ОКТОПУС

СИСТЕМА КОМПЛЕКСНОЙ АНТИВИРУСНОЙ ПРОВЕРКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Описание процессов, обеспечивающих поддержание жизненного цикла

Москва

2022г.

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

Версия документа

Мая 25, 2022

СОДЕРЖАНИЕ

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.	ПЭВМ	Персональная электронно-вычислительная машина
9.	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 «Система комплексной антивирусной проверки программного обеспечения «Октопус» (далее – система ОКТОПУС) относится к классу систем антивирусных мультисканеров и предназначена для усиления безопасности ИТ-инфраструктуры организаций.

3.1 ПО, необходимое для функционирования системы ОКТОПУС

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

Для эксплуатации системы ОКТОПУС на рабочем месте необходимо использовать веб-браузеры с версиями не ниже, указанных в таблице 3**Error! Reference source not found.**.

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 системы ОКТОПУС, написано на следующих языках программирования: Assembler, Bash, C, C++, C#, Python.

4 Процессы, обеспечивающие поддержание жизненного цикла

Поддержание жизненного цикла системы ОКТОПУС осуществляется за счет сопровождения системы, включающего в себя следующие сервисные процессы:

1. Поставка и настройка системы (первичная и в процессе эксплуатации);

2. Техническая поддержка пользователей;

3. Проведение обновления системы.

Сопровождение системы ОКТОПУС необходимо для:

– Обеспечения гарантий корректного функционирования системы и дальнейшего развития её функционала;

– Отсутствия простоя в работе по причине невозможности функционирования системы (аварийная ситуация, ошибки в работе и т.п.).

4.1 Требования к квалификации специалистов

Специалисты, осуществляющие техническое сопровождение системы ОКТОПУС, должны обладать навыками и знаниями, указанными в таблице 4:

Таблица 4. Квалификация персонала

№	Персонал	Квалификация
1.	Администратор	Практический опыт и профессиональные знания по установке, настройке и сопровождению высоконагруженных систем класса антивирусного мультисканера. Хорошее знание серверной инфраструктуры на базе операционной системы Linux.
2.	Инженер	Знание топологии сети ИТ- инфраструктуры, понимание принципов использования лицензионных программных продуктов. Опыт интеграции

№	Персонал	Квалификация
		систем безопасности в существующую ИТ-инфраструктуру организации.

Общие требования к специалистам, осуществляющим администрирование ПО:

- опыт в администрировании систем Debian/RHEL
- опыт в администрировании СУБД (PostgreSQL, MongoDB)
- знание основ сетевого администрирования
- знание технологий контейнеризации (Docker)
- опыт в администрировании SIEM (syslog)
- опыт в администрировании почтовых серверов (SMTP)
- опыт в администрировании ICAP клиентов
- знание основ резервного копирования

5 Первичная настройка системы ОКТОПУС

Данный раздел предназначен для первичной настройки системы ОКТОПУС и дальнейшей работы в системе.

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

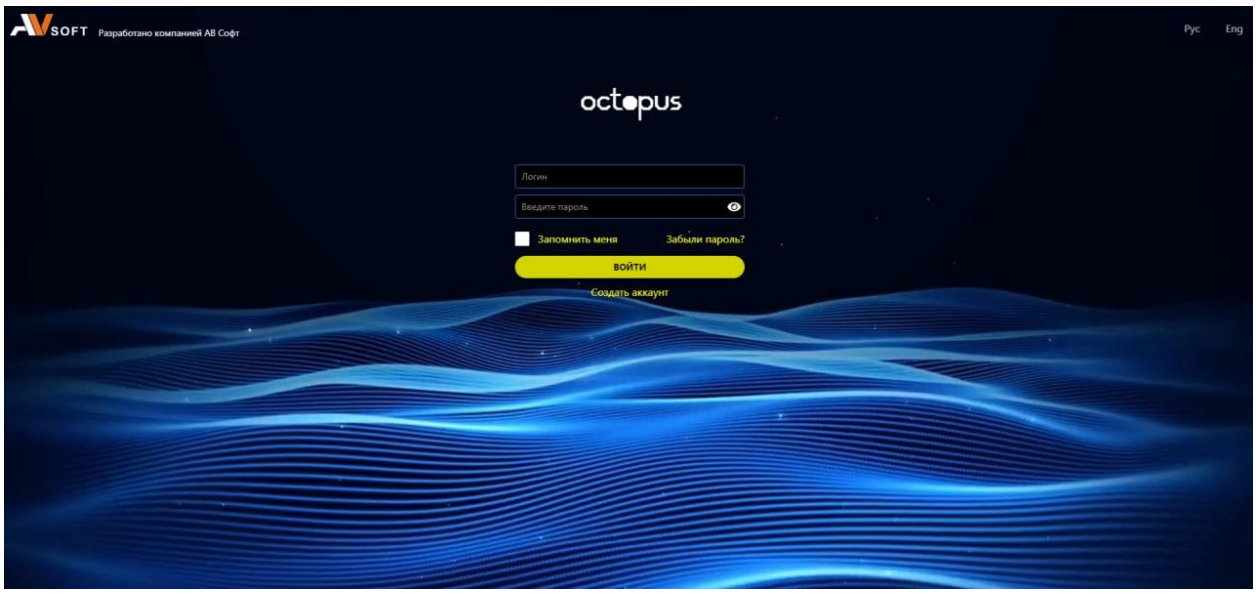

Рисунок 1. Страница авторизации в системе ОКТОПУС

Раздел «Настройки» доступен администратору системы ОКТОПУС и не доступен в пользовательском интерфейсе.

Во вкладке «Пользователи» находится информация о пользователях системы ОКТОПУС (Рисунок 2).

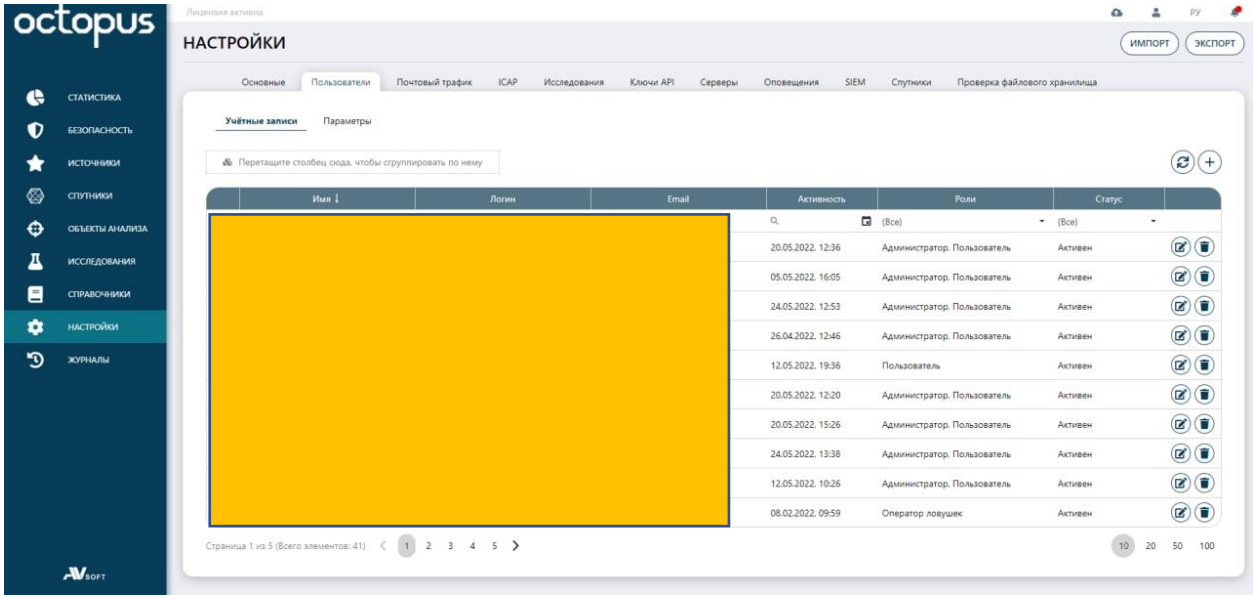

Рисунок 2. Раздел «Настройки» вкладка «Пользователи»

Для регистрации нового пользователя в системе ОКТОПУС 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 системы ОКТОПУС 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 системе ОКТОПУС.

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

6 Обновление системы ОКТОПУС

Система ОКТОПУС поддерживает два типа обновления:

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

Для обновления по сети можно использовать системную консоль.

6.1. 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
```

6.2. Физический носитель

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

7 Резервное копирование

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

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

Резервному копированию (РК) подлежит 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, устанавливаемые на рабочие станции для копирования данных.

В качестве такой системы, для резервного копирования данных ОКТОПУС может использоваться система резервного копирования,

имеющаяся у Заказчика. При отсутствии у Заказчика штатной системы резервного копирования, она может быть создана специально для системы ОКТОПУС. 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 4.

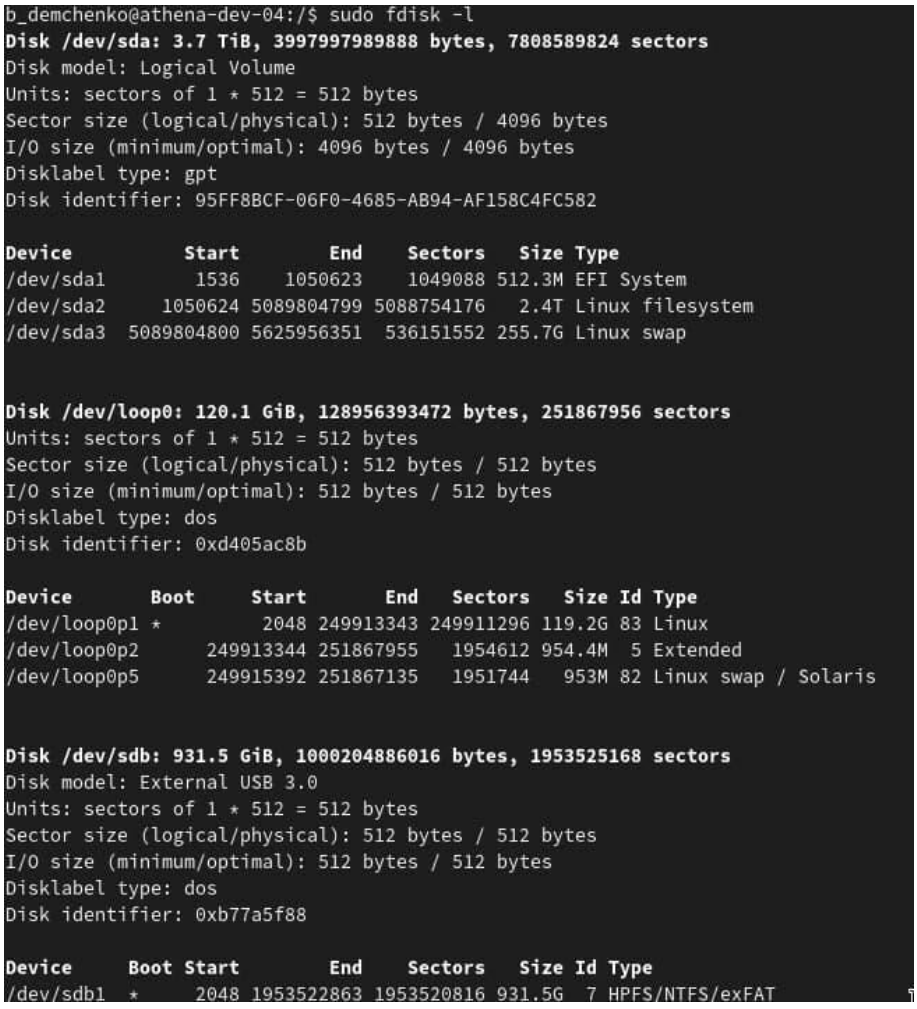

Рисунок 4. Результат выполнения команды fdisk -l

Далее необходимо создать директорию для монтирования диска

следующей командой (пример):

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

Далее необходимо указать диск для резервной 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 Неисправности

Рассмотрим неисправности, которые могут возникнуть в ходе работы с системой ОКТОПУС. Представлены в таблице 5.

Таблица 5. Неисправности

№ п/п	Проблема	Решение проблемы
1	Слишком долгое время исследований	1.1 Проверить свободные ресурсы на сервере через веб-интерфейс. Журналы – Мониторинг 1.2 В случае если замедлены статические исследования необходимо проверить лог файл /avsoft/static/logs/Result_Checker.log. В поисках строки "ID: X, ArchiveID: X CheckInfo: No modules with names: [...]" Если в [...] будут указано имя антивируса, то отключить его через вебинтерфейс

9 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.

9.1 Требования к квалификации специалистов тех. поддержки

Специалисты, осуществляющие техническое сопровождение системы ОКТОПУС, 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