



PALITRA

Система централизованного
управления и мониторинга

Руководство пользователя

Контактная информация

127106, г. Москва, ул. Гостиничная, д.5

Тел.: +7 (495) 988-92-25

E-mail: office@avsw.ru

www.avsw.ru/about/contacts

Авторское право

ООО «АВ Софт»

www.avsw.ru

© 2010-2023 ООО «АВ Софт»

Версия документа

Руководство пользователя v1.0

Март 24, 2023.

Настоящий документ является собственностью ООО «АВ Софт» (далее — «АВ Софт») и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения «АВ Софт».

СОДЕРЖАНИЕ

1	Термины и определения	4
2	Сокращения и значения.....	5
3	Назначение программы	6
3.1	Общие сведения	6
4	Авторизация и элементы управления	6
4.1	Элементы управления веб-интерфейсом	7
5	Проверки	10
6	Панель управления.....	10
7	Настройки	11
7.1	Основные	11
7.2	Пользователи.....	11
7.3	Серверы.....	14
8	Журналы.....	16

1 Термины и определения

В настоящем документе используются термины и определения, представленные в таблице 1.

Таблица 1. Термины и определения

№	Термин	Определение
1.	Инсталляция	Программное обеспечение компании АВ Софт

2 Сокращения и значения

В настоящем документе используется перечень сокращений, представленный в таблице 2.

Таблица 2. Сокращения и значения

№	Сокращение	Значение
1.	API	Application Programming Interface
2.	CPU	Central Processing Unit
3.	DNS	Domain Name System
4.	HTTP	Hypertext Transfer Protocol
5.	БД	База данных
6.	ВМ	Виртуальная машина
7.	ВПО	Вредоносное программное обеспечение
8.	ОС	Операционная система
9.	ПО	Программное обеспечение
10.	ИС	Имитационная среда

3 Назначение программы

Система централизованного управления и мониторинга AVSOFT PALITRA (далее – Система PALITRA) предназначена для управления отдельными инсталляциями продуктов компании АВ Софт.

3.1 Общие сведения

Система предназначена для выполнения следующих задач:

- Агрегация и хранение логов
- Построение отчетов
- Управление настройками
- Сбор статистической информации
- Отслеживание состояния функциональных модулей
- Отображение всех проверок в едином интерфейсе системы
- Централизованное распространение настроек на все инсталляции

Перед началом работы с системой PALITRA у администратора необходимо получить логин и пароль от учетной записи пользователя.

4 Авторизация и элементы управления

Для авторизации в системе PALITRA необходимо ввести логин и пароль, полученный у администратора (Рисунок 1).

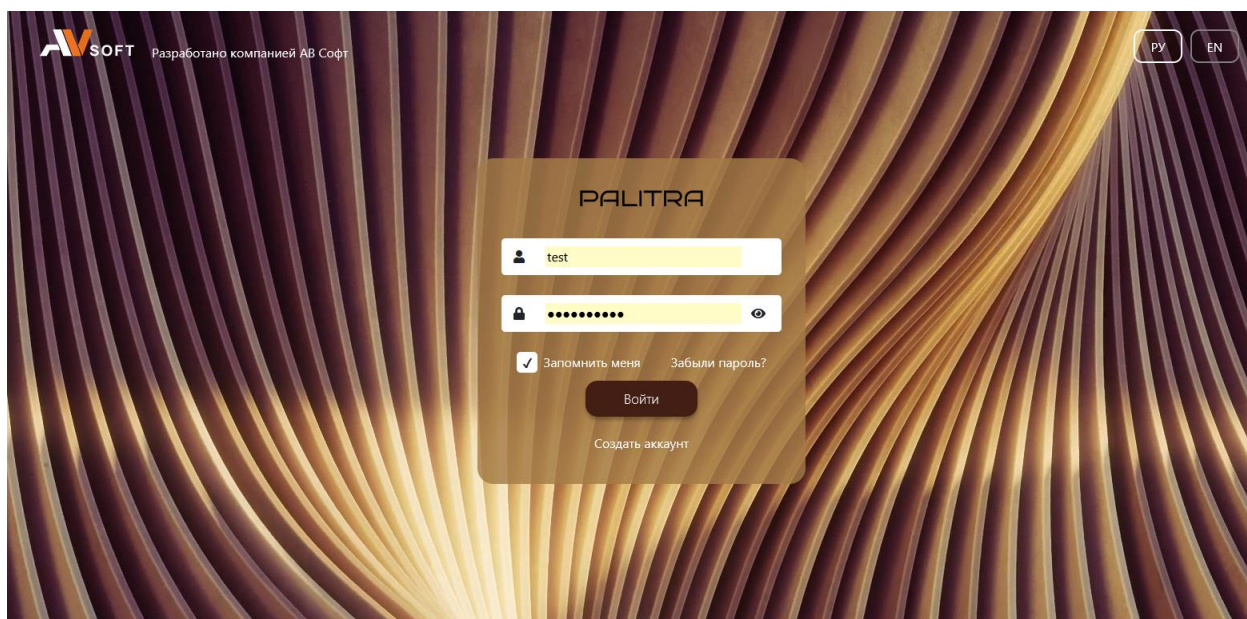


Рисунок 1. Страница авторизации пользователя в системе PALITRA

После прохождения авторизации осуществляется переход в веб-интерфейс системы PALITRA, в котором присутствуют функциональные разделы, описанные в таблице 3.




Таблица 3. Описание функциональных разделов в системе










№	Раздел	Описание
1.	Проверки	Содержит информацию по всем проверкам файлов на отдельных инсталляциях системы ATHENA.
2.	Панель управления	Содержит информацию по подключенным к системе PALITRA отдельным инсталляциям системы ATHENA.
3.	Настройки	Содержит основные настройки системы PALITRA.
4.	Журналы	Содержит информацию по мониторингу всех логических и физических модулей в системе, а также регистрацию действий пользователей.




4.1 Элементы управления веб-интерфейсом

Описание, назначение и настройки по умолчанию элементов управления веб-интерфейсом системы PALITRA представлены в таблице 4.

Таблица 4. Элементы управления интерфейсом

№	Элемент	Назначение	Изображение
1.	Значок «Выход»	Выполняет выход из системы	
2.	Значок «Календарь»	Выполняет переход в форму выбора даты	
3.	Значок «Профиль»	Позволяет перейти в личный аккаунт пользователя в системе	

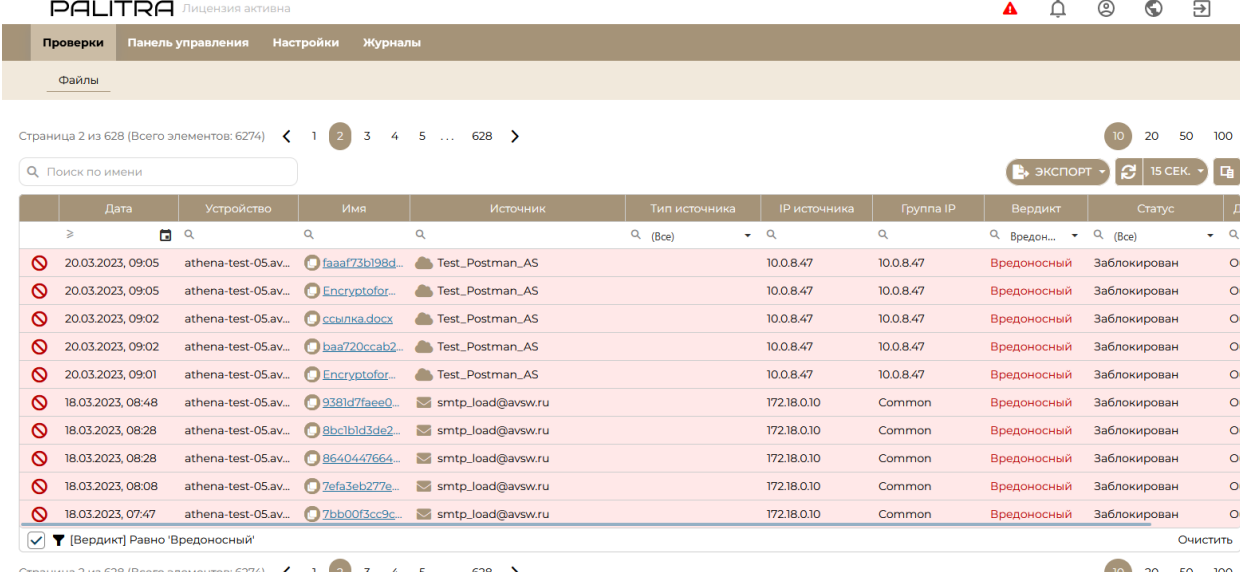
№	Элемент	Назначение	Изображение
4.	Значок «Выпадающий список»	Позволяет выбрать язык отображения интерфейса	
5.	Кнопка «Уведомления»	Позволяет увидеть уведомления, которые выдает система	
6.	Кнопка «Неактивные модули»	Появляется при каких-либо уведомлениях	
7.	Кнопка «Обновить»	Обновление данных в таблице	
8.	Кнопка «Добавить»	Выполняет добавление новой сущности	
9.	Кнопка «Редактировать»	Выполняет редактирование	
10.	Кнопка «Фильтр»	Фильтр, который выполняет фильтрацию, если в поисковом поле таблицы введены данные	
11.	Кнопка «Экспортировать все»	Скачиваются в выбранном формате	
12.	Кнопка «Удалить»	При нажатии на кнопку будет осуществлено удаление выбранной записи	

№	Элемент	Назначение	Изображение
13.	Кнопка «Настройки»	При нажатии на кнопку отобразится форма для изменения настроек	
14.	Кнопка «Закрепить»	При нажатии на кнопку произойдет закрепление записи в таблице	
15.	Кнопка «Открепить»	При нажатии на кнопку закрепленная в таблице запись будет откреплена	
16.	Кнопка «Загрузка файла»	При нажатии на кнопку отобразится форма для подтверждения выгрузки файла на рабочую станцию	
17.	Кнопка «Информация»	При нажатии на кнопку отобразится форма, содержащая информацию о машине	

Элементы управления веб-интерфейсом имеют всплывающие подсказки, которые отображают их названия.

5 Проверки

В разделе «Проверки» отображается файловый поток с отдельных инсталляций системы ATHENA (Рисунок 2).



The screenshot shows the PALITRA interface with the 'Checks' section active. The table displays the following data:

Дата	Устройство	Имя	Источник	Тип источника	IP источника	Группа IP	Вердикт	Статус
20.03.2023, 09:05	athena-test-05.av...	faaf73b198d...	Test_Postman_AS	(Все)	10.0.8.47	10.0.8.47	Вредоносный	Заблокирован
20.03.2023, 09:05	athena-test-05.av...	Encryptofor...	Test_Postman_AS	(Все)	10.0.8.47	10.0.8.47	Вредоносный	Заблокирован
20.03.2023, 09:02	athena-test-05.av...	ссылка.docx	Test_Postman_AS	(Все)	10.0.8.47	10.0.8.47	Вредоносный	Заблокирован
20.03.2023, 09:02	athena-test-05.av...	baaf720ccab2...	Test_Postman_AS	(Все)	10.0.8.47	10.0.8.47	Вредоносный	Заблокирован
20.03.2023, 09:01	athena-test-05.av...	Encryptofor...	Test_Postman_AS	(Все)	10.0.8.47	10.0.8.47	Вредоносный	Заблокирован
18.03.2023, 08:48	athena-test-05.av...	9381d7faee0...	smtp_load@avsw.ru	(Все)	172.18.0.10	Common	Вредоносный	Заблокирован
18.03.2023, 08:28	athena-test-05.av...	8bc1bd3de2...	smtp_load@avsw.ru	(Все)	172.18.0.10	Common	Вредоносный	Заблокирован
18.03.2023, 08:28	athena-test-05.av...	8640447664...	smtp_load@avsw.ru	(Все)	172.18.0.10	Common	Вредоносный	Заблокирован
18.03.2023, 08:08	athena-test-05.av...	7efa3eb277e...	smtp_load@avsw.ru	(Все)	172.18.0.10	Common	Вредоносный	Заблокирован
18.03.2023, 07:47	athena-test-05.av...	7bb00f3cc9c...	smtp_load@avsw.ru	(Все)	172.18.0.10	Common	Вредоносный	Заблокирован

Рисунок 2. Раздел «Проверки»

6 Панель управления

В разделе «Панель управления» присутствует информация по отдельным инсталляциям, подключенным к системе PALITRA для передачи данных (Рисунок 3).



The screenshot shows the PALITRA interface with the 'Management Panel' section active. The table displays the following data:

Устройство	Тип системы	Дата регистрации	Версия	Активно	Ключ
athena-test-05.avsw.ru		14.02.2023, 17:19	3.0.5	<input checked="" type="checkbox"/>	[Redacted]
athena-dev-04.avsw.ru		20.03.2023, 15:37	3.1.3	<input checked="" type="checkbox"/>	[Redacted]

Рисунок 3. Раздел «Панель управления»

По каждой инсталляции присутствует возможность загрузки файла системных логов с указанием определенного интервала времени (Рисунок 4).

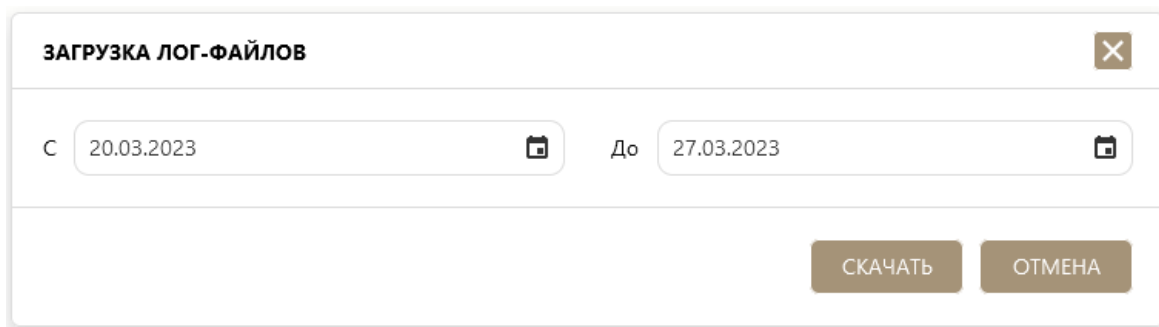


Рисунок 4. Загрузка лог-файлов

7 Настройки

7.1 Основные

В разделе «Настройки» присутствует вкладка «Основные», которые содержит информацию по лицензии на систему PALITRA. При помощи кнопки «Импорт» можно осуществить загрузку лицензионного ключа (Рисунок 5).

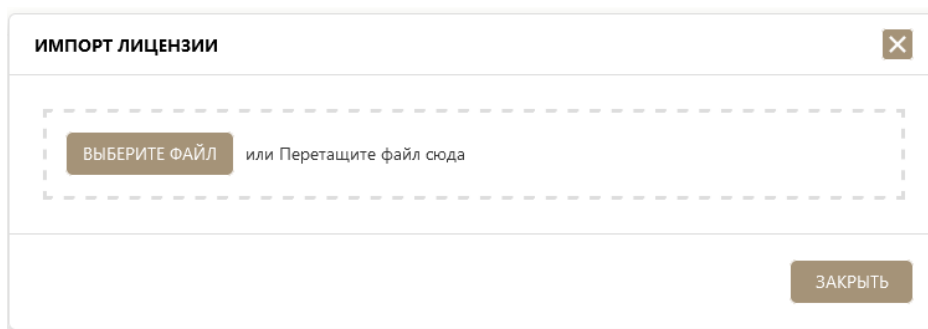


Рисунок 5. Импорт лицензии

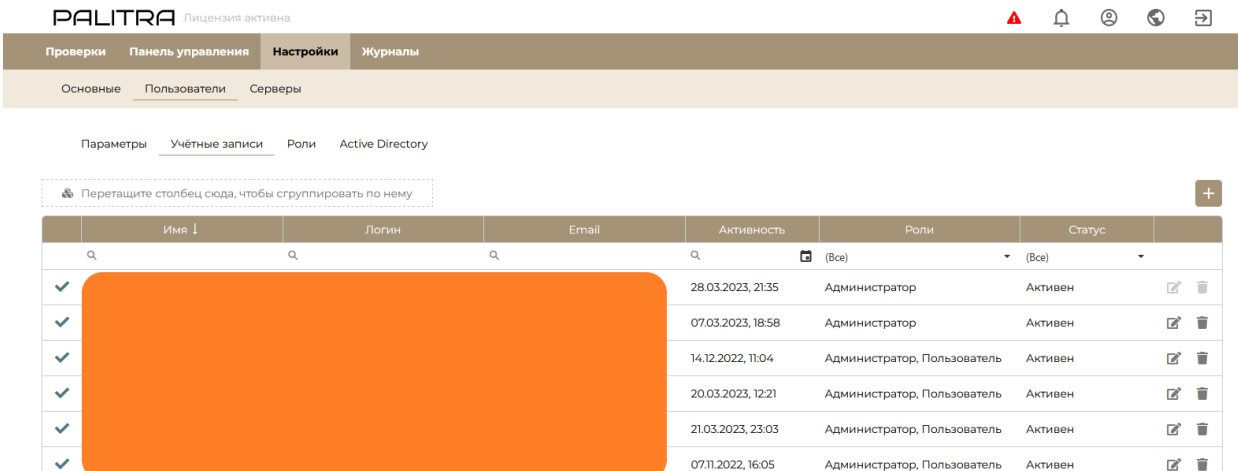
7.2 Пользователи

Во вкладке «Пользователи» присутствуют параметры пользовательской сессии, где можно выставить значение бездействия до блокировки - период времени, по истечении которого, в случае бездействия пользователя, произойдет блокировка текущей сессии (Рисунок 6).



Рисунок 6. Параметры пользовательской сессии

Вкладка «Пользователи» содержит учетные записи пользователей всех пользователей (Рисунок 7).

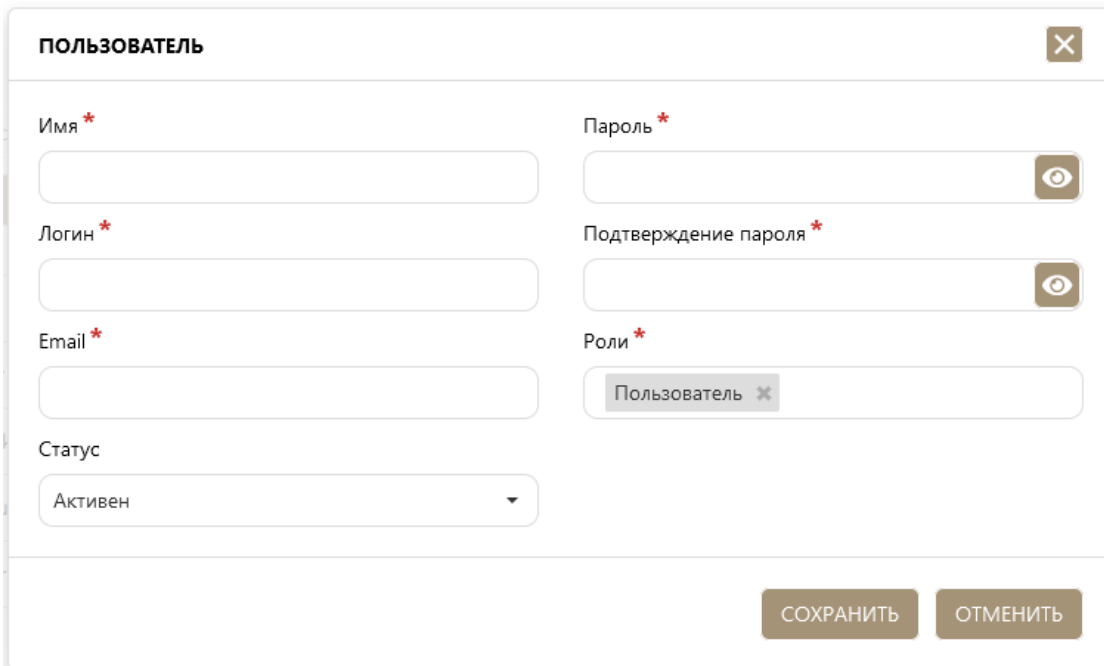


The screenshot shows the PALITRA web interface. At the top, there is a navigation bar with tabs: Проверки, Панель управления, **Настройки**, and Журналы. Below this, there are sub-tabs: Основные, **Пользователи**, and Серверы. Further down, there are more sub-tabs: Параметры, **Учётные записи**, Роли, and Active Directory. A table displays a list of users with columns: Имя, Login, Email, Активность, Роли, and Статус. The first column has checkmarks. The second column is obscured by an orange rectangle. The table contains six rows of user data.

Имя	Логин	Email	Активность	Роли	Статус
✓			28.03.2023, 21:35	Администратор	Активен
✓			07.03.2023, 18:58	Администратор	Активен
✓			14.12.2022, 11:04	Администратор, Пользователь	Активен
✓			20.03.2023, 12:21	Администратор, Пользователь	Активен
✓			21.03.2023, 23:03	Администратор, Пользователь	Активен
✓			07.11.2022, 16:05	Администратор, Пользователь	Активен

Рисунок 7. Учетные записи пользователей

Для добавления нового пользователя необходимо нажать кнопку «Добавить» и заполнить в функциональной форме все требуемые поля (Рисунок 8).



The screenshot shows a form titled 'ПОЛЬЗОВАТЕЛЬ' with a close button (X) in the top right corner. The form contains several input fields and a dropdown menu. The fields are: Имя*, Пароль*, Логин*, Подтверждение пароля*, Email*, Роли*, and Статус. The 'Роли*' field has a dropdown menu with 'Пользователь' selected. The 'Статус' field has a dropdown menu with 'Активен' selected. At the bottom right, there are two buttons: СОХРАНИТЬ and ОТМЕНИТЬ.

Рисунок 8. Добавление нового пользователя

! Роли администраторов может назначить пользователь с правами администратора.

Для активации или блокировки пользователя необходимо выставить нужное значение в поле «Статус».

Вкладка «Пользователи» содержит роли и ролевую модель, для добавления новой роли с определенным набором прав необходимо нажать кнопку «Добавить» и выбрать нужные права и доступы (Рисунок 9).

НАСТРОЙКИ РОЛИ

Роль *

Разрешения

- Возможность изменять итоговый вердикт после проведенного исследования
- Скачивание файлов из системы
- Добавление, редактирование и удаление учётных записей
- Доступ к функционалу по обновлению системы
- Доступ к разделу "Справочники -> Системные"
- Доступ к разделу "Справочники -> Аналитические"
- Доступ к разделу "Журналы"
- Доступ к разделу "Объекты анализа"
- Доступ к разделу "Исследования"

СОХРАНИТЬ ОТМЕНИТЬ

Рисунок 9. Ролевая модель

Вкладка «Пользователи» содержит интеграцию с Active Directory. Для инициации подключения необходимо (Рисунок 10).

PALITRA Лицензия активна

Проверки Панель управления **Настройки** Журналы

Основные Пользователи Серверы

Параметры Учётные записи Роли Active Directory

Active Directory

Аутентификация через AD

IP контроллера домена *

Область поиска пользователя: DN по умолчанию

Общее имя

Организационное подразделение

Сервер: Домен по умолчанию

Домен: Домен по умолчанию

СОХРАНИТЬ

Идентификаторы Active Directory

Идентификатор	Тип	Роли Athena
	(Все)	
Нет данных		

Рисунок 10. Active Directory

Для интеграции с AD необходимо заполнить функциональный раздел «Идентификаторы Active Directory» при помощи кнопки «Добавить» (Рисунок 11).

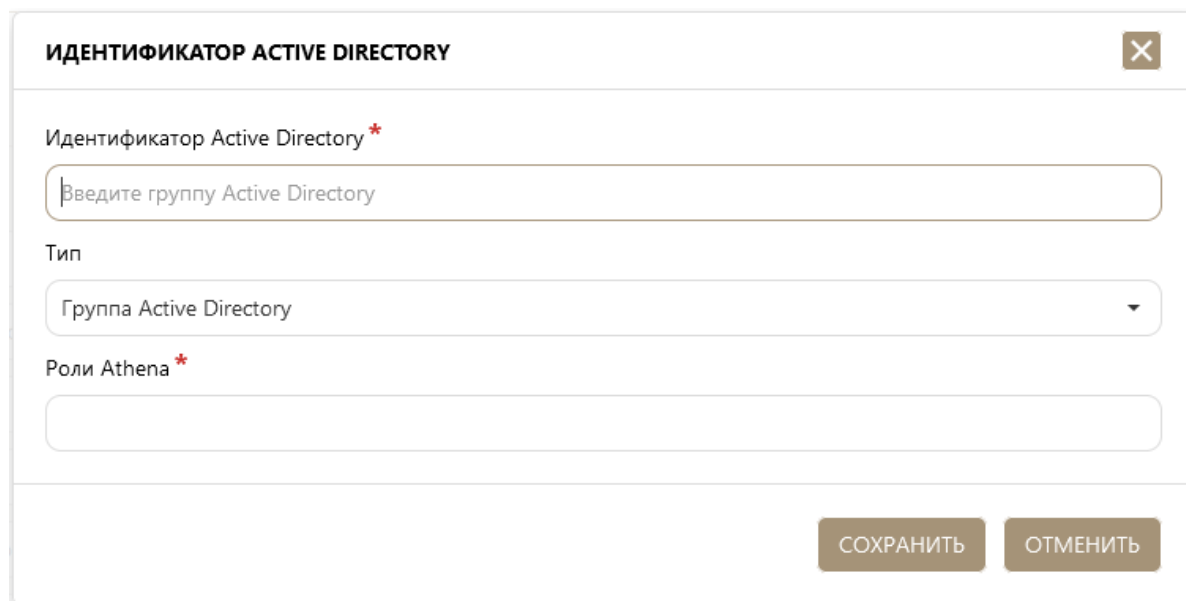


Рисунок 11. Идентификатор Active Directory

Если определенному пользователю из AD назначить роль в системе PALITRA, то необходимо заполнить функциональный раздел «Active Directory». По умолчанию, если этого не делать, то пользователь AD будет пользователем.

Аутентификация через AD - включение данного флага активирует службу каталогов Active Directory.

IP контроллера домена - IP адрес сервера, контролирующего область компьютерной сети.

Область поиска пользователя - режим поиска уникальных имен в AD. В AD каждой записи назначается DN (distinguished name / уникальное имя).

К AD идет подключение при каждой попытке входа пользователя.

7.3 Серверы

Во вкладке «Серверы» отображается «Мониторинг», в котором присутствует информация и состояние по функциональным модулям системы PALITRA (Рисунок 12).

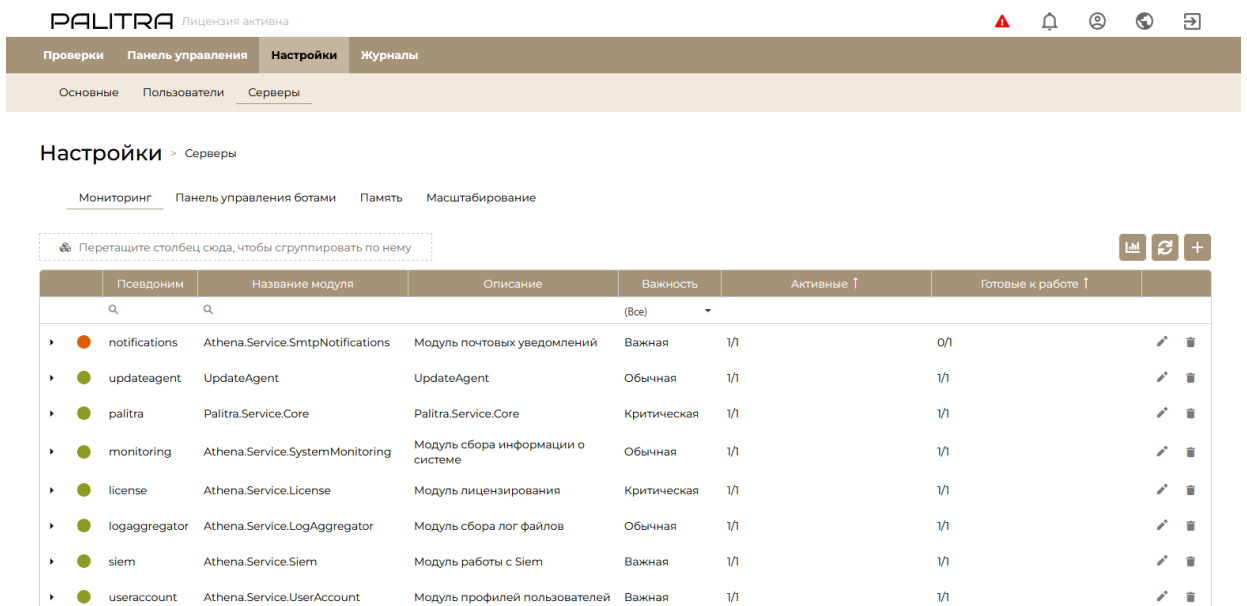


Рисунок 12. Мониторинг функциональных модулей системы PALITRA

Во вкладке «Серверы» присутствует управление хранением данных (Рисунок 13).

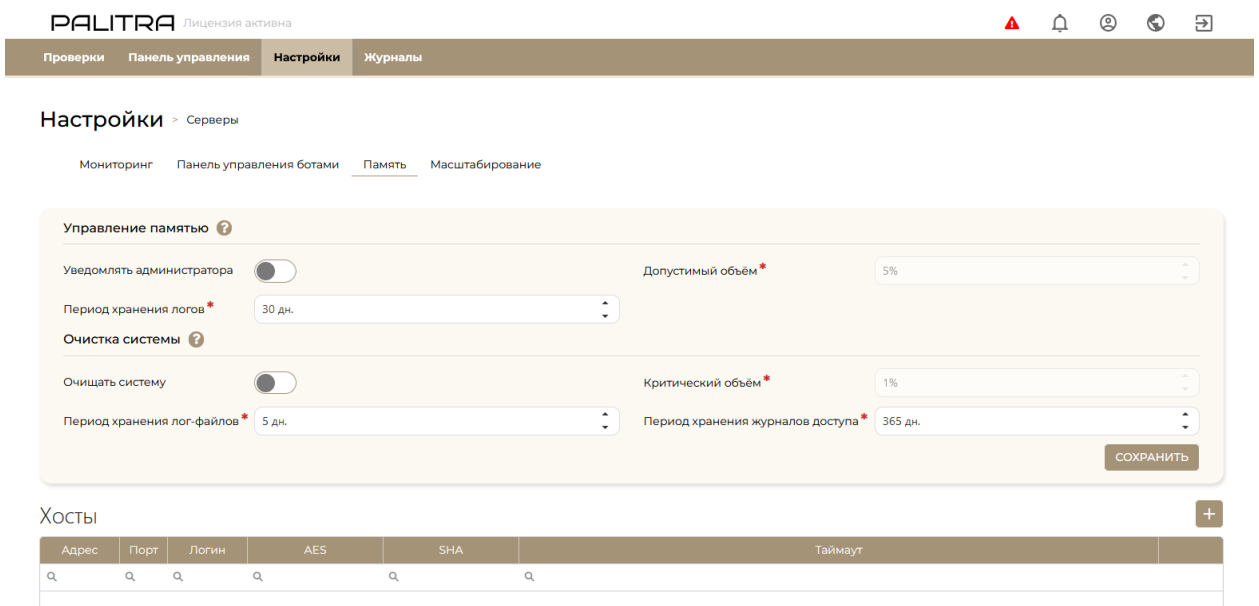


Рисунок 13. Управление хранением данных

Уведомлять администратора - при включении данного флага администратору системы будут приходить уведомления о превышении установленного допустимого объема.

Допустимый объём - объём свободной памяти, при достижении которого система отправит уведомления администраторам о состоянии оставшейся памяти на сервере системы.

Период хранения логов - выбор периода, в течение которого будут храниться лог-файлы.

8 Журналы

В разделе «Журналы» присутствует вкладка «Журнал событий», которая отображает значимые действия всех пользователей в системе PALITRA (Рисунок 14).

Дата события ↓	Имя пользователя	Важность	Устройство	Сообщение
		(Все)		
		Низкая		Редактирование пароля
		Низкая		Подтверждение пароля -> [login=PinkStar]
		Низкая		Подтверждение пароля
		Низкая		Редактирование пароля
		Низкая		Подтверждение пароля -> [login=test]
		Низкая		Подтверждение пароля
		Низкая		Подтверждение пароля
		Низкая		Подтверждение пароля -> [login=test]
		Низкая		Создание пользователя
		Низкая		Создание пользователя

Рисунок 14. Журнал событий

Вкладка «Журнал доступа» содержит данные по авторизации пользователей в веб-интерфейсе и подключения по API (Рисунки 15 - 16).

Создано ↓	Логин	Имя пользователя	Устройство	IP-адрес	Результат
28.03.2023, 21:35				10.0.8.66	Успешно
27.03.2023, 20:00				10.0.8.66	Успешно
26.03.2023, 21:02				10.0.8.66	Успешно
24.03.2023, 20:30				10.0.8.66	Успешно
24.03.2023, 20:29				10.0.8.66	Ошибка
21.03.2023, 23:04				10.0.8.66	Успешно
21.03.2023, 23:03				10.0.8.3	Успешно
21.03.2023, 22:52				10.0.8.66	Ошибка
21.03.2023, 22:52				10.0.8.66	Ошибка

Рисунок 15. Журнал авторизации пользователей

Вход пользователей Подключение API

Перетащите столбец сюда, чтобы сгруппировать по нему

Создано	Действие	Метод	Источник	Токен	Описание	Результат
29.03.2023, 19:17	Загрузка файла на проверку	POST	traffic	473920520-edf0-48a7-b11f-7839n9903c	Описание	Успешно
29.03.2023, 17:41	Загрузка файла на проверку	POST	api	53883520-hs78-48a7-s82ng-780c5dcfd8	Описание	Успешно
29.03.2023, 17:19	Загрузка файла на проверку	POST	user	7820-20s-hk23-93h6-2nx7-2730lk904nm	Описание	Успешно
29.03.2023, 17:09	Загрузка файла на проверку	POST	api	473920520-edf0-48a7-b11f-7839n9903c	Описание	Успешно
29.03.2023, 16:59	Загрузка файла на проверку	POST	traffic	92hnd00-ksn2-434c-c56g-250c5c67cfd8	Описание	Успешно
29.03.2023, 16:45	Загрузка файла на проверку	POST	traffic	53883520-edf0-48a7-b11f-780c5d77cfd8	Описание	Успешно
29.03.2023, 16:15	Загрузка файла на проверку	POST	traffic	53883520-edf0-48a7-b11f-780c5d77cfd8	Описание	Успешно
29.03.2023, 16:10	Загрузка файла на проверку	POST	api	7820-20s-hk23-93h6-2nx7-2730lk904nm	Описание	Успешно
29.03.2023, 15:55	Загрузка файла на проверку	POST	api	53883520-edf0-48a7-b11f-780c5d77cfd8	Описание	Успешно
29.03.2023, 15:19	Загрузка файла на проверку	POST	user	92hnd00-ksn2-434c-c56g-250c5c67cfd8	Описание	Успешно

Страница 1 из 13 < 1 2 3 4 5 ... 13 > 10 20 50 100

Рисунок 16. Журнал подключений по API