|  |  |
| --- | --- |
|  |  |
| **Средство защиты информации**  **для контроллера «МТК-30.КП»**  Руководство администратора КСЗ  RU.АДМШ.421457-04 34 01  Версия 1.2 | |
| Москва, 2023 | |

**АННОТАЦИЯ**

Настоящий документ содержит инструкции по установке и эксплуатации комплекса средств защиты (КСЗ) информации ПО контроллера «МТК-30.КП».

КСЗ состоит их встроенных средств защиты информации (ВСЗИ) контроллера «МТК-30.КП» и программы «Конфигуратор », предназначенной для администрирования ВСЗИ.

В документе описаны принципы администрирования ВСЗИ, типовые функции и задачи безопасности администратора, а также описываются конкретные инструменты для выполнения этих функций и задач.

Настоящий документ предназначен для персонала эксплуатирующей организации, задействованного эксплуатации в программно-технических средств ПТК «Систел».

Оформление программного документа «Руководство Администратора по безопасности» произведено по требованиям ЕСПД (ГОСТ 19.101-77 [[1]](#footnote-1)1), ГОСТ 19.103-77 [[2]](#footnote-2)2), ГОСТ 19.104-78\* [[3]](#footnote-3)3), ГОСТ 19.105-78\* [[4]](#footnote-4)4), ГОСТ 19.106-78\* [[5]](#footnote-5)5), ГОСТ 19.402-78\* [[6]](#footnote-6)6), ГОСТ 19.604-78\* [[7]](#footnote-7)7)).

**СОДЕРЖАНИЕ**

[1 СТРУКТУРА КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ 5](#_Toc149055435)

[2 ЗАДАЧИ АДМИНИСТРИРОВАНИЯ СЗИ 7](#_Toc149055436)

[2.1 Минимальный состав технических средств 7](#_Toc149055437)

[2.2 Минимальный состав программных средств 7](#_Toc149055438)

[2.3 Требования к пользователям Программы 7](#_Toc149055439)

[2.4 Функции и задачи администрирования СЗИ 7](#_Toc149055440)

[3 УСТАНОВКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 8](#_Toc149055441)

[3.1 Установка ПО МЗИ 8](#_Toc149055442)

[3.2 Контроль результа установка ПО МЗИ 8](#_Toc149055443)

[3.3 Проверки установки ПО МЗИ 9](#_Toc149055444)

[3.4 Настройка первичной конфигурации МЗИ 10](#_Toc149055445)

[3.5 Установка программы «Конфигуратор» 11](#_Toc149055446)

[3.6 Проверка конфигурация МЗИ с помощью ПО «Конфигуратор» 11](#_Toc149055447)

[4 УПРАВЛЕНИЕ ПОДКЛЮЧЕНИЕМ К МЗИ 13](#_Toc149055448)

[4.1 Организация защищённого канала связи 13](#_Toc149055449)

[4.2 Настройка подключения 13](#_Toc149055450)

[4.3 Подключение к серверу МЗИ 15](#_Toc149055451)

[4.4 Вход в Программу 20](#_Toc149055452)

[5 УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ 25](#_Toc149055453)

[5.1 Работа с учётными записями пользователей 25](#_Toc149055454)

[5.2 Управление доступом пользователей 32](#_Toc149055455)

[5.3 Настройка политик безопасности 37](#_Toc149055456)

[6 КОНТРОЛЬ ЦЕЛОСТНОСТИ 40](#_Toc149055457)

[6.1 Интерфейс ручного контроля целостности системы 40](#_Toc149055458)

[6.2 Списки контроля целостности 42](#_Toc149055459)

[6.3 Процедура проверки целостности 45](#_Toc149055460)

[7 АРХИВИРОВАНИЕ И ВОССТАНОВЛЕНИЕ 47](#_Toc149055461)

[7.1 Выгрузка эталонной копии компоненты ПО МТК-30.КП: 47](#_Toc149055462)

[7.2 Выгрузка резервной копии конфигурации ПО МТК-30.КП: 48](#_Toc149055463)

[7.3 Восстановление компонент СПО контроллера из выгруженной эталонной копии 49](#_Toc149055464)

[7.4 Восстановление конфигурации МЗИ и СПО из резервной копии 51](#_Toc149055465)

[7.5 Процедура замены файла 53](#_Toc149055466)

[8 АНАЛИЗ И УПРАВЛЕНИЕ СОБЫТИЯМИ БЕЗОПАСНОСТИ 54](#_Toc149055467)

[8.1 Интерфейс работы с журналом аудита 55](#_Toc149055468)

[8.2 Чтение записей журнала аудита 57](#_Toc149055469)

[8.3 Выборочное чтение записей аудита 58](#_Toc149055470)

[8.4 Просмотр ранее загруженных журналов аудита 60](#_Toc149055471)

[8.5 Очистка журнала аудита 61](#_Toc149055472)

[8.6 Загрузка журнала аудита на syslog-сервер 63](#_Toc149055473)

[8.7 Регистрируемые события безопасности 64](#_Toc149055474)

[9 УПРАВЛЕНИЕ УСПД 66](#_Toc149055475)

[Приложение. Сообщения оператору 67](#_Toc149055476)

[10 Обновление программного обеспечения 69](#_Toc149055477)

[10.1 ПОРЯДОК ОБНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 69](#_Toc149055478)

[Список определений и сокращений 70](#_Toc149055479)

СТРУКТУРА КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ

Комплекс средств защиты (КСЗ) для контроллера «МТК-30.КП» состоит из встроенных средств защиты информации программного обеспечения контроллера (СЗИ ПО Систел) и программы «Конфигуратор», предназначенной для администрирования СЗИ (Рисунок 1).



Рисунок 1 – Структура КСЗ для контроллера «МТК-30.КП»

СЗИ ПО Систел состоят из набора программных Модулей Защиты Информации (далее по тексту – МЗИ), которые реализуют функции защиты информации, обрабатываемой контроллером (далее – *функции безопасности*):

* идентификация и аутентификация пользователей (ИАФ)
* управление доступом (УПД)
* аудит безопасности (АУД)
* контроль целостности (ОЦЛ)
* обеспечение доступности (ОДТ)
* защита программных компонентов СЗИ (ЗИС)
* управление конфигурацией (ЗИС, УПД, ИАФ)

Один из модулей выполняет функции *диспетчера подключений* клиентских мест пользователей к программной среде контроллера.

Администратор ПТК «Систел» использует ПО «Конфигуратор» на АРМ управления ИБ для управления функциями безопасности МЗИ. Для установки доверенного соединения ПО «Конфигуратор» использует компонент МЗИ:клиент[[8]](#footnote-8) (устанавливается на всех клиентских АРМ ПТК «Систел») для обращения к диспетчеру подключений контроллера посредством протокола *systel.link* через интерфейс ИФБО.1

Для выполнения установленных технологических операций операторы системы телемеханики (ТМ) подключаются серверу СПО Zemon (технологическое ПО) через интерфейс ИНТ.2 и протокол *http.* В процессе подключения клиентских приложений формируется запрос на авторизацию через внутренний интерфейс ИФБО.2 в программную среду МЗИ для выполнения обязательной авторизация пользователей-операторов (Рисунок 1).

Любые обращения авторизированных пользователей к информационным объектам контроллера осуществляются с обязательной процедурой проверки прав доступа в МЗИ через специальный интерфейс ИФБО.2.

МЗИ используют набор конфигурационных файлов, в которых определяются параметры (настройки) функций безопасности. Редактирование конфигурационных файлов МЗИ и последующая их загрузка в защищённое хранилище ПО контроллера осуществляется с помощью ПО «Конфигуратор».

ПО «Конфигуратор» используется для процедур восстановления конфигураций МЗИ, создания резервных копий и восстановления компонент ПО контроллера, для скачивания журнала аудита, а также для процедур тестирования функций безопасности.

Контроллеры серии «МТК-30.КП» поставляются с предустановленным СПО Zemon, включая встроенные программные средства защиты информации.

# ЗАДАЧИ АДМИНИСТРИРОВАНИЯ СЗИ

## Минимальный состав технических средств

Программа «Конфигуратор» устанавливается на персональном компьютере (ноутбук) стандартной архитектуры, который носит название «АРМ администратора».

## Минимальный состав программных средств

Программа функционирует под управлением ОС Windows. Программа использует набор стандартных Windows GUI приложений и реализует стандартный интерфейс пользователя.

Для обеспечения доступа из Программы к МЗИ используется протокол TCP/IP.

Для работы ПО «Конфигуратор» должен быть установлен распространяемый пакет Visual C++ для Visual Studio 2019.

## Требования к пользователям Программы

Доступ пользователей к управлению МЗИ осуществляется из программы «Конфигуратор» на основе установленных правил разграничения доступа.

Для обеспечения доступа к функциям управления МЗИ контроллера должны быть созданы учётные записи и типовые роли пользователей cо следующими правами:

* **Администратор Системы.** Выполняет настройку, отладку и диагностику СПО Zemon. Доступны все функции управления МЗИ с помощью ПО «Конфигуратор»
* **Аудитор.** Имеет разрешения по чтению событий журнала аудита и обзор реестра событий безопасности с целью анализа инцидентов.
* **Инженер службы эксплуатации.** Оперативный персонал, имеющий ограниченное право на чтение конфигураций и ошибок системы, выполнению операций по обновлению ПО, включая операции по контролю целостности компонент СПО Zemon.

## Функции и задачи администрирования СЗИ

Администрирование СЗИ осуществляется уполномоченным администратором по безопасности. Для обеспечения безопасности информации в соответствие с данным руководством уполномоченный администратор обязан:

* установить защищённое соединение с рабочего компьютера администратора с программной средой МЗИ (п.4.1)
* создать пользователей, которым надлежит осуществлять доступ к контроллеру и функциям управления СЗИ на основе механизмов разграничения доступа и защиты информации (раздел 5).
* выполнить аудит событий информационной безопасности контроллера. Анализ событий необходим для выявления ошибок в настройках и корректировки правил разграничения доступа, а также для своевременного реагирования на осуществление несанкционированного доступа к защищаемой информации. (п.8)
* сформировать конфигурацию и настроить механизмы работы СЗИ. Загрузить конфигурацию СЗИ в контроллер и отладить функционирование СЗИ.
* Выполнить архивирование программных компонент и данных конфигурационных настроек (п.7.1, 7.2).

# УСТАНОВКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

## Установка ПО МЗИ

Установка программных компонент МЗИ производится в программную среду контроллера, которая включает установленную версию ОС Linux и технологическое CПО Zemon. В ОС Linux должны быть зарегистрированы пользователи – администратор системы «root» и основной пользователь CПО Zemon – «zemon».

Для установки ПО МЗИ используется файл с дистрибутивом ПО МЗИ mziSystelInstall-YYMMDDhhmm.tgz и файл с секретным «ключом» дистрибутива. Файлы с дистрибутивом МЗИ и с ключом передаются Организации согласованным способом.

Для установки дистрибутива СЗИ необходимо выполнить следующие шаги.

1. Установить режим командной строки для входа в систему под учётной записью ОС Linux - **root**.
2. Скопировать с носителя USB архив с дистрибутивом и файл с ключом защиты дистрибутива.
3. Распаковать архив с дистрибутивом:

tar xzf mziSystelInstall-YYMMDDhhmm.tgz

В результате появляется директория **mziSystel** с файлами дистрибутива МЗИ.

1. Переход в директорию mziSystel. Данная папка содержит зашифрованный архив mziDistrib.mzi с файлами МЗИ, программу для распаковывания этого архива, скрипт для его развёртывания mziInstall.sh, файл ReadMe.txt с датой создания дистрибутива, а также файлы md5.sum и sha.sum с контрольными суммами всех файлов в этой директории и файла-архива, который получается после распаковки файла mziDistrib.mzi.
2. Запустить установку МЗИ командой:

./mziInstall.sh -k path\_to\_key\_file

1. По окончанию установки необходимо перезагрузить контроллер.

systemctl reboot

## Контроль результа установка ПО МЗИ

* + - Установлены программные компоненты МЗИ в разделы каталога /**home/iss**, который в рабочем режиме контроллера имеет доступ только для чтения.
    - Сформирован набор конфигурационных файлов МЗИ:
* /home/iss/sys/issSysParam.cfg
* /work/iss/Config/issConfigBase.cfg
* /work/iss/Check/CheckTableW.cfg
* /work/iss/Check/issSysConfig.cfg
  + - Установлены исполняемые файлы МЗИ issAuditSrv, issCheckSrv, issCheckStart, issServer в директории /home/iss/bin, и автономная программа восстановления компонентов МЗИ issRecovery в директории /home/iss/recovery.
    - Установлены рабочие библиотеки МЗИ libauditsrv.so, libcheck.so, libconnectsrv.so, libissaudit.so, libmathconv.so, libusercontrol.so, libuserdefs.so в директории /home/iss/lib.
    - Установлен файл лога аудита issAudit.log в директории /work/iss/Audit.
    - Установлен файл с эталонной копией ПО МЗИ ISS.mzi.ref в директории /work/iss/Reference/iss/ и его копия на защищённом средствами ОС от записи разделе в директории /home/iss/adm.
    - Установлен файл с резервной копией конфигурации МЗИ ISS.mzi.rsv в директории /work/iss/Reserve/iss/.
    - Сформированы учётные записи iss и issadmin. При этом пользователь iss является владельцем всех объектов МЗИ, но у него отсутствует возможность интерактивного входа в систему. Пользователь issadmin является «администратором» МЗИ и предназначен для обслуживания МЗИ в случае аварийных ситуаций и для обновления ПО МЗИ.
    - Права доступа пользователей ОС **zemon, iss, issadmin** настроены по следующим правилам:
* пользователь “**zemon**” имеет доступ только к файлам СПО Zemon, а также предоставляет доступ к своим файлам членам группы пользователей “**zemon**”.
* пользователь “**iss**” имеет доступ к файлам МЗИ и, как член группы “**zemon**”, к файлам и каталогам пользователя “**zemon**”, а также предоставляет доступ к своим файлам членам группы пользователей “**iss**”.
* пользователь “**issadmin**”, как член группы “**iss**”, имеет доступ к файлам и каталогам пользователя “**iss**”, то есть, к исполняемым и конфигурационным файлам МЗИ.

## Проверки установки ПО МЗИ

1. Перезагрузка ПО контроллера
2. В режиме командной строки осуществить вход в Систему под учётной записью issadmin
3. Проконтролировать запущенные процессы МЗИ issAuditSrv, issCheckSrv issServer:

ps aux|grep iss

iss … … 19264 5520 pts/2 … /home/iss/bin/issAuditSrv

iss … … 9996 5576 pts/0 … /home/iss/bin/issCheckSrv

iss … … 28436 5204 pts/1 … /home/iss/bin/issServer

1. Строго рекомендуется изменяем стандартный пароль пользователя issadmin на пароль, удовлетворяющий политике безопасности Организации (см п.4.7).

## Настройка первичной конфигурации МЗИ

Установка МЗИ осуществляется на подготовленную программную среду контроллера, которая включает ОС Linux и СПО Zemon.

Установка ПО МЗИ производится по алгоритму, описанному в п.3.1.1.

Настройка первичной конфигурации МЗИ производится установочным скриптом в процессе развёртывания дистрибутива.

В процессе развёртывания дистрибутива программа установки производит следующие действия.

* + 1. Программные компоненты МЗИ устанавливаются в разделы каталога /**home/iss**, который в рабочем режиме контроллера имеет доступ только для чтения.
    2. Настраиваются права доступа пользователей **zemon, iss, issadmin** по следующим правилам:
* пользователь “**zemon**” имеет доступ только к файлам СПО Zemon, а также предоставляет доступ к своим файлам членам группы пользователей “**zemon**”.
* пользователь “**iss**” имеет доступ к файлам МЗИ и, как член группы “**zemon**”, к файлам и каталогам пользователя “**zemon**”, а также предоставляет доступ к своим файлам членам группы пользователей “**iss**”.
* пользователь “**issadmin**”, как член группы “**iss**”, имеет доступ к файлам и каталогам пользователя “**iss**”, то есть, к исполняемым и конфигурационным файлам МЗИ.

1. Создаются файлы конфигураций МЗИ в директориях каталога **/work/iss**, который имеет доступ на чтение и на запись для членов группы “**iss**”. В процессе инициализации файлов конфигурации создается файл аудита **issAudit.log,** в который в процессе установки записывается информация о создании конфигурационных файлов и события безопасности, возникающие при инициализации ПО контроллера.
2. В директории **/etc/systemd/system**, расположенной на защищенном от записи корневом разделе диска “**/**”, и доступной только администратору ОС «**root**», создаются конфигурационные файлы с инструкциями по запуску компонент МЗИ для системного менеджера управления службами **systemd**.
3. Конфигурация ОС настраивается таким образом, что администратору ОС “**root**” запрещен удалённый доступ в контроллер. В штатном или минимальном режимах функционирования контроллера удалённый доступ к контроллеру невозможен для всех пользователей (поскольку сервер “**sshd**” при старте ОС не запускается). Сервер удалённого доступа **sshd** может быть запущен либо автоматически при возникновении аварийной ситуации, либо специальной командой с АРМ администратора МЗИ.
4. В разделе **/home/iss** создаётся системный конфигурационный файл МЗИ **issSysParam.cfg**, который содержит информацию для генерации ключевой информации, применяемой в механизмах шифрования для защиты конфигурационных файлов МЗИ и файла журнала аудита.
5. Создаётся основной рабочий конфигурационный файл МЗИ, который содержит информацию об учётных записях пользователей и их ролевых профилях, настройки правил парольной политики, групповые и общие параметры безопасности. Также в этом файле содержится описание событий (привязка расширенной информации о событиях к кодам событий) и параметров доступа (привязка разрешений доступа к кодам запросов).
6. Создаётся набор стандартных ролей.
7. Создаются стандартные пользователи.
8. Все настройки, описанные в п.11,12,13 создаются в процессе развёртывания дистрибутива из описаний в текстовых конфигурационных файлах, поставляемых в составе дистрибутива, и могут быть изменены по запросу клиента.
9. Создаётся файл контрольных сумм исполняемых компонентов и конфигурационных файлов МЗИ.
10. Создаётся файл с эталонной копией ПО МЗИ и записывается в раздел **/home/iss**, который в рабочем режиме защищён от записи.

Все файлы конфигураций МЗИ и контрольных сумм являются зашифрованными базами SQLite и защищены от несанкционированного доступа механизмами защиты информации МЗИ.

Доступ к конфигурационным файлам также ограничен (чтение и запись) средствами ОС для системного пользователя **iss** и членов рабочей группы **iss**. Для пользователей c другим системным профилем (**zemon**) доступ к конфигурационным файлам МЗИ полностью закрыт.

## Установка программы «Конфигуратор»

Установка ПО «Конфигуратор» осуществляется с помощью распаковки подготовленного дистрибутива ISSClientSetup\_номер\_версии.

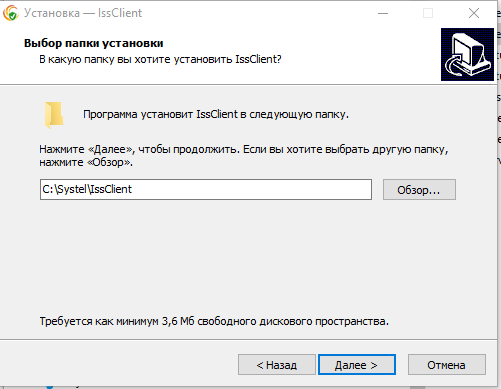


Рисунок 3.5.1 Установка ПО "Конфигуратор"

Необходимо следовать шагам инсталлятора, чтобы завершить установку.

## Проверка конфигурация МЗИ с помощью ПО «Конфигуратор»

После выполнения вышеописанных действий Администратору КСЗ необходимо проконтролировать первичную настройку с помощью ПО «Конфигуратор»:

1. Подключиться к серверу МЗИ с помощью ПО «Конфигуратор» (п.4.3)
2. Проверить целостность компонент (п. 6.1).
3. Проанализировать записанные события безопасности (п. 8 «Анализ и управление событиями безопасности»).
4. Проверить и отредактировать настройки безопасности, в т.ч.настройки парольной политики (5.3 «Настройка политик безопасности»).
5. Проверить и настроить список ролей. По умолчанию создаются три роли:

* "Администратор" – Администратор безопасности
* "Аудитор" – Аудитор системы безопасности
* "Оператор" – Оператор прикладной системы (СПО Zemon)

1. Настроить список пользователей МЗИ. Для этого вызвать окно «Пользователи», считать список текущих пользователей и отредактировать его (5.1 «Работа с учетными записями пользователей»). По умолчанию при инициализации системы создаются два пользователя:

* Admin\Администратор
* Audit\Аудитор

1. Проверить и отредактировать матрицу правил разграничения доступа. Для этого вызвать окно «Правила разграничения доступа» (5.2 «Управление доступом пользователей»).

# УПРАВЛЕНИЕ ПОДКЛЮЧЕНИЕМ К МЗИ

## Организация защищённого канала связи

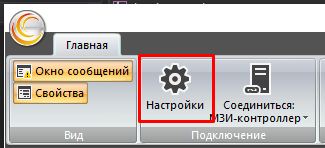
При удалённом управлении функциями МЗИ необходимо выполнить требование обеспечения конфиденциальности информации, передаваемой по каналам связи. С этой целью требуется организовать защищённый канал связи по протоколу TCP/IP.

Настройка протокола IPSec между сервером и клиентским АРМ описана в приложении «Руководство по настройке протокола IPSec для ПТК «Systel» (Приложение 2)

## Настройка подключения

Для доступа пользователя к программной среде МЗИ необходимо установить сетевое соединение с выбранным МЗИ-сервером. Вначале необходимо настроить список серверов для подключения. Для этого на панели инструментов «Главная» необходимо нажать кнопку «Настройки» для вызова интерфейса настройки списка серверов для подключения

(Рисунок 4.2.1).



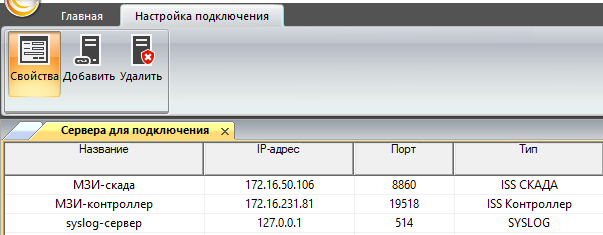
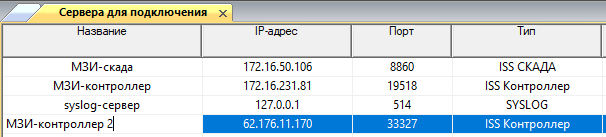


Рисунок 4.2.1 Окно редактирования серверов для подключения

В результате появится новое окно «Сервера для подключения» в рабочей области, в котором можно:

1. Добавить новый сервер в список, нажав кнопку «Добавить» раздела «Настройка подключения» ленты инструментов;
2. Отредактировать данные существующих серверов (Рисунок 4.2.2): изменить имя, IP-адрес подключения, порт, описание. Сделать это можно кликнув двойным щелчком на необходимое поле (после чего станет активен режим редактирования) и ввести необходимые изменения. Тип сервера необходимо выбрать из ниспадающего списка. Доступны следующие типы:
   * ISS контроллер — МЗИ-сервер работает на УСПД.
   * ISS СКАДА — МЗИ-сервер работает на сервере ОИК.
   * Syslog — параметры сервера соответствуют адресу syslog-сервера. Данный тип сервера указывается в том случае, когда необходимо осуществить экспорт данных аудита, полученных от МЗИ-сервера, в syslog. К такому серверу невозможно подключится из ПО «Конфигуратор».



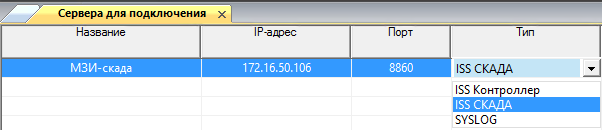


Рисунок 4.2.2 Редактирование сервера для подключения

1. Удалить сервер из списка, выбрав его из списка и нажав кнопку ленты инструментов «Удалить».

На панели инструментов после появления окна также появится контекстная вкладка «Настройка подключения» с функциональными кнопками.

|  |  |  |
| --- | --- | --- |
| **Вид**  **кнопки** | **Название кнопки** | **Пояснение** |
|  | Свойства | Вызывает окно свойств |
|  | Добавить сервер | Добавляет новый сервер в список серверов |
|  | Удалить сервер | Удаляет выбранный сервер |

Список добавленных для подключения серверов будет отображен в меню кнопки «Соединиться» панели инструментов «Главная» (Рисунок 4.2.3). Название выбранного сервера из списка будет являться дополнительной подписью к кнопке «Соединиться».

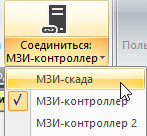


Рисунок 4.2.3 Кнопка для выбора сервера подключения

Если кнопка «Соединиться» будет нажата без выбранного сервера для подключения, то в окне «Сообщения» будет выведено соответствующее предупреждение (Рисунок 4.2.4).

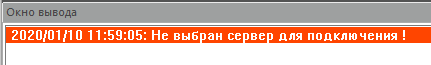


Рисунок 4.2.4 Вывод предупредительного сообщения

## Подключение к серверу МЗИ

После нажатия кнопки «Соединиться» с выбранным сервером для подключения произойдет TCP/IP соединение с выбранным сервером, и, при удачном соединении, появится окно входа в Систему для идентификации пользователя (Рисунок 4.3.1).

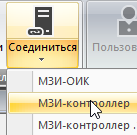
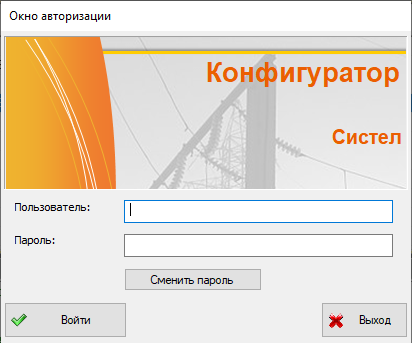
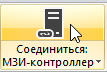
 

Рисунок 4.3.1 Окно авторизации

Окно авторизации имеет следующие элементы управления:

1. Поле «Пользователь», в которое необходимо ввести идентификатор (логин) учетной записи.
2. Поле «Пароль», в которое необходимо ввести аутентификатор.
3. Кнопка «Сменить пароль», после нажатия на которую отобразиться диалог смены пароля.
4. Кнопка «Войти» инициирует соединение с выбранным сервером.
5. Кнопка «Выход» закрывает окно авторизации.

В открывшемся окне авторизации необходимо ввести идентификатор и секрет (пароль) пользователя и нажать кнопку «Войти». При удачной авторизации пользователя установится рабочая сессия между клиентом и сервером, и пользователю станут доступны команды, соответствующие его роли. При этом кнопка ленты инструментов «Соединиться» поменяет название на «Соединен» (Рисунок 4.3.2).

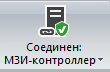
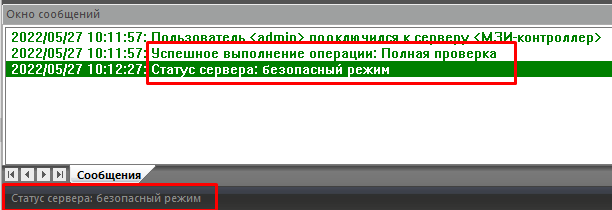


Рисунок 4.3.2 Отображение состояния присоединения на кнопке подключения

После успешного соединения с сервером МЗИ в окно сообщений оператору будет выведен результат проверки целостности Системы (если у пользователя есть соответствующие права), а также текущее состояние сервера: безопасный или минимальный режим.



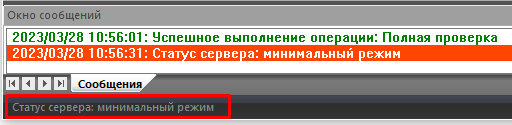


Рисунок 4.3.3 Возможные сообщения оператору после успешного присоединения к Системе

Обработка ошибок авторизации

В случаях ошибок авторизации вход для пользователя может быть заблокирован. Ниже представлен перечень ошибок авторизации и способы их разрешения.

* Неверный логин или пароль при подключении к МЗИ (Рисунок 4.3.4) — будет отображено количество оставшихся попыток ввода корректных данных. Количество допустимых попыток входа задается в настройках безопасности (п.5.3). После превышения допустимого количества попыток входа учетная запись пользователя будет заблокирована на некоторое время (п.5.3).

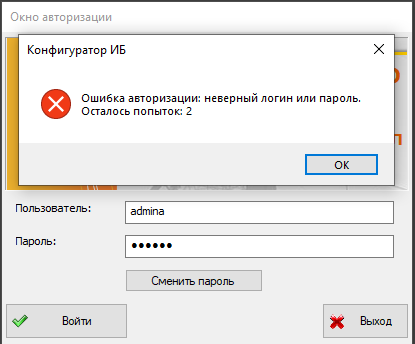




Рисунок 4.3.4 Неверный логин или пароль при подключении к МЗИ

* Ошибка при подключении к сервису (Рисунок 4.3.5) — может быть следствием разрыва соединения сервером после превышения количества допустимых попыток входа.

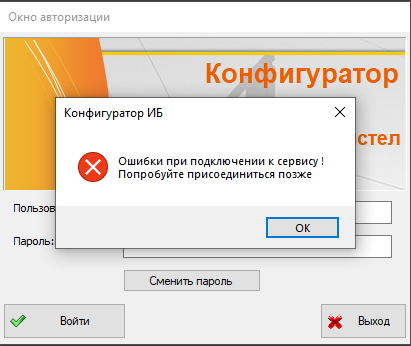


Рисунок 4.3.5 Ошибка при подключении к сервису

* Превышено максимальное количество попыток входа (Рисунок 4.3.6) — появляется при попытке вновь подключится к серверу МЗИ с корректными данными.

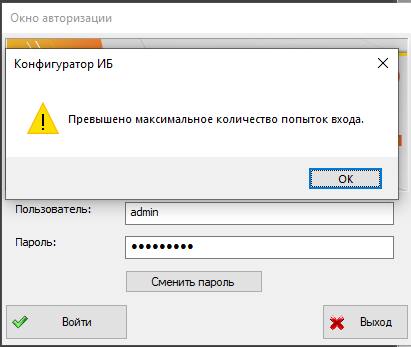


Рисунок 4.3.6 Превышено максимальное количество попыток входа

* Пароль устарел (Рисунок 4.3.7) — сообщение появляется в случаях, когда необходимо изменить собственный пароль перед авторизацией в МЗИ. После нажатия кнопки «ОК» в информационном окне появится новое окно, куда необходимо ввести новый пароль.

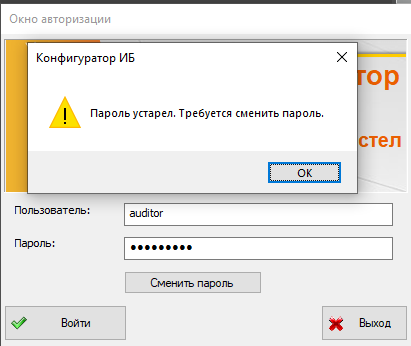
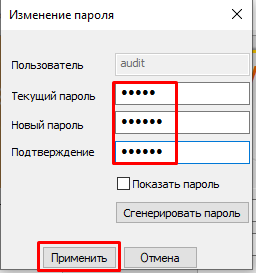
 

Рисунок 4.3.7 Пароль устарел

Изменение пароля учетной записи при первом входе

При необходимости изменить пароль своей учетной записи пользователь может во время присоединения к Системе вызвать окно «Изменение пароля» нажав кнопку «Сменить пароль» в окне авторизации после ввода логина и текущего пароля.

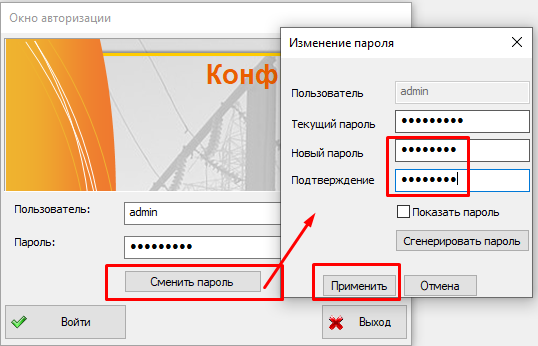
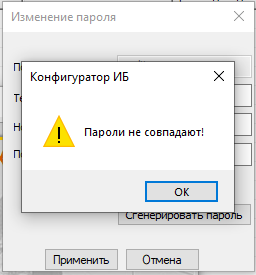


Рисунок 4.3.8 Изменение собственного пароля пользователя

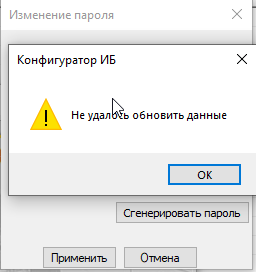
В появившемся окне необходимо ввести текущий пароль и новый пароль в соответствующих полях. В поле «Подтверждение» необходимо повторно ввести нужный пароль.

После нажатия кнопки «Применить» отобразиться результат операции:

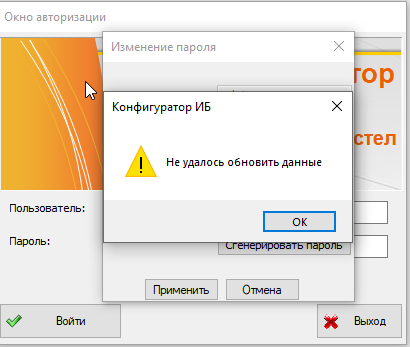
1. Если пароли в окне «Новый пароль» и «Подтверждение» не совпадают, отобразиться соответствующее предупреждение.

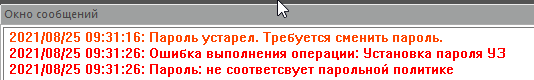


1. При неправильном текущем пароле отобразиться предупреждение.



1. При несоответствии нового пароля текущей парольной политике появится предупреждение.





Отключение от сервера

При повторном нажатии на кнопку соединения (при статусе «Соединен») произойдет разрыв соединения с активным сервером, а все загруженные в «Конфигуратор» данные очистятся.

## Вход в Программу

После выполнения всех настроек для подключения к программной среде МЗИ (п 4.3) следует вызвать «Конфигуратор». Интерфейс входа в Программу представлен на Рисунок 4.4.1. После успешной авторизации Пользователю предоставляется Главный интерфейс Программы.

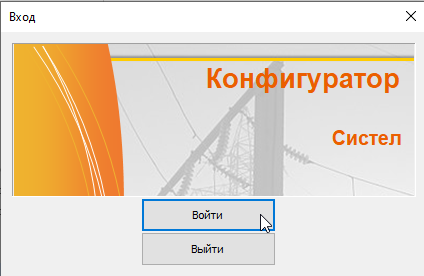
**

Рисунок 4.4.1 Окно входа в ПО «Конфигуратор»

Интерфейс Программы

Главный интерфейс программы «Конфигуратор» содержит (Рисунок 4.4.2):

1. Рабочую область, где отображаются данные конфигурации МЗИ.
2. Окно «Сообщения», куда выводиться сообщения о ходе работы Программы, а также сообщения Оператору, получаемые от МЗИ.
3. Набор кнопок на ленте инструментов для запросов к серверам МЗИ.
4. Окно «Свойства», где отображаются дополнительные функциональные свойства.

В функциональной панели интерфейса Конфигуратора имеется возможность просмотра конфигурации (для пользователей Администратор и Оператор), а также вносить изменения в конфигурацию (только для Администратора).

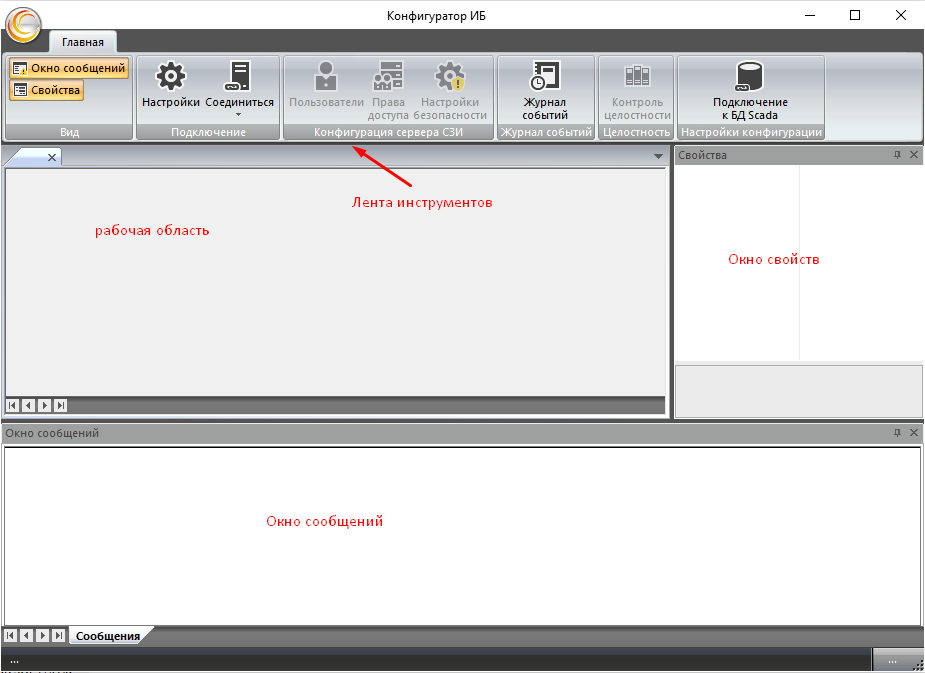


Рисунок 4.4.2 Главное окно программы «Конфигуратор»

Лента инструментов

В Таблице 1 представлены кнопки управления вкладки «Главная» ленты инструментов конфигуратора.

Таблица 1 – Главная функциональная панель интерфейса

|  |  |  |
| --- | --- | --- |
| **Вид кнопки** | **Название** | **Пояснение** |
|  | Окно сообщений | Отобразить/скрыть окно сообщений |
|  | Свойства | Отобразить/скрыть окно свойств |
|  | Настройки | Вызывает интерфейс настройки списка серверов для подключения |
|  | Соединиться | Выбор сервера для подключения из списка и запрос на установку соединения с выбранным сервером ЗИ |
|  | Соединен | Повторное нажатие на кнопку после успешного соединения приведет к отключению от текущего сервера |
|  | Пользователи | Вызов интерфейса управления идентификацией и аутентификацией пользователей (см. п. 5.1).Активна после удачного подключения к серверу СЗИ. |
|  | Права доступа | Вызов интерфейса управления матрицей прав разграничения доступа (см. п. 5.2). Активна после удачного подключения к серверу СЗИ. |
|  | Настройки безопасности | Вызов интерфейса управления правилами безопасности сервера ЗИ (см. п.5.3). Активна после удачного подключения к серверу СЗИ. |
|  | Журнал событиями безопасности | Вызов интерфейса мониторинга и управления событиями безопасности (см. п.8).  Активна после запуска Программы. Без подключения к серверу МЗИ доступны только функции чтения ранее загруженных журналов. |
|  | Контроль целостности | Вызов интерфейса управления системой целостности (см. п. 6.1). Активна после удачного подключения к серверу СЗИ. |

Рабочая область

В рабочей области отображаются данные конфигураций, полученные от МЗИ:сервер. Каждая категория безопасности расположена в отдельном окне (вкладке) рабочей области. Для вызова определённой вкладки необходимо нажать кнопку ленты инструментов:

* Кнопка «Пользователи» вызывает окно «Пользователи», в котором происходит управление учетными записями.
* Кнопка «Права доступа» вызывает окно «Правила разграничения доступа», в котором происходит управление матрицей прав доступа.
* Кнопка «Настройки безопасности» вызывает окно «Настройки безопасности», в котором происходит редактирование параметров политик безопасности.
* Кнопка «Журнал аудита» вызывает окно «Журнал аудита», в котором происходит вызов журнала аудита СЗИ.
* Кнопка «Контроль целостности» вызывает окно «Контроль целостности системы», в котором происходит контроль целостности системы, а также функции резервирования и восстановления компонент.

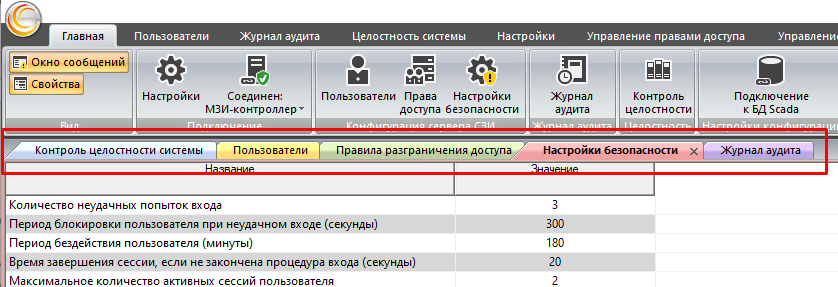
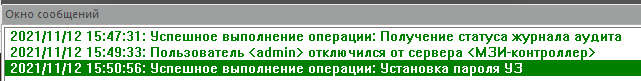


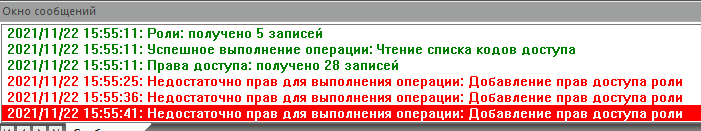
Рисунок 4.4.3 Окна рабочей области

Окно сообщений Оператору

Окно сообщений оператору представляет собой окно, расположенное в нижней части интерфейса пользователя. В этом окне отображаются сообщения, связанные с действиями пользователя МЗИ (результат выполнения запросов), а также сообщения МЗИ (например, о заполнении журнала аудита).

Сообщения-предупреждения отображены оранжевым цветом. Сообщения об отказе выполнения операций — красным. Сообщения об успешно выполненной операции — зеленым. Остальные сообщения отображены черным цветом (Рисунок 4.4.4).







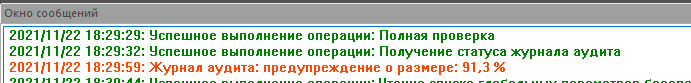


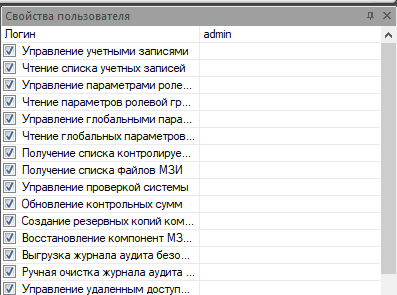
Рисунок 4.4.4 Пример сообщений оператору

Полный список возможных сообщений оператору находится в разделе «Приложение. Сообщения оператору».

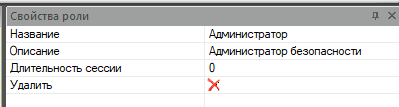
Окно свойств

Окно свойств расположено в правой части интерфейса пользователя. Содержит вспомогательную информацию:

* Отображение прав конкретного пользователя, прочитанные из его роли (см. п. 3.7.1)



* Отображение свойств роли (см. п.3.8.3).



# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

В СЗИ ПО Систел реализован принцип ролевого управления доступом пользователей, предусматривающий использование специальных групп пользователей (ролевые группы или роли) и формирование правил разграничения доступа к информационным объектам ПО контроллера.

Разграничение доступа пользователей на основе ролей осуществляется путем включения учётной записи пользователя в ролевую группу, для которой определены типы доступа к информационным объектам ПО контроллера. В данной реализации МЗИ пользователь может быть включён только в одну ролевую группу.

Правила разграничения доступа (ПРД) предусматривают назначение прав доступа (или привилегий) для каждой группы пользователей из списка привилегий, который изначально сформирован производителем ПО контроллера.

Список привилегий включает следующие группы прав доступа:

* настройками параметров технологического управления СПО
* чтение записей журнала аудита МЗИ
* настройками параметров функций безопасности МЗИ
* дистанционное управление конфигурациями СПО и МЗИ контроллера (загрузка, очистка, откат, архивирование восстановление, перезагрузка, др.)

Проверка прав доступа осуществляется при каждом обращении пользователя (приложения) к информационным объектам ПО контроллера по идентификатору субъекта и сетевому адресу компьютера (АРМ пользователя).

Администратор имеет возможность создания и удаления ролей, а также изменения (редактирования) прав разграничения доступа для каждой роли. Администратору предоставляется возможность модификации правил разграничения доступом путём редактирования списков привилегий доступа.

Идентификация пользователей в программной среде контроллера осуществляться с использованием имен учетных записей. Аутентификация пользователя осуществляться путём применения паролей условно-постоянного действия.

После успешной проверки учётных данных, пользователю предоставляется сеанс связи (сеанс работы) с Системой. Обеспечивается возможность предоставления одному пользователю нескольких сеансов работы с разных рабочих мест пользователей.

## Интерфейс работы с учётными записями пользователей

Управление пользователями в программе «Конфигуратор» осуществляется с помощью выделенного интерфейса (Рисунок 5.1.1). Для перехода к интерфейсу управления пользователями необходимо нажать кнопку «Пользователи» главной панели ленты инструментов (Рисунок 5.1.31).

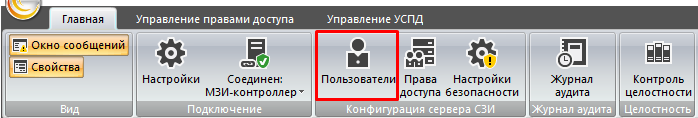
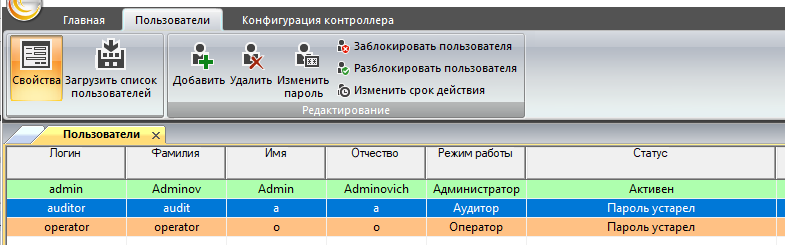


Рисунок 5.1.2 Вызов окна "Пользователи"



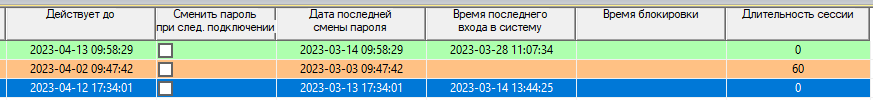


Рисунок 5.1.3 Интерфейс окна «Пользователи»

Для работы со списком пользователей используются кнопки контекстной вкладки (Рисунок 5.1.4) ленты «Пользователи». Перечень и описание функциональных элементов приведен в Таблица 2.

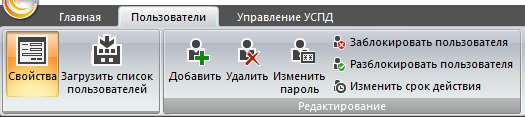


Рисунок 5.1.4 Контекстная вкладка окна "Пользователи"

Чтение списка зарегистрированных учётных записей пользователей осуществляется путём нажатия кнопки «**Загрузить список пользователей**». Для каждого пользователя отображается следующая информация:

1. Логин.
2. ФИО.
3. Режим работы, уровень доступа.
4. Статус учетной записи: активна, заблокирована администратором, заблокирована сервером безопасности, устаревший пароль.
5. Дата, до которой действует УЗ.
6. Флаг о смене пароля при следующем входе пользователя в систему.
7. Дата последней смены пароля.
8. Дата и время последнего входа в систему.
9. Дата блокировки УЗ (если статус «заблокирована»).
10. Длительность сессии по умолчанию (в минутах). При значении «0» время сессии не ограничено.
11. Список прав пользователя доступен в окне «Свойства» при выделении строки конкретного пользователя.

ВАЖНО: Для новой конфигурации МЗИ, создаваемой при установке ПО МЗИ (3.1.4), создаётся 2-е учётные записи - администратор и аудитор.

Таблица 2 – Кнопки управления списком пользователей

|  |  |
| --- | --- |
| **Название элемента** | **Пояснение** |
|  | Вызывает окно свойств |
|  | Вызов команды запроса списка пользователей к серверу СЗИ. При удачном выполнении команды в окне «Пользователи» отобразиться список учетных записей МЗИ. |
|  | Вызов окна создания нового пользователя (п. 5.1.4) |
|  | Вызов команды удаления выбранного пользователя (п. 5.1.5) |
|  | Вызов окна изменения пароля выбранного пользователя |
|  | Вызов команды блокировки выбранного пользователя |
|  | Вызов команды разблокировки выбранного пользователя |
|  | Вызов окна выбора времени действия выбранной УЗ пользователя |

ВАЖНО: Все операции с учетными записями пользователей доступны только пользователям с соответствующими правами. При посылке команды на сервере МЗИ проверяется соответствие операции выданным правам. Если у пользователя недостаточно прав для выполнения, тогда в окне сообщений появится сообщение об отказе выполнения операции.

На Рисунок 5.1.5 демонстрируется запись аудита об отказе в выполнении операции

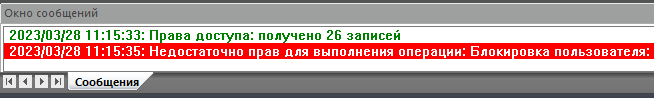


Рисунок 5.1.6 Сообщение об отказе выполнения операции

После загрузки списка учетных записей пользователю, обладающего правом редактирования УЗ, будут доступны функции редактирования этих записей.

Редактирование информации об учетной записи

При двойном щелчке на поле «Фамилия», «Имя», «Отчество» появится возможность отредактировать данные путем ввода нового значения (Рисунок 5.1.7). Поле «Логин» отредактировать нельзя.

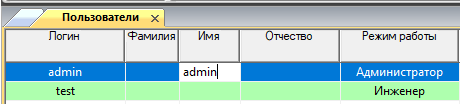


Рисунок 5.1.7 Поля для редактирования ФИО пользователя УЗ

При выборе поля «Режим работы» появится выпадающий список ролей, которые можно назначить пользователю (Рисунок 5.1.8).

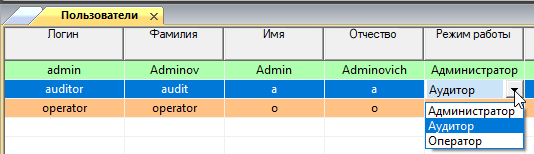


Рисунок 5.1.8 Поле выбора роли УЗ

При выборе пользователя из списка, в окне «Свойства» появится список прав пользователя (Рисунок 5.1.9).

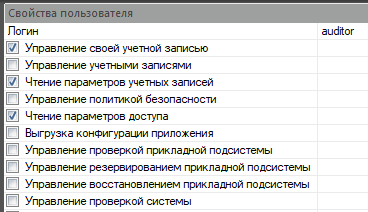


Рисунок 5.1.9 Окно свойств пользователя со списком прав

Список прав пользователя соответствует правам роли. Редактировать права доступа в этом окне нельзя.

Изменение статуса учетной записи

В поле «Статус» отображен список статусов учетной записи, которые могут быть назначены администратором системы (Рисунок 5.1.10).

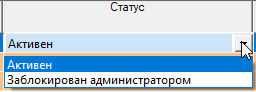


Рисунок 5.1.10 Поле выбора статуса УЗ

Изменить статус учетной записи можно с помощью кнопок раздела ленты инструментов «Пользователи»: «Заблокировать пользователя», «Разблокировать пользователя» (Рисунок 5.1.11). После выбора УЗ в списке эти кнопки станут активными.

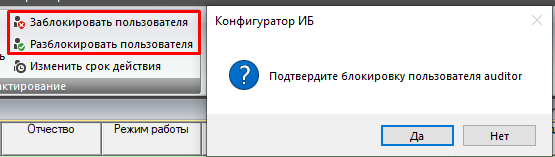


Рисунок 5.1.11 Изменение статуса УЗ с помощью кнопок ленты инструментов

При выделении поля «Действует до» появится кнопка «…», после нажатия на которую появится окно «Выбор даты», где можно выбрать дату, до которой будет действовать УЗ (Рисунок 5.1.12).

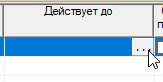
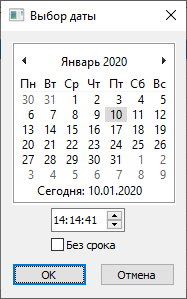
 

Рисунок 5.1.12 Поле выбора даты действия УЗ

Поле «Выбор даты» действия учётной записи (Рисунок 5.1.12) может быть вызвано отдельной кнопкой «Изменить срок действия» для принудительного изменения срока действия пароля пользователя администратором Системы (Рисунок 5.1.11).

Модификация пароля учетной записи

Для того, чтобы пользователь при следующем логине в систему самостоятельно сменил собственный пароль необходимо поставить флаг в поле «Сменить пароль при следующем подключении» (Рисунок 5.1.13). После чего статус УЗ пользователя изменится на «Пароль устарел» (требования парольной политики).

ВАЖНО: при начальной конфигурации пользователи, созданные по умолчанию («Администратор», «Аудитор»), имеют такой флаг и должны изменить пароль при входе в систему (см. п. 4.3.2,Рисунок 4.3.8).

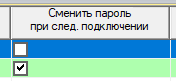


Рисунок 5.1.13 Поле для отметки о принудительной смене пароля пользователем

Администратор, имеющий право «управление учетными записями» может принудительно установить постоянный пароль любой учетной записи. Для этого необходимо выделить УЗ пользователя в списке пользователей и нажать кнопку «Изменить пароль» вкладки «пользователи» ленты инструментов (Рисунок 5.1.14).

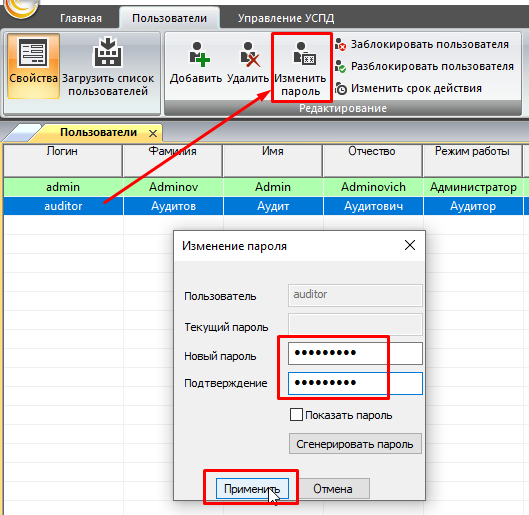


Рисунок 5.1.14 Изменение пароля администратором

Администратор может сгенерировать случайный пароль пользователю. Для этого в окне смены пароля необходимо нажать кнопку «Сгенерировать пароль». После чего в поле «Новый пароль» отобразиться временный сгенерированный пароль.

ВАЖНО: этот пароль необходимо записать и передать пользователю, т.к. после закрытия этого окна невозможно будет отобразить текущий пароль.

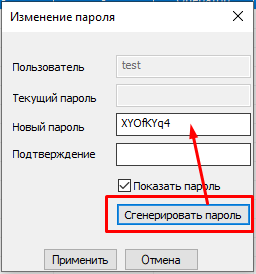


Рисунок 5.1.15 Установка случайного пароля

Добавление пользователей

Для добавления нового пользователя системы необходимо нажать кнопку «Добавить» на вкладке «Пользователи» ленты инструментов (Рисунок 5.1.16). После чего появится окно, в котором необходимо заполнить необходимую информацию:

1. Логин;
2. имя пользователя;
3. пароль и подтверждение пароля. Сам пароль при наборе будет отображен символами «\*».
4. Роль — выбрать из списка ролей. Это обязательное поле.

Далее необходимо нажать кнопку «Добавить»

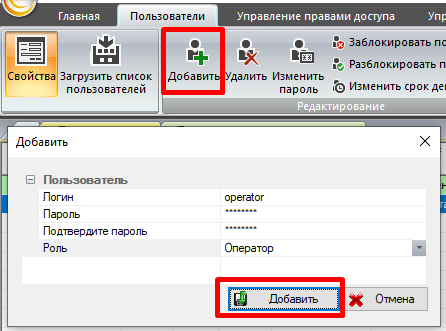


Рисунок 5.1.16 Диалог создания пользователя

Удаление пользователей

Чтобы удалить учетную запись пользователя необходимо выбрать ее в списке, а затем нажать кнопку «Удалить» на ленте инструментов. После этого в появившемся окне подтвердить операцию (Рисунок 5.1.17). Результат выполнения команды будет отображен в окне сообщений.

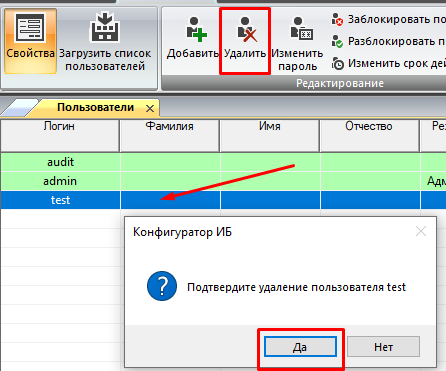




Рисунок 5.1.17 Удаление учетной записи

## Управление доступом пользователей

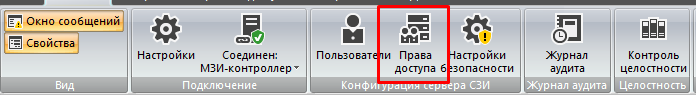
Права доступа пользователей назначаются путём включения его учётной записи в одну из ролевых групп. Каждая ролевая группа имеет набор разрешённых операций по управлению функциями МЗИ и СПО Zemon – права доступа ролевых групп. Полный список разрешённых операций приведён в Таблице 3.

Таблица 3 – Операции по управлению функциями МЗИ и СПО Zemon

|  |  |
| --- | --- |
| **Название операции** | **Пояснение** |
| Чтение списка учетных записей | Право получения списка УЗ пользователей |
| Управление учетными записями | Право дает возможность изменять состав и параметры учетных записей: создание, удаление, редактирование (установка пароля, изменение ФИО, блокировка УЗ и т.д.) См. 5.1. |
| Чтение параметров ролевой группы | Чтение правил разграничения доступа (матрицы ПРД) |
| Управление параметрами ролевой группы | Возможность редактирования матрицы ПРД: изменение состава ролевых групп, редактирование состава прав ролевых групп. См. раздел 5.2. |
| Чтение параметров политики безопасности | Возможность получения списка параметров конфигурации, которые является общими для всех пользователей, а именно: количество неудачных попыток входа, период бездействия пользователя до автоматического отсоединения, парольные политики и т.д. Полный список см. раздел 5.3. |
| Управление глобальными параметрами безопасности | Возможность изменения значений глобальных параметров безопасности, например, установление минимальной длины пароля. См. раздел 5.3 |
| Чтение списка контролируемых систем | Право получения списка контролируемых компонент.  См. раздел 6.1 |
| Получение списка файлов МЗИ | Право получения списка контролируемых файлов МЗИ. Как правило только администратору доступно право читать состав файлов МЗИ. |
| Управление проверкой системы | Право запуска механизмов ручной проверки целостности компонент ПО Системы (МЗИ и СПО)  См. раздел 6.1 |
| Обновление контрольных сумм | Право установки (путём записи) эталонных контрольных сумм |
| Создание резервных копий компонент МЗИ | Право создания и выгрузки на АРМ резервной копии конфигурации МЗИ |
| Восстановление компонент МЗИ из резервных копий | Право загрузить на устройство резервную копию конфигурации МЗИ и восстановить из нее конфигурацию |
| Выгрузка журнала аудита безопасности | Право выполнить операцию выгрузки журнала аудита (раздел 8) |
| Ручная очистка журнала аудита безопасности | Право с помощью команд ПО «Конфигуратор» удалить старые записи аудита (в процентном соотношении от текущего заполнения, все записи ранее определенной даты). |
| Управление удаленным доступом к УСПД | Право запуска демонов SSH и удалённой перезагрузки контроллера |
| Управление приложением | Право на запуск и останов программных компонент прикладного ПО контроллера |
| Управление проверкой прикладной подсистемы | Право запуска механизмов ручной проверки целостности только компонент СПО (прикладное ПО Zemon) |
| Создание резервных копий компонент СПО | Право на выполнение операций по созданию резервных копий исполняемых файлов СПО |
| Восстановление компонент СПО из резервных копий | Право на выполнение установленных операций по восстановлению из резервных копий исполняемых файлов СПО |
| Создание резервных копий конфигурации СПО | Право на выполнение операций по созданию резервных копий конфигурационных файлов СПО |
| Выгрузка рабочих архивов и логов приложения | Право на выполнение установленных операций по выгрузке рабочих архивов и логов приложения |
| Выгрузка конфигурации приложения | Право на выгрузку рабочих конфигурационных файлов СПО |
| Исполнение команд ТУ | Право на исполнение команд ТУ (невозможно через ПО «Конфигуратор») |
| Установка ручных значений | Право на установку значений технологических параметров объекта (невозможно через ПО «Конфигуратор») |
| Управление полукомплектами | Право на управление режимом работы полукомплектов контроллера (невозможно через ПО «Конфигуратор») |
| Включение тестового сигнала | Право на включение тестового сигнала в телемеханическом канале вводе/вывода (невозможно через ПО «Конфигуратор») |

Изменения прав доступа ролевых групп

Для перехода в окно редактирования прав доступа ролевой группы необходимо нажать на кнопку главной панели ленты инструментов «**Права доступа**». После чего появится окно «**Правила разграничения доступа**» (Рисунок 5.2.1).



Окно данного интерфейса представляет собой таблицу, в которой определяется разрешённые операции управления для ролевых групп – Матрица правил разграничения доступа (ПРД).

Администратор имеет совокупное право изменять состав разрешённых операций для каждой роли.

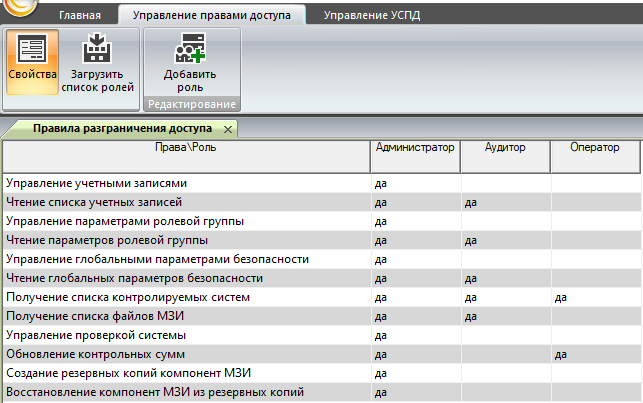


Рисунок 5.2.1 Интерфейс окна "Правила разграничения доступа"

Для изменения состава прав доступа для роли необходимо в окне «Правила разграничения доступа» в соответствующей ячейке права для роли вызвать подменю, в котором необходимо выбрать признак наличия/отсутствия данного права для роли (Рисунок 5.2.2).

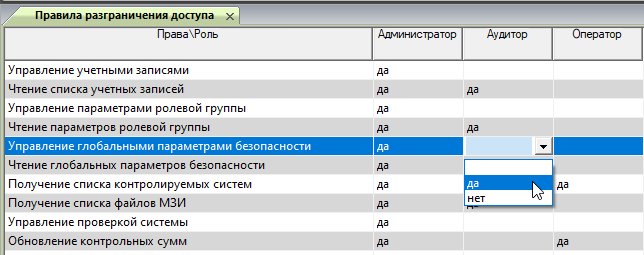


Рисунок 5.2.2 Редактирование ПРД

Добавление новой роли

Для добавления новой роли в окне «Правила разграничения доступа» на контекстной панели «Управление правами доступа» ленты инструментов необходимо нажать кнопку «Добавить роль».

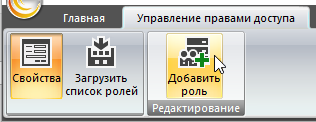


Рисунок 5.2.3 Вызов окна добавления новой роли

После чего появится диалоговое окно для добавления новой роли. В этом окне необходимо заполнить поля: название роли; описание роли, если необходимо; выбрать роль, от которой будут наследоваться права новой роли при создании. Впоследствии права новой роли можно отредактировать как было описано в разделе 5.2.1.

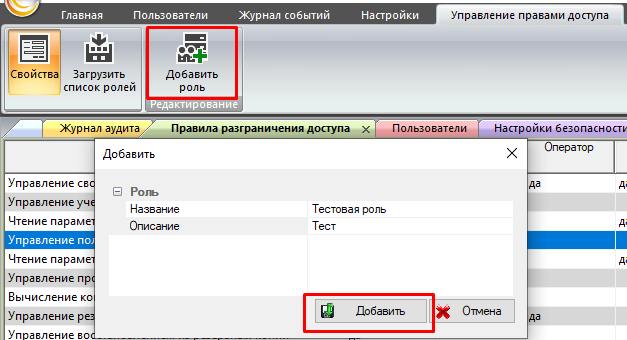
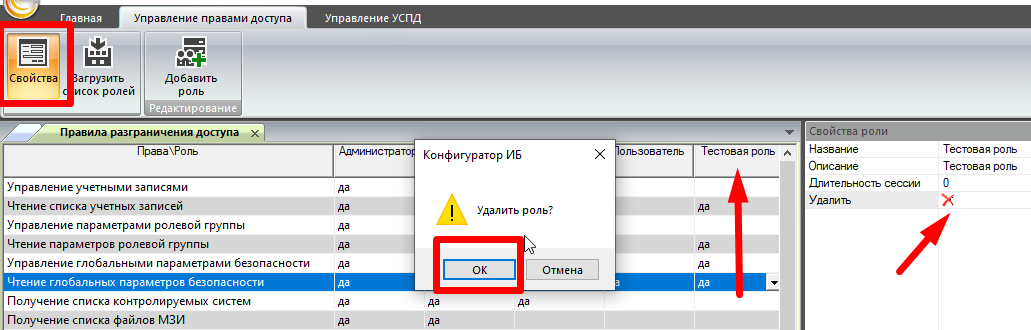


Рисунок 5.2.4 Добавление новой роли

Удаление роли

Для удаления роли необходимо открыть окно свойств. В окне «Правила разграничения доступа» выбрать нужную роль. При этом в окне свойств отобразится информация о выбранной роли, а также появится кнопка для удаления роли.



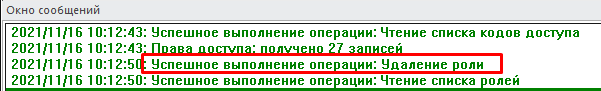


Рисунок 5.2.5 Удаление роли

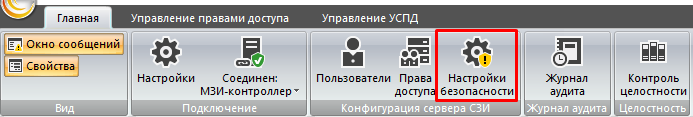
После успешного выполнения операции информация в окне «Правила разграничения доступа» обновится.

## Настройка политик безопасности

Под «политикой безопасности» в данном контексте понимается настройка таких параметров конфигурации МЗИ, исполнение которых являются обязательным для всех пользователей.

Для перехода к настройкам параметров политики безопасности МЗИ необходимо нажать на кнопку «Настройки безопасности» ленты инструментов. После чего появится окно со списком настроек общих параметров безопасности, которые хранятся в базе МЗИ:сервер.

Актуализировать список параметров безопасности можно путём нажатия кнопки «Загрузить» вкладки «Настройки» ленты инструментов.



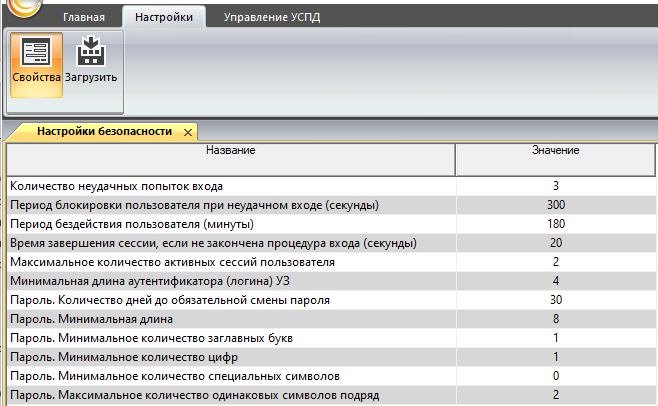
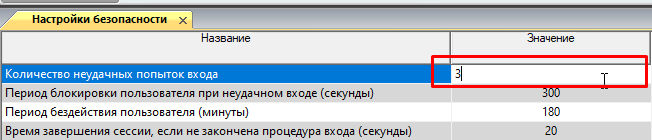


Рисунок 5.3.1 Окно настроек безопасности

Редактирование значений параметров осуществляется двойным щелчком на поле «Значение» конкретного параметра (Рисунок 4.9.2). После чего формируется команда изменения параметра безопасности и отправляется на сервер МЗИ. Результат выполнения команды отображается в окне «Окно сообщений».

Рисунок 5.3.2 Редактирование настроек безопасности

Список параметров доступных для редактирования представлен в Таблица 4.

Таблица 4 – Список настроек безопасности

|  |  |
| --- | --- |
| Название | Описание |
| Количество неудачных попыток входа | Сколько неудачных попыток входа (неправильные логин/пароль, попытка входа с заблокированной УЗ и т.п.) есть у пользователя прежде чем соединение с сервером будет разорвано.  По умолчанию равно 3 |
| Период блокировки пользователя при неудачном входе (секунды) | Сколько секунд пользователь не сможет присоединиться к серверу (с тем же логином) после неудачной попытки.  По умолчанию равно 300 секунд |
| Период бездействия пользователя (минуты) | Время в минутах в течении которого сессия еще поддерживается если пользователь не выполняет никаких действий с МЗИ. Время сбрасывается после совершения действия.  По умолчанию равно 180 минут |
| Время завершения сессии, если не закончена процедура входа (секунды) | Время, в течение которого необходимо произвести аутентификацию МЗИ после присоединения  По умолчанию равно 20 секунд |
| Максимальное количество активных сессий пользователя | Допустимое количество одновременных авторизированных сессий одного пользователя при работе с МЗИ  По умолчанию равно двум |
| Минимальная длина аутентификатора УЗ (логин) | Минимальная длина логина пользователя. По умолчанию равна 4 |
| Пароль. Количество дней до обязательной смены пароля | Сколько времени (в днях) будет действовать текущий пароль пользователя после последней смены пароля  По умолчанию равно 30 дням |
| Пароль. Минимальная длина | Минимальная длина пароля УЗ.  По умолчанию равно 8 |
| Пароль. Минимальное количество заглавных букв | Минимальное количество заглавных букв.  По умолчанию равно 1 |
| Пароль. Минимальное количество цифр | Минимальное количество цифр.  По умолчанию равно 1. |
| Пароль. Минимальное количество специальных символов | Минимальное количество специальных символов (%-&)  По умолчанию равно 0 |
| Пароль. Максимальное количество одинаковых символов подряд | Сколько подряд одинаковых символов допускается в пароле  По умолчанию равно 2 |

# КОНТРОЛЬ ЦЕЛОСТНОСТИ

С целью обеспечения неизменности программной структуры ПО Систел реализованы механизмы проверки целостности компонент СПО и МЗИ на наличие ошибок контрольных сумм. Проверка целостности компонент ПО контроллера осуществляется путём сравнения расчётных контрольных сумм с эталонными значениями в 2-х режимах:

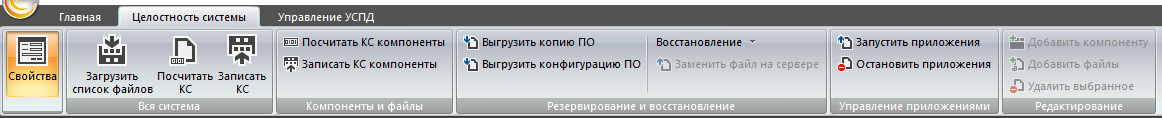
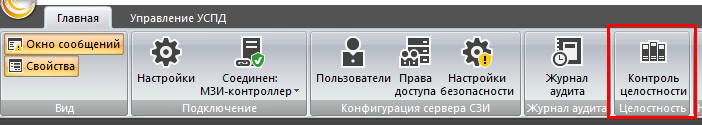
* ручная проверка
* автоматическая проверка при инициализации ПО контроллера

ВАЖНО. При создании начальной конфигурации МЗИ контроллера создаются «списки контроля» файлов для проверки с помощью алгоритмов контрольного суммирования, а также файлы эталонных контрольных сумм для СПО и МЗИ контроллера. Хранение файлов эталонных контрольных сумм в программной среде контроллера реализовано в защищенном виде, затрудняющем их несанкционированную модификацию (п.3.4)

Для выполнения функции ручного контроля целостности пользователю должно быть назначена привилегия «Управление проверкой системы» или «Управление проверкой прикладной подсистемы» (см Таблица 3).

## Интерфейс ручного контроля целостности системы

Для проверки перерасчета и записи контрольных сумм используется интерфейс «Контроль целостности системы», вызываемый соответствующей кнопкой главной панели ленты.



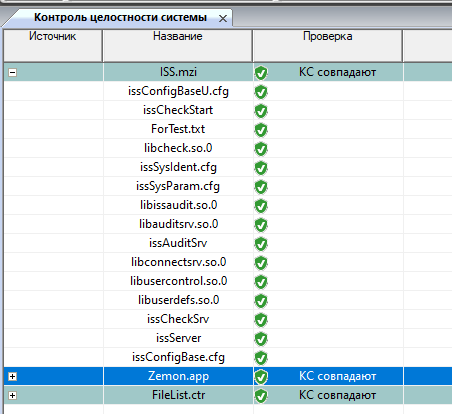


Рисунок 6.1.1 Список компонент для контроля целостности

Таблица 5 – Команды контекстной вкладки «Целостность системы» ленты инструментов

|  |  |
| --- | --- |
| **Название элемента** | **Пояснение** |
|  | Вызывает окно свойств |
|  | Посылка команды запроса списка контролируемых файлов. При успешном выполнении команды полученный список отобразится в окне «Контроль целостности системы» |
|  | Посылка команды пересчета контрольной суммы всех компонент. После операции в колонке «Проверка» отобразится результат выполнения команды. |
|  | Посылка команды на сервер для пересчета контрольной суммы всех компонент и запись результата в качестве эталона.  После операции в поле «Проверка» для файлов отобразится результат выполнения команды. |
|  | Пересчет контрольных сумм отдельной компоненты |
|  | Запись контрольной суммы в качестве эталонной выбранной компоненты |
|  | Создание эталонной копии компоненты (доступно для МЗИ контроллера) и выгрузка ее на АРМ в качестве резервной |
|  | Создание резервной копии конфигурации выбранной компоненты и выгрузка ее на АРМ |
|  | * Загрузить копию ПО — загрузка на сервер резервной копии ПО из списка ранее загруженных на АРМ * Загрузить конфигурацию ПО — загрузка на сервер резервной копии конфигурации из списка ранее загруженных на АРМ * Восстановление ПО из эталона — запуск процедуры восстановления ПО выбранной компоненты из существующей на сервере эталонной копии — не доступно для МЗИ-контроллер |
|  | Загрузка файла на сервер  После нажатия кнопки появляется окно с выбором файла, который необходимо загрузить на сервер. |
|  | Позволяет запустить приложения, относящиеся к выбранной компоненте. |
|  | Позволяет остановить приложения, относящиеся к выбранной компоненте. |
|  | Добавление новой компоненты в список (не доступно для МЗИ МТК-30) |
|  | Добавление нового файла в список проверки (не доступно для МЗИ МТК-30) |
|  | Удаление компоненты или файла из списка контроля (не доступно для МЗИ МТК-30) |

## Списки контроля целостности

В рабочей области окна «Контроль целостности системы» после нажатия кнопки «**Загрузить список файлов**» будет отображён список компонент и файлов, проверяемых подсистемой контроля целостности МЗИ, который установлен производителем контроллера.

Компоненты в списке отмечены цветом и имеют раскрывающийся список файлов, относящихся к этой компоненте (Рисунок 6.2.1).

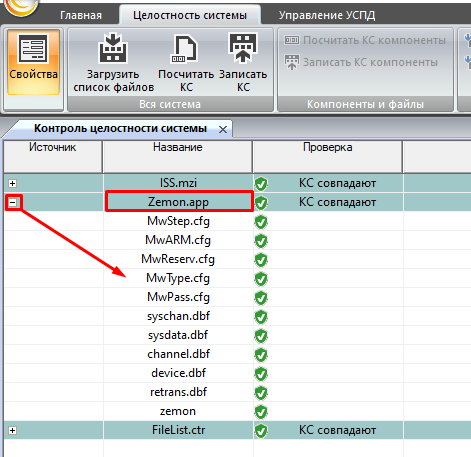


Рисунок 6.2.1 Список компонент и файлов

Для контроля целостности с помощью МЗИ присутствуют следующие файлы, сгруппированные в отдельные компоненты:

1. Компонента «ISS.mzi». Представлена исполняемыми файлами и библиотеками МЗИ, а также конфигурационными файлами МЗИ.

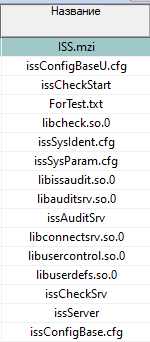


Рисунок 6.2.2 Список файлов МЗИ

1. Компонента «Zemon.app». представлена исполняемыми файлами и библиотеками СПО «Zemon», а также конфигурационными файлами СПО «Zemon».

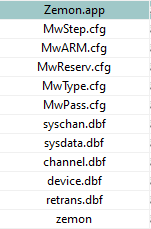


Рисунок 6.2.3 Список файлов СПО

1. Компонента «FileList.ctr». Представлена специальными файлами, содержащими списки для контроля состава файлов МЗИ в контролируемых директориях (файлы с расширением «.lst»). Также содержит скриптовый файл «mklstfile.sh» запускаемый при контроле состава файлов.

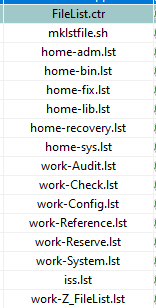


Рисунок 6.2.4Список файлов контроля состава

Списки файлов МЗИ фиксируются изготовителем и содержат следующие файлы:

* «home-adm.lst» содержит список файлов в директории «/home/iss/adm»;
* «home-bin.lst» содержит список файлов в директории «/home/iss/bin»;
* «home-fix.lst» содержит список файлов в директории «/home/iss/fix»;
* «home-lib.lst» содержит список файлов в директории «/home/iss/lib»;
* «home-recovery.lst» содержит список файлов в директории «/home/iss/recovery»;
* «home-sys.lst» содержит список файлов в директории «/home/iss/sys»;
* «work-Audit.lst» содержит список файлов в директории «/work/iss/Audit»;
* «work-Check.lst» содержит список файлов в директории «/work/iss/Check»;
* «work-Config.lst» содержит список файлов в директории «/work/iss/Config»;
* «work-Reference.lst» содержит список файлов в директории «/work/iss/Reference»;
* «work-Reserve.lst» содержит список файлов в директории «/work/iss/Reserve»;
* «work-System.lst» содержит список файлов в директории «/work/iss/System»;
* «work-Z-FileList.lst» содержит список файлов в директории «/work/iss/Z-FileList»;
* «iss.lst» содержит список директорий на момент первичного запуска МЗИ.

Если в контролируемой директории появится новый файл или удалится файл, который в ней должен находиться, то соответствующий файл компоненты «FileList.ctr» будет отмечен ошибкой.

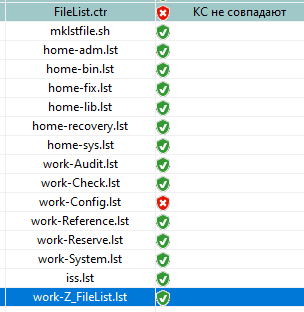


Рисунок 6.2.5 Ошибка в составе файлов директории

Эта ошибка означает, что в директории «work/iss/Config» нарушен состав файлов (отсутствует файл либо добавлен неизвестный файл).

## Процедура проверки целостности

Для запуска процедуры проверки целостности Системы необходимо:

1. Получить список всех компонент нажав на кнопку «**Загрузить список файлов**» ленты инструментов.
   1. Для проверки всей Системы необходимо нажать кнопку «Посчитать КС» раздела «Вся система» (Рисунок 6.3.1).

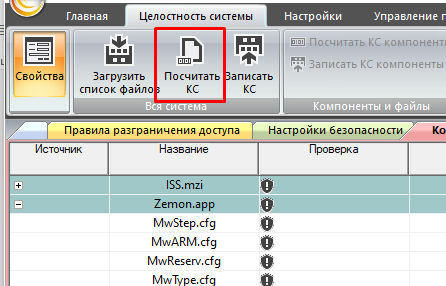


Рисунок 6.3.1 Запуск процедуры проверки КС всей системы

* 1. Для проверки целостности отдельной компоненты необходимо: выбрать необходимую компоненту в списке, нажать кнопку «Посчитать КС компоненты» раздела «Компоненты и файлы» ленты инструментов.

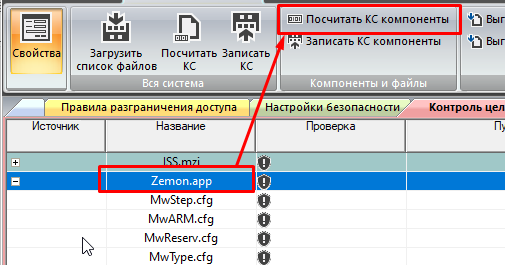
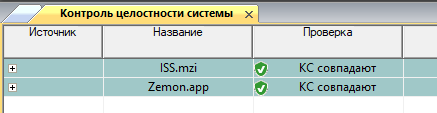


Рисунок 6.3.2 Запуск процедуры проверки КС отдельной компоненты

1. Результат операции отобразится в окне «Окно сообщений», а также в поле «Проверка».



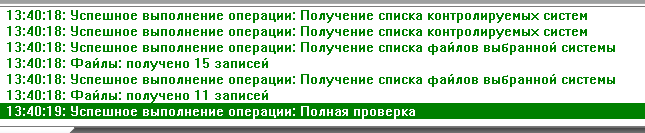


Рисунок 6.3.3 Отображение результата проверки КС

# АРХИВИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

Для случаев серьёзных программных сбоев ПО контроллера, предусмотрены механизмы резервного копирования и восстановление информации.

ВАЖНО. Архивы ПО контроллера создаются и хранятся на АРМ управления в защищённом от несанкционированного просмотра и модификации виде.

Механизм архивирования формирует следующие типы архивов:

* эталонная копия исполняемого кода СПО МТК-30 (firmware)и МЗИ (с расширением «.ref»)*.*
* резервная копия конфигурации СПО и МЗИ (с расширением «.rsv»).

Механизм архивирования осуществляет формирование архивной копии и её выгрузку в хранилище архивов на АРМ администратора.

Архивирование и восстановление ПО осуществляется по командам ленты инструментов вкладки «Целостность системы» конфигуратора.

## Выгрузка эталонной копии компоненты ПО МТК-30.КП:

1. Вызвать окно «Контроль целостности системы» путем нажатия кнопки «Контроль целостности» главной ленты инструментов.
2. Нажать кнопку «Загрузить список файлов».
3. Выбрать компоненту в списке загруженных файлов (ISS.mzi или Zemon.app).
4. Нажать кнопку «Выгрузить копию ПО» ленты инструментов.

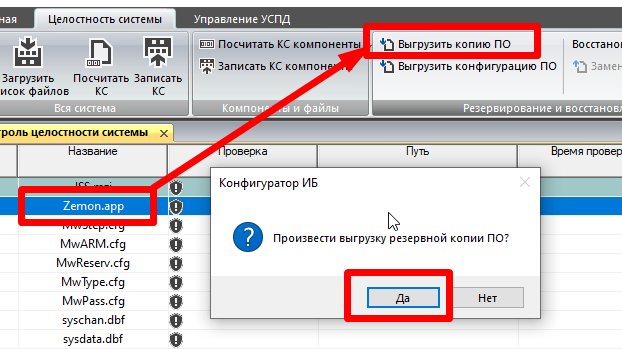




Рисунок 7.1.1 Создание эталонной копии компоненты

1. На АРМ открыть папку с установленным ПО Конфигуратор, перейти в подпапку rcv\IP-адрес источника. Найти только что загруженный файл, который будет иметь вид «YYMMDDHHMMSS-НазваниеКомпоненты.ref», где «YYMMDDHHMMSS» — время создания копии на сервере. Расширение файла «\*.ref» указывает на тип копии ПО (эталонная).

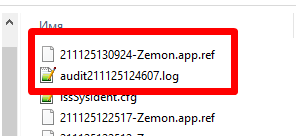


Рисунок 7.1.2 Архив с выгруженной копией ПО

## Выгрузка резервной копии конфигурации ПО МТК-30.КП:

1. Вызвать окно «Контроль целостности системы» путем нажатия кнопки «Контроль целостности» главной ленты инструментов.
2. Нажать кнопку «Загрузить список файлов».
3. Найти и выделить в списке компоненту, отвечающую за ПО контроллера (ISS.mzi или Zemon.app).
4. Нажать кнопку ленты инструментов «Выгрузить конфигурацию ПО». В появившемся окне подтверждения операции нажать «Да». Убедиться в успешном выполнении операции.

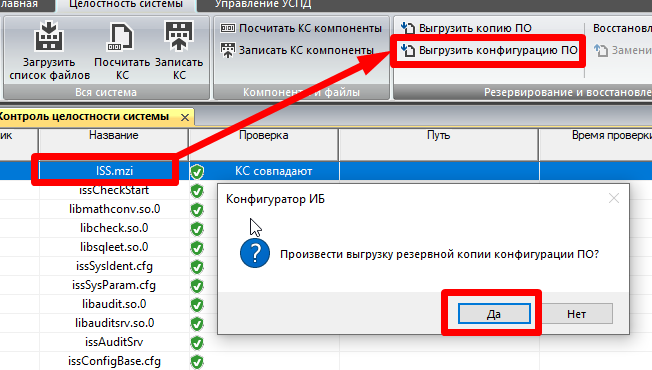




Рисунок 7.2.1 Выгрузка резервной копии конфигурации

1. На АРМ открыть папку с установленным ПО Конфигуратор, перейти в подпапку rcv\IP-адрес источника. Найти только что загруженный файл, который будет иметь вид «YYMMDDHHMMSS-ISS.mzi.rsv», где «YYMMDDHHMMSS» — время создания копии на сервере. Расширение файла «\*.rsv» указывает на тип копии ПО (резервная).

## Восстановление компонент СПО контроллера из выгруженной эталонной копии

В случаях необходимости восстановления компонент системы предусмотрены команды восстановления.

В случаях, когда необходимо произвести откат к предыдущей версии СПО, необходимо произвести загрузку на устройство ранее сохраненной копии.

1. В окне «Контроль целостности системы», выбрать компоненту СПО (например, «Zemon.app»), а затем выбрать пункт меню «Восстановление->Загрузить копию ПО».

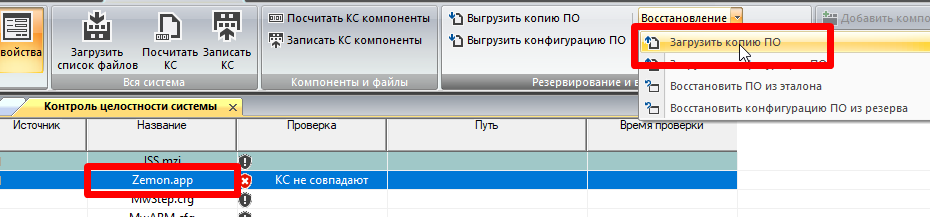
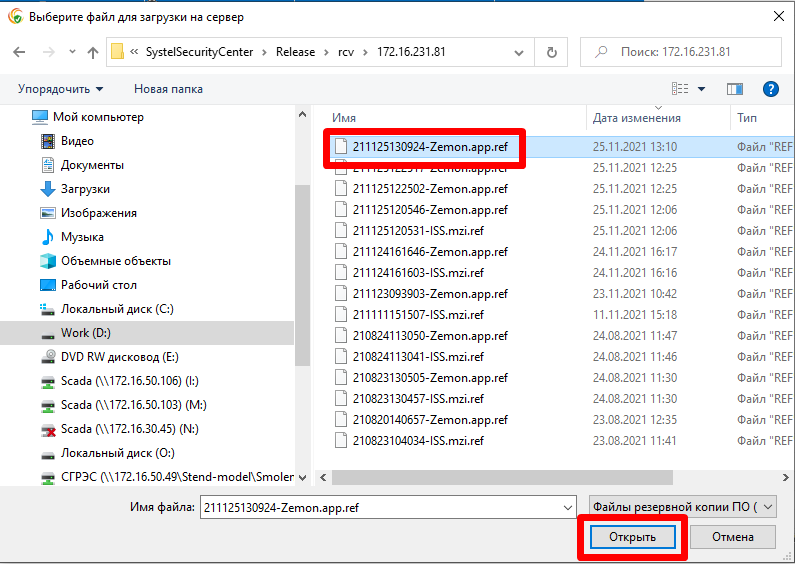


Рисунок 7.3.1 Загрузка резервной копии ПО на сервер

1. В появившемся диалоговом окне выбрать резервную копию СПО контроллера из списка ранее загруженных копий.



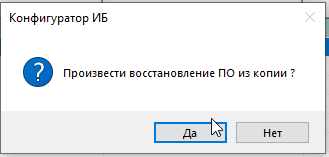


Рисунок 7.3.2 Выбор резервной копии компоненты для загрузки на сервер

1. Дождаться сообщения в окне сообщений об успешном выполнении операции «Загрузка копии компоненты» и «Восстановление из эталонной копии».



Рисунок 7.3.3 - Сообщение об успешной загрузке компоненты

1. После восстановления компонент программного обеспечения необходимо обновить эталонные контрольные суммы. Для этого в окне «Контроль целостности системы» выделить компоненту «Zemon.app» и нажать кнопку «Записать КС компоненты».

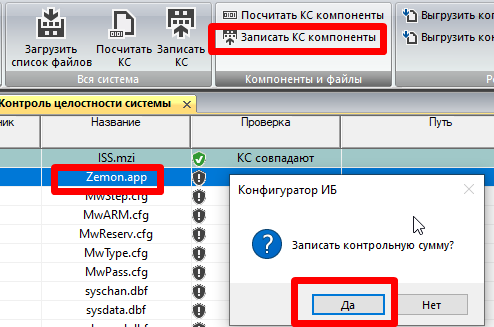


Рисунок 7.3.4 Обновление КС компонент

1. Перейти на вкладку «Управление «УСПД» ленты инструментов и нажать кнопку «Перезагрузка УСПД». После чего произойдет отключение от сервера МЗИ.

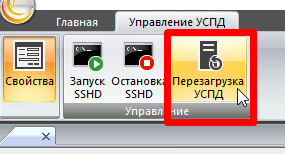


Рисунок 7.3.5 Перезагрузка УСПД из "Конфигуратора"

1. После перезагрузки контроллера повторно подключиться с помощью ПО «Конфигуратор» к МЗИ контроллера и осуществить контроль целостности компонент.

## Восстановление конфигурации МЗИ и СПО из резервной копии

Для отката конфигурации МЗИ к ранее выгруженной копии следует:

1. Пройти процедуру авторизации в Системе под учётной записью «Администратор».
2. Вызвать окно «Контроль целостности системы» путем нажатия кнопки ленты «Контроль целостности». Загрузить список файлов.
3. Найти и выделить в списке компоненту, отвечающую за МЗИ («ISS.mzi»).
4. В окне «Контроль целостности системы», выбрать компоненту «ISS.mzi», а затем выбрать пункт меню «Восстановление->Загрузить конфигурацию ПО».

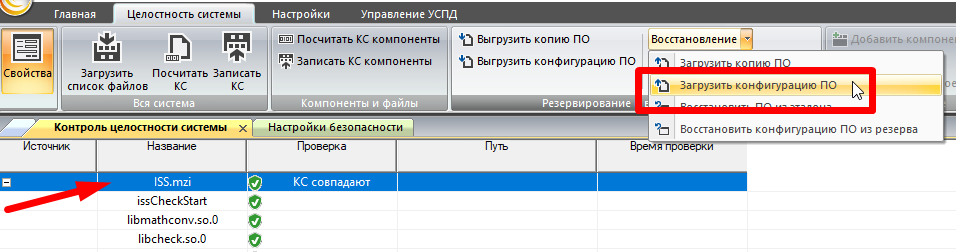
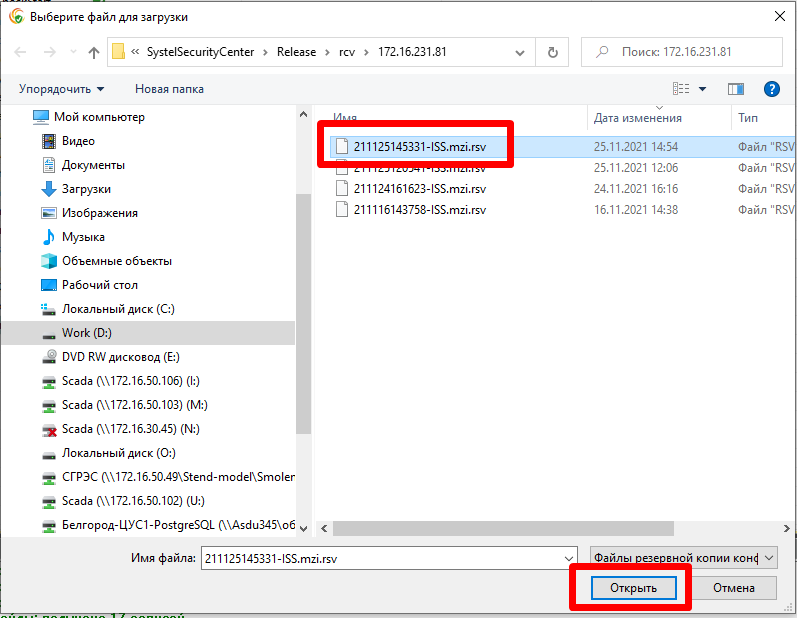


Рисунок 7.4.1 Вызов команды загрузки конфигурации МЗИ на сервер

1. В появившемся диалоговом окне выбрать ранее выгруженную резервную копию конфигурации МЗИ в папке /rcv/IP-адрес/дата-ISS.mzi.rsv.



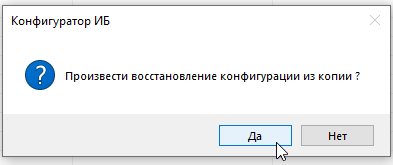


Рисунок 7.4.2 – Выбор резервной копии компоненты для загрузки на сервер

1. Дождаться сообщения об успешном выполнении операции.



1. После успешного восстановления компонент сервер автоматически разорвет соединение со всеми клиентами.
2. Осуществить повторное подключение к МЗИ-контроллера.
3. Перейти в окно «Настройки безопасности» и убедится, что измененной значение параметра безопасности откатилось к предыдущему.
4. Повторно посчитать контрольные суммы компонент. Убедиться в отсутствии ошибок целостности компонент.
5. Осуществить просмотр журнала аудита и убедиться в наличии сообщений безопасности (Рисунок 7.4.3).

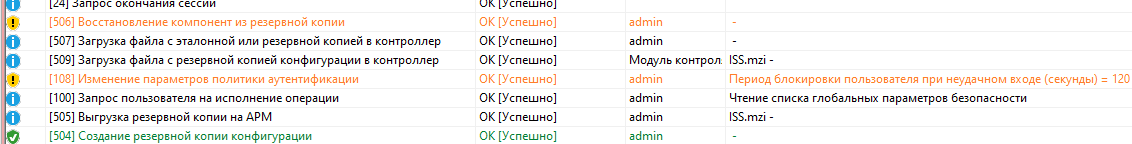


Рисунок 7.4.3 Сообщения аудита при откате конфигурации

## Процедура замены файла

С помощью ПО «Конфигуратор» можно заменить какой-либо файл СПО на контроллере. Для этого необходимо воспользоваться командой «Заменить файл на сервере» вкладки «Целостность системы» ленты инструментов.

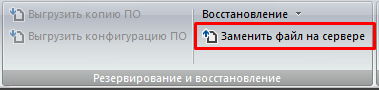
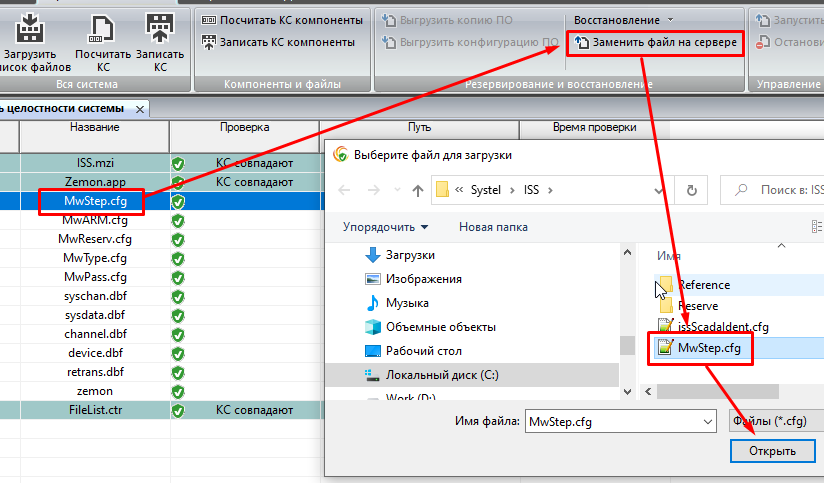


Рисунок 7.5.1 Кнопка для вызова команды замены файла

Для этого необходимо:

1. Пройти процедуру авторизации в Системе под учётной записью «Администратор».
2. Вызвать окно «Контроль целостности системы» путем нажатия кнопки ленты «Контроль целостности». Загрузить список файлов.
3. Найти и выделить в списке файл СПО («Zemon.app»), который необходимо заменить.
4. Нажать кнопку «Заменить файл на сервере». Выбрать файл из списка и подтвердить операцию.



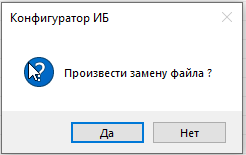


Рисунок 7.5.2 Замена файла СПО на устройстве

# АНАЛИЗ И УПРАВЛЕНИЕ СОБЫТИЯМИ БЕЗОПАСНОСТИ

В МЗИ контроллера выполняется непрерывный мониторинг (контроль) нарушений свойств защищаемой информации, включающий сбор, запись и хранение информации о событиях безопасности следующих категорий:

* попытки авторизации пользователей;
* контроль и изменение параметров рабочих сеансов пользователей;
* запрос на доступ к защищаемому ресурсу (чтение данных, запуск программы, запись на носитель, выдача на печать информации);
* создание и уничтожение объекта доступа, обращение к объектам доступа;
* контроль целостности программного обеспечения;
* изменение параметров политики безопасности (включая политику паролей);
* операции с учётными данными пользователей и ролевыми группами;
* действия с журналом аудита

Журнал аудита представляет собой файл базы данных SQLite (/work/iss/Audit/issAudit.log), который доступен для чтения только уполномоченным пользователям МЗИ. Файл базы данных SQLite создается при инициализации МЗИ.

ВАЖНО. При заполнении файла журнала аудита более чем на 90% от установленного размера, МЗИ формирует сообщение, предписывающее администратору выполнить выгрузку и очистку журнала аудита. Невыполнение предписания о ручной очистке журнала аудита в последующем приводит к формированию сообщения 100% заполнении файла журнала аудита. При этом осуществляется автоматическое удаление старых записей аудита с формированием соответствующих уведомлений в окне сообщений оператору.

Записи журнала аудита защищены криптографическим механизмом платформы SQLite с помощью закрытого ключа, который включён в состав программного кода МЗИ и является секретом производителя.

Каждая запись аудита имеет отметку времени регистрируемого события, набор полей, описывающий категорию события, и подсистему, к которой данное событие относится, описание события с набором параметров и контрольная сумма всех вышеперечисленных полей.

Процесс чтения записей журнала аудита осуществляется в 2-а этапа: выгрузка файла журнала аудита на АРМ управления ИБ и чтение записей журнала аудита из локального файла.

1. Авторизированный пользователь использует клиентское приложение «Конфигуратор», для формирования запроса МЗИ на выгрузку журнала аудита по протоколу *systel.link.*
2. МЗИ проверяет наличие права чтения журнала аудита для роли пользователя;
3. При условии наличия права, МЗИ создаёт копию журнала аудита в виде защищённого архива и экспортирует его на АРМ управления по протоколу *systel.link*;
4. После завершения процедуры экспорта МЗИ удаляет копию журнала аудита на УСПД;
5. ПО «Конфигуратор», получив зашифрованный архив, распаковывает и расшифровывает его общим ключом.
6. Далее информация сохраняется в локальном файле в подпапке «issClient\rcv\IP-адрес сервера» ПО «Конфигуратор» в формате *«auditГодМесяцДатаВремя.log*» в преобразованном виде с помощью ключа, известного программе «Конфигуратор».
7. Чтение записей журнала аудита осуществляется из локального файла авторизированным пользователем программы «Конфигуратор».

Выгрузка информации о событиях безопасности (журнал аудита) на АРМ управления осуществляется в защищённом виде. Применяется протокол IPSec, который обеспечивает проверку подлинности источника данных, защиту целостности и конфиденциальность данных.

Доступ на выгрузку журнала аудита обеспечивается только для уполномоченных пользователей в соответствие с правами разграничения доступа (Таблица 3).

Предусмотрена пересылка событий безопасности на внешний syslog-сервер из программы «Конфигуратор».

## Интерфейс работы с журналом аудита

Функции взаимодействия с журналом аудита находятся на контекстной вкладке «Журнал аудита» ленты инструментов. Для вызова которой необходимо нажать кнопку «Журнал аудита» главной вкладки ленты инструментов.

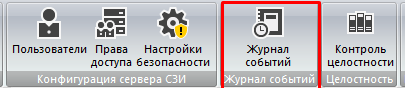


Рисунок 8.1.1 Вызов вкладки «Журнал аудита»

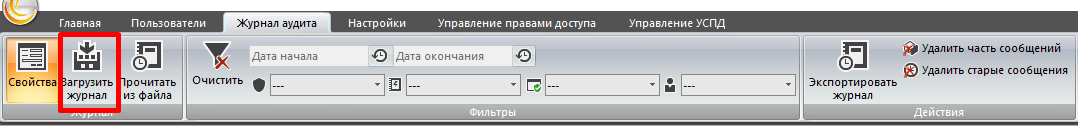
Команды, доступные на контекстной вкладке «Журнал событий» ленты инструментов, описаны в Таблице 6.

Таблица 6 – Команды контекстной вкладки «Журнал событий» ленты инструментов

|  |  |
| --- | --- |
| **Название элемента** | **Пояснение** |
|  | Вызывает окно свойств журнала аудита. |
|  | Посылка команды на получения файла журнала аудита с сервера МЗИ.  Файл с журналом аудита помещается в папку «rcv\ip-адрес источника\auditГГММДДЧЧММСС.log» с установленным ПО «Конфигуратор»  После удачной загрузки файла события отобразятся в окне «Журнал аудита» |
|  | Чтения событий из ранее загруженного журнала аудита. Команда не требует подключения к МЗИ. |
|  | Очистка примененных фильтров |
|  | Экспорт текущего журнала аудита в syslog.  Предварительно должно быть настроено подключение к syslog-серверу (п.3.4). |
|  | Посылка команды серверу МЗИ на удаление 20% самых старых событий. |
|  | Посылка команды серверу МЗИ на удаление событий, записанных ранее определенной даты (появление окна выбора даты). |

## Чтение записей журнала аудита

Для вызова журнала аудита необходимо на главной панели ленты инструментов нажать кнопку «Журнал событий». Сразу появляется окно просмотра журнала событий безопасности. Для отображения записей необходимо нажать кнопку «Загрузить журнал» на контекстной панели «Журнал событий» ленты инструментов. После чего на сервер отправится запрос на получение журнала событий и результат отобразится в интерфейсе.



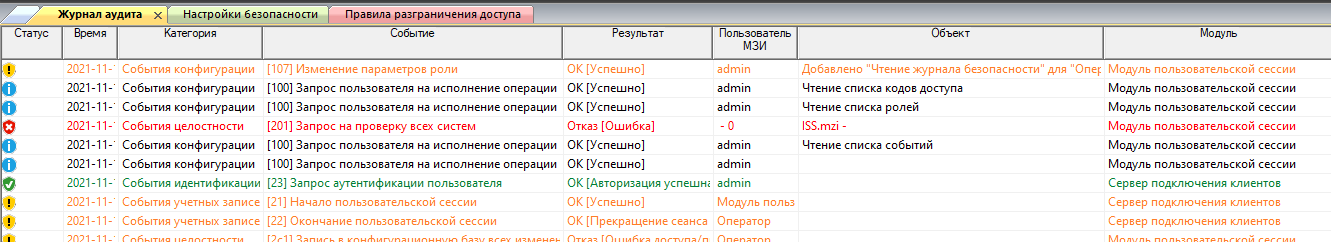


Рисунок 8.2.1 Вид окна журнала событий безопасности

Каждая запись, отображаемая в реестре событий журнала аудита, содержит следующую информацию:

* статус: информационное, ошибка, предупреждение, успех.
* дата и время;
* категория события безопасности;
* название события безопасности и [код] безопасности;
* результат события (ошибка, успех);
* пользователь, связанный с регистрируемым событием;
* объект регистрируемого события;
* модуль, связанный с регистрируемым событием;
* текст с дополнительной информацией (если есть).

Записи аудита безопасности располагаются снизу-вверх. Таким образом самые новые записи находятся вверху списка.

При выгрузке журнала аудита происходит его сохранение на диске в папке «rcv/IP-адрес сервера» с именем «audit\_Дата\_Время.log».

## Выборочное чтение записей аудита

Для выбора из общего реестра требуемых событий безопасности применяются фильтры. На контекстной вкладке ленты инструментов «Журнал событий» находится панель «Фильтры» (Рисунок 8.3.1)

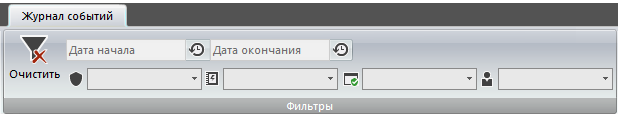


Рисунок 8.3.1 Панель фильтров журнала событий

При нажатии кнопок «Дата начала» и «Дата окончания» вызывается диалоговое окно выбора даты для фильтрации полученного списка событий по дате (Рис.). А ниспадающие списки позволят отфильтровать события безопасности по следующим критериям:

1. Статус события: информация, предупреждение, ошибка.
2. Категория события.
3. Пользователь, в чей сеанс сгенерировано событие (если есть).

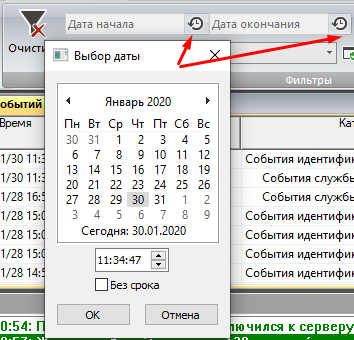


Рисунок 8.3.2 Фильтр по дате сообщения

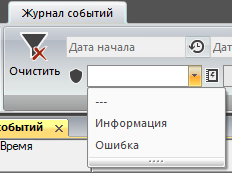


Рисунок 8.3.3 Фильтр по типу сообщения

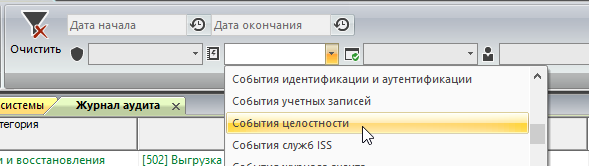


Рисунок 8.3.4 Фильтр по категории сообщения

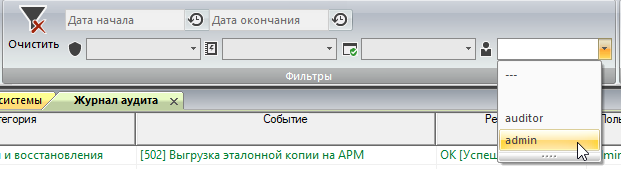


Рисунок 8.3.5 Фильтр по пользователю, в чей сеанс сгенерировано сообщение

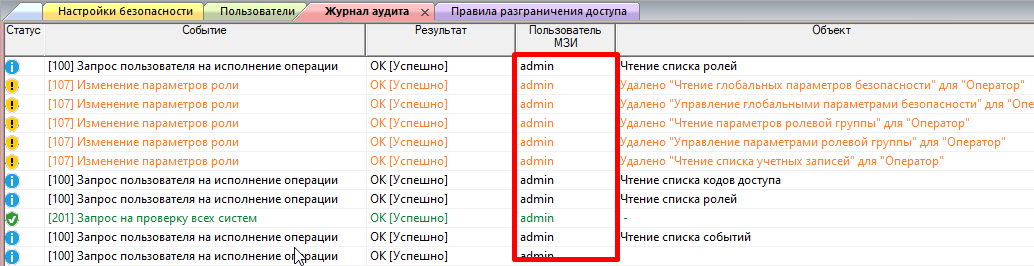


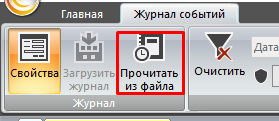
Рисунок 8.3.6 Выборочный просмотр событий аудита

Для сброса выбранных фильтров необходимо нажать кнопку «Очистить» контекстной вкладки «Журнал аудита» ленты инструментов.

## Просмотр ранее загруженных журналов аудита

В программе «Конфигуратор» существует возможность просмотра ранее загруженных журналов аудита. При этом подключение к серверу МЗИ не требуется.

1. Вызвать окно «Журнал аудита» нажатием кнопки «Журнал аудита» ленты инструментов.
2. Нажатием кнопки «прочитать из файла» вызвать диалоговое окно выбора файла журнала аудита для чтения. По умолчанию все копии журнала аудита, полученные от серверов МЗИ, сохраняются в подпапку «rcv\IP-адрес сервера» ПО «Конфигуратор ИБ».
3. Выбрать из списка нужный журнал который был загружен в папку«rcv/IP-адрес сервера» с именем «audit\_Дата\_Время.log». Нажать кнопку «Открыть».
4. Убедится в отображении данных аудита.



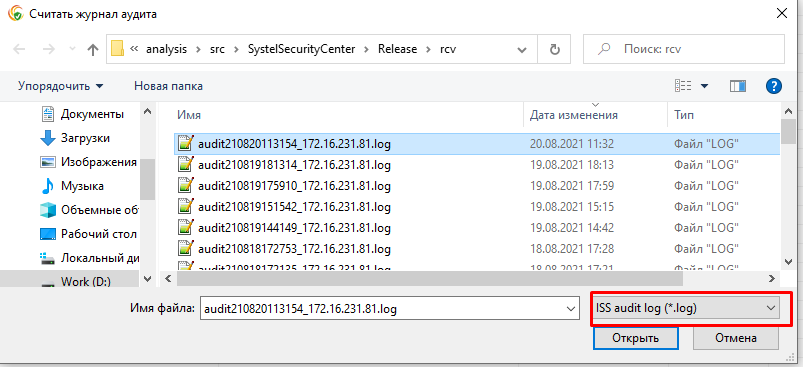


Рисунок 8.4.1 Чтение ранее выгруженных из контроллера событий аудита

## Очистка журнала аудита

На устройстве установлено ограничение по размеру журнала аудита. В связи с этим необходимо осуществлять периодическую выгрузку данных аудита на АРМ с помощью команды «Загрузить журнал».

При достижении текущего размера журнала аудита в 90% от максимального в окне сообщений «Конфигуратора» отобразится сообщение, представленное на рисунке.

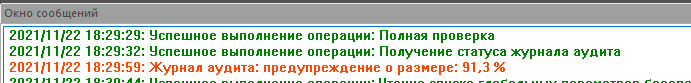


Рисунок 8.5.1 Сообщения о размере журнала аудита

Если оператором не было предпринято никаких действий по ручной очистке, тогда по достижению 100% размера журнала аудита произойдет его автоматическая очистка до размера 80% от максимального (Рисунок 8.5.2).

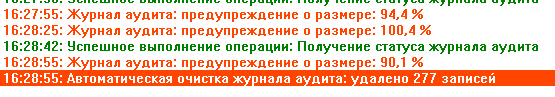
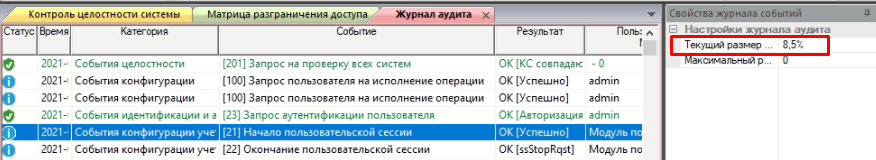


Рисунок 8.5.2 Сообщение об автоматической очистке журнала аудита

В окне свойств журнала событий отображается текущий уровень заполнения журнала событий (в % от максимального).



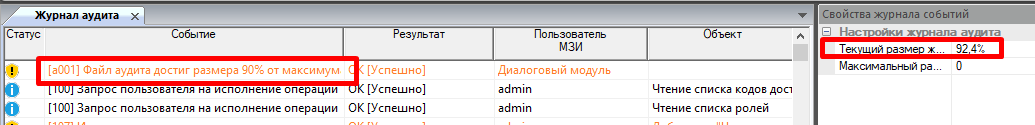


Рисунок 8.5.3 Свойства журнала событий

Для ручной очистки журнала аудита необходимо:

1. На ленте инструментов раздела «Журнал аудита» вызвать одну из команд удаления записей аудита, а именно:

* кнопка «Удалить часть сообщений» позволяет удалять порциями по 20% самых старых событий аудита
* кнопка «Удалить старые сообщения» позволяет установить дату, ранее которой будут удалены все записи аудита.

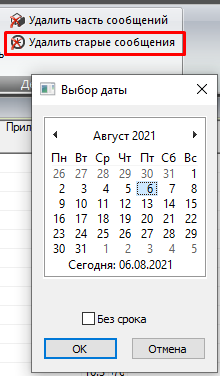
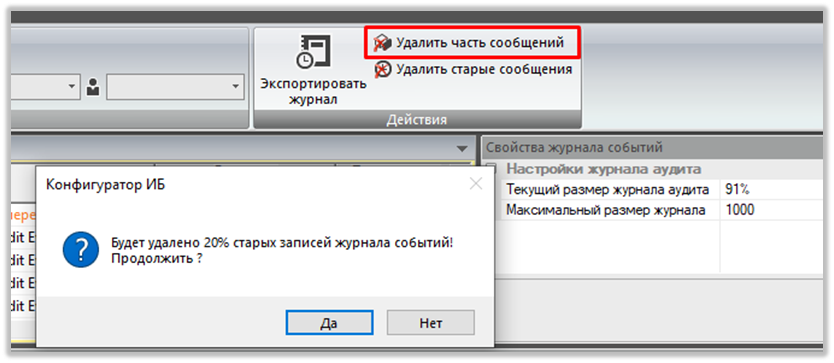


Рисунок 8.5.4 Способы очистки журнала аудита

1. Вызвать одну из команд. В журнале появятся соответствующие записи аудита ()Рисунок 8.5.5.

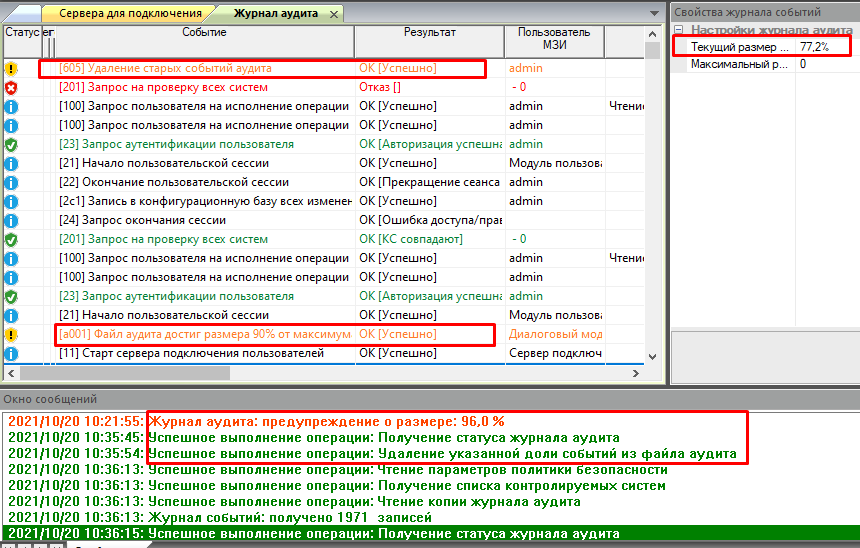


Рисунок 8.5.5 Сообщения об успешной загрузке и очистке журнала аудита

## Загрузка журнала аудита на syslog-сервер

В случаях, когда необходимо выгрузить данные журнала аудита на *syslog-сервер*, предусмотрен механизм экспорта ранее выгруженных журналов аудита с помощью программы «Конфигуратор». Для этого предварительно необходимо произвести настройку доступа к серверу *syslog* (раздел 3.5).

1. Нажать кнопку «Загрузить журнал» ленты инструментов.
2. Нажать кнопку «Экспортировать журнал». В появившемся окне подтвердить операцию. Дождаться окончания выгрузки данных.

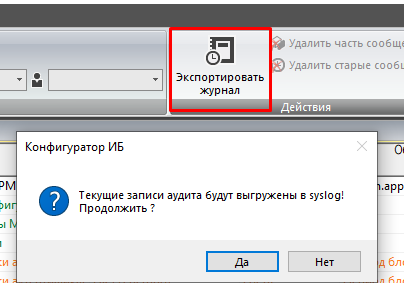


Рисунок 8.6.1 Экспорт журнала аудита

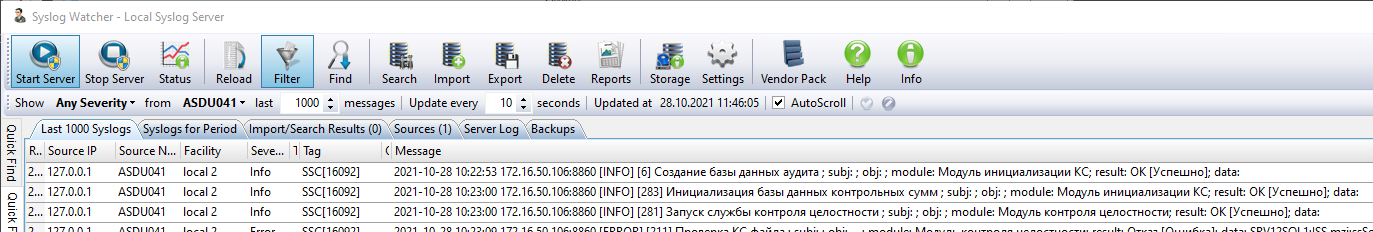


Рисунок 8.6.2 Сообщения аудита, переданные в syslog через Конфигуратор ИБ

## Регистрируемые события безопасности

В журнале безопасности МЗИ фиксируются события безопасности, представленные в Таблице 7.

Таблица 7 – События безопасности журнала аудита

|  |  |
| --- | --- |
| **Идентификатор события** | **Название события** |
| 1 | Старт сервера аудита |
| 2 | Останов сервера аудита |
| 11 | Старт сервера подключения пользователей |
| 13 | Останов сервера подключения пользователей |
| 21 | Начало пользовательской сессии |
| 22 | Окончание пользовательской сессии |
| 23 | Запрос аутентификации пользователя |
| 24 | Запрос окончания сессии |
| 100 | Запрос пользователя на исполнение операции |
| 101 | Установка пароля пользователя |
| 102 | Добавление нового пользователя |
| 103 | Удаление пользователя |
| 104 | Изменение параметров пользователя |
| 105 | Добавление новой роли |
| 106 | Удаление роли |
| 107 | Изменение параметров роли |
| 108 | Изменение параметров политики аутентификации |
| 110 | Требование смены пользовательского пароля |
| 111 | Блокировка пользователя |
| 112 | Разблокировка пользователя |
| 1A1 | Запрос пользователя на разрешение доступа к операции |
| 201 | Запрос на проверку всех систем |
| 202 | Запрос на проверку компоненты МЗИ или СПО |
| 211 | Запрос пользователя на проверку целостности файла |
| 2A1 | Замена файла на загруженный с АРМа |
| 2A2 | Восстановление файла из копии |
| 281 | Старт сервера резервирования и контроля целостности |
| 282 | Останов сервера резервирования и контроля целостности |
| 291 | Старт программы проверки целостности и инициализации МЗИ |
| 292 | Останов программы проверки целостности и инициализации МЗИ |
| 2C1 | Запись в конфигурационную базу всех измененных параметров |
| 2B1 | Обновление контрольных сумм всех компонент указанного раздела |
| 2B2 | Обновление контрольных сумм всех компонент МЗИ и СПО |
| 300 | Запрос на останов всех компонент МЗИ и СПО |
| 301 | Запрос на запуск всех компонент указанного приложения |
| 302 | Запрос на останов всех компонент указанного приложения |
| 501 | Создание эталонной копии ПО |
| 502 | Выгрузка эталонной копии на АРМ |
| 503 | Восстановление компонент из эталонной копии |
| 504 | Создание резервной копии конфигурации |
| 505 | Выгрузка резервной копии компоненты на АРМ |
| 506 | Восстановление компонент из резервной копии |
| 507 | Загрузка файла с эталонной или резервной копией в контроллер |
| 508 | Загрузка файла с эталонной копией в контроллер |
| 509 | Загрузка файла с резервной копией в контроллер |
| 604 | Выгрузка копии файла аудита на АРМ |
| 605 | Удаление старых событий аудита |
| A001 | Файл аудита достиг размера 90% от максимума |
| A002 | Файл аудита достиг максимального размера |
| A003 | Произведено автоматическое удаление старых событий до размера аудита 90% (Max) |
| E002 | Запуск на контроллере сервера удалённого доступа sshd |
| E003 | Остановка на контроллере сервера удалённого доступа sshd |
| E004 | Перезагрузка контроллера |
| DC01 | Инициализация таблицы с описанием событий |
| DC02 | Занесение записи с параметрами для подключения Конфигуратора |
| DC03 | Инициализация таблицы с параметрами политики безопасности |
| DC04 | Инициализация таблицы масок прав доступа |
| DC05 | Инициализация таблицы требуемых для исполнения операций прав доступа |
| DC06 | Инициализация таблицы ролей |
| DC07 | Инициализация таблицы пользователей |
| DCEC | Подготовка базы контрольных сумм компонентов МЗИ и СПО |

# УПРАВЛЕНИЕ УСПД

С помощью ПО «Конфигуратор» можно посылать сервисные команды для управления работой контроллера. Доступные команды представлены в Таблица 6.

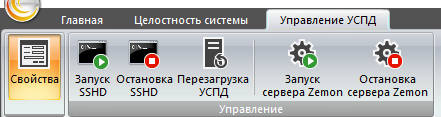


Рисунок 8.7.1 Сервисные команды УСПД

Таблица 6 – Команды УСПД

|  |  |
| --- | --- |
| **Название элемента** | **Пояснение** |
|  | Вызывает окно свойств журнала аудита. |
|  | Посылка команды на запуск ssh демона. По умолчанию при штатной работе УСПД невозможно напрямую установить сессию с устройством через SSH. Предварительно Администратор МЗИ (либо другой пользователь с необходимыми правами) должен отправить запрос на запуск демона SSH. |
|  | Посылка команды для остановки ssh демона. По умолчанию при штатной работе УСПД невозможно напрямую установить сессию с устройством через SSH. |
|  | Посылка команды на устройство для его перезагрузки |
|  | Посылка команды на устройство для запуска СПО Zemon |
|  | Посылка команды на устройство для остановки СПО Zemon |

## Приложение. Сообщения оператору

|  |  |  |
| --- | --- | --- |
| **Номер сообщения п/п** | **Сообщение** | **Тип** |
| 1 | Подключение к серверу | Успех |
| 2 | Сервер прервал соединение | Предупреждение |
| 3 | Не выбран сервер для подключения | Предупреждение |
| 4 | Не указан порт для подключения | Предупреждение |
| 5 | Не указан IP-адрес для подключения | Предупреждение |
| 6 | Нет подключения к серверу | Ошибка |
| 7 | Доступ для этой программы закрыт | Ошибка |
| 8 | Доступ для данного пользователя закрыт | Ошибка |
| 9 | Недостаточно прав для выполнения операции: [название\_операции] | Ошибка |
| 10 | Ошибка выполнения операции: | Ошибка |
| 11 | Удаление всех администраторов невозможно: | Ошибка |
| 12 | Удаление присоединенных пользователей невозможно. Необходимо завершить сеансы пользователей | Ошибка |
| 13 | Успешное выполнение операции: [название\_операции] | Успех |
| 14 | Пользователь [имя] подключился к серверу. | Успех |
| 15 | Пользователь [имя] отключился от сервера. | Успех |
| 16 | Ошибки при подключении к серверу. | Ошибка |
| 17 | Ошибка авторизации: неверный логин или пароль. | Ошибка |
| 18 | Ошибка авторизации: пользователь уже идентифицирован под другим логином. Необходимо переподключится к серверу. | Ошибка |
| 19 | Ошибка авторизации: доступ для данного пользователя закрыт. | Ошибка |
| 20 | Превышено максимальное количество попыток входа. | Ошибка |
| 21 | Превышено максимальное количество активных сессий учетной записи. | Ошибка |
| 22 | Пароль устарел. Требуется сменить пароль. | Предупреждение |
| 23 | Учетная запись заблокирована. | Ошибка |
| 24 | Подключение: время сессии заканчивается. Осталось [N] минут | Предупреждение |
| 25 | [a001] Предупреждение о размере журнала аудита: [N]% | Предупреждение |
| 26 | [a003] Автоматическая очистка журнала аудита: удалено [N] записей | Предупреждение |
| 27 | Статус сервера: минимальный режим | Предупреждение |
| 28 | Статус сервера: безопасный режим | Успех |
| 29 | Сервер [имя]: имя сервера успешно изменено на [\_имя\_] | Успех |
| 30 | Сервер [имя]: IP-адрес сервера успешно изменен | Успех |
| 31 | Сервер [имя]: тип сервера успешно изменен | Успех |
| 32 | Пользователи: получено [N] записей | Успех |
| 33 | Роли: получено [N] записей | Успех |
| 34 | Права доступа: получено [N] записей | Успех |
| 35 | Файлы: получено [N] записей | Успех |
| 36 | Журнал аудита: получено [N] записей | Успех |

# Обновление программного обеспечения

При выпуске критических обновлений, влияющих на безопасность ПО контроллера «МТК-30.КП», разработчик информирует пользователей согласованным способом (п.5.3 документ «Средства защиты информации для ПТК «Систел». Формуляр. RU.АДМШ.421457-45 30 01).

Проверка администратором полученных обновлений и корректности их применения должна проводиться при помощи программы ФИКС 2.0.2.

В случае обнаружения «посторонних» (незарегистрированных) программ, нарушения целостности программного обеспечения, работа должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией и организованы работы по анализу и ликвидации негативных последствий данного нарушения.

Выполнение обновления осуществляется в соответствии с порядком обновления ПО.

## ПОРЯДОК ОБНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Обновления передаются Организации согласованным способом на CD-диске, который содержит установочные архивы обновлений и установочный ключ.

ВАЖНО: CD-диск с обновлениями содержит контрольные суммы архивов обновлений. Перед установкой обновлений необходимо проконтролировать контрольные суммы с помощью ПО ФИКС 2.0.2

1. В режиме командное окно войти в программную среду контроллера под учётной записью issadmin
2. Архив с дистрибутивом и файлом и установочным ключом следует разместить в структуре каталогов пользователя issadmin.
3. Запустить утилиту, которая распаковывает архив с дистрибутивом. При этом автоматически запускается сервис установки обновления.
4. Этот сервис останавливает службы МЗИ, перемонтирует соответствующий раздел файловой системы в режиме с разрешенной записью и запускает программу issRecovery. которая восстанавливает новое ПО из архива на место старого.
5. Программа issRecovery восстанавливает содержащиеся в архиве файлы. Для этого программа проверяет контрольную сумму каждой записи, копирует из архива содержимое файла по указанному пути, восстанавливает владельца файла и права доступа к нему. О результате восстановления архива в лог аудита записывается специальное сообщение.
6. После восстановления файлов установочная программа вычисляет новые контрольные суммы по алгоритму контроля целостности МЗИ
7. Затем сервис создаёт новую эталонную копию ПО МЗИ и копирует её на раздел, который в рабочем режиме монтируется только на запись.
8. Производится перезапуск контроллера.
9. После обновления ПО вся предыдущая конфигурация контроллера сохраняется.

Список определений и сокращений

| **Термин** | **Полная форма** |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| ВСЗИ | Встроенные средства защиты информации |
| МЗИ | Модуль Защиты информации |
| КСЗ | Комплекс средств защиты информации |
| ПТК | Программно-технический комплекс |
| МТК-30.КП | контроллер серии «МТК-30.КП» |
| ПО | Программное обеспечение |
| СПО | Специализированное программное обеспечение |
| НСД | Несанкционированный доступ |
| КЦ | Контроль целостности |
| КС | Контрольные суммы |
| ПРД | Правила разграничения доступа |
|  |  |
|  |  |

1. 1) ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов [↑](#footnote-ref-1)
2. 2) ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов [↑](#footnote-ref-2)
3. 3) ГОСТ 19.104-78\* ЕСПД. Основные надписи [↑](#footnote-ref-3)
4. 4) ГОСТ 19.105-78\* ЕСПД. Общие требования к программным документам [↑](#footnote-ref-4)
5. 5) ГОСТ 19.106-78\* ЕСПД. Общие требования к программным документам, выполненным печатным способом [↑](#footnote-ref-5)
6. 6) ГОСТ 19.402-78\* ЕСПД. Описание программы [↑](#footnote-ref-6)
7. 7) ГОСТ 19.604-78\* ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом [↑](#footnote-ref-7)
8. МЗИ:клиент является компонентом средств защиты информации программного комплекса «ОИК Систел», Технические условия, RU.АДМШ.421457-05 97 01 [↑](#footnote-ref-8)