L O K I

Система ложной ИТ-инфраструктуры

Описание процессов, обеспечивающих поддержание жизненного цикла

Москва
2021

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

Июль 08, 2021.

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.	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.	Кибератака	Несанкционированное воздействие на вычислительную систему специальными программными средствами с целью нарушения её работы, получения доступа к чувствительной информации.
3.	Ловушка	Контейнер сенсора имитирующий узел в сети.
4.	Приманка	Значимые для кибератаки данные, ведущие на ловушку.
5.	СУБД MongoDB	Документоориентированная система управления БД, не требующая описания схемы таблиц.
6.	СУБД Postgres	Свободная объектно-реляционная система управления БД.
7.	Технология Deception (англ. обман)	Технология ИБ, которая предназначена для борьбы с направленными атаками, атаками нулевого дня и вредоносным ПО.

3 Общие положения

Программный комплекс «LOKI – система ложной ИТ-инфраструктуры» (далее – ПК LOKI) относится к системам класса ложных распределенных целей, предназначенных для защиты ИТ-инфраструктуры организаций от сетевых кибератак. Он использует технологию защиты от кибератак Deception (обмана) и предназначен для инициации активного взаимодействия со злоумышленником, сбора информации о его деятельности и проверки собранных артефактов.

3.1 ПО, необходимое для функционирования ПК LOKI

Программный комплекс «LOKI – система ложной ИТ-инфраструктуры» функционирует в среде ОС Debian не ниже 9 (девятой) версии, установленной на ПЭВМ с аппаратной платформой Intel x86_64.

Для эксплуатации ПК LOKI требуются вычислительные ресурсы не менее указанных в таблице 3 и таблице 4Таблица 3.

Таблица 3. Требования к серверу управления

№ п/п	Характеристики оборудования	Минимальные требования
1.	Архитектура	Intel x86_84
2.	ОС	Debian не ниже 9 (девятой) версии
3.	Процессор	4 ядра
4.	Оперативная память	12 GB
5.	SSD диск	256 GB (2шт) RAID1
6.	Сеть	10/100/1000 Мбит/с (2 шт.)

Таблица 4. Требования к сенсорам

№ п/п	Характеристики оборудования	Минимальные требования
1.	Процессор	2 ядра

№ п/п	Характеристики оборудования	Минимальные требования
2.	Оперативная память	3 GB
3.	SSD диск	100 GB (2шт) RAID1
4.	Сеть	10/100/1000 Мбит/с (2 шт.)

3.2 Языки программирования, на которых написано изделие

Программы, входящие в состав ПК LOKI написаны на языках C, Python, Java.

4 Процессы, обеспечивающие поддержание жизненного цикла

Поддержание жизненного цикла ПК LOKI 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 LOKI 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 LOKI, 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.

5 Первичная настройка ПК LOKI

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

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

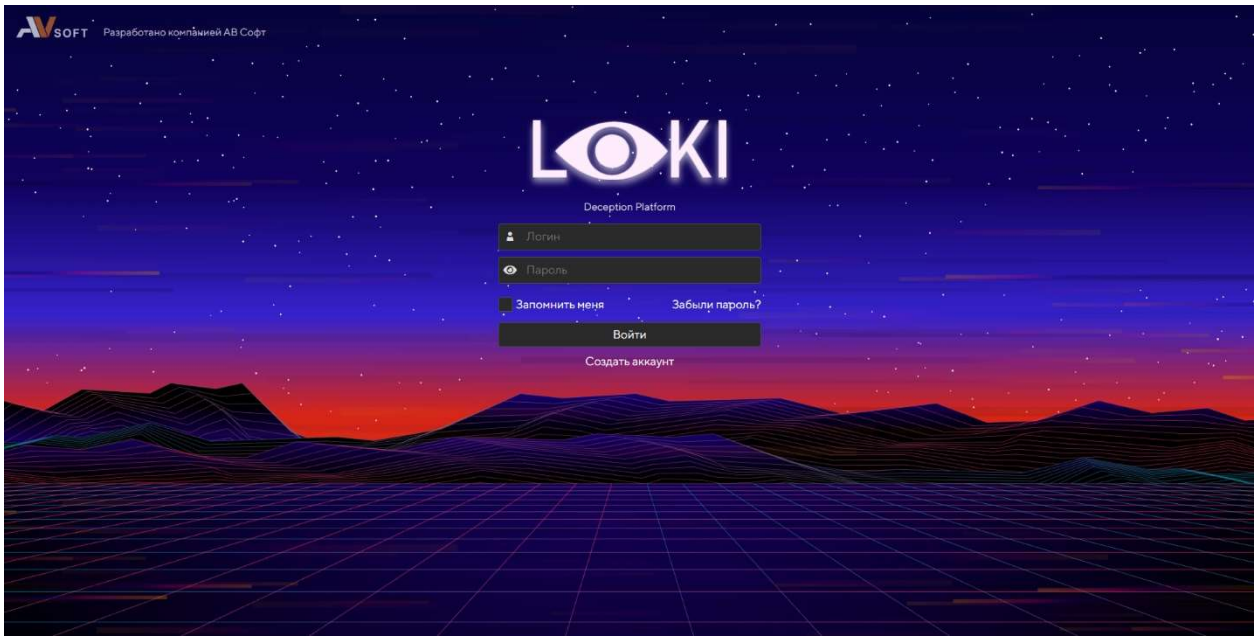

Рисунок 1. Страница авторизации в ПК LOKI

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

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

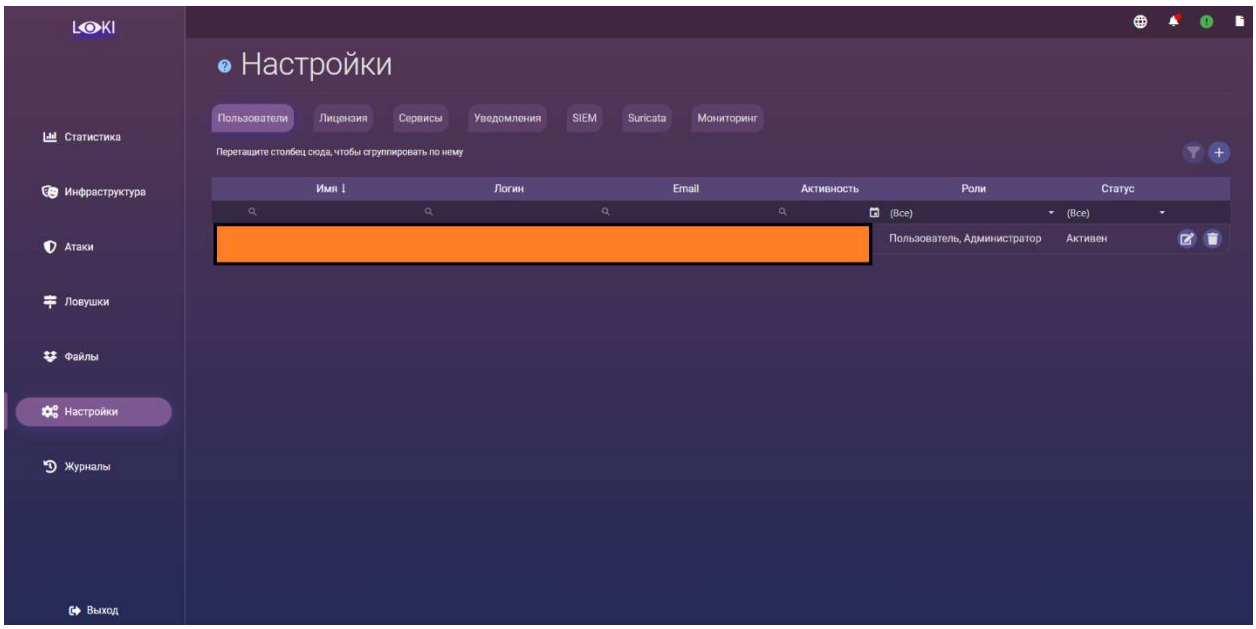

Рисунок 2. Раздел «Настройки» вкладка «Пользователи»

Для регистрации нового пользователя в ПК LOKI 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 LOKI 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 LOKI.

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

Во вкладке **«Сервисы»** располагается информация о серверах, на которых располагаются ловушки и прокси сервисах, используемых для ловушек (Рисунок 4).

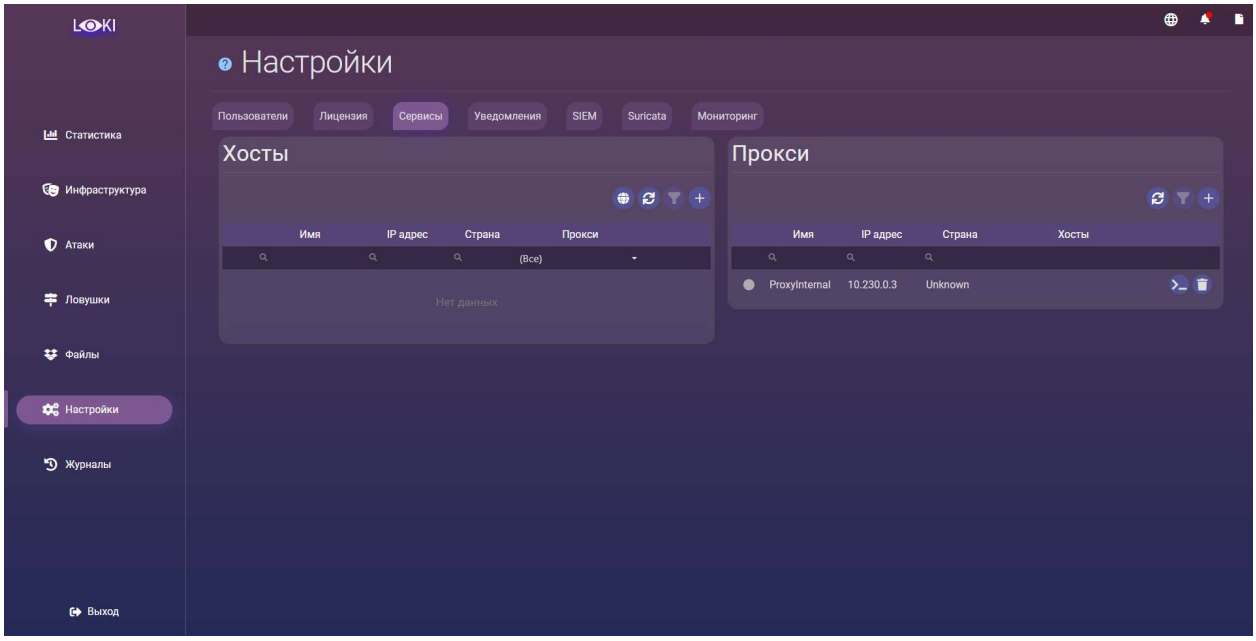

Рисунок 4. Раздел «Настройки» вкладка «Сервисы»

Для добавления нового прокси-сервера необходимо выполнить следующие шаги:

1. Получить доступ к VPS серверу и выполнить подключение по ssh и root пользователя.
2. Открыть веб-интерфейс ПК LOKI и перейти в раздел «Настройки» – вкладка «Сервисы».
3. Нажать кнопку «Добавить прокси» и во всплывающем вписать туда IP адрес VPS, Port от ssh, Login от пользователя (нужны повышенные привилегии, поэтому root), Пароль от пользователя.
4. Нажать сохранить и дождаться окончания установки (сигнализироваться будет окончанием пульсации иконки статуса).

Во вкладке **«Уведомления»** присутствует возможность настройки уведомлений по электронной почте и в Telegram о значимых событиях в системе (Рисунок 5).

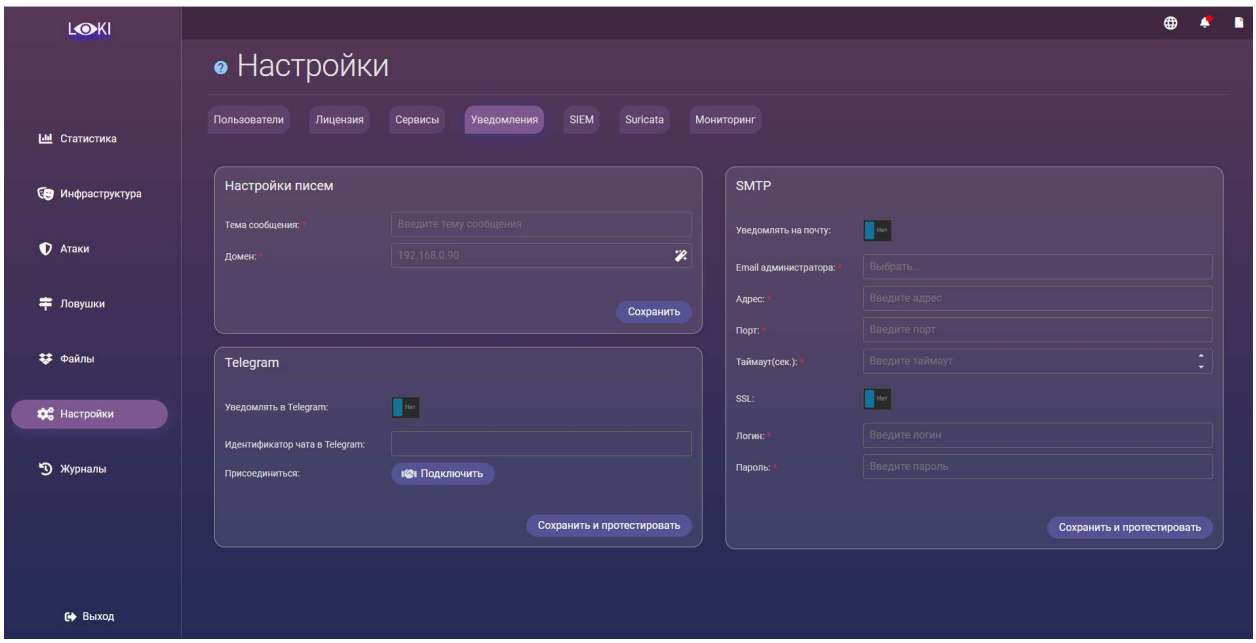

Рисунок 5. Раздел «Настройки» вкладка «Уведомления»

Во вкладке «SIEM» осуществляется интеграция с SIEM-сервисом (Рисунок 6). SIEM-системы, предназначены для анализа информации, поступающей от других систем, и выявления отклонений от норм по определенным критериям.

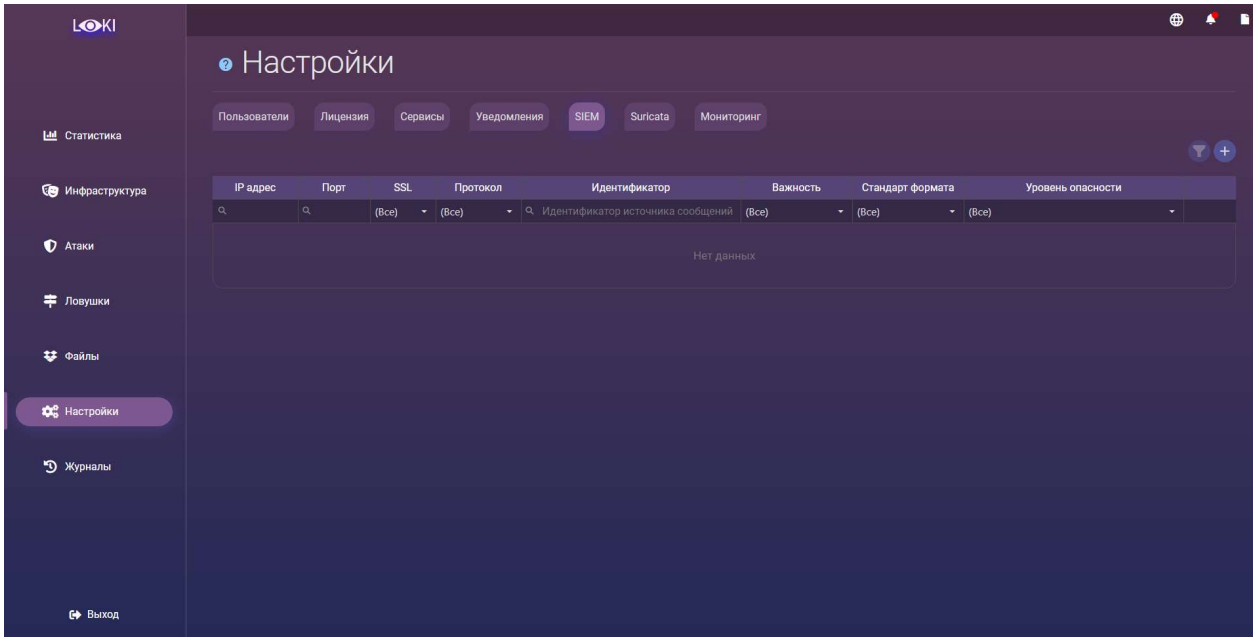

Рисунок 6. Раздел «Настройки» вкладка «SIEM»

Для добавления нового SIEM необходимо нажать на кнопку «Добавить строку» и приступить к заполнению полей во всплывающей форме (Рисунок 7).

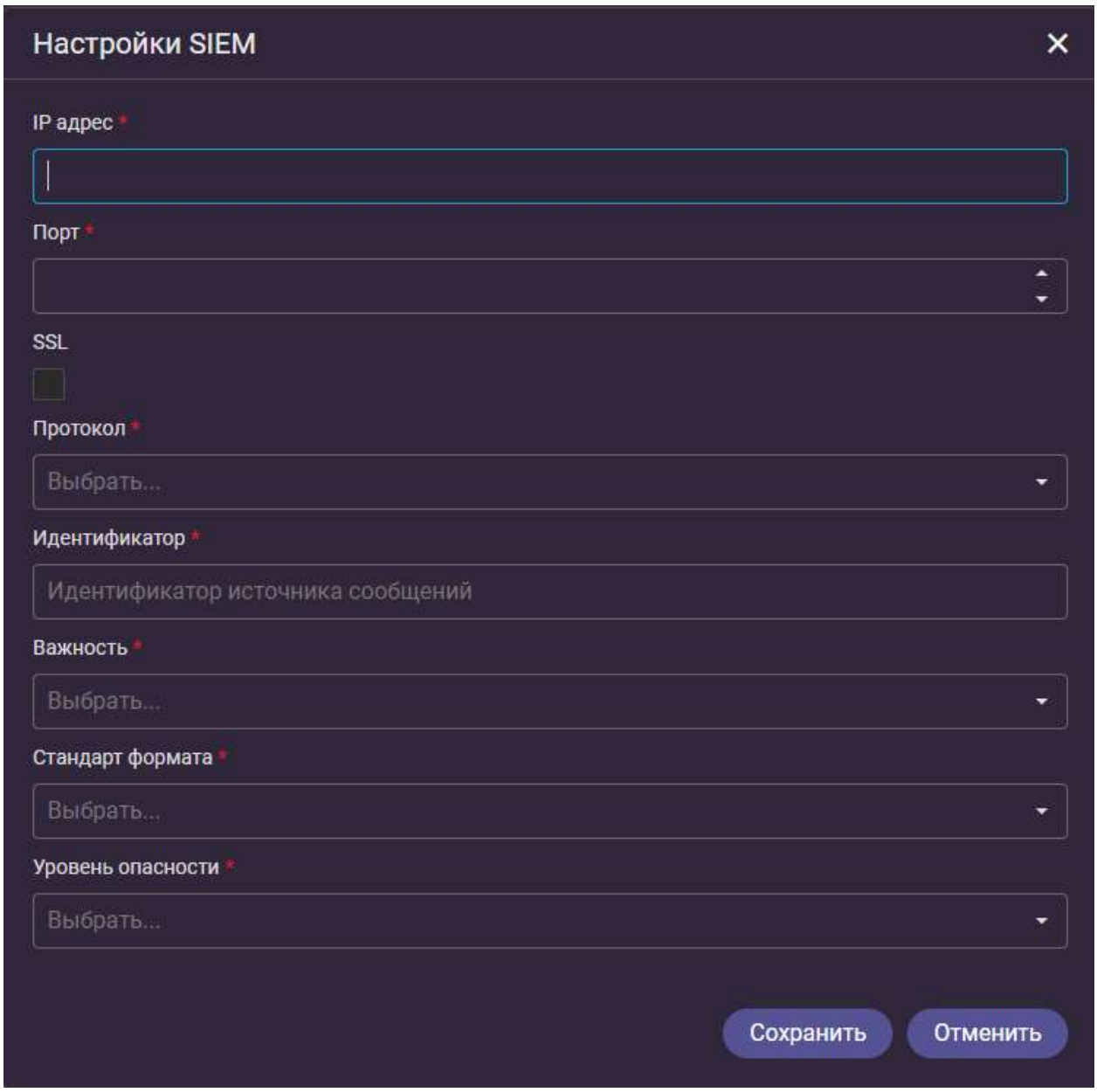

Рисунок 7. Добавление SIEM в систему LOKI

Поля, отмеченные звездочкой, обязательны к заполнению. По окончании ввода данных необходимо нажать кнопку «Сохранить».

Во вкладке «Suricata» присутствует список правил внешнего аналитического сервиса Suricata (Рисунок 8). Suricata является инструментом по обработке входящих пакетов, который позволяет предотвращать попадание вредоносных пакетов в инфраструктуру.

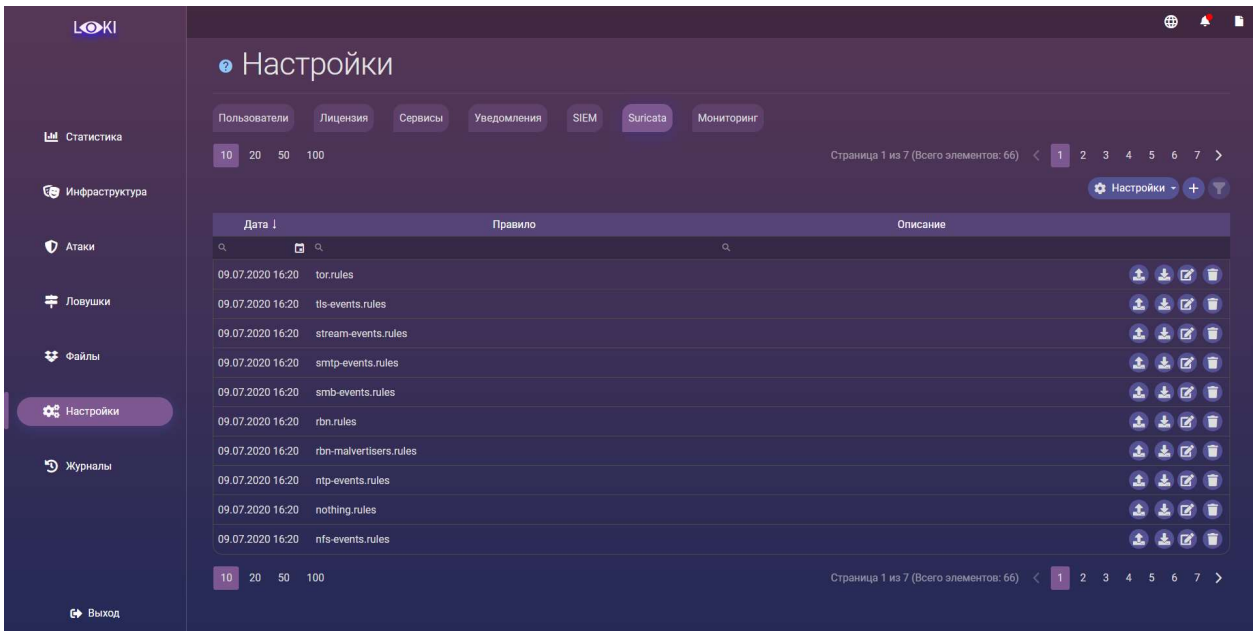

Рисунок 8. Раздел «Настройки» вкладка «Suricata»

При добавлении нового правила необходимо воспользоваться кнопкой «Добавить правило», выполнить загрузку необходимых файлов и нажать кнопку «Загрузить». При успешной загрузке пользователю отобразится уведомление, что загрузка выполнена успешно.

В разделе «Настройки» во вкладке «Мониторинг системы» в реальном времени отображается состояние модулей в системе (Рисунок 9. Раздел «Настройки» вкладка «Мониторинг системы»Рисунок 9 9).

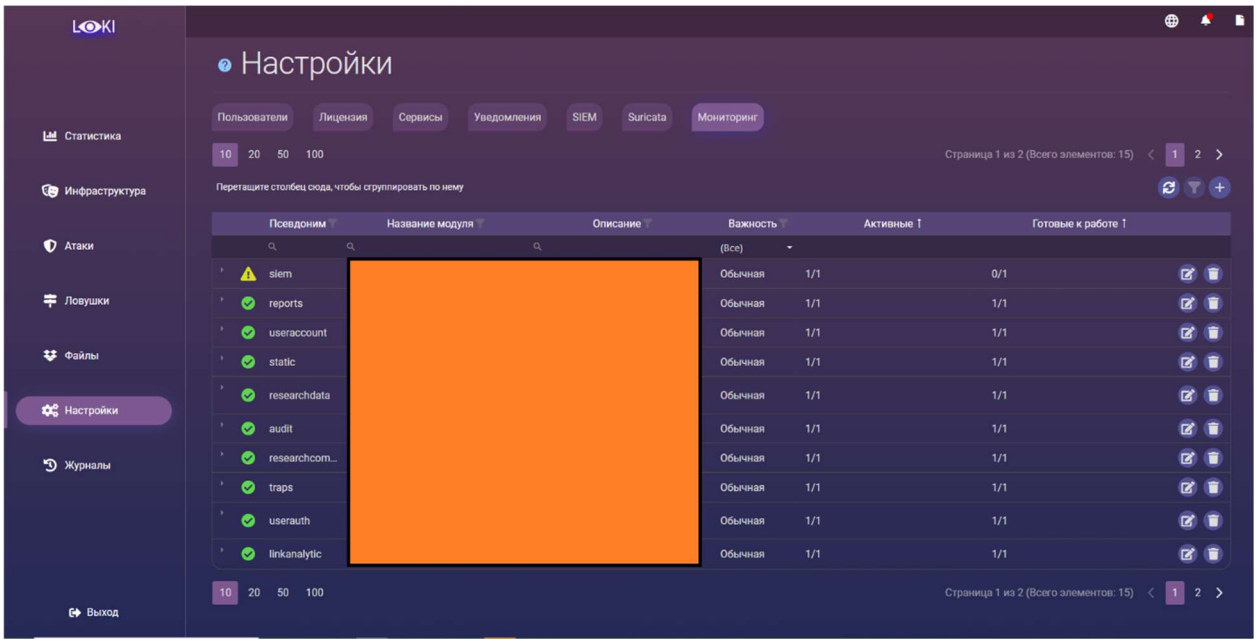

Рисунок 9. Раздел «Настройки» вкладка «Мониторинг системы»

6 Раздел «Журналы»

Данный раздел доступен администратору ПК LOKI и не доступен в пользовательском интерфейсе. Логин, пароль администратора по умолчанию предоставляет разработчик программного обеспечения (Рисунок 10).

В данном разделе присутствует мониторинг CPU, использование памяти, данные по оборудованию, различные проблемы, связанные с ПК LOKI. Все данные выгружаются из системы мониторинга Zabbix.

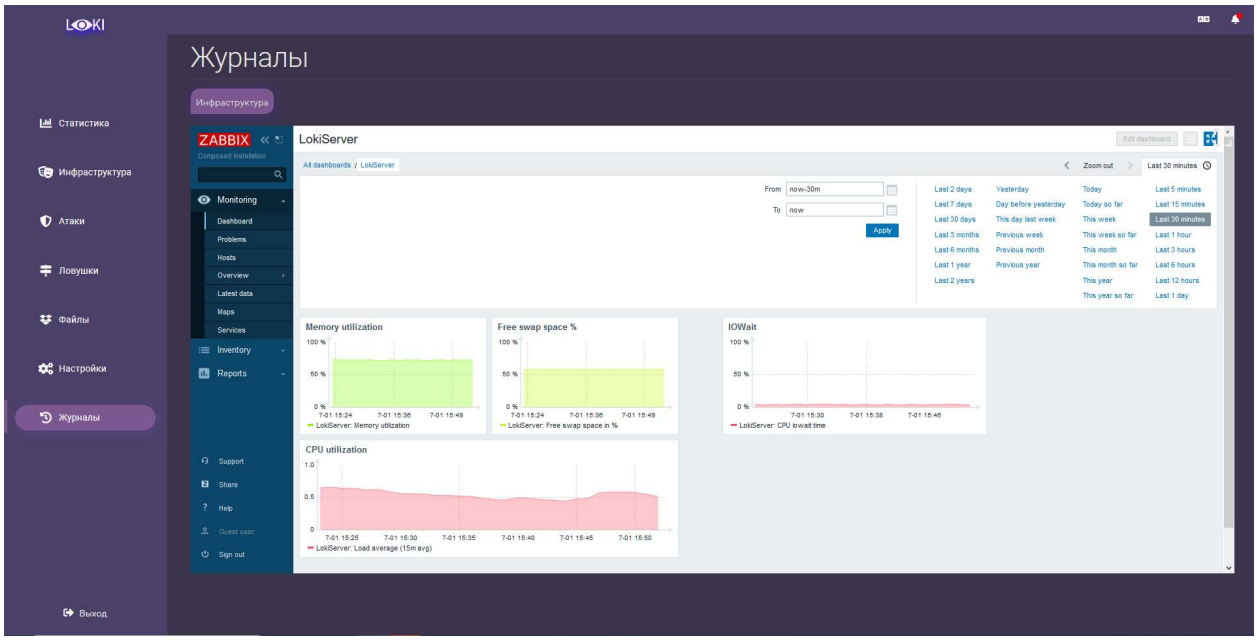

Рисунок 10. Раздел «Журналы»

7 Обновление ПК LOKI

Каждый модуль ПК LOKI обновляется в ручном режиме. На данный момент обновления доступны для следующих модулей:

- Модуль визуализации данных;
- Модуль сканирования инфраструктуры;
- Модуль визуализации данных.

Для каждого модуля необходимо проделать следующие действия:

1. Перейти в веб-интерфейс агента обновлений https://<SERVER_IP>/update_agent/, вместо <SERVER_IP> указать IP-адрес ПК LOKI;
2. Найти в списке модуль с именем <Module_Name>, где <Module_Name> имя текущего модуля для обновления;
3. Перейти на вкладку «Информация», нажав на иконку монитора;
4. Если кнопка обновления активна, необходимо на неё нажать;
5. После страница будет переведена на вкладку «Журнал», в котором будет отображаться ход обновления (Рисунок 11).

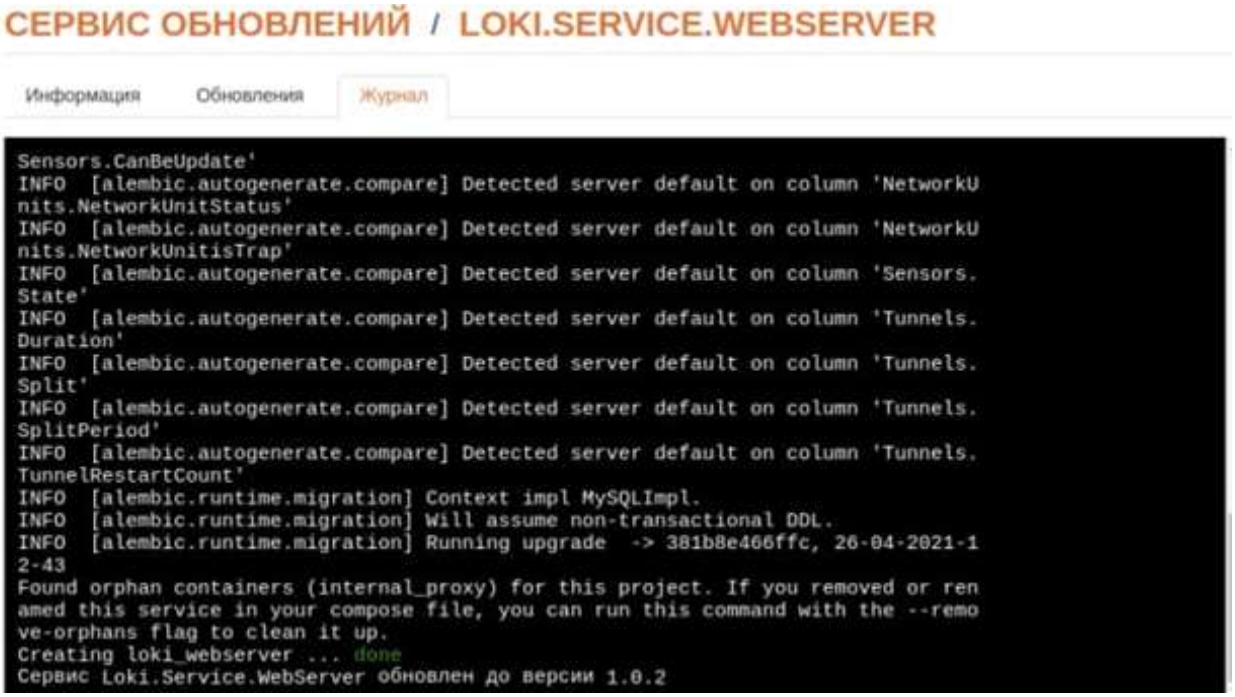

Рисунок 11. Журнал обновлений

6. По окончанию обновления должна появиться надпись

«Сервис обновлён до версии x.x.x» (Рисунок 12).

Рисунок 12. Результат обновлений

8 Возможные проблемы

ПК LOKI представляет собой комплекс из программных модулей, которые взаимно интегрированы и связаны тем или иным способом между собой. Рассмотрим проблемы, которые могут возникнуть в ходе работы с ПК LOKI представлены в таблице 5Таблица 5. Возможные проблемы.

Таблица 5. Возможные проблемы

№ п/п	Проблема	Решение проблемы

1.	Запущено слишком большое количество ловушек (недостаточное количество ресурсов на ловушке ОЗУ, процессор)	1.1 Если активна отвечает консоль, то необходимо подключится к сенсору, затем получить список контейнеров командой:
		`docker rm -f $(docker ps -a | grep -v filebeat | awk '{print $1}' | grep -v CONTAINER)`
		1.2 В случае если удалённый терминал не отвечает необходимо произвести перезагрузку сенсора командой:
		`cat /etc/network/interfaces`

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 ПК LOKI, 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;

10 Резервное копирование

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

- Системы резервного копирования, имеющие клиент-серверную архитектуру;
- Автономные системы резервного копирования.

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 ПЭВМ для копирования данных.

В качестве такой системы, для резервного копирования данных ПК LOKI может использоваться система резервного копирования, имеющаяся у Заказчика. Для подключения к ней, на ПЭВМ с установленным программным обеспечением ПК LOKI необходимо осуществить установку клиентского программного обеспечения системы резервного копирования и осуществить его настройку.

При отсутствии у Заказчика штатной системы резервного копирования, она может быть создана специально для ПК LOKI. Для этого в состав изделия должен быть включён сервер резервного копирования.

Автономные системы резервного копирования не требуют использования дополнительного серверного оборудования. Они позволяют осуществлять резервное копирование на внешние носители данных. В качестве программного обеспечения рекомендуется использовать программу для резервного копирования и восстановления данных Duplicati.

Ответственность за своевременность и правильность осуществления резервного копирования и хранение копий несет системный администратор.