



Athena Sandbox

**СИСТЕМА ЗАЩИТЫ ОТ
ЦЕЛЕНАПРАВЛЕННЫХ АТАК**

**Описание процессов, обеспечивающих поддержание
жизненного цикла**

**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	Перечень сокращений	4
2	Перечень терминов и определений	5
3	Общие положения	6
3.1	ПО, необходимое для функционирования ПК ATHENA	6
3.2	Языки программирования, на которых написано изделие	6
4	Процессы, обеспечивающие поддержание жизненного цикла	7
4.1	Требования к квалификации специалистов	7
5	Первичная настройка ПК ATHENA	8
6	Обновление ПК ATHENA	11
6.1	Веб-интерфейс	11
6.2	Консоль	13
6.3	Физический носитель	13
7	Резервное копирование	14
7.1	Автономные сервисы	14
7.2	Клиент-серверные сервисы	14
7.3	Монтирование диска	15
8	Техническая поддержка пользователей	17
8.1	Требования к квалификации специалистов тех. поддержки	17

1 Перечень сокращений

В настоящем документе используется перечень сокращений, представленный в таблице 1.

Таблица 1. Перечень сокращений

№ п/п	Сокращение	Значение
1.	IP-адрес	Уникальный сетевой идентификатор устройства (от англ. Internet Protocol)
2.	TCP/IP	Протокол управления передачей/Межсетевой протокол (от англ. Transmission Control Protocol/Internet Protocol)
3.	URL	Унифицированный указатель ресурса (от англ. Uniform Resource Locator)
4.	БД	База данных
5.	Модель OSI	Сетевая модель стека сетевых протоколов OSI/ISO (от англ. The Open Systems Interconnection model)
6.	ОЗУ	Оперативное запоминающее устройство
7.	ОС	Операционная система
8.	ПК	Программный комплекс
9.	ПЭВМ	Персональная электронно-вычислительная машина
10.	СУБД	Система управления базами данных

2 Перечень терминов и определений

В настоящем документе используются термины и определения, представленные в таблице 2.

Таблица 2. Перечень терминов и определений

№ п/п	Термин	Определение
1.	Docker-compose	Инструментальное средство, входящее в состав Docker. Предназначено для решения задач, связанных с развёртыванием проектов.
2.	СУБД MongoDB	Документоориентированная система управления БД, не требующая описания схемы таблиц.
3.	СУБД Postgres	Свободная объектно-реляционная система управления БД.

3 Общие положения

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

3.1 ПО, необходимое для функционирования ПК ATHENA

ПК ATHENA функционирует в среде ОС Debian не ниже 9 (девятой) версии, установленной на ПЭВМ с аппаратной платформой Intel x86_64.

Для эксплуатации ПК ATHENA на рабочем месте необходимо использовать веб-браузеры с версиями не ниже, указанных в таблице 3. **Ошибка! Источник ссылки не найден..**

Таблица 3. 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

3.2 Языки программирования, на которых написано изделие

Программное обеспечение входящее в состав ПК ATHENA написано на следующих языках программирования: Assembler, Bash, C, C++, C#, Python.

4 Процессы, обеспечивающие поддержание жизненного цикла

Поддержание жизненного цикла ПК ATHENA осуществляется за счет сопровождения комплекса, включающего в себя следующие сервисные процессы:

1. Поставка и настройка программного комплекса (первичная и в процесс эксплуатации);
2. Техническая поддержка пользователей;
3. Проведение обновления программного комплекса.

Сопровождение ПК ATHENA необходимо для:

- Обеспечения гарантий корректного функционирования ПК и дальнейшего развития её функционала;
- Отсутствия простоя в работе по причине невозможности функционирования ПК (аварийная ситуация, ошибки в работе и т.п.).

4.1 Требования к квалификации специалистов

Специалисты, осуществляющие техническое сопровождение ПК ATHENA, должны обладать следующими навыками и знаниями:

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

5 Первичная настройка ПК ATHENA

Данный раздел предназначен для первичной настройки ПК ATHENA и дальнейшей работы в системе.

Для авторизации в системе необходимо в адресной строке браузера ввести URL ATHENA. Внешний вид страницы авторизации показан на рисунке 1. После прохождения авторизации осуществляется переход в веб-интерфейс ПК ATHENA.

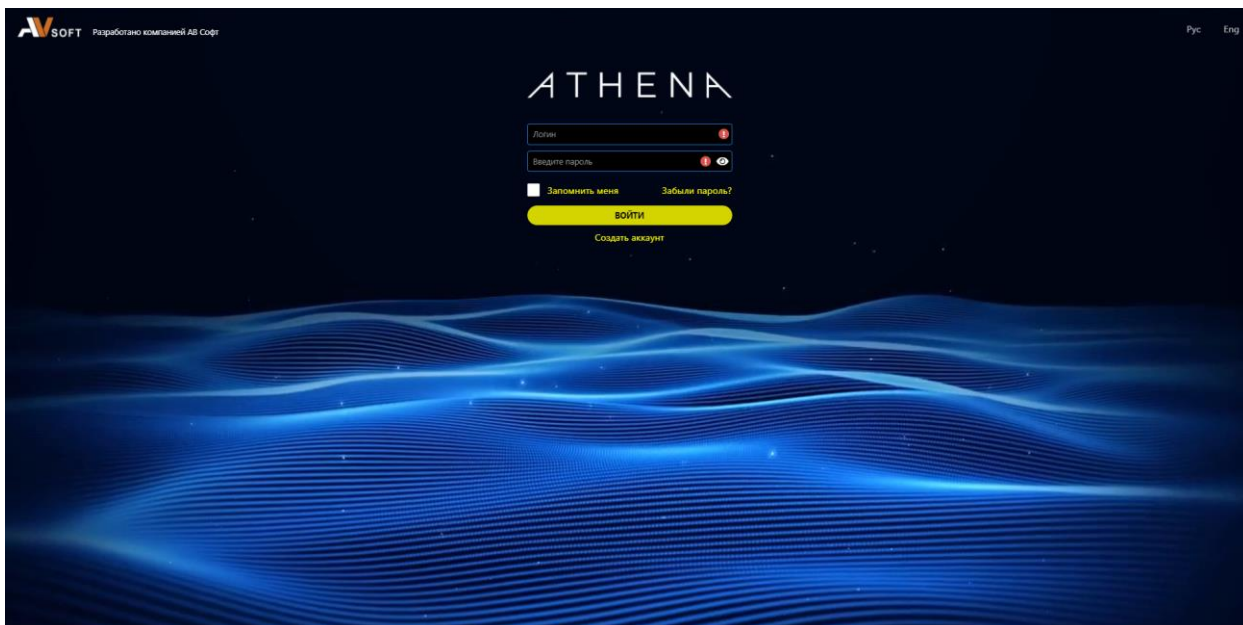


Рисунок 1. Страница авторизации в ПК ATHENA

Раздел «Настройки» доступен администратору ПК ATHENA и не доступен в пользовательском интерфейсе.

Во вкладке «Пользователи» находится информация о пользователях ПК ATHENA (Рисунок 2).

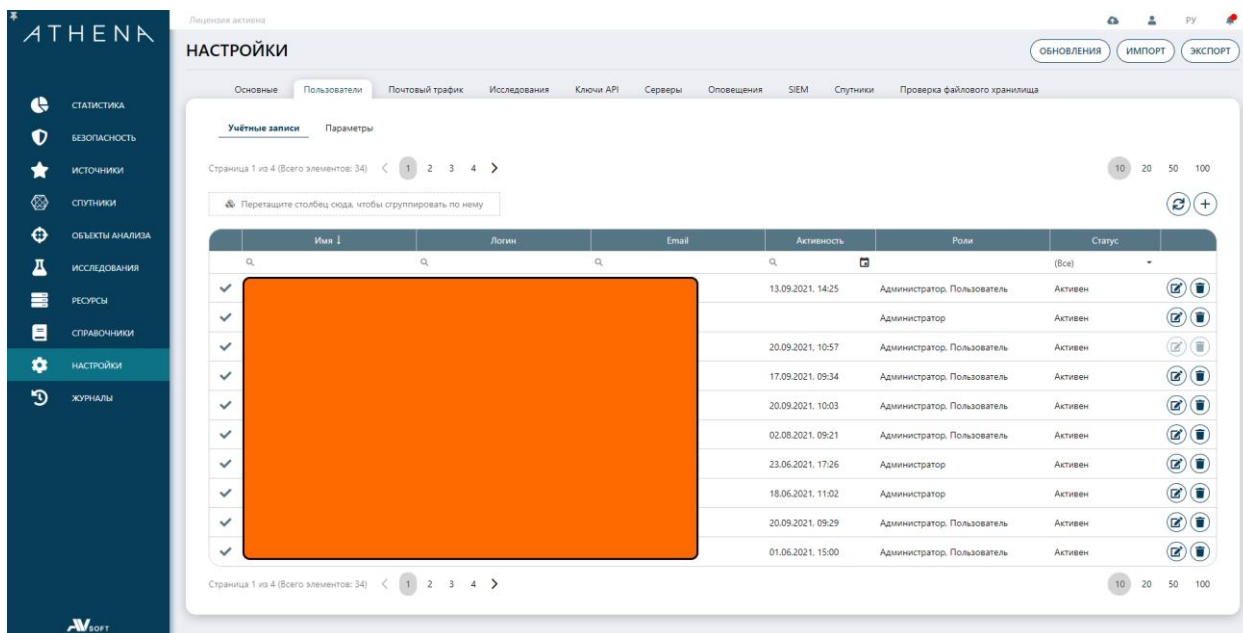


Рисунок 2. Раздел «Настройки» вкладка «Пользователи»

Для регистрации нового пользователя в ПК ATHENA необходимо на странице авторизации нажать кнопку «Создать аккаунт» и заполнить все требуемые поля (Рисунок 3).

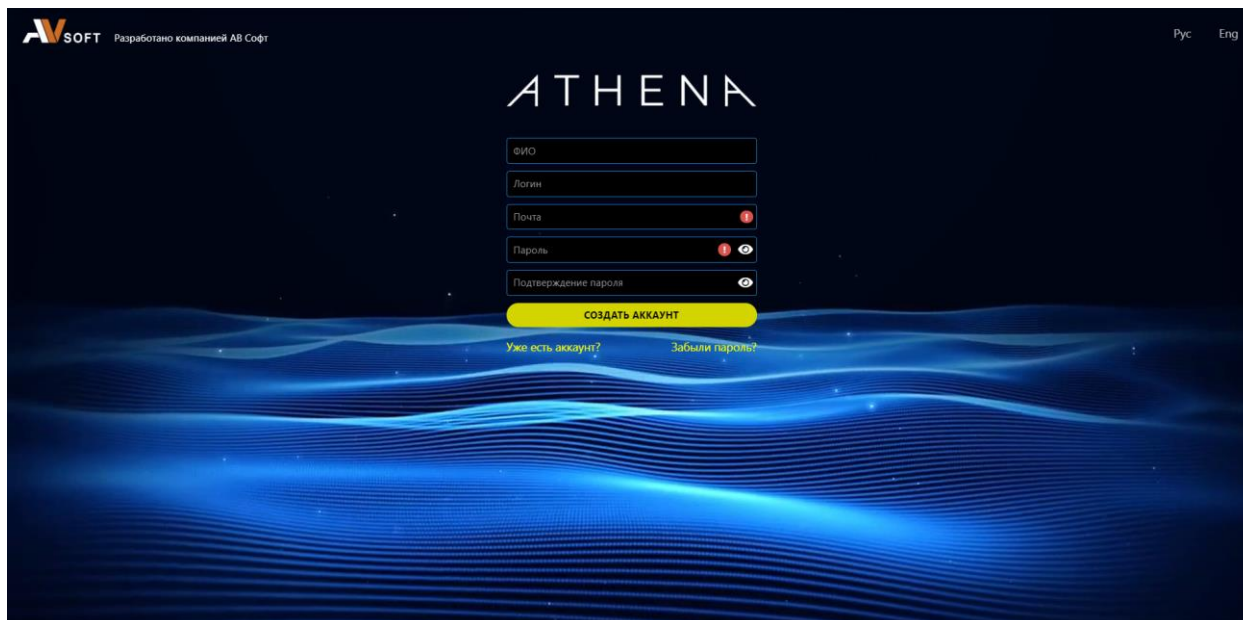


Рисунок 3. Заполнение формы регистрации

После завершения ввода данных необходимо нажать кнопку «Создать аккаунт». Далее администратор ПК ATHENA должен выполнить подтверждение нового пользователя в разделе «Настройки» во вкладке «Пользователи», где необходимо нажать на иконку «Изменить статус» и выполнить подтверждение пользователя. После этого пользователь сможет осуществить авторизацию в ПК ATHENA.

При необходимости блокировки пользователя, но не удаления, необходимо в разделе «Настройки» во вкладке «Пользователи» нажать на иконку «Редактировать» и выбрать блокировку пользователя.

6 Обновление ПК ATHENA

Система ATHENA поддерживает два типа обновления:

- по сети;
- локально с помощью с usb накопителя.

Для обновления по сети можно использовать системную консоль и веб-интерфейс системы.

6.1. Веб-интерфейс

Для применения нового релиза посредством веб-интерфейса необходимо перейти в разделе «Настройки» и воспользоваться кнопкой «Обновить» (Рисунок 4).

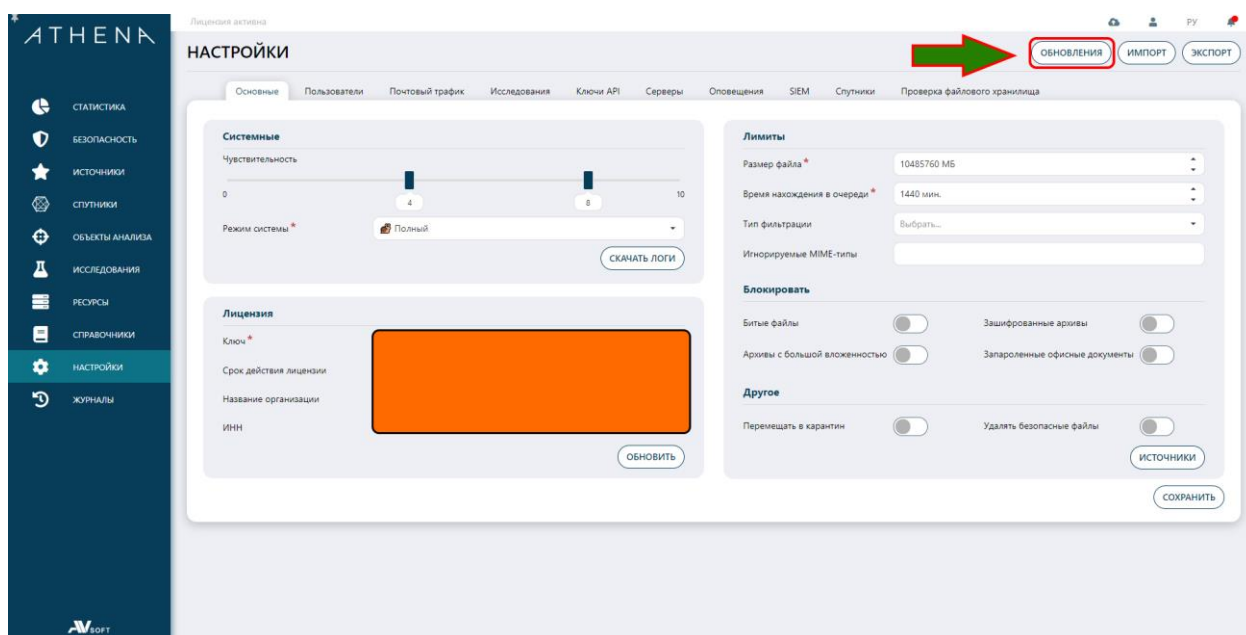


Рисунок 4. Активация функции обновления системы

Далее осуществится переход в сервис обновлений, в котором будут представлены наименования модулей и версии пакетов. Для обновления информации о версиях пакетов необходимо нажать кнопку «Обновить репозиторий» (Рисунок 5).

СЕРВИС ОБНОВЛЕНИЙ

Обновить репозиторий

Перетащите столбец сюда, чтобы сгруппировать по нему

Найти...

Наименование	Текущая	Последняя	Статус	
analytics		1.1.9	Не установлен	🔄
athena-analytics		1.3.2.12	Не установлен	🔄
athena-analytics-en		1.3.6	Не установлен	🔄
athena-analytics-ru	1.3.6	1.3.6	Установлен	🔄
athena-commands-pm		1.3.0	Не установлен	🔄
athena-commands-vm		1.2.16	Не установлен	🔄
athena-dynamic		1.0	Не установлен	🔄
athena-interface	1.9.6	1.9.6	Установлен	🔄
athena-service-agents	1.3.0	1.3.1	Установлен	🔄
athena-service-analytic	2.5.6	2.5.6	Установлен	🔄
athena-service-audit	1.0.9	1.0.9	Установлен	🔄
athena-service-discovery	1.2.3	1.2.3	Установлен	🔄
athena-service-linkanalytic	1.1.1	1.1.1	Установлен	🔄
athena-service-maintance	1.1.2	1.1.2	Установлен	🔄
athena-service-mobile	1.0.4	1.0.4	Установлен	🔄
athena-service-networkanalytic	1.2.6	1.2.6	Установлен	🔄
athena-service-reports	1.1.7	1.1.7	Установлен	🔄
athena-service-researchcomparator	1.1.7	1.1.7	Установлен	🔄
athena-service-researches	1.4.5	1.4.6	Установлен	🔄
athena-service-researchevents	1.6.7	1.6.7	Установлен	🔄

10 20 50

1 2 3 4 5 6 7

Рисунок 5. Сервис обновлений

Для обновления пакета необходимо нажать на иконку «Обновить», которая откроет окно обновлений пакета (Рисунок 6).

СЕРВИС ОБНОВЛЕНИЙ / ATHENA-ANALYTICS

Информация Обновления Журнал

Имя: athena-analytics

Текущая версия: 0.0.0

Доступная версия: 1.3.2.12

Состояние: Не установлен

Архитектура: amd64

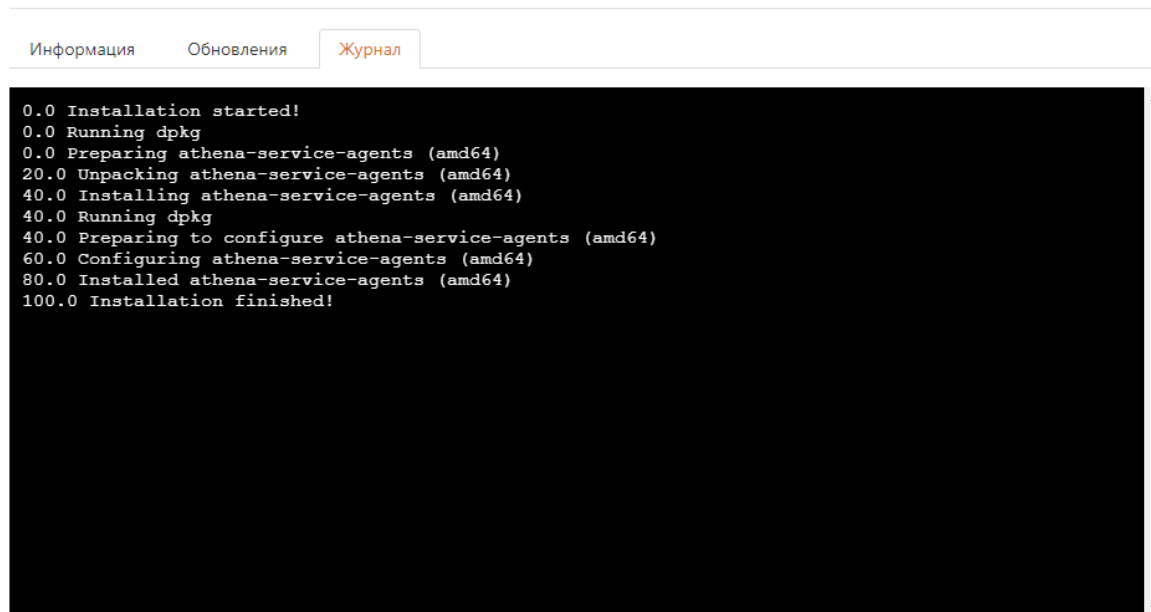
Обновить

Рисунок 6. Обновление пакета

В открывшемся окне необходимо нажать кнопку «Обновить», которая

отобразит системный журнал обновления пакета (Рисунок 7).

СЕРВИС ОБНОВЛЕНИЙ / ATHENA-SERVICE-AGENTS



```
Информация Обновления Журнал
0.0 Installation started!
0.0 Running dpkg
0.0 Preparing athena-service-agents (amd64)
20.0 Unpacking athena-service-agents (amd64)
40.0 Installing athena-service-agents (amd64)
40.0 Running dpkg
40.0 Preparing to configure athena-service-agents (amd64)
60.0 Configuring athena-service-agents (amd64)
80.0 Installed athena-service-agents (amd64)
100.0 Installation finished!
```

Рисунок 7. Системный журнал обновления пакета

При успешном завершении обновления вывод в системном журнале будет заканчиваться ответом «Installation finished».

6.2. Консоль

Для обновления через консоль необходимо выполнить авторизацию по SSH, далее выполнить команду просмотра списка доступных пакетов для обновления:

```
sudo apt update
```

Далее необходимо скачать и установить все доступные для обновления пакеты следующей командой:

```
sudo apt upgrade
```

6.3. Физический носитель

Физический носитель с репозиториями пакетов для обновления выдается инженерами компании АВ Софт.

7 Резервное копирование

Резервное копирование данных системы ATHENA может быть реализовано с использованием систем резервного копирования следующих типов:

- системы резервного копирования, имеющие клиент-серверную архитектуру;
- автономные системы резервного копирования.

Резервному копированию (РК) подлежат следующая информация:

- системные программы и наборы данных - невозобновляемому (однократному, эталонному) РК;
- прикладное программное обеспечение и наборы данных - невозобновляемому РК;
- наборы данных, генерируемые в течение операционного дня и содержащие ценную информацию (журналы транзакций, системный журнал и т.д.) - периодическому возобновляемому РК.

Безопасность резервных копий обеспечивается:

- хранением резервных копий вне системы (в других помещениях, на другой территории);
- соблюдением мер физической защиты резервных копий;
- строгой регламентацией порядка использования резервных копий.

7.1. Автономные сервисы

Автономные системы резервного копирования не требуют использования дополнительного серверного оборудования. Они позволяют осуществлять резервное копирование на внешние носители данных.

7.2. Клиент-серверные сервисы

Системы резервного копирования, имеющие клиент-серверную архитектуру, имеют в своём составе серверное программное обеспечение, устанавливаемое на сервер резервного копирования, и клиентское программное обеспечение для различных версий ОС, устанавливаемое на рабочие станции для копирования данных.

В качестве такой системы, для резервного копирования данных системы ATHENA может использоваться система резервного копирования, имеющаяся у Заказчика. При отсутствии у Заказчика штатной системы резервного копирования, она может быть создана специально для системы ATHENA. В качестве программного обеспечения рекомендуется использовать кроссплатформенное клиент-серверное программное обеспечение Duplicati.

7.3. Монтирование диска

Для переноса резервной копии на диск необходимо осуществить его монтирование в систему. Для этого необходимо выполнить команду вывода списка доступных внутренних и внешних дисков:

```
fdisk -l
```

Результат выполнения команды представлен на рисунке 8.

```
b_demchenko@athena-dev-04:/$ sudo fdisk -l
Disk /dev/sda: 3.7 TiB, 3997997989888 bytes, 7808589824 sectors
Disk model: Logical Volume
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: gpt
Disk identifier: 95FF8BCF-06F0-4685-AB94-AF158C4FC582

Device            Start      End      Sectors  Size Type
/dev/sda1         1536     1050623  1049088  512.3M EFI System
/dev/sda2        1050624  5089804799  5088754176  2.4T Linux filesystem
/dev/sda3        5089804800  5625956351  536151552  255.7G Linux swap

Disk /dev/loop0: 120.1 GiB, 128956393472 bytes, 251867956 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xd405ac8b

Device      Boot    Start      End      Sectors  Size Id Type
/dev/loop0p1 *                2048  249913343  249911296  119.2G 83 Linux
/dev/loop0p2          249913344  251867955  1954612  954.4M  5 Extended
/dev/loop0p5          249915392  251867135  1951744  953M  82 Linux swap / Solaris

Disk /dev/sdb: 931.5 GiB, 1000204886016 bytes, 1953525168 sectors
Disk model: External USB 3.0
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xb77a5f88

Device      Boot    Start      End      Sectors  Size Id Type
/dev/sdb1 *                2048  1953522863  1953520816  931.5G  7 HPFS/NTFS/exFAT
```

Рисунок 8. Результат выполнения команды fdisk -l

Далее необходимо создать директорию для монтирования диска следующей командой (пример):

```
mkdir /mnt/backup/
```

Далее необходимо указать диск для ревервной копии следующей командой:

```
mount /dev/sdb1 /mnt/backup (вместо /dev/sdb1/ указывается диск)
```

Далее необходимо выполнить следующую команду проверки директории, в которую монтировался внешний диск:

```
df -h /mnt/backup/
```


8 Техническая поддержка пользователей

В рамках технической поддержки программного комплекса оказываются следующие услуги:

- Помощь в установке;
- Помощь в настройке и администрировании;
- Помощь в установке обновлений;
- Помощь в поиске и устранении проблем в случае некорректной установки обновления;
- Пояснение функционала модулей программного комплекса, помощь в эксплуатации.

В рамках технической поддержки в случае выявления каких-либо проблем в работе необходимо сообщить об этом факте одним из способов (в порядке уменьшения приоритета):

- На адрес электронной почты office@avsw.ru;
- Позвонив по телефону: +7(495)988-92-25.

8.1 Требования к квалификации специалистов тех. поддержки

Специалисты, осуществляющие техническое сопровождение ПК ATHENA, должны обладать следующими навыками и знаниями:

- Знание и умение управлять сервисами system;
- Знание и умение управлять docker, docker-compose;
- Администрирование СУБД Postgres, MongoDB;
- Знание стека TCP/IP;
- Знание модели OSI;