсе управления пользователем. В окне появится запрос о подтверждении удаления пользователя (см. рисунок 20). В случае положительного ответа, пользователь будет удален из базы пользователей.

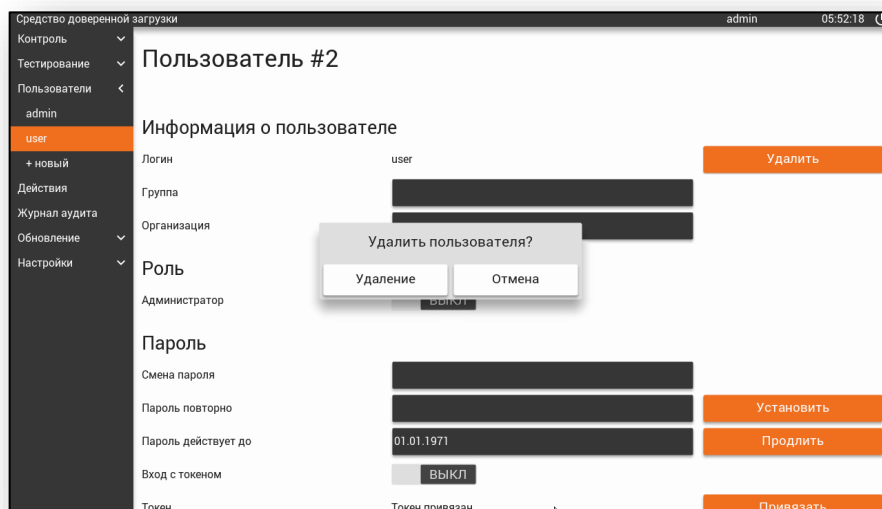


Рисунок 20 - Удаление пользователя

Функция удаления недоступна для текущей учетной записи, т.е. администратор не может удалить себя. Так же, администратор не может лишиться самого себя роли «Администратор». Это сделано для исключения возможности потери доступа к администрированию СДЗ.

Если все же нужно удалить учетную запись администратора, следует создать

другую учетную запись, дать ей права администратора, перезагрузить устройство, войти от имени нового администратора и удалить старую учетную запись.

5.3.4. Смена пароля пользователя

Смена пароля учетной записи пользователя может осуществляться несколькими способами:

- 1) Смена пароля пользователем;
- 2) Смена пароля с помощью интерфейса администратора СДЗ.

Смена пароля пользователем. Пользователь может самостоятельно выполнять смену пароля своей учетной записи, при условии, если администратор СДЗ установил соответствующие настройки (см. п. 5.7.1). Смена пароля может осуществляться, как по запросу пользователя, так и по истечению срока действия пароля учетной записи пользователя.

Если администратор СДЗ «TSM» установил соответствующие настройки, позволяющие пользователю осуществлять смену пароля, то в интерфейсе аутентификации пользователя в верхнем левом углу появится пункт **«Установить новый пароль»** и напоминающее сообщение «Не забывайте регулярно менять пароль» (Сообщение выводится при вводе логина пользователя) (см. рисунок 20).

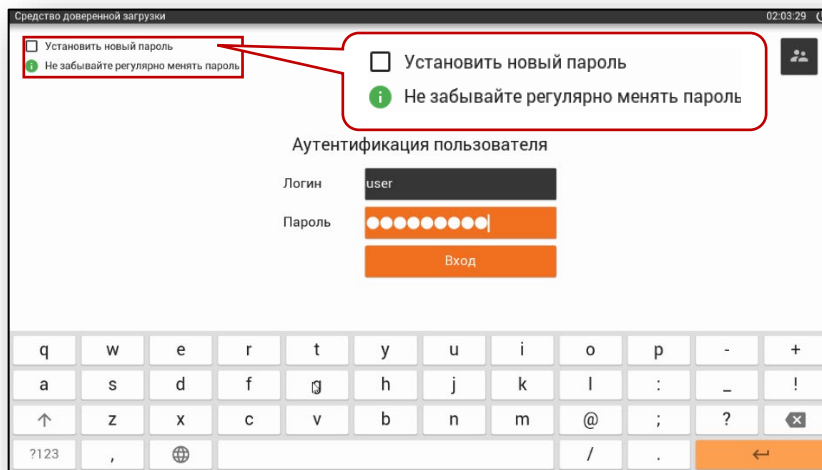



Рисунок 21 - Смена пароля пользователем

Для выполнения смены пароля пользователем отметьте флажком пункт **«Установить новый пароль»**, после введите логин и действующий пароль учетной записи пользователя и нажмите кнопку .

Далее в появившемся интерфейсе (см. рисунок 22) выполнить следующие действия:



Обновление пароля

Текущий пароль

Новый пароль

Еще раз

Пропустить Обновить

Рисунок 22 - Интерфейс обновления пароля пользователем

- 1) В поле **«Текущий пароль»** ввести текущий (действующий) пароль учетной записи пользователя;
- 2) В поле **«Новый пароль»** ввести корректный пароль, отвечающий установленным требованиям сложности пароля (см. п. 5.7.1), а в поле **«Пароль повторно»** ввести значение нового пароля еще раз.
- 3) Для сохранения нового пароля нажать кнопку **«Обновить»**.

При успешной смене пароля учетной записи пользователя выполняется загрузка ОС.

В случае если вход в интерфейс произошел по ошибке, то для продолжения загрузки ОС нажмите кнопку **«Пропустить»**.

Смена пароля с помощью интерфейса администратора СДЗ. В некоторых ситуациях, например, когда пользователь забыл свой пароль или ему недоступна возможность смены пароля, администратору необходимо задать пользователю новый пароль.

Для этого в графическом интерфейсе администрирования СДЗ нужно выбрать пункт основного меню **«Пользователи»** и найти нужного пользователя в списке учетных записей.

Далее, в появившемся интерфейсе редактирования параметров пользователя, выполнить следующие действия:

- 1) В поле **«Пароль»** ввести корректный пароль, отвечающий установленным

требованиям сложности пароля (см. п. 5.7.1), а в поле **«Пароль повторно»** ввести значение нового пароля еще раз;

2) Для сохранения нового пароля нажать кнопку .

Если изменение пароля прошло успешно, то на экране появится соответствующее сообщение (см. рисунок 23).

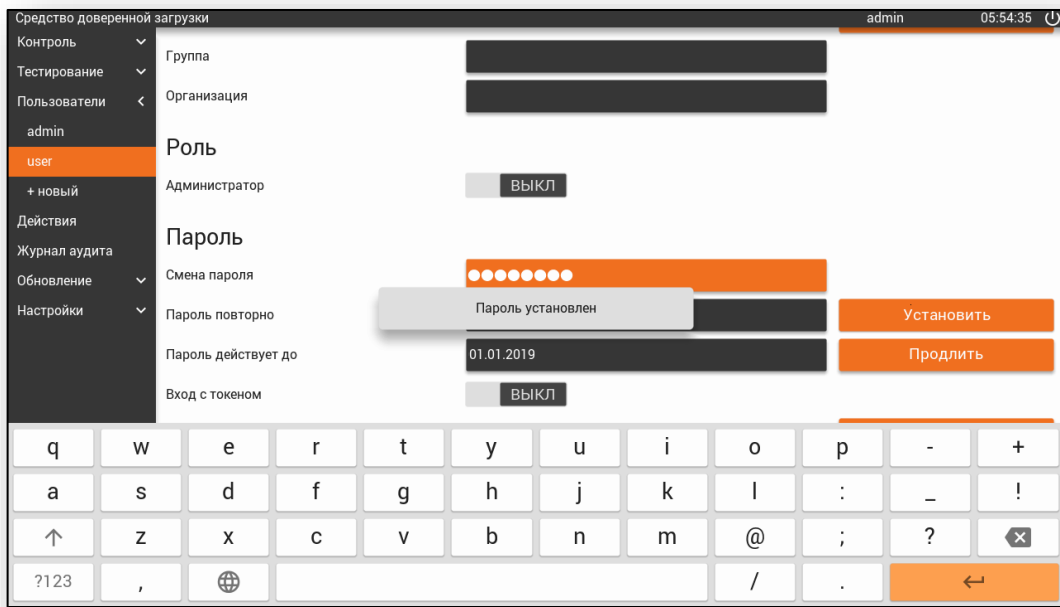
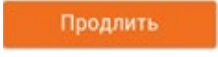


Рисунок 23 - Сообщение об успешной смене пароля

5.3.5. Продление действия пароля пользователя

Для того чтобы установить новую дату действия пароля, перейдите в пункт основного меню **«Пользователи»**, в появившемся списке учетных записей выберите нужного пользователя, далее в поле **«Пароль действует до»** введите новую дату действия пароля и нажмите . В случае если новая дата действия пароля указана корректно, на экране появится соответствующее сообщение (см. рисунок 24).

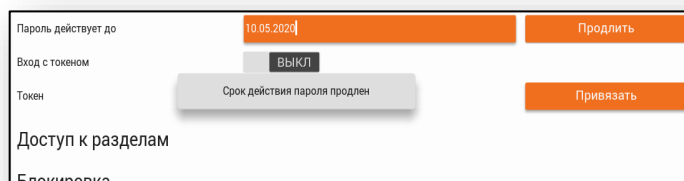




Рисунок 24 - Сообщение об успешном продлении действия пароля

5.3.6. Привязка токена к учетной записи пользователя

В СДЗ «TSM» для учетной записи пользователя может быть применено требование использования двухфакторной аутентификации с вводом логина, пароля и предъявлением токена.

Для привязки токена к учетной записи пользователя выполните следующие действия:

- 1) Выберите пункт главного меню **«Пользователи»**;
- 2) В появившемся списке учетных записей выберите нужного пользователя;
- 3) В появившемся интерфейсе редактирования параметров пользователя для активации двухфакторной аутентификации установите переключатель **«Вход с токеном»** в положении **«ВКЛ»**;
- 4) Подключите токен, вставив его в USB-порт;
- 5) Далее нажать кнопку .

Примечание. Эта операция может выполняться и в обратном порядке: сначала нажать на кнопку , а затем подключить токен. Этот способ применяется при управлении мышью, если для подключения токена к порту USB потребуется отключить мышь.

После привязки токена для учетной записи на экране СВТ будет выведено соответствующее сообщение (см. рисунок 25). Таким образом, после включения двухфакторной аутентификации, помимо ввода логина и пароля потребуется предъявлять привязанный токен.

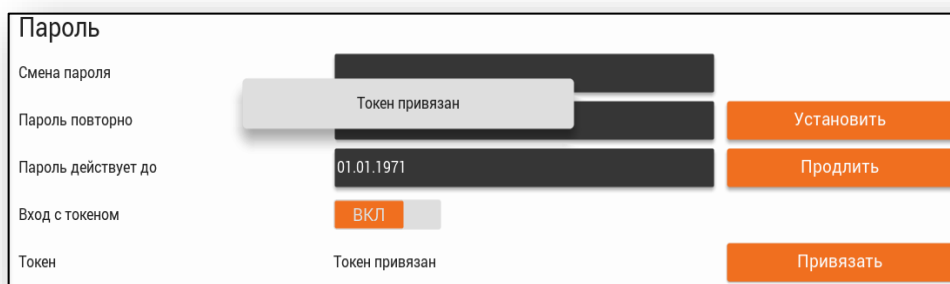


Рисунок 25 - Сообщение о успешной привязке токена

5.3.7. Наделение пользователя правами администратора

Для того чтобы наделить пользователя правами администратора перейдите в пункт основного меню **«Пользователи»**, в появившемся списке учетных записей

выберите нужного пользователя. После чего напротив пункта **«Администратор»** установите переключатель в положение **ВКЛ**.

5.3.8. Управление доступом пользователя к разделам ЗН

В случае если администратор СДЗ при настройке доступа к разделам ЗН установил режим **«USER»** (см. п. 5.1.2), в интерфейсе управления учетными записями пользователя станут доступны дополнительные пункты параметров пользователя в группе доступ к разделам (см. рисунок 26).

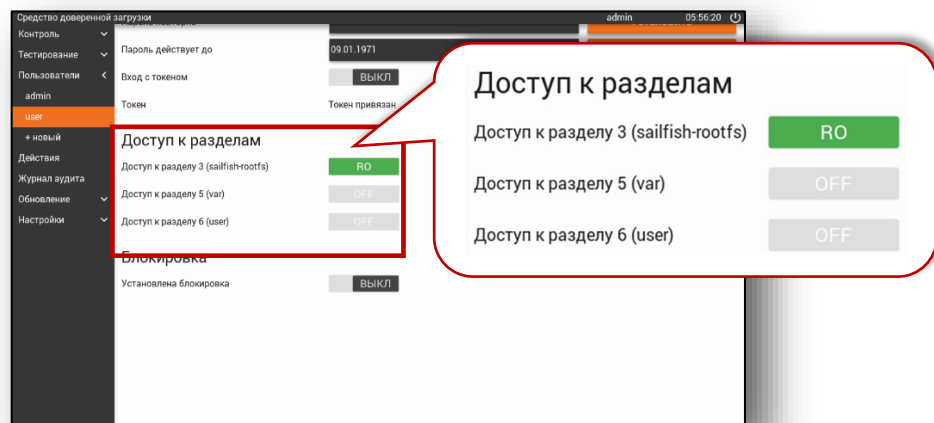


Рисунок 26 - Настройка доступа пользователя к разделам ЗН

Таким образом, для того чтобы настроить индивидуально каждому пользователю доступ к разделам ЗН, выполните следующие действия:

- 1) Выберите пункт главного меню **«Пользователи»**;
- 2) В появившемся списке учетных записей выберите нужного пользователя;
- 3) В появившемся интерфейсе редактирования параметров пользователя, напротив пункта **«Доступ к разделу (имя раздела)»** выберите из списка тип доступа:

- **OFF** – всем пользователям запрещен доступ к разделу ЗН (установлен по умолчанию);
- **RO** – позволяет всем пользователям доступ к разделу ЗН в режиме просмотра;
- **RW** – позволяет всем пользователям доступ к разделу ЗН в режиме просмотра и редактирования.

5.3.9. Блокировка и разблокировка пользователя

Средство блокировки учетной записи пользователя предназначено для предотвращения несанкционированного использования СВТ. В этом режиме пользователь не сможет загрузить ОС, даже при верном вводе пароля.

Блокировка учетной записи пользователя может выполняться:

- 1) **Администратором СДЗ.** Осуществляется, в случае если пользователь был скомпрометирован;
- 2) **Автоматически.** Осуществляется при превышении определенного количества попыток ввода неверного пароля или по истечению срока действия пароля.

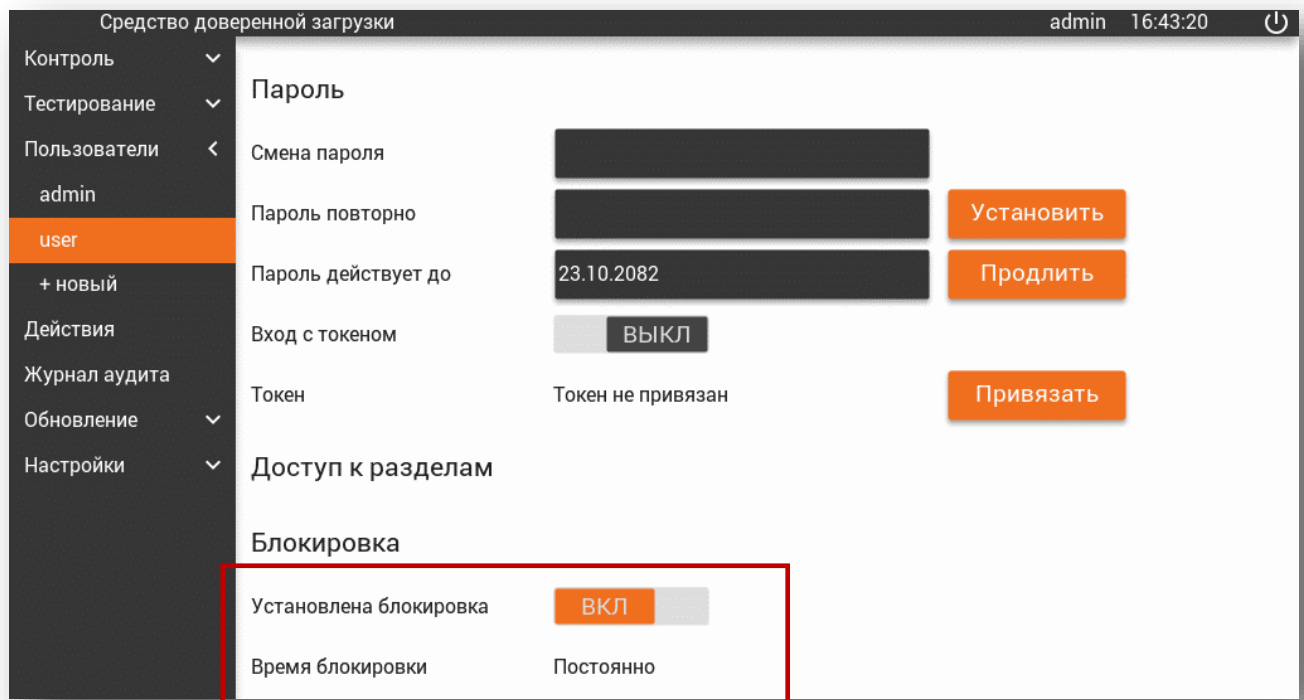


Рисунок 27 - Блокировка учетной записи пользователя


В случае, если учетная запись заблокирована, в поле **“Время блокировки”** указывается срок действия блокировки:

- “До 19:50:09 15.10.2018” – блокировка, установленная до определенного времени, возникает при превышении установленного количества попыток ввода пароля пользователя, если тип блокировки в таком случае – TIMEOUT.
- “Постоянно” – постоянная блокировка, установленная администратором


или при превышении установленного количества попыток ввода пароля пользователя, если тип блокировки в таком случае – FOREVER.

- “Прошло, будет разблокирован” – означает, что время блокировки по TIMEOUT прошло и блокировка будет снята автоматически при следующей идентификации пользователя.

Чтобы заблокировать учетную запись пользователя, выберите пункт основного меню **«Пользователи»** и найдите нужное имя пользователя в списке учетных записей.

В появившемся интерфейсе редактирования параметров пользователя установить переключатель **«Установлена блокировка»** в положение  ВКЛ. После этого учетная запись будет заблокирована на неопределенное время (статус “Постоянно”).

Для разблокировки учетной записи пользователя выберите пункт основного меню **«Пользователи»** и найдите нужное имя пользователя в списке учетных записей.

В появившемся интерфейсе редактирования параметров пользователя установить переключатель **«Установлена блокировка»** в положение  ВЫКЛ.

5.3.10. Сообщения, возникающие при управлении учетной записью пользователя

Таблица 10 – Список сообщений, возникающий при управлении учетной записью пользователя

| № | Этап | Наименование ошибки | Причина | Действие администратора |
|---|--------------------------|--|--|--|
| 1 | Интерфейс «Области» | - | - | - |
| 2 | Интерфейс «Разделы» | «Выберите один или несколько разделов» | Не выбран раздел из списка для проверки контроля целостности | Для запуска процедуры проверки контроля целостности раздела или обновления контрольных суммы раздела требуется выбрать один или несколько разделов через элемент управления «чек-бокс» |
| 3 | Интерфейс «Пользователи» | «Пароли не совпадают» | Пароль введенный в поле [Пароль] и [Повторите пароль] не совпали | Заново вводить пароли до их совпадения |
| 4 | | «Пароль должен быть не менее 6 символов» | Пароль не соответствует минимальной длине | Указать пароль, который будет состоять как минимум из 6 символов |
| 5 | | «В пароле должны быть строчные буквы» | Пароль не соответствует требованиям метрики | Установить пароль, соответствующий метрике |
| 6 | | «В пароле должны быть прописные буквы» | | |

| | | | | |
|----|---------------------------|---|---|---|
| 7 | | «В пароле должны быть цифры» | | |
| 8 | | «В пароле должны быть символы» | | |
| 9 | | «Пользователь с таким именем уже существует» | Логин (имя) введенный в поле [Логин] уже существует в списке учетных записей пользователя | Выбрать другое имя пользователя |
| 10 | | «Подключите токен для привязки» | Попытка привязки токена без подключенного токена | Для продолжения привязки пользователь должен подключить токен |
| 11 | Интерфейс «Журнал аудита» | «Журнал аудита полностью заполнен. События не аудируются. Примите меры» | Нехватка памяти | Для того чтобы события стали вновь вноситься в журнал аудита, администратор должен очистить журнал аудита |

5.4. Описание пункта меню «Действия»

При входе в графический интерфейс администрирования СДЗ «TSM» и выбора пункта основного меню «**Действия**», на экран выводится интерфейс, представленный на рисунке 28.

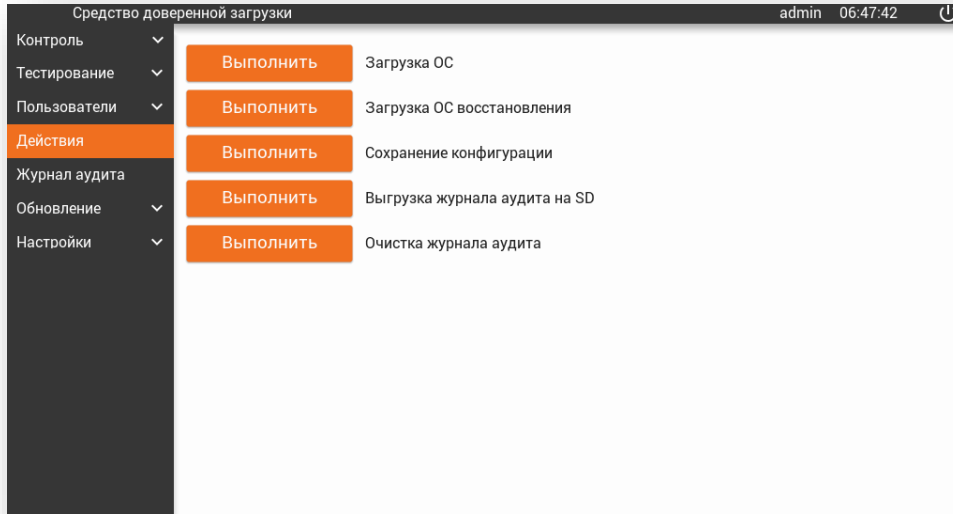



Рисунок 28 - Графический интерфейс пункта меню «Действия»

Данный графический интерфейс позволяет администратору выполнять:

- 1) **Загрузку ОС** – позволяет администратору СДЗ перейти к загрузке основной ОС;
- 2) **Загрузка ОС восстановления** – позволяет администратору СДЗ загрузить вспомогательную ОС восстановления в случае повреждения разделов ЗН с установленной основной ОС для дальнейшего восстановления ее штатными утилитами;
- 3) **Сохранение конфигурации** – позволяет сохранить выполненные настройки;
- 4) **Выгрузка журнала аудита на SD** – позволяет сохранить все записи журнала аудита на ЗН;
- 5) **Очистку журнала аудита** – позволяет очистить записи в журнале аудита.

Для выполнения **загрузки ОС** выберите пункт основного меню «**Действия**» и напротив пункта «**Загрузка ОС**» нажмите кнопку . После выполнения данного действия происходит выход из интерфейса администрирования и начинается загрузка ОС.

В случае необходимости выполнить **загрузки ОС восстановления** выберите пункт основного меню **«Действия»** и напротив пункта **«Загрузка ОС восстановления»** нажмите кнопку **Выполнить**. После чего на экране появится запрос о подтверждении запуска ОС восстановления (см. рисунок 29). В случае положительного ответа происходит выход из интерфейса администрирования и начинается загрузка ОС восстановления.

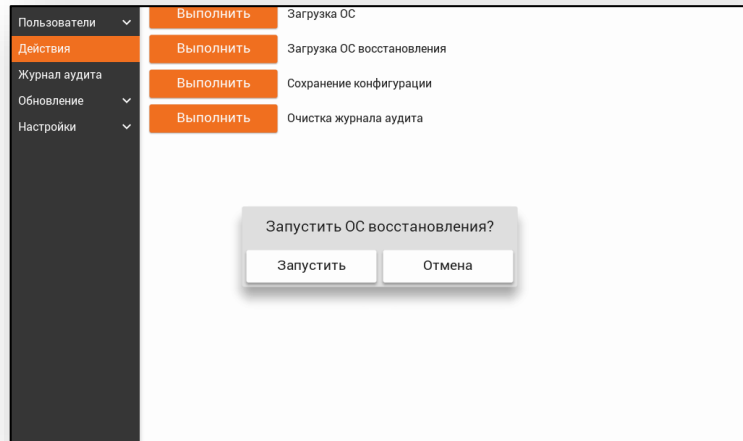


Рисунок 29 - Запуск ОС восстановления

Примечание. Перед запуском ОС восстановления следует выполнить ее установку, которая полностью идентична процессу установки основной ОС, а также ее отладку (см. п. 5.6.3 и 5.7.4).

Для сохранения выполненных настроек СДЗ выберите пункт основного меню **«Действия»** и в отобразившемся интерфейсе нажмите кнопку **Выполнить** напротив пункта **«Сохранение конфигурации»**. После выполнения данного действия будет произведено сохранение параметров настроек СДЗ «TSM».

Для сохранения журнала аудита выберите пункт основного меню **«Действия»** в отобразившемся интерфейсе нажмите кнопку **Выполнить** на против пункта **«Выгрузка журнала аудита на SD»**. После чего на экран будет выведено сообщение о успешном сохранении журнала аудита, а также будет указан путь к файлу на ЗН и его название.

Примечание. Для удобства импортирования журнал аудита в вспомогательную программу, он будет сохранен в нескольких форматах файла: Microsoft Office XML (расширение .xml) и CSV (расширение .csv).

Для очистки журнала аудита выберите пункт основного меню **«Действия»** и в

отобразившемся интерфейсе нажмите кнопку **Выполнить** напротив пункта **«Очистка журнала аудита»**. После чего на экран будет выводиться соответствующее сообщение (см. рисунок 30) и данные будут удалены, а в журнал будет занесено событие о очистке.



Рисунок 30 - Уведомление об очистке журнала аудита

Примечание. После очистки журнала первой записью в журнале становится запись типа «Очистка журнала аудита Администратором», но ее номер продолжает нумерацию, начатую до очистки журнала.

5.5. Регистрация и аудит

Важным средством обеспечения безопасности является механизм протоколирования событий администрирования СДЗ «TSM», входа пользователей, проверки целостности и редактирования учетных записей пользователей в журнале аудита.

5.5.1. Описание пункта меню «Журнал аудита»

Работа с журналом аудита осуществляется путем выбора основного меню **«Журнал аудита»** в графическом интерфейсе администрирования СДЗ «TSM» (см. рисунок 31).

| # | Ст. | Класс | Пользователь | Дата | Время |
|------|-----|-------|--|------------|----------------|
| 2961 | ✓ | АУТ | admin | 24.10.2018 | 13:41:10 UTC+3 |
| | | | Успешная аутентификация по паролю: Итоговое решение | | |
| 2962 | ✓ | АУТ | admin | 24.10.2018 | 13:41:10 UTC+3 |
| | | | Успешная авторизация | | |
| 2963 | ✓ | ПИТ | admin | 24.10.2018 | 13:41:24 UTC+3 |
| | | | Выключение питания | | |
| 2964 | ✓ | ПИТ | | 24.10.2018 | 13:41:30 UTC+0 |
| | | | Запуск: Начало работы журнала аудита | | |
| 2965 | ✓ | АПП | | 24.10.2018 | 13:41:31 UTC+3 |
| | | | Тестирование аппаратного обеспечения | | |
| 2966 | ✓ | ПИТ | | 24.10.2018 | 13:41:32 UTC+3 |
| | | | Самотестирование: При старте | | |
| 2967 | ✓ | АУТ | admin | 24.10.2018 | 13:41:50 UTC+3 |
| | | | Успешная идентификация | | |
| 2968 | ✓ | АУТ | admin | 24.10.2018 | 13:41:50 UTC+3 |
| | | | Успешная аутентификация по паролю: Итоговое решение | | |
| 2969 | ✓ | АУТ | admin | 24.10.2018 | 13:41:50 UTC+3 |
| | | | Успешная авторизация | | |
| 2970 | ✓ | АДМ | admin | 24.10.2018 | 13:43:34 UTC+3 |
| | | | Настройки пользователя: user, password_expiry = 23.10.2019 | | |

Рисунок 31 - Общий вид журнала аудита

«Журнал аудита» позволяет администратору выполнить следующие функции:


- 1) Просмотр списка событий;
- 2) Применение механизма фильтрации при просмотре списка событий;
- 3) Аудит безопасности.

Графический интерфейс представляет собой таблицу, в которой содержатся следующие поля, представленные в таблице 11.

Таблица 11 - Элементы интерфейса «Журнал аудита»

| Свойство | Описание |
|--------------|--|
| # | Сквозной номер записи |
| Дата/Время | Дата и время события |
| Статус | Определяет результат ФБ (успешно или неуспешно) |
| Пользователь | Определяет имя пользователя, от имени которого произошло событие |

| Класс | Определяет идентификатор события безопасности. Принимаемые значения: <table border="1" data-bbox="582 293 1249 750"> <thead> <tr> <th data-bbox="582 293 758 342">Значение</th> <th data-bbox="758 293 1249 342">Описание</th> </tr> </thead> <tbody> <tr> <td data-bbox="582 342 758 392">ПИТ</td> <td data-bbox="758 342 1249 392">Питание</td> </tr> <tr> <td data-bbox="582 392 758 441">АУТ</td> <td data-bbox="758 392 1249 441">Аутентификация</td> </tr> <tr> <td data-bbox="582 441 758 490">АПП</td> <td data-bbox="758 441 1249 490">Аппаратное обеспечение</td> </tr> <tr> <td data-bbox="582 490 758 539">ЦЕЛ</td> <td data-bbox="758 490 1249 539">Целостность</td> </tr> <tr> <td data-bbox="582 539 758 589">АДМ</td> <td data-bbox="758 539 1249 589">Администрирование</td> </tr> <tr> <td data-bbox="582 589 758 696">УДЛ</td> <td data-bbox="758 589 1249 696">Удаленное администрирование</td> </tr> <tr> <td data-bbox="582 696 758 750">ОС</td> <td data-bbox="758 696 1249 750">Запуск ОС</td> </tr> </tbody> </table> | Значение | Описание | ПИТ | Питание | АУТ | Аутентификация | АПП | Аппаратное обеспечение | ЦЕЛ | Целостность | АДМ | Администрирование | УДЛ | Удаленное администрирование | ОС | Запуск ОС |
|---------------------------|---|----------|----------|-----|---------|-----|----------------|-----|------------------------|-----|-------------|-----|-------------------|-----|-----------------------------|----|-----------|
| Значение | Описание | | | | | | | | | | | | | | | | |
| ПИТ | Питание | | | | | | | | | | | | | | | | |
| АУТ | Аутентификация | | | | | | | | | | | | | | | | |
| АПП | Аппаратное обеспечение | | | | | | | | | | | | | | | | |
| ЦЕЛ | Целостность | | | | | | | | | | | | | | | | |
| АДМ | Администрирование | | | | | | | | | | | | | | | | |
| УДЛ | Удаленное администрирование | | | | | | | | | | | | | | | | |
| ОС | Запуск ОС | | | | | | | | | | | | | | | | |
| Вторая строка с описанием | Определяет название события | | | | | | | | | | | | | | | | |

Нажатие на кнопки  осуществляет перемещение по списку событий и позволяет просматривать предыдущие или следующие записи.

5.5.2. Механизм фильтрации записей в журнале аудита

Для удобства просмотра необходимой информации в журнале аудита предусмотрен механизм фильтрации событий. Использование фильтра дает возможность отсеять ненужные данные в журнале так, что они становятся невидимы при просмотре. В то же время информация при использовании фильтра из журнала не удаляется.


Для фильтрации событий нажмите кнопку  **Фильтр** в интерфейсе журнала аудита и выберите необходимые параметры фильтра в открывшемся окне (см. рисунок 32).


Рисунок 32 - Общий вид механизма фильтрации

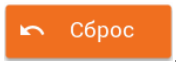
Механизм фильтрации позволяет сортировать события по следующим параметрам, которые приведены в таблице 12.

Таблица 12 – Параметры механизма фильтрации

| № | Название пункта параметра | Название подпункта параметра | Описание |
|---|---------------------------|------------------------------|--|
| 1 | Условия | Пользователь | Поле определяет имя пользователя. Фильтр будет показывать записи от имени которого произошло событие |
| 2 | | Дата, от | Поля определяют интервал времени. Фильтр будет показывать события, которые были зарегистрированы в указанных границах временного интервала |
| 3 | | Дата, по | |

| | | | |
|----|---------------|-----------------------------|---|
| 4 | | Содержит текст | Поле определяет событие по введенному тексту (ключевому слову). Фильтр будет показывать записи по тексту сообщения, комментария, имени пользователя |
| 5 | Успешность | Успех | Поля определяют тип события. Фильтр будет показывать записи по результату успешности выполнения события |
| 6 | | Отказ/ошибка | |
| 7 | Класс события | Все | Поля определяют класс события. Фильтр будет сортировать записи по выбранному классу действия события |
| 8 | | Питание | |
| 9 | | Аутентификация | |
| 10 | | Аппаратное обеспечение | |
| 11 | | Целостность | |
| 12 | | Администрирование | |
| 13 | | Удаленное администрирование | |
| 14 | | Запуск ОС | |

Если необходимые параметры для фильтрации записей были заданы, нажмите кнопку . В результате на экране появится графический интерфейс со списком записей, удовлетворяющий заданным условиям.

Для возврата к стандартным настройкам параметров фильтрации необходимо нажать кнопку .

В случае переполнения журнала аудита предусмотрена функция его очистки (см. подраздел 5.4).

5.5.3. Аудит безопасности

Одной из возможностей с работой журнала аудита является выполнение аудита безопасности, необходимость которой обусловлена следующими обстоятельствами:

- 1) Обнаружение попыток вторжения является важнейшей задачей системы защиты, поскольку ее решение позволяет минимизировать ущерб от взлома и собирать информацию о методах вторжения;

- 2) Подсистема защиты СДЗ «TSM» может не отличить случайные ошибки пользователей от злонамеренных действий. Администратор, просматривая журнал аудита, сможет установить, что произошло при вводе пользователем неправильного пароля — ошибка легального пользователя или атака злоумышленника. Если пользователь пытался угадать пароль 20—30 раз, то это явная попытка подбора пароля;
- 3) Если администратор ОС обнаружил, что против системы проведена успешная атака, ему важно выяснить, когда была начата атака и каким образом она осуществлялась;
- 4) Администраторы ОС должны иметь возможность получать информацию не только о текущем состоянии системы, но и о том, как ОС функционировала в недавнем прошлом.

Примечания:

- 1) Аудит безопасности выполняется администратором, как из графического интерфейса СДЗ, так и при помощи вспомогательных программ, которые позволяют импортировать журналы аудита из файла (см. подраздел 5.4);
- 2) В некоторых случаях, при импортировании журнала аудита для чтения в вспомогательную программу, следует указать, что символом-разделителем является запятая.

К числу событий, которые могут представлять опасность для СДЗ «TSM», относят следующие:

- 1) Вход или выход из СЗД;
- 2) Операции с настройками СДЗ;
- 3) Смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.)
- 4) Проблемы с доверенной загрузкой

Так как в журнал аудита фиксируются все события СДЗ «TSM», то это затрудняет анализ событий и поэтому в журнале предусмотрена возможность их фильтрации по параметрам. Подробное описание параметров и процесса фильтрации событий представлено в пункте 5.5.2.

Фильтрация событий должен выполняться таким образом, чтобы в журнале аудита обязательно отображались:

- 1) Попытки входа/выхода пользователей из системы;

- 2) Попытки изменения списка пользователей;
- 3) Попытки изменения политик безопасности.

Окончательный же выбор событий, которые будут анализироваться, возлагается на администратора.

5.6. Описание пункта меню «Обновление»

5.6.1. Описание подпункта меню «СДЗ «TSM»»

В СДЗ «TSM» реализована возможность обновления ее программных компонентов двумя способами:

- **В автономном режиме функционирования.** Обновление осуществляется через графический интерфейс администрирования СДЗ «TSM», путем установки файлов обновления с внешнего носителя информации - SD-карты;

- **В сетевом режиме функционирования.** Обновление осуществляется удаленно через центр УУ, путем загрузки файлов обновления в указанный раздел ЗН с последующей установкой.

Порядок выполнения действий обновления программных компонентов СДЗ «TSM» в **автономном режиме**:

1. Компания-изготовителя СДЗ «TSM» доводит до потребителя информацию о выпуске обновлений ПО и мер, направленных на нейтрализацию выявленных уязвимостей, через сообщения в информационной ленте сайта компании изготовителя СДЗ «TSM» (<http://www.aladdin-rd./support/>);
2. Потребитель при получении указанной информации выполняет загрузку обновления с web-сервера компании-изготовителя (<http://www.aladdin-rd.ru/support/downloads/>) на внешний носитель информации. При необходимости может быть заказан новый установочный комплект СДЗ «TSM». Также, по запросу, компания-изготовитель высылает заверенное извещение об изменении, содержащее контрольные суммы дистрибутива обновления.



Внимание. Запись файлов обновления осуществляется в предварительно созданную папку updates, расположенную в корне внешнего носителя информации.

3. Далее, установите внешний носитель (SD-карту) информации в SD-слот СВТ и выполните вход в графический интерфейс обновления СДЗ (см. рисунок 33), выбрав пункт основного меню **«Обновление»** и далее

подпункт «СДЗ «TSM»».

Примечание. Установка внешнего носителя информации (SD-карты) в SD-слот осуществляется строго перед запуском СВТ.



Рисунок 33 - Интерфейс обновления СДЗ

4. В графическом интерфейсе обновления СДЗ, выберите нужный файл образа, отметив его флагом, далее нажмите кнопку **Проверить**, после чего на экран будет выведено информационное окно;

Примечание. Дистрибутивы обновления могут храниться, как на внешнем носителе информации, так и на указанном разделе ЗН.

5. В появившемся окне ознакомиться с содержанием дистрибутива обновления СДЗ «TSM» и провести ее верификацию, путем сверки контрольных сумм полученного дистрибутива обновления с контрольными суммами, указанными в извещении об изменении;

6. После ознакомления и верификации выполняется установка обновления, для этого нажмите кнопку **Установить**, процесс установки отображается в нижней части информационного окна (см. рисунок 34). В ином случае нажмите кнопку **Закреть**;

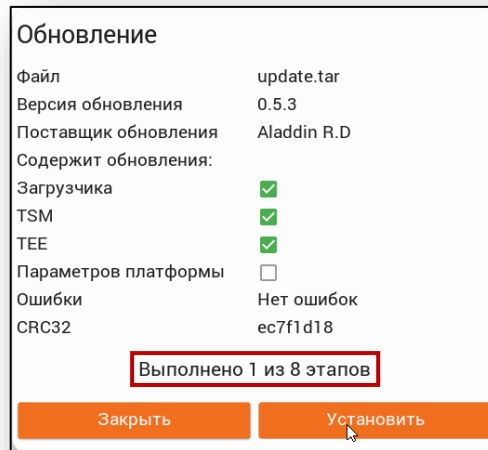


Рисунок 34 - Процесс установки пакетов обновления

Порядок выполнения действий обеспечивающие загрузку файлов обновлений СДЗ «TSM» и выполнение их установки **в сетевом режиме**:

1. Обеспечить загрузку файлов обновлений из центра УУ в указанный раздел ЗН на СВТ. Для этого предварительно между ними настроить доверенный канал следующим образом:
 - Настроить сертифицированное ПО обеспечивающее доверенный канал с центром УУ;
 - Выполнить настройку параметров технических мер контроля управления (см. п. 5.7.5);
2. Далее выполнить установку обновлений, которая возможна двумя способами:
 - **Администратором СДЗ**. Верификация и установка аналогична пунктам 4-6 процедуры обновления программных компонентов СДЗ «TSM» в автономном режиме;
 - **Через центр УУ**. Верификация и установка происходят автоматически по команде полученной по доверенному каналу из центра УУ.

5.6.2. Описание подпункта меню «Резервные копии»

В некоторых случаях возможны ситуации, когда по причине не корректной установки обновлений СДЗ «TSM» происходит повреждение или удаления его исполняемых файлов. Решить эту проблему можно выполнив восстановление СДЗ «TSM».

Таким образом в данном пункте приведено описание следующих действий, позволяющие выполнить восстановление СДЗ «TSM»:

1. Создание резервной копии на основе текущего ПО;
2. Восстановление СДЗ по резервной копии;
3. Восстановление СДЗ к заводским настройкам.

Для выполнения действий, связанных с процессом восстановления СДЗ «TSM» выберите пункт основного меню **«Обновления»** и перейдите в подпункт **«Резервные копии»**, далее на экране появиться интерфейс (см. рисунок 35) с параметрами и элементами управления для восстановления СДЗ «TSM», который разбит на следующие группы:

1. **Текущее ПО** – содержит информацию по текущей версии ПО установленной на СБТ и позволяет выполнить создание резервной копии;
2. **Резервная копия** – содержит информацию о резервной копии, а также позволяет осуществить восстановление и при необходимости выполнить ее удаление;
3. **Заводское ПО** – содержит информацию о изначальной версии ПО установленной на СБТ и при необходимости позволяет выполнить восстановление СДЗ «TSM» к изначальному заводскому ПО.

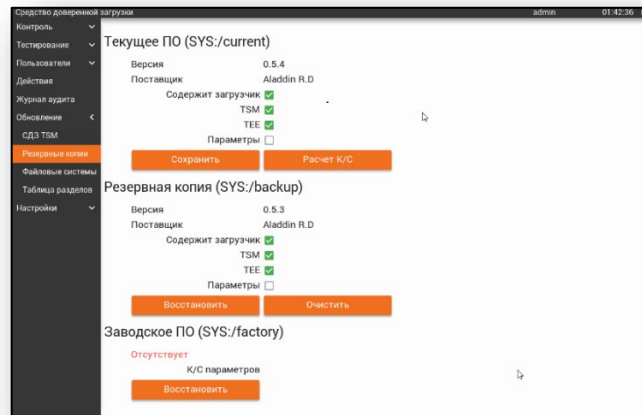
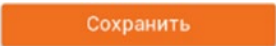


Рисунок 35 - Интерфейс восстановления СДЗ «TSM»

Для **создания резервной копии на основе текущего ПО** в интерфейсе восстановления СДЗ «TSM» выбрать группу **«Текущее ПО»**, далее ознакомьтесь с информацией о параметрах данной версии ПО и нажмите кнопку . После чего на экране появиться запрос о подтверждении создания резервной копии (см. рисунок 36).

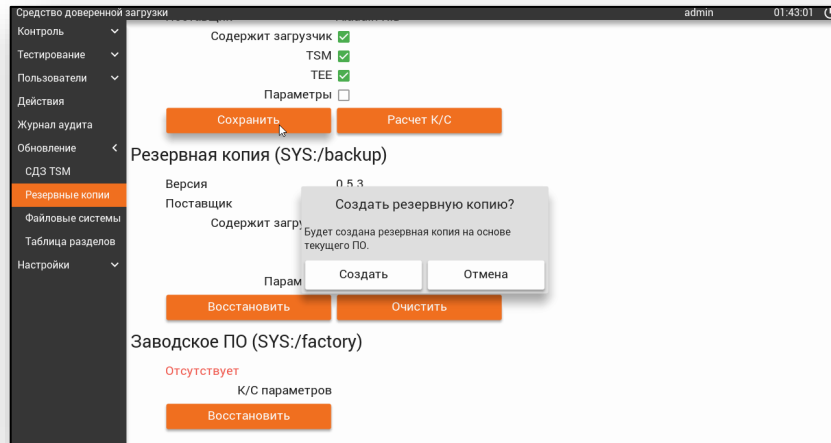


Рисунок 36 – Запрос о подтверждении создания резервной копии

При положительном ответе происходит создание резервной копии текущей версии ПО и на экран выводится сообщение об успешном ее создании (см. рисунок 37).

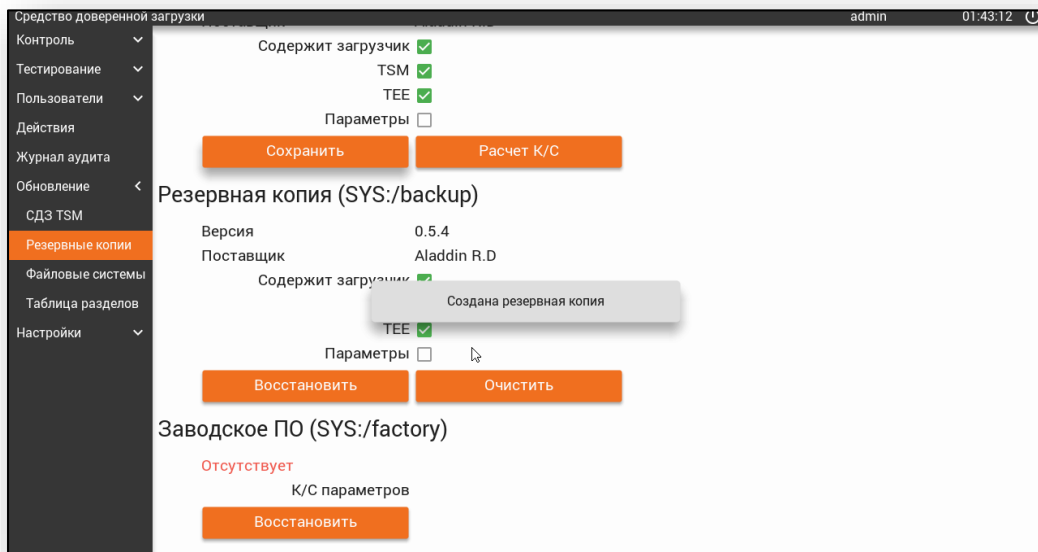


Рисунок 37 - Сообщение об успешном создании резервной копии

Примечание. Данную процедуру рекомендуется выполнять после каждого успешного обновления СДЗ «TSM».

В случае если при обновлении версии СДЗ «TSM» произошли изменения хотя бы в одном из его компонентов, то его КС будет изменена. Для того чтобы узнать новую КС компонента, а также КС компонентов, входящие в резервную копию и

изначальную заводскую версию СДЗ «TSM» нажмите кнопку

Расчет К/С

После чего в интерфейсе будут отображены КС компонентов всех версий СДЗ «TSM» (см. рисунок 38).

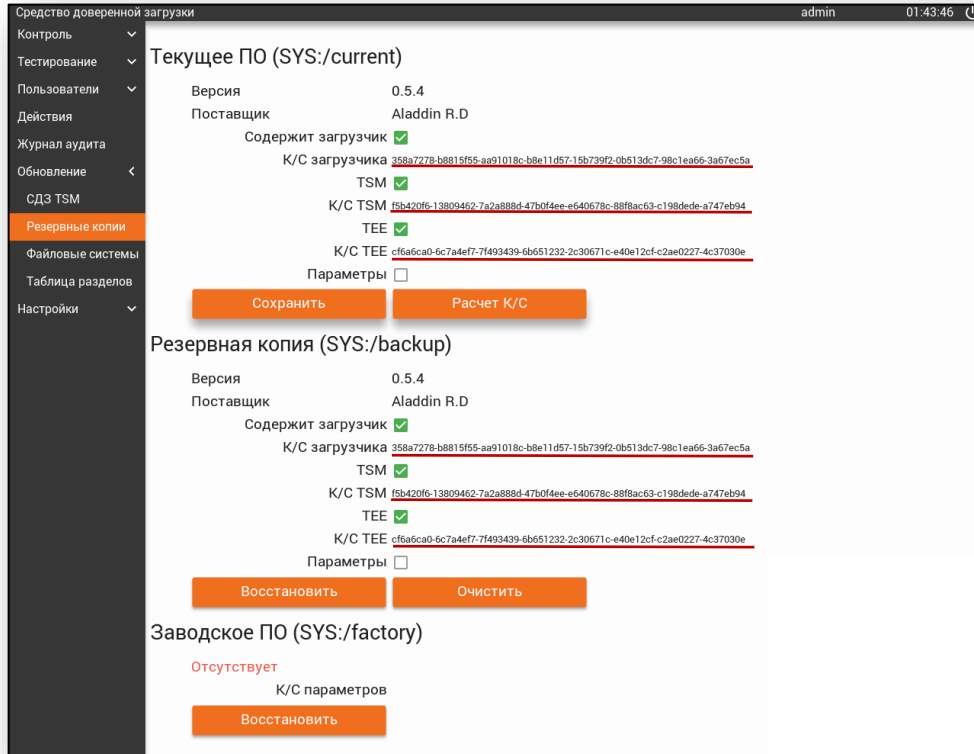


Рисунок 38 - Расчет КС компонентов всех версий СДЗ «TSM»

Для **восстановления СДЗ по резервной копии** в интерфейсе восстановления СДЗ «TSM» выбрать группу **«Резервная копия»**, далее ознакомьтесь с информацией о параметрах резервной копии и нажмите кнопку **Восстановить**. После чего на экране появится запрос о подтверждении восстановления резервной копии СДЗ (см. рисунок 39).

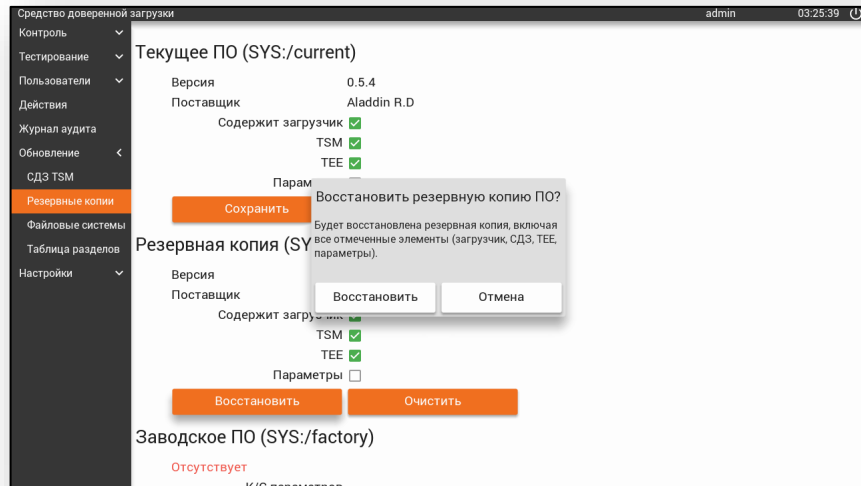


Рисунок 39 – Запрос о подтверждении восстановления резервной копии

При положительном ответе происходит восстановление СДЗ до версии резервной копии и на экран выводится сообщение об успешном восстановлении (см. рисунок 40).

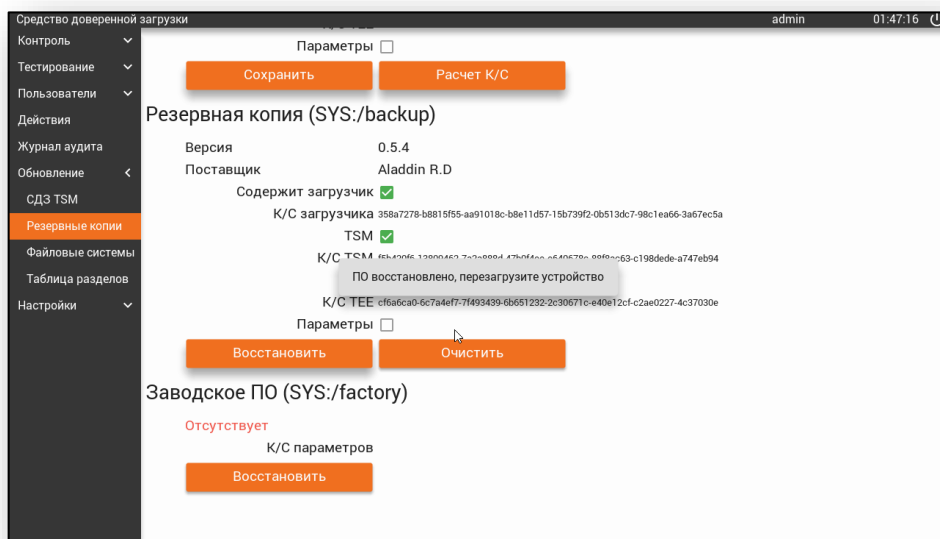



Рисунок 40 - Сообщение об успешном восстановлении СДЗ «TSM»

В случае необходимости выполнить удаление резервной копии СДЗ «TSM» нажмите кнопку , после чего на экране появится запрос на удаление резервной копии (см. рисунок 41).

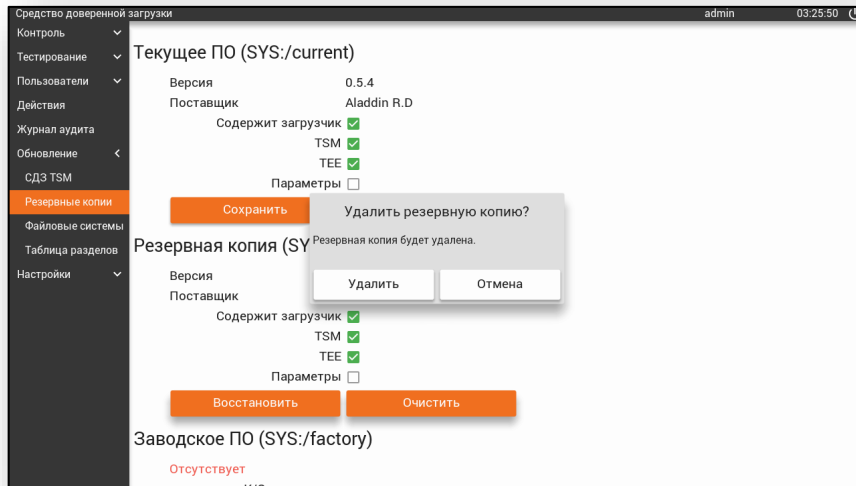


Рисунок 41 – Запрос о подтверждении удаления резервной копии

При положительном ответе происходит удаление резервной копии и на экран выводится сообщение об ее успешном удалении (см. рисунок 42).

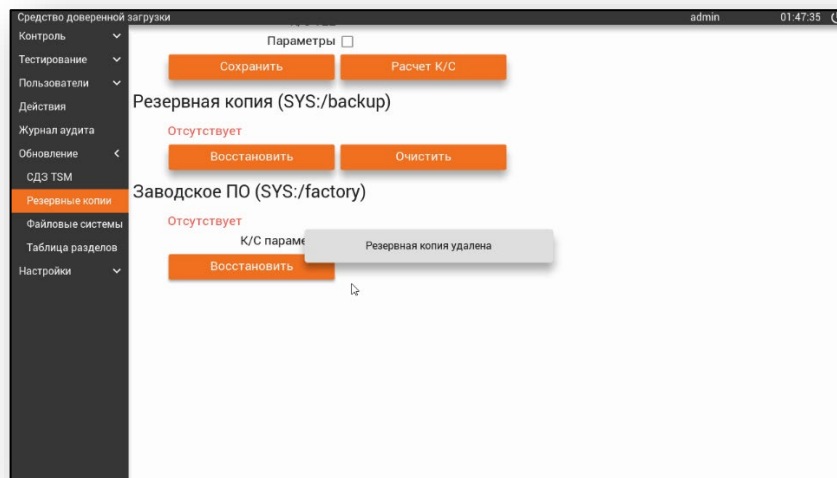



Рисунок 42 - Сообщение об успешном удалении резервной копии

Восстановление СДЗ к заводским настройкам выполняется в том случае, если по какой-то причине невозможно выполнить восстановление СДЗ по резервной копии, для этого в интерфейсе восстановления СДЗ «TSM» выбрать группу «**Заводское ПО**», далее ознакомьтесь с информацией о параметрах изначального заводского ПО и нажмите кнопку . После чего на экране появиться запрос о подтверждении восстановления изначальной заводской копии ПО (см. рисунок 43).

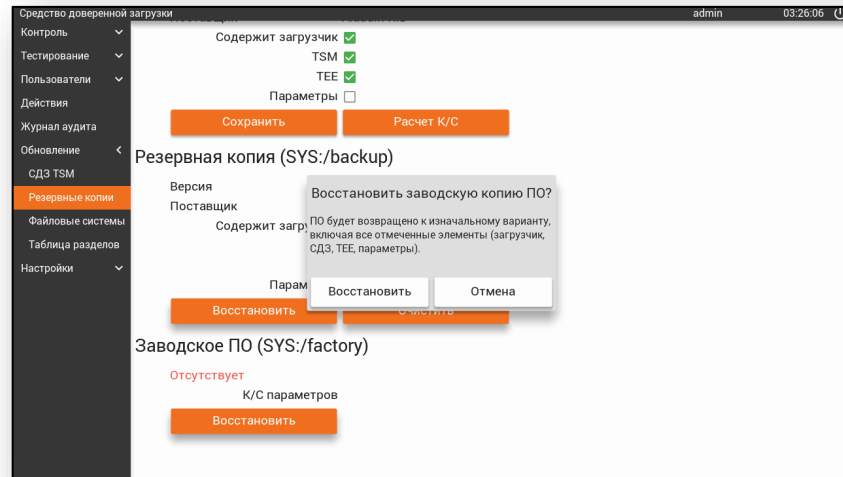


Рисунок 43 – Запрос о подтверждении восстановления изначальной заводской копии ПО

При положительном ответе происходит восстановление к изначальной заводской копии ПО и на экран выводится сообщение об ее успешном восстановлении.

5.6.3. Описание подпункта меню «Файловые системы»

СДЗ «TSM» предусматривает возможность установки ОС на СВТ, ее восстановления и обновления из графического интерфейса администрирования СДЗ «TSM».

Примечание. Перед началом установки ОС, администратору СДЗ следует убедиться, что область ЗН разбита на требуемое количество разделов (см. п. 5.1.2). В случае если количество разделов ЗН не соответствует требованию устанавливаемой ОС производится разбиение области ЗН на требуемое количество разделов путем изменения параметров таблицы разделов ЗН, для этого следует выполнить действия, описанные в пункте 5.6.4.

Установка ОС. Для того, чтобы установить ОС на СВТ через графический интерфейс администрирования СДЗ «TSM», выполните следующие действия:

1. Выберите пункт основного меню **«Обновление»** и перейдите в подпункт **«Файловые системы»**. На экране появится интерфейс (см. рисунок 44) содержащий список файлов образов;

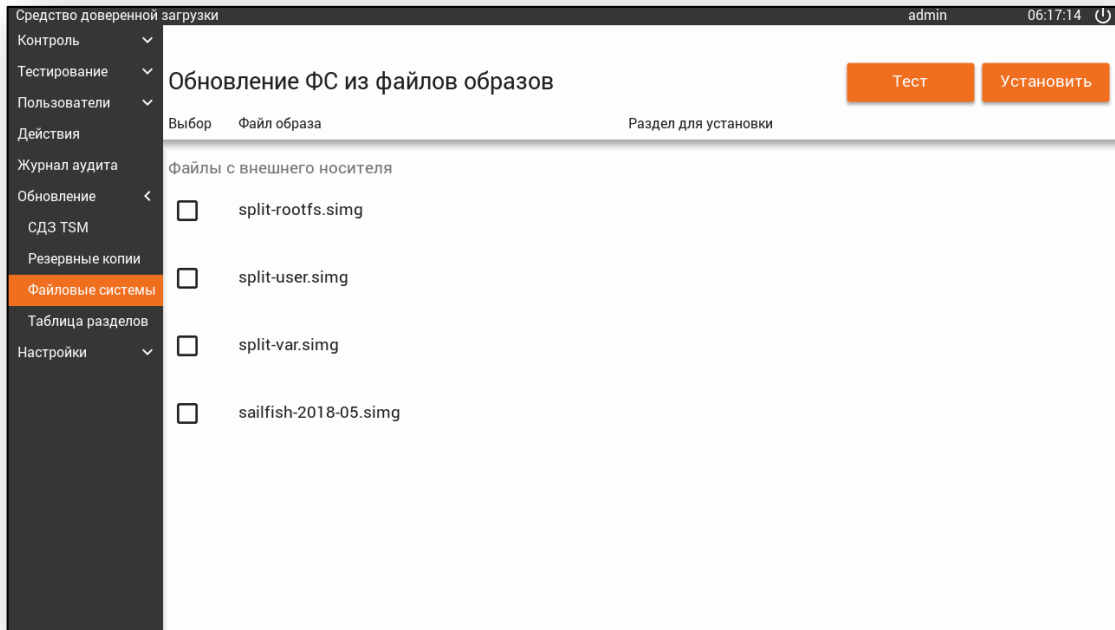


Рисунок 44 - Интерфейс с перечнем файлов образов

2. Из списка выберите файл образа, содержащий в себе ОС и установите отметку выбора;
3. Далее, следует указать раздел ЗН для установки ОС, для этого нажмите на появившееся поле напротив выбранного файла и выберите необходимый раздел ЗН из выпадающего списка;
4. После того, как указали раздел ЗН для установки ОС, выполняется проверка на совместимость форматов файлов и на наличие свободного места на разделе, для этого нажмите кнопку **Тест**. Если при проверке не выявлены ошибки, выполняется установка по нажатию кнопки **Установить**, в ином случае следует выбрать другой раздел ЗН.
5. При успешной установке основной ОС администратор СДЗ должен указать место, откуда будет производиться загрузка ОС. Для этого выполняются действия, описанные в пункте 5.7.3.

Восстановление ОС. Ошибочные действия пользователя, логические ошибки и т.д. могут привести к частичному или полному нарушению работоспособности ОС, что приводит к необходимости выполнения восстановления ОС. Таким образом, при нарушении работы ОС в СДЗ «TSM» предусмотрена функция восстановления ОС следующими способами:

1. **Полная перезапись раздела с установленной ОС.** Используется только в тех случаях, когда нельзя восстановить поврежденные фрагменты раздела с установленной ОС и осуществляется идентично процессу установки ОС, которые описаны выше;
2. **Восстановление поврежденных файлов раздела штатными утилитами ОС восстановления.** Восстановления работоспособности ОС данным способом осуществляется через ОС восстановления, где расположены утилиты. Таким образом, следует выполнить следующие действия:
 - Выполнить загрузку ОС восстановления (см. подраздел 5.4);
 - Далее, выберите и запустите требуемый утилита для восстановления разделов основной ОС.

Обновление ОС. В СДЗ «TSM» реализована функция обеспечивающая обновление основной ОС и она возможно несколькими способами:

1. **Штатными средствами ОС.** Данный способ выполняется штатными средствами ОС и применяется при сетевом режиме работы СДЗ «TSM». Предварительно выполняется настройка прав доступа к разделам ЗН, смотри пункт 5.1.2;
2. **Через графический интерфейс администрирования СДЗ «TSM».** Данный способ применяется при автономном режиме работы СДЗ «TSM», а сам процесс и идентичен процессу установки основной ОС, который описан выше.

5.6.4. Описание подпункта меню «Таблица разделов»

В зависимости от устанавливаемого дистрибутива ОС, количество разделов на ЗН может меняться и в связи с этим в СДЗ «TSM» реализована функция, позволяющая администратору СДЗ изменять состав (создавать и удалять разделы ЗН) и значения параметров разделов ЗН, для этого в графическом интерфейсе администрирования СДЗ «TSM» выберите пункт основного меню **«Обновление»** и перейдите в подпункт **«Таблица разделов»**. После чего на экране появиться интерфейс «Таблица разделов», содержащий текущую информацию о составе и параметрах разделов на ЗН, а также элементы управления (см. рисунок 45).

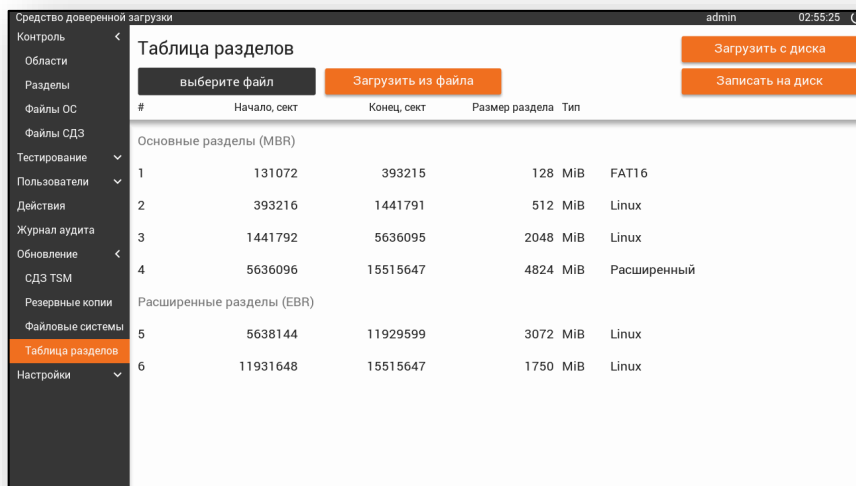

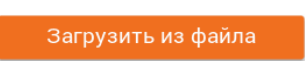




Рисунок 45 - Интерфейс таблицы разделов

Подробное описание параметров разделов и элементов управления в интерфейсе «Таблица разделов» представлено в таблице 13.

Таблица 13 - Описание параметров разделов и элементов управления

| № п\п | Обозначение | Описание |
|-------|--|---|
| 1 | # - номер раздела | Порядковый номер раздела, как его учитывает СДЗ |
| 2 | Начало, сект | Отображает начальный сектор раздела ЗН |
| 3 | Конец, сект | Отображает конечный сектор раздела ЗН |
| 4 | Размер раздела | Размер раздела занимаемый на ЗН |
| 5 | Тип | Тип файловой системы раздела |
| 6 |  - всплывающий список | При нажатии на поле появляется всплывающий список с txt-файлами, содержащие новые параметры для изменения таблицы разделов ЗН |
| 7 |  | При нажатии на кнопку в интерфейсе отображаются предлагаемые новые параметры таблицы разделов ЗН |
| 8 |  | При нажатии на кнопку в интерфейсе отображаются текущие параметры таблицы разделов ЗН |
| 9 |  | При нажатии на кнопку выполняется установка новых параметров таблицы разделов ЗН |

Далее, для осуществления изменения таблицы разделов необходимо:

1. Предварительно сформировать txt-файла в текстовом редакторе, который будет содержать новые параметры таблицы разделов ЗН (см. Приложение Б);

Примечание. Создаваемые txt-файлы должны располагаться в каталоге updates на ЗН.

- Выбрать из всплывающего списка сформированный txt-файл и нажать кнопку **Загрузить из файла**, после чего на экране будет отображена информация о новых параметрах таблицы разделов ЗН. Если же txt-файл не был выбран, то на экране появится сообщение об ошибке (см. рисунок 46);

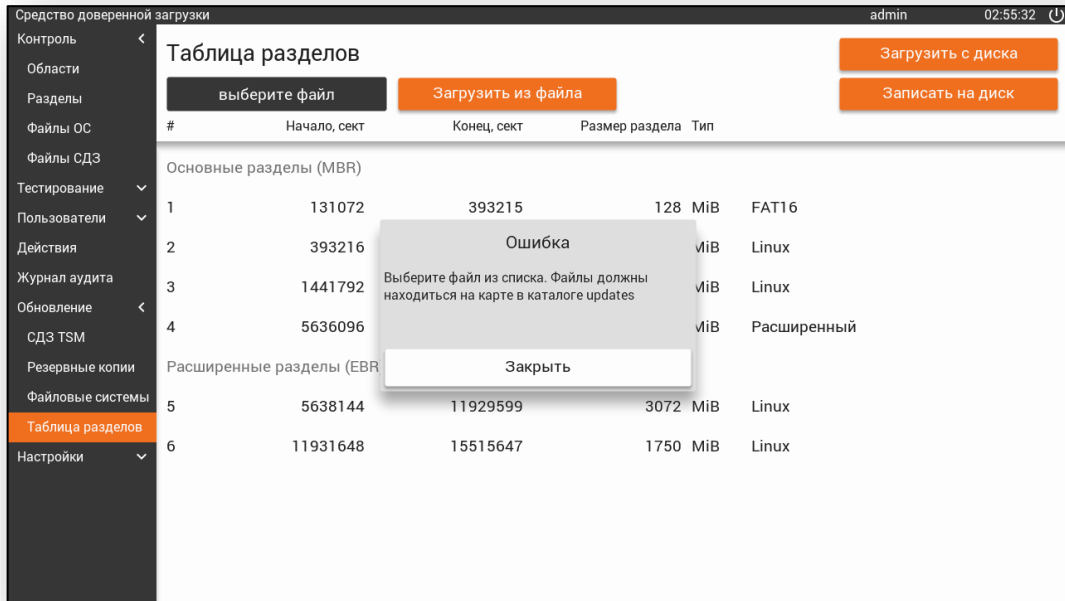


Рисунок 46 - Ошибка вывода информации о новых параметрах таблицы разделов ЗН

- Выполнить сравнение текущих параметров таблицы разделов ЗН с новыми (с целью убедиться в отсутствии ошибок при формировании txt-файла с изменениями) для этого воспользуйтесь кнопками **Загрузить с диска** и **Загрузить из файла**, они позволят переключаться между текущими и новыми параметрами таблицы разделов ЗН;
- Убедившись в отсутствии ошибок, нажать кнопку **Записать на диск** и на экране появится запрос о подтверждении изменения таблицы разделов ЗН (см. рисунок 47).

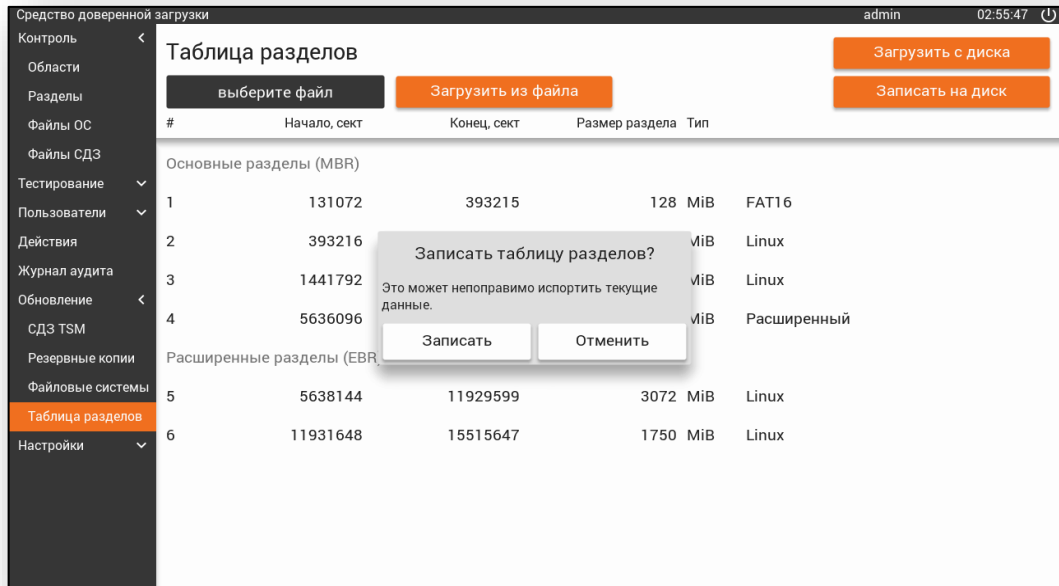


Рисунок 47 - Предложение о выполнении изменения таблицы разделов.

При положительном ответе выполняется установка изменений таблицы разделов ЗН, в ином случае выполняется отмена установки.

Описание пункта меню «Настройки»

При выборе пункта основного меню **«Настройки»**, на экране, под пунктом меню выводится список следующих настроек:

- 1) Аутентификация;
- 2) Дата и время;
- 3) Файлы ОС;
- 4) Восстановление;
- 5) Управление.

5.7.1. Описание подпункта меню «Аутентификация»

Для настройки параметров входа в СВТ с установленным СДЗ «TSM», необходимо выбрать пункт основного меню **«Настройки»** и перейти в подпункт **«Аутентификация»**. На экран выведется интерфейс (см. рисунок 48) с отображением параметров настройки аутентификации и качества паролей.

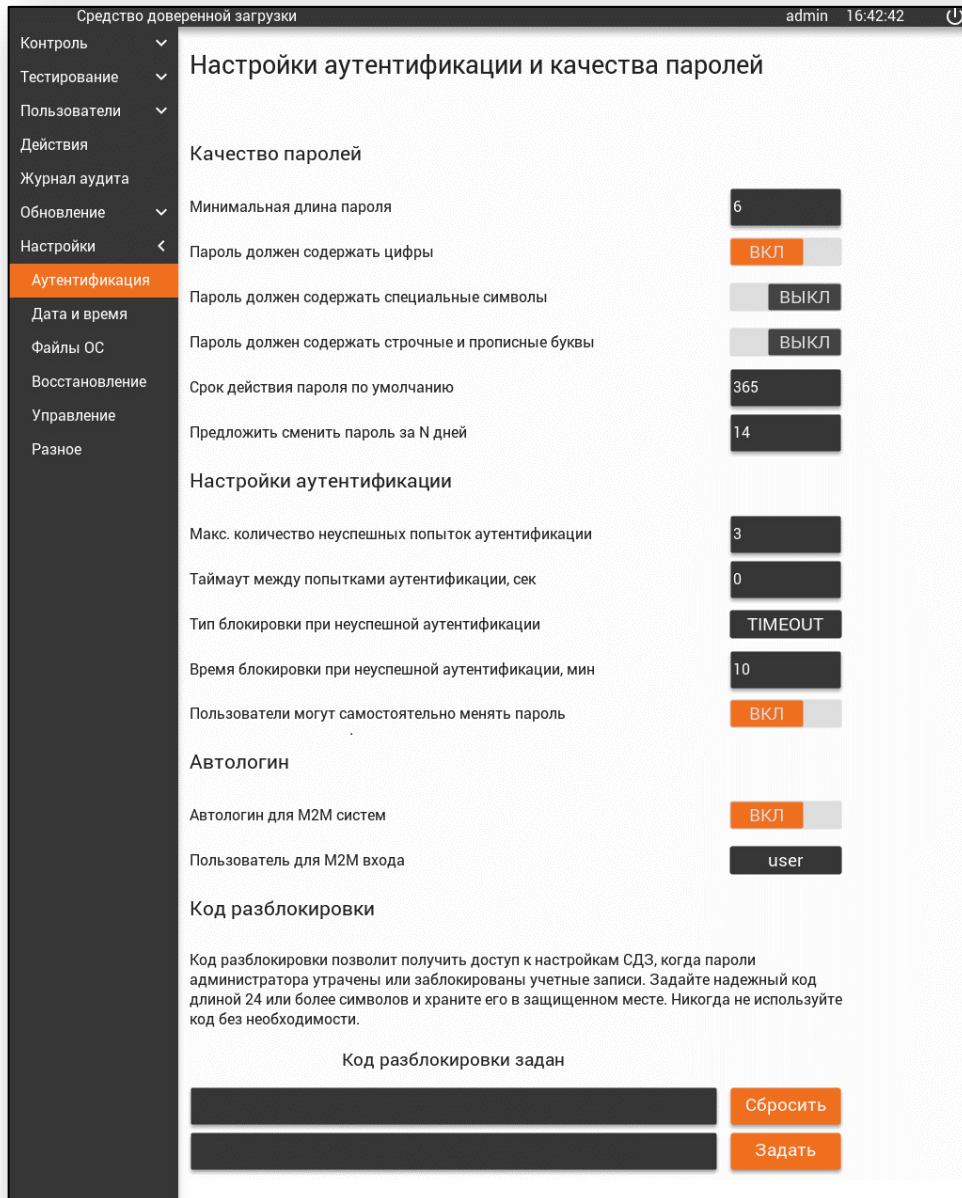


Рисунок 48 - Интерфейс со списком параметров аутентификации

Описание параметров настройки качества паролей, аутентификации, кода разблокировки и автологина, представлены в таблицах 14-17.

Таблица 14 - Список параметров качества паролей

| Параметр политики | Описание | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|----|---|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--|---|---|---|---|---|---|---|---|---|---|---|--|--|--|--|--|--|--|--|--|
| Минимальная длина пароля | <p>Данным параметром устанавливается ограничение на минимальную длину пароля. Если число символов в поле меньше установленного значения, то на экране появится предупреждение.</p> <p>Следует иметь в виду, что если в процессе работы изменено значение длины пароля, то у зарегистрированных учетных записей пользователя она останется прежней до первой смены ими пароля.</p> <p>Возможное значение параметра: от 6 до 14 символов</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Пароль должен содержать цифры | <p>Если данный параметр включен (значение переключателя «ВКЛ»), то при создании пароля в нем должны присутствовать цифры.</p> <p>Возможное значение параметра: «Да/Нет».</p> <p>Пример. У пользователя имеется пароль «password», если описанная выше опция активирована, то при смене пароля на «passwordd» выведется сообщение «В пароле должны быть цифры». Правильной будет смена пароля, например, с «password» на «password12»</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Пароль должен содержать специальные символы | <p>Если данный параметр включен (значение переключателя «ВКЛ»), то при создании пароля в нем должны присутствовать специальные символы, такие как:</p> <table border="1" data-bbox="692 1417 1425 1630"> <tbody> <tr> <td>~</td><td>!</td><td>@</td><td>#</td><td>\$</td><td>%</td><td>^</td><td>&</td><td>*</td><td>(</td> </tr> <tr> <td>)</td><td>_</td><td>-</td><td>+</td><td>{</td><td>}</td><td>[</td><td>]</td><td>\</td><td> </td> </tr> <tr> <td>:</td><td>;</td><td>"</td><td>'</td><td><</td><td>></td><td>,</td><td>.</td><td>?</td><td>/</td> </tr> <tr> <td>=</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </tbody> </table> <p>Возможное значение параметра: «Да/Нет».</p> <p>Пример. Если у пользователя имеется пароль «password1», и если выше описанная опция активирована, то при смене пароля на «password2» выведется сообщение «В пароле должны быть символы». Правильной будет смена пароля, например, с «password1» на «password#»</p> | ~ | ! | @ | # | \$ | % | ^ | & | * | (|) | _ | - | + | { | } | [|] | \ | | : | ; | " | ' | < | > | , | . | ? | / | = | | | | | | | | | |
| ~ | ! | @ | # | \$ | % | ^ | & | * | (| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|) | _ | - | + | { | } | [|] | \ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| : | ; | " | ' | < | > | , | . | ? | / | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| = | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | |
|--------------------------------------|---|
| Наличие прописных букв | <p>Если данный параметр включен (значение переключателя «ВКЛ»), то при создании пароля в нем должны присутствовать строчные и прописные буквы.</p> <p>Возможное значение параметра: «Да/Нет».</p> <p>Пример: Если у пользователя имеется пароль «password1», и, если выше описанная опция активирована, то при смене пароля на «paсsword1» выведется сообщение «В пароле должны быть прописные буквы». Если пользователь сменит пароль «password1» на «paСsword1», то операция успешно завершится</p> |
| Срок действия пароля по умолчанию | <p>Данным параметром устанавливается срок действия пароля по умолчанию для всех пользователей при выполнении смены пароля учетной записи пользователем или продления его срока действия. По истечению установленного срока СДЗ автоматически предложит пользователю сменить пароль при аутентификации.</p> <p>Возможное значение параметра: 1 до 1000 дней</p> |
| Напоминание о смене пароля за N дней | <p>С помощью данного параметра система защиты позволит напоминать пользователю о том, что через определенное количество дней необходимо сменить пароль.</p> <p>Напоминание о предстоящей смене пароля будет появляться на экране при аутентификации пользователя или администратора, начиная с того момента, когда до смены пароля осталось количество дней, равное установленному значению для этой политики.</p> <p>Возможное значение параметра: от 1 до 60 дней</p> |

Таблица 15 - Список параметров политики аутентификации

| Параметр политики | Описание |
|---|---|
| Максимальное количество неуспешных попыток аутентификации | <p>Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе пароля. Если при входе на защищенное СБТ пользователь ввел неверный пароль, то система выдаст предупреждение «Неверный пароль». Если число ошибок больше допустимого, учетная запись будет заблокирована на определенное время, и пользователь не сможет загрузить компьютер и ОС. При этом система защиты выдаст сообщение «Пользователь заблокирован».</p> <p>Возможное значение параметра: от 1 до 8 попыток</p> |
| Таймаут между попытками аутентификации, сек | <p>Значение, установленное для этого параметра, регламентирует время между неудачными попытками ввода пароля. В данный интервал времени вход невозможен.</p> <p>Возможное значение параметра: от 0 до 30 сек</p> |
| Тип блокировки при неуспешной аутентификации | <p>Данный параметр позволяет выбрать способ блокировки учетной записи пользователя. Если установлено значение параметра «FOREVER», то учетная запись заблокируется навсегда. Если установлено значение параметра «TIMEOUT», то учетная запись пользователя будет заблокирована на определенное время, по истечении которой учетная запись автоматически разблокируется.</p> <p>Возможное значение параметра: «FOREVER /TIMEOUT»</p> |

| | |
|---|--|
| Время блокировки при неуспешной аутентификации, мин | <p>Данный параметр позволяет установить, сколько времени учетная запись будет заблокирована после того, как пользователь ввел неверный пароль больше допустимого числа раз. В этот временной интервал пользователь не сможет загрузить ОС. По истечении указанного времени учетная запись автоматически разблокируется, и пользователь снова получит возможность ввести пароль. Сбросить автоматическую блокировку досрочно может только администратор СДЗ.</p> <p>Возможное значение параметра: от 1 до 30 минут</p> |
| Пользователи могут самостоятельно менять пароль | <p>Если данный параметр включен, то пользователь может самостоятельно проводить смену своего пароля, в том числе и по истечении срока действия</p> <p>Возможное значение параметра: «ВКЛ/ВЫКЛ»</p> |

Таблица 16 – Настройки кода разблокировки

| Параметр | Описание |
|-------------------|---|
| Поле статуса | Сообщение “Задайте код разблокировки здесь” приглашает задать код, если он еще не установлен. Если код установлен, сообщается “Код разблокировки задан” |
| Два поля ввода | Для задания кода разблокировки требуется ввести его в оба этих поля. Код в первом и втором поле должен совпасть. |
| Кнопка “Задать” | При нажатии кнопки значение из поля ввода сохраняется как код разблокировки |
| Кнопка “Сбросить” | При нажатии кнопки код разблокировки удаляется |

Таблица 17 - Список параметров автологина

| Параметр | Описание |
|--------------------------|--|
| Автологин для М2М систем | <p>Данный параметр позволяет установить автоматическую загрузку ОС. Если данный параметр включен, то при последующей загрузке СВТ, на экран, после инициализации данных СДЗ, будет выводиться интерфейс автоматической загрузки, который будет</p> |

| | |
|----------------------------|---|
| | <p>уведомлять пользователя о том, что через определенное время будет произведена автоматическая загрузка ОС. Для прерывания процесса автоматической загрузки ОС при появлении интерфейса, нажмите кнопку «Отмена».</p> <p>Возможное значение параметра: «ВКЛ/ВЫКЛ».</p> <p>Примечание. Перед включением параметра «автологин» администратор СДЗ должен создать отдельную учетную запись пользователя для автологина с минимальными правами доступа, которые будут соответствовать политике безопасности организации</p> |
| Пользователь для M2M входа | Выбор учетной записи пользователя, под которой будет выполняться автоматическая загрузка ОС |

Примечание. В СВТ АС и ИС, для которых необходимо осуществлять автозагрузку штатной ОС, во время работы СДЗ «TSM» должна быть обеспечена возможность физического доступа к интерфейсам взаимодействия с СВТ только для лица, которое однозначно ассоциировано с учетной записью уполномоченного пользователя, используемой для загрузки штатной ОС. При этом учетная запись пользователя СДЗ «TSM», используемая для загрузки штатной ОС СВТ не должна быть соотнесена с ролью «Администратор».

В автоматических устройствах на базе СВТ, которые функционируют без участия пользователя (оператора), во время работы СДЗ «TSM» должна быть исключена возможность физического доступа лиц, которые не являются специалистами, ответственными за его эксплуатацию (администраторами) к интерфейсам взаимодействия с СВТ.

При невозможности выполнения данного условия параметр «Автологин для M2M систем» в настройках СДЗ «TSM» должен быть установлен в состояние ВЫКЛ.

5.7.2. Описание подпункта меню «Дата и время»

В СЗД «TSM» предусмотрены собственные часы реального времени, или RTC, которые питаются от автономного источника питания (батарейка). Они используются для упорядочивания регистрации событий в журнале аудита по времени и дате, а также для контроля срока действия пароля.




При первом запуске СДЗ в режиме администрирования, пользователь с ролью

администратора СДЗ может столкнуться с проблемой неправильно заданных часовых поясов, текущей даты и времени. В данном случае, чтобы выполнить соответствующие настройки СДЗ «TSM», перейдите в пункт основного меню «**Настройки**», а затем в списке настроек выберите «**Дата и время**». Далее на экране появится интерфейс (см. рисунок 49) с параметрами, которые разбиты на следующие группы:

- 1) Дата. Устанавливает день, месяц и год;
- 2) Время. Устанавливает часы и минуты;
- 3) Часовой пояс. Устанавливается необходимый часовой пояс.



Рисунок 49 - Интерфейс настройки даты и времени

Процесс настройки выполняется при помощи кнопок с изображением стрелок  и . Для сохранения установок следует нажать кнопку .

Примечание. Если при каждом запуске СДЗ отображается неверное время и дата, значит, вышла из строя батарейка часов реального времени (RTC). Для устранения неполадки требуется заменить батарейку.

5.7.3. Описание подпункта меню «Файлы ОС»

Для того чтобы указать место, откуда будет производиться загрузка ОС, а также раздел загрузки и хранения файлов образов обновлений выберите пункт основного меню «**Настройки**» и перейдите в подпункт «**Файлы ОС**», далее на экран выводится

интерфейс с отображением параметров установки разделов ОС и полного пути к файлу ядра основной ОС и к файлу параметров ядра основной ОС (см. рисунок 50), которые разбиты на группы:

- 1) - Разделы ОС. Устанавливает системный и загрузочный раздел ОС;
- 2) - Файлы ОС. Указывает полный путь в разделе ОС к файлу ядра и к его параметрам ядра основной ОС.
- 3) - Раздел обновления. Устанавливает раздел обновления для СДЗ «TSM» и ОС, а также указывает путь к каталогу загрузки и хранения файлов образов обновлений в данном разделе.

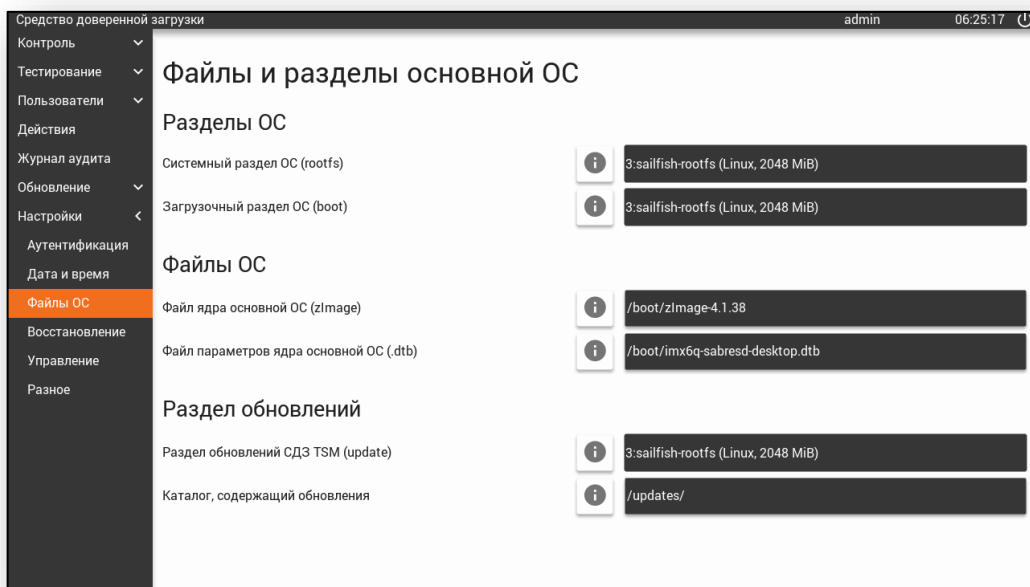


Рисунок 50 – Интерфейс расположения файлов и разделов основной ОС

Полное описание параметров установки файлов и разделов основной ОС, представлено в таблице 18.

Таблица 18 - Описание параметров установки файлов и разделов основной ОС

| № п/п | Обозначение группы | Параметры настройки | Описание |
|-------|--------------------|------------------------------|--|
| 1 | Разделы ОС | Системный раздел ОС (rootfs) | Устанавливает раздел ЗН от куда будут загружаться исполняемые и конфигурационные файлы, системные файлы, системные |

| | | | |
|---|--------------------|---|---|
| | | | библиотеки ОС |
| 2 | | Загрузочный раздел ОС (boot) | Устанавливает раздел ЗН от куда будут загружаться образ ядра (zImage) и его параметр (.dtb) ОС. Может совпадать с rootfs |
| 3 | Файлы ОС | Файл ядра основной ОС (zImage) | Указывает полный путь к файлу ядра относительно раздела boot |
| 4 | | Файл параметров ядра основной ОС (.dtb) | Указывает полный путь к файлу .dtb относительно раздела boot. Если значение не установлено, используется имя по умолчанию для платформы |
| 5 | Разделы обновлений | Раздел обновлений СДЗ TSM (update) | Устанавливает раздел ЗН, куда будут загружаться обновления. Может совпадать с любым системным или пользовательским разделом |
| 6 | | Каталог, содержащий обновления | Указывает каталог, содержащий обновления на разделе update |

5.7.4. Описание подпункта меню «Восстановление»

Для того чтобы указать место, откуда будет производиться загрузка ОС восстановления, необходимо:

1. Выбрать пункт основного меню **«Настройки»** и перейти в подпункт

«Восстановление»;

2. В появившемся интерфейсе (см. рисунок 51) подтвердить установку ОС восстановления, переведя переключатель **«Установлена ОС восстановления»** в положение **ВКЛ**;

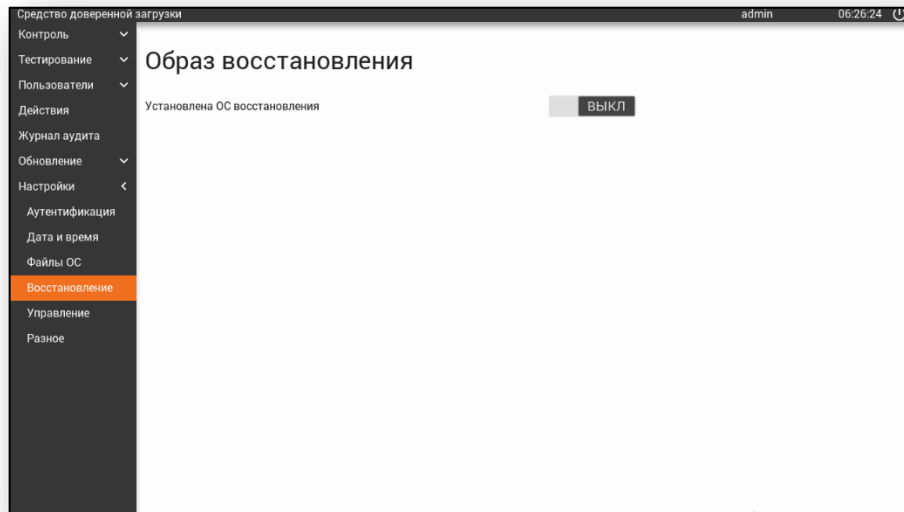


Рисунок 51 - Интерфейс расположения файлов и разделов ОС восстановления

3. Далее, следует произвести установку следующих параметров (см. рисунок 52):
- Раздел с ОС восстановления (recovery) – из выпадающего списка выбирается раздел от куда будут загружаться ядро, исполняемые и конфигурационные файлы, системные библиотеки;
 - Путь и имя файла ядра (zimage) – указывается полный путь к файлу ядра относительно раздела recovery;
 - Путь и имя файла параметров ядра (.dtb) – указывается полный путь к файлу параметров ядра относительно раздела recovery.

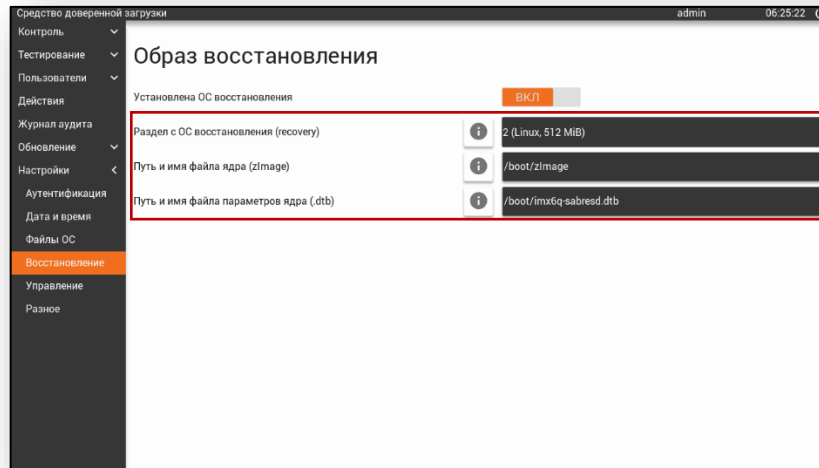


Рисунок 52 - Параметры настройки образа восстановления

5.7.5. Описание подпункта меню «Управление»

СДЗ «TSM» поддерживает функцию удаленного управления, что предполагает установление соединения с неким сервером для выполнения следующих действий:

- 1) Получение и исполнение команд от удаленного доверенного центра управления;
- 2) Передача в ЦУ результатов исполнения команд;
- 3) Выгрузка журнала аудита в ЦУ;
- 4) Обновление компонентов СДЗ и ОС по командам из ЦУ.

Выполнение перечисленных действий осуществляется во взаимодействии с:

- 1) СПО «Доверенная среда исполнения»;
- 2) Трастлет удаленного управления.

Стоит отметить, что СДЗ «TSM» не создает и не поддерживает канал управления самостоятельно. Вместо этого СДЗ полагается на наличие сертифицированного ПО, способное обеспечить целостность и доверенность канала управления.

Таким образом СДЗ «TSM» не обеспечивает настройку удаленного управления, а ограничивается настройкой технических мер контроля для управления.

Для настройки технических мер контроля для управления выберите пункт основного меню **«Настройки»** и перейдите в подпункт **«Управление»**.

Далее на экран выводится интерфейс с отображением следующих параметров (см. рисунок 53), которые разбиты на группы:

- 1) Удаленное управление;

2) Контроль соединения с центром УУ после запуска ОС.

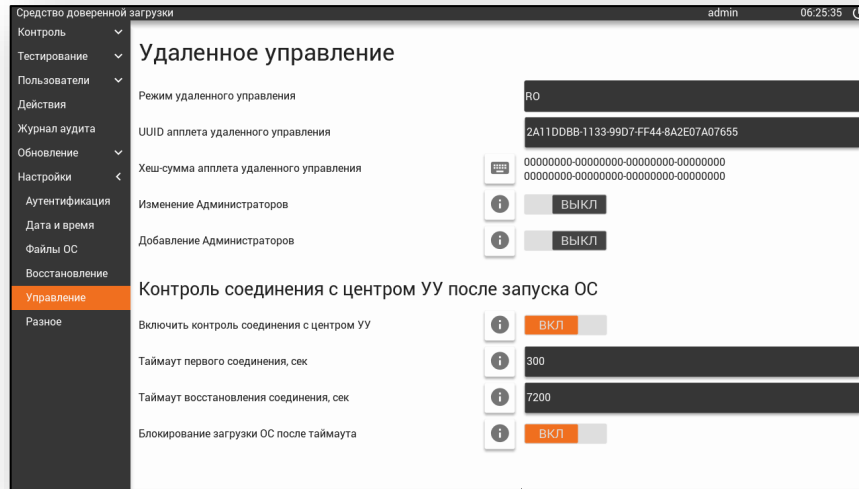


Рисунок 53 - Параметры настройки технических мер контроля для управления

Описание параметров настройки и их значений представлено в таблице 19.

Таблица 19 – Описание параметров настройки технических мер контроля для управления

| № п/п | Обозначение группы | Параметры настройки | Описание | | | | | | | | |
|----------|------------------------------------|--|---|----------|----------|-------|-------------|------|---------------|------|-----------------|
| 1 | Удаленное управление | Режим удаленного управления | Устанавливает режим удаленного управления. Принимаемые значения: <table border="1"> <thead> <tr> <th>Значение</th> <th>Описание</th> </tr> </thead> <tbody> <tr> <td>[OFF]</td> <td>Нет доступа</td> </tr> <tr> <td>[RO]</td> <td>Только чтение</td> </tr> <tr> <td>[RW]</td> <td>Чтение и запись</td> </tr> </tbody> </table> | Значение | Описание | [OFF] | Нет доступа | [RO] | Только чтение | [RW] | Чтение и запись |
| Значение | | Описание | | | | | | | | | |
| [OFF] | Нет доступа | | | | | | | | | | |
| [RO] | Только чтение | | | | | | | | | | |
| [RW] | Чтение и запись | | | | | | | | | | |
| 2 | UUID апплета удаленного управления | Указывается идентификатор трастлета удаленного управления. Возможное значение параметра: Значение параметра указано в ПО обеспечивающий доверенный канал управления. | | | | | | | | | |

| | | | |
|---|---|---|---|
| 3 | | Хеш-сумма апплета удаленного управления | Указывается контрольная сумма трастлета удаленного управления. Возможное значение параметра: Значение параметра указано в ПО обеспечивающий доверенный канал управления. |
| 4 | | Изменение Администраторов | Устанавливает управление учетными записями администратора. Возможное значение параметра: «ВКЛ/ВЫКЛ». |
| 5 | | Добавление Администратора | Устанавливает присвоение пользователям роли администратора. Возможное значение параметра: «ВКЛ/ВЫКЛ». |
| 6 | Контроль соединения с центром УУ после загрузки | Включить контроль соединения с центром УУ | Выполняет контроль установленного соединения при работе ОС с центром удаленного управления. В случае потери связи работа ОС завершается. Возможное значение параметра: «ВКЛ/ВЫКЛ». |
| 7 | | Таймаут первого соединения, сек | Устанавливает время с момента старта ОС для установления соединения с центром УУ. Если соединение не установлено за этот период, работа ОС завершается. Возможное значение параметра: от 1 до 7200 сек. |
| 8 | | Таймаут восстановления соединения, сек | Указывает максимальный интервал пропадания |

| | | | |
|---|--|---|---|
| | | | соединения с центром УУ после первого установления соединения. Если соединение не восстанавливается за этот период, работа ОС завершается. Возможное значение параметра: от 1 до 86400 сек. |
| 9 | | Блокирование загрузки ОС после таймаута | Позволяет выполнять блокировку повторного входа пользователя (без роли администратора СДЗ) и загрузку ОС после таймаута соединения Возможное значение параметра: «ВКЛ/ВЫКЛ». |

Примечание: В СВТ АС и ИС, в том числе включающих и автоматические устройства на базе СВТ, для которых обеспечиваются расширенные возможности по хранению и анализу данных аудита СДЗ «TSM» и/или существует необходимость удаленного управления работой и параметрами СДЗ «TSM», должна быть исключена возможность физического доступа к интерфейсам взаимодействия с СВТ для лиц, которые не являются пользователями.

Для передачи данных аудита и команд (данных) управления между программным интерфейсом СДЗ «TSM» и программным интерфейсом средства (агента) удаленного управления должен быть организован доверенный канал. При этом, меры защиты информации, используемые при реализации доверенного канала должны соответствовать требованиям нормативных документов ФСТЭК России. При необходимости должны использоваться средства криптографической защиты информации, сертифицированные в системе сертификации ФСБ России.

Доверенный маршрут для уполномоченного пользователя средства (агента) удаленного управления должен обеспечиваться собственными механизмами средства (агента) удаленного управления, осуществляющими идентификацию, аутентификацию и управление доступом, либо для его реализации должны использоваться (при необходимости) внешние средства защиты информации,

имеющие аналогичные механизмы. Меры защиты информации, используемые при реализации доверенного маршрута должны соответствовать требованиям нормативных документов ФСТЭК России.

Лицо, которое ассоциировано с учетной записью уполномоченного пользователя с ролью «Администратор», используемой для локального управления СДЗ «TSM», должно быть одновременно ассоциировано с учетной записью уполномоченного пользователя средства (агента) удаленного управления. Правила управления доступом должны обеспечивать для данного уполномоченного пользователя средства (агента) удаленного управления выполнение действий по управлению СДЗ «TSM» через доверенный канал.

При невозможности выполнения данных условий параметр «Режим удаленного управления» функции безопасности «Управление работой и параметрами» СДЗ «TSM» должен быть отключен.

5.7.6. Описание подпункта меню «Разное»

Для выполнения дополнительных механизмов настройки СДЗ «TSM» выберите пункт основного меню **«Настройки»** и перейдите в подпункт **«Разное»**. Далее на экране будет выведен интерфейс с дополнительными параметрами настройки (см. рисунок 54) разбитые на следующие группы:

- Журнал аудита;
- Опции ОС и TEE;
- Контроль целостности ФС.

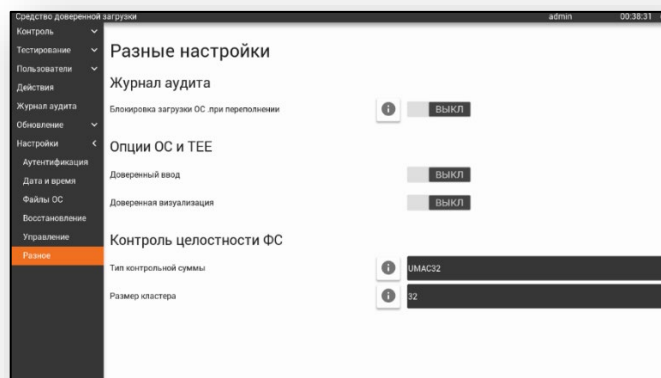


Рисунок 54 - Интерфейс с дополнительными параметрами СДЗ «TSM»

Группа **«Журнал аудита»** содержит параметр блокировки загрузки ОС пользователем при переполнении журнала аудита, для того чтобы активировать

данный параметр переведите переключатель в положение **ВКЛ**. Таким образом при переполнении журнала аудита на этапе инициализации данных СДЗ «TSM» появится сообщение о невозможности выполнить загрузку ОС пользователем и будет разрешён вход только в режиме администрирования.

Группа **«Опции ОС и TEE»** содержит параметры, обеспечивающие возможность использования доверенного ввода и доверенной визуализации из ОС, для того чтобы активировать данные параметры переведите переключатель напротив пункта **«Доверенный ввод»** и **«Доверенная визуализация»** в положение **ВКЛ**.

Группа **«Контроль целостности ФС»** содержит параметры, позволяющий выбрать алгоритм расчета КС, применяемый при контроле ФС, а также установить размер кластера для подсчета КС. Для этого напротив пунктов **«Тип контрольной суммы»** и **«Размер кластера»** из всплывающего списка выберите алгоритм расчета контрольной суммы и размер кластера (см. рисунок 55).

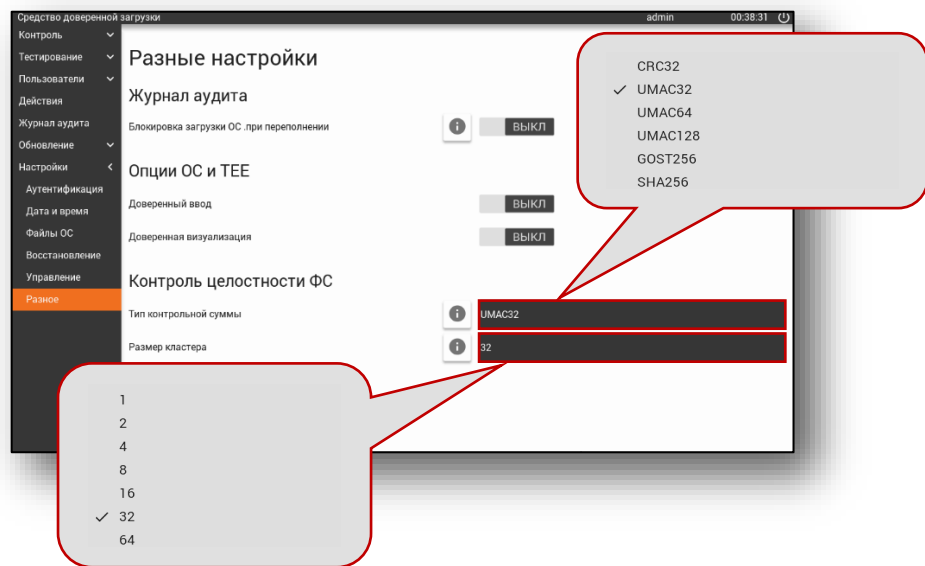




Рисунок 55 – Дополнительные параметры настройки контроля целостности ФС

6. ВЫХОД ИЗ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА АДМИНИСТРИРОВАНИЯ СДЗ «TSM»

Выход из интерфейса администрирования СДЗ «TSM» осуществляется следующими способами:

- 1) Загрузка ОС (см. подразд. 5.4);
- 2) Выключение СВТ. Для этого необходимо нажать кнопку , расположенную в заголовке окна. После чего на экране появится всплывающее окно (см. рисунок 56), в котором нужно нажать кнопку .

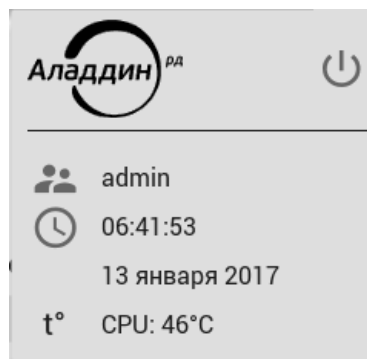


Рисунок 56 - Всплывающее окно

При нажатии на эту кнопку на экране будет выведено сообщение, требующее подтверждения выключения СВТ (см. рисунок 57). В случае положительного ответа будет выполнен выход из графического интерфейса администрирования СДЗ «TSM» и произойдет выключение СВТ.

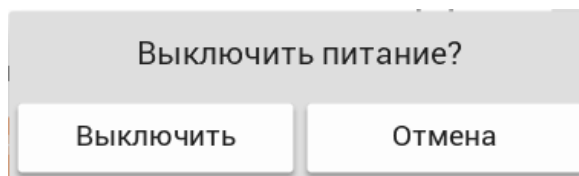


Рисунок 57 - Выключение СВТ

ПРИЛОЖЕНИЕ А

Варианты разбиения ЗН на разделы и значения параметров настройка доступа к разделам ЗН

Выполнение процесса разбиения ЗН на разделы является важной частью перед установкой ОС, т.к. нужно знать на какое количество разделов следует разбить ЗН, для того чтобы подготовить место для размещения объектов ОС и вспомогательных объектов (подробное описание объектов указано в подразделе 3.6).

Таким образом, в данном приложении представлены варианты схем разбиения ЗН на разделы (Таблица 20) и даны ориентировочные размеры (Таблица 21), а также значения параметров настройки доступа к разделам ЗН (Таблица 22) для каждого из варианта, которые обеспечивают их целостность и защиту.

Примечания:

- 1) Приведенные варианты схемы разбиения ЗН и значения параметров настройки доступа не являются обязательными к исполнению и имеют рекомендательный характер;
- 2) Для каждого раздела можно дать ориентировочный размер, но в значительной степени размер разделов будет зависеть от устанавливаемой ОС, поэтому в таблице 21 приводятся ориентировочные размеры для ОС Linux Debian.

Таблица 20 - Варианты разбиения ЗН на разделы и их описание

| Обозначение | Разделы | Описание |
|-------------|-----------------------|--|
| V1 | Sys + RootFS | При этом варианте, ОС находится на разделе RootFS и включает файлы для загрузки ОС и пользовательские данные. RootFS в этом случае должен иметь формат Ext2/Ext3. |
| V2 | Sys + Boot + RootFS | При этом варианте, файлы для загрузки ОС размещаются на разделе Boot, и этот раздел должен иметь формат FAT/FAT32 или Ext2/Ext3. Раздел RootFS может быть отформатирован в любую ФС, поддерживаемую ядром. |
| V3 | Sys + Boot + RootFS + | Данный вариант аналогичен предыдущему + добавляется раздел |

| | | |
|----|----------------------------|---|
| | Recovery ¹ | Recovery. Что касается Recovery, то допустимым является формат ФС Ext2/Ext3, так как с раздела будут читаться образ ядра и Device Tree в случае загрузки ОС восстановления. |
| V4 | Sys + Boot + RootFS + User | При этом варианте, файлы для загрузки ОС размещаются на разделе Boot, и этот раздел должен иметь формат FAT/FAT32 или Ext2/Ext3. Раздел RootFS может быть отформатирован в любую ФС, поддерживаемую ядром. Раздел User хранит пользовательские данные и может иметь любой формат ФС. Данный вариант позволяет перезаписывать раздел RootFS, содержащий все файлы ОС, не нарушая данных пользователей. |
| V5 | Sys + RootFS + Var + User | При этом варианте, файлы для загрузки ОС размещаются на разделе Rootfs, как и часть файлов операционной системы: библиотеки, исполняемые файлы и файлы настроек в каталоге /etc. Раздел RootFS должен быть отформатирован в Ext2/Ext3. В раздел Var помещается содержимое каталогов /var, /tmp и некоторых других. Формат ФС раздела Var – любой. Раздел User хранит пользовательские данные (/home) и может иметь любой формат ФС, В случае если используется удаленное обновление, то в данном варианте, в качестве раздела Update должен использоваться Var, на нем создается каталог с именем, например, /var/updates. Это может быть не совсем |

¹ Раздел Recovery может быть добавлен в любую схему без изменений ее сути. Дальше мы не будем включать Recovery для простоты.

| | | |
|----|---|--|
| | | удобно, так как СДЗ TSM потребуется доступ к разделу Var и поэтому он должен будет иметь формат Ext2 или Ext3. Администратор может захотеть для раздела Var файловую систему с журналированием, так как для Read/Write раздела это имеет смысл, но журналирование недоступно в Ext2/3. Поэтому для удаленного обновления удобно сделать отдельный раздел Update (смотри ниже), он может нести ФС FAT/FAT32 либо Ext2/Ext3: |
| V6 | Sys + RootFS + Var + User + Update | При этом варианте раздел RootFS должен содержать Ext2/Ext3, а Var и User могут иметь любую ФС, что достаточно гибко для любых применений. Так как RootFS – Read-Only, она спокойно будет работать с ФС Ext2 или Ext3, без журнала, так как он в этом случае не нужен. |
| V7 | Sys + Boot + RootFS + Var + User + Update | И, наконец, самый гибкий с точки зрения выбора ФС вариант. Здесь Boot и Update должны иметь тип FAT/FAT32 или Ext2/3, а RootFS, Var и User могут нести любую ФС. |

Таблица 21 – Ориентировочные размеры разделов ЗН

| Название раздела | Размер | Примечание |
|------------------|-----------|--|
| Sys | 8-64 Мб | – |
| Boot | 16-128 Мб | Размер зависит от необходимости хранить старые версии ядра Linux при обновлении, как это делают некоторые сборки |
| Recovery | 16-512 Мб | Размер зависит от типа ОС. Сборка Buildroot уместится в 16 Мб, урезанная инсталляция Debian может влезть в 512Мб |

| | | |
|--------|------------------------------------|---|
| RootFS | ≥2 Гб | В варианте с Read-Only RootFS 2Гб хватает на полную установку Debian 9 с графической подсистемой. В варианте с Read/Write полная система уместится в 4Гб. Вариант, собранный из Buildroot, влезет и в 128Мб |
| Var | ≥3 Гб | При установке полного Debian 9 под Var нужно около 3Гб, потому что там хранятся все изменяемые файлы, включая все пакеты обновлений. При установке урезанных версий Linux раздел Var можно значительно уменьшить. |
| User | Зависит от пользовательских данных | Можно предположить, что для систем с графическим интерфейсом под User стоит выделить не менее 512Мб |
| Update | От 1 Мб | Если речь идет только о обновлении СДЗ TSM, то подойдет любой раздел больше 1Мб. Если есть задача обновлять и разделы ОС, размер Update должен быть значительно больше – 2Гб и более. |

Таблица 22 – Рекомендуемые значения параметров настройки доступа к разделам ЗН

| | V1 | V2 | V3 | V4 | V5 | V6 | V7 |
|----------|-------------|------------|-------------|------------|------------|------------|------------|
| Sys | Без доступа | | | | | | |
| Boot | – | Read-Only | Read-Only | Read-Only | – | – | Read-Only |
| RootFS | Read/Write | Read/Write | Read/Write | Read/Write | Read-Only | Read-Only | Read/Only |
| Var | – | – | – | – | Read/Write | Read/Write | Read/Write |
| User | – | – | – | Read/Write | Read/Write | Read/Write | Read/Write |
| Update | – | – | – | – | – | Read/Write | Read/Write |
| Recovery | – | – | без доступа | – | – | – | – |

ПРИЛОЖЕНИЕ Б

Формирование txt-файла для изменения параметров таблицы разделов ЗН

Как уже было сказано, при установке ОС на СВТ важно разбить ЗН на правильное количество разделов, которое соответствовало бы требованиям инсталляционного комплекта ОС. Для этого администратор СДЗ должен произвести соответствующие изменения в таблице разделов ЗН, которые бы удовлетворяли требованиям для установки ОС на СВТ.

Так, в пункте 5.6.4 говорится, что для того чтобы произвести изменения в таблице разделов ЗН предварительно требуется сформировать txt-файл с параметрами разбиения. Для этого воспользуйтесь любым текстовым редактором позволяющий создавать файлы в формате .txt и создайте текстовый документ, в котором в виде строк будут указаны следующие параметры разбиения ЗН:

part start size type.

Описание параметров строки и его значений представлено в таблице 23 – Параметры разбиения ЗН.

Таблица 23 – Параметры разбиения ЗН

| Обозначение | Описание |
|-------------|--|
| Part | Указывает обозначение основных разделов ЗН. Возможное значение: 1...4 |
| | Указывает обозначение расширенных разделов ЗН. Возможное значение: e (также можно указывать 5...32, но нумерация не сохранится, они будут добавлены в порядке появления в файле) |
| Start | Указывает начальный сектор раздела ЗН. Пример обозначения: <ul style="list-style-type: none"> - 131072 – точный номер сектора ЗН - auto – автоматически указывает сектор начала раздела (всегда для расширенного раздела ЗН) |
| Size | Указывает размер раздела ЗН Пример обозначения: <ul style="list-style-type: none"> - 128k – 128 килобайт - 128M – 128 мегабайт - 128G - 128 гигабайт |

| | |
|------|--|
| | - auto – автоматически устанавливает размер создаваемого раздела ЗН |
| Type | Указывает тип ФС на разделе ЗН Возможные значения: <ul style="list-style-type: none"> - 0x00 – 0xFF – идентификатор файловой системы, представленный в виде числа в шестнадцатеричной форме; - FAT32; - Linux; - Ext |

Примечание:

- 1) Количество строк в txt-файле соответствует количеству разделов, на которые будет разбит ЗН;
- 2) Разбить ЗН можно всего на 4 основных раздела, причем один из них будет является расширенным разделом, который может содержать несколько логических. Это обусловлено тем, что в MBR под таблицу разделов выделено 64 байта, а каждая запись занимает 16 байт.

Для большей наглядности, приведен пример содержимого txt-файла, который демонстрирует вариант разбиение ЗН на три основных раздела и один расширенный, со следующими параметрами:

```

1  131072  128M  0xC
2  auto    auto   Linux
3  auto    auto   Ext
e  auto    auto   Linux

```