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 16/с.31

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).

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.

Настоящий документ актуален для версий прикладного ПО 4.0.0.24876 и выше, встроенного ПО 7.1.0.9.

СОДЕРЖАНИЕ

Обозначения и сокращения

cid – configured IED description (файл описания конфигурации устройства)

DDoS – distributed denial of service (распределенный отказ в обслуживании)

DoS – denial of service (отказ в обслуживании)

FTP – file transfer protocol (протокол передачи файлов по сети)

IP-адрес – internet protocol (протокол интернета)

IT – information technology (информационные технологии)

VLAN – virtual local area network (виртуальная локальная сеть)

Wi-Fi – wireless fidelity (беспроводная точность)

АРМ – автоматизированное рабочее место

АСУ – автоматизированная система управления

АСУ ТП – автоматизированная система управления технологическими процессами

ИБ – информационная безопасность

ИЧМ – интерфейс человек-машина

ООО НПП «ЭКРА» – общество с ограниченной ответственностью научно-производственное предприятие «ЭКРА»

ПО – программное обеспечение

РЗА – релейная защита и автоматика

РЭ – руководство по эксплуатации

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 программ:

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;

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;

г) предварительные требования:

– Internet Explorer 6 или более поздней версии, Mozilla Firefox, Google Chrome;

– Microsoft Office 2003 или более поздней версии.

3 Безопасная установка и настройка ПО

3.1 Идентификация и аутентификация

3.1.1 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).

3.1.2 Вводимая аутентификационная информация не передается по сети открытым текстом и хранится в памяти терминала в нечитаемом виде. Пользователю предоставляется только количество введенных символов во время выполнения аутентификации.

3.1.3 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 информационной безопасности.

3.1.4 В терминале авторизация пользователя осуществляется по паролю (рисунок 1).

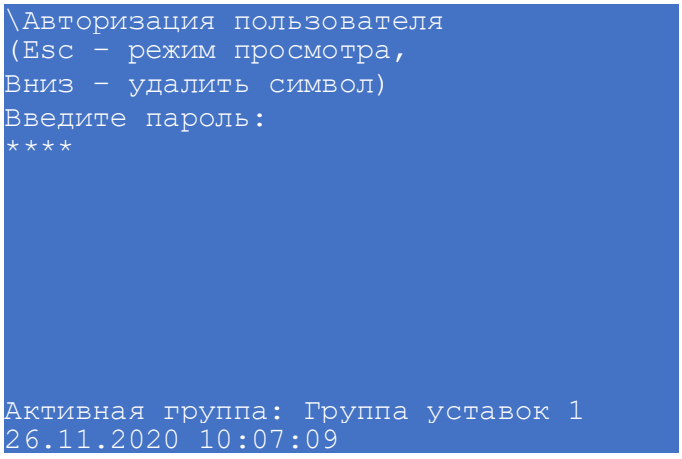


Рисунок 1

При вводе неверного пароля пользователю разрешается только просматривать параметры терминала.

3.1.5 В программе Smart Monitor авторизация пользователя происходит при нажатии на панели инструментов на кнопку 

. Форма авторизации пользователя приведена на рисунке 2.

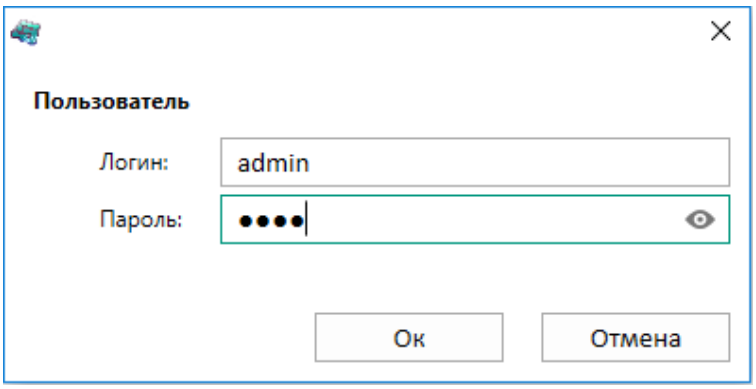


Рисунок 2

Для предотвращения несанкционированного доступа, пароли пользователей по умолчанию (см. таблицу 1) необходимо изменить на пароли сложностью не менее семи (цифровых) символов.

Таблица 1 – Данные пользователей

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

3.1.6 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.

3.1.7 При вводе правильных данных открывается рабочая область программы. При вводе неправильных данных выдается сообщение (рисунок 3).

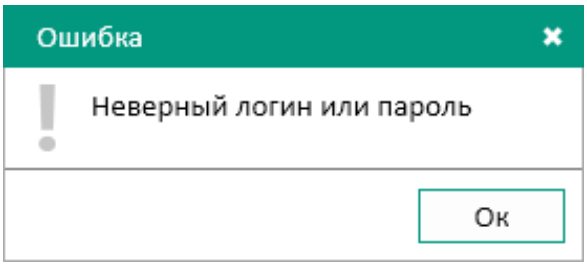


Рисунок 3

После трех неуспешных попыток авторизации с вводом неверного пароля пользователя блокируется возможность повторной авторизации на установленное разработчиком время и выводится сообщение о блокировке (рисунок 4).

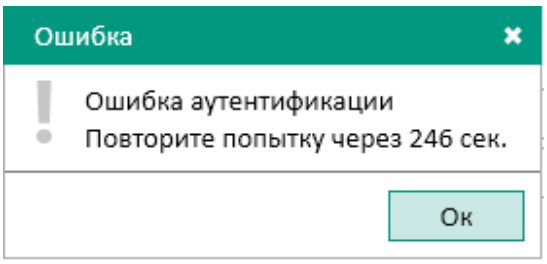


Рисунок 4

3.1.8 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 5).

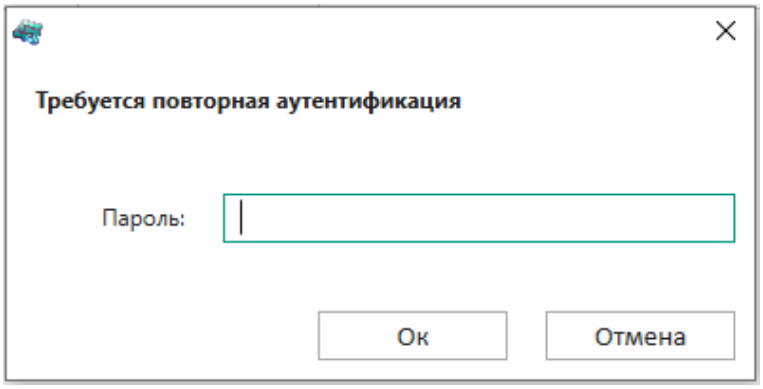


Рисунок 5

3.1.9 Настройка указанного времени происходит в пункте меню «дерева» проекта программы **Уставки** –> **Системные параметры** –> **Параметры терминала** (рисунок 6, поз.1) в поле **Дисплей** параметр **Тайм-аут доступа** (рисунок 6, поз. 2).

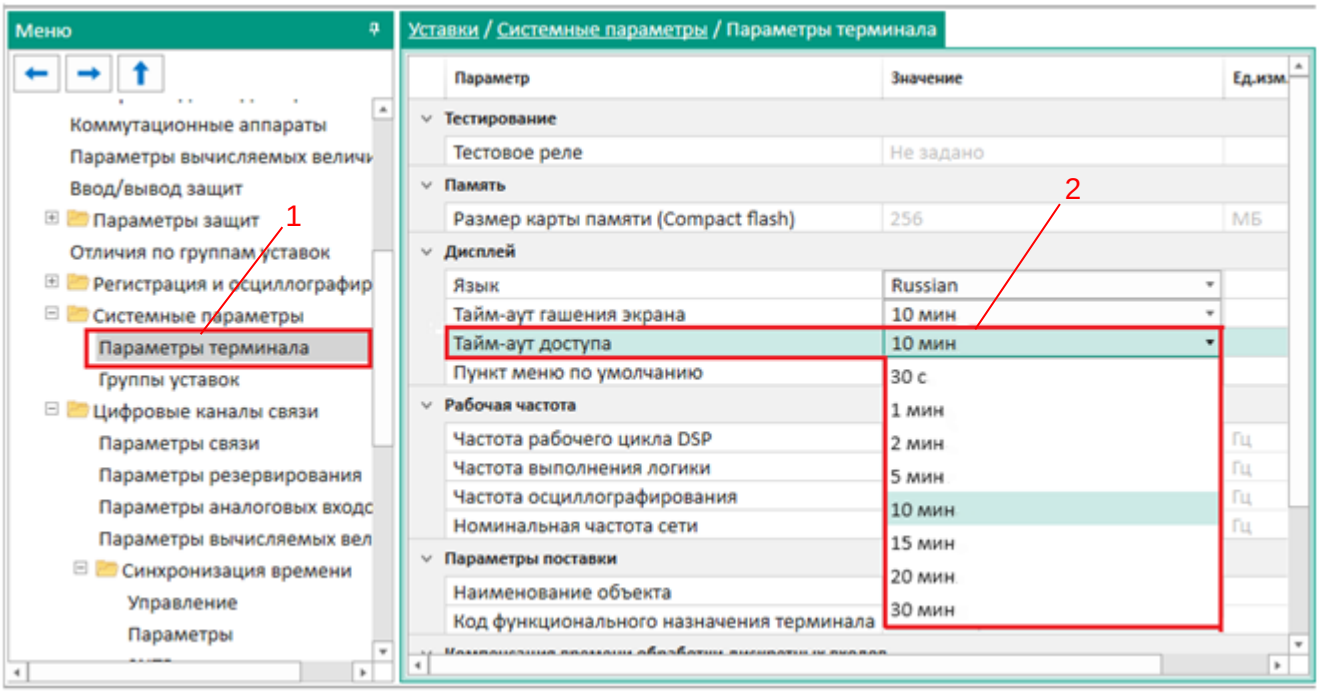


Рисунок 6

3.1.10 При возникновении технической или организационной необходимости (компрометация пароля, установка времени жизни пароля) реализована возможность изменения своего пароля пользователем (см. рисунок 7, поз.1).

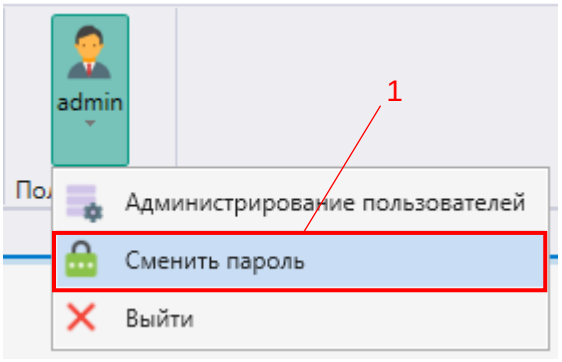


Рисунок 7

3.1.11 Изменение пароля возможно выполнить:

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

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

–> **Сменить пароль**).

3.1.12 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.

3.1.13 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 8).

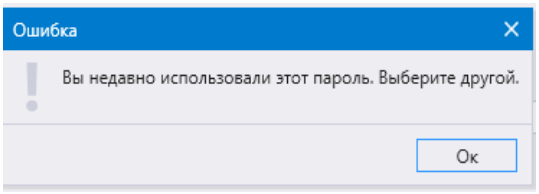


Рисунок 8

После успешной смены пароля пользователем требуется повторно авторизоваться в программе Smart Monitor (рисунок 9).

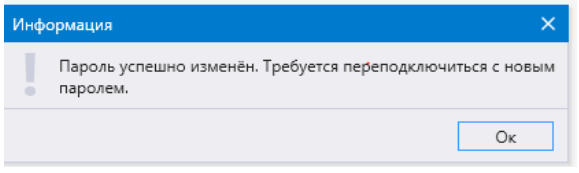


Рисунок 9

3.1.14 Пользователю с ролью «Администратор» предоставлена возможность задания срока действия (времени жизни) пароля для каждого пользователя в диапазоне от 0 до 999 дней (рисунок 10).

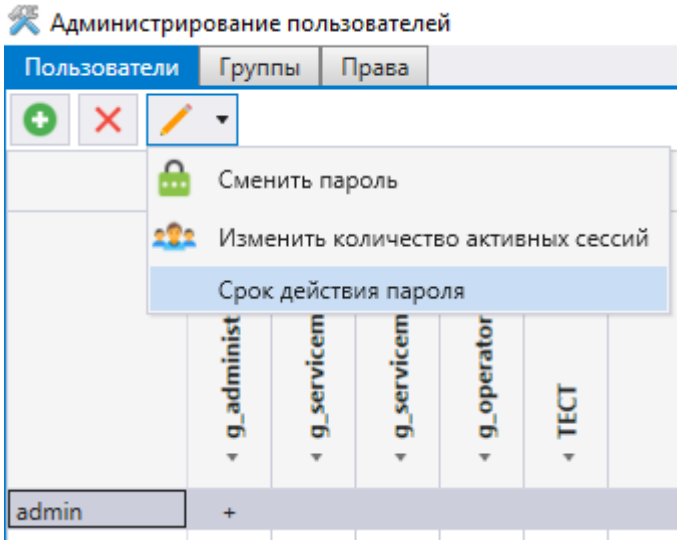


Рисунок 10

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 11).

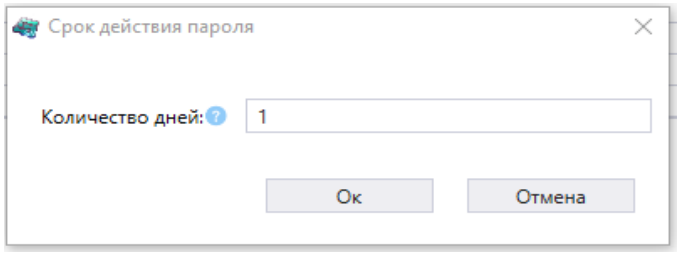


Рисунок 11

В программе Smart Monitor предусмотрена функция напоминания пользователю об истечении срока действия пароля, с предоставлением возможности заблаговременно сменить пароль (рисунок 12).

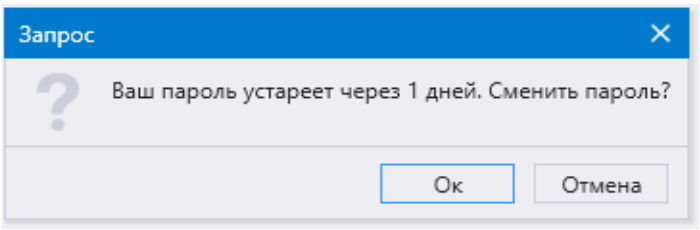


Рисунок 12

Счетчик ранее отсчитанного времени срока действия пароля сбрасывается только после смены пароля (рисунок 13).

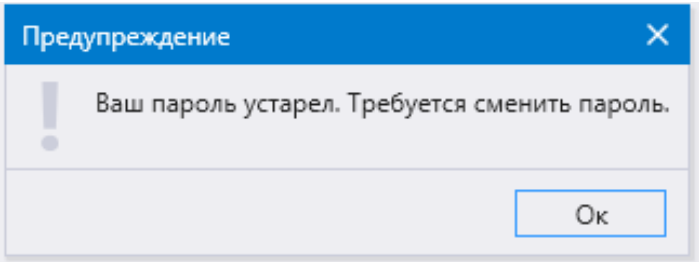


Рисунок 13

3.2 Управление доступом

3.2.1 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.

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.

Таблица 2 – Разграничение прав доступа пользователей по умолчанию

Права	Роли			
	Администратор	Наладчик РЗА	Наладчик АСУ	Оператор
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
Переключение групп уставок	Выполнение	Выполнение	Выполнение	Выполнение
Управление мнемосхемой	Выполнение	Выполнение	Выполнение	Выполнение

Права	Роли			
	Администратор	Наладчик РЗА	Наладчик АСУ	Оператор
Сброс сигнализации	Выполнение	Выполнение	Выполнение	Выполнение
Файлы-осциллограмм, cid-файл, отчеты по уставкам и протоколам связи	Чтение	Чтение	Чтение	Чтение
Замена конфигурации и обновление ПО	Выполнение / изменение	Выполнение / изменение	Выполнение / изменение	–
Запись по FTP (по умолчанию отключен)	Выполнение	–	–	–

3.2.2 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.

3.2.3 В терминале реализовано ограничение числа параллельных активных сеансов доступа (настраиваемый параметр) для каждой учетной записи пользователя при подключении через программу Smart Monitor (см. рисунок 14).

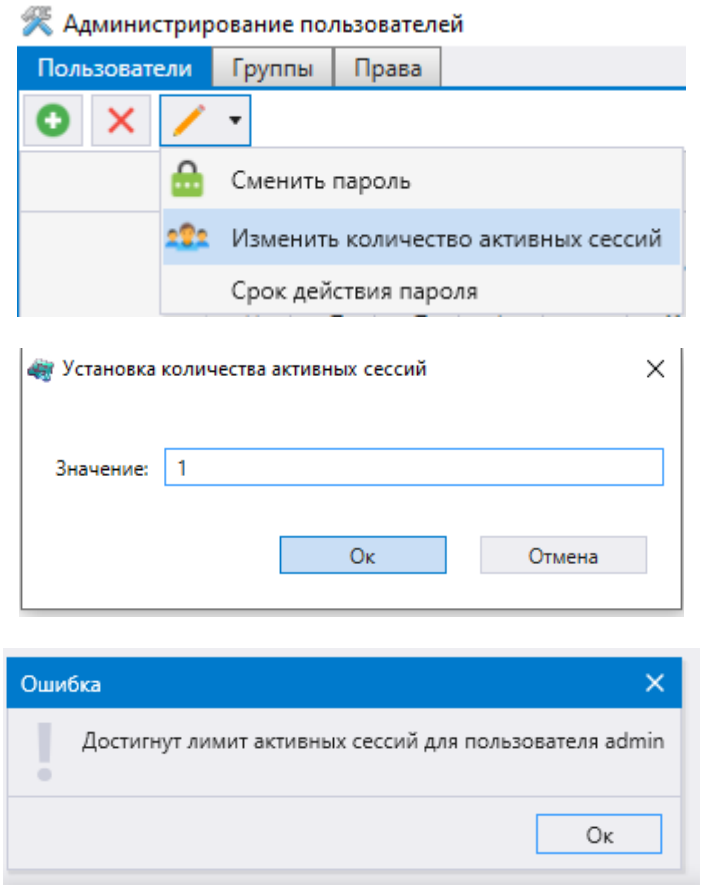


Рисунок 14

При подключении к терминалу под учетной записью пользователя, которая уже авторизована, производится проверка разрешенных параллельных соединений. В случае превышения этого числа доступ блокируется, при этом фиксируется событие в журнале ИБ «Попытка превышения количества активных сессий пользователя. Параллельные сеансы запрещены».

3.2.4 Окно центра администрирования пользователями вызывается из главного окна через кнопку 

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

Окно (рисунок 15) состоит из трех вкладок:

– Пользователи;

– Группы;

– Права.

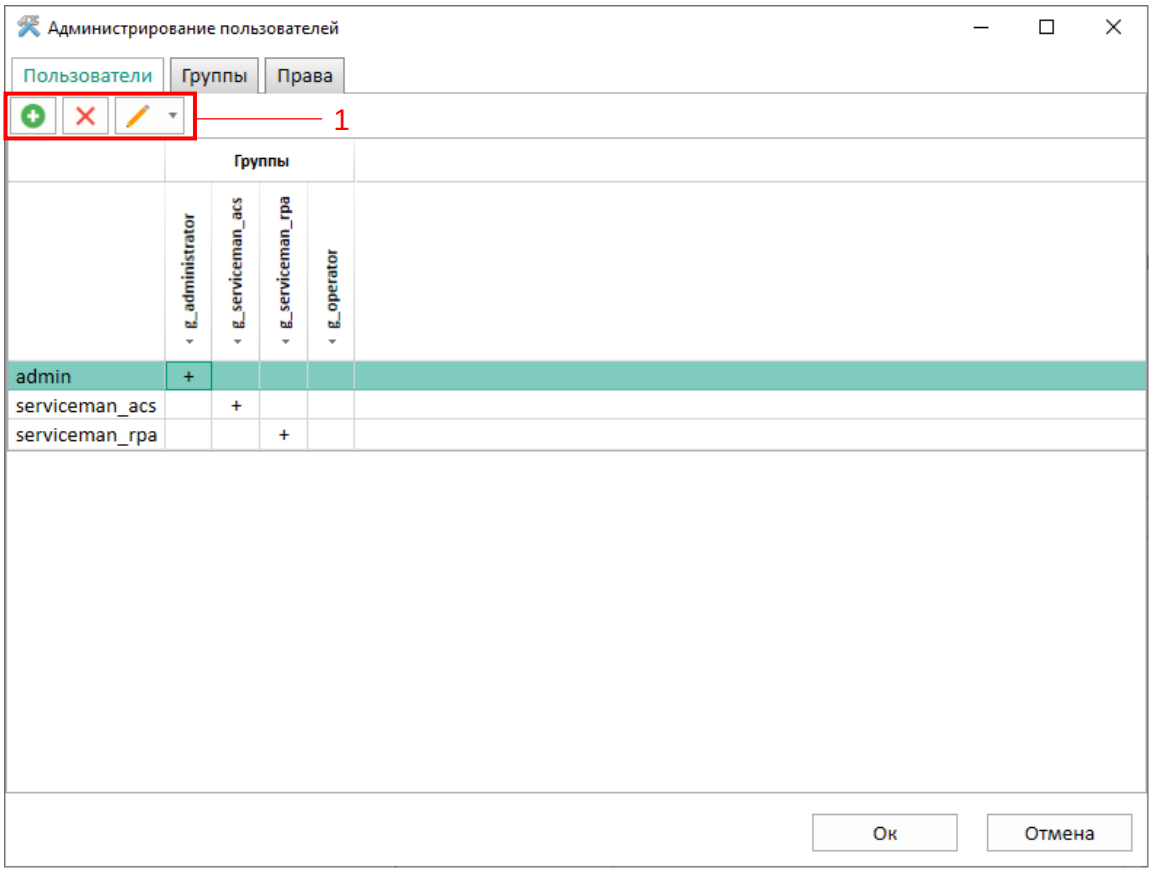


Рисунок 15

3.2.4.1 На вкладке **Пользователи** осуществляются операции над учетными записями пользователей. Операции доступны через панель инструментов  (см. рисунок 15, поз. 1).

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 16) необходимо ввести данные нового пользователя.

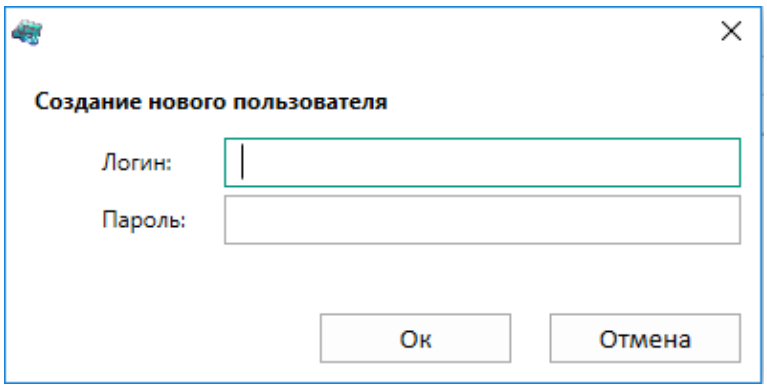


Рисунок 16

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

3.2.4.2 На вкладке **Группы** (см. рисунок 17) осуществляются операции над группами. Название группы можно редактировать, нажав левой кнопкой мыши на название.

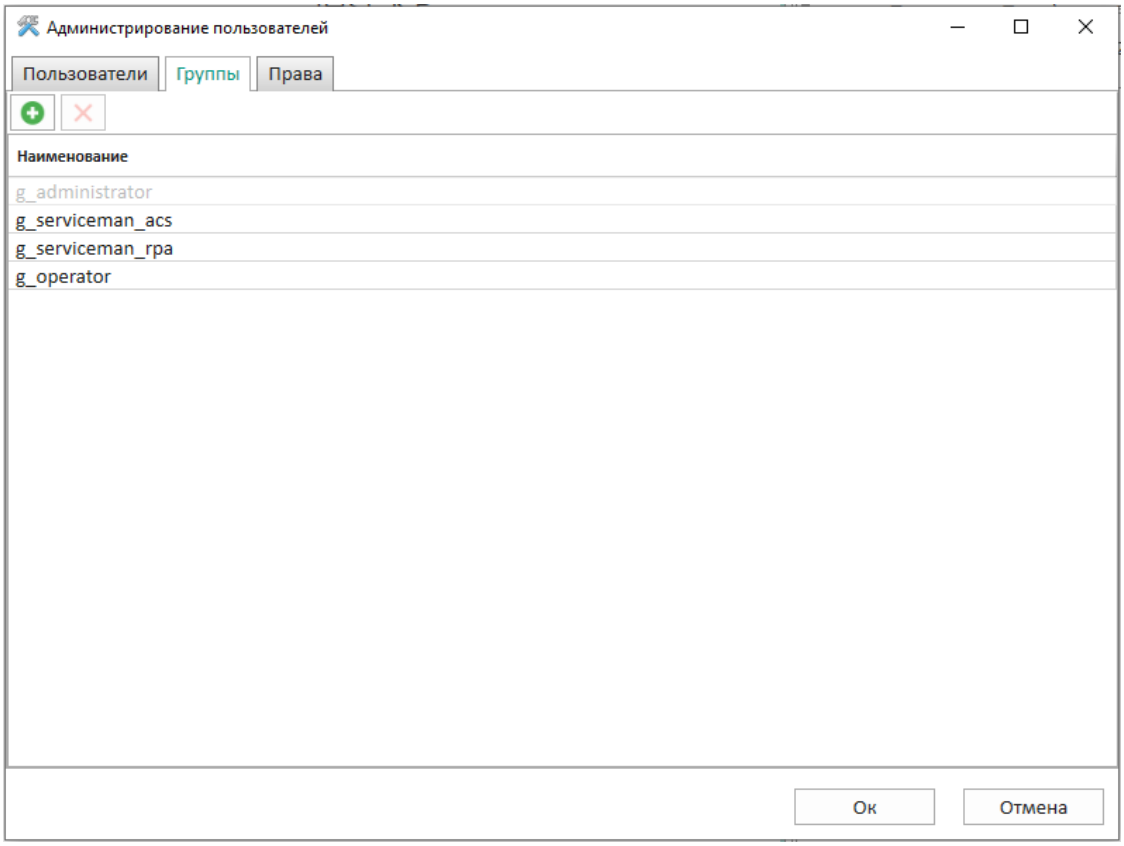


Рисунок 17

Добавление новой группы осуществляется нажатием кнопки  . При этом в отображаемом окне (см. рисунок 18) необходимо ввести имя для новой группы. После добавления новая группа появится во вкладках **Пользователи** и **Права** в столбце **Группы**.

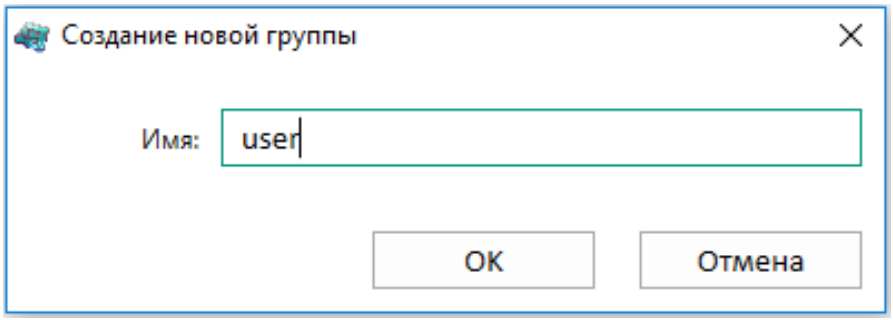


Рисунок 18

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

3.2.4.3 Вкладка **Права** (см. рисунок 19) предназначена для задания разрешений и прав доступа группам.

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

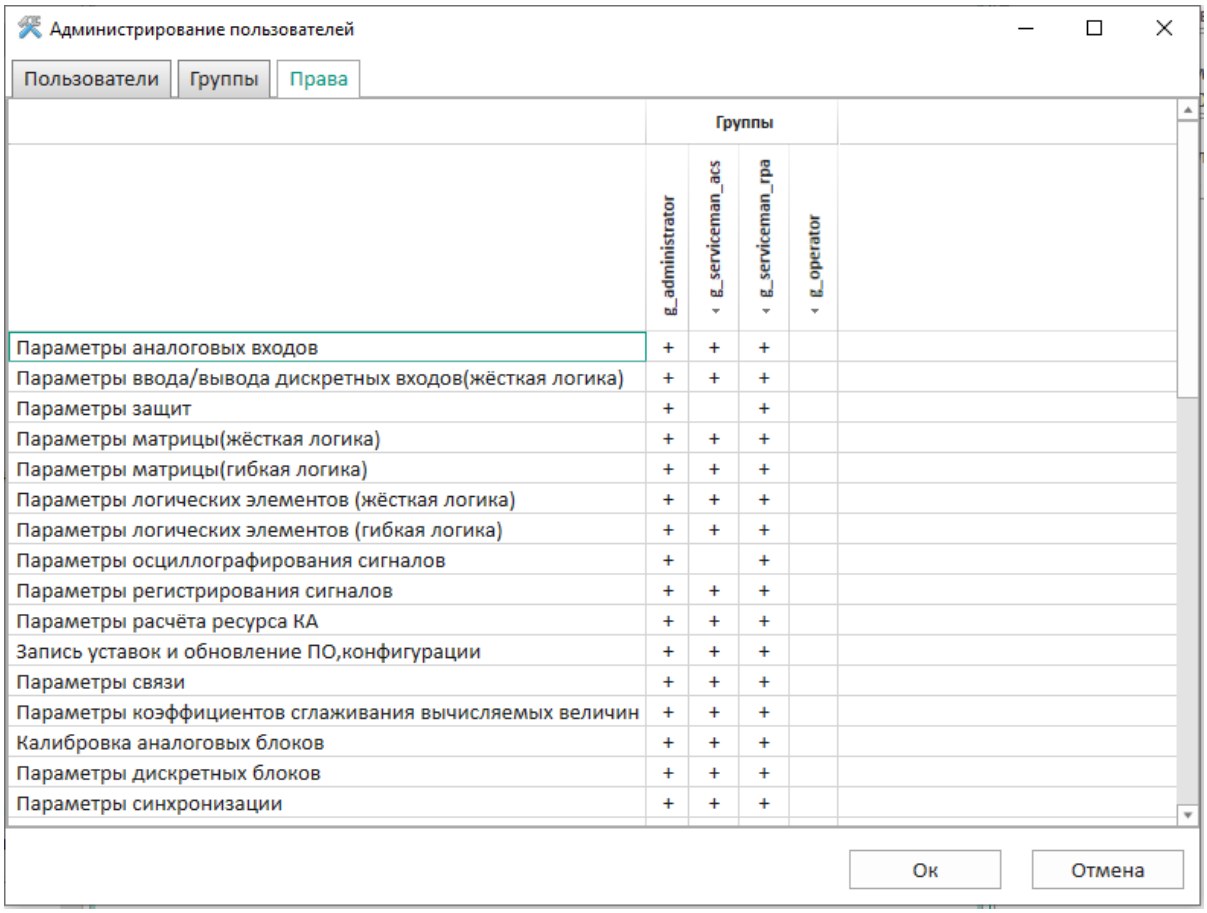


Рисунок 19

Предусмотрена гибкая настройка прав доступа для назначения прав группам пользователей и возможность управления функциями в логической схеме (см. рисунок 20).

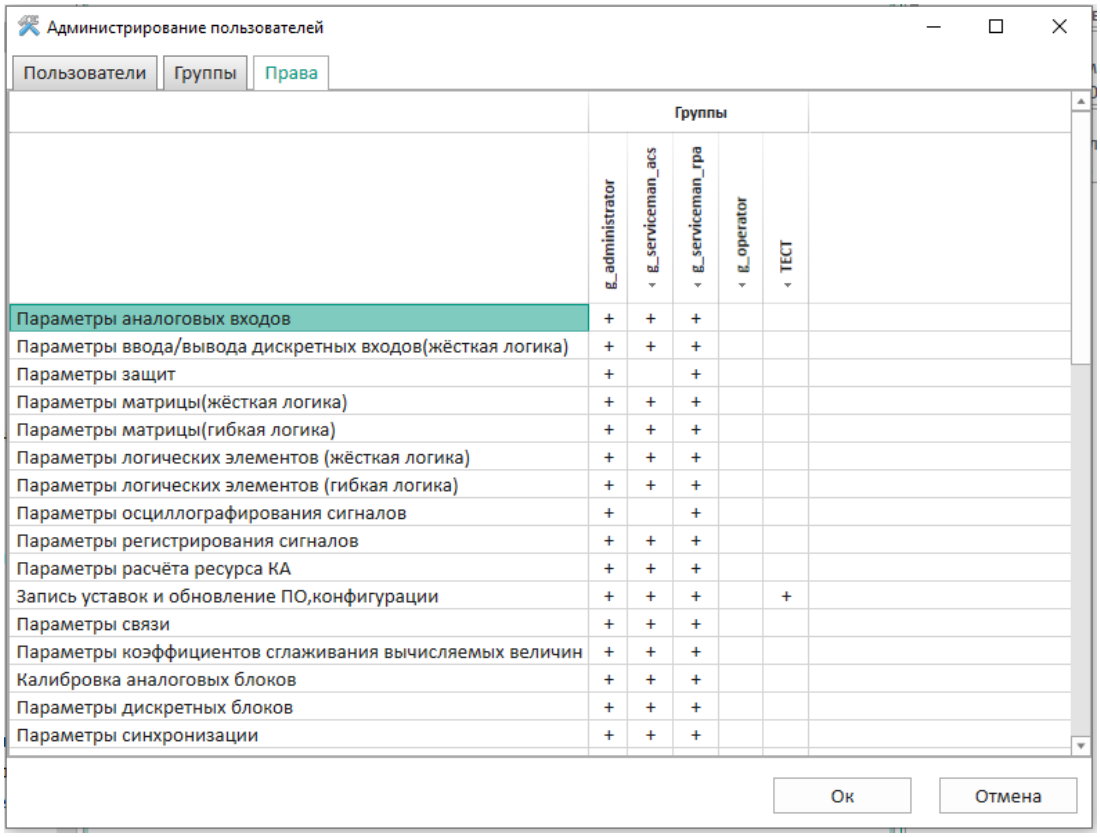


Рисунок 20

3.2.5 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/редактирование/удаление ролей и учетных записей пользователей, 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;

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 3.

Таблица 3 – Разграничение прав доступа пользователей

Права	Роли	
	Администратор	Инженер
Администрирование пользователей	Выполнение	–
Журнал событий ИБ	Чтение	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
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

3.3 Регистрация событий безопасности

3.3.1 Записи в журнале событий ИБ:

– содержат дату и время возникновения события;

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

– содержат тип событий.

3.3.2 Связанные с безопасностью операции пользователей в терминале регистрируются в качестве событий безопасности в энергонезависимую память терминала. Перечень регистрируемых событий приведен в таблице 4.

Таблица 4 – 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);
Все случаи использования механизма аутентификации пользователя	
Все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя	
Блокировка ИЧМ и возможности авторизации в программе Smart Monitor при достижении установленного количества неверного ввода пароля	
Попытки разблокирования интерактивного сеанса	

Событие в терминале	Регистрируемые данные
Изменение прав доступа группы пользователей	6) Действие; 7) Протокол подключения; 8) Порт подключения; 9) Источник события / идентификатор (серийный номер) съемного носителя информации
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 информационной безопасности (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 съемных носителей информации (при обновлении ПО и конфигурации, скачивании файлов)	
Активность канала связи, шторм по Ethernet	

3.3.3 Операции, связанные с безопасностью пользователей в терминале, выполненные в программе Smart Monitor, регистрируются в качестве событий безопасности в энергонезависимую память АРМ. Перечень регистрируемых событий приведен в таблице 5.

Таблица 5 – 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)	

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

3.3.5 Просмотр журнала событий ИБ по умолчанию доступен только пользователю с правами «Администратор» через пункт меню  –> **Выгрузить журнал событий информационной безопасности с устройства** (см. рисунок 21).

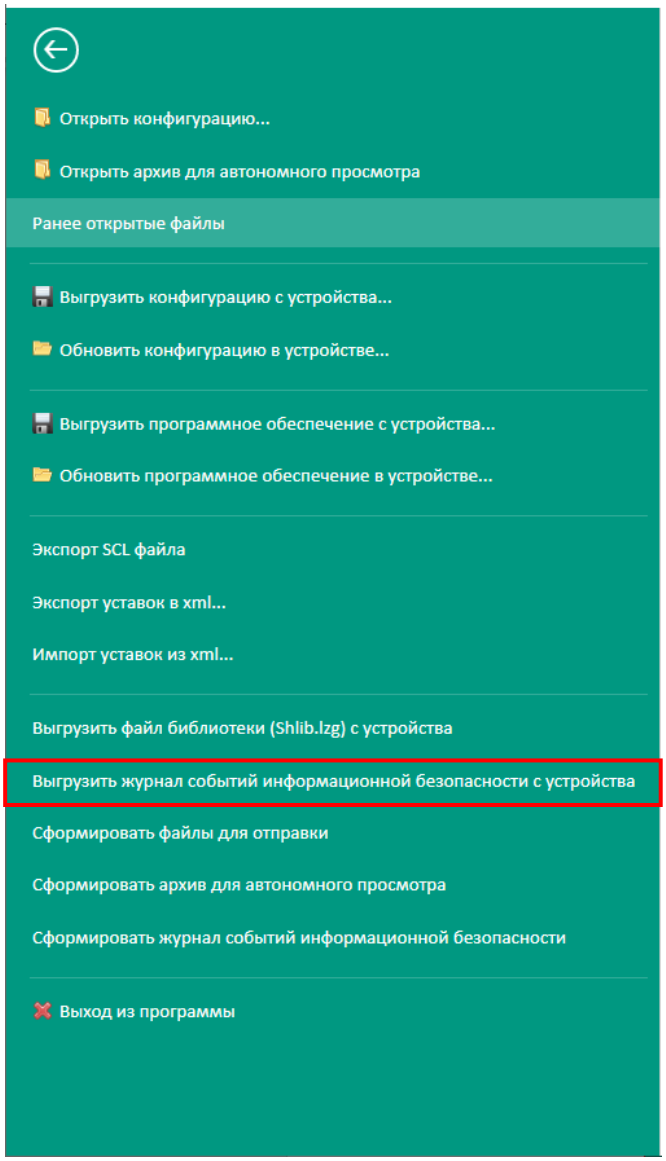


Рисунок 21

Далее необходимо выбрать место для сохранения архивированного файла и нажать кнопку **Сохранить** (см. рисунок 22, поз. 1).

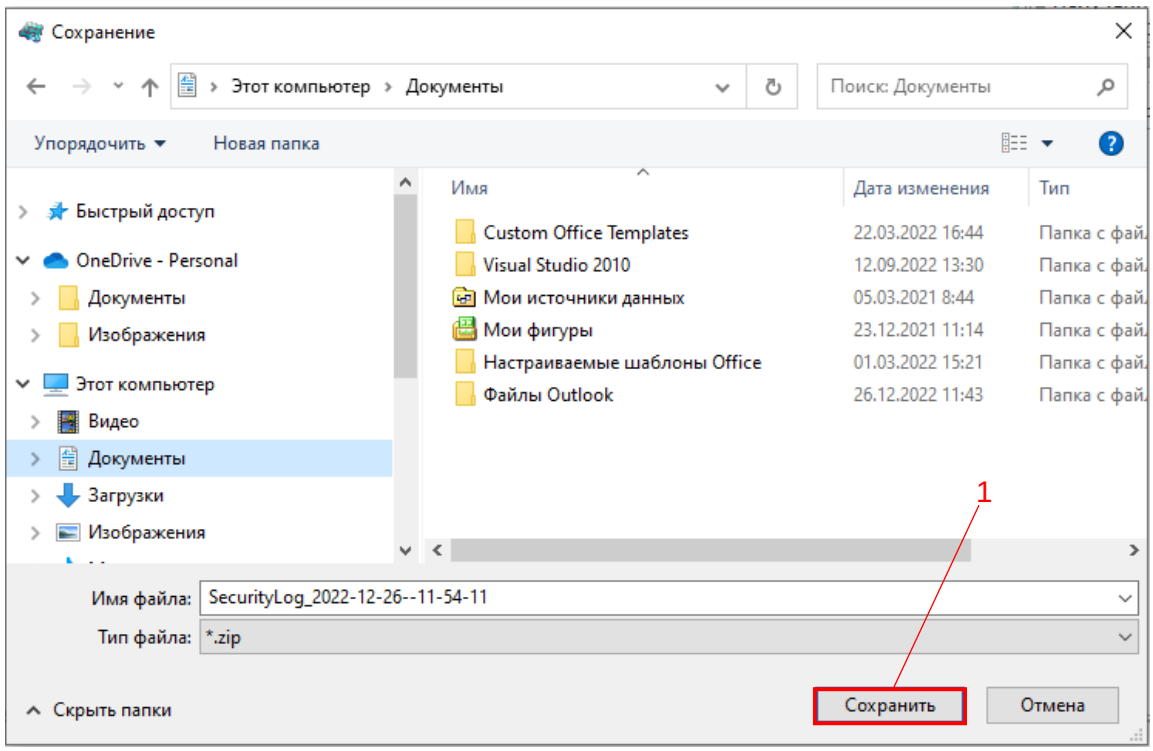


Рисунок 22

При успешном формировании файла появится информационное окно (см. рисунок 23).

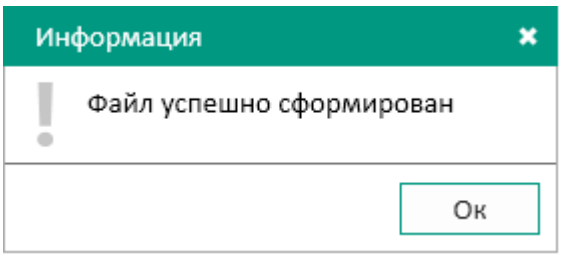
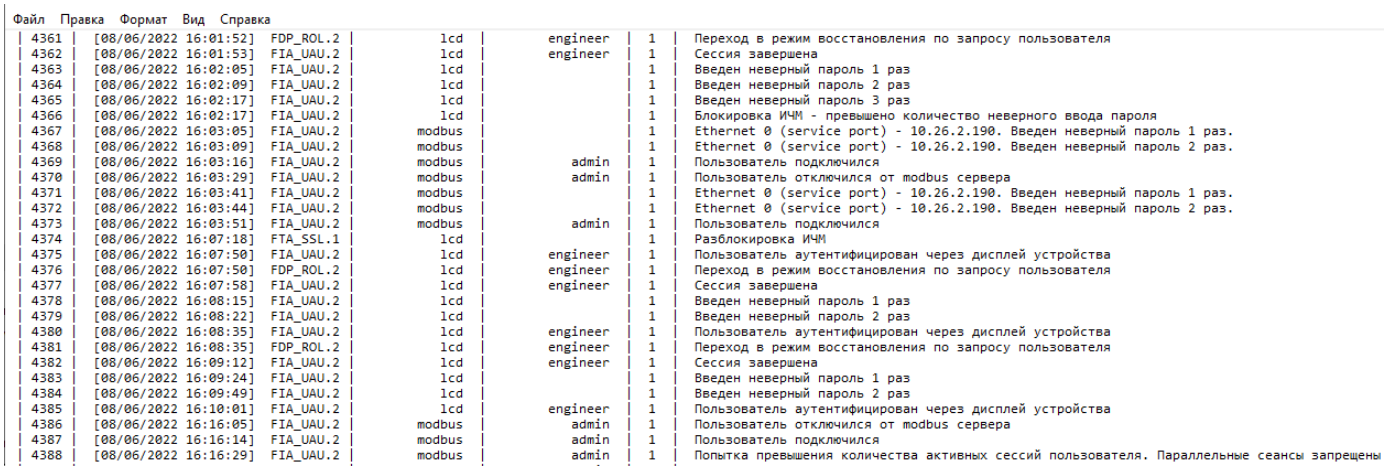


Рисунок 23

Далее следует разархивировать сохраненный файл. Пример содержания журнала событий ИБ приведен на рисунке 24.



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 24

3.4 Контроль использования съемных носителей информации

3.4.1 В программе E3_SW91 осуществляется контроль ввода (вывода) информации на носители информации.

Контроль ввода (вывода) информации на носители информации предусматривает:

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

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

– запрет действий по вводу (выводу) информации для пользователей, не имеющих полномочий на ввод (вывод) информации на носители информации;

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

Программа E3_SW91 определяет идентификатор съемных носителей. Съемный носитель имеет файловую систему FAT32.

Возможность обновления ПО терминала со съемных носителей разрешена только после авторизации пользователя с соответствующими правами доступа. Авторизация пользователя в терминале осуществляется по паролю (рисунок 25).

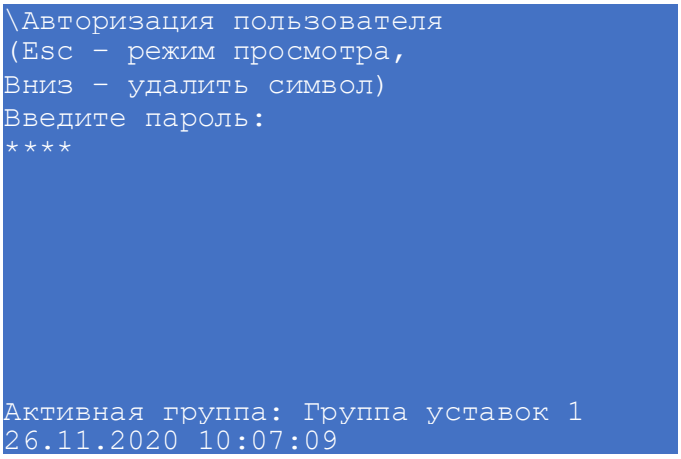


Рисунок 25

Действия пользователей и события по вводу (выводу) информации на съемных носителях регистрируются в журнале событий информационной безопасности. Просмотр журнала событий информационной безопасности по умолчанию доступен только пользователю с ролью «Администратор» через программу Smart Monitor: пункт меню  –> **Выгрузить журнал событий информационной безопасности с устройства** (см. рисунок 21).

3.5 Обеспечение целостности

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

3.5.2 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).

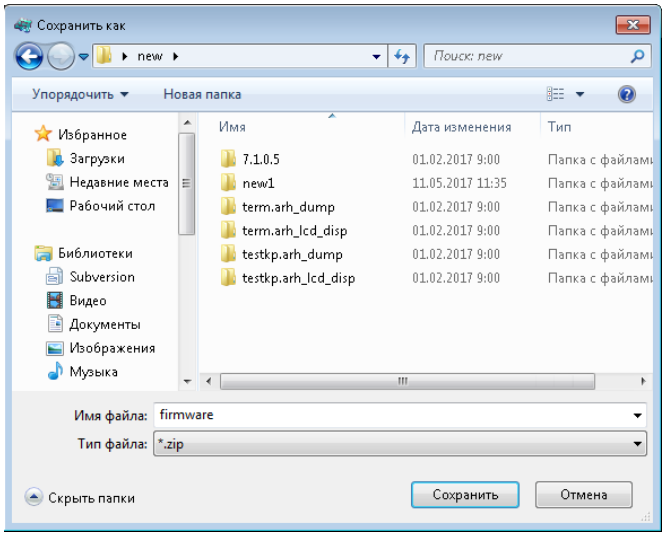
3.5.3 Результаты проверок целостности исполняемой программы или данных фиксируются в журнале событий ИБ.

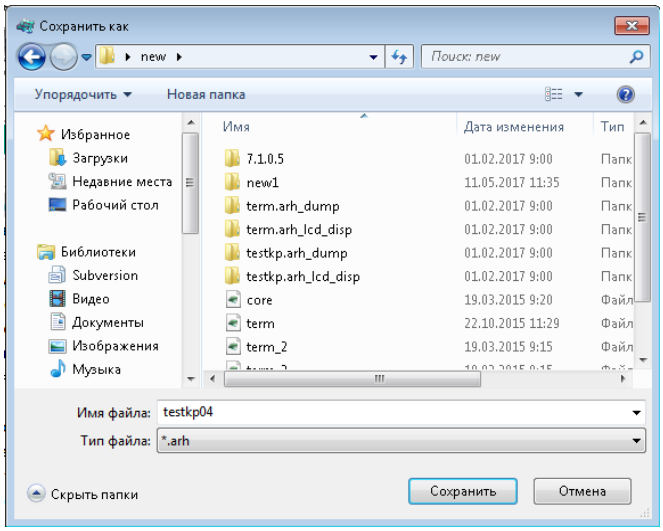
3.6 Обеспечение доступности

3.6.1 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 «Ошибка при проверке архива файлов прошивки» и «Ошибка при проверке архива конфигурации».

3.6.2 Под процессом резервного копирования ПО терминала следует понимать создание резервных копий файлов ПО и конфигурации терминала с помощью программы 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.

3.6.3 Создание резервных копий файлов ПО терминала и конфигурации происходит в пункте меню  –> **Сохранить программное обеспечение …** и в пункте меню  –> **Сохранить конфигурацию …** (рисунок 26).





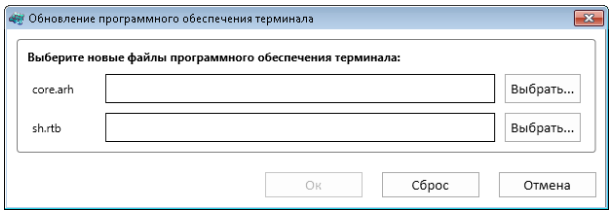
а) сохранение ПО б) сохранение конфигурации

Рисунок 26

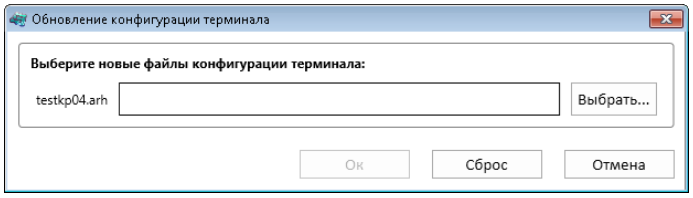
Для поддержания актуальности данных содержащихся в резервных копиях необходимо определить периодичность резервного копирования данных терминала. Периодичность создания резервных копий данных определяется в рамках текущей эксплуатации.

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

3.6.4 Загрузка прикладного ПО происходит в пункте меню  –> **Обновить программное обеспечение…** и пункт меню  –> **Обновить конфигурацию…**(рисунок 27).



а) обновление ПО



б) обновление конфигурации

Рисунок 27

3.6.5 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.

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

3.7 Обеспечение действий в нештатных ситуациях

3.7.1 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 27), загрузив предыдущие (заводские) версии ПО и конфигурации терминала.

3.7.2 Восстановления ПО, при возникновении нештатных ситуаций предусматривает:

– восстановление ПО из резервных копий;

– возврат ПО в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование.

3.7.3 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.

4 Описание действий по реализации функций безопасности среды функционирования ПО терминала

4.1.1 Для обеспечения выполнения функций безопасности в среде функционирования ПО должны выполняться требования безопасности информации среды функционирования ПО терминала, а именно:

– должны быть обеспечены установка, конфигурирование и управление ПО терминала в соответствии с эксплуатационной документацией;

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

– должны быть обеспечены совместимость компонентов ПО терминала с компонентами средств вычислительной техники автоматизированной системы;

– должен быть ограничен 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;

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

4.1.2 В процессе использования программы Smart Monitor, на АРМ пользователя должны быть реализованы меры антивирусной защиты.

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 машинные носители информации;

– контроль подключения съемных носителей информации.

4.1.3 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.

5 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 документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					
–					31				02.2023