ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ «ЭКРА»

УТВЕРЖДЕН

ЭКРА.00095-01 95 01-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ТЕРМИНАЛА МИКРОПРОЦЕССОРНОГО СЕРИИ ЭКРА 200

Информационная безопасность

Руководство администратора

ЭКРА.00095-01 95 01

Листов 30/с.60

2023

Изм. №1 от 08.12.2023

Замечания и предложения по руководству администратора направлять по адресу ekra@ekra.ru

АННОТАЦИЯ

Настоящий документ является руководством администратора программного обеспечения (ПО) терминала микропроцессорного серии ЭКРА 200 (далее – терминал), встроенного (программа E3_SW91) и прикладного (программы Конфигуратор и Smart Monitor, входящие в комплекс программ EKRASMS-SP).

Руководство администратора содержит описание:

– действий по приемке поставленного терминала;

– действий по безопасной установке и настройке;

– действий по реализации функций безопасности среды функционирования терминала, в том числе по конфигурированию компонентов ПО при первоначальной установке и изменению базовых настроек безопасности;

– ограничений условий эксплуатации терминала;

– правил и процедур обеспечения ИБ при эксплуатации терминала.

Настоящий документ актуален для версий прикладного ПО 4.0.0.24876 и выше, встроенного ПО 7.1.0.9[1)].

[1)] Возможно применение документа и для иной версии прикладного ПО и ПО терминала. Таблица соответствия версий ПО и изменения документа представлена на сайте https://soft.ekra.ru/smssp/ru/downloads/documents/.

СОДЕРЖАНИЕ

Обозначения и сокращения

ADU – application data unit (блок прикладных данных)
cid – configured IED description (файл описания конфигурации устройства)
CRC – cyclic redundancy check (циклический избыточный код)
DDoS – distributed denial of service (распределенный отказ в обслуживании)
DoS – denial of service (отказ в обслуживании)
FAT – file allocation table (таблица размещения файлов)
FAU_GEN – security audit data generation (генерация данных аудита безопасности)
FAU_SAR – security audit review (обзор аудита безопасности)
FAU_STG – security audit event storage (хранение событий аудита безопасности)
FDP_ACC – access control policy (политика контроля доступа)
FDP_ACF – security attribute based access control (управление доступом на основе атрибутов безопасности)
FDP_ROL – rollback (откат к исходному состоянию)
FDP_SDI – stored data integrity (целостность хранимых данных)
FIA_AFL – authentication failures (отказы аутентификации)
FIA_ATD – user attribute definition (определение атрибутов пользователя)
FIA_UAU – user authentication (аутентификация пользователя)
FIA_UID – user identification (идентификация пользователя)
FMT_MSA – management of security attributes (управление атрибутами безопасности)
FMT_MTD – management of TSF data (управление учетными данными пользователей)
FMT_SMF – specification of management functions (спецификация функций управления)
FMT_SMR – security management roles (роли в управлении безопасностью)
FPT_STM – reliable time stamps (надежные временные метки)
FTA_SSL – session locking (блокировка сеанса)
FTP – file transfer protocol (протокол передачи файлов по сети)
IP – internet protocol (межсетевой протокол)
IT – information technology (информационные технологии)
RFC – request for comments (документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети)
SFV – simple file verification (файлы для контроля целостности файлов, используют контрольную сумму для ее проверки)
TSF – the safety functions (функция безопасности)
VLAN – virtual local area network (виртуальная локальная сеть)
Wi-Fi – wireless fidelity (беспроводная связь)
АВЗ – антивирусная защита

АРМ	–	автоматизированное рабочее место
АСУ	–	автоматизированная система управления
АСУ ТП	–	автоматизированная система управления технологическими процессами
АУД	–	аудит безопасности
АЦП	–	аналогово-цифровой преобразователь
ДНС	–	действия в нештатных ситуациях
ЗИС	–	защита информационной системы
ЗНИ	–	защита носителей информации
ЗТС	–	защита технических средств и систем
ИАФ	–	идентификация и аутентификация
ИБ	–	информационная безопасность
ИЧМ	–	интерфейс человек-машина
КП	–	комплекс программ
МЭК	–	международная электротехническая комиссия
ОДТ	–	обеспечение доступности
ОО	–	объект оценки
ООО НПП «ЭКРА»	–	общество с ограниченной ответственностью научно-производственное предприятие «ЭКРА»
ОПО	–	обновления ПО
ОПС	–	ограничение программной среды
ОС	–	операционная система
ОЦЛ	–	обеспечение целостности
ПК	–	персональный компьютер
ПО	–	программное обеспечение
РЗА	–	релейная защита и автоматика
РФ	–	Российская Федерация
РЭ	–	руководство по эксплуатации
СМНИ	–	съемные машинные носители информации
УКФ	–	управление конфигурацией
УПД	–	управление доступом
ФСТЭК	–	федеральная служба по техническому и экспортному контролю

1 Действия при приемке терминала

Действия при приемке терминала проводятся в соответствии с разделами 2 и 3 документа ЭКРА.650321.001 РЭ «Терминалы микропроцессорные серии ЭКРА 200. Руководство по эксплуатации».

2 Назначение и условия выполнения ПО

2.1 Состав и назначение

Внутреннее ПО терминала состоит из:

– встроенного ПО (программа E3_SW91), входящего в состав терминала и обеспечивающее реализацию базовых задач;

– прикладного ПО (программы Конфигуратор, Smart Monitor, входящие в состав комплекса программ EKRASMS-SP), определяющего пользовательские алгоритмы функционирования и параметры настройки на объекте.

2.2 Системные требования

Минимальные системные требования для функционирования КП EKRASMS-SP:

а) операционные системы:

– Windows Vista SP1 или более поздняя версия;

– Windows Server 2008 (не поддерживается в основной роли сервера);

– Windows Server 2008 R2 (не поддерживается в основной роли сервера);

– Windows Server 2012 R2 (не поддерживается в основной роли сервера);

– Windows 7;

– Windows 8;

– Windows 8.1;

– Windows 10;

– Astra Linux 1.7.4 (с использованием пакета Wine);

б) поддерживаемые архитектуры:

– x86;

– x64;

в) аппаратные требования:

1) процессор с тактовой частотой 1,7 ГГц или выше, 2 Гбайт (для 32-разрядной системы) или 4 Гбайт (для 64-разрядной системы) оперативной памяти или больше;

2) минимальное место на диске:

– x86 – 850 Мбайт;

– x64 – 4 Гбайт.

3 Идентификация и аутентификация

3.1 Общие сведения

3.1.1 В процессе выполнения идентификации и аутентификации пользователей реализуются меры защиты согласно таблице 1.

Таблица 1 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	
ИАФ.7	Защита аутентификационной информации при передаче	
FIA_AFL.1.1	Обработка отказов аутентификации	ГОСТ Р ИСО/ МЭК 15408-2-2013
FIA_AFL.1.2	Обработка отказов аутентификации	
FIA_ATD.1.1	Определение атрибутов пользователя	
FIA_UAU.2.1	Аутентификация до любых действий пользователя	
FIA_UAU.7.1	Аутентификация с защищенной обратной связью. Защита аутентификационной информации от внешнего наблюдения	
FIA_UID.2.1	Идентификация до любых действий пользователя	
FTA_SSL.1.1	Блокирование сеанса доступа пользователя при неактивности	
FTA_SSL.1.2	Блокирование сеанса доступа пользователя при неактивности	

Объектом доступа в терминале является управляющая («командная») информация, обеспечивающая управление критически важными устройствами объектов (процессов передачи электроэнергии) и информационное обеспечение управления такими устройствами (процессами).

Субъектами доступа к вышеперечисленному объекту является эксплуатационный персонал подстанции.

3.1.2 ПО поддерживает для каждого пользователя:

– идентификацию пользователя по логину. Идентификация пользователя происходит до разрешения любого действия (кроме чтения);

– аутентификацию пользователя по паролю. Аутентификация пользователя происходит до разрешения любого действия (кроме чтения).

3.1.3 Вводимая аутентификационная информация защищена от внешнего наблюдения, не передается по сети открытым текстом и хранится в памяти терминала в нечитаемом виде. Пользователю предоставляется только количество введенных символов во время выполнения аутентификации.

3.1.4 После трех неуспешных попыток авторизации с вводом неверного пароля пользователя:

– пользователю отказывается в доступе, возможность повторной авторизации блокируется на установленное разработчиком время;

– фиксируется запись в журнале событий ИБ.

3.1.5 Для разблокирования интерактивного сеанса после определяемого разработчиком интервала времени необходима повторная успешная авторизация пользователя.

3.2 ПО терминала (программа E3_SW91)

3.2.1 Терминал выполняет свои функции на базе операционной системы реального времени. Для идентификации и аутентификации субъекта доступа в терминале вносится информация о пользователях (имя пользователя, пароль), которым присваиваются полномочия (роли) в соответствии с должностными обязанностями субъекта.

Авторизация пользователя в терминале осуществляется по паролю (рисунок 1).

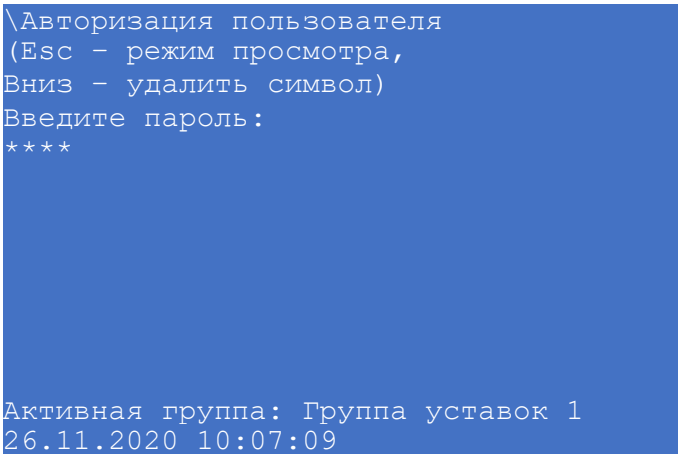


Рисунок 1

При вводе неверного пароля пользователю разрешается только просматривать параметры терминала.

После трех попыток ввода неверного пароля блокируется возможность повторной авторизации на установленное разработчиком время и на дисплее терминала выводится сообщение «Аутентификация пользователя заблокирована, доступен только просмотр».

После неудачных попыток ввода логина/пароля фиксируется запись в журнал событий ИБ. Просмотр журнала событий ИБ по умолчанию доступен только пользователю с ролью «Администратор» через программу Smart Monitor: пункт меню  –> **Загрузить журнал событий информационной безопасности терминала**. При необходимости имеется возможность предоставления доступа к чтению журнала событий безопасности пользователем с ролью «Инженер». Пример содержания журнала событий ИБ приведен на рисунке 2.

```
| 0001 | [10/09/2021 08:07:09] FMT_SMF.1 |       main  |           | 1 | Время включения терминала: 10/09/2021 08:07:09
| 0002 | [10/09/2021 08:07:09] FMT_SMF.1 |       main  |           | 1 | Запуск логирования событий информационной безопасности
| 0003 | [10/09/2021 08:07:31] FDP_SDI.2 |   archiver  |           | 1 | Проверка файла прошивки прошла успешно.
| 0004 | [10/09/2021 08:07:32] FDP_SDI.2 |   archiver  |           | 1 | Проверка файла конфигурации прошла успешно.
| 0005 | [10/09/2021 08:07:32] FDP_SDI.2 |   archiver  |           | 1 | Проверка архива прав доступа прошла успешно.
| 0006 | [10/09/2021 08:10:01] FMT_SMR.1 | permissions |           | 1 | Созданы учетные записи и пароли пользователей по умолчанию.
| 0007 | [10/09/2021 08:10:01] FMT_MSA.3 |       acl   |           | 1 | Используются пароли пользователей по умолчанию
| 0008 | [10/09/2021 08:10:27] FMT_MTD.1 |    updater  |           | 1 | Пуск обновлённой прошивки - версия: 7.1.1.1.0, порт: Картридер, 
| 0009 | [10/09/2021 08:10:28] FMT_MTD.1 |    updater  |           | 1 | Пуск обновлённой конфигурации - версия: 1.22.0, порт: Картридер,
| 0010 | [10/09/2021 08:14:43] FDP_ACF.1 |       main  |           | 1 | Дата и время предыдущего выкл. терминала 10/09/2021 08:13:44

.....

| 9994 | [10/09/2021 08:14:43] FMT_SMF.1 |       main  |           | 1 | Время включения терминала: 10/09/2021 08:14:43
| 9995 | [10/09/2021 08:14:43] FMT_SMF.1 |       main  |           | 1 | Запуск логирования событий информационной безопасности
| 9996 | [10/09/2021 08:15:02] FDP_SDI.2 |   archiver  |           | 1 | Проверка файла прошивки прошла успешно.
| 9997 | [10/09/2021 08:15:02] FDP_SDI.2 |   archiver  |           | 1 | Проверка файла конфигурации прошла успешно.
| 9998 | [10/09/2021 08:15:02] FDP_SDI.2 |   archiver  |           | 1 | Проверка архива прав доступа прошла успешно.
| 9999 | [10/09/2021 08:15:08] FMT_MSA.3 |       acl   |           | 1 | Используются пароли пользователей по умолчанию
| 0001 | [10/09/2021 08:23:59] FDP_ACF.1 |       main  |           | 1 | Дата и время предыдущего выкл. терминала 10/09/2021 08:16:56
```

Рисунок 2

3.2.2 При истечении срока действия пароля имеется возможность смены пароля пользователем. Смена пароля происходит в программе Smart Monitor в пункте **Сервисное меню** –> **Изменение пароля**.

3.2.3 При отсутствии активности в течение определенного времени, интерактивный сеанс пользователя завершается. Настройка указанного времени происходит в программе Smart Monitor в пункте меню «дерева» проекта **Уставки** –> **Системные параметры** –> **Параметры терминала** (рисунок 3, поз. 1) в поле **Дисплей** параметр **Тайм-аут доступа** (рисунок 3, поз. 2). Тайм-аут доступа настраивается в диапазоне от 0,5 до 180 мин. Доступные параметры настройки тайм-аута доступа: 0,5; 1; 2; 5; 10; 15; 20; 30; 180 мин. Для применения изменений необходимо записать уставки в терминале. Запись уставок в терминале происходит при нажатии на панели инструментов на кнопку  .

Записать

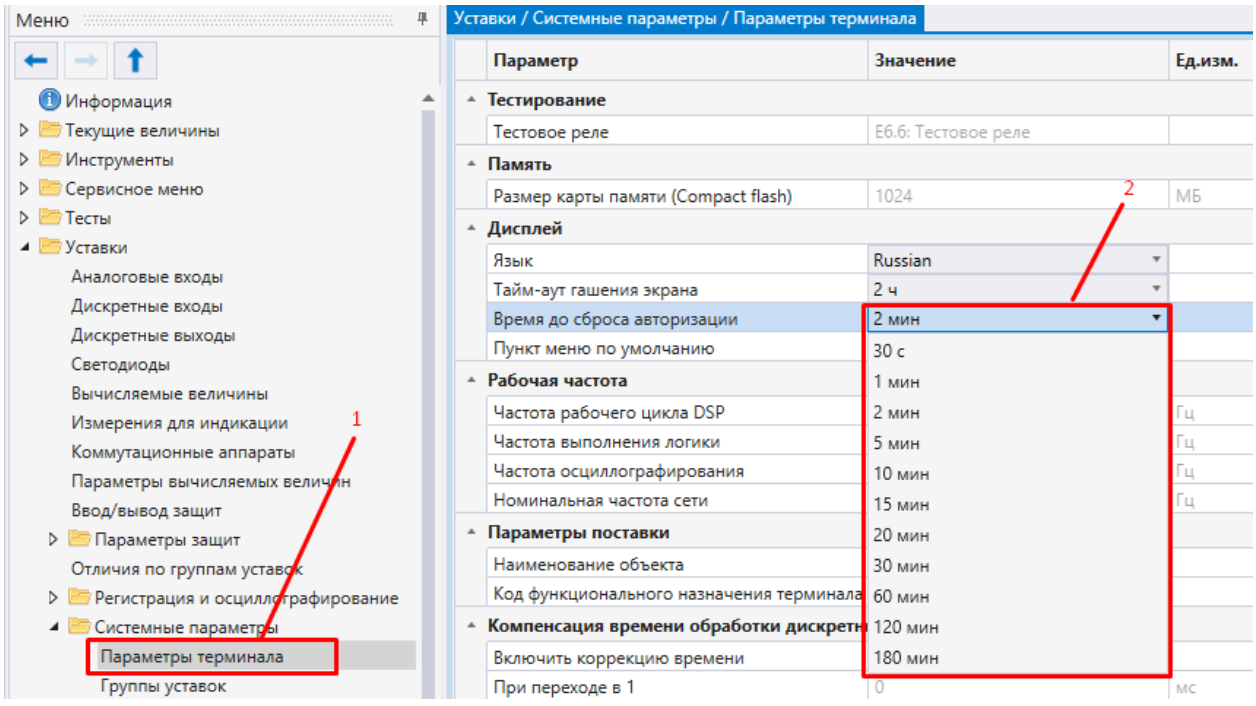


Рисунок 3

3.2.4 Базовая конфигурация терминала содержит следующие учетные записи и роли:

- администратор;
- инженер РЗА;
- инженер АСУ;
- оперативный персонал.

В случае утери пароля пользователя с ролью «Администратор» (после изменения значения пароля по умолчанию), требуется обратиться в службу технической поддержки предприятия-изготовителя по электронной почте support@ekra.ru или по телефону: (8352) 220-130 добавочный номер 1410.

Аутентификационная информация не передается по сети открытым текстом. Защита аутентификационной информации при загрузке новых учетных записей в терминал и при аутентификации пользователей осуществляется путем хеширования данных.

Аутентификационная информация хранится в памяти терминала в нечитаемом виде.

3.2.5 Ограничение доступа эксплуатационного персонала для выполнения конфигурирования терминала осуществляется следующими уровнями доступа (ролями) (таблица 2):

- администратор;
- инженер РЗА;
- инженер АСУ;
- оперативный персонал.

Таблица 2 – Разграничение прав доступа пользователей по умолчанию

Права	Роли			
	Администратор	Инженер РЗА	Инженер АСУ	Оперативный персонал
Администрирование пользователей	Выполнение	-	-	-
Журнал событий ИБ	Чтение	-	-	-
Настройка параметров дисплея (время бездействия, время блокировки ИЧМ и т.п.)	Изменение	-	-	-
Сброс на заводские настройки	Выполнение	-	-	-
Перевод терминала в сервисный режим (режим восстановления, обновления)	Выполнение	-	-	-
Уставки функций РЗА	Чтение / Изменение	Чтение / Изменение	Чтение	Чтение
Настройка регистратора аварийных событий (осциллограф, регистратор)	Чтение / Изменение	Чтение / Изменение	Чтение	Чтение
Перевод терминала в тестовый режим	Выполнение	Выполнение	Выполнение	-
Системные настройки, (IP-адрес, скорость работы последовательного порта, системное время, язык меню)	Чтение / Изменение	Чтение / Изменение	Чтение / Изменение	Чтение
Режим (места) управления: местное/ дистанционное	Выполнение	Выполнение	Выполнение	Выполнение

Права	Роли			
	Администратор	Инженер РЗА	Инженер АСУ	Оперативный персонал
Переключение групп уставок	Выполнение	Выполнение	Выполнение	Выполнение
Управление мнемосхемой	Выполнение	Выполнение	Выполнение	Выполнение
Сброс сигнализации	Выполнение	Выполнение	Выполнение	Выполнение
Файлы-осциллограмм cid-файл, отчеты по устав-кам и протоколам связи	Чтение	Чтение	Чтение	Чтение
Замена конфигурации и об-новление ПО	Выполнение / изменение	Выполнение / изменение	Выполнение / изменение	-
Включение и отключение портов связи	Выполнение	-	-	-
Запись по FTP (по умолча-нию отключен)	Выполнение	-	-	-

3.3 Программа Smart Monitor

3.3.1 На рисунке 4 представлены настройки включения и отключения портов связи Smart Monitor.

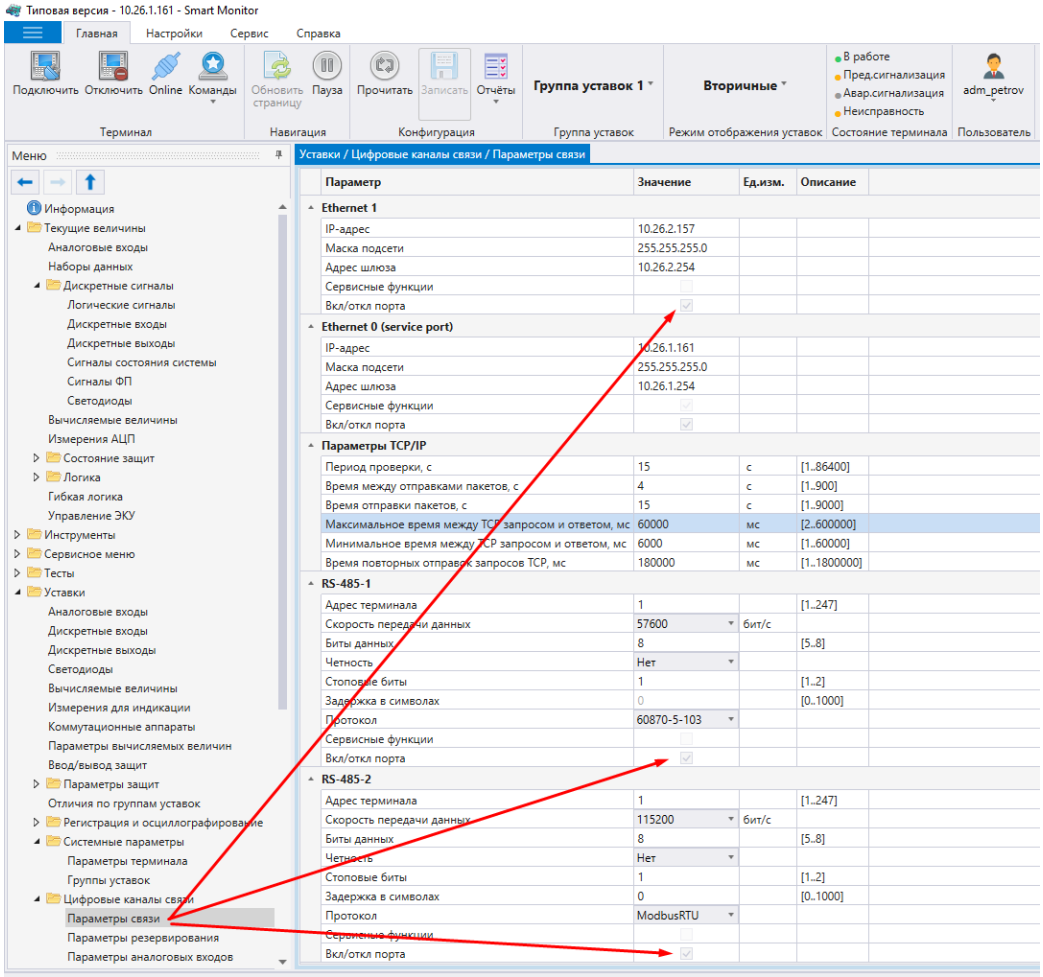


Рисунок 4

3.3.2 Авторизация пользователя происходит при нажатии на панели инструментов на кнопку 

. Форма авторизации пользователя приведена на рисунке 5.

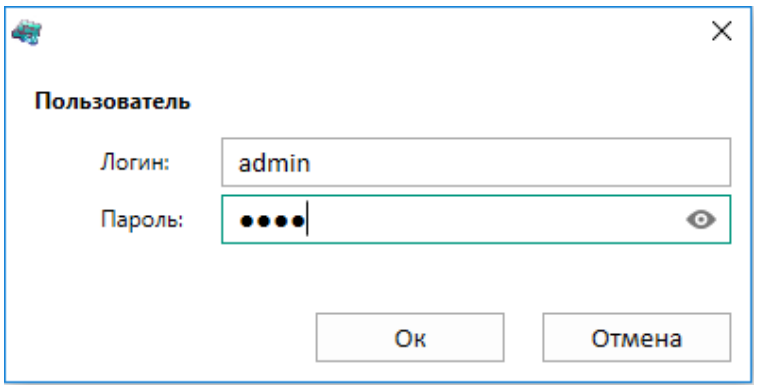


Рисунок 5

Для предотвращения несанкционированного доступа, пароли пользователей по умолчанию (см. таблицу 3) необходимо изменить на пароли сложностью не менее семи (цифровых) символов.

Таблица 3 – Данные пользователей

Пользователь	Логин	Пароль по умолчанию
Администратор	admin	0100
Наладчик АСУ	serviceman_acs	0200
Наладчик РЗА	serviceman_rpa	0300
Оперативный персонал	operator	0400

3.3.3 При использовании паролей пользователей по умолчанию в журнале событий ИБ фиксируется сообщение об использовании паролей по умолчанию до того момента, пока пароль по умолчанию не будет изменен.

При вводе правильных данных открывается рабочая область программы. При вводе неправильных данных выдается сообщение (рисунок 6).

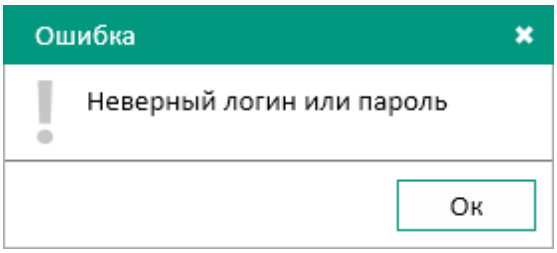


Рисунок 6

После трех неуспешных попыток авторизации с вводом неверного пароля пользователя блокируется возможность повторной авторизации на установленное разработчиком время и выводится сообщение о блокировке (рисунок 7).

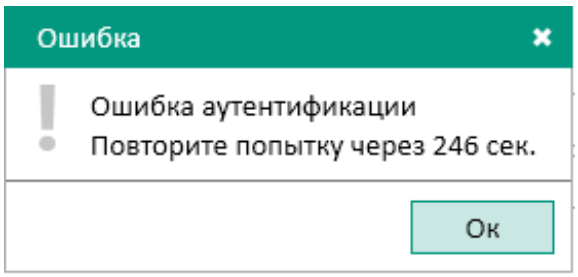


Рисунок 7

При этом выполняется запись в журнал событий ИБ (см. рисунок 2).

3.3.4 Аутентификация пользователей в терминале через программу Smart Monitor осуществляется по протоколу Modbus, модифицированному для безопасной авторизации пользователей и позволяющему удостовериться в подлинности данных аутентификации с обеих сторон. Аутентификационная информация не передается по сети в открытом виде по модифицированному протоколу Modbus. Протокол аутентификации клиентов является адаптацией дайджест-аутентификации согласно RFC 2617. Пакеты внутренних функций передаются не в стандартной форме с помощью ADU, а с помощью специальной пользовательской функции Modbus № 100.

3.3.5 При отсутствии активности в программе Smart Monitor в течение времени, определенного администратором, интерактивный сеанс пользователя завершается и на экран выводится окно для ввода пароля (см. рисунок 8).

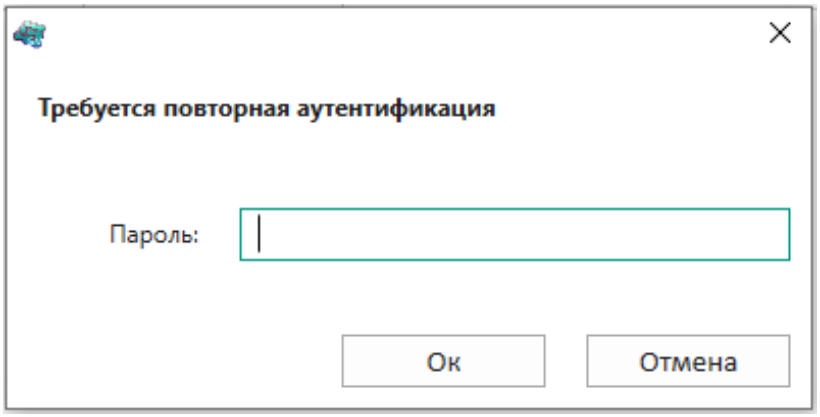


Рисунок 8

3.3.6 Пользователю с ролью «Администратор» доступна функция создания дополнительных учетных записей пользователей, нажатием на кнопку  (кнопка на панели инструментов 

–> **Администрирование пользователей** –> вкладка **Пользователи**) (рисунок 9). События, связанные с администрированием пользователя, фиксируется в журнале событий ИБ.

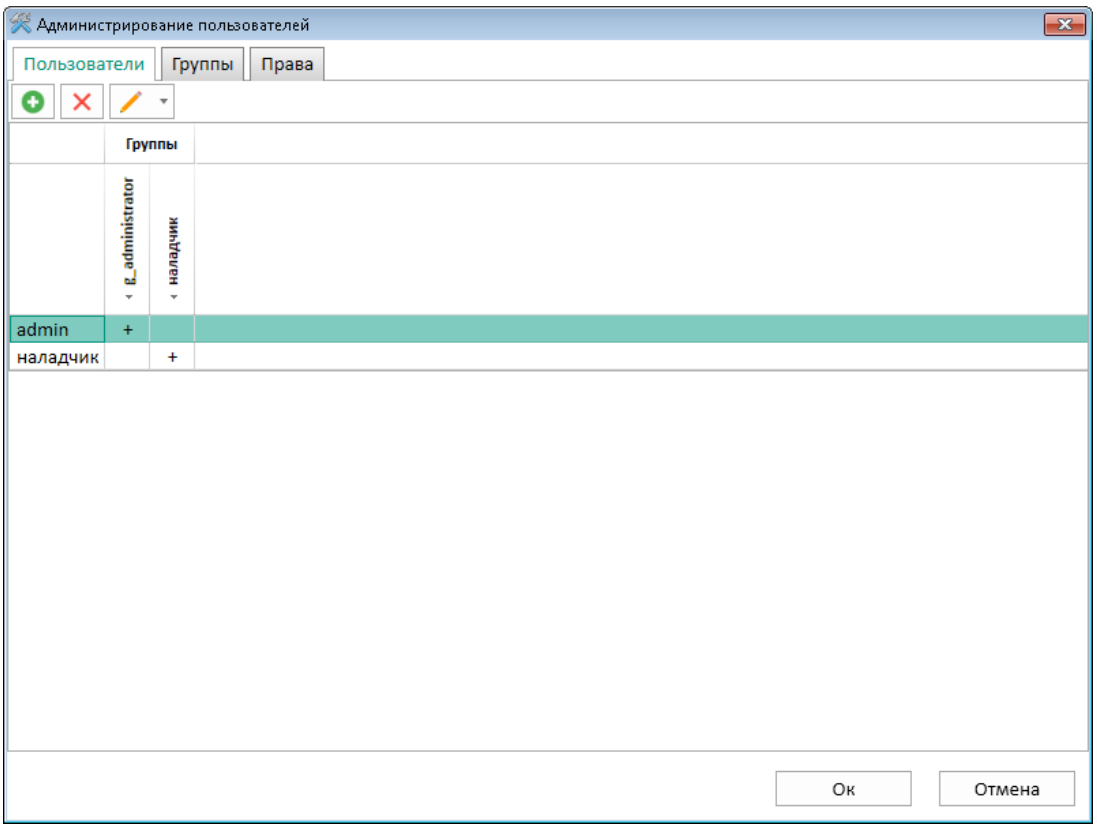


Рисунок 9

Назначение прав новым группам пользователей производится по вкладке **Права** (кнопка на панели инструментов 

–> **Администрирование пользователей** –> вкладка **Права**) (рисунок 10).

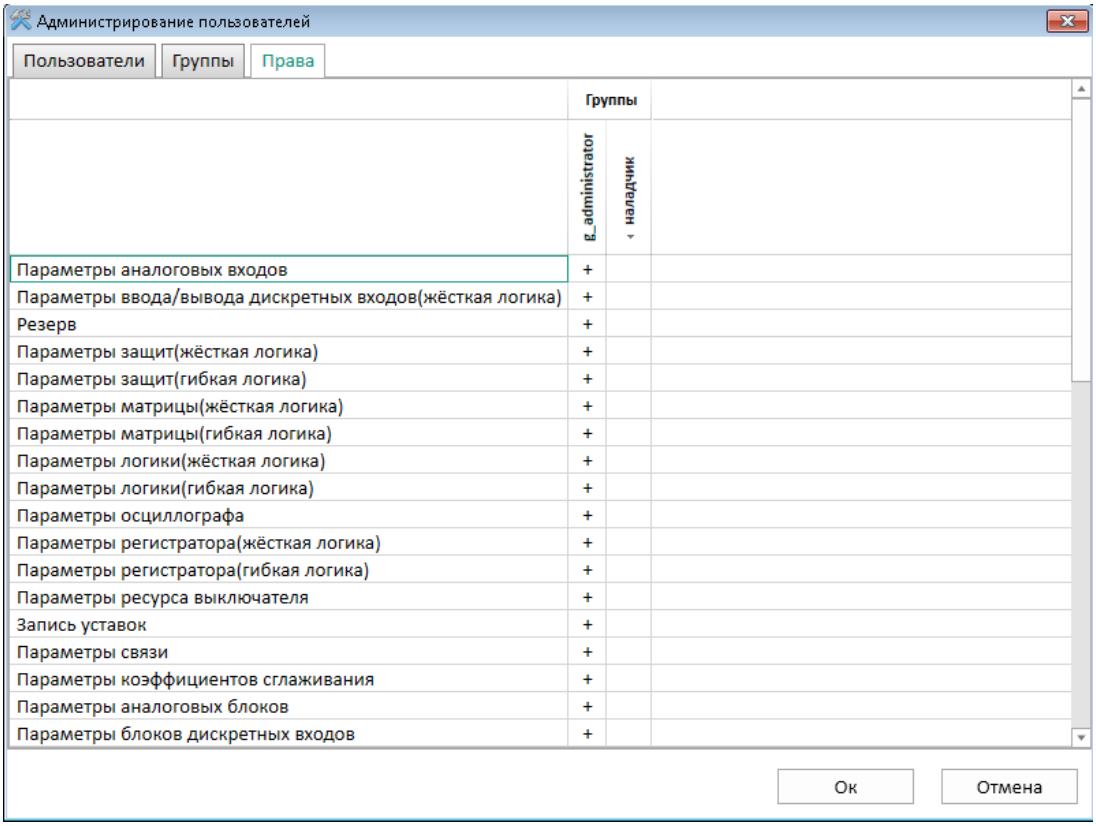


Рисунок 10

Предусмотрена гибкая настройка прав доступа для назначения прав группам пользователей и возможность управления функциями в логической схеме (рисунок 11).

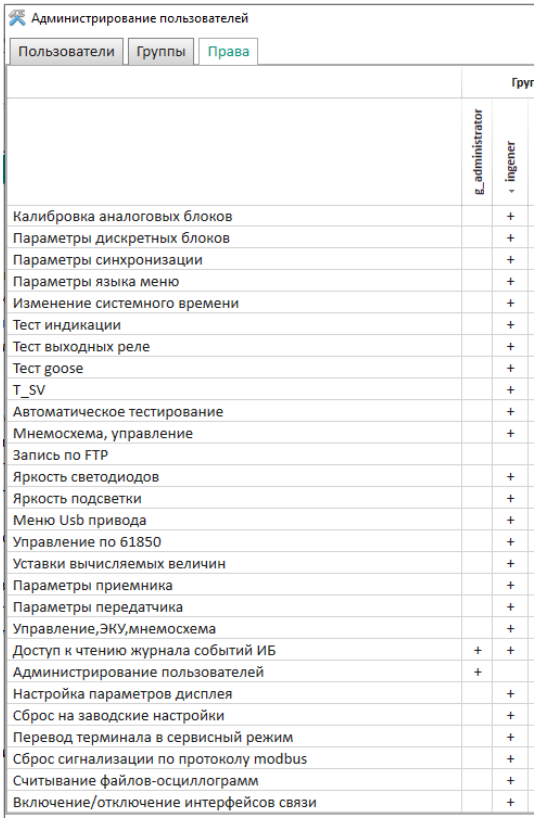


Рисунок 11

3.3.7 Разграничение доступа пользователей терминала настраивается в соответствии с их должностными обязанностями и предназначено для предотвращения несанкционированных действий пользователя по управлению коммутационным оборудованием, изменению режимов и настроек терминала. Запрещается наделение одной учетной записи пользователя несколькими ролями. С целью обеспечения безопасной эксплуатации необходимо настроить права доступа группам пользователей с ролью «Администратор» и «Инженер» в соответствии с требованиями по разграничению прав доступа:

– пользователю с ролью «Администратор» настраиваются права для назначения и изменения паролей, чтения событий в журнале событий безопасности с запретом возможности обновления системного ПО и внесения изменений в параметры настройки (уставки) и алгоритмы функционирования устройства;

– пользователю с ролью «Инженер» настраиваются права для обновления системного ПО и внесения изменений в параметры настройки (уставки) и алгоритмы функционирования устройства, чтения журнала событий безопасности с запретом возможности назначения и(или) изменения паролей сторонних учетных записей.

3.3.8 Для каждой учетной записи пользователя предусмотрена возможность запрета использования старых паролей. Глубина запрета использования – четыре старых (предыдущих) пароля.

3.3.9 При возникновении технической или организационной необходимости (компрометация пароля, установка времени жизни пароля) реализована возможность изменения своего пароля пользователем (см. рисунок 12, поз.1).

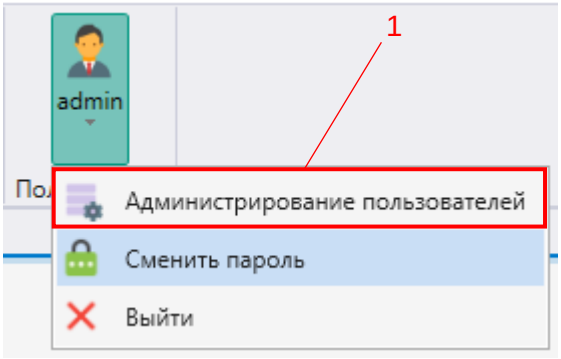


Рисунок 12

3.3.10 Изменение пароля возможно выполнить:

1) в ПО терминала. Для смены пароля необходимо выбрать в пункте меню **Сервисное меню** –> **Изменение пароля** (см. рисунок 13);

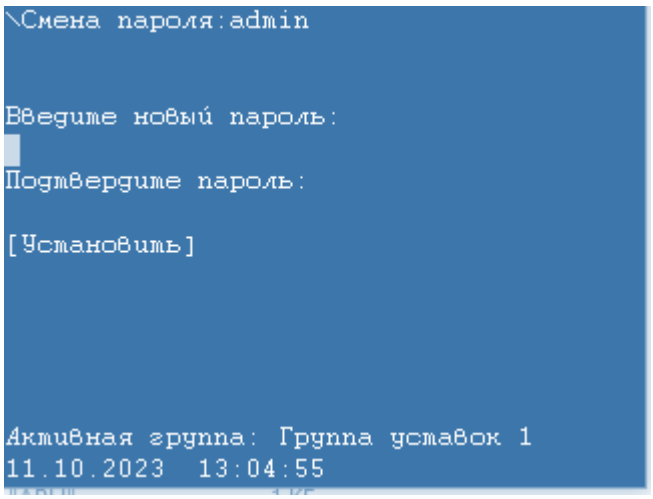


Рисунок 13

2) в программе Smart Monitor. Для смены пароля необходимо выбрать во вкладке **Права** (кнопка на панели инструментов 

–> **Сменить пароль**).

3.3.11 Функции безопасности предъявляют следующие требования к паролям пользователей:

1) пароль должен состоять только из следующих цифр: 0 – 9;

2) не допускается использование пароля с количеством цифр менее семи.

3.3.12 При изменении пароля «Администратором» или самим пользователем возможность повторного задания старых паролей (четыре старых (предыдущих)) запрещена. При этом на экран выводится сообщение об ошибке (рисунок 14).

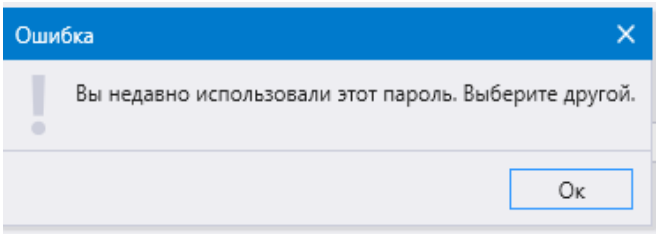


Рисунок 14

После успешной смены пароля пользователем требуется повторно авторизоваться в программе Smart Monitor (рисунок 15).

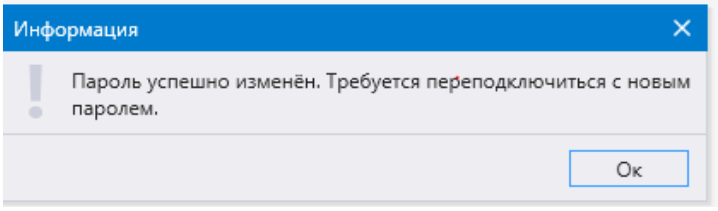


Рисунок 15

3.3.13 Пользователю с ролью «Администратор» предоставлена возможность задания срока действия (времени жизни) пароля для каждого пользователя в диапазоне от 0 до 999 дней (рисунок 16).

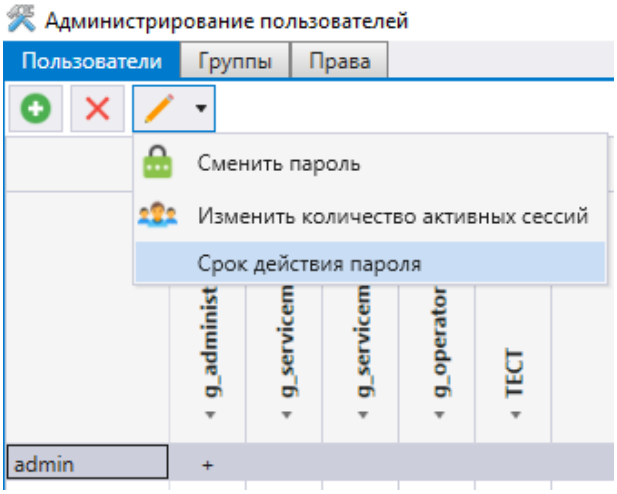


Рисунок 16

Параметр «Количество дней» по умолчанию – 0, срок действия пароля не ограничен. Выбор и последующее применение пользователем с ролью «Администратор» значения параметра «Количество дней» от 1 до 999 формирует функцию обратного отсчета времени, по истечению заданного времени доступ пользователя к программе Smart Monitor ограничивается (рисунок 17).

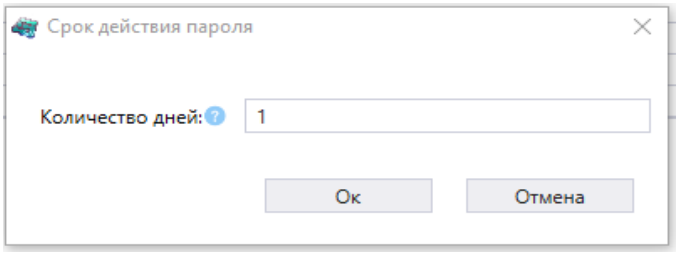


Рисунок 17

В программе Smart Monitor предусмотрена функция напоминания пользователю об истечении срока действия пароля, с предоставлением возможности заблаговременно сменить пароль (рисунок 18).

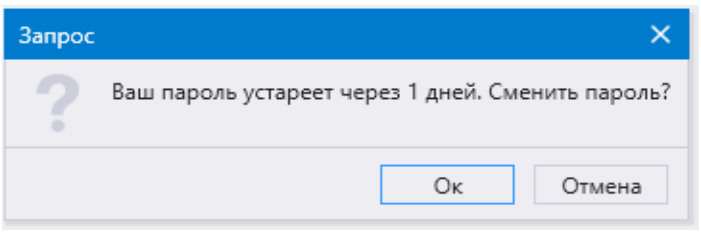


Рисунок 18

Счетчик ранее отсчитанного времени срока действия пароля сбрасывается только после смены пароля (рисунок 19).

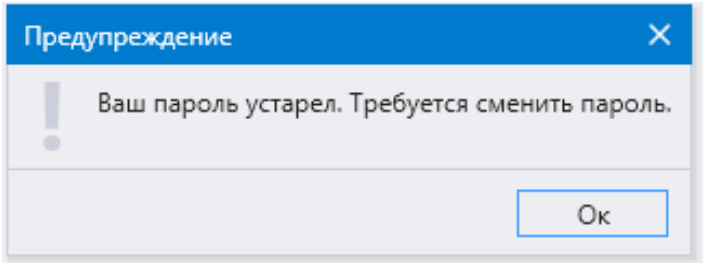


Рисунок 19

4 Управление доступом

4.1 Общие сведения

4.1.1 Управление доступом позволяет реализовать меры защиты согласно таблице 4.

Таблица 4 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
УПД.0	Регламентация правил и процедур управления доступом	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
УПД.1	Управление учетными записями пользователей	
УПД.3	Доверенная загрузка	
УПД.4	Разделение полномочий (ролей) пользователей	
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную систему)	
УПД.9	Ограничение числа параллельных сеансов доступа	
FDP_ACC.1	Ограниченное управление доступом	ГОСТ Р ИСО/ МЭК 15408-2-2013
FDP_ACF.1.1	Управление доступом, основанное на атрибутах безопасности	
FDP_ACF.1.2	Управление доступом, основанное на атрибутах безопасности	
FDP_ACF.1.3	Управление доступом, основанное на атрибутах безопасности	
FDP_ACF.1.4	Управление доступом, основанное на атрибутах безопасности	
FDP_ROL.2.1	Расширенный откат к исходному состоянию	
FDP_ROL.2.2	Расширенный откат к исходному состоянию	
FIA_AFL.1.1	Обработка отказов аутентификации	
FIA_AFL.1.2	Обработка отказов аутентификации	
FMT_MSA.1.1	Управление учетными записями пользователей. Возможность модифицировать атрибуты безопасности только уполномоченным пользователям	
FMT_MSA.3.1	Инициализация статических атрибутов	
FMT_MSA.3.2	Инициализация статических атрибутов	
FMT_MTD.1	Управление учетными записями пользователей	
FMT_SMF.1.1	Управление учетными записями пользователей (спецификация функций управления)	
FMT_SMR.1.1	Назначение минимально необходимых прав и привилегий	
FMT_SMR.1.2	Назначение минимально необходимых прав и привилегий	
FTA_SSL.1.1	Блокирование сеанса доступа пользователя при неактивности	
FTA_SSL.1.2	Блокирование сеанса доступа пользователя при неактивности	

4.1.2 ПО поддерживает для каждого пользователя:

– ролевой доступ к объектам и операциям согласно должностной инструкции;

– ролевой контроль доступа к объектам основываясь на атрибутах безопасности пользователя (идентификатор и роль пользователя), атрибутах безопасности объекта (идентификатор объекта, разрешения для объекта).

При попытке доступа на выполнение/изменение объекта, модуль прав доступа ПО разрешает либо запрещает доступ пользователю в соответствии с правами группы, к которой он принадлежит.

4.1.3 По умолчанию пользователь с ролью «Администратор» имеет возможность:

– выполнить откат к исходному состоянию;

– определить интервал времени до перехода в режим «только для чтения»;

– добавлять и удалять пользователей, редактировать учетные записи пользователей и свойства объекта.

4.1.4 После трех неуспешных попыток авторизации с вводом неверного пароля пользователя:

– доступ пользователю запрещается, возможность повторной авторизации блокируется на установленное разработчиком время;

– выполняется запись в журнале событий ИБ терминала.

4.1.5 Для разблокирования интерактивного сеанса после определяемого разработчиком интервала времени необходима повторная успешная аутентификация пользователя.

4.1.6 При загрузке терминала проверяются контрольные суммы исполняемых файлов для контроля целостности системы. Система самодиагностики терминала непрерывно выполняет проверку целостности исполняемой программы и данных (стартовая и циклическая (не реже одного раза в сутки)).

4.1.7 При загрузке и в процессе функционирования терминала выполняется самодиагностика аппаратных модулей. При сбоях в работе модуля устанавливается неисправность.

4.1.8 Для каждой учетной записи пользователя обеспечивается ограничение числа параллельных сеансов доступа.

4.1.9 Пользователь с ролью отличной от «Администратора» не имеет доступа к внесению изменений в права доступа пользователей терминала, а также добавлению, удалению пользователей и смене пароля иных пользователей.

Разграничение прав доступа пользователей по умолчанию представлено в таблице 2.

4.2 ПО терминала (программа E3_SW91)

4.2.1 При загрузке и в процессе функционирования терминала система самодиагностики проверяет контрольные суммы исполняемых файлов для контроля целостности ПО терминала. Терминал выдает неисправности «Проверка контроля целостности архива файлов прошивки прошла не успешно» и «Проверка контроля целостности архива конфигурации прошла не успешно» для привлечения внимания пользователя и выполнения возврата к резервным копиям ПО по установленным производителем правилам. Просмотр

неисправностей в журнале событий ИБ по умолчанию доступен только пользователю с ролью Администратор»: в программе Smart Monitor пункт меню  –> **Загрузить журнал событий информационной безопасности терминала**.

4.2.2 Также система самодиагностики при загрузке и в процессе функционирования терминала выполняет диагностику аппаратных модулей. При сбоях в работе модуля устанавливается неисправность «Неисправность системных блоков». Просмотр наименования неисправности доступен через меню терминала: **Диагностика** –> **Состояние блоков**.

Примечание – Более подробная информация о возможных неисправностях терминала изложена в инструкции по устранению неисправностей ЭКРА.650320.001 И1.

4.2.3 ПО поддерживает для каждого пользователя:

– ролевой доступ к объектам и операциям согласно должностной инструкции;

– ролевой контроль доступа к объектам основываясь на атрибутах безопасности пользователя (идентификатор и роль пользователя), атрибутах безопасности объекта (идентификатор объекта, разрешения для объекта).

При попытке доступа на выполнение/изменение объекта модуль прав доступа ПО разрешает, либо запрещает доступ пользователю, в соответствии с правами группы, к которой он принадлежит.

4.2.4 В терминале реализовано ограничение числа параллельных активных сеансов доступа (настраиваемый параметр) для каждой учетной записи пользователя при подключении через программу Smart Monitor (см. рисунок 20).

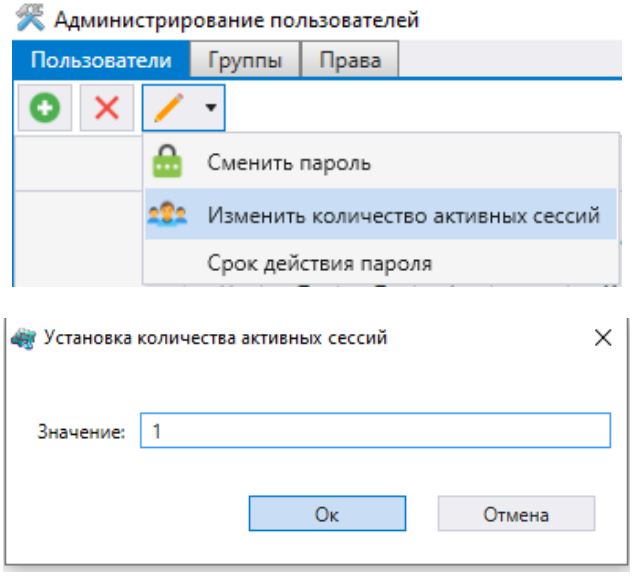


Рисунок 20

При подключении к терминалу под учетной записью пользователя, которая уже авторизована, производится проверка разрешенных параллельных соединений. В случае превышения этого числа доступ блокируется (рисунок 21), при этом фиксируется событие в

журнале ИБ «Попытка превышения количества активных сессий пользователя. Параллельные сеансы запрещены».

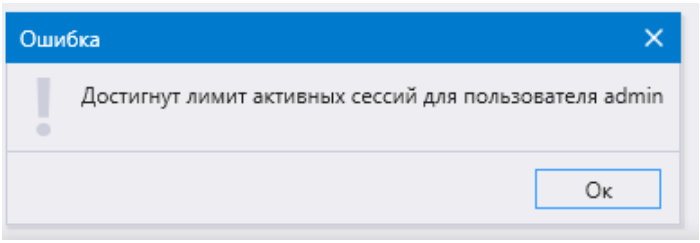
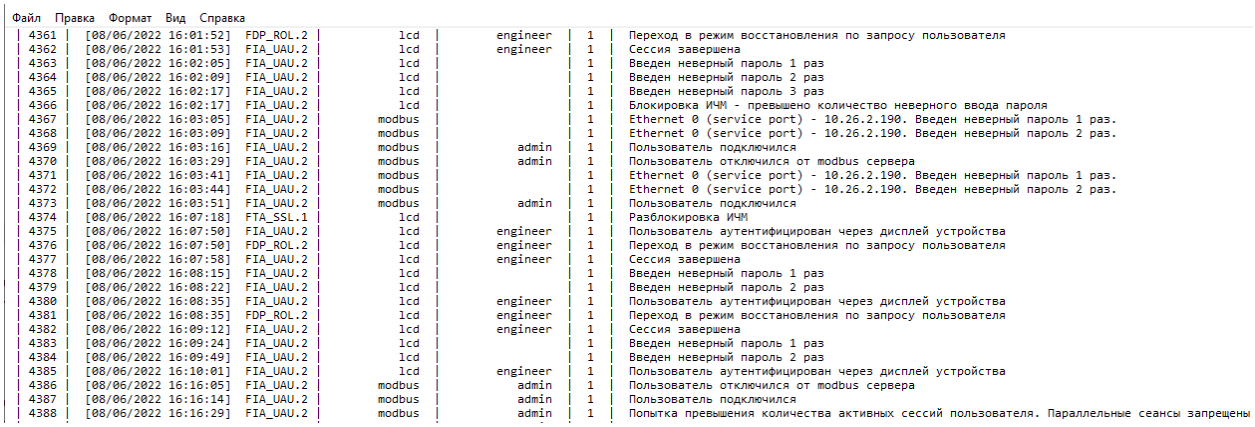


Рисунок 21

Пример содержания журнала событий ИБ приведен на рисунке 22.



Файл Правка Формат Вид Справка

4361	[08/06/2022 16:01:52]	FDP_ROL.2	lcd	engineer	1	Переход в режим восстановления по запросу пользователя
4362	[08/06/2022 16:01:53]	FIA_UAU.2	lcd	engineer	1	Сессия завершена
4363	[08/06/2022 16:02:05]	FIA_UAU.2	lcd		1	Введен неверный пароль 1 раз
4364	[08/06/2022 16:02:09]	FIA_UAU.2	lcd		1	Введен неверный пароль 2 раз
4365	[08/06/2022 16:02:17]	FIA_UAU.2	lcd		1	Введен неверный пароль 3 раз
4366	[08/06/2022 16:02:17]	FIA_UAU.2	lcd		1	Блокировка ИЧМ - превышено количество неверного ввода пароля
4367	[08/06/2022 16:03:05]	FIA_UAU.2	modbus		1	Ethernet 0 (service port) - 10.26.2.190. Введен неверный пароль 1 раз.
4368	[08/06/2022 16:03:09]	FIA_UAU.2	modbus		1	Ethernet 0 (service port) - 10.26.2.190. Введен неверный пароль 2 раз.
4369	[08/06/2022 16:03:16]	FIA_UAU.2	modbus	admin	1	Пользователь подключился
4370	[08/06/2022 16:03:29]	FIA_UAU.2	modbus	admin	1	Пользователь отключился от modbus сервера
4371	[08/06/2022 16:03:41]	FIA_UAU.2	modbus		1	Ethernet 0 (service port) - 10.26.2.190. Введен неверный пароль 1 раз.
4372	[08/06/2022 16:03:44]	FIA_UAU.2	modbus		1	Ethernet 0 (service port) - 10.26.2.190. Введен неверный пароль 2 раз.
4373	[08/06/2022 16:03:51]	FIA_UAU.2	modbus	admin	1	Пользователь подключился
4374	[08/06/2022 16:07:18]	FTA_SSL.1	lcd		1	Разблокировка ИЧМ
4375	[08/06/2022 16:07:50]	FIA_UAU.2	lcd	engineer	1	Пользователь аутентифицирован через дисплей устройства
4376	[08/06/2022 16:07:50]	FDP_ROL.2	lcd	engineer	1	Переход в режим восстановления по запросу пользователя
4377	[08/06/2022 16:07:58]	FIA_UAU.2	lcd	engineer	1	Сессия завершена
4378	[08/06/2022 16:08:15]	FIA_UAU.2	lcd		1	Введен неверный пароль 1 раз
4379	[08/06/2022 16:08:22]	FIA_UAU.2	lcd		1	Введен неверный пароль 2 раз
4380	[08/06/2022 16:08:35]	FIA_UAU.2	lcd	engineer	1	Пользователь аутентифицирован через дисплей устройства
4381	[08/06/2022 16:08:35]	FDP_ROL.2	lcd	engineer	1	Переход в режим восстановления по запросу пользователя
4382	[08/06/2022 16:09:12]	FIA_UAU.2	lcd	engineer	1	Сессия завершена
4383	[08/06/2022 16:09:24]	FIA_UAU.2	lcd		1	Введен неверный пароль 1 раз
4384	[08/06/2022 16:09:49]	FIA_UAU.2	lcd		1	Введен неверный пароль 2 раз
4385	[08/06/2022 16:10:01]	FIA_UAU.2	lcd	engineer	1	Пользователь аутентифицирован через дисплей устройства
4386	[08/06/2022 16:16:05]	FIA_UAU.2	modbus	admin	1	Пользователь отключился от modbus сервера
4387	[08/06/2022 16:16:14]	FIA_UAU.2	modbus	admin	1	Пользователь подключился
4388	[08/06/2022 16:16:29]	FIA_UAU.2	modbus	admin	1	Попытка превышения количества активных сессий пользователя. Параллельные сеансы запрещены

Рисунок 22

4.2.5 Окно центра администрирования пользователей вызывается из главного окна через кнопку 

–> **Администрирование пользователей** на панели инструментов.

Окно (рисунок 23, поз. 1) состоит из трех вкладок:

– Пользователи;

– Группы;

– Права.

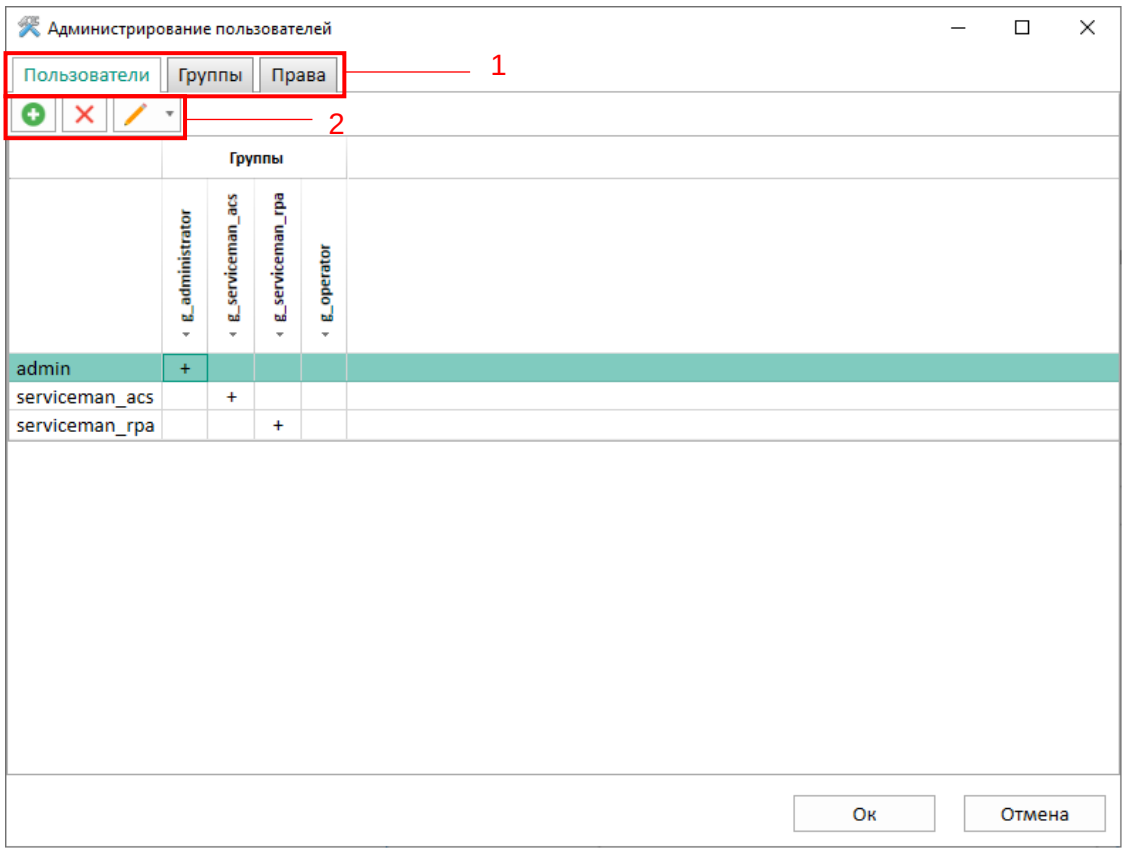


Рисунок 23

4.2.5.1 На вкладке **Пользователи** осуществляются операции над учетными записями пользователей. Операции доступны через панель инструментов (см. рисунок 23, поз. 2).

Изменение, удаление и смена пароля пользователя доступны только после выбора соответствующего пользователя из списка.

Логин пользователей может состоять из символов «A – Z», «a – z», «А – Я», «а – я», «0 – 9». Максимальное количество символов логина: 16. Пароль может состоять только из символов «0 – 9». Максимальное количество символов пароля: 16.

Добавление нового пользователя осуществляется нажатием кнопки . При этом в отображаемом окне (см. рисунок 24) необходимо ввести данные нового пользователя.

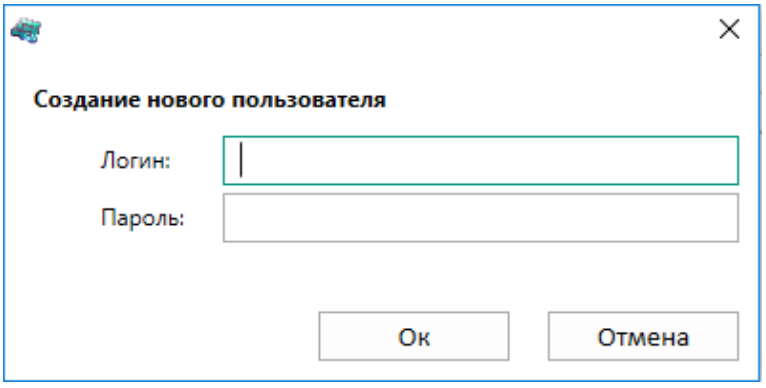


Рисунок 24

Удаление пользователя осуществляется нажатием кнопки  . При этом появится диалоговое окно подтверждение удаления.

4.2.5.2 На вкладке **Группы** (см. рисунок 25) осуществляются операции над группами. Название группы можно редактировать, нажав левой кнопкой мыши на название.

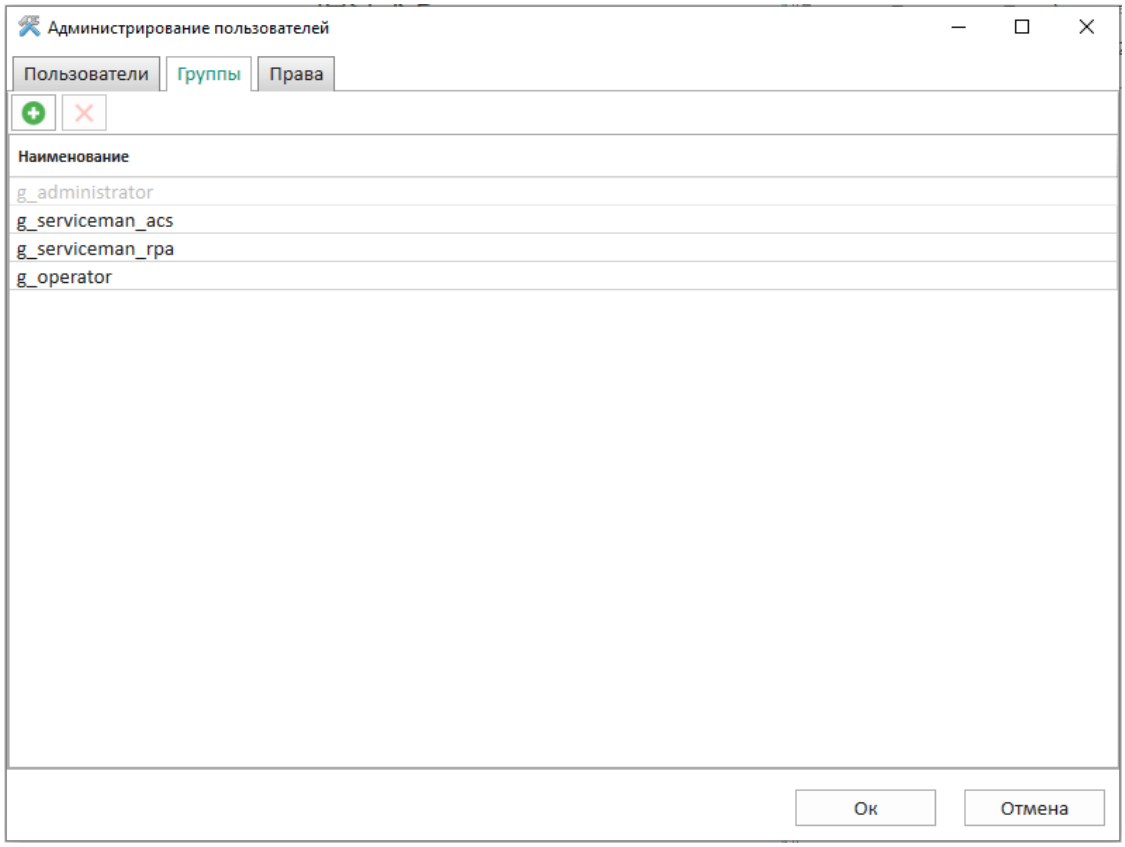


Рисунок 25

Добавление новой группы осуществляется нажатием кнопки  . При этом в отображаемом окне (см. рисунок 26) необходимо ввести имя для новой группы. После добавления новая группа появится во вкладках **Пользователи** и **Права** в столбце **Группы**.

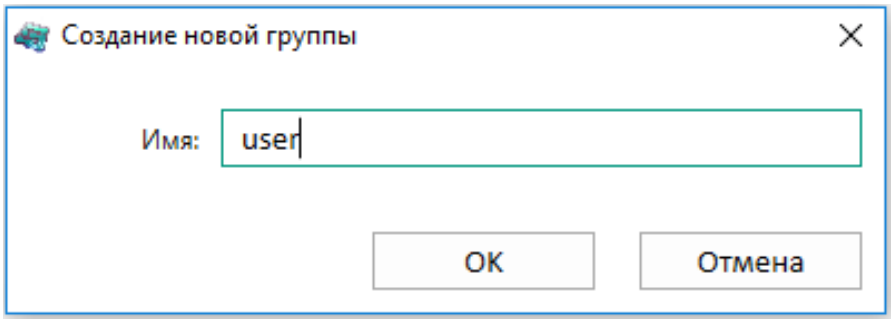


Рисунок 26

Удаление группы осуществляется нажатием кнопки  после исключения всех пользователей из группы. При этом появится диалоговое окно подтверждение удаления.

4.2.5.3 Вкладка **Права** (см. рисунок 27) предназначена для задания разрешений и прав доступа группам.

Управление разрешением осуществляется установкой/снятием плюсов «+» в ячейке таблицы прав в столбце требуемой группы.

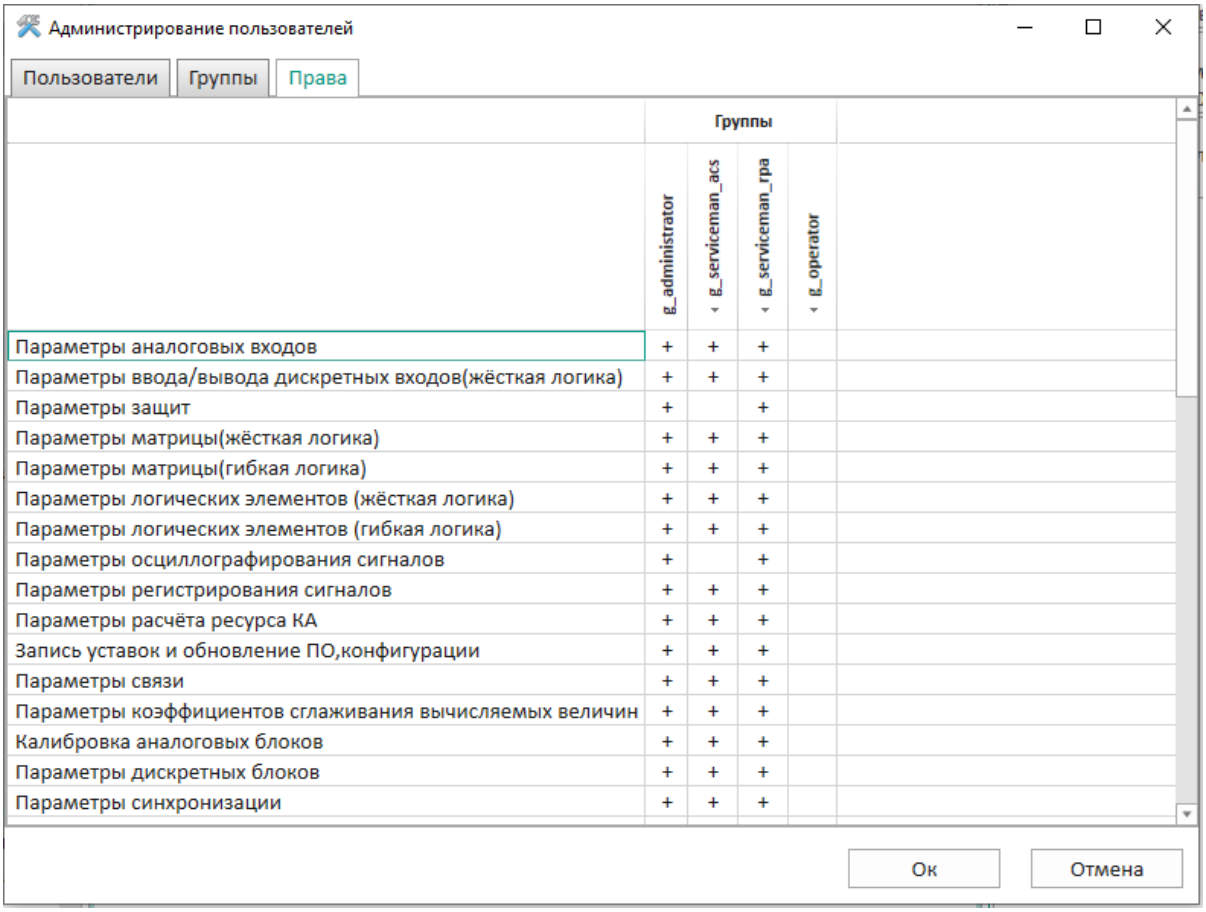


Рисунок 27

4.2.6 Программа Smart Monitor позволяет удалять/изменять роли и учетные записи пользователей, заданные по умолчанию, разграничивать права пользователей, таким образом, что каждый пользователь, используя имя и пароль для входа в систему, получал доступ только к той информации, на работу с которой он имеет право.

Разграничение прав доступа пользователей терминала настраивается в соответствии с их должностными обязанностями и предназначено для предотвращения несанкционированных действий пользователя по управлению коммутационным оборудованием, изменению режимов и настроек терминала. Запрещается наделение одной учетной записи пользователя несколькими ролями. С целью обеспечения безопасной эксплуатации необходимо настроить права доступа группам пользователей в соответствии с требованиями по разграничению прав доступа:

1) пользователю с ролью «Администратор» настраиваются права для создания/редактирования/удаления ролей и учетных записей пользователей, изменения паролей, чтения событий в журнале событий безопасности с запретом возможности обновления си-

стемного ПО и внесения изменений в параметры настройки (уставки) и алгоритмы функционирования устройства;

2) пользователю с ролью «Инженер» настраиваются права для обновления системного программного обеспечения и внесения изменений в параметры настройки (уставки) и алгоритмы функционирования устройства, чтения журнала событий безопасности с запретом возможности назначения и(или) изменения паролей сторонних учетных записей.

Разграничение прав доступа пользователей с ролью «Администратор» и «Инженер» представлено в таблице 5.

Таблица 5 – Разграничение прав доступа пользователей

Права	Роли	
	Администратор	Инженер
Администрирование пользователей	Выполнение	–
Журнал событий ИБ	Чтение	Чтение
Включение и отключение портов связи	–	Выполнение
Настройка параметров дисплея (время бездействия, время блокировки ИЧМ и т.п.)	–	Изменение
Сброс на заводские настройки	–	Выполнение
Перевод терминала в сервисный режим (режим восстановления, обновления)	–	Выполнение
Уставки функций РЗА	–	Чтение / Изменение
Настройка регистратора аварийных событий (осциллограф, регистратор)	–	Чтение / Изменение
Перевод терминала в тестовый режим	–	Выполнение
Системные настройки (IP-адрес, скорость работы последовательного порта, системное время, язык меню)	–	Чтение / Изменение
Режим (места) управления: местное/ дистанционное	–	Выполнение
Переключение групп уставок	–	Выполнение
Управление мнемосхемой	–	Выполнение
Сброс сигнализации	–	Выполнение
Файлы-осциллограмм, cid-файл, отчеты по уставкам и протоколам связи	–	Чтение
Замена конфигурации и обновление ПО	–	Выполнение / Изменение

Разграничение доступа пользователей терминала доступно только пользователю с ролью «Администратор» и только после авторизации пользователя. Форма авторизации пользователя приведена на рисунке 5.

Пользователь с ролью отличной от «Администратора» не имеет доступа к внесению изменений в права доступа пользователей терминала, а также добавлению, удалению пользователей или смене пароля других пользователей (рисунок 28).

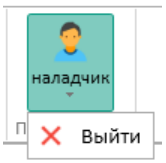


Рисунок 28

Настройка и изменение прав доступа пользователей осуществляется нажатием на кнопку 

(кнопка 

на панели инструментов –> **Администрирование пользователей**) (рисунок 9). Применение измененных или новых параметров не требует перезагрузки терминала.

Назначение прав управления функциями в логической схеме для групп пользователей производится с помощью матриц прав доступа (рисунок 11).

Если у пользователей используются пароли по умолчанию, то в журнале событий ИБ фиксируется сообщение об использовании паролей по умолчанию до того момента, пока пароль по умолчанию не будет изменен.

5 Ограничение программной среды

5.1 Общие сведения

5.1.1 Ограничение программной среды позволяет реализовать меры защиты согласно таблице 6.

Таблица 6 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
ОПС.0	Регламентация правил и процедур ограничения программной среды	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
ОПС.2	Управление установкой (инсталляцией) компонентов ПО	
ОЦЛ.1	Контроль целостности ПО	

5.1.2 В процессе проверки файлов на уникальные идентификаторы (контрольные суммы) реализуется мера защиты УКФ.3: Установка (инсталляция) только разрешенного к использованию ПО.

5.1.3 Установка (инсталляция) в информационной системе ПО и(или) его компонентов доступна только пользователю с ролью «Администратор».

5.1.4 Обеспечивается контроль целостности (состояния) запускаемых компонентов ПО в соответствии с ОЦЛ.1.

5.1.5 В автоматизированной системе обеспечивается регистрация событий, связанных с контролем состояния и обновлением запускаемых компонентов ПО.

5.2 ПО терминала (программа E3_SW91)

5.2.1 ПО устанавливается с помощью программы Smart Monitor. При установке ПО проверяются файлы на уникальные идентификаторы (контрольные суммы), подтверждающие, что они разрешены к установке. В случае несовпадения контрольных сумм файлов ПО выдается сообщение об ошибке (рисунок 29).

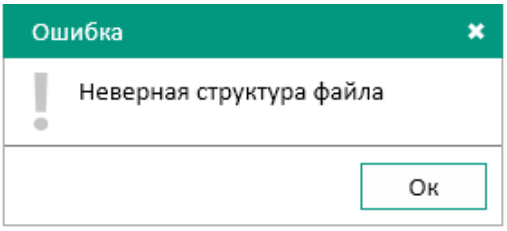


Рисунок 29

5.2.2 Установка ПО в терминал с помощью программы Smart Monitor по умолчанию доступна только пользователю с ролью «Администратор».

6 Регистрация событий безопасности

6.1 Общие сведения

6.1.1 Регистрация событий безопасности позволяет реализовать меры защиты согласно таблице 7.

Таблица 7 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
АУД.0	Регламентация правил и процедур аудита безопасности	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	
АУД.4	Регистрация событий безопасности	
АУД.6	Защита информации о событиях безопасности	
FAU_GEN.1.1	Генерация данных аудита	ГОСТ Р ИСО/ МЭК 15408-2-2013
FAU_GEN.1.2		
FAU_GEN.2.1	Ассоциация идентификатора пользователя	
FAU_SAR.1.1	Просмотр журналов аудита	
FAU_SAR.1.2		
FAU_STG.1.1	Защищенное хранение журнала аудита	
FAU_STG.1.2		
FAU_STG.4.1	Предотвращение потери данных аудита	

6.1.2 Записи в журнале событий ИБ:

– генерируются для событий, подвергаемых аудиту;

– содержат дату и время возникновения события, подвергаемого аудиту;

– содержат уникальный номер, присвоение уникальных номеров производится по сквозному принципу;

– содержат тип событий, потенциально подвергаемых аудиту.

6.1.3 Ассоциируется каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором события, либо с процессом (в случаях, когда невозможно зафиксировать идентификатор пользователя).

6.1.4 Программа Smart Monitor позволяет пользователю с ролью «Администратор» читать журналы событий ИБ с терминала. Журналы событий ИБ понятны и отражают суть возникшего события.

6.1.5 Интерфейс пользователя поддерживает:

– запрет удаления записей в журнале событий ИБ;

– предотвращение несанкционированной модификации хранимых записей аудита в журнале событий ИБ;

– запись поверх самых старых хранимых записей аудита при переполнении журнала событий ИБ.

6.2 ПО терминала (программа E3_SW91)

6.2.1 Связанные с безопасностью операции пользователей в терминале регистрируются в качестве событий безопасности в энергонезависимую память терминала. Каждое событие, потенциально подвергаемое аудиту, ассоциируется с идентификатором пользователя, который был инициатором событий, либо с процессом (в случаях, когда невозможно зафиксировать идентификатор пользователя). Перечень регистрируемых событий приведен в таблице 8.

Таблица 8 – Регистрируемые события действий пользователя

Событие в терминале	Регистрируемые данные
Загрузка (останов), перезагрузка устройства	1) Время и дата события; 2) Тип события; 3) Объект события (программный модуль, в котором произошло событие); 4) Имя пользователя, совершившего событие, либо процесса, подлежащего регистрации (в случаях, когда возможно зафиксировать имя пользователя); 5) Результат события (1 – успешно, 0 – неуспешно); 6) Действие; 7) Протокол подключения; 8) Порт подключения; 9) Источник события / идентификатор (серийный номер) СМНИ
Все случаи использования механизма аутентификации пользователя	
Все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя	
Блокировка возможности авторизации пользователя при достижении установленного количества неверного ввода пароля	
Попытки разблокирования интерактивного сеанса	
Изменение прав доступа группы пользователей	
Изменение настройки по умолчанию разрешающих правил	
Запросы на выполнение операций на объекте, на который распространяется ролевая политика доступа	
Изменения конфигурации терминала: логики работы, настроек, уставок	
Создание, редактирование, удаление ролей пользователей, изменение паролей пользователей	
Изменения настроек синхронизации времени, текущей даты/времени, изменение часового пояса	
Результат проверки контрольных сумм файлов ПО, конфигурации терминала и архива прав доступа пользователей	
Журнал событий ИБ (скачивание, начало циклической перезаписи)	
Подключение к сервисному порту	
Операции по переходу в сервисный режим и сбросу терминала до заводских настроек	
Попытки превышения активных сессий пользователя	
Обновление ПО и конфигурации терминала	
Использование СМНИ (при обновлении ПО и конфигурации, скачивании файлов)	
Активность канала связи, шторм по Ethernet	
Включение и отключение портов связи	

6.2.2 Для предотвращения потери данных аудита событий безопасности, при переполнении журнала событий ИБ, предусмотрена функция цикличной перезаписи самых старых записей новыми записями.

6.2.3 События безопасности имеют уникальный номер. Присвоение уникальных номеров производится по сквозному принципу.

6.2.4 Записи журнала событий ИБ сортируются по номерам и датам создания.

6.2.5 При сбросе ПО терминала до заводских настроек записи журнала событий ИБ сохраняются.

6.3 Программа Smart Monitor

6.3.1 Операции, связанные с безопасностью пользователей в терминале, выполненные в программе Smart Monitor, регистрируются в качестве событий безопасности в энергонезависимую память АРМ. Каждое событие, потенциально подвергаемое аудиту, ассоциируется с идентификатором пользователя, который был инициатором события, либо с процессом (в случаях, когда невозможно зафиксировать идентификатор пользователя). Перечень регистрируемых событий приведен в таблице 9.

Таблица 9 – Регистрируемые события действий пользователя

Событие в терминале	Регистрируемые данные
Все случаи использования механизма аутентификации пользователя	1) Время и дата события; 2) Данные пользователя: логин пользователей; 3) Действие
Все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя	
Изменение конфигурации терминала: логики работы, настроек, уставок	
Переключение группы уставок	
Изменение файла конфигурации	
Изменение файла ПО (core.arh, sh.rtb)	
Изменение прав доступа группы пользователей	
Создание, редактирование, удаление ролей пользователей, изменение паролей пользователей	
Журнал событий ИБ (скачивание, начало циклической перезаписи)	

6.3.2 Для предотвращения потери данных журнала событий безопасности, при достижении максимального размера журнала событий ИБ, предусмотрена функция цикличной перезаписи самых старых записей новыми записями.

6.3.3 Содержимое журнала событий ИБ может просматривать только пользователь с ролью «Администратор» через программу Smart Monitor, для этого необходимо подключиться к терминалу, авторизоваться под пользователем с ролью «Администратор» и скачать журнал событий ИБ: пункт меню  –> **Выгрузить журнал событий информационной безопасности с устройства** (см. рисунок 30).

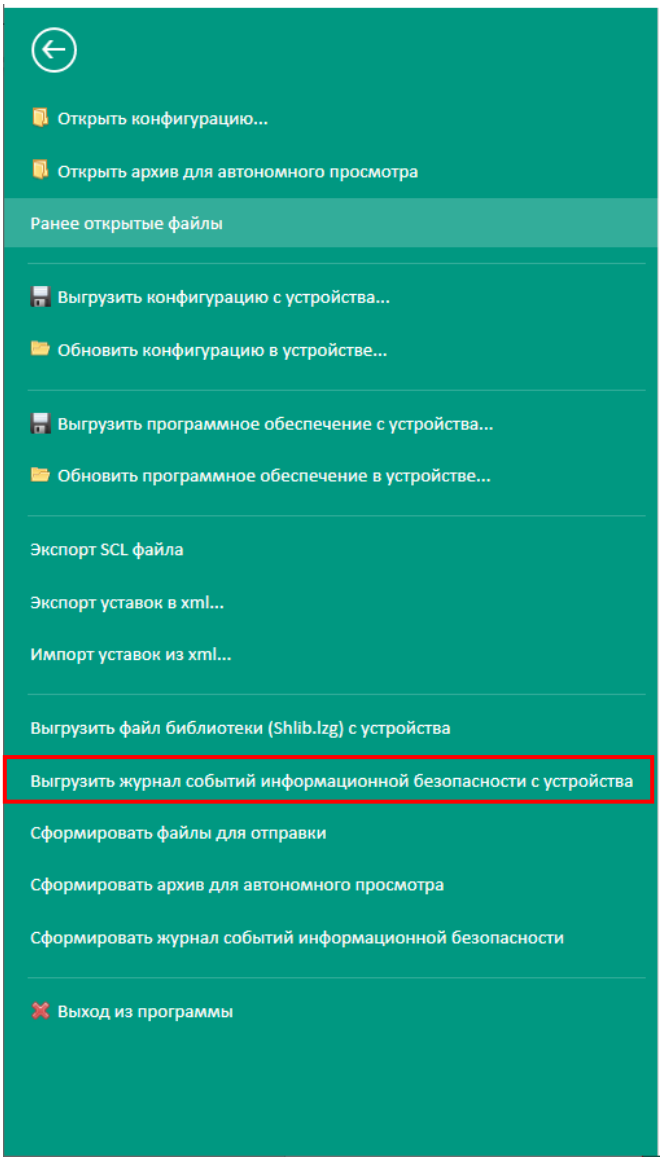


Рисунок 30

Далее необходимо выбрать место для сохранения архивированного файла и нажать кнопку **Сохранить** (см. рисунок 31, поз. 1).

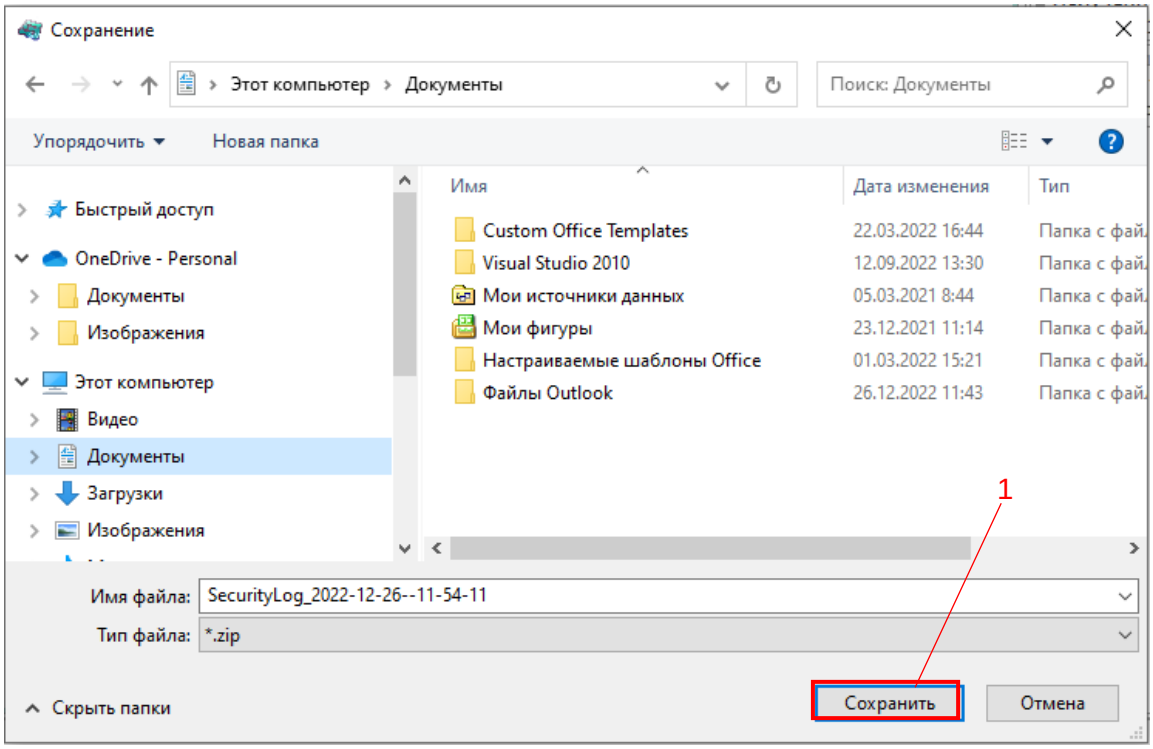


Рисунок 31

При успешном формировании файла появится информационное окно (см. рисунок 32).

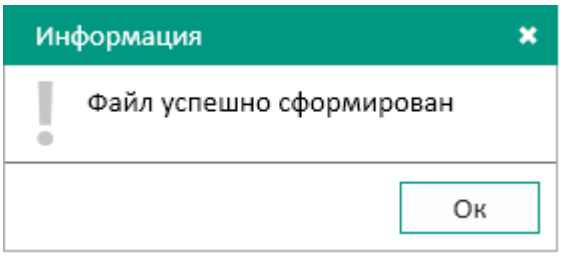


Рисунок 32

Далее следует разархивировать сохраненный файл.

7 Контроль использования СМНИ

7.1 Общие сведения

7.1.1 В процессе контроля использования интерфейсов ввода (вывода) информации на СМНИ реализуются меры защиты согласно таблице 10.

Таблица 10 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
ЗНИ.0	Регламентация правил и процедур защиты СМНИ	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на СМНИ	

7.1.2 Реализован контроль использования интерфейсов ввода (вывода) информации на СМНИ.

7.2 ПО терминала (программа E3_SW91)

7.2.1 В программе E3_SW91 осуществляется контроль ввода (вывода) информации на СМНИ.

Контроль ввода (вывода) информации на СМНИ предусматривает:

– определение типов СМНИ, ввод (вывод) информации на которые подлежит контролю;

– определение категорий пользователей, которым предоставлены полномочия по вводу (выводу) информации на СМНИ;

– запрет действий по вводу (выводу) информации для пользователей, не имеющих полномочий на ввод (вывод) информации на СМНИ, и на СМНИ, на которые запрещен ввод (вывод информации);

– регистрацию действий пользователей и событий по вводу (выводу) информации на СМНИ.

Программа E3_SW91 определяет тип СМНИ. СМНИ имеет файловую систему FAT32.

Возможность обновления ПО терминала с СМНИ разрешена только после авторизации пользователя с соответствующими правами доступа (см. рисунок 1).

Действия пользователей и события по вводу (выводу) информации на СМНИ регистрируются в журнале событий ИБ.

8 Обеспечение целостности

8.1 Общие сведения

8.1.1 Пломбирование терминалов производится специальной этикеткой, разрушающейся при вскрытии устройства, расположенной на задней плите терминала. Эксплуатационному персоналу необходимо выполнять процедуры контроля состояния пломб, чтобы убедиться, что пломба не нарушена.

8.1.2 Базовое ПО обеспечивает непрерывный самоконтроль, контроль достоверности входной информации, а также выполнение процедур контроля технических средств, что в свою очередь реализует меры защиты согласно таблице 11.

Таблица 11 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
ОЦЛ.1	Контроль целостности ПО	
FDP_SDI.2.1	Контроль целостности информации (Мониторинг целостности хранимых данных и предпринимаемые действия)	ГОСТ Р ИСО/ МЭК 15408-2-2013
FDP_SDI.2.2	Контроль целостности информации (Мониторинг целостности хранимых данных и предпринимаемые действия)	
FMT_MTD.1	Управление учетными записями пользователей	

8.2 ПО терминала (программа E3_SW91)

8.2.1 Обеспечивается контроль целостности ПО при запуске и в процессе функционирования терминала.

Для каждого объекта и всех объектов в целом создаются контрольные суммы, которые проверяются при загрузке и в процессе функционирования терминала.

При наличии ошибки контрольных сумм для каждого объекта реализована возможность загрузки данных по умолчанию (эталонных), что осуществляется путем отката к предыдущей или заводской версии ПО и конфигурации. Способы возврата к резервным копиям ПО приведены в 14.2 и 14.3. Терминал выдает неисправности «Проверка контроля целостности архива файлов прошивки прошла не успешно» и «Проверка контроля целостности архива конфигурации прошла не успешно» для привлечения внимания пользователя и выполнения возврата к резервным копиям ПО по установленным производителем правилам. Просмотр неисправностей в журнале событий ИБ по умолчанию доступен только пользователю с ролью «Администратор»: пункт меню  –> **Загрузить журнал событий информационной безопасности терминала**.

8.3 Программа Smart Monitor

8.3.1 Контроль целостности компонентов ПО осуществляется по контрольным суммам в процессе загрузки и циклически, в процессе функционирования терминала.

8.3.2 При нарушении целостности исполняемого ПО выполнение программы завершается выдачей в АСУ ТП сигнала «Неисправность» (за исключением случаев отсутствия технической возможности отправки сигнала, обусловленной сбоем ПО).

8.3.3 Результаты проверок целостности исполняемой программы или данных фиксируются в журнале событий ИБ.

9 Обеспечение доступности

9.1 Общие сведения

9.1.1 Резервное копирование данных системы позволяет реализовать меры защиты согласно таблице 12.

Таблица 12 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
ОДТ.0	Регламентация правил и процедур обеспечения доступности	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
ОДТ.5	Обеспечение возможности восстановления информации	
ОДТ.6	Обеспечение возможности восстановления ПО при нештатных ситуациях	

9.1.2 Обеспечена возможность восстановления информации (ПО и конфигурации) из резервных копий.

Восстановление информации из резервных копий предусматривает:

– обеспечение требуемых условий непрерывности функционирования информационной системы и доступности информации;

– восстановление информации (ПО и конфигурации) из резервных копий;

– регистрацию событий, связанных с восстановлением информации из резервных копий.

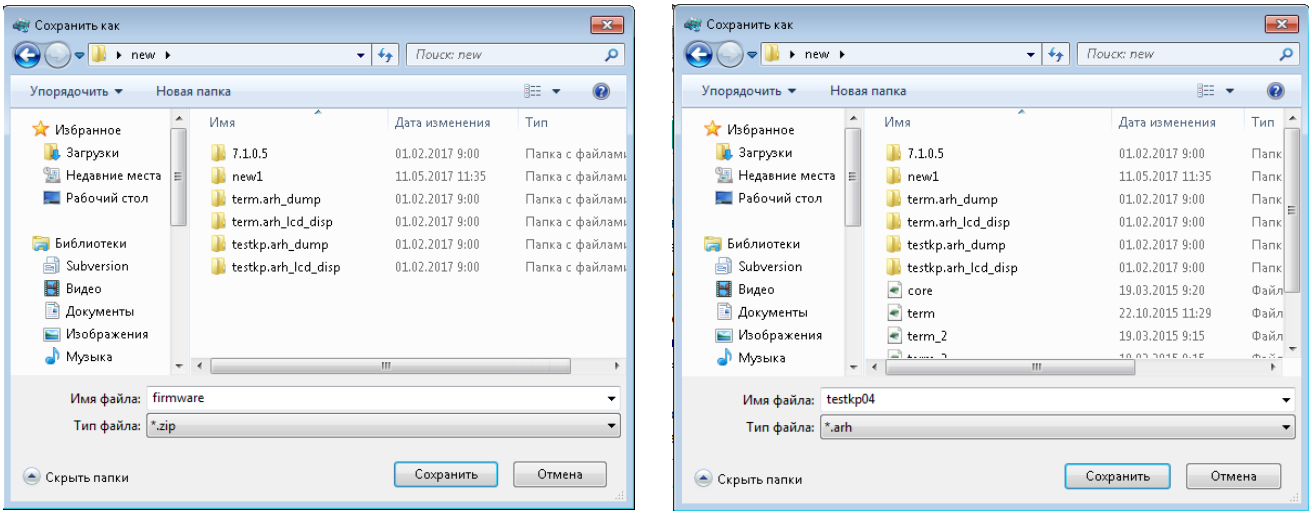
9.2 ПО терминала (программа E3_SW91)

При несоответствии контрольных сумм компонентов ПО терминал переходит в режим неисправности для привлечения внимания пользователя и выполнения возврата к резервным копиям ПО по установленным производителем правилам. Терминал выдает неисправности в журнале событий «Проверка контроля целостности архива файлов прошивки прошла не успешно» и «Проверка контроля целостности архива конфигурации прошла не успешно». Просмотр неисправностей в журнале событий ИБ по умолчанию доступен только пользователю с ролью «Администратор»: пункт меню  –> **Загрузить журнал событий информационной безопасности терминала**. Способы возврата к резервным копиям ПО приведены в 14.2 и 14.3.

9.3 Программа Smart Monitor

9.3.1 Под процессом резервного копирования ПО терминала следует понимать создание резервных копий файлов ПО терминала и конфигурации с помощью комплекса программ Smart Monitor. Эти файлы должны быть сохранены на компьютере эксплуатационного персонала. При необходимости файлы могут быть повторно загружены в терминал, реализуя, таким образом, процедуру восстановления.

Создание резервных копий файлов ПО терминала и конфигурации происходит в пункте меню –> **Сохранить программное обеспечение …** и в пункте меню –> **Сохранить конфигурацию …** (рисунок 33).



а) сохранение ПО б) сохранение конфигурации

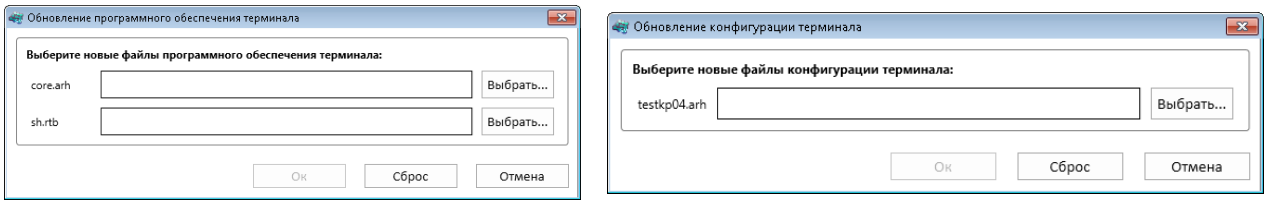
Рисунок 33

Для поддержания актуальности данных содержащихся в резервных копиях необходимо определить периодичность резервного копирования данных терминала. Периодичность создания резервных копий данных определяется в рамках текущей эксплуатации.

Рекомендуется производить резервное копирование, каждый раз, перед внесением изменений в ПО или конфигурацию терминала.

9.3.2 Для загрузки и отладки прикладного ПО, а также диагностики терминала предусмотрен комплекс программ EKRASMS-SP, поставляемый комплектно с терминалом.

Загрузка прикладного ПО происходит в пункте меню –> **Обновить программное обеспечение…** и пункт меню –> **Обновить конфигурацию…** (рисунок 34).



а) обновление ПО б) обновление конфигурации

Рисунок 34

9.3.3 Диагностика и отладка прикладного ПО происходит в «дереве» проекта в пункте **Сервисное меню** и **Тесты**.

Для поддержания актуальности данных, содержащихся в резервных копиях, необходимо определить периодичность резервного копирования данных терминала. Периодичность создания резервных копий данных определяется в рамках текущей эксплуатации.

Рекомендуется производить резервное копирование каждый раз перед внесением изменений в ПО или конфигурацию терминала.

9.3.4 Восстановление ПО и конфигурации из резервных копий предусматривает:

– обеспечение требуемых условий непрерывности функционирования информационной системы и доступности информации;

– восстановление информации (ПО и конфигурации) из резервных копий;

– регистрацию событий, связанных с восстановлением информации из резервных копий.

9.3.5 Инструкция по установке обновлений ПО приведена в документе ЭКРА.650321.014 И «Инструкция по замене и восстановлению конфигурации и программного обеспечения».

10 Защита технических средств и систем

10.1 Общие сведения

10.1.1 Защита технических средств и систем позволяет реализовать меры защиты согласно таблице 13.

Таблица 13 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
ЗТС.2	Организация контролируемой зоны	
ЗТС.3	Управление физическим доступом	
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	

10.1.2 Мера защиты реализуется исключением бесконтрольного нахождения посторонних лиц на территории контролируемой зоны и иными организационно-техническими мерами, реализуемыми на объекте. Физическое ограничение доступа терминалов выполняется размещением терминалов в запираемых шкафах с датчиками открытия дверей и(или) помещениях с сигнализацией (аппаратных), ограничивающих доступ к ним посторонних лиц.

10.1.3 Запрет использования аутентификационной информации по умолчанию.

10.1.4 Прокладка кабельных сетей таким образом, чтобы максимально ограничить несанкционированный доступ к ним.

10.1.5 Физическая охрана объекта в соответствии с требованиями законодательства РФ.

10.1.6 Контроль и управление физическим доступом к терминалу, а также в помещения и сооружения, в которых они установлены, предотвращающие несанкционированный физический доступ к ним.

10.1.7 Разграничение прав доступа пользователей терминала настраивается в соответствии с их должностными обязанностями и предназначено для предотвращения несанкционированных действий пользователя по управлению коммутационным оборудованием, изменению режимов и настроек терминала.

10.2 Программа Smart Monitor

10.2.1 Настройка разграничения доступа пользователей терминала доступна только пользователю с ролью «Администратор» и только после авторизации пользователя. Форма авторизации представлена на рисунке 5.

11 Защита информационной (автоматизированной) системы и ее компонентов

11.1 Общие сведения

11.1.1 Защита информационной системы (автоматизированной) системы и ее компонентов позволяет реализовать меры защит согласно таблице 14.

Таблица 14 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями (описание приведено в п.2)	
ЗИС.34	Защита от угроз отказа в обслуживании	

11.1.2 Внешние меры защиты в составе среды функционирования ОО для защиты от угроз отказа в обслуживании приведены в разделе 15.

11.1.3 Условием повышенной информационной нагрузки является реализация атаки, направленной на нарушение функционирования или прекращение функционирования цифрового оборудования и систем за счет создания повышенной информационной нагрузки на него. При условии повышенной информационной нагрузки внутренний регистратор событий терминала не содержит записей о событиях неисправности и изменениях состояния логических сигналов, которые не регламентированы конфигурацией терминала.

11.2 ПО терминала (программа E3_SW91)

В условиях повышенной информационной нагрузки на порты связи терминал не отвечает на запросы подключения от программы Smart Monitor. После прекращения повышенной информационной нагрузки терминал обрабатывает запросы на подключения от программы Smart Monitor в штатном режиме. При этом внутренний регистратор событий терминала не содержит записей о событиях неисправности и изменениях состояния логических сигналов, которые не регламентированы конфигурацией терминала (пункт меню «дерева» проекта **Инструменты** –> **Регистратор событий** (рисунок 35)).

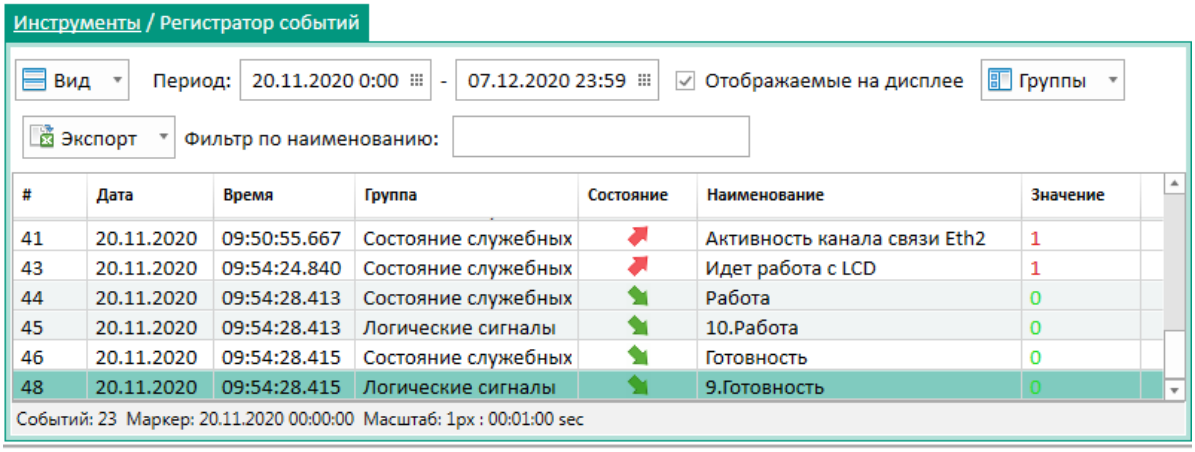


Рисунок 35

При этом фиксируется запись «Шторм по Ethernet» в журнале событий ИБ терминала. После прекращения повышенной информационной нагрузки на порты связи терминала, терминал начинает обрабатывать запросы на подключение программы Smart Monitor.

12 Управление обновлениями ПО

12.1 Общие сведения

12.1.1 Управление обновлениями внутреннего ПО терминала позволяет реализовать меры защиты согласно таблице 15.

Таблица 15 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
ОПО.0	Регламентация правил и процедур управления обновлениями ПО	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
ОПО.1	Получение обновлений ПО от доверенного источника	
ОПО.2	Контроль целостности обновлений ПО	
ОПО.4	Установка обновлений ПО	

12.1.2 Обновление ПО терминала производится через сервисный порт (сервисный порт не интегрируется в АСУ и локальные сети).

12.1.3 Перед обновлением ПО запускается процедура проверки контрольных сумм. При несоответствии контрольных сумм компонентов ПО, обновление не применяется.

12.1.4 При успешном обновлении ПО терминала, фиксируется отсутствие сообщений об ошибках в разделе «Диагностика».

12.2 ПО терминала (программа E3_SW91)

ВНИМАНИЕ: ПЕРЕД ВЫПОЛНЕНИЕМ РАБОТ ПО ЗАМЕНЕ КОНФИГУРАЦИИ И ПО НЕОБХОДИМО ВЫВЕСТИ ТЕРМИНАЛ ИЗ РАБОТЫ!

12.2.1 Возможность получения обновления внутреннего ПО терминала осуществляется способами, гарантирующими его целостность. Обновление внутреннего ПО терминала производится самостоятельно эксплуатационным персоналом либо специалистами по наладке и сервису производителя.

12.2.2 Информация о поставочных версиях ПО с описанием истории изменений в обновлениях ПО приводится на официальном сайте изготовителя, расположенном по адресу https://soft.ekra.ru/smssp/ru/main/. Пользователи получают обновления ПО на доверенном носителе после официального запроса в адрес предприятия-изготовителя.

Перед применением обновления ПО пользователю необходимо выполнить расчет значений контрольных сумм файлов полученного ПО и сверить их со значениями эталонных контрольных сумм файлов ПО, предоставленных совместно с ПО и формуляре.

Расчет значений контрольных сумм файлов ПО возможно произвести в программе Total Commander. На правой панели программы Total Commander выделить файлы ПО, контрольные суммы которых требуется получить, и выбрать: пункт меню **Файлы** –> **Посчитать CRC-суммы (CRC32, MD5, SHA)…** (рисунок 36).

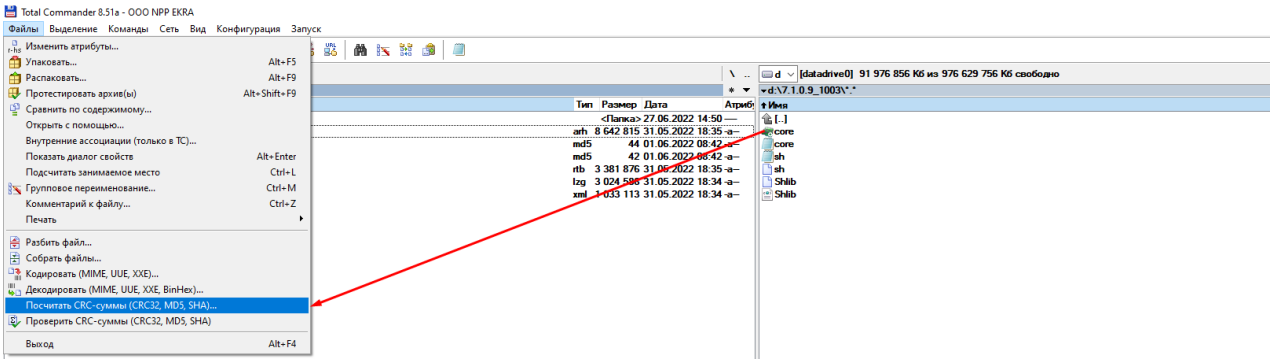


Рисунок 36

В появившемся окне **Создание файлов контрольных сумм (CRC)** (рисунок 37) установить флажок **Для каждого файла создать отдельный CRC-файл,** если он не установлен, и выбрать необходимый **Тип контрольной суммы**. Типы контрольных сумм, среди которых требуется выбрать необходимый тип при создании файлов контрольных сумм, представлены в таблице 16.

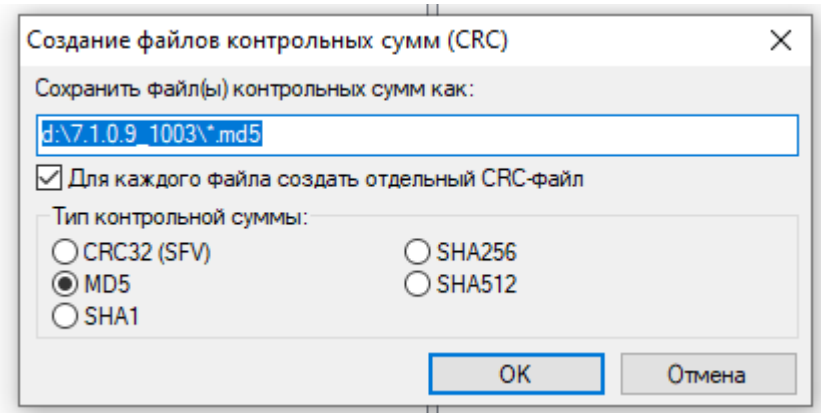


Рисунок 37

Таблица 16 – Тип контрольной суммы

Тип контрольной суммы	Описание
CRC32 (SFV)	Создает контрольные суммы CRC32, записывая их в файл в формате SFV. Самый быстрый метод, но с минимальной надежностью
MD5	Создает контрольные суммы MD5. Они более надежны, чем контрольные суммы CRC32, поскольку длиннее и используют более сложный алгоритм. Для записи контрольных сумм используется нижний регистр
SHA1	Создает контрольные суммы SHA1, еще более криптостойкие, чем MD5
SHA256	Создает контрольные суммы SHA2 с выбранной битовой длиной (например, SHA256 будет иметь длину в 256 битов)
SHA512	SHA512 будет иметь длину в 512 битов

Сравнить расчет значений контрольных сумм файлов полученного ПО со значениями эталонных контрольных сумм файлов ПО, предоставленных совместно с ПО (рисунок 38).

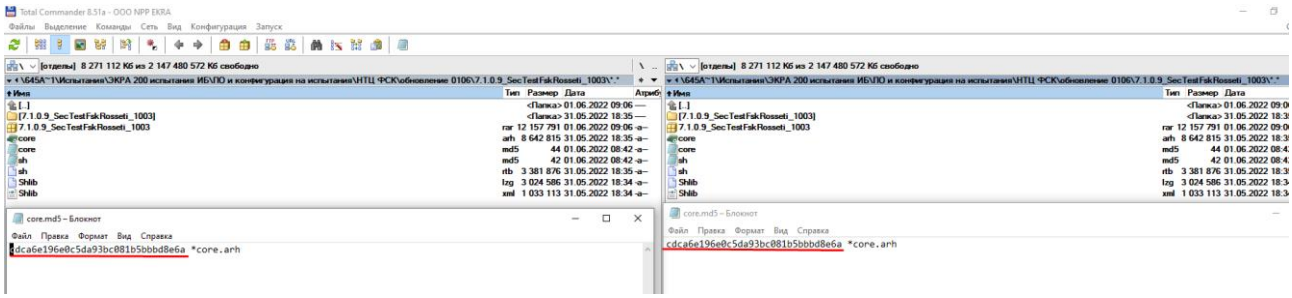


Рисунок 38

При несовпадении рассчитанных значений контрольных сумм с полученными от производителя значениями, установка обновления не осуществляется, требуется обратиться в службу технической поддержки.

12.2.3 Обновление внутреннего ПО терминала производится с помощью программы Smart Monitor (пункт меню –> **Обновить программное обеспечение…** и пункт меню –> **Обновить конфигурацию…**(рисунок 34)) и представляет собой замену файлов базового и прикладного ПО.

12.2.4 Обновления и необходимая документация инструментального ПО EKRASMS-SP размещается на сайте https://soft.ekra.ru/smssp/ru/main/. Эксплуатационный персонал (при необходимости) самостоятельно скачивает и устанавливает обновления прикладного ПО EKRASMS-SP.

12.2.5 При скачивании ПО EKRASMS-SP требуется:

– проверить подлинность ПО EKRASMS-SP посредством электронной подписи. Если подлинность ПО EKRASMS-SP не подтверждена, необходимо обратиться в службу технической поддержки предприятия-изготовителя;

– перед установкой ПО EKRASMS-SP сравнить контрольные суммы полученного ПО EKRASMS-SP с эталонным контрольными суммами, предоставляемыми совместно с ПО EKRASMS-SP. При расхождении контрольных сумм с эталонными значениями необходимо обратиться в службу поддержки предприятия-изготовителя;

– произвести установку ПО EKRASMS-SP.

13 Обеспечение действий в нештатных ситуациях

13.1 Общие сведения

13.1.1 Регламентация правил и процедур обеспечения действий в нештатных ситуациях позволяет реализовать меры защиты согласно таблице 17.

Таблица 17 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
ДНС.1	Разработка плана действий в нештатных ситуациях	
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций	
ДНС.4	Резервирование ПО, технических средств, каналов связи на случай возникновения нештатных ситуаций	
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	

13.1.2 Меры включают в себя возможность восстановления ПО при возникновении нештатных ситуаций.

13.1.3 Для обеспечения возможности восстановления ПО в автоматизированной системе должны быть приняты соответствующие планы по действиям персонала при возникновении нештатных ситуаций.

13.1.4 При возникновении нештатных ситуаций пользователь с соответствующими правами доступа может произвести откат на предыдущие (заводские) версии ПО и конфигурации терминала в пункте меню  –> **Обновить программное обеспечение…** и в пункте меню  –> **Обновить конфигурацию…**(рисунок 34), загрузив предыдущие (заводские) версии ПО и конфигурации терминала.

13.1.5 Возможность восстановления ПО, при возникновении нештатных ситуаций предусматривает:

– восстановление ПО из резервных копий (дистрибутивов) ПО;

– возврат автоматизированной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей автоматизированной системы;

– выполнение требований нормативных и организационно-распределительных документов, регламентирующих деятельность организации в области обеспечения ИБ;

– регулярное обновление ОС, прикладного ПО;

– управление установкой (инсталляцией) компонентов ПО, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов ПО;

– установку (инсталляцию) только разрешенного к использованию ПО и(или) его компонентов;

– анализ и оперативное реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации;

– периодический мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них в соответствии с порядком, установленным внутренними нормативными документами;

– управление идентификаторами (логинами пользователей), средствами аутентификации (паролями пользователей), учетными записями пользователей (включая своевременное создание, удаление и блокирование);

– контроль установки обновлений ПО;

– документирование информации (данных) об изменениях в конфигурации автоматизированной системы управления и ее системы защиты;

– обучение пользователей в части соблюдения правил обеспечения ИБ.

13.1.6 Правила и процедуры восстановления (в том числе планы по действиям персонала и порядок применения компенсирующих мер) отражаются в организационно-распорядительных документах.

13.2 ПО терминала (программа E3_SW91)

13.2.1 Выполнить восстановление или произвести откат на предыдущую (заводскую) версию ПО терминала при возникновении нештатных ситуаций может пользователь с соответствующими правами доступа в режиме «Восстановление ПО». Переход в режим «Восстановление ПО» производится через пункт меню **Сервисное меню** –> **Переход в режим восстановления** (рисунок 39). Для перехода в режим «Восстановления ПО» необходимо выбрать соответствующий пункт меню и перезагрузить терминал.

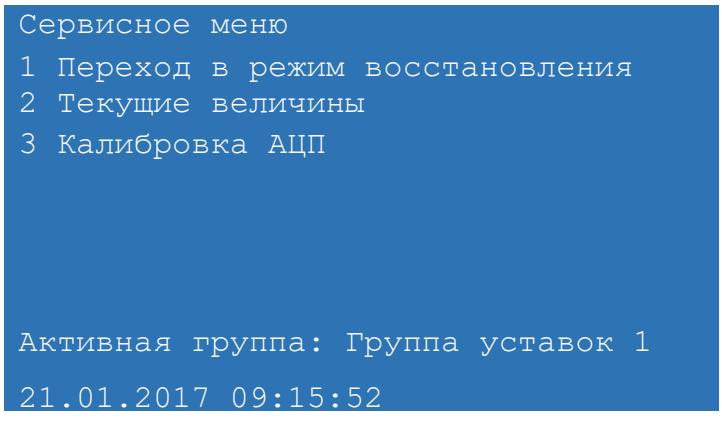


Рисунок 39

При попытке пользователя без соответствующих прав доступа перейти в режим «Восстановления ПО» на дисплее терминала выдается сообщение «Неправильный пароль».

13.2.2 Периодический мониторинг результатов регистрации событий безопасности возможен в журнале событий ИБ.

13.3 Программа Smart Monitor

13.3.1 Произвести откат на предыдущие (заводские) версии ПО и конфигурации терминала при возникновении нештатных ситуаций может пользователь с соответствующими правами доступа в пункте меню  –> **Обновить программное обеспечение…** и в пункте меню  –> **Обновить конфигурацию…**(рисунок 34), загрузив предыдущие (заводские) версии ПО и конфигурации терминала.

13.3.2 При обновлении ПО запускается процедура проверки контрольных сумм, при несоответствии контрольных сумм компонентов ПО, терминал переходит в режим неисправности для привлечения внимания пользователя и выполнения возврата к резервным копиям ПО по установленным производителем правилам.

14 Управления конфигурацией информационной (автоматизированной) системы

14.1 Общие сведения

14.1.1 Действия по внесению изменений в базовую конфигурацию ПО терминала и его подсистемы защиты информации регистрируются в журнале событий безопасности.

14.1.2 В терминале должен быть выделен сервисный интерфейс для обновления встроенного программного обеспечения.

14.1.3 Обновление встроенного программного обеспечения терминала по сервисному интерфейсу обеспечивается посредством специального программного обеспечения, входящего в комплект поставки.

14.1.4 Переключение сервисного интерфейса в режим готовности к выполнению команд по обновлению программного обеспечения осуществляется локально посредством вывода терминала из работы.

14.1.5 После обновления программного обеспечения терминала сохраняются роли и пароли пользователей.

14.1.6 При легитимном внесении изменений (обновлении) в ПО терминала контрольные суммы ПО пересчитываются, что в свою очередь реализует меры защиты согласно таблице 18.

Таблица 18 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
УКФ.3	Установка (инсталляция) только разрешенного к использованию ПО	
УКФ.4	Контроль действий по внесению изменений	
FDP_ROL.2.1	Расширенный откат к исходному состоянию	ГОСТ Р ИСО/ МЭК 15408-2-2013
FDP_ROL.2.2	Расширенный откат к исходному состоянию	
FPT_STM.1.1	Надежные метки времени	

14.1.7 ПО терминала позволяет выполнить откат к заводской конфигурации или предшествующей конфигурации.

14.1.8 ПО терминала способно изменять значение внутренних часов терминала.

14.2 ПО терминала (программа E3_SW91)

14.2.1 В режиме «Восстановление ПО» пользователь с ролью «Администратор» может выполнить восстановление или произвести откат на предыдущую (заводскую версию) ПО терминала. Переход в режим «Восстановление ПО» производится через пункт меню **Сервисное меню** –> **Переход в режим восстановления** (рисунок 39). Для перехода в ре-

жим «Восстановления ПО» необходимо выбрать соответствующий пункт меню и перезагрузить терминал.

14.2.2 При попытке пользователя с ролью отличной от «Администратора» перейти в режим «Восстановления ПО» на дисплее терминала выдается сообщение «Неправильный пароль».

14.2.3 При настройке текущего времени терминала в ручном режиме происходит синхронизация времени с внешним источником точного времени.

14.3 Программа Smart Monitor

14.3.1 Пользователь с ролью «Администратор» может произвести откат на предыдущие версии ПО и конфигурации терминала в пункте меню  –> **Обновить программное обеспечение…** и в пункте меню  –> **Обновить конфигурацию…**(рисунок 34), загрузив предыдущие (заводские) версии ПО и конфигурации терминала.

14.3.2 При попытке пользователя с ролью, отличной от «Администратора», произвести откат на предыдущие версии ПО и конфигурации выдается сообщение (рисунок 40).

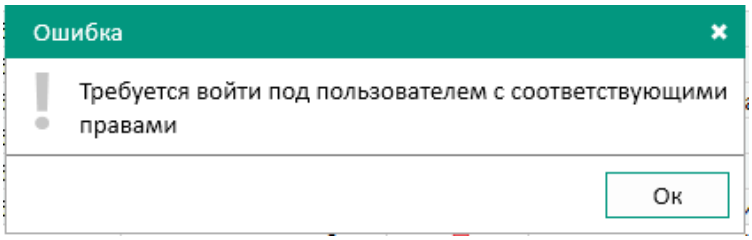


Рисунок 40

15 Описание действий по реализации функций безопасности среды функционирования ПО терминала

15.1 Для обеспечения выполнения функций безопасности в среде функционирования ПО выполняются требования безопасности информации среды функционирования ПО терминала, а именно:

– обеспечивается установка, конфигурирование и управление ПО терминала в соответствии с эксплуатационной документацией;

– персонал, ответственный за функционирование ПО терминала, обеспечивает функционирование ПО терминала, руководствуясь эксплуатационной документацией;

– обеспечивается совместимость компонентов ПО терминала с компонентами средств вычислительной техники автоматизированной системы;

– ограничивается доступ к критичным функциям ПО терминала посредством подключения через сервисный порт и ограничения доступа по белым спискам IP-адресов;

– персоналу, ответственному за функционирование ПО терминала, необходимо выполнять процедуры контроля состояния пломб, расположенных на задней плите терминала, чтобы убедиться, что пломба не нарушена;

– отключается возможность автоматического обновления операционной системы на АРМ пользователя и иных компонентов ПО среды функционирования. Установка обновлений ПО проводится администратором только после оценки всех сопутствующих рисков согласно методическим рекомендациям ФСТЭК России.

15.2 В процессе использования программы Smart Monitor, на АРМ пользователя реализовываются меры антивирусной защиты согласно таблице 19.

Таблица 19 – Перечень реализованных мер

Идентификатор	Описание требования	Нормативный документ
АВ3.0	Регламентация правил и процедур антивирусной защиты	Приказ ФСТЭК России № 239 от 25 декабря 2017 г.
АВ3.1	Реализация антивирусной защиты	
АВ3.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	

На АРМ пользователя используется антивирусное ПО, включенное в единый реестр российских программ для электронных вычислительных машин и баз данных.

Централизованный контроль, администрирование и управление средствами антивирусной защиты осуществляется при помощи консоли администрирования.

Антивирусная защита предназначена для защиты от вредоносного ПО, контроля целостности и контроля подключения внешних носителей на АРМ.

Антивирусная защита выполняет следующие функции:

– постоянная защита файловой системы АРМ от вирусов, троянских программ и червей;

– проверка заданных областей файловой системы серверов и АРМ от вирусов путем запуска проверок на них как вручную, так и по расписанию;

– мониторинг запуска, установки и изменения ПО и выдача соответствующих оповещений;

– централизованное получение и распространение баз вирусных описаний (сигнатур) последней (актуальной) версии;

– централизованное управление параметрами антивирусной защиты;

– фиксация событий безопасности в части антивирусной защиты;

– извещение пользователей и администраторов о событиях антивирусной защиты в соответствии с настройками системы оповещения;

– ограничение одновременных рабочих процессов для снижения ресурсопотребления;

– применение изменений политики и программных модулей без перезагрузки операционной системы защищаемых узлов;

– блокирование доступа к сетевым файловым ресурсам с не доверенных узлов (блокирование сессий);

– передачу событий ИБ из антивирусного ПО в систему сбора, анализа и корреляции событий информации (при наличии);

– мониторинг операций с файлами и папками в заданной области файловой системы (контроль целостности программной среды);

– защита файлов от шифрования;

– формирование отчетов по результатам работы комплекса;

– контроль использования интерфейсов ввода (вывода) информации на СМНИ;

– контроль подключения СМНИ.

15.3 Для защиты от внешних угроз безопасности информации должны применяться меры защиты в составе среды функционирования ПО терминала, такие как:

1) сегментирование локальной вычислительной сети АСУ. В этих целях предусматривается выделение следующих VLAN:

– сегмент нижнего уровня (полевой уровень);

– сегмент среднего уровня (уровень присоединения);

– сегмент верхнего уровня (подстанционный уровень);

– сегмент администрирования сетевых устройств (сегмент IT-менеджмента);

2) отключение неиспользуемых сервисов активного сетевого оборудования, предоставляющих возможность организации/возникновения DoS или других видов атак на сетевые ресурсы или ресурсы самого активного сетевого оборудования;

3) межсетевое экранирование с учетом транспортных адресов отправителя и получателя (сетевой адрес, порт) при осуществлении информационного взаимодействия с внешними автоматизированными и информационными системами или информационно-телекоммуникационными сетями;

4) обнаружение компьютерных атак, направленных на дестабилизацию работы активного сетевого оборудования, серверов и АРМ и другого оборудования АСУ, а также атак, использующих уязвимости компонентов АСУ;

5) использование сигнатурного и поведенческого метода распознавания сетевых атак и защиты от DoS и DDoS атак, сканирования портов.

16 Ограничения условий эксплуатации

Эксплуатация ПО терминала должна выполняться с соблюдением следующих условий:

– эксплуатация должна допускаться в пределах контролируемой (охраняемой) зоны объектов капитального строительства;

– дистанционный доступ и управление (технологическое обслуживание) должно быть обеспечено только с персонально-вычислительного компьютера с управляющим ПО, подключенного к сервисному порту;

– передача информации по беспроводным сетям связи должна быть исключена;

– безопасность операционной системы Windows для прикладного ПО должна быть обеспечена применением дополнительных мер (блокировка автоматических обновлений, отключение Wi-Fi и других неиспользуемых сетевых интерфейсов, межсетевое экранирование, антивирусное средство, резервное копирование данных);

– аутентификационная информация (пароли пользователей) по умолчанию должна быть заменена;

– разграничение прав доступа пользователей терминала должно настраиваться в соответствии с их должностными обязанностями для предотвращения несанкционированных действий пользователя по управлению коммутационным оборудованием, изменению режимов и настроек терминала.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докумен-те	Номер документа	Входящий номер сопрово-дительного документа и дата	Подпись	Дата
	изме-ненных	заме-ненных	новых	анну-лиро-ванных					
–					31				02.2023
1					60				12.2023