УТВЕРЖДЕН

643.СПЕШ.24031-01 96 01-ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «Центрум-ДЗ»

Руководство пользователя

643.СПЕШ.24031-01 96 01

Листов 16

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

2024

АННОТАЦИЯ

Настоящий документ является руководством пользователя (далее – Руководство) для программного обеспечения «Центрум-ДЗ».

Руководство содержит общие сведения о программном обеспечении, его характеристиках, а также порядке выполнения различных операций при эксплуатации программного обеспечения.

Руководство разработано с учетом положений ГОСТ 19.505–79 «Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению».

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование

Полное наименование программного обеспечения: «Центрум-ДЗ».

В рамках настоящего документа употребляется также обозначение ПО.

Обозначение: 643.СПЕШ.24031-01.

«Центрум-ДЗ» – это российское программное обеспечение. Организация-разработчик: Акционерное общество «Эшелон – Северо-Запад» (АО «Эшелон-СЗ»).

Сайт организации-разработчика: https://nwechelon.ru/.

Организация-правообладатель: Акционерное общество «Эшелон – Северо-Запад» (АО «Эшелон-СЗ»).

1.2. Назначение

1.2.1. Функциональное назначение

ПО предназначено для осуществления функций централизованного контроля и управления аппаратно-программными модулями доверенной загрузки (АПМДЗ).

1.2.2. Эксплуатационное назначение

ПО реализовано в виде клиент-серверного программного обеспечения – системной службы и приложения для управления и настройки программного обеспечения «Центрум-ДЗ» с графическим пользовательским интерфейсом.

1.3. Функции ПО

Основными функциями ПО являются:

- сбор с АПМДЗ данных о событиях;
- ведение журнала событий АПМДЗ с их классификацией по уровню угрозы информационной безопасности;
- управление шаблонами контроля целостности файлов, а также секторов и разделов жесткого диска;
- контроль и управление АПМДЗ с помощью графического интерфейса пользователя;
- настройка классификации событий по уровню угрозы информационной безопасности.

2. ОПИСАНИЕ ХАРАКТЕРИСТИК ПО

2.1. Общее программное обеспечение, необходимое для работы ПО

Для функционирования ПО в рамках локальной сети, состоящей из АРМ и сервера, на сервере и АРМ должна быть установлена ОС Astra Linux Special Edition РУСБ.10015-01 (версия 1.6 «Смоленск») и СУБД PostgreSQL.

2.2. Состав ПО

«Центрум-ДЗ» представляет собой клиент-серверное программное обеспечение и состоит из системной службы, запускаемой автоматически при старте операционной системы на АРМ, и приложения для управления и настройки программного обеспечения «Центрум-ДЗ» с графическим пользовательским интерфейсом, устанавливаемого на локальный сервер.

2.3. Технические средства, необходимые для работы ПО

Для выполнения ПО оборудование должно иметь характеристики не хуже:

- процессор с архитектурой x86-64 (AMD, Intel);
- оперативная память – не менее 1 ГБ;
- объем свободного дискового пространства – не менее 500 МБ;
- сетевая плата: Ethernet 100 Мбит/с (или адаптер Wi-Fi).

Приведенные выше требования к техническим средствам являются минимально допустимыми. Применение более производительных технических средств улучшает эксплуатационные свойства ПО.

2.4. Уровень квалификации пользователя

Установка ПО в процессе основного жизненного цикла выполняется силами организации-заказчика. Для установки ПО сотрудник организации-заказчика должен обладать основными навыками работы с ПЭВМ под управлением ОС Linux. Установка производится согласно «Инструкции по установке», поставляемой в комплекте с дистрибутивом ПО.

Эксплуатация выполняется конечными пользователями, которые должны обладать навыками работы на персональном компьютере под управлением ОС Linux.

3. ПОДГОТОВКА К РАБОТЕ

Пользователи получают доступ к «Центрум-ДЗ» путем установки дистрибутива ПО на ПЭВМ. Сведения об установке ПО содержатся в документе «Инструкция по установке», поставляемом в комплекте с дистрибутивом ПО.

4. РАБОТА С «ЦЕНТРУМ-ДЗ»

4.1. Типовые операции

4.1.1. Запуск и останов

Для того, чтобы запустить серверную часть ПО (приложение для управления и настройки программного обеспечения «Центрум-ДЗ» с графическим пользовательским интерфейсом) необходимо найти ярлык загрузки серверной части ПО и дважды щелкнуть по нему левой кнопкой мыши. Авторизация пользователя в серверной части ПО не требуется.

Для того, чтобы остановить серверную часть ПО необходимо однократно нажать левой кнопкой мыши кнопку с изображением крестика в верхнем правом углу окна приложения.

Запуск клиентской части ПО (системной службы) происходит автоматически при загрузке операционной системы и не требует действий со стороны пользователя.

Прекращение работы клиентской части ПО происходит вместе с прекращением работы операционной системы и не требует действий со стороны пользователя.

4.1.2. Журналирование событий АПМДЗ

Аудит журналов событий АПМДЗ ведется автоматически. Со всех АРМ в составе локальной сети с установленными экземплярами клиентской части ПО собираются данные о событиях в режиме реального времени и отображаются во вкладке «События» в окне серверной части ПО.

Для того, чтобы просмотреть события АРМ в составе локальной сети, необходимо перейти во вкладку «События» в окне серверной части ПО (Рис. 1).

В указанном разделе в режиме реального времени отображаются записи о событиях АРМ в составе локальной сети, содержащие время события, уровень угрозы[1], тип события и идентификатор АРМ, с которого поступили данные о событии.

---

[1] Уровень угрозы выражен числом от 0 до 15, задается вручную настройками серверной части ПО и остается на усмотрение пользователя ПО.

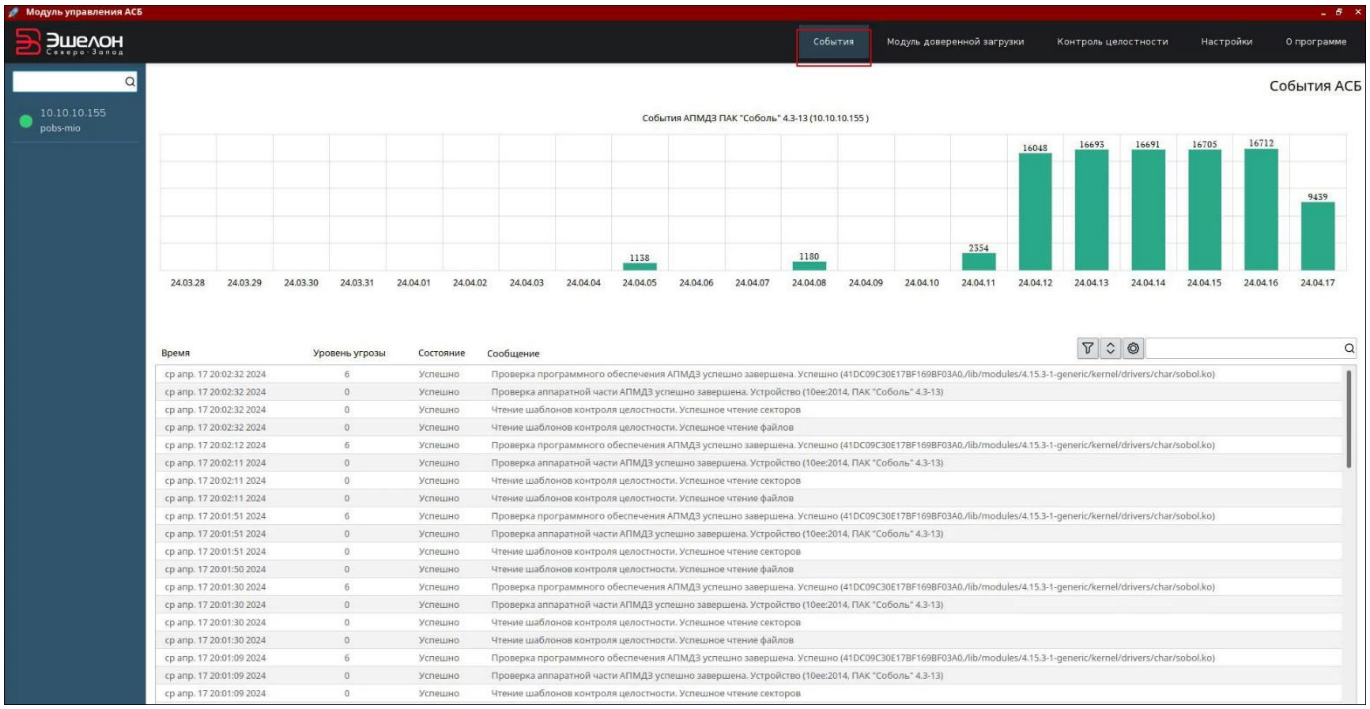

Рис. 1

4.1.3. Просмотр событий входа пользователей в систему

Аудит событий входа пользователей в систему ведется автоматически. Со всех АРМ в составе локальной сети с установленными экземплярами клиентской части ПО собираются данные о событиях входа в режиме реального времени и отображаются во вкладке «Модуль доверенной загрузки» в окне серверной части ПО.

Для того, чтобы просмотреть события входа пользователей в систему АРМ в составе локальной сети, необходимо перейти во вкладку «Модуль доверенной загрузки» в окне серверной части ПО (Рис. 2).

В указанном разделе отображаются данные о последнем успешном входе пользователей в систему АРМ, содержащие сведения об имени, типе и персональном идентификаторе пользователя, а также о дате и времени последнего входа с точностью до секунд.

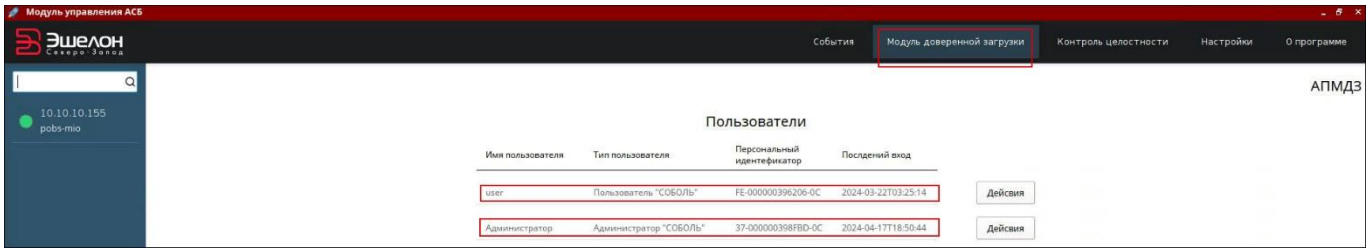

Рис. 2

4.1.4. Управление АПМДЗ с помощью графического интерфейса пользователя

Управление АПМДЗ посредством серверной части ПО включает в себя добавление и удаление секторов, разделов и файлов, подлежащих контролю целостности при загрузке системы АРМ, а также блокировку и разблокировку АРМ в составе локальной сети.

Для того, чтобы добавить или удалить секторы, разделы и файлы, подлежащие контролю целостности, необходимо выполнить шаги, описанные ниже.

Шаг 1. Перейти в раздел «Контроль целостности» в окне серверной части ПО и выбрать одну из функциональных кнопок в правой части окна: «Добавить файл», «Удалить файл», «Добавить сектор», «Удалить сектор», «Добавить раздел», «Удалить раздел» (Рис. 3), в зависимости от того, какое из действий требуется совершить.

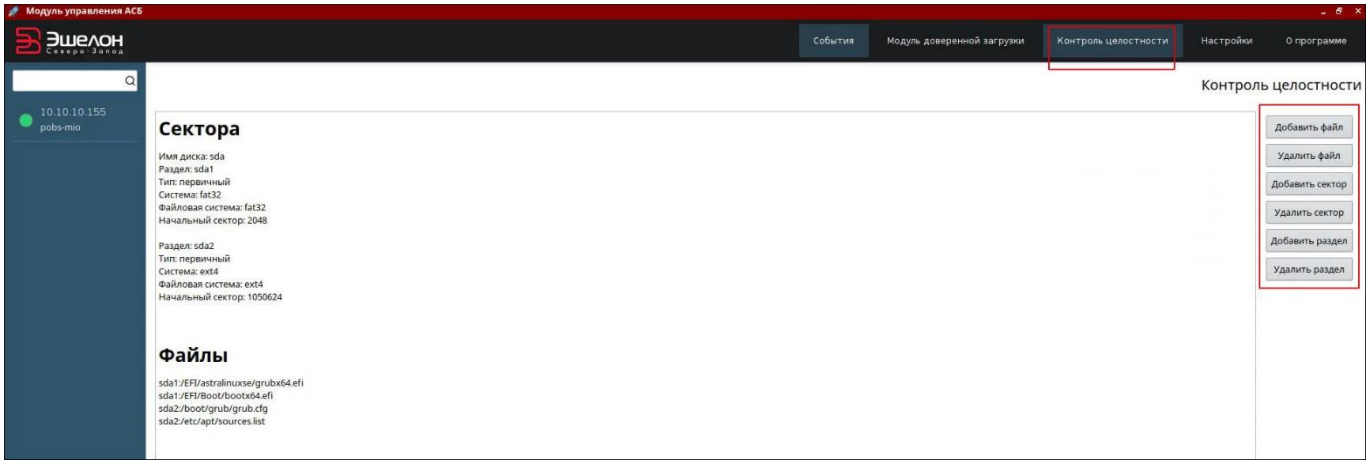

Рис. 3

Шаг 2. В появившемся всплывающем окне ввести данные сектора, раздела или файла, который требуется начать или прекратить контролировать на целостность при загрузке системы АРМ (Рис. 4).

В результате описанных выше шагов в разделе «Контроль целостности», в перечне секторов, разделов и файлов, подлежащих контролю целостности, добавятся новые записи (при добавлении), либо исчезнут существовавшие ранее (при удалении).

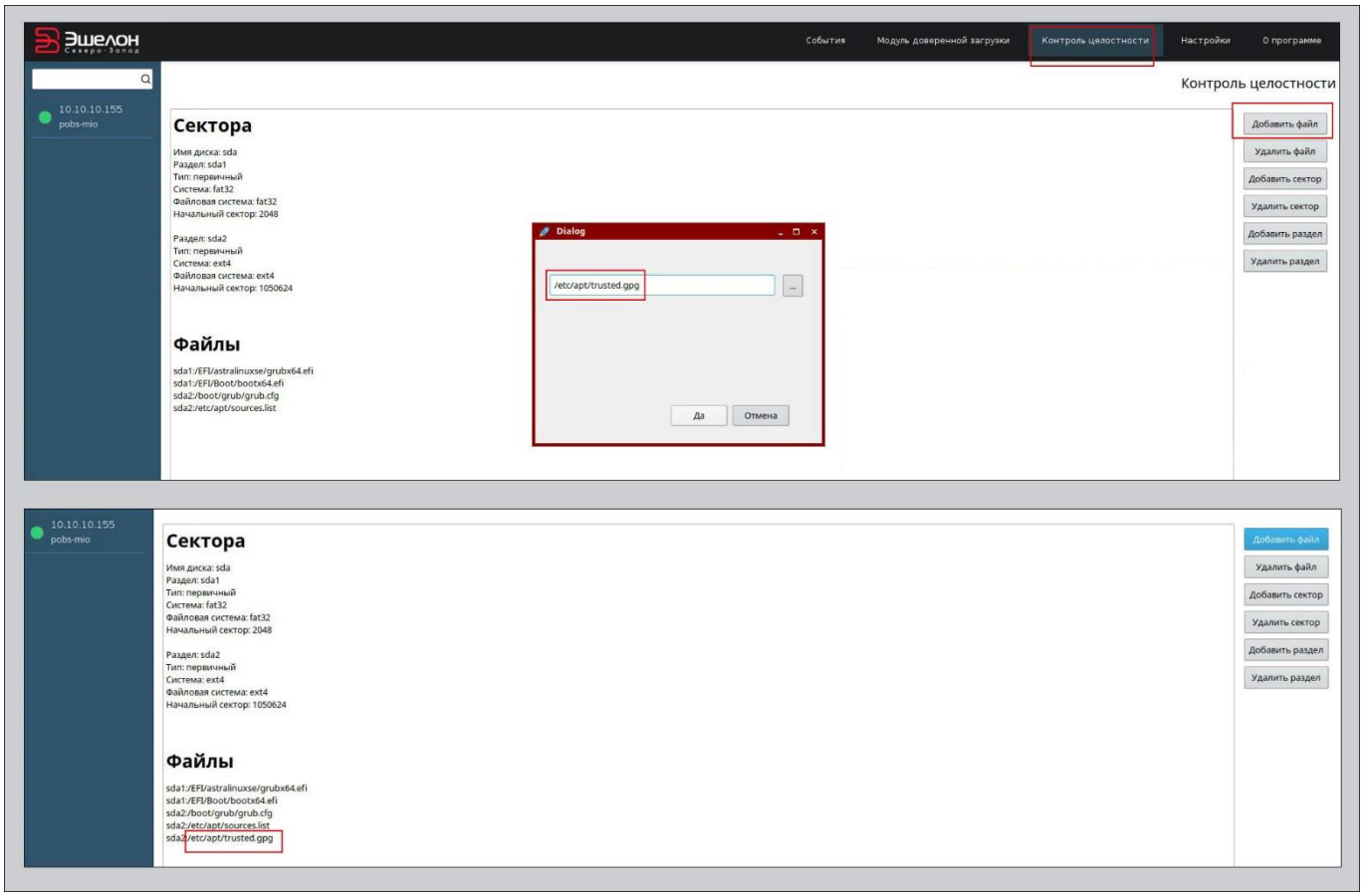

Рис. 4

Блокировка АРМ в составе локальной сети может осуществляться как вручную, так и автоматически. Разблокировка осуществляется только вручную.

Автоматическая блокировка АРМ происходит в случае, если произошло событие, на которое ПО реагирует блокировкой АРМ согласно настройкам.

Чтобы настроить автоматическую блокировку необходимо перейти в раздел «Настройки» в окне серверной части ПО и выбрать строку «Блокировка пользователей» в выпадающем списке поля внутри строки типа события (Рис. 5). Нажать кнопку «Сохранить» в нижнем правом углу экрана.

После выполнения этих действий в случае, если на АРМ произойдет событие, реакцией на которое выбрана блокировка, такое АРМ будет автоматически заблокировано.

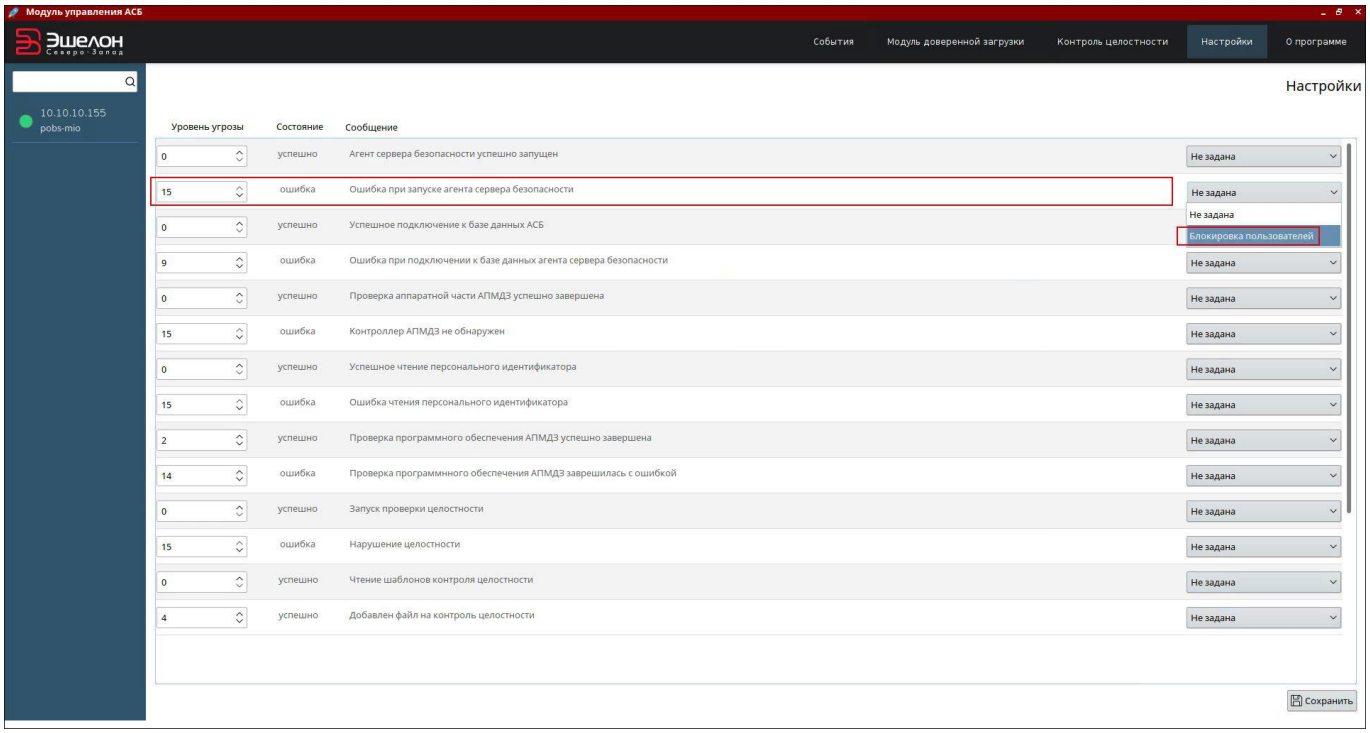

Рис. 5

Чтобы заблокировать АРМ вручную необходимо войти в раздел «Модуль доверенной загрузки» в окне серверной части ПО, выбрать в списке АРМ, которое необходимо заблокировать и нажать кнопку «Заблокировать АРМ» под надписью «Информация о АПМДЗ» справа (Рис. 6).

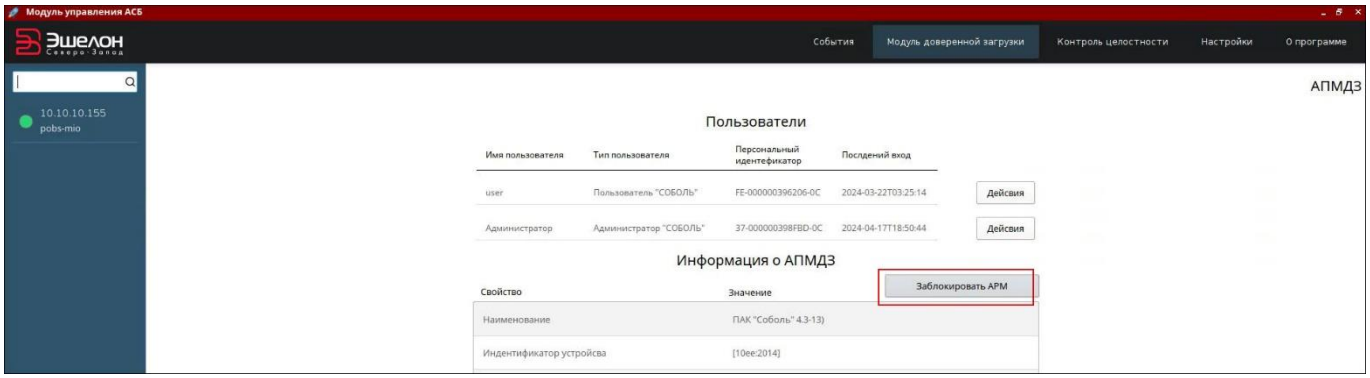

Рис. 6

Чтобы разблокировать АРМ вручную необходимо войти в раздел «Модуль доверенной загрузки» в окне серверной части ПО, выбрать в списке АРМ, которое необходимо разблокировать и нажать кнопку «Разблокировать АРМ» под надписью «Информация о АПМДЗ» справа (Рис. 7).

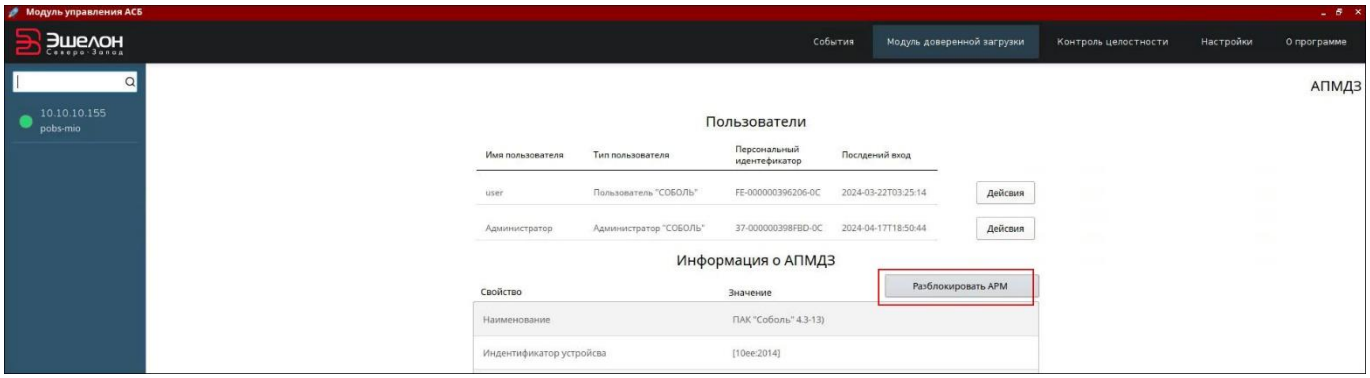

Рис. 7

4.1.5. Настройка классификации событий по уровню угрозы

Настройка классификации уровня угрозы событий, происходящих на АРМ в составе локальной сети, осуществляется вручную в серверной части ПО и заключается в присвоении каждому типу событий уровня, выраженного числом от 0 до 15. Присваиваемый уровень угрозы остается на усмотрение пользователя.

Для того, чтобы присвоить уровень угрозы событиям, необходимо перейти в раздел «Настройки» в окне серверной части ПО и ввести необходимые числовые значения от 0 до 15 в поля внутри строк типов событий, для которых необходимо настроить классификацию. Нажать кнопку «Сохранить» в нижнем правом углу экрана.

После выполнения вышеописанных действий записи о событиях в разделе «События» будут появляться с выбранным числовым выражением в столбце «Уровень угрозы» (Рис. 8).

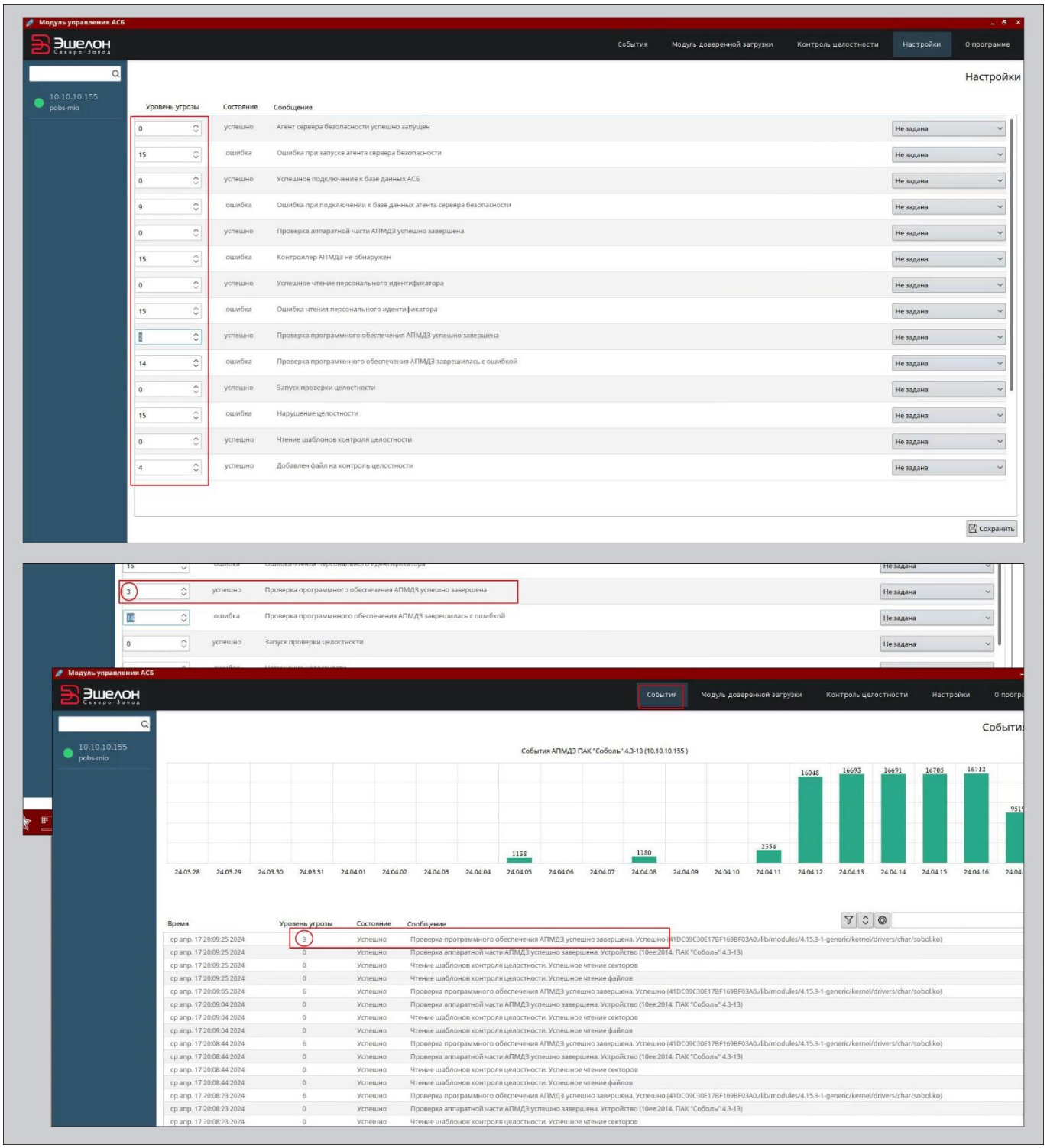

Рис. 8

4.2. Решение проблем

4.2.1. Техническая поддержка

В случае возникновения проблем пользователь может обратиться в службу технической поддержки по электронной почте: mail@nwechelon.ru.

Время работы технической поддержки: по будням с 09:00 до 18:00 (по московскому времени).

4.2.2. Типовые проблемы

4.2.2.1. Не ведется аудит журналов событий АРМ в составе локальной сети

Если в журнале событий АПМДЗ не отображаются данные о событиях одного, нескольких или всех АРМ, входящих в локальную сеть, следует удостовериться, что искомые АРМ корректно подключены к локальной сети. Устранить проблемы с сетевым подключением, дождаться обновления журнала событий АПМДЗ в серверной части ПО, которое произойдет автоматически при корректном подключении АРМ.

4.2.2.2. АРМ заблокировано, вход в систему не осуществляется

Если АРМ локальной сети заблокировано и пользователь не может осуществить вход в систему, необходимо в серверной части ПО (в приложении для управления и настройки ПО) перейти во вкладку «Информация о АПМДЗ», выбрать искомое АРМ в списке входящих в локальную сеть, удостовериться, что для выбранного АРМ не активирована кнопка блокировки (если АРМ не заблокировано, кнопка имеет вид «Заблокировать АРМ»). Если кнопка блокировки АРМ активна (имеет вид «Разблокировать АРМ»), нажать ее.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АПМДЗ	аппаратно-программный модуль доверенной загрузки
АРМ	Автоматизированное рабочее место
ОС	операционная система
ПО	программное обеспечение
ПЭВМ	персональная электронно-вычислительная машина

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводи-тельного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулиро-ванных					