Athena Sandbox

СИСТЕМА ЗАЩИТЫ ОТ ЦЕЛЕНАПРАВЛЕННЫХ АТАК

Инструкция по развертыванию

на 28 листах

Москва
2021г.

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
© 2010-2021 ООО «АВ Софт»

Версия документа

Сентябрь 17, 2021.

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».

Документ может быть изменен без предварительного уведомления.

СОДЕРЖАНИЕ

1 Термины и определения

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

Таблица 1. Термины и определения

№	Термин	Определение
1.	Автоматический режим работы системы	Режим работы системы, в котором файлы и приложения, поступающие на интерфейс системы, автоматически загружаются в систему и анализируются на предмет нелегитимного поведения.
2.	Виртуальная машина	Программная система, эмулирующая аппаратное обеспечение, используемая в системе для проведения динамических исследований.
3.	Песочница	Изолированная среда с контролируемым набором ресурсом, которая имитируем персональный компьютер или мобильное устройство, для исполнения программного обеспечения и анализа его поведения.
4.	Сессия исследования программного обеспечения	Последовательность действий, включающая в себя запуск эмулируемой среды, загрузку и запуск в ней программного обеспечения, получение данных о поведении программного обеспечения, их последующий анализ, выгрузку программного обеспечения и остановку эмулируемой среды.
5.	Экспертный режим работы системы	Режим работы системы, в котором пользователь, имеющий роль аналитика, самостоятельно загружает файл или приложение для анализа в системе.
6.	Эталон	Модель сценария исследования в виртуальной машине, на основании которой осуществляется

№	Термин	Определение
		копирование виртуальных эмулируемых сред.
7.	Физическая машина	Физическая система, эмулирующая аппаратное обеспечение, используемая в системе для проведения динамических исследований.

2 Сокращения и значения

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

Таблица 2. Сокращения и значения

№	Сокращение	Значение
1.	AD	Active Directory
2.	API	Application programming interface
3.	CPU	Central processing unit
4.	FTP	File transfer protocol
5.	KVM	Kernel-based virtual machine
6.	LDAP	Lightweight directory access protocol
7.	MAC	Media access control
8.	MTA	Mail transfer agent
9.	OSI	Open systems interconnection model
10.	RAID	Redundant array of independent disks
11.	SAS	Serial attached SCSI
12.	SIEM	Security information and event management
13.	SSD	Solid-state drive
14.	SSL	Secure sockets layer
15.	USB	Universal serial bus
16.	VNC	Virtual network computing
17.	БД	База данных
18.	ВМ	Виртуальная машина

№	Сокращение	Значение
19.	ИС	Исследовательская среда
20.	ЛСС	Логическая схема сети
21.	МЭ	Межсетевой экран
22.	ОС	Операционная система
23.	ПО	Программное обеспечение

3 Общие сведения о программе

Программный комплекс «ATHENA SANBOX – система защиты от целенаправленных атак» (далее – ПК ATHENA) предназначен для усиления безопасности ИТ- инфраструктуры организаций. ПК ATHENA совмещает в себе классы систем мультисканера и «песочницы».

3.1. Основные технологии

Основные технологии, используемые в ПК ATHENA, представлены в таблице 3.

Таблица 3. Программное обеспечение для ПК ATHENA

№	Наименование программного обеспечения	Версии
1.	Android SDK	26.1.1
2.	Debian	9, 10
3.	Docker	18.09.4
4.	Flask	1.2
5.	Libvirt	5.6.0
6.	MongoDB	4.0.0
7.	PostgreSQL	9.4.21
8.	Python	3.5, 3.7
9.	QEMU	4.0.0
10.	RabbitMQ	3.7.17

3.2. Основные возможности

ПК ATHENA принимает на проверку файлы из различных источников, которые включают в себя:

- веб-трафик;
- почтовый трафик;

- сетевой трафик;
- мессенджеры;
- сервера и рабочие станции;
- ручная загрузка;
- API.

ПК ATHENA поддерживает проверку следующих типов объектов:

- файлов;
- архивов;
- веб-ссылок;
- мобильных приложений.

ПК ATHENA принимает на анализ любые типы файлов, примеры:

- исполняемые файлы (EXE, ELF, CMD);
- офисные документы (DOCX, XLSX, PPTX, PDF, RTF);
- мобильные приложения (APK);
- архивы, включая многотомные и защищенные паролем (ZIP, JAR);
- скрипты (BAT, SH).

В динамическом анализе поддерживаются следующие ОС:

- Microsoft Windows XP–10;
- Linux:
  - Debian 9.4.0;
  - Fedora 28;
  - RedOS «Муром»;
  - RHEL 8.0;
  - Astra Orel 2.12;
  - Ubuntu 18.04.

3.3. Возможности интеграции

ПК ATHENA имеет API-интерфейс для интеграции с другими системами. Интеграция системы возможна со следующими классами систем:

- NGFW;
- SIEM;
- «Песочницы»;
- Мультисканеры;
- Платформы на Deception.

3.4. Возможности развертывания

ПК ATHENA поддерживает развертывание на следующих типах инфраструктур:

- Физическая;
- Виртуальная;
- Облачная.

> **!** **Виртуальная и облачная инфраструктура должны обязательно поддерживать вложенную виртуализацию.**

4 Требования

4.1. Квалификационные

Перед началом работы с настоящим документов рекомендуется ознакомиться с руководством пользователя ПК ATHENA.

Требования к специалистам, осуществляющим администрирование ПК ATHENA:

- уверенное знание операционной системы (далее - ОС) на базе ядра Linux;
- знание основ сетевого администрирования;
- знание технологий контейнеризации (Docker);
- знание технологий виртуализации (QEMU-KVM, VMware).

4.2. Технологические

Для развёртывания ПК ATHENA необходимо использовать серверное оборудование с характеристиками не хуже, указанных в таблице 4.

Таблица 4. Характеристики оборудования

№	Параметр	Минимальные
1.	Модель процессора	Intel(R) Xeon(R) CPU E5-2603 v4 @1.7GHz
2.	Количество ядер процессора	12
3.	Оперативная память	16 ГБ
4.	Диск	200 GB
5.	Сеть	10/100/1000 Мбит/с (2 шт.)

4.3. Требования к браузерам

В таблице 5 представлены минимальные требования к версиям браузера, необходимые для функционирования веб-интерфейса ПК ATHENA.

Таблица 5. Минимальные версии браузера

№	Браузер	Версия браузера
1.	Chrome	80
2.	Edge	80
3.	Firefox	74
4.	Opera	67
5.	Safari	13.1
6.	Internet Explorer	Не поддерживается

4.4. Требования к сетевым схемам

Для интеграции и координации обновлений ПК ATHENA в ИТ-инфраструктуру инженерам компании АВ Софт необходимо предоставить логические схемы сети (далее – ЛСС) уровней L1/2 и L3 модели взаимодействия открытых систем OSI и таблицу маршрутизации.

ЛСС должна отображать компоненты сети и средства взаимодействия между ними. Подробное описание всех компонентов ЛСС представлено в таблице 6.

Таблица 6. Данные логической схемы сети

№	Параметры	Описание
1.	Подсети	LAN, VLAN
2.	Идентификаторы	Идентификаторы VLAN, маски и адреса
3.	Протоколы сетевой маршрутизации	IPv4 и IPv6

№	Параметры	Описание
4.	Сетевые устройства	Межсетевые экраны, маршрутизаторы, сетевые концентраторы

5 Структура программы

Программное обеспечение ПК «ATHENA» имеет архитектуру, показанную на рисунке 1.

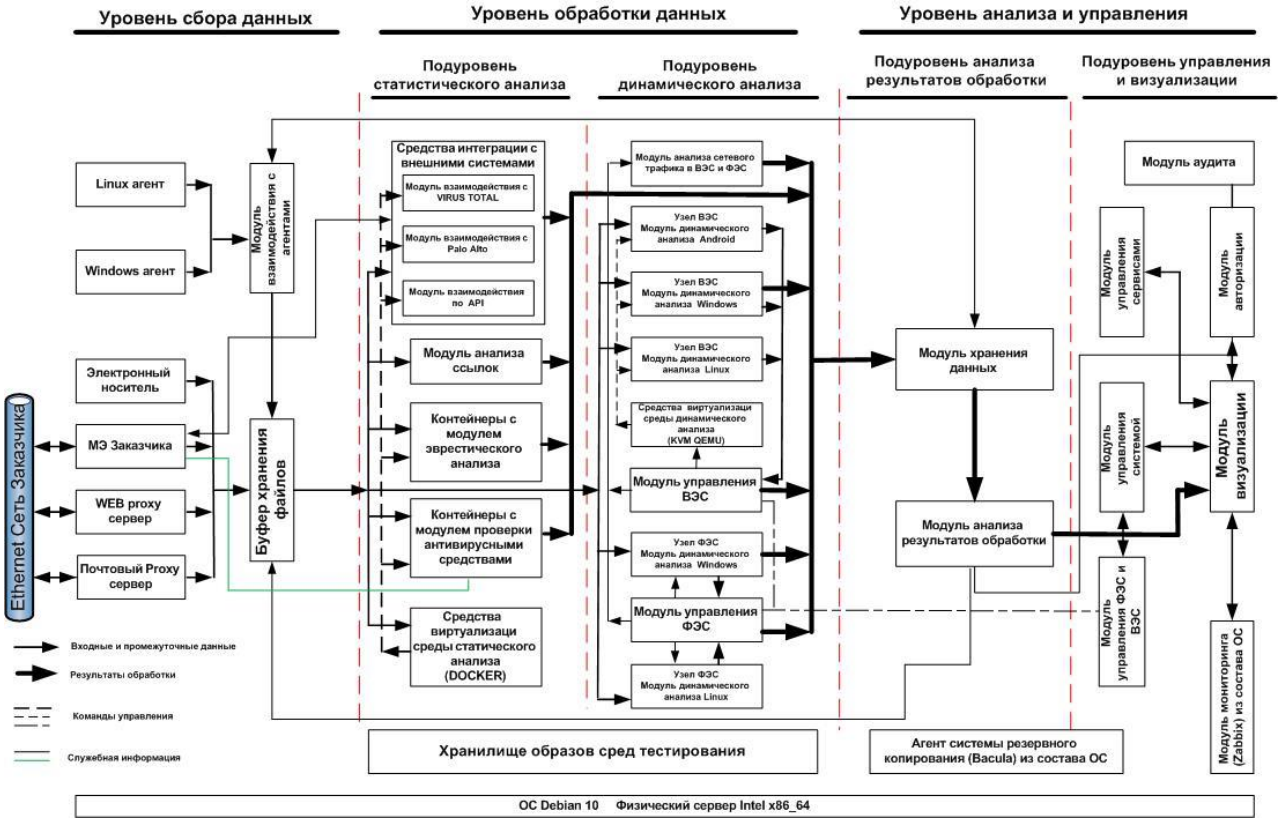

Рисунок 1. Архитектура ПО ПК ATHENA

В соответствии с приведённой архитектурой, структурная схема ПО ПК ATHENA будет иметь вид, приведённый на рисунке 2.

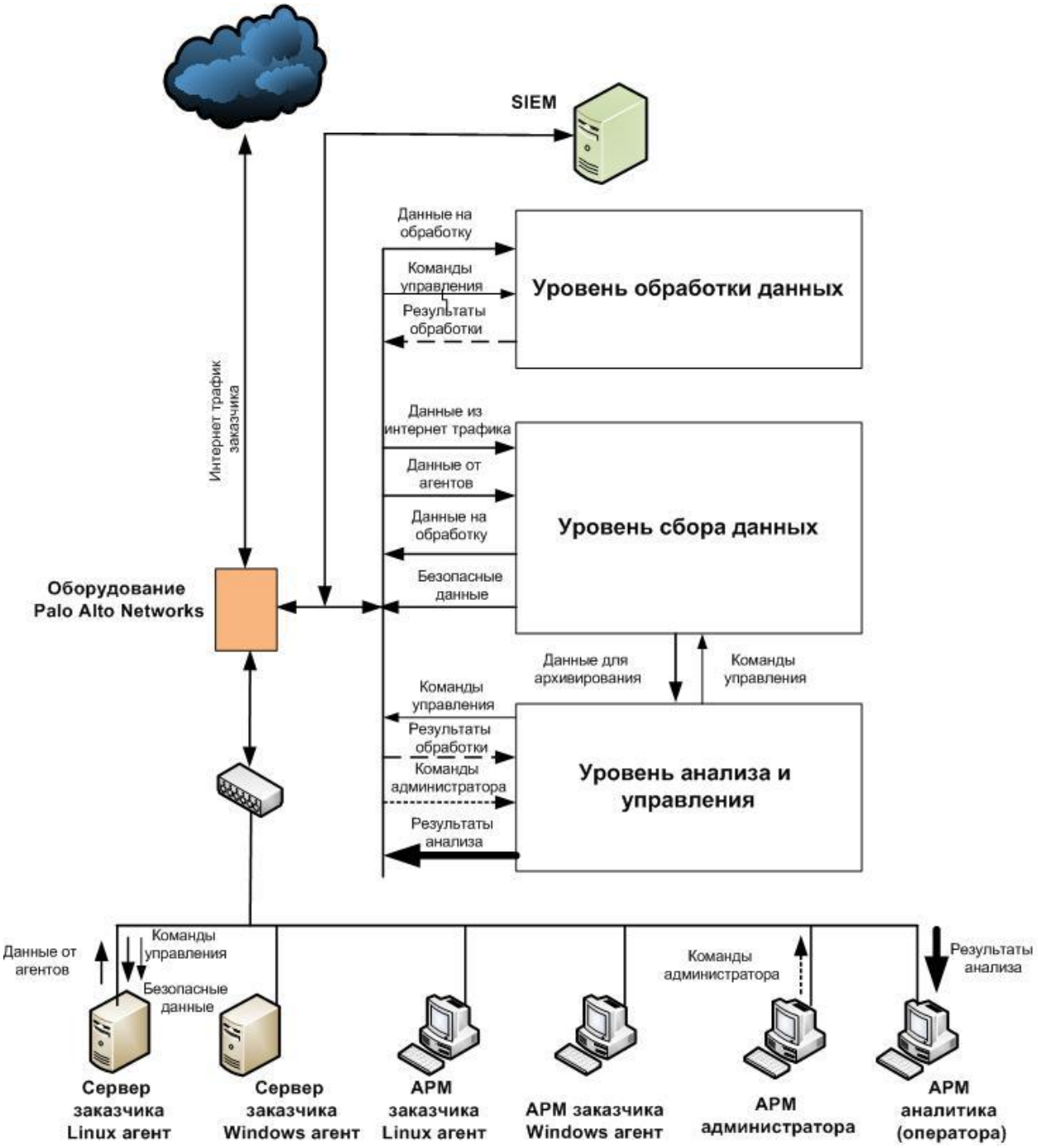

Рисунок 2. Структурная схема ПК ATHENA

Программное обеспечение каждого уровня ПК ATHENA является модульным и включает набор функциональных компонент. Каждый компонент имеет интерфейс управления и внутреннюю логику работы.

ПО ПК ATHENA имеет интерфейс управления. Команды пользователя проходят синтаксический анализ, затем вызываются интерфейсные методы компонентов, необходимые для выполнения команды.

Связь с аппаратными средствами серверов осуществляется через драйвер аппаратных средств.

Связи между основной процедурой и функциями программы выполняются в виде стандартных вызовов подпрограмм.

5.1. Уровень сбора данных

Основными элементами уровня сбора данных являются:

- прокси веб–сервер;
- прокси почтовый–сервер;
- ICAP-сервер.

Прокси сервера выполняют функцию буферного хранения запросов и данных, которыми обмениваются пользователи информационной системы Заказчика с внешними информационными ресурсами, на период анализа наличия в них вредоносного программного обеспечения.

ICAP-сервер обеспечивает получение данных из прокси веб–сервера и направление их на исследования.

5.2. Уровень обработки (исследований) данных

Основными элементами уровня обработки данных являются:

- файловое хранилище объектов исследования;
- среда исследования;
- средства управления средой исследования;
- модуль интеграции с внешними источниками информации об объектах исследования.

5.2.1. Файловое хранилище объектов исследования

Файловое хранилище обеспечивает безопасное хранение объектов, направленных на исследование. Загрузка объектов в файловое хранилище осуществляется из внешней сети через МЭ.

5.2.2. Среда исследования

Среда исследования предназначена для проведения статических и динамических исследований выбранных объектов. Она обеспечивает

проведение исследований как в виртуальных средах, так и на физических серверах.

Виртуальная среда исследования обеспечивает проведения исследований с использованием как виртуальных машин, так и контейнеров.

Типы используемых антивирусных средств, модулей синтаксического анализа файлов и нейронных сетей согласуются с Заказчиком.

Также подлежит согласованию с Заказчиком перечень программного обеспечения (ОС, СУБД, офисные средства и т.д.), используемый в среде тестирования для эмуляции программной среды Заказчика.

5.2.3. Средства управления средой исследования

Средства управления средой исследования позволяют управлять виртуальной средой исследования (виртуальной эмулируемой средой, далее - ВЭС) с помощью модуля управления ВЭС и физической средой исследования (физической эмулируемой средой, далее - ФЭС) с помощью модуля управления ФЭС.

Использование ФЭС целесообразно в следующих случаях:

– при проведении динамических исследований используется ПО (приложения) запуск которого в виртуальной среде не целесообразен или не возможен;

– при проведении динамических исследований требуется использование реальных устройств (принтеров, видеокарт и т.д.);

– у Заказчика имеются не используемые ПЭВМ (возможно устаревшие), которые возможно использовать для проведения динамических исследований, это позволит сэкономить средства на закупке вычислительных ресурсов.

5.2.4. Модуль интеграции с внешними источниками информации

Модуль интеграции с внешними источниками информации об объектах исследования предназначен для получения данных об анализируемом объекте из внешних аналитических ресурсов, например, баз данных антивирусных систем и аналитических веб-сервисов исследования ПО, а также об артефактах исследования ПО (ip-адреса и домены, к которым выполнялись подключения в ходе исследования поведения ПО).

5.3. Уровень анализа и управления

Уровень анализа и управления обеспечивает решение следующих основных задач:

- управление процессом исследования объектов в среде тестирования;
- анализ результатов исследования на основе базы решающих правил;
- отображение результатов анализа исследований;
- авторизацию пользователей ПК ATHENA;
- мониторинг состояния системы.

Уровень анализа и управления можно разделить на два подуровня:

- подуровень анализа результатов обработки;
- подуровень управления и визуализации.

Подуровень анализа результатов обработки включает:

- модуль хранения данных исследований;
- модуль анализа результатов исследований.

Подуровень управления и визуализации включает:

- модуль управления;
- модуль визуализации;
- модуль управления средой исследования;
- модуль управления сервисами;
- модуль авторизации;
- модуль мониторинга состояния системы.

6 Установка серверного программного обеспечения

Серверное программное обеспечение ПК ATHENA поставляется в виде образов виртуальных машин. Для получения образа виртуальной машины с установленным и предварительно сконфигурированным программным обеспечением необходимо обратиться в центральный офис компании AVSoft по телефону: **+7 (495) 988-92-25** или по e-mail: **office@avsw.ru**.

После получения образа и загрузки на рабочее место необходимо произвести развертывание. Для этого в гипервизоре выполнить следующие действия.

В главном меню программы VMware выбрать пункт «Create/Register VM» (Рисунок 3).

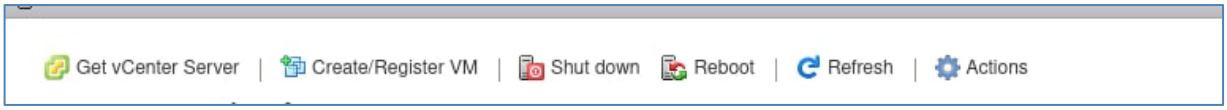

Рисунок 3. Главное меню программы VMware

Далее в отобразившемся окне выбрать пункт «Deploy a virtual machine from an OVF or OVA file» и нажать кнопку «Next» (Рисунок 4).

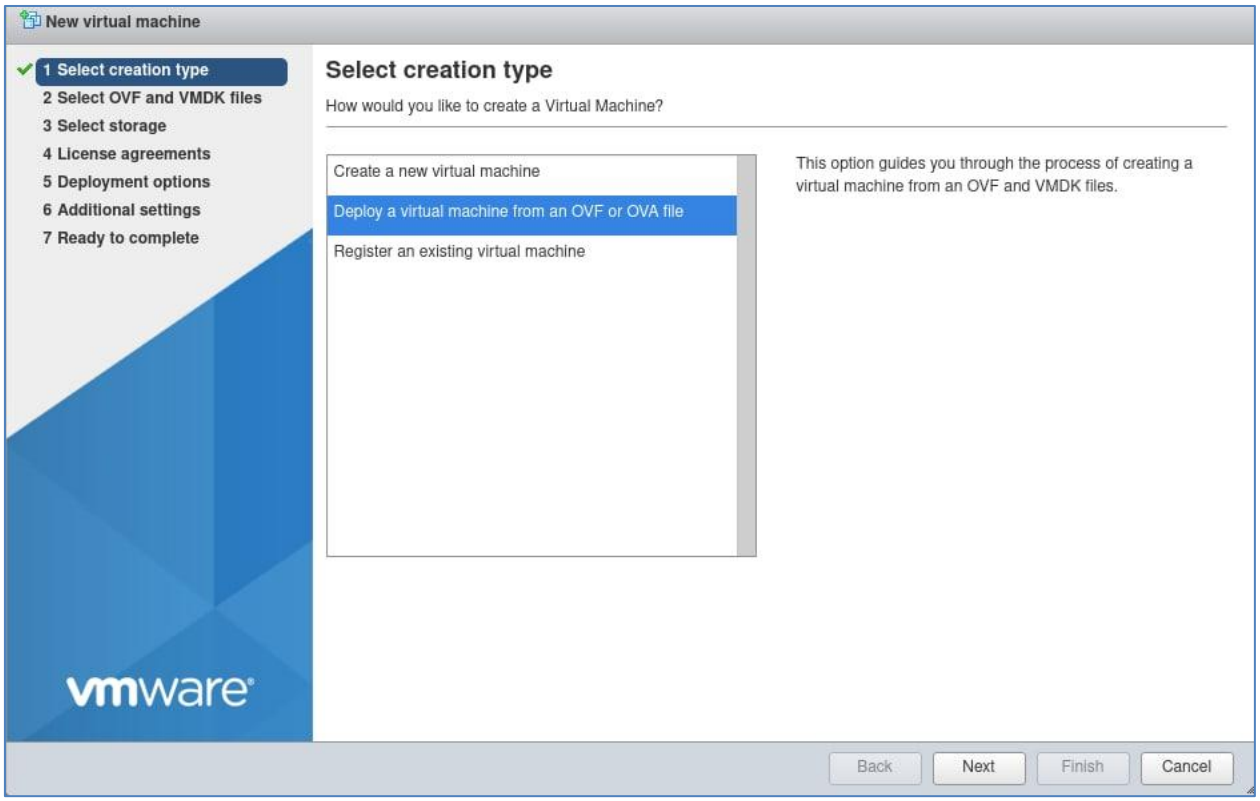

Рисунок 4. Выбор типа создаваемой виртуальной машины

Далее в отобразившемся окне необходимо ввести имя для добавляемой виртуальной машины и выбрать/перетащить файл виртуальной машины (*.ovf/*.ova) и нажать кнопку «Next» (Рисунок 5).

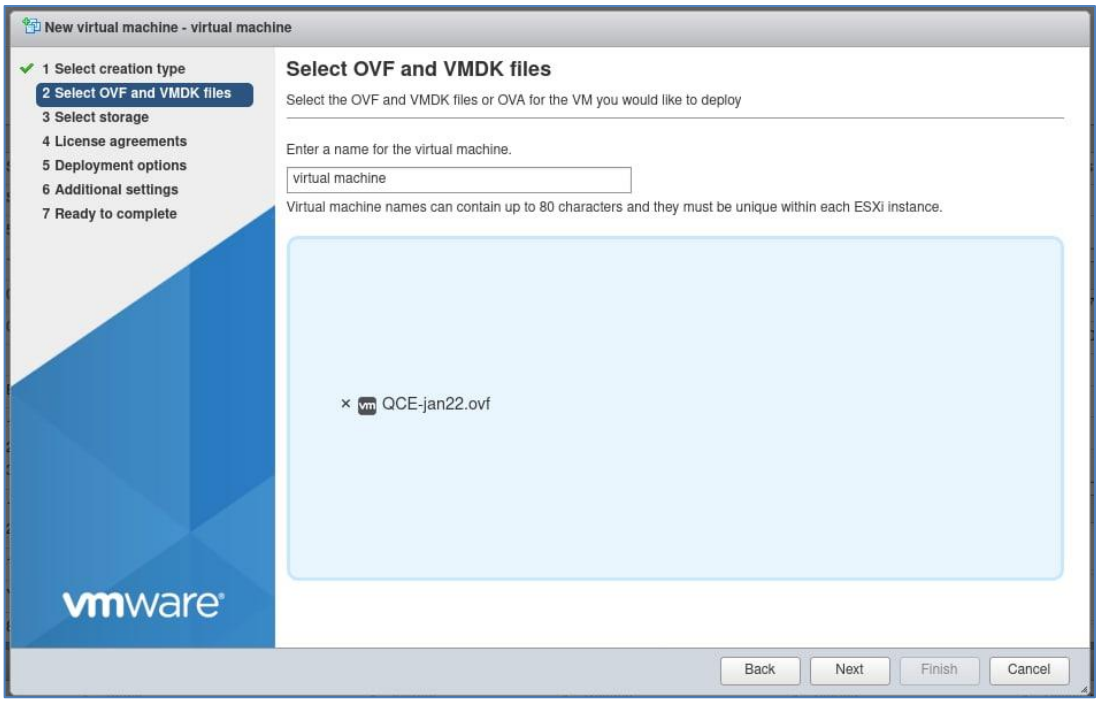

Рисунок 5. Выбор файла OVF

Далее необходимо выбрать хранилище для размещения виртуальной машины (Рисунок 6).

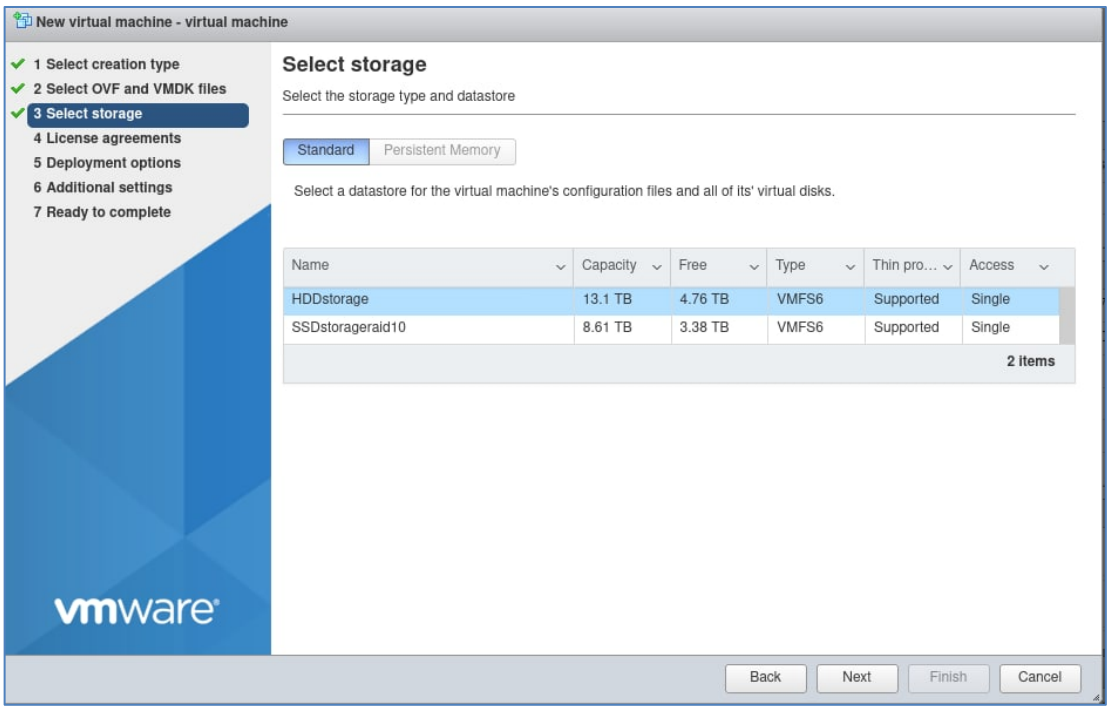

Рисунок 6. Выбор хранилища

Далее необходимо указать параметры развертывания как показано на рисунке ниже и нажать кнопку «Next» (Рисунок 7).

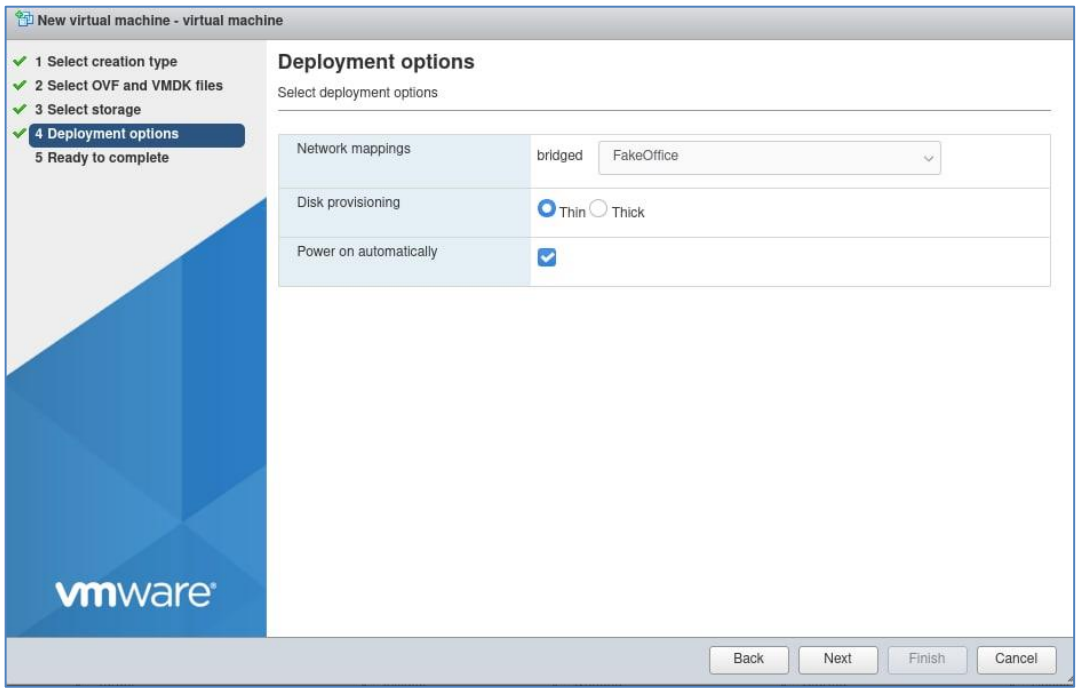

Рисунок 7. Выбор параметров развертывания

Далее, после нажатия на кнопку «Finish» автоматически осуществится запуск виртуальной машины (Рисунок 8).

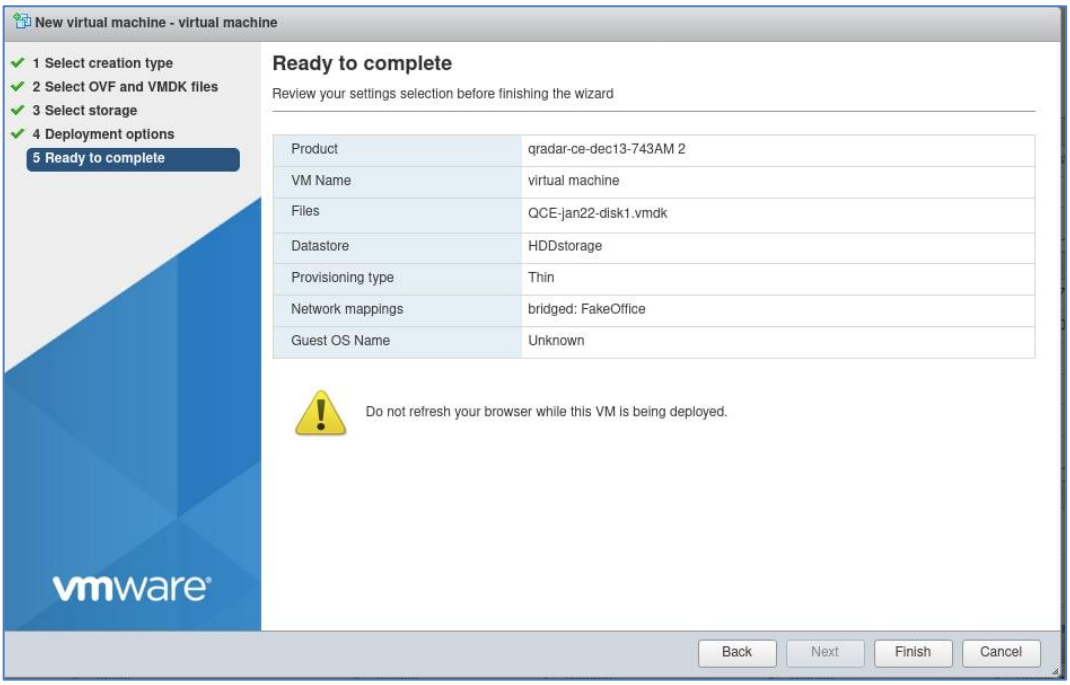

Рисунок 8. Завершающий этап создания виртуальной машины

7 Активация и настройки

После установки серверной части необходимо выполнить авторизацию в графическом интерфейсе ПК ATHENA и активировать лицензию для работы с ней.

Для авторизации в системе пользователем с правами администратора, необходимо ввести следующие учетные данные: «administrator/kRG4iaaB!».

7.1. Активация лицензии

Для активации лицензии на использование ПК ATHENA необходимо перейти в раздел «Настройки» → «Основные» → «Лицензия» (Рисунок 20).

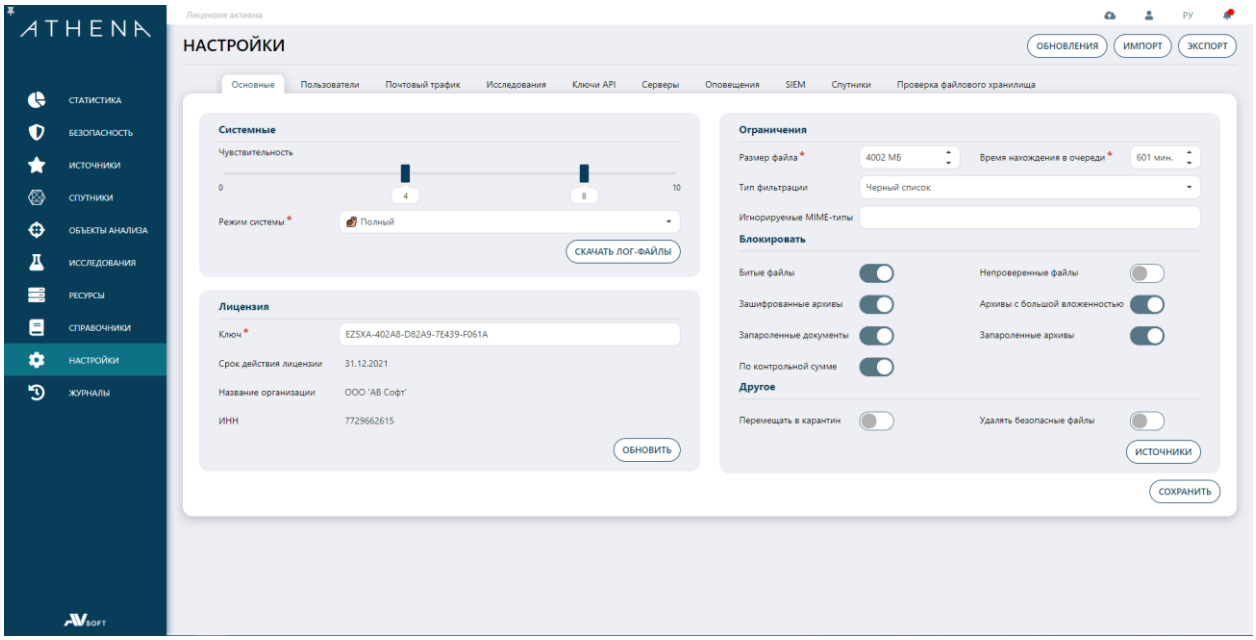

Рисунок 9. Активация лицензии

Далее необходимо в поле «Ключ» указать ключ активации лицензии, предоставленный поставщиком программного обеспечения, который автоматически заполнить следующие поле в функциональном блоке:

- Срок действия лицензии;
- Название организации;
- ИНН.

После заполнения поля «Ключ» необходимо нажать кнопку «Обновить». Если действие выполнено успешно, то отобразится сообщение, что «Настройки сохранены».

7.2. Раздел «Настройки»

В разделе «Настройки» осуществляется настройка всех модулей системы. Также в данном разделе реализована возможность импорта и экспорта настроек системы из файла и в файл соответственно.

Для экспортирования настроек предназначена кнопка «Экспорт», расположенная в правой верхней части экрана, после нажатия на которую автоматически начнется выгрузка файла с сохраненным настройками системы. Пример выгрузки файла с сохраненными настройками представлен ниже (Рисунок 10).

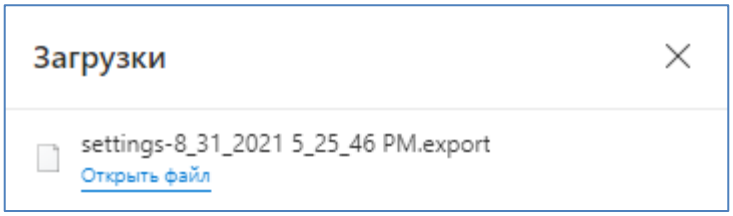

Рисунок 10. Загрузка файла с сохраненными настройками

Для импортирования настроек предназначена кнопка «Импорт», расположенная в правой верхней части экрана, после нажатия на которую отобразится форма «Импорт» (Рисунок 11).

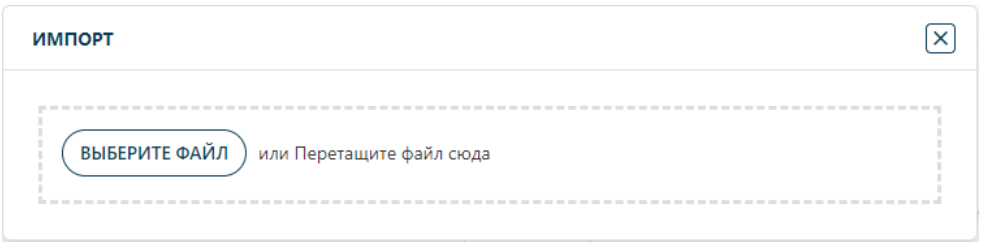

Рисунок 11. Форма «Импорт»

Далее необходимо выбрать/перетащить файл, содержащий сохраненные настройки системы. После этого в нижней части экрана отобразится уведомление об успешном применении сохраненных настроек (Рисунок 12).

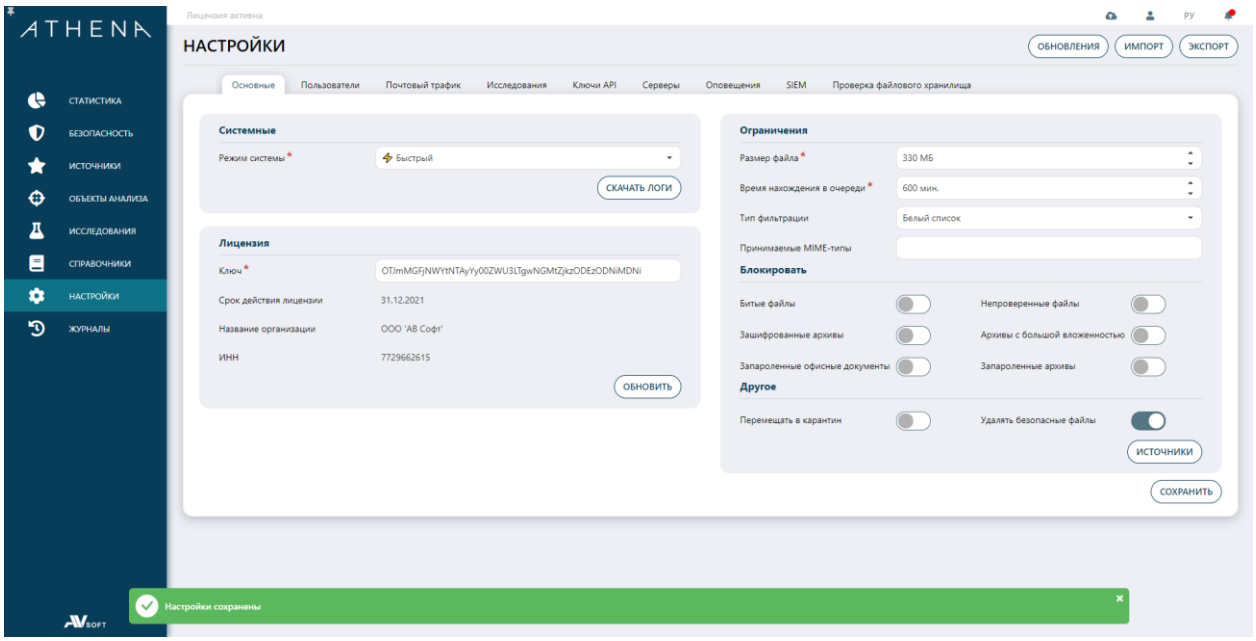

Рисунок 12. Уведомление об успешном применении сохраненных настроек

Во вкладке «Основные» администратор может выполнить настройку общих системных параметров, описанных в таблице 7.

Таблица 7. Описание общих системных настроек

№	Параметры	Описание
1.	**Системные**	
1.1.	Чувствительность	Пороговые лимиты аналитик динамического анализа, рекомендуемые по умолчанию: 0 - 4 (безопасный вердикт) 8 – 7 (подозрительный вердикт) 8 – 10 (вредоносный вердикт) (Подробнее можно ознакомиться в руководстве аналитика ПК ATHENA).
1.2.	Режим системы	Режимы работы системы, которые можно переключать в зависимости от целей использования системы. Полный режим включает в себя все проверки файла в статическом анализе и получение полной информации по его синтаксической

№	Параметры	Описание
		структуре, что требует от системы ресурсов больше, чем в быстром режиме. Быстрый режим исключает долгие по времени этапы проверки в статическом анализе и предназначен для быстрой проверки больших объемов трафика. Данный режим исключает: 1) Все парсеры кроме apk, ole, pdf 2) Поиск ссылок 3) Проверка типов файлов в архивах
2.	**Лимиты**	
2.1.	Размер файла (байт)	Максимальный размер файла, загружаемый в систему на проверку.
2.2.	Тип фильтрации	Черный список – проверяется все, кроме указанных в поле ниже MIME-типов. Белый список – проверят только те MIME типы, что указано в поле ниже.
2.3.	Игнорируемые MIME-типы	MIME-типы, которые не допускаются на проверку в систему (применимо только для черного списка).
2.4.	Принимаемые MIME-типы	MIME-типы, которые допускаются на проверку в систему (применимо только для белого списка).
3.	**Системные операции**	
3.1.	Очистка	Удаление всех исследований в очереди на исследование.
3.2.	Повтор	Повторная отправка на анализ ошибочных исследований (лимит не более 500 последних

№	Параметры	Описание
		не проверенных).
4.	**Лицензия**	
4.1.	Ключ	Ключ активации лицензии.
4.2.	Срок действия лицензии	Период действия ключа активации лицензии.
4.3.	Название организации	Наименование организации, которой принадлежит ключ активации лицензии.
4.4.	ИНН	ИНН организации, которой приобрела ключ активации лицензии.

7.3. Управление пользователями

В ПК ATHENA управление пользователями осуществляется во вкладке «Пользователи» (Рисунок 24).

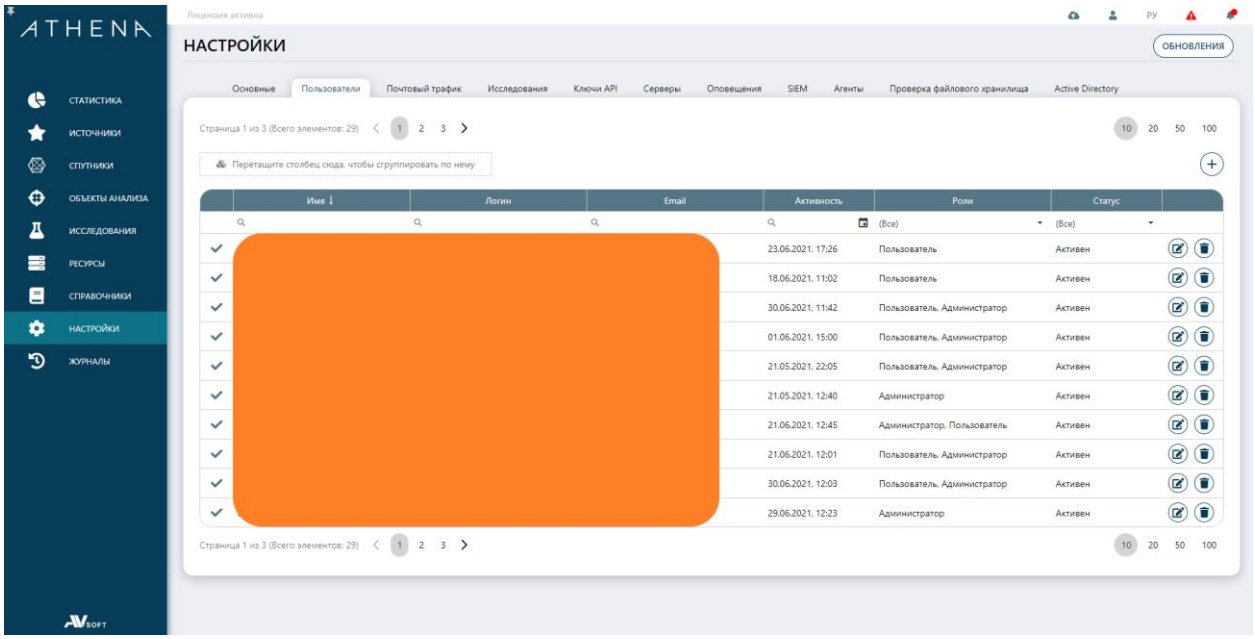

Рисунок 13. Вкладка «Пользователи»

Для добавления нового пользователя в ПК ATHENA необходимо нажать на кнопку с иконкой «Добавить», далее осуществится переход в форму для заполнения регистрационных данных о новом пользователе (Рисунок 25).

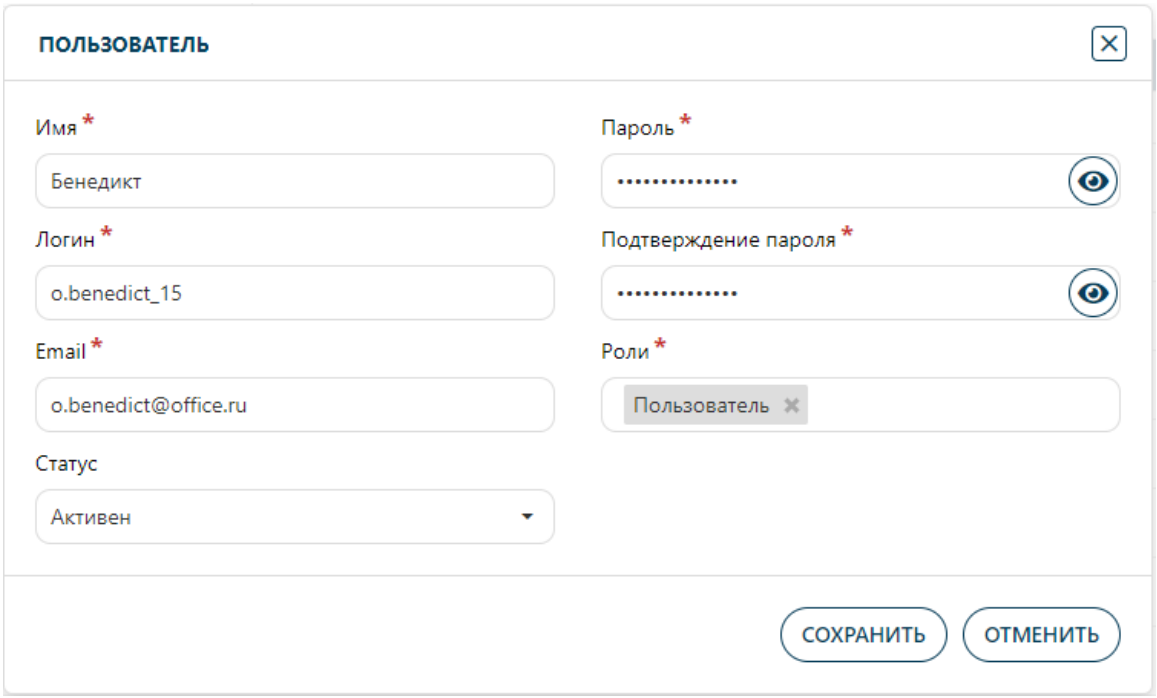

Рисунок 14. Добавление нового пользователя

Далее необходимо указать параметры полей, описанные в таблице 8.

Таблица 8. Описание параметров для создания нового пользователя

№	Параметры	Описание
1.	Имя	Имя пользователя в системе.
2.	Логин	Логин для авторизации в системе.
3.	Email	Электронная почта для подтверждения авторизации и восстановления пароля.
4.	Статус	Статус пользователя в системе, который имеет два состояния: – Заблокирован; – Активен.
5.	Пароль	Пароль для входа в систему.
6.	Подтверждение пароля	Подтверждение пароля для входа в систему.
7.	Роли	Пользовательские роли в системе с предустановленным набором прав:

№	Параметры	Описание
		– Пользователь (не имеет доступа к настройкам системы) – Администратор (имеет доступ ко всем разделам в системе)

По окончании ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что новый созданный пользователь отобразился в общей таблице всех пользователей системы.

Для блокировки пользователя в системе необходимо нажать на иконку «Редактировать» и в окне профиля пользователя «Пользователь» в поле «Статус» в выпадающем меню выбрать «Заблокирован», далее необходимо нажать кнопку «Сохранить» и удостовериться, что в общей таблице пользователей измененный статус пользователя отобразился корректно.