



Система защиты
ИТ-инфраструктуры от кибератак
на базе технологии Deception

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 v5.0

Май 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	5
2	Общие сведения о программе	7
2.1	Общий алгоритм работы системы	7
2.2	Техническая поддержка системы.....	8
3	Авторизация.....	8
3.1	Элементы управления веб-интерфейсом	10
4	Раздел «Статистика»	13
5	Раздел «Инфраструктура»	14
5.1	Вкладка «Сенсоры»	14
5.2	Сканирование сети и развертывание ловушек	15
5.3	Сканирование уязвимостей	22
5.4	Промышленные сенсоры	23
5.5	Исследовательские сенсоры	35
5.6	Карта сети.....	39
5.7	Active Directory	40
5.8	Расписания.....	42
5.9	Сравнение сканирований	45
5.10	Агенты	46
6	Раздел «Атаки»	47
6.1	Анализ атак.....	47
6.2	Сценарии реагирования	52
7	Раздел «Ловушки».....	54
8	Раздел «Приманки».....	60
9	Раздел «Файлы».....	67

10	Развертывание приманок.....	67
10.1	Развертывание приманок с использованием агента	69
10.2	Автоматическое развертывание приманок.....	71
10.3	Ручное развертывание приманок.....	75

1 Термины и определения

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

Таблица 1. Термины и определения

№	Термин	Определение
1.	Deception	Технология имитации ложных целей для привлечения к ним кибератак и защиты реальных устройств
2.	Suricata	Внешний аналитический сервис для анализа сетевого трафика
3.	Кибератака	Несанкционированное воздействие на вычислительную систему организации специальными программными средствами с целью нарушения её работы, получения доступа к конфиденциальной информации
4.	Ловушка	Имитация реального устройства на определенном уровне
5.	Приманка	Значимые для кибератаки данные, ведущие на ловушку и размещаемые на реальных устройствах
6.	Сенсор	Модуль сканирования и развертывания ловушек в подсети ИТ-инфраструктуры

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

Таблица 2. Перечень сокращений

№	Сокращение	Значение
1.	AD	Active Directory
2.	DNS	Domain Name System
3.	FQDN	Fully Qualified Domain Name

№	Сокращение	Значение
4.	IP	Internet Protocol
5.	MAC	Media Access Control
6.	SIEM	Security Information and Event Management
7.	SOC	Security Operations Center – Операционный центр безопасности
8.	SSH	Secure Shell
9.	TCP	Transmission Control Protocol
10.	URL	Uniform Resource Locator
11.	APM	Автоматизированное рабочее место
12.	ИТ	Информационные технологии
13.	ПО	Программное обеспечение

2 Общие сведения о программе

Система защиты ИТ-инфраструктуры LOKI (далее – система LOKI) относится к системам класса ложных распределенных целей, предназначенных для защиты ИТ-инфраструктуры организаций от внутренних и внешних кибератак. Данный класс систем использует технологию Deception (технологию имитации цифровых двойников устройств) и предназначен для мониторинга кибератак, инициации взаимодействия со злоумышленником, сбора информации о его деятельности и блокировки распространения кибератак.

Основная задача платформы заключается в детектировании подключений к ловушкам, имитирующим реальные сервисы предприятия, и в оперативном оповещении сотрудников службы безопасности о факте атаки в режиме реального времени. Также система LOKI способна осуществлять интерактивное взаимодействие со злоумышленником, чтобы собрать как можно больше о нем информации, которая может помочь при расследовании инцидента.

В настоящем документе дано описание пользовательского функционала на базе графического веб-интерфейса системы LOKI.

Функционал системы реализован в составе законченного комплекта ПО, не требует доработки и/или разработки дополнительных программных средств с использованием API или иного дополнительного ПО.

В системе поддерживается два типа локализации: русская и английская. Все создаваемые пользователем объекты могут иметь названия и описания как на русском, так и на английском языке.

2.1 Общий алгоритм работы системы

1. Пользователь выполняет сканирование подсетей своей ИТ-инфраструктуры, в которых расположены сенсоры системы.
2. Система в автоматическом режиме подбирает подходящие типы ловушек из своего каталога. Пользователь, при необходимости, может их изменить.
3. После выбора типов ловушек система автоматически высчитывает их максимальное допустимое количество, в зависимости от количества ресурсов. Пользователь, при необходимости, может его изменить.

4. Осуществляется развертывание ловушек в подсети, после чего они отобразятся на графической карте в системе.
5. Производится генерация и скачивание приманок на реальные рабочие места пользователей.
6. Осуществляется развертывание приманок на рабочие места пользователей и отображение их на графической карте в системе.
7. Система осуществляет проверку устройств в ИТ-инфраструктуре пользователя на наличие уязвимостей из базы данных CVE.

2.2 Техническая поддержка системы

Для системы LOKI предусмотрена возможность получения технической поддержки производителя на территории присутствия Заказчика в Российской Федерации на русском или английском языках. Для оказания сервиса технической поддержки производителем могут быть заключены соответствующие договоры/соглашения с аффилированными организациями и/или организациями, имеющими право действовать от лица правообладателя ПО (партнеры, агенты и т.п.). Контактную информацию можно найти на официальном сайте компании «АВ Софт» (<https://avsw.ru/>).

Прием и реагирование на обращения осуществляется по телефону, через веб-портал или по электронной почте в будние дни. Время реагирования на обращение – в течение 24 часов с момента обращения.

Также компания «АВ Софт» предоставляет для своих клиентов:

- возможность скачивания последних обновлений программного обеспечения LOKI;
- доступ к базе знаний компании (техническая документация, форумы, ответы тех. поддержки на запросы пользователей).

3 Авторизация

Для авторизации в системе LOKI необходимо в адресной строке браузера ввести URL, полученный у администратора. Внешний вид страницы авторизации показан на рисунке 1.

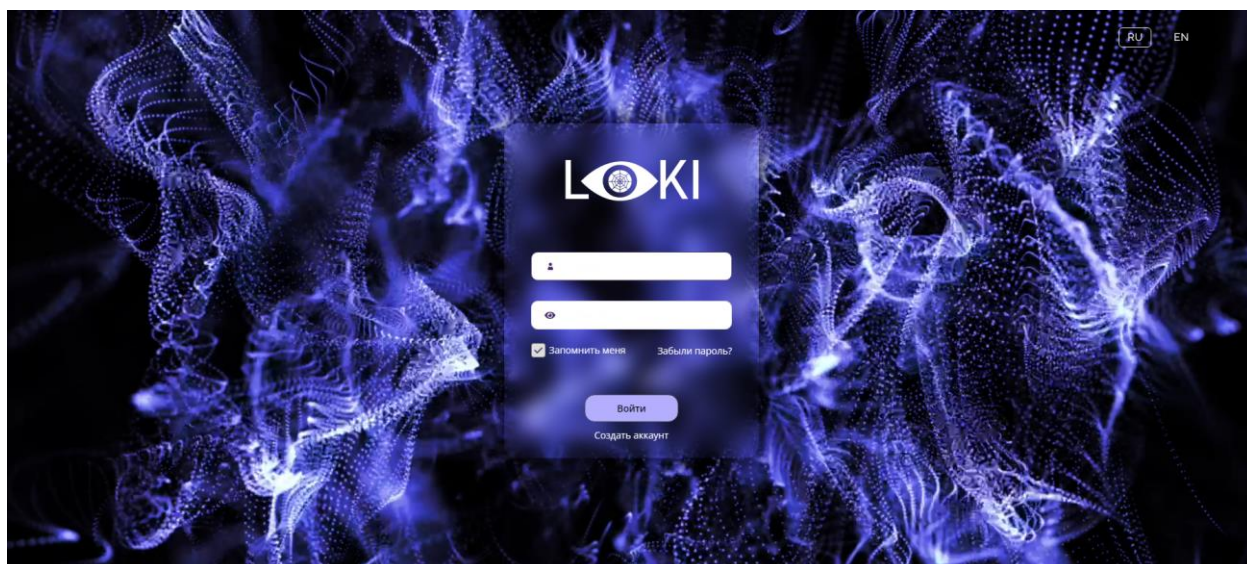


Рисунок 1. Страница авторизации пользователя в LOKI

Далее следует выполнить регистрацию и авторизацию в системе: ввести логин и пароль учетной записи.

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

Таблица 3. Описание функциональных разделов в системе






№	Раздел	Описание
1.	Статистика	Содержит статистическую информацию по атакам, приманкам и ловушкам
2.	Инфраструктура	Содержит информацию об установленных в организации сенсорах, развёрнутых ловушках и приманках, а также их настройки
3.	Атаки	Содержит информацию по зафиксированным атакам и задания для офицеров по безопасности для расследования инцидента
4.	Ловушки	Содержит информацию по доступным к развертыванию ловушкам и приманкам
5.	Приманки	Отображает информацию об размещенных на рабочих местах приманках
6.	Файлы	Содержит информацию по всем файлам, обнаруженным в процессе атаки на ловушки

№	Раздел	Описание
7.	Справочники	Содержит гибкие справочники по белому списку IP адресов, информацию по доменам и IP, а также список уязвимостей и правила SURICATA используемых в системе
8.	Настройки	Содержит настройки по всем компонентам системы
9.	Журналы	Содержит информацию по мониторингу всех логических и физических модулей в системе, а также регистрацию действий пользователей

3.1 Элементы управления веб-интерфейсом

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

Таблица 4. Описание элементов управления интерфейсом

№	Элемент интерфейса	Назначение	Изображение
1.	Иконка «Выход»	Выход из системы	
2.	Иконка «Фильтрация»	Фильтрация данных в поисковом поле	
3.	Иконка выбора параметров фильтрации	Выбор параметра, по которому будет осуществляться фильтрация	
4.	Иконка «Выпадающий список»	Выбор значения из отображаемого списка	
5.	Иконка «Обновить»	Обновление таблицы	

№	Элемент интерфейса	Назначение	Изображение
6.	Иконка «Переподключить»	Переподключение выбранного сенсора, обновление выбранного образа ловушки	
7.	Иконка «Мастер настройки»	Управление настройками выбранного сенсора	
8.	Иконка «Информация»	Информация об объекте, указанном в столбце «Имя»	
9.	Иконка «Редактировать»	Корректировка информации о выбранном объекте	
10.	Иконка «Удалить»	Удаление информации о выбранном объекте	
11.	Иконка «Удалить все»	Удаление текущих уведомлений системы	
12.	Иконка «Отметить проверенными»	Отметка всех атак как проверенные	
13.	Иконка «Отчет»	Отчет о выбранной атаке	
14.	Иконка «Отметить проверенным»	Отмечает отчет по атаке как проверенный	
15.	Иконка «Запустить сканирование»	Запуск процесса сканирования	
16.	Иконка «Остановить»	Остановка процесса	
17.	Иконка «Отменить сканирование»	Остановка процесса сканирования	
18.	Иконка «История сканирований»	Просмотр архива сканирований устройств на	

№	Элемент интерфейса	Назначение	Изображение
		уязвимости	
19.	Иконка «SSH»	Подключение по протоколу SSH	
20.	Иконка «Уведомления»	Просмотр текущих уведомлений системы	
21.	Иконка «Отметить всё прочитанным»	Отмечает все текущие уведомления системы как проверенные	
22.	Иконка «Документация»	Скачивание документации	
23.	Иконка «API»	Просмотр документации по API	
24.	Иконка «Язык»	Выбор языка интерфейса	
25.	Иконка «Помощь»	При нажатии на кнопку система отображает подсказки по функциональным блокам выбранного раздела	
26.	Иконка «Запустить»	Запуск ловушки	
27.	Иконка «Добавить»	Удаление выбранного объекта	
28.	Иконка «Группировка»	Группировка данных в таблице по выбранным столбцам	
29.	Иконка «Сортировка»	Сортировка данных в столбцах таблицы	

№	Элемент интерфейса	Назначение	Изображение
30.	Иконка «Все ловушки»	Просмотр списка активных исследовательских ловушек	
31.	Иконка «Получить логи»	Скачивание лог-файлов ловушки	
32.	Иконка «Карта сети»	Просмотр карты подсети сенсора	
33.	Иконка «Обновить приманки»	Обновление приманок на рабочих местах	
34.	Иконка «Описание»	При нажатии на кнопку система отображает описание параметров настроек, доступных для редактирования	
35.	Иконка «Информация»	Информация о выбранной исследовательской ловушке	
36.	Иконка «Переключить редактирование»	При нажатии на кнопку поля функционального раздела становятся доступны для редактирования	
37.	Иконка «Настройки сертификата»	Импорт сертификата для подключения к системе SIEM	
38.	Иконка «Скачать»	Скачивание пакета правил Suricata	

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

4 Раздел «Статистика»

При входе в систему пользователю открывается по умолчанию страница раздела «Статистика» вкладка «Статистика использования» (Рисунок 2).

Рисунок 2. Раздел «Статистика» вкладка «Статистика использования»

В данном разделе отображаются все зафиксированные атаки на ловушки в режиме реального времени. Для просмотра более подробной информации по атаке необходимо нажать на иконку «Отчет». Также в данной вкладке отображается следующая статистическая информация:

- Топ 5 ловушек, на которые совершались атаки
- Топ 5 протоколов, задействованных при атаке
- Топ 5 приманок, задействованных при атаке

Во вкладке «Статистика размещения» отображается информация об активных сетевых устройствах, приманках и ловушках (Рисунок 3).



Рисунок 3. Раздел "Статистика" вкладка "Статистика размещения"

5 Раздел «Инфраструктура»

В разделе «Инфраструктура» осуществляется управление сенсорами, ловушками и приманками.

5.1 Вкладка «Сенсоры»

В системе LOKI представлены два типа сенсоров: промышленные и исследовательские. Промышленные сенсоры размещаются внутри инфраструктуры организации и предназначены для выявления несанкционированного проникновения. Исследовательские сенсоры размещаются в сети Интернет и предназначены для сбора информации об киберугрозах.

Вкладка «Промышленные» содержит информацию о сенсорах в

подсетях организации (Рисунок 4).

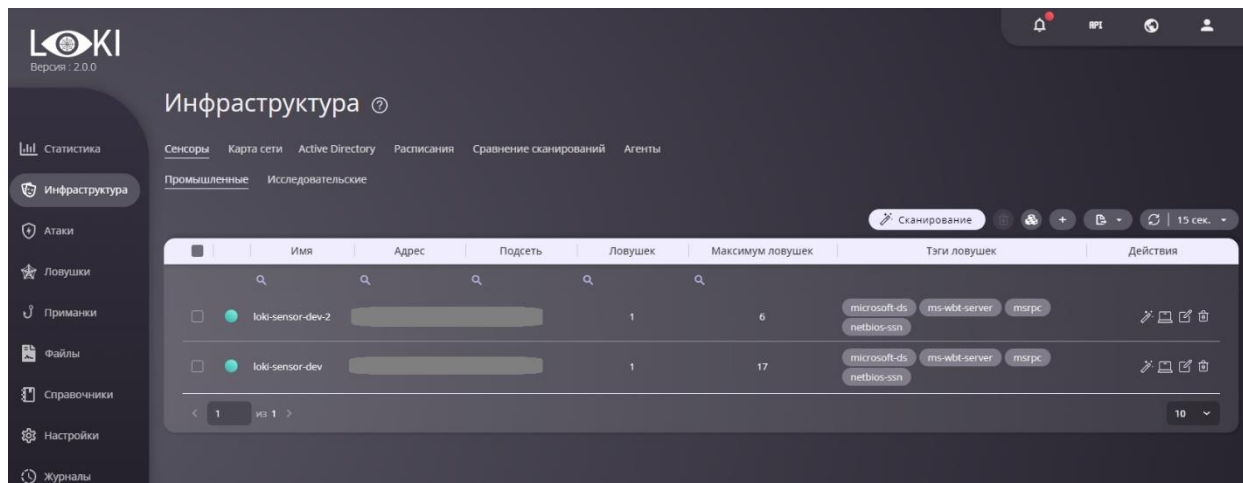


Рисунок 4. Раздел «Инфраструктура»

Также в данной вкладке присутствуют инструменты для развертывания сети ловушек в ИТ-инфраструктуре организации и сканирования устройств на наличие уязвимостей.

5.2 Сканирование сети и развертывание ловушек

Алгоритм сканирования сети и развертывания ловушек в ИТ-инфраструктуре включает в себя 4 основных шага:

1. Сканирование сети
2. Подбор ловушек
3. Развертывание ловушек
4. Развертывание приманок

Для осуществления сканирования ИТ-инфраструктуры с последующим развертыванием ловушек необходимо нажать кнопку «Сканировать». В появившемся окне необходимо выбрать сенсор в нужной подсети и указать тип сканирования — «сканирование сети», после осуществляем и «сканирование уязвимостей». Порядок подключения и настройки сенсора описаны в Руководстве администратора системы LOKI. Чтобы начать сканирование, необходимо нажать на кнопку «Запустить» (Рисунок 5). После этого начнется процесс сканирования, где будут формироваться обнаруженные устройства (Рисунок 6).



Рисунок 5. Окно запуска сканирования

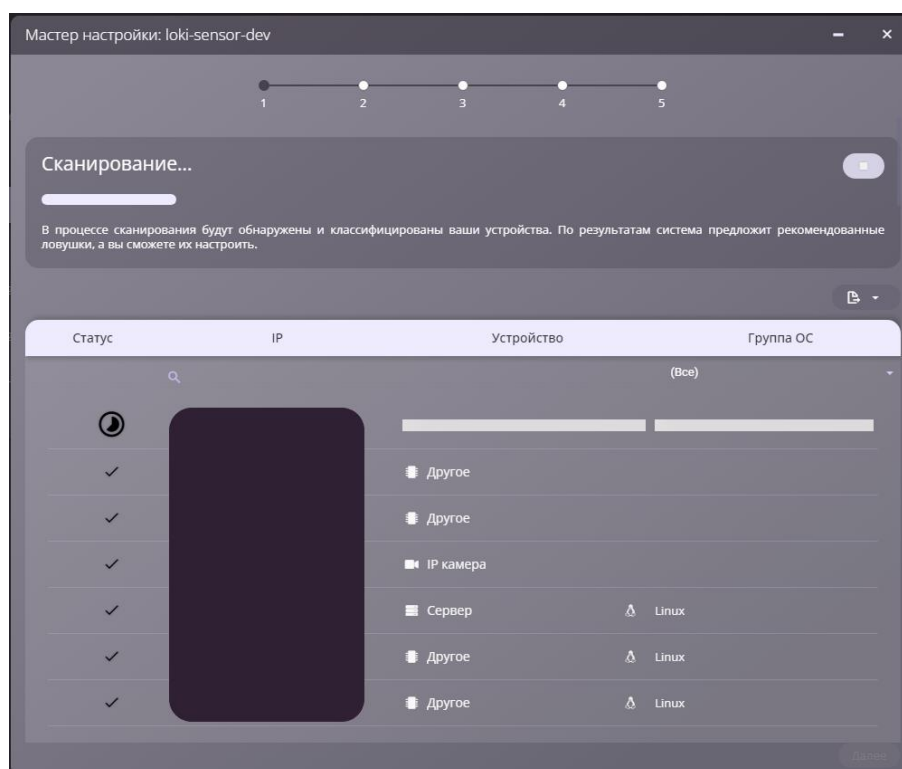


Рисунок 6. Процесс сканирования

После завершения сканирования отобразится список активных устройств в подсети, а также список рекомендуемых к установке ловушек (Рисунок 7).

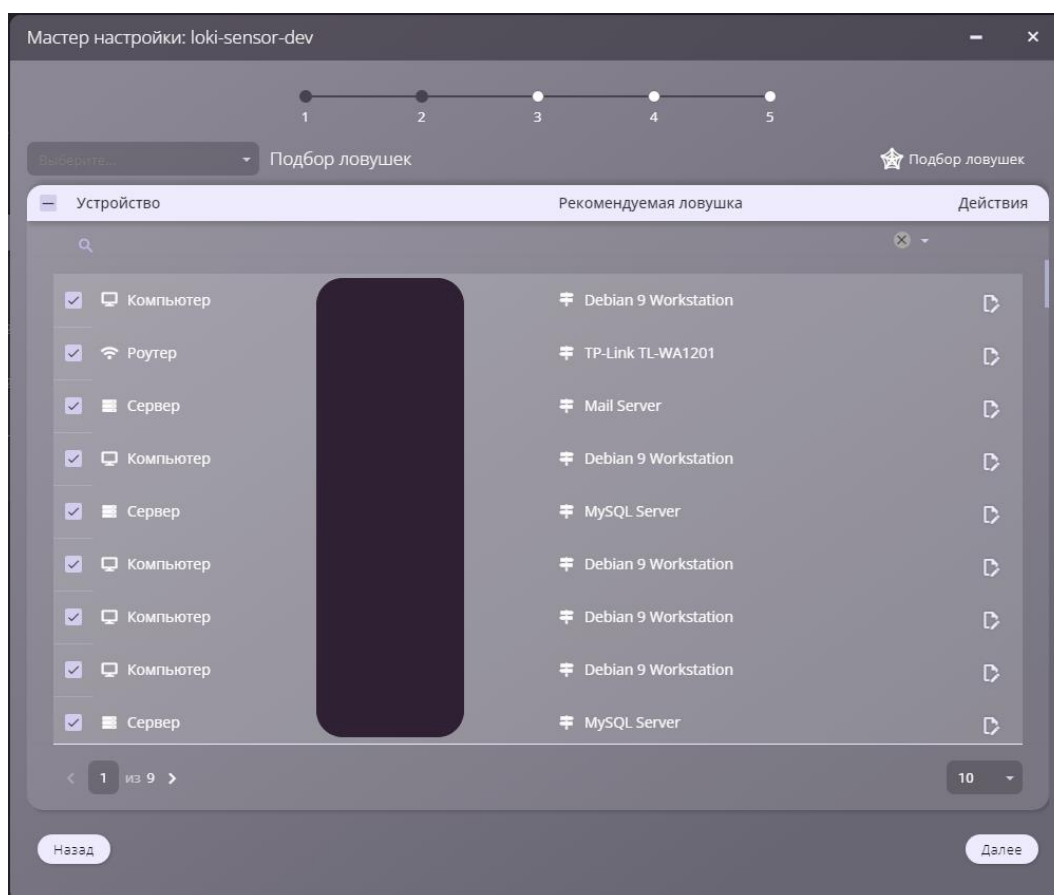


Рисунок 7. Результаты сканирования

При необходимости, список подобранных устройствам ловушек можно отредактировать с помощью кнопки «Подбор ловушек» или с помощью иконки «Редактировать» напротив выбранного устройства. При использовании кнопки «Подбор ловушек» необходимо предварительно отметить галочками те устройства, для которых планируется изменение подобранной ловушки. Затем следует нажать кнопку «Далее». (Рисунок 8).

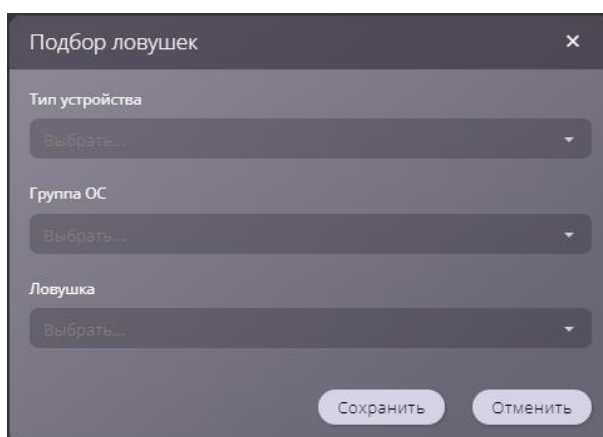


Рисунок 8. Окно «Подбор ловушек»

С помощью выпадающего списка над таблицей с устройствами можно произвести выделение сразу нескольких устройств в зависимости от наличия

подобранной ловушки.

Также над таблицей с устройствами имеется поле с иконкой в виде лупы, с помощью которого можно осуществлять поиск данных по всей таблице.

Далее следует подтвердить список устанавливаемых ловушек и указать требуемое количество различных типов ловушек (Рисунок 9).

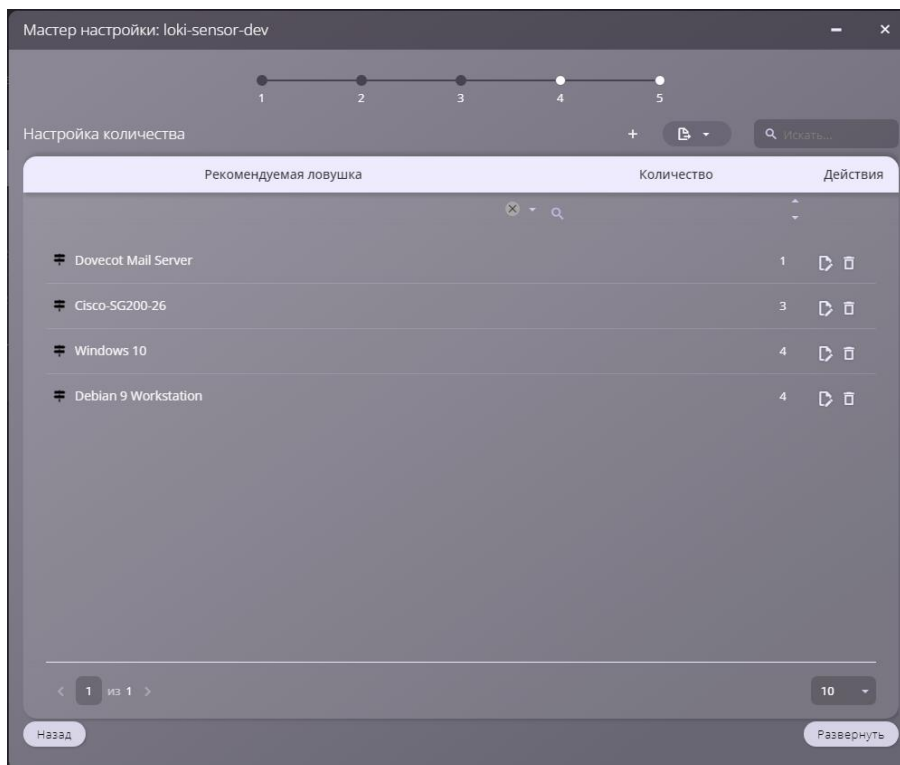


Рисунок 9. Редактирование количества ловушек

Изменение количества каждого типа ловушек может быть произведено с помощью кнопки «Редактировать» (Рисунок 10).

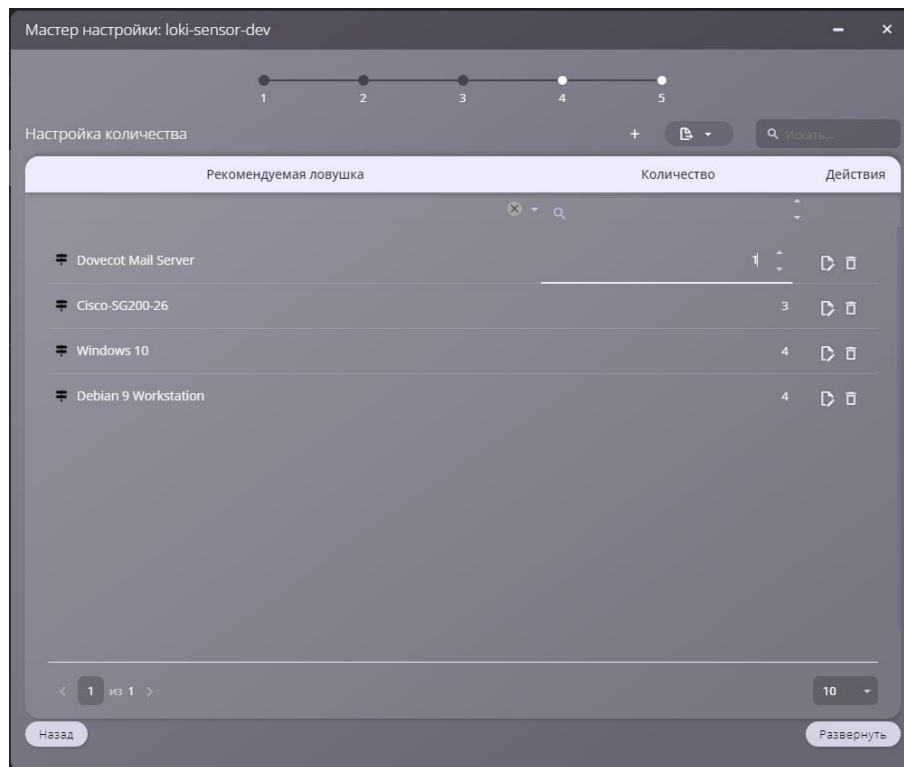


Рисунок 10. Изменение количества устанавливаемых ловушек

Количество ловушек рассчитывается системой в зависимости от объема памяти на сенсоре. При превышении максимального числа ловушек, доступных для установки, система отобразит предупреждение о превышении допустимого лимита (Рисунок 11).

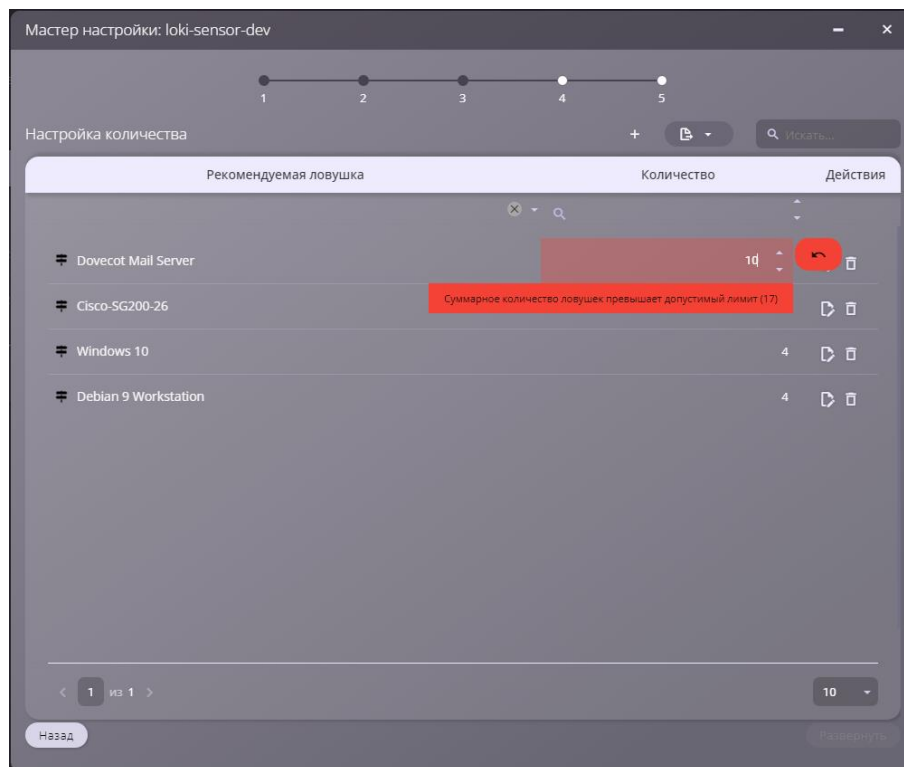


Рисунок 11. Предупреждение о превышении лимита ловушек

Для того, чтобы дополнить список другими типами ловушек, следует нажать на иконку «Добавить», для удаления типа ловушки из списка – на кнопку «Удалить» напротив соответствующей ловушки. Как и на предыдущем этапе здесь также имеется специальное поисковое поле над таблицей с ловушками.

После завершения ввода данных следует нажать кнопку «Развернуть». Далее необходимо подтвердить кнопкой «Да» действие в окне «Подтверждение» (Рисунок 12).

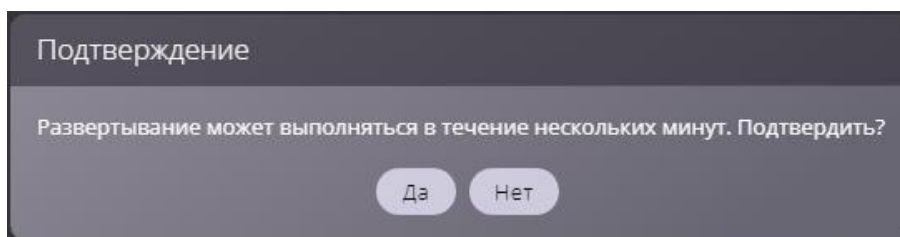


Рисунок 12. Подтверждение развертывания ловушек

Процесс развертывания ловушек в ИТ-инфраструктуре организации занимает несколько минут.

Завершающим этапом процесса сканирования подсети и развертывания в ней ловушек является установка приманок на рабочие места (Рисунок 13). Для скачивания приманок для систем Windows и Linux необходимо нажать соответствующие кнопки.

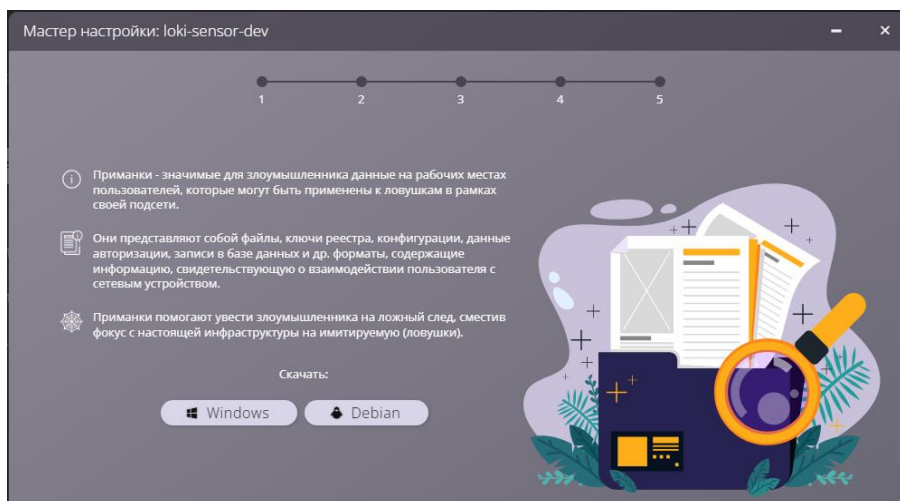


Рисунок 13. Скачивание приманок для установки на рабочие места

Приманки надо периодически обновлять, чтобы они оставались актуальными и привлекательными для злоумышленников. После любых операций с ловушками осуществляется автоматическая генерация новых приманок. Для того, чтобы скачать обновленные приманки необходимо в разделе «Инфраструктура» найти нужный сенсор и нажать на иконку «Информация» напротив его имени. В открывшемся окне перейти во вкладку

«Приманки» и нажать кнопку «Windows» или «Debian» в зависимости от системы, в которой планируется развертывание приманок (Рисунок 14).

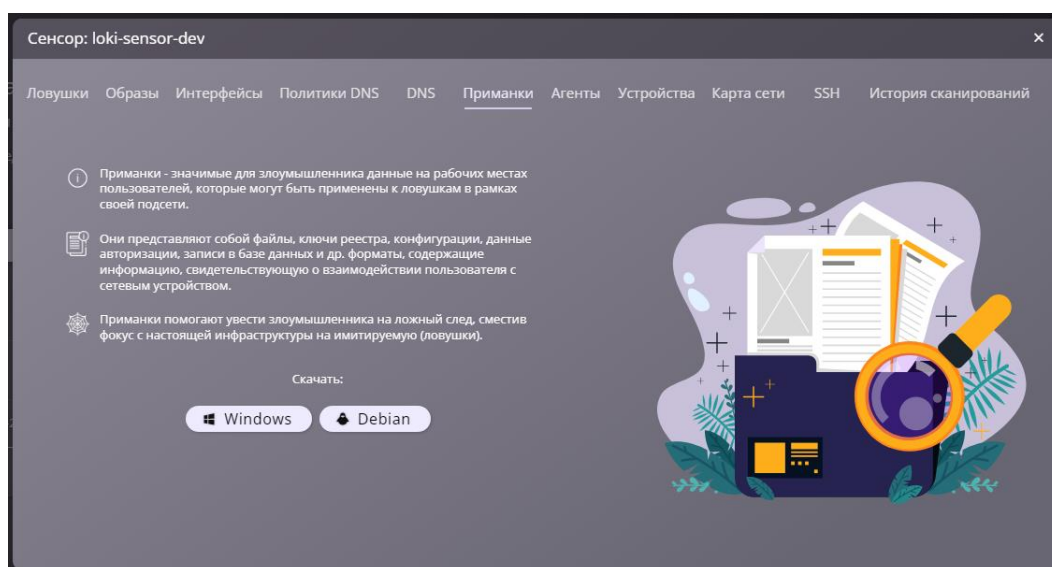


Рисунок 14. Вкладка «Приманки»

Если сканирование было остановлено по желанию пользователя, его можно продолжить. Для этого необходимо в разделе «Инфраструктура» во вкладке «Сенсоры» нажать на кнопку «Мастер настройки» напротив сенсора, которым ранее проводилось сканирование. В открывшемся окне можно осуществить перезапуск сканирования, нажав кнопку «Запустить сканирование» (Рисунок 15).

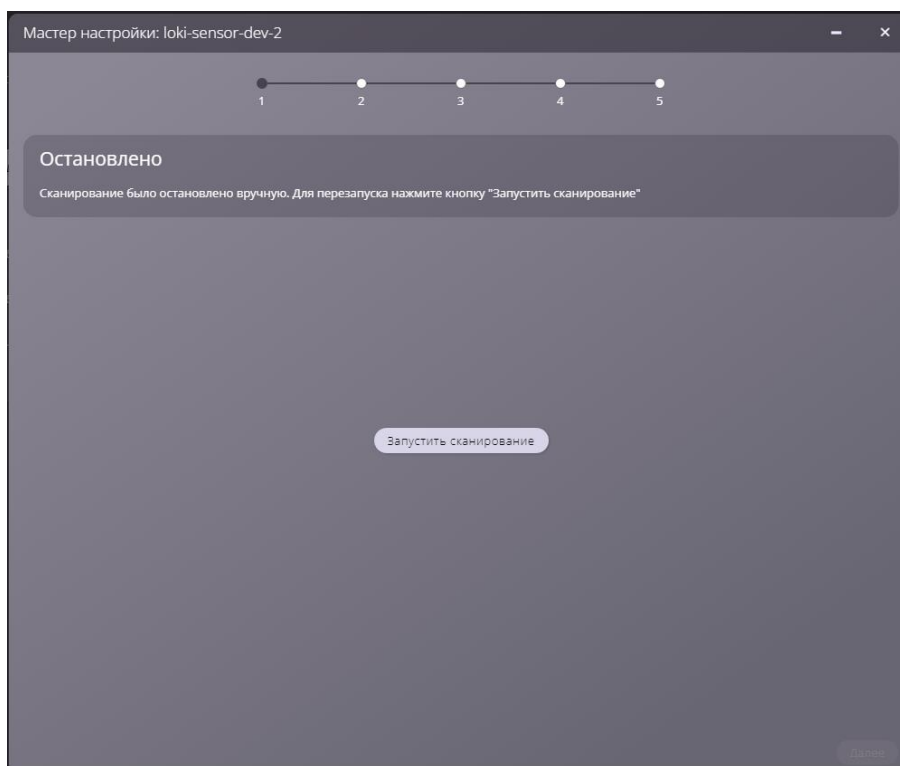


Рисунок 15. Перезапуск сканирования

Далее необходимо подтвердить кнопкой «Да» действие в окне «Подтверждение» (Рисунок 16).

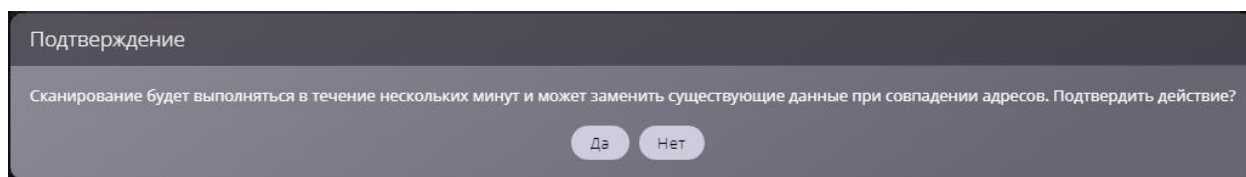


Рисунок 16. Подтверждение сканирования

5.3 Сканирование уязвимостей

Для осуществления сканирования уязвимостей ИТ-инфраструктуры необходимо нажать кнопку «Сканирование» во вкладке «Сенсоры» в разделе «Инфраструктура». В появившемся окне необходимо выбрать сенсор в нужной подсети и указать тип сканирования – «Сканирование уязвимостей». В поле «Цель» можно указать адрес конкретного устройства для проведения индивидуального сканирования, в противном случае сенсор проведёт сканирование уязвимостей всей доступной ему части инфраструктуры. Чтобы перейти к запуску сканирования, необходимо нажать на кнопку «Запустить» (Рисунок 17).

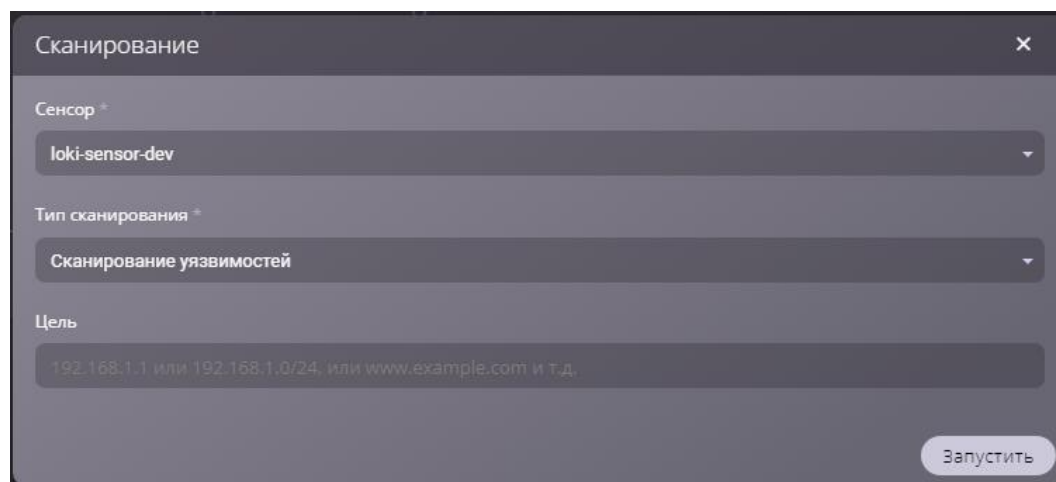


Рисунок 17. Сканирование уязвимостей

В появившемся окне с помощью иконки «История сканирований» можно посмотреть результаты предыдущих сканирований. Чтобы запустить новое сканирование, необходимо нажать на кнопку «Запустить сканирование».

По ходу сканирования в таблице под строкой состояния будут появляться выявленные уязвимости. С помощью иконки «Отменить сканирование» можно остановить процесс сканирования уязвимостей.

Результатом сканирования является список уязвимостей, выявленных в

устройствах организации, с указанием CVE ID и списка IP-адресов уязвимых устройств.

5.4 Промышленные сенсоры

Для просмотра информации по сенсору во вкладке «Сенсоры» → «Промышленные» необходимо нажать на иконку «Информация» напротив выбранного сенсора. В появившемся окне во вкладке «Ловушки» отображаются ловушки, развернутые на выбранном сенсоре (Рисунок 18).

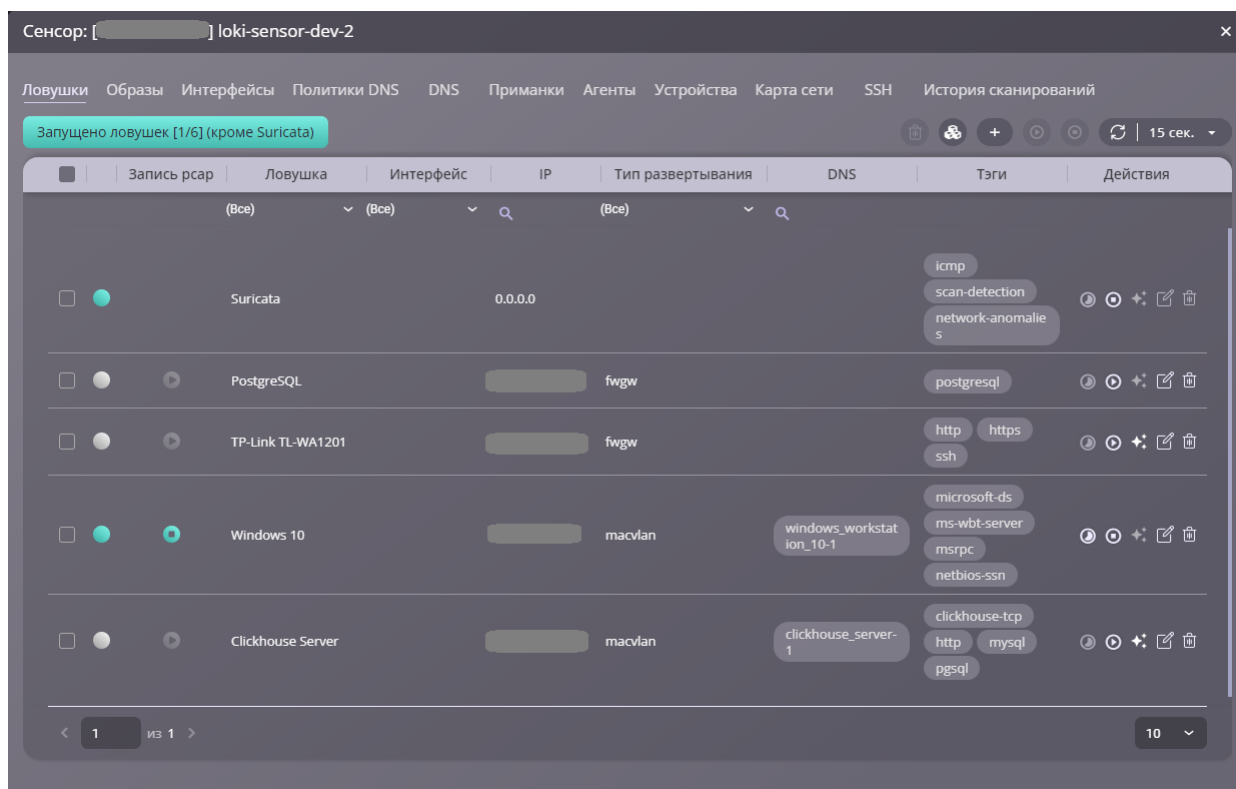


Рисунок 18. Вкладка «Ловушки»

По каждой ловушке отображается её название, IP-адрес, тип ее развертывания, тэги, характеризующие её функционал, и состояние в виде цветной индикации: зелёный – ловушка запущена, оранжевый – процесс включения/отключения, серый – остановленное состояние ловушки. С помощью описанных ранее иконок можно осуществлять запуск, остановку и удаление выбранных ловушек, а также скачать их лог-файлы. При нажатии иконки «Редактировать» в появившемся окне можно задать новые IP и MAC адреса ловушки, выбрать доступный тип развертывания в соответствующем поле, а также изменить текущее доменное имя (Рисунок 19). После завершения ввода данных необходимо нажать на кнопку «Сохранить».

Рисунок 19. Редактирование ловушки

Для добавления новой ловушки необходимо воспользоваться кнопкой «Добавить». В появившемся окне необходимо выбрать тип ловушки из раскрывающегося списка, поля «IP», «MAC», «DNS» и «Интерфейс» заполняются при необходимости (Рисунок 20). В случае сохранения пустых упомянутых полей IP, MAC, тип развертывания и DNS адреса ловушки генерируются автоматически. После завершения ввода данных необходимо нажать на кнопку «Сохранить».

Рисунок 20. Добавление ловушки

В случае http/https ловушек система предоставляет возможность задать содержимое отображаемой веб-страницы. Редактирование шаблона страницы можно осуществить с помощью иконки «Шаблон стартовой страницы» (Рисунок 21).

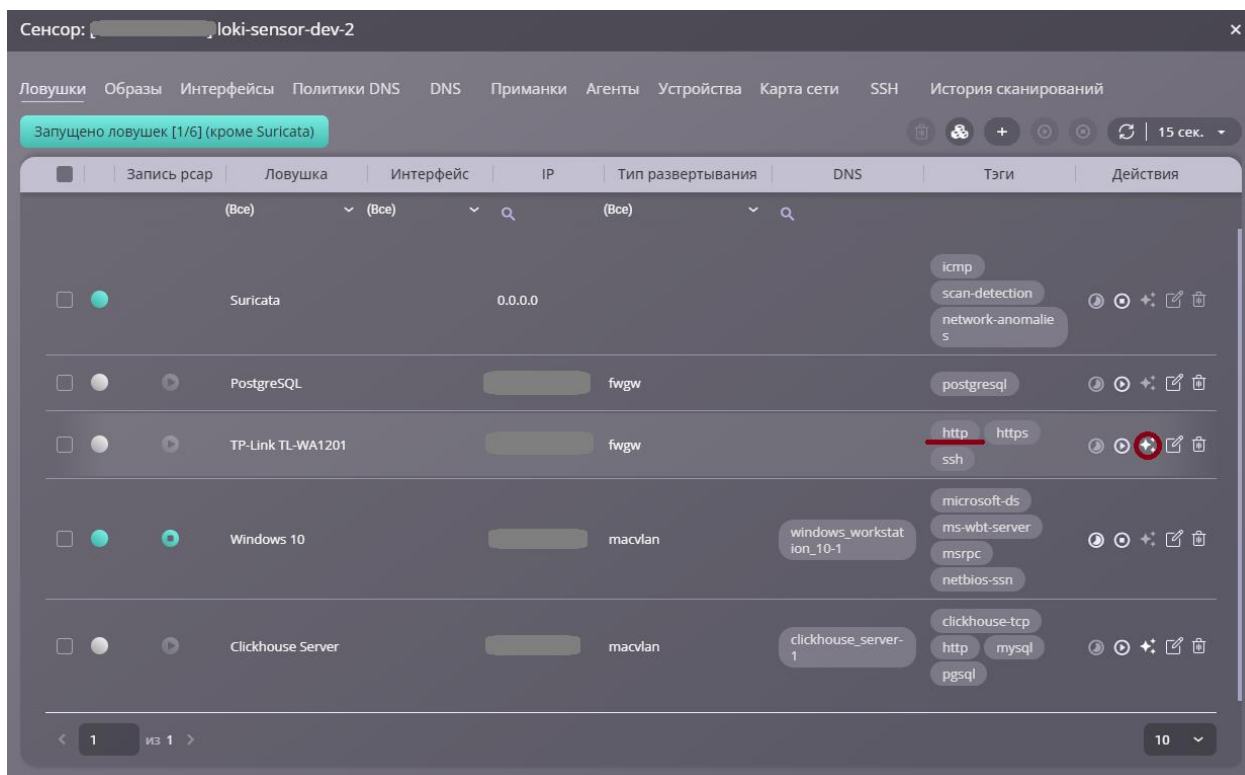


Рисунок 21. Иконка «Шаблон стартовой страницы»

В появившемся окне можно осуществить загрузку HTML файла с данными для стартовой страницы ловушки (Рисунок 22). При загрузке на ловушку пользовательской HTML страницы поддерживается формат UTF-8.

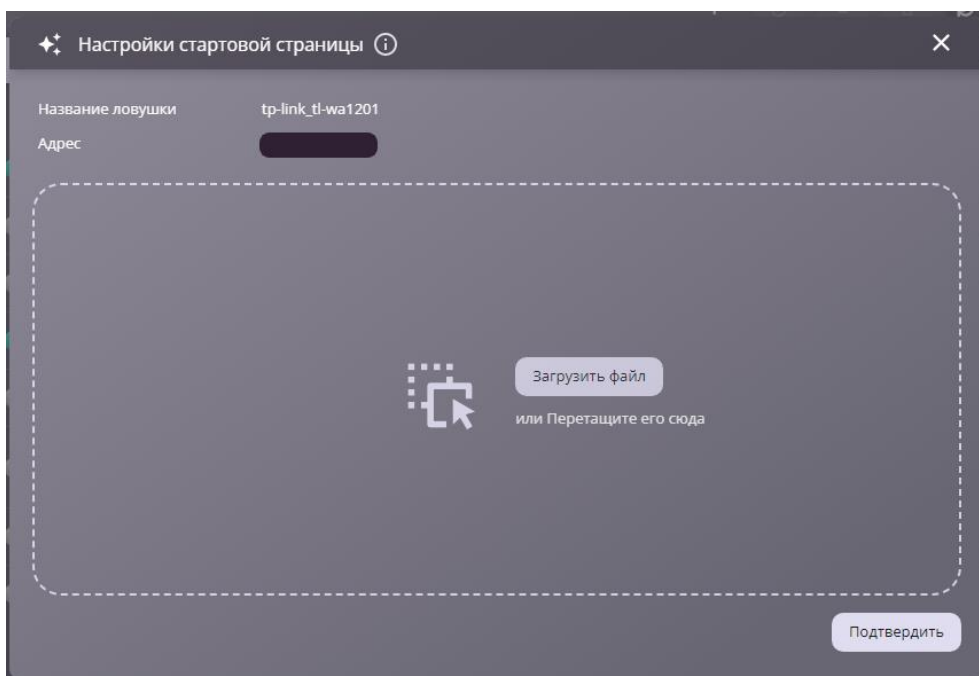


Рисунок 22. Редактирование шаблона стартовой страницы ловушки

После загрузки шаблона необходимо нажать на кнопку «Подтвердить», а затем осуществить перезапуск ловушки с помощью иконок «Остановить» и «Запустить».

При выделении галочками несколько ловушек становятся доступны групповые операции запуска, остановки и удаления с помощью соответствующих иконок над таблицей с ловушками (Рисунок 23).

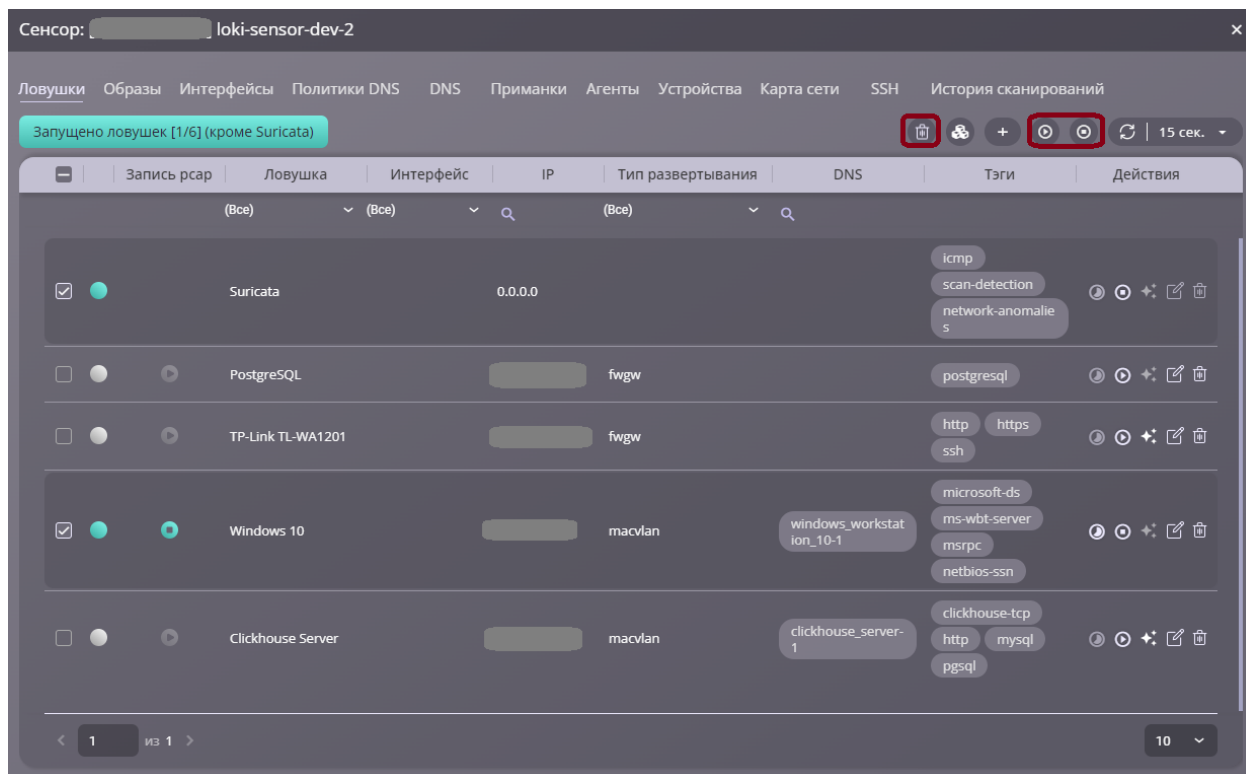


Рисунок 23. Групповые операции над ловушками

При удалении любых объектов в системе LOKI с помощью иконки «Удалить» система всегда отображает окно подтверждения (Рисунок 24).

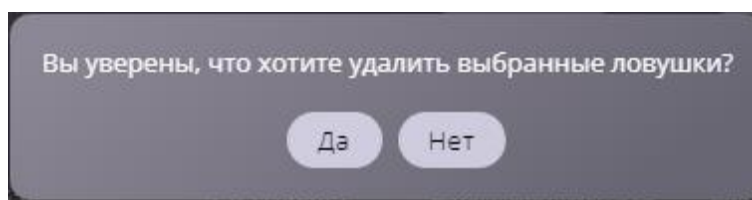


Рисунок 24. Окно подтверждения

Во вкладке «Образы» отображается список образов ловушек, доступных для развертывания на сенсоре (Рисунок 25). В данной вкладке доступны операции удаления выбранных образов и добавления новых с помощью описанных ранее иконок. По аналогии с предыдущей вкладкой при выделении нескольких образов становится доступна операция группового удаления образов.

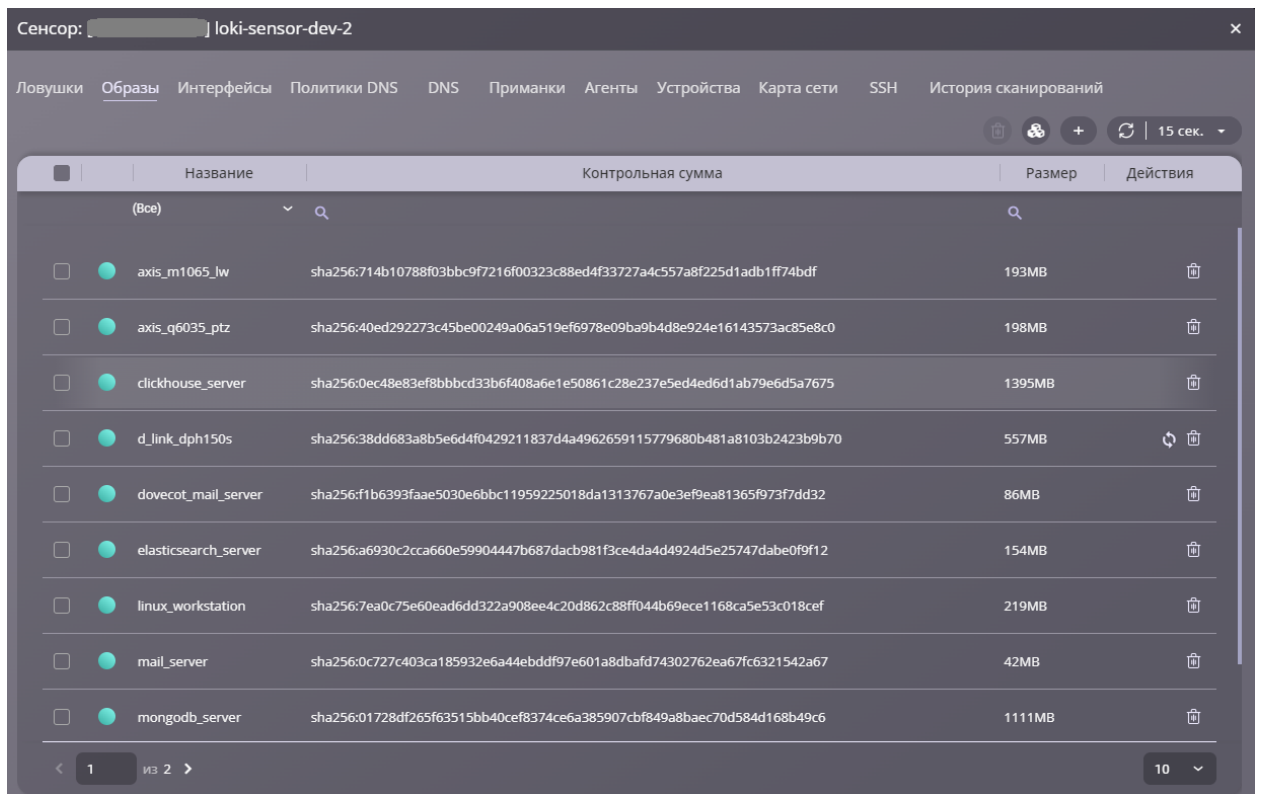


Рисунок 25. Вкладка «Образы»

При добавлении нового образа с помощью иконки «Добавить» в появившемся окне необходимо выбрать в выпадающем списке название образа для установки на сенсор (Рисунок 26). После выбора образа необходимо нажать на кнопку «Сохранить».

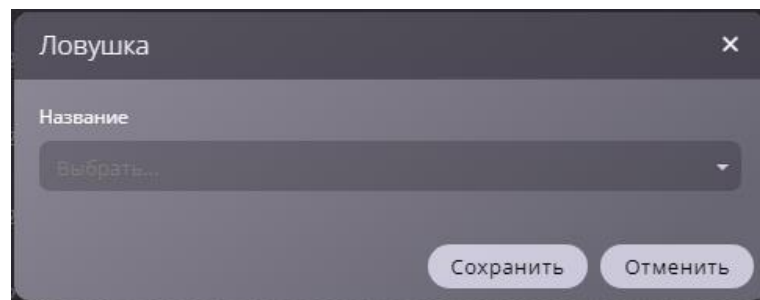


Рисунок 26. Добавление образа на сенсор

Во вкладке «Интерфейсы» представлен список сетевых интерфейсов, установленных на сенсоре (Рисунок 27).

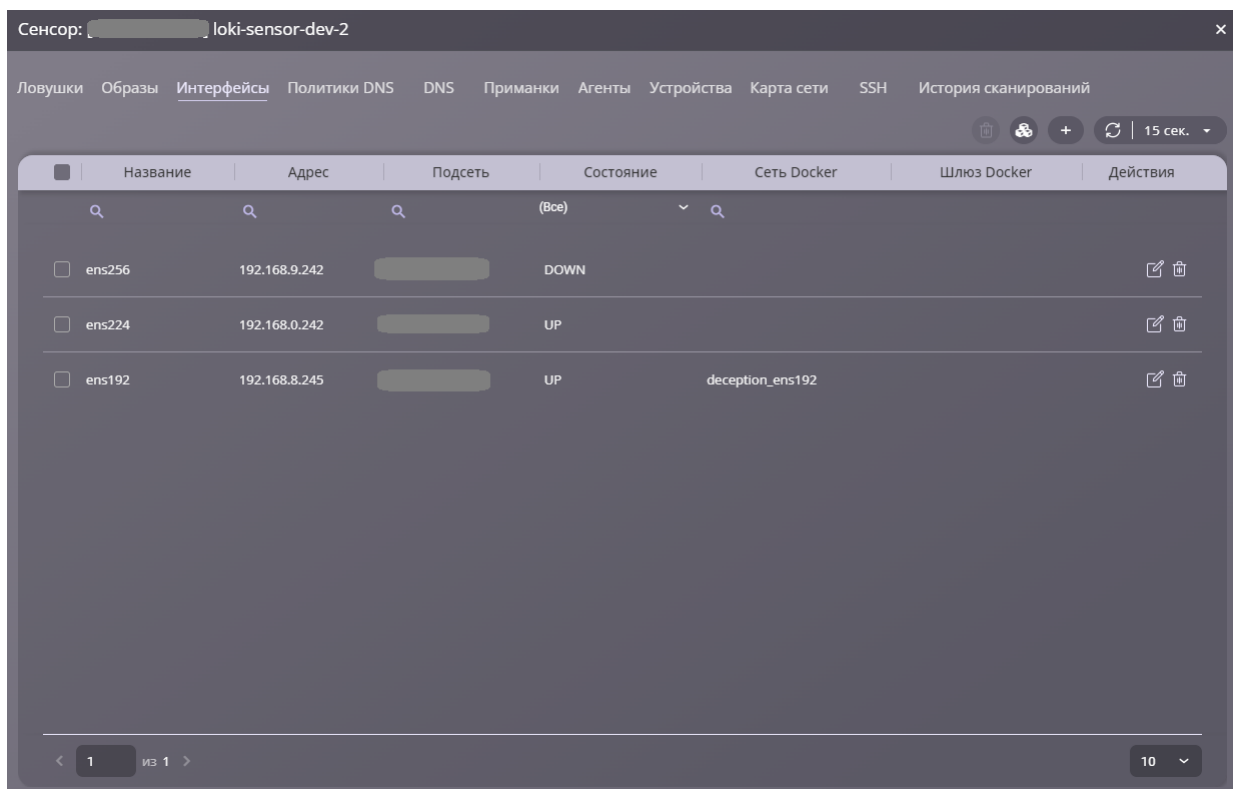


Рисунок 27. Вкладка «Интерфейсы»

Во вкладке «Политики DNS» (Рисунок 28) система предоставляет возможность задать правила автоматического создания FQDN ловушек для обеспечения соответствия используемым в инфраструктуре Заказчика наименованиям объектов (записям DNS).

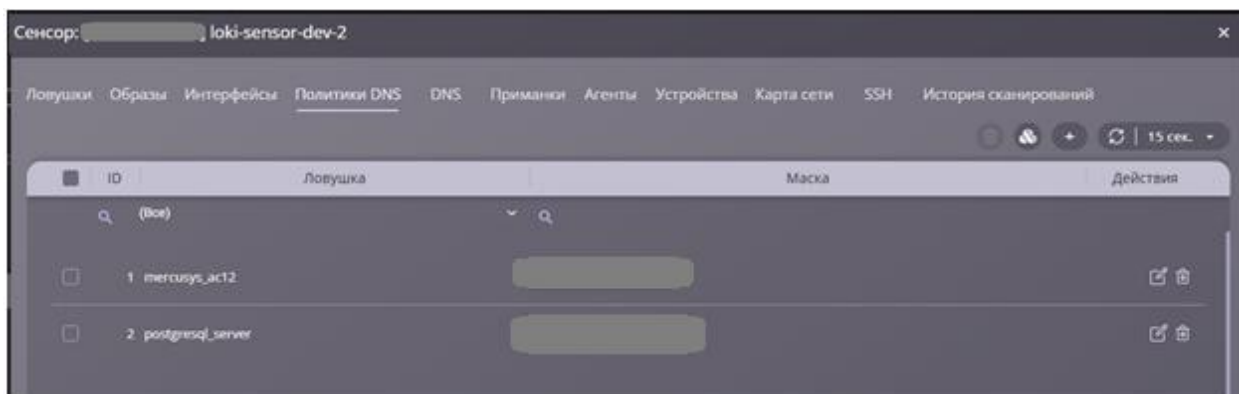


Рисунок 28. Вкладка «Политики DNS»

Во вкладке «DNS» представлен список доменных имен, назначенных ловушкам (Рисунок 29).

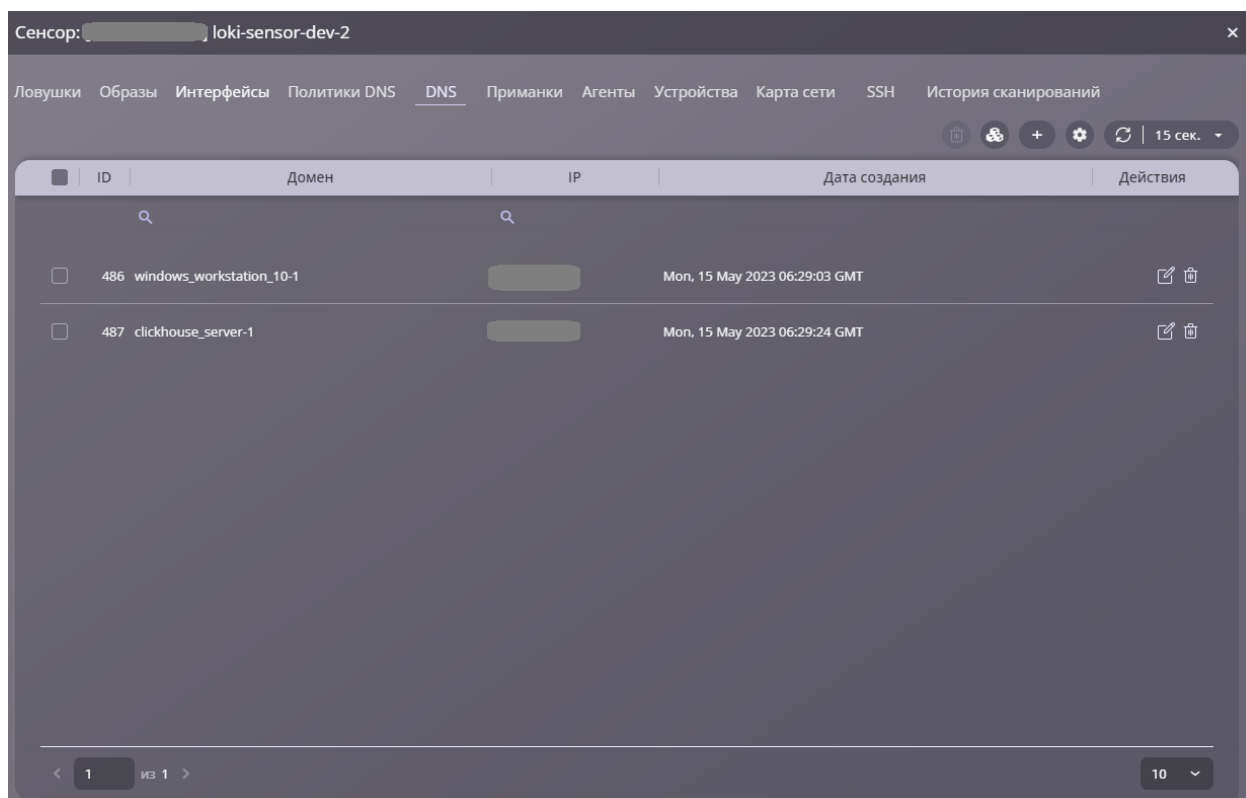


Рисунок 29. Вкладка «DNS»

После каждого развертывания ловушек система автоматически присваивает доменные имена новым ловушкам. Для того, чтобы изменить заданный FQDN ловушки, необходимо воспользоваться иконкой «Редактировать». В открывшемся окне пользователь может самостоятельно изменить доменное имя ловушки в поле «DNS» (Рисунок 30).

Рисунок 30. Редактирование DNS настроек ловушек

Аналогичные поля заполняются при добавлении доменного имени произвольному IP-адресу в подсети вручную с помощью иконки «Добавить».

Во вкладке «Приманки» предоставляется возможность скачивания приманок для последующей установки на устройства с операционными системами Linux и Windows (Рисунок 31).

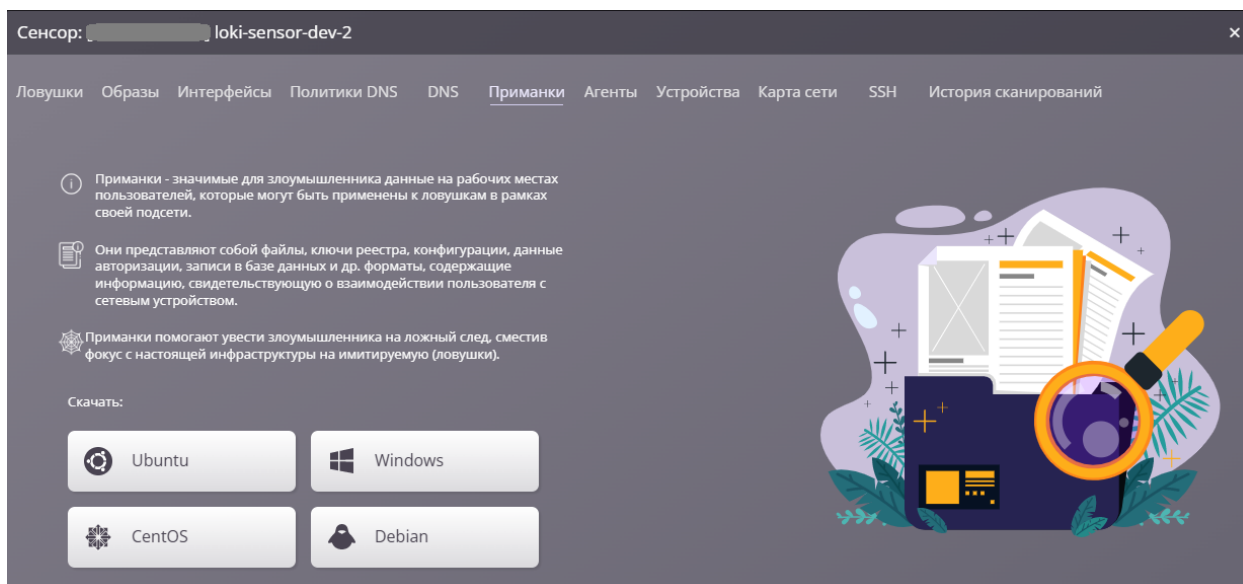


Рисунок 31. Вкладка «Приманки»

Во вкладке «Агенты» осуществляется скачивание агентов под операционные системы Windows и Linux (Рисунок 32). С помощью агентов можно осуществлять автоматическую установку и обновление приманок на устройствах, проверять наличие уязвимостей в программном обеспечении системы и пресекать распространение атаки в сети.

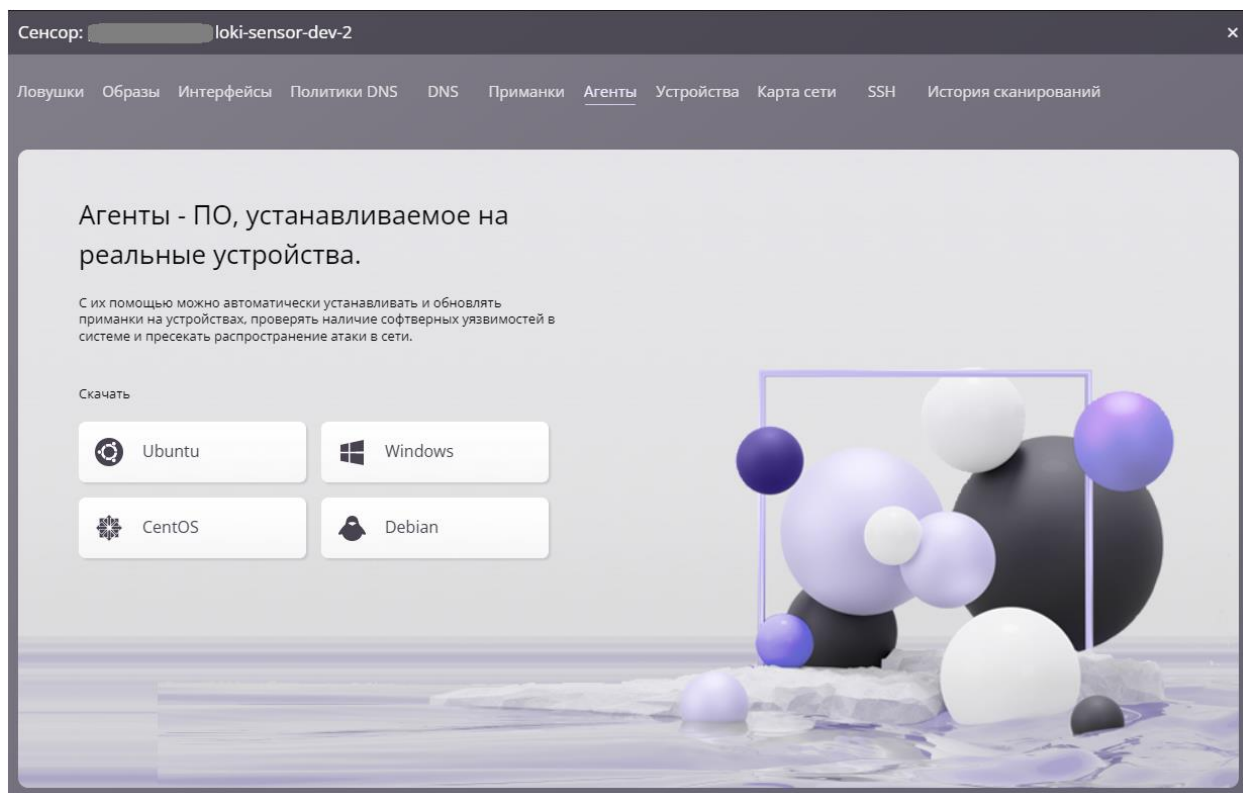


Рисунок 32. Вкладка «Агенты»

Во вкладке «Устройства» представлен список реальных устройств, расположенных в подсети выбранного сенсора с указанием их IP-адреса, типа и

операционной системы (Рисунок 33). В данной вкладке доступны операции добавления, редактирования и удаления из списка устройств с помощью соответствующих иконок. Зеленым горят устройства, которые необходимо проверить, серым соответственно горят те устройства, которые уже были проверены, также это можно сделать вручную, нажав на кнопку напротив «Отметить проверенным».

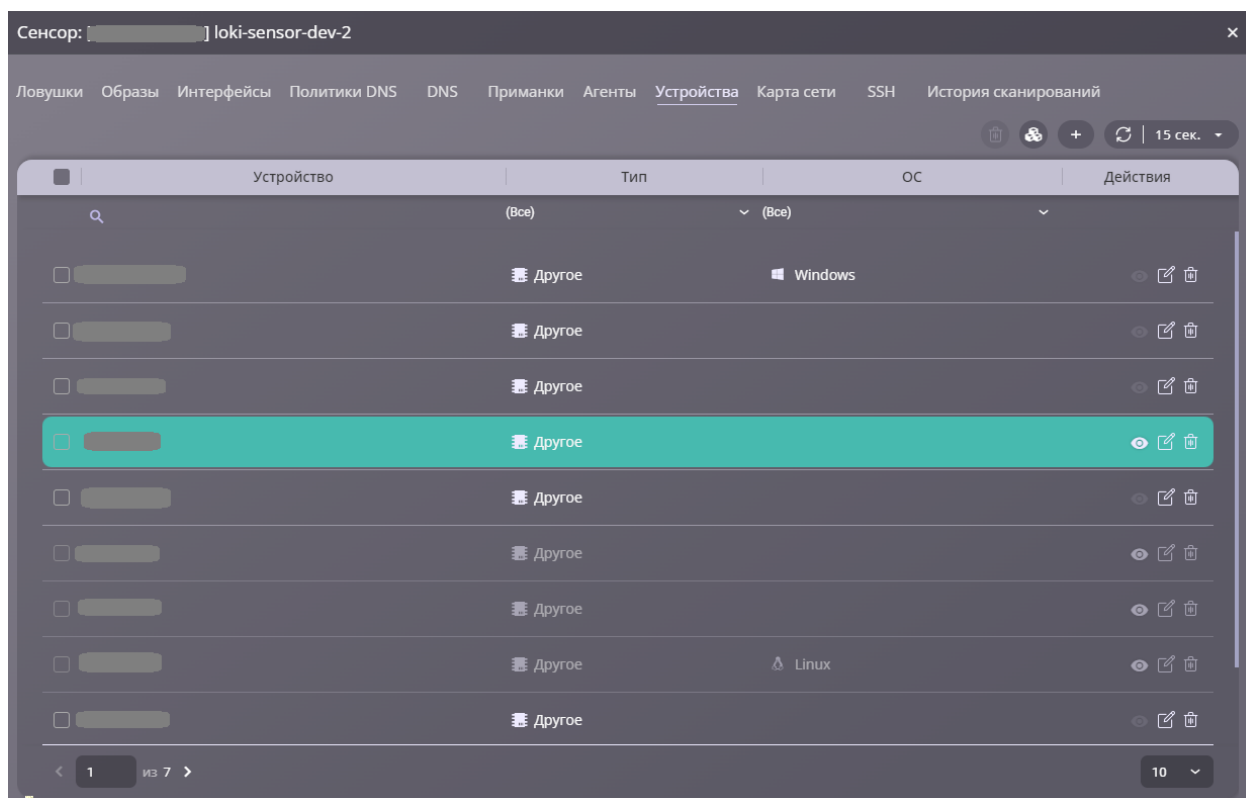


Рисунок 33. Вкладка «Устройства»

При добавлении нового устройства с помощью иконки «Добавить» в появившемся окне необходимо указать IP-адрес, тип и операционную систему нового устройства (Рисунок 34). После внесения данных необходимо нажать на кнопку «Сохранить».

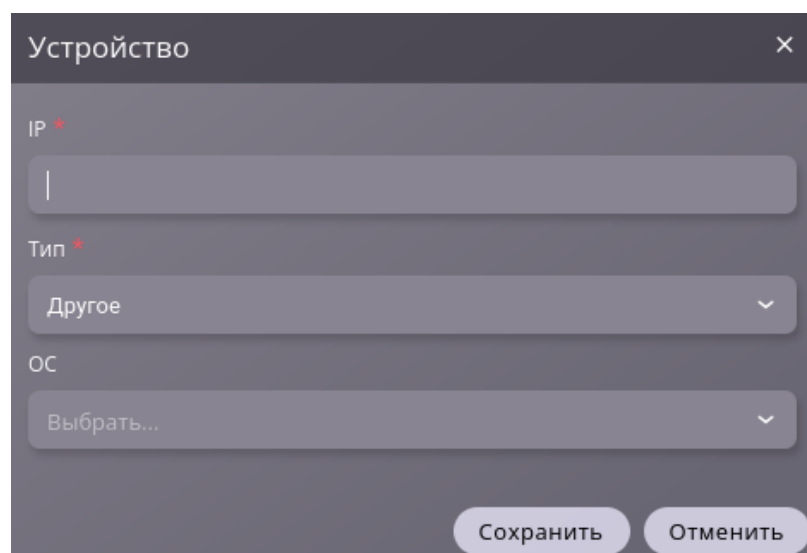


Рисунок 34. Добавление нового устройства

Аналогичные поля предоставляются для корректировки при редактировании устройства из списка с помощью иконки «Редактировать».

Во вкладке «Карта сети» отображается интерактивная карта подсети, в которой установлен сенсор (Рисунок 35). На карте с помощью цветовой индикации отображаются реальные устройства, развернутые ловушки и приманки.

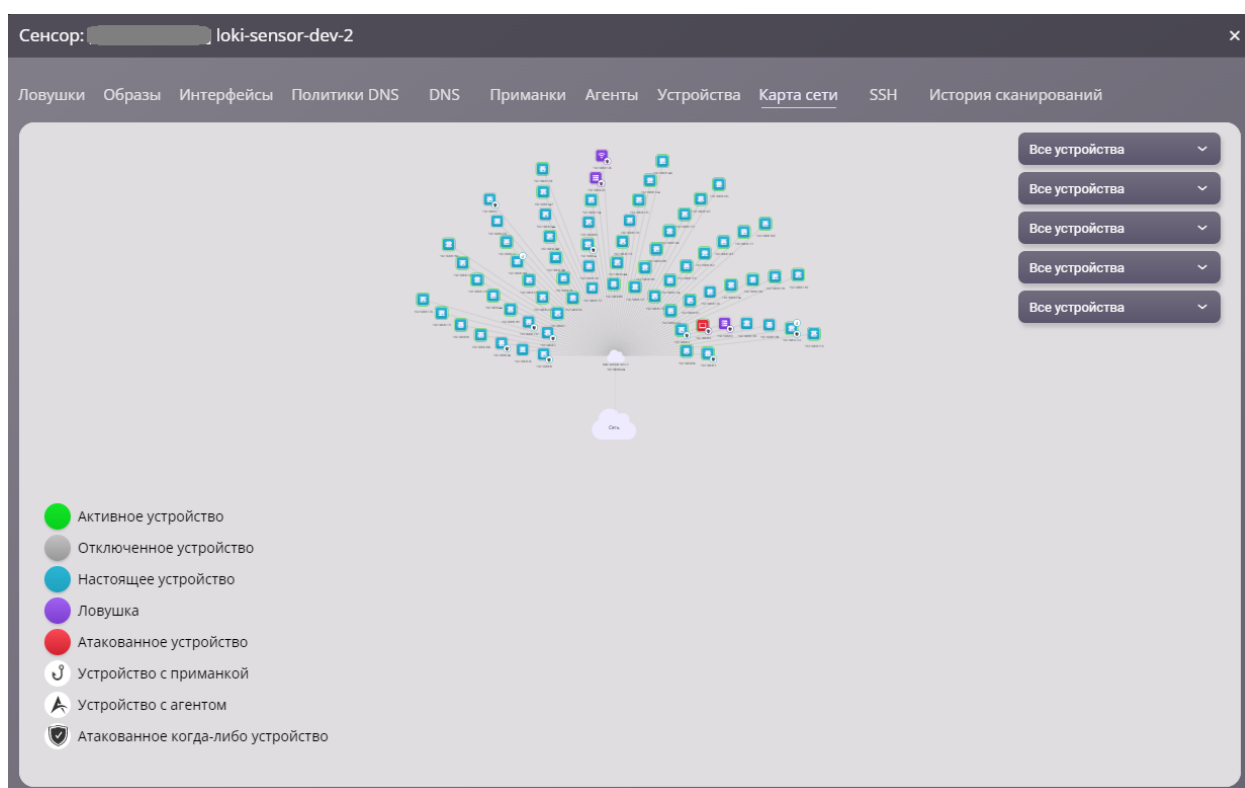


Рисунок 35. Вкладка «Карта сети»

При нажатии на любое устройство или ловушку на карте выводится подробная информация по выбранному объекту, которая включает в себя IP-

адрес, тип и операционную систему.

Во вкладке «SSH» осуществляется управление сенсором по протоколу SSH (Рисунок 36).

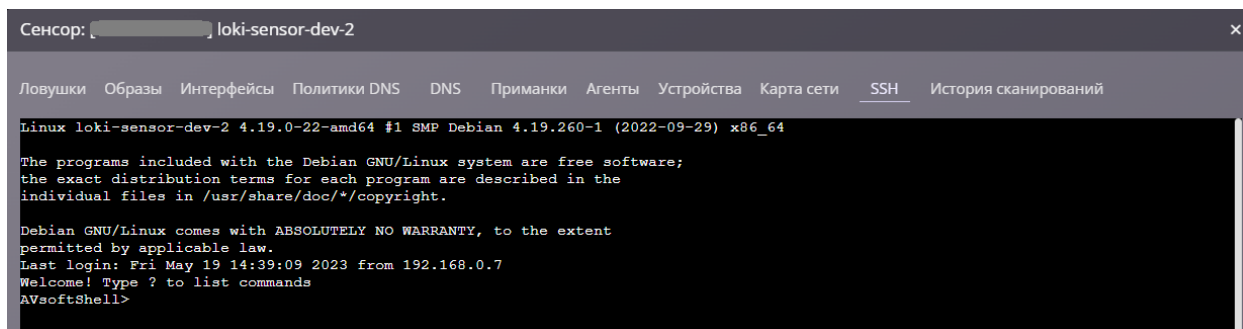


Рисунок 36. Вкладка «SSH»

Во вкладке «История сканирований» → «Сетевые» отображается список ранее проведенных сканирований выбранным сенсором (Рисунок 37). С помощью соответствующих иконок «Карта сети» и «Удалить» можно посмотреть карту сети по результатам выбранного сканирования или удалить результаты данного сканирования.

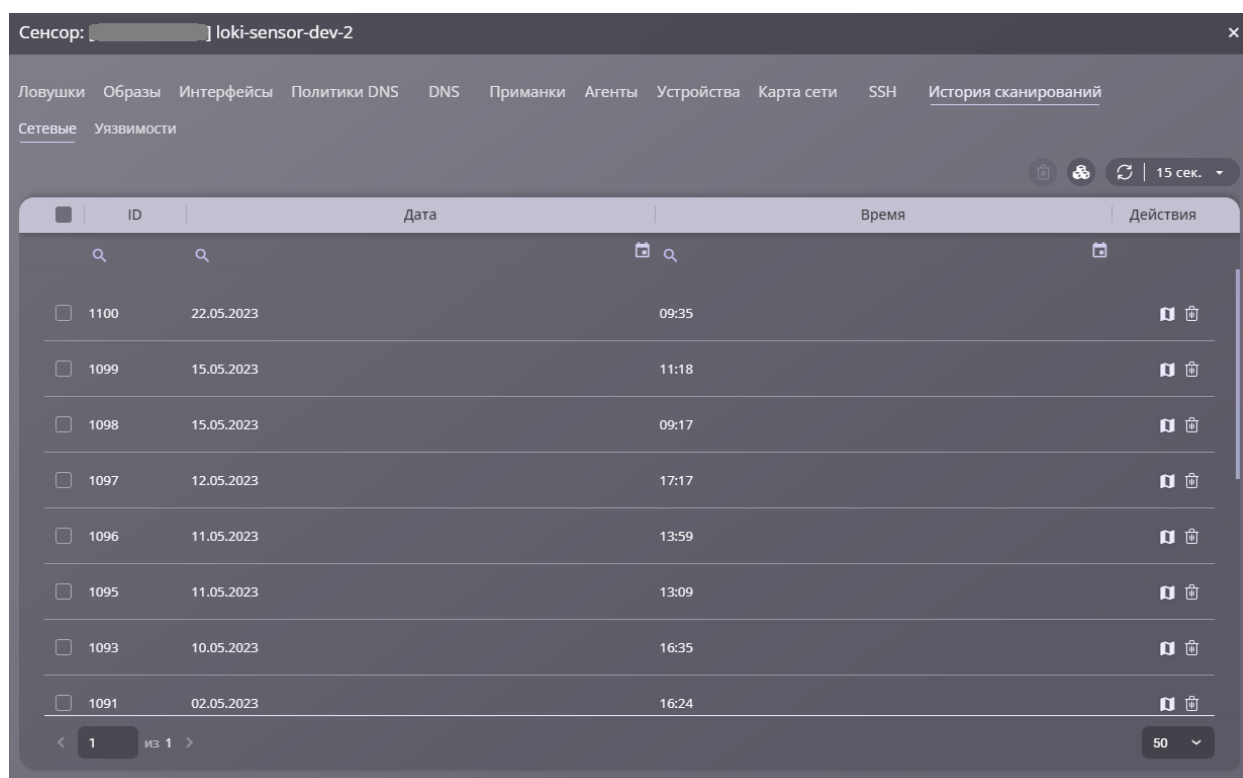


Рисунок 37. Вкладка «История сканирований»

Во вкладке «История сканирований» → «Уязвимости» отображается список ранее проведенных сканирований на уязвимости выбранным сенсором (Рисунок 38).

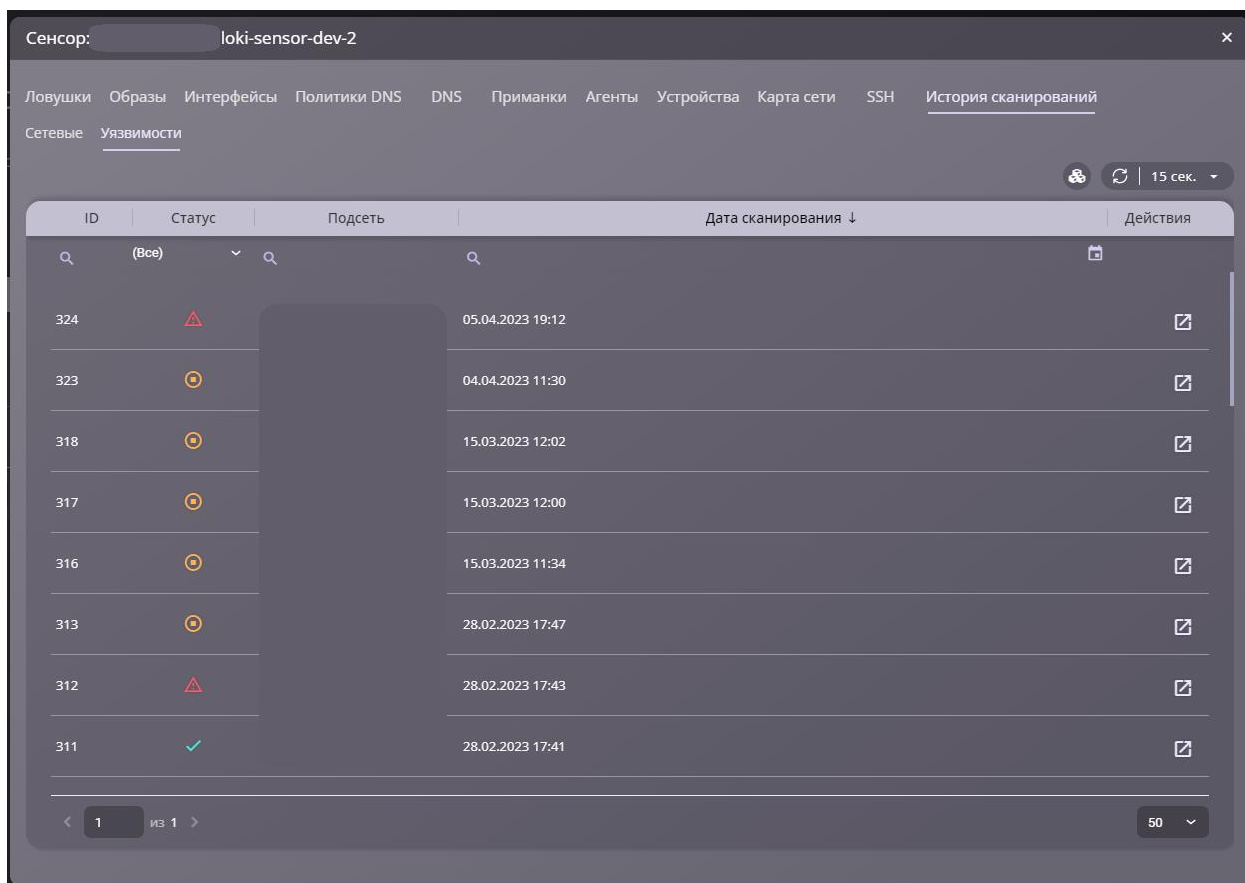


Рисунок 38. Вкладка «Уязвимости»

Для ознакомления с результатами сканирования на уязвимости устройств выбранной подсети можно нажать на активную иконку в столбце «Действия» (Рисунок 39).

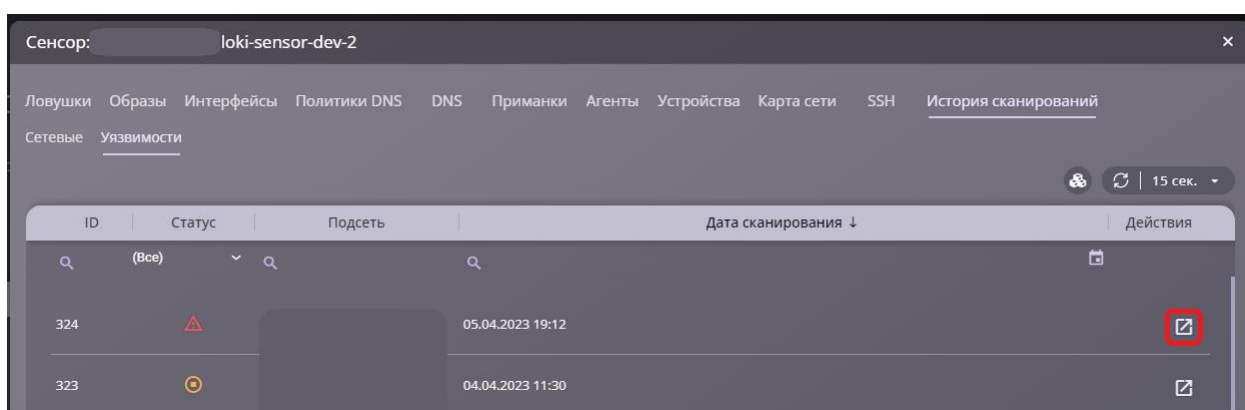


Рисунок 39. Активная иконка «Открыть»

В открывшемся окне будет представлена информация по найденным уязвимостям во время сканирования (Рисунок 40).

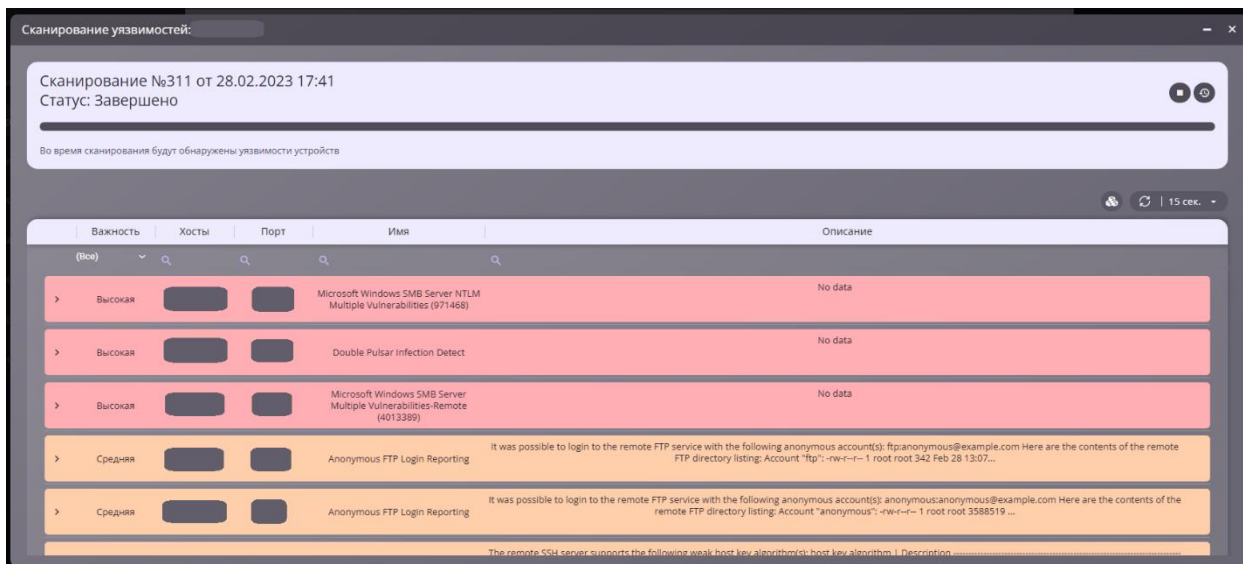


Рисунок 40. Таблица найденных во время сканирования уязвимостей

5.5 Исследовательские сенсоры

В вкладке «Исследовательские» отображаются все подключенные к системе LOKI сенсоры и размещенные на них ловушки, развернутые вне инфраструктуры организации. Данный раздел содержит перечень внешних сенсоров и исследовательских ловушек, цель которых – собирать данные о проведенных на них атаках и предоставлять их в систему LOKI для более глубокого изучения артефактов атак (Рисунок 41).

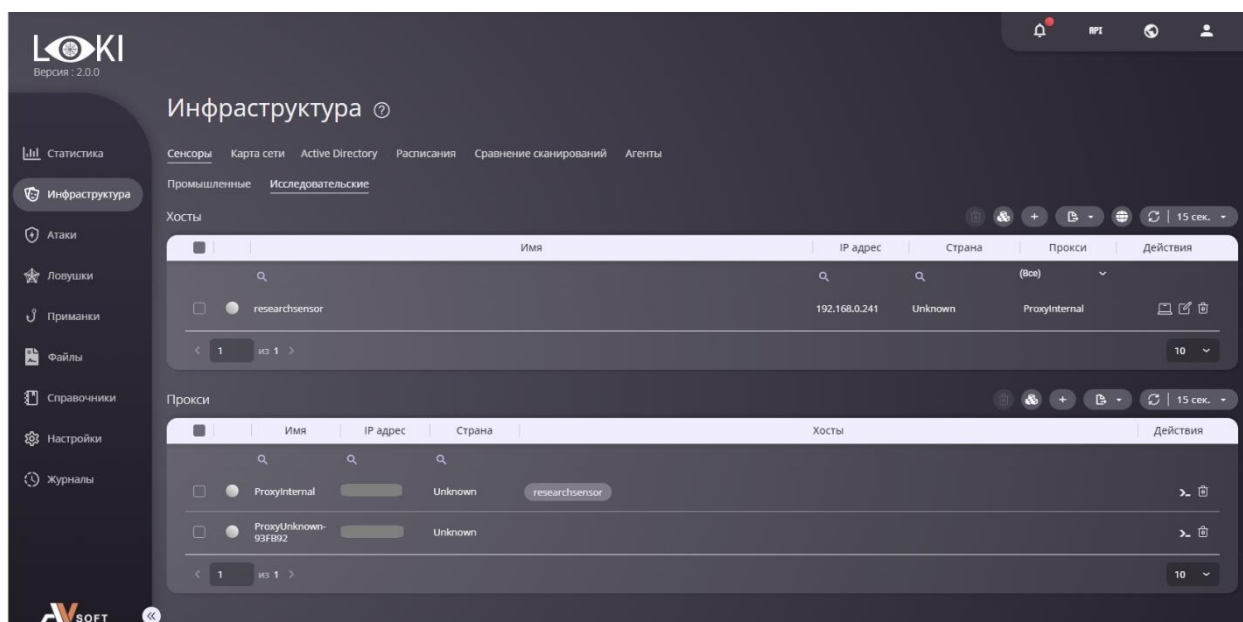


Рисунок 41. Вкладка «Исследовательские»

Таблица «Хосты» вкладки «Сервисы» содержит список внешних сенсоров с отображением установленных на них ловушек и их образов. Слева от сенсора располагается индикатор его активности.

Подключение нового внешнего сенсора к системе LOKI осуществляется при помощи иконки «Добавить» над таблицей «Хосты» (Рисунок 42).

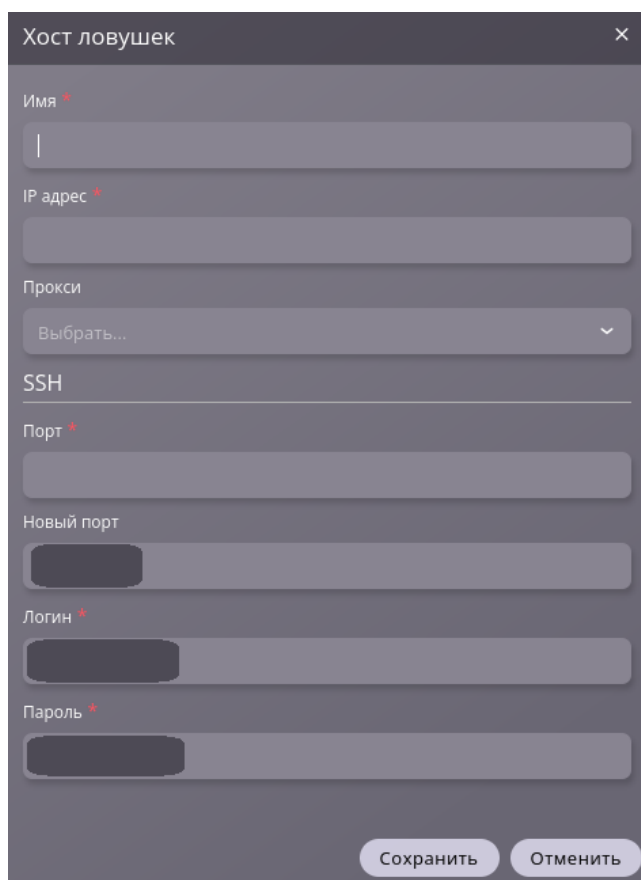


Рисунок 42. Добавление внешнего сенсора

В открывшейся форме необходимо заполнить поля в соответствии с их описанием в таблице 5.

Таблица 5. Поля формы добавление сенсора

№	Поле	Описание поля
1.	Имя	Произвольное имя внешнего сенсора
2.	IP-адрес	IP-адрес сенсора для SSH подключения
3.	Прокси	Прокси-сервер, используемый для соединения с сенсором
4.	SSH порт	Порт для SSH подключения. Содержит предустановленный параметр
5.	SSH новый порт	Новый порт для SSH подключения. Возможность указать параметр вручную.

№	Поле	Описание поля
6.	Логин	Имя пользователя для SSH сессии
7.	Пароль	Пароль пользователя для SSH сессии

После заполнения полей следует нажать на кнопку «Сохранить».

Для внесения изменений в данные внешнего сенсора, следует нажать на иконку «Редактировать» напротив сенсора в таблице «Хосты». В открывшейся форме, аналогичной форме добавления нового внешнего сенсора, следует внести нужные изменения и нажать кнопку «Сохранить».

Для просмотра данных по внешнему сенсору в таблице «Хосты» следует нажать на иконку «Информация» напротив него (Рисунок 43).

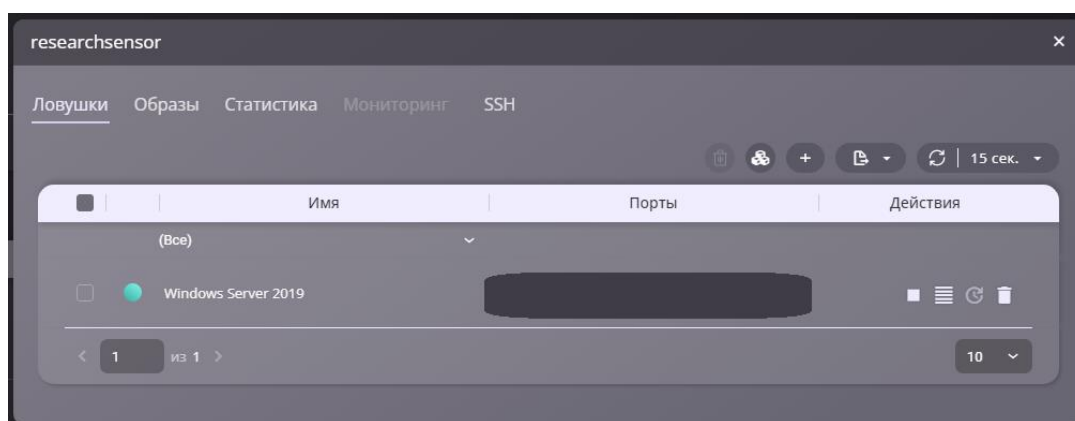


Рисунок 43. Информация о внешнем сенсоре

Во вкладке «Ловушки» формы информации о внешнем сенсоре перечислены все ловушки, размещенные на данном сенсоре. Количество размещенных ловушек зависит от технических характеристик сенсора.

Слева от ловушки отображается индикатор ее активности. Справа – элементы управления ловушкой. При нажатии иконку «Выключить» запустится процесс выключения активной ловушки. У выключенной ловушки появится иконка «Включить» для ее запуска. При нажатии на иконку «Получить логи», система сформирует файл, содержащий записи всех событий данной ловушки.

Во вкладке «Образы» формы информации о внешнем сенсоре содержится перечень образов, доступных к установке на ловушки данного сенсора (Рисунок 44).

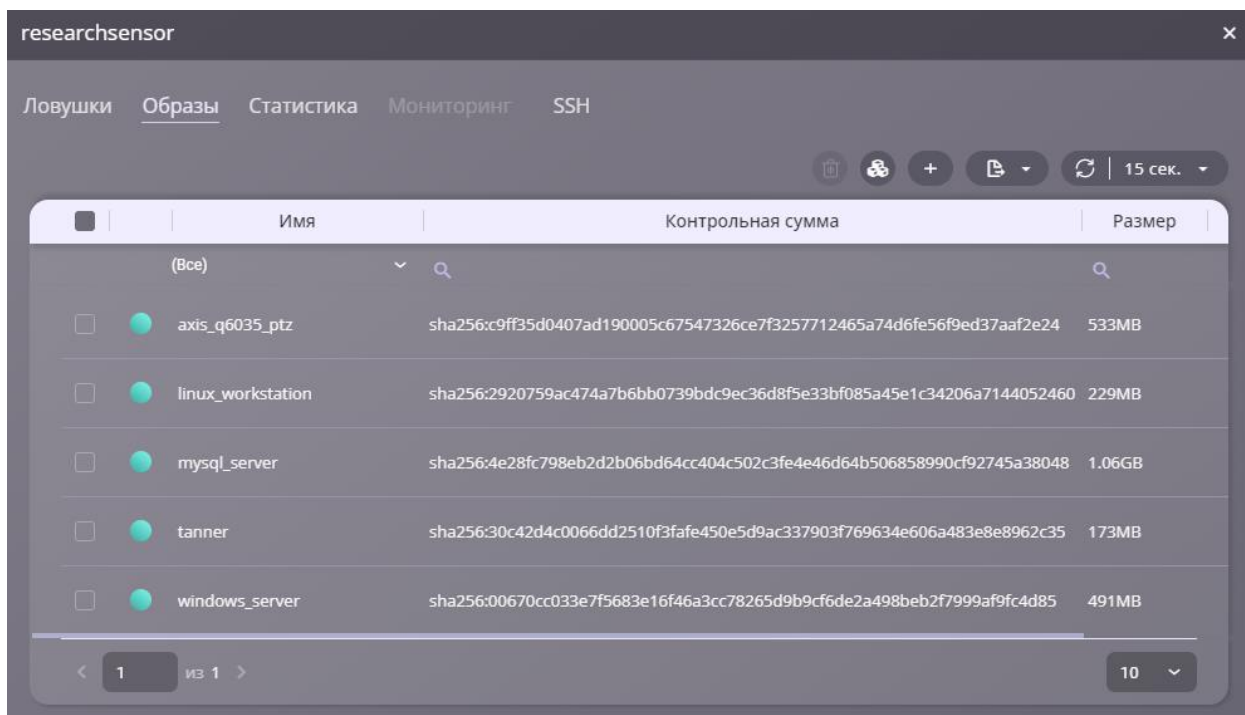


Рисунок 44. Список образов

Вкладка «Статистика» содержит статистические данные по подключениям к ловушкам в виде интерактивных графиков и диаграмм.

Вкладка «SSH» формы информации о внешнем сенсоре предоставляет защищенное подключение к сенсору по SSH.

Таблица «Прокси» содержит список используемых прокси-серверов с возможностью подключения к ним по SSH (Рисунок 41).

Прокси-серверы отвечают за установку и поддержание соединения с внешними сенсорами. Без прокси-сервера внешний сенсор не виден из сети. В сети видны только ловушки, установленные на нем, чтобы провоцировать злоумышленников их атаковать. Добавить внешний сенсор можно только через прокси-сервер, и поддерживать связь с таким сенсором тоже может только прокси-сервер.

Для добавления нового прокси-сервера надо нажать на кнопку «Добавить» в правом верхнем углу таблицы «Прокси» (Рисунок 45).

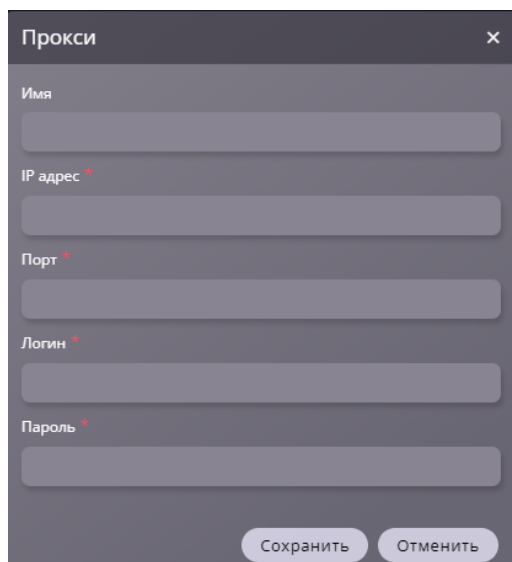


Рисунок 45. Добавление прокси-сервера

После заполнения данных по новому прокси-серверу необходимо нажать на кнопку «Сохранить».

Слева от прокси-сервера в таблице «Прокси» отображается индикатор его активации, справа – элементы управления сервером. При нажатии на иконку «SSH» предоставляется возможность защищенного подключения по SSH туннелю к данному прокси-серверу (Рисунок 46).

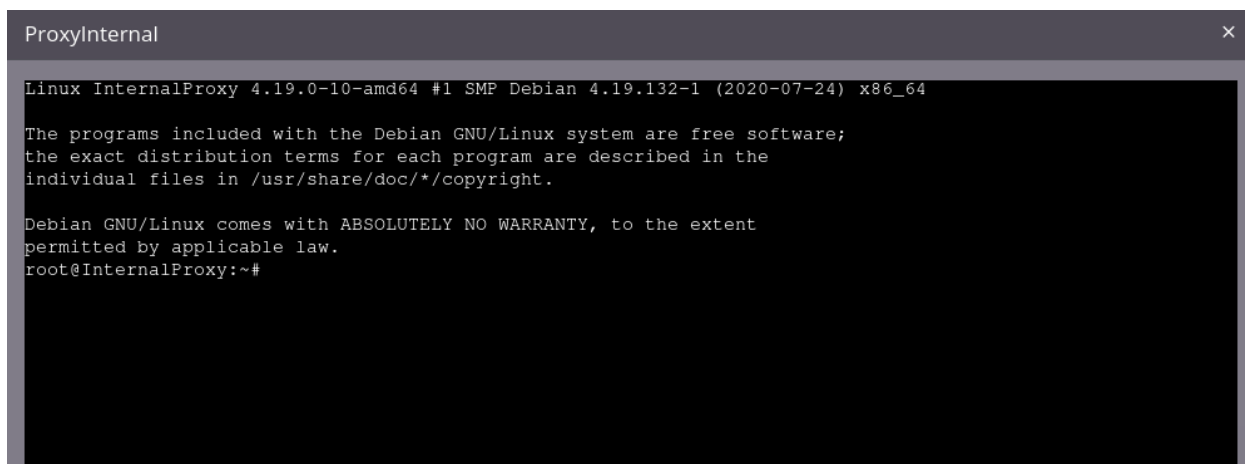


Рисунок 46. Подключение к прокси-серверу

5.6 Карта сети

Вкладка «Карта сети» раздела «Инфраструктура» отображает информацию по реальным устройствам, зафиксированным в организации по результатам сканирования, и развернутым ловушкам (Рисунок 47).

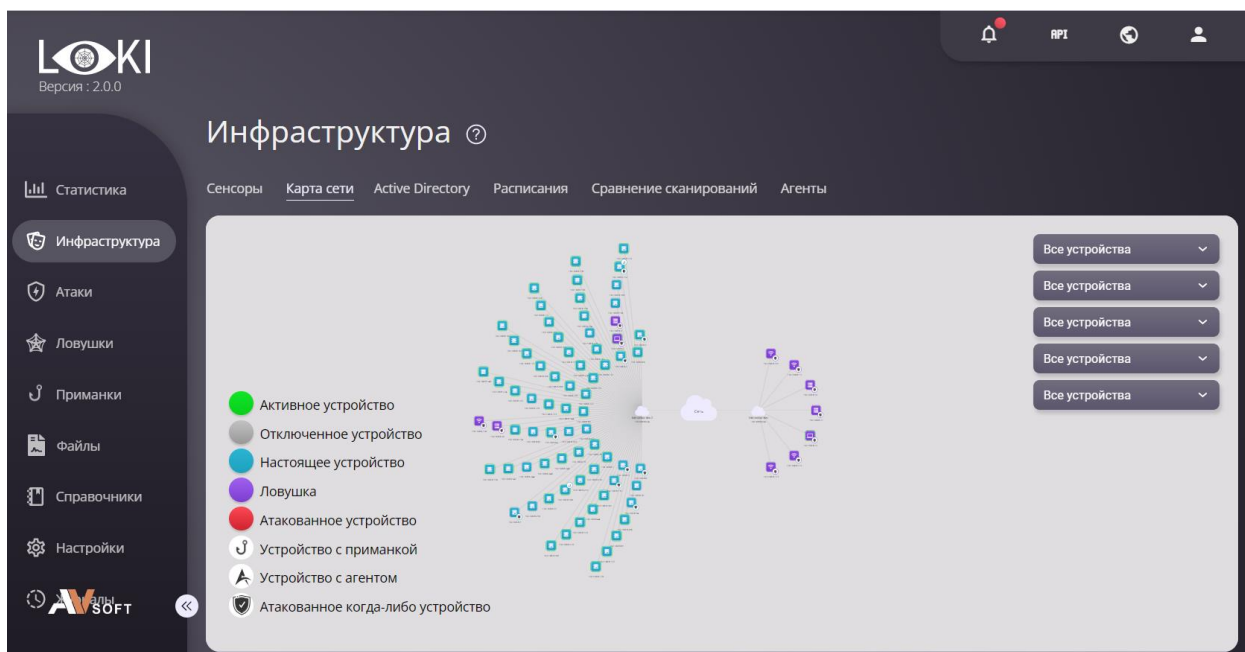


Рисунок 47. Вкладка «Карта сети»

При подключении злоумышленника к ловушке, на карте сети она отобразится красным цветом, сигнализируя об атаке на нее (Рисунок 48).

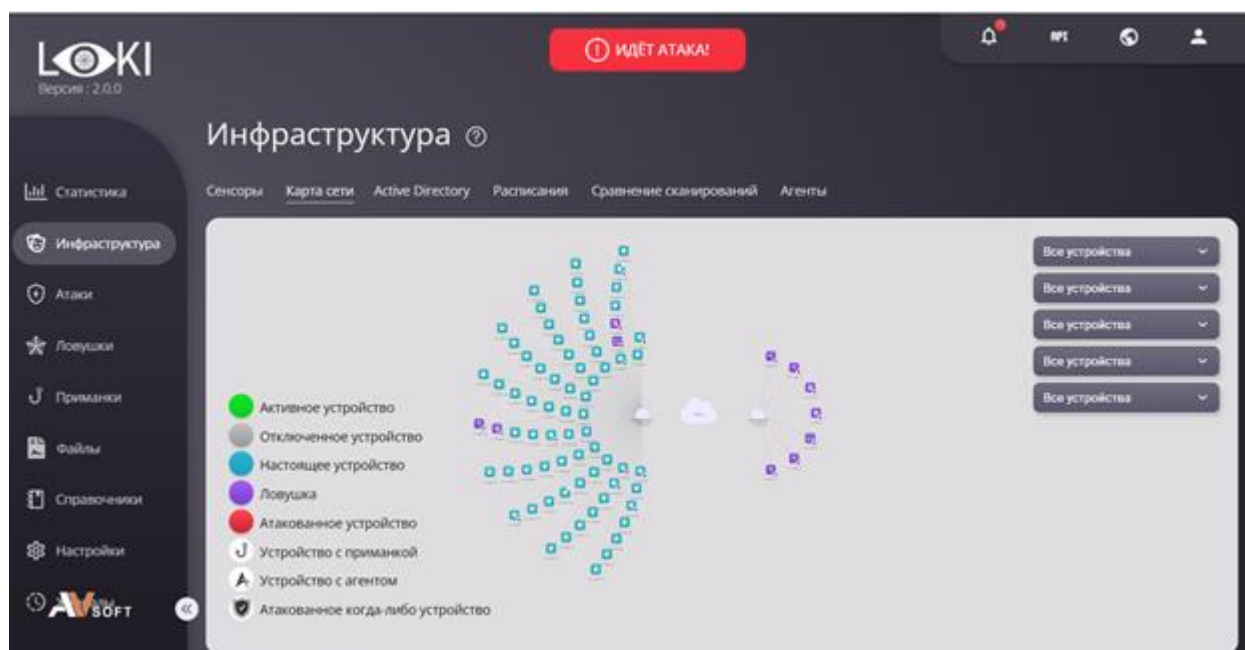


Рисунок 48. Отображение атаки на ловушку

5.7 Active Directory

В разделе «Инфраструктура» во вкладке «Active Directory» представлен список серверов Active Directory, к которым подключена система LOKI (Рисунок 49).

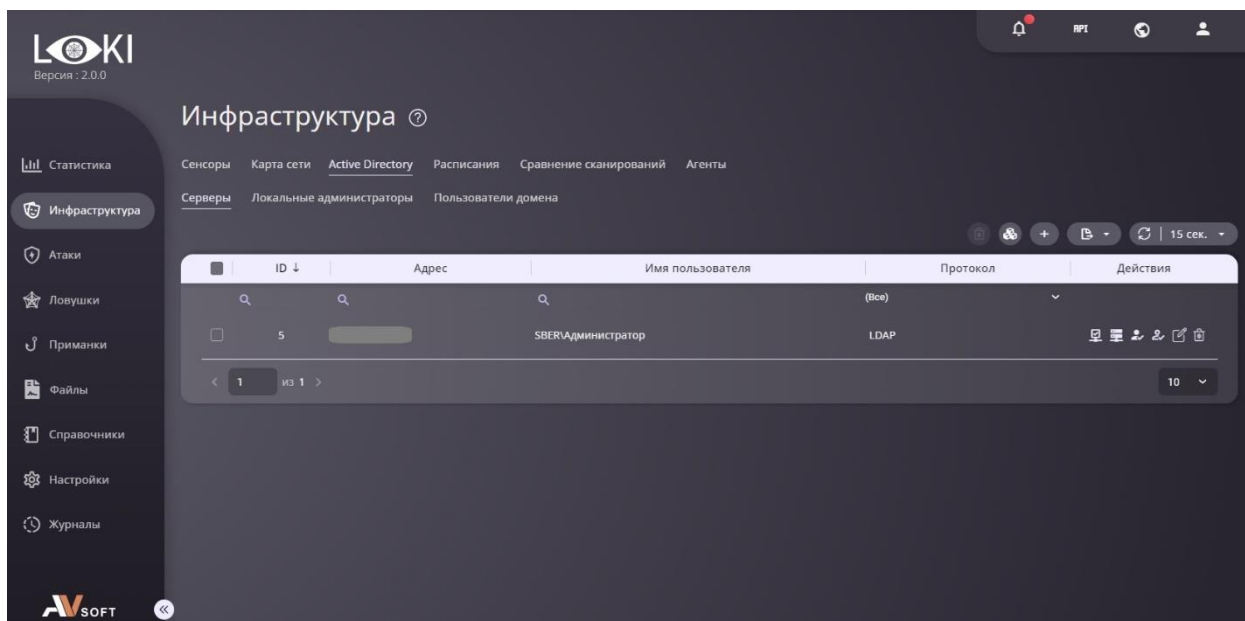


Рисунок 49. Вкладка «Серверы»

Интеграция со службой каталогов Active Directory позволяет осуществлять мониторинг учетных записей в домене, а также отслеживать неудачные попытки авторизации в инфраструктуре организации. Помимо этого, система предоставляет возможность использовать учетные записи AD в приманках.

При успешном подключении к серверу AD во вкладке «Локальные администраторы» отобразится список учетных записей локальных администраторов на устройствах в контролируемых доменах (Рисунок 50).

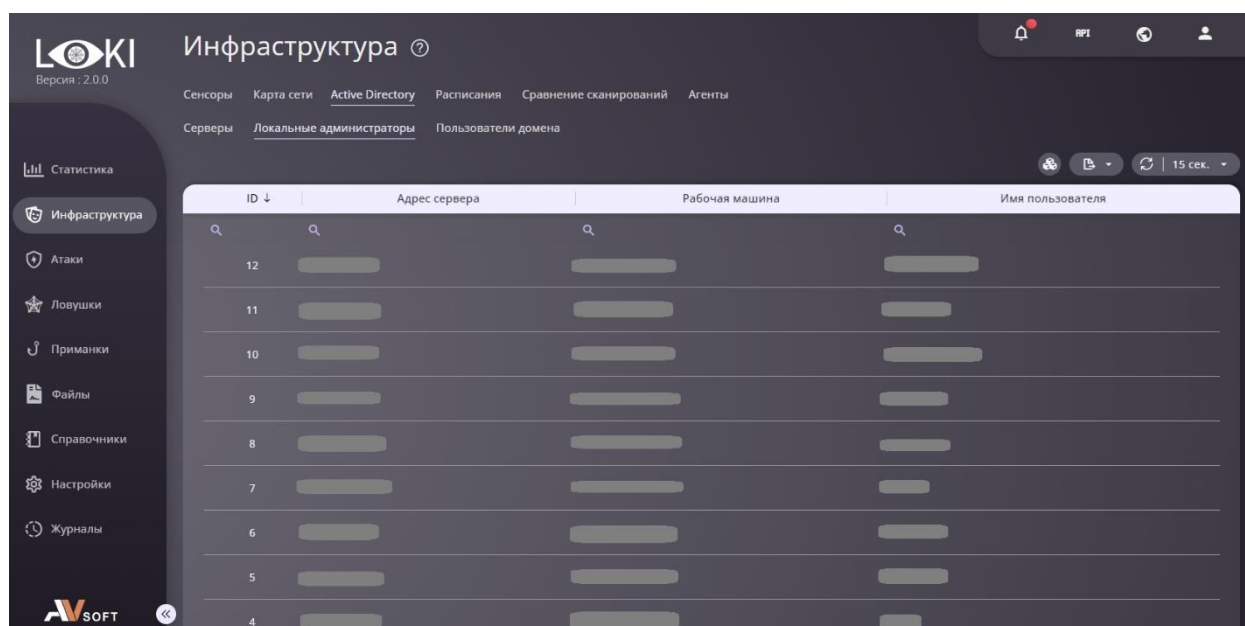


Рисунок 50. Вкладка «Локальные администраторы»

Помимо этого, во вкладке «Пользователи» отобразится полный список пользователей службы каталогов Active Directory с дополнительной

информацией по статусу учетной записи и актуальности пароля (Рисунок 51).

LOKI

версия: 2.0.0

Статистика

Инфраструктура

Атаки

Ловушки

Приманки

Файлы

Справочники

Настройки

Журналы

Инфраструктура

Сенсоры

Карта сети

Active Directory

Расписания

Сравнение сканирований

Агенты

Серверы

Локальные администраторы

Пользователи домена

15 сек.

ID пользователя	Имя пользователя	Последний вход	Заблокирован	Ложный	Не используется	Пароль истек	Пароль истекает	Пароль изменен	Адрес сервера	Компонент домена
09b50007-2429-4b50-93aa-9b70bc3f1b45		22.11.2022 10:49						21.11.2022 17:43	192.168.0.152	sber.test
0a1b087-b699-4f12-96b8-d265a25b8c7								18.04.2023 22:20	192.168.0.152	sber.test
0a95e42f-d26b-496b-8bc7-585461c04ef	ADMIN001-WIN	25.04.2023 18:12						28.03.2023 10:00	192.168.0.152	sber.test
148b8aa6-7f15-4b4a-ac85-2509fa5ade66								26.01.2023 13:43	192.168.0.152	sber.test
182d3743-c55b-4e3d-91a1-ac25a0954da6									192.168.0.152	sber.test
19182746-5568-4476-a4a6-6c726584c8a		19.04.2023 11:39						05.04.2023 13:37	192.168.0.152	sber.test
1a1f159f-6a8c-463a-baf3-1032ad3999c		19.04.2023 09:41						19.04.2023 09:26	192.168.0.152	sber.test
2068d8c-7a94-4f85-8882-1f6349485f6d		28.03.2023 22:32						30.12.2022 12:30	192.168.0.152	sber.test
296f0f48-9fa1-4ab1-bd85-8ad5b7c896a								03.05.2023 18:07	192.168.0.152	sber.test
2ab05106-b665-4210-8355-040810cb6ab2	Deploy User							20.12.2022 16:32	192.168.0.152	sber.test

1 из 5

10

AVSOFT

Рисунок 51. Вкладка «Пользователи домена»

5.8 Расписания

Система LOKI предоставляет возможность автоматического сканирования, управления ловушками, распространения и обновления приманок в соответствии с установленными расписаниями (предустановленными или определенными пользователем).

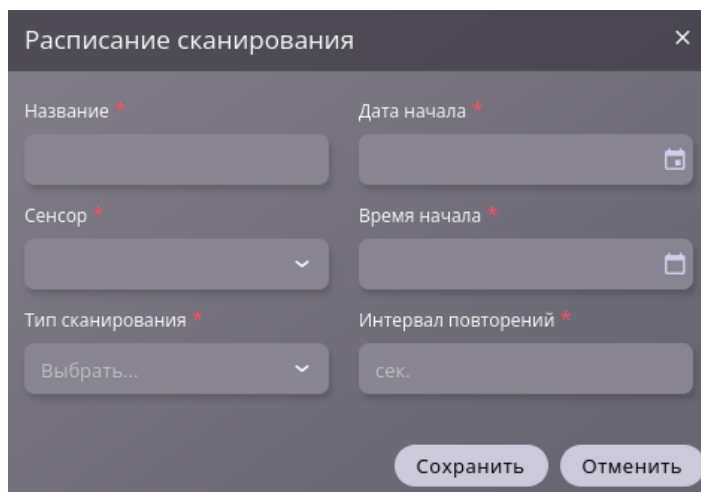
В разделе «Инфраструктура» во вкладке «Расписания» представлены расписания автоматического сканирования, развертывания ловушек и обновления приманок (Рисунок 52).

Название	Сенсор	Тип сканирования	Интервал повторений	Крайнее	Новое	Действие
Scan	lali-sensor-dev	Сканирование на уязвимости	00:00:10	14.04.2023 12:51		
TestScan	lali-sensor-dev	Сканирование CVE	00:00:05	14.04.2023 12:40		

Рисунок 52. Вкладка «Расписания»

Для того, чтобы создать автоматическое сканирование, необходимо во вкладке «Расписание сканирований» нажать на иконку «Добавить» над таблицей. В появившемся окне «Расписание сканирования» нужно указать в соответствующих полях название расписания, имя сенсора, тип сканирования,

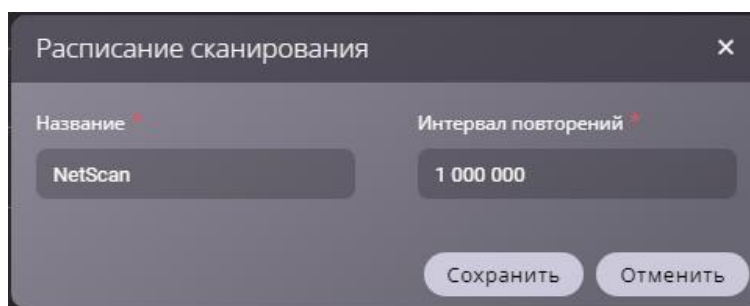
дату, время и периодичность (Рисунок 53).



The screenshot shows a form titled "Расписание сканирования" (Scanning Schedule) with a close button (X) in the top right corner. The form contains six input fields arranged in two columns. The left column has: "Название" (Name) with a red asterisk, "Сенсор" (Sensor) with a red asterisk and a dropdown arrow, and "Тип сканирования" (Scanning type) with a red asterisk and a dropdown arrow labeled "Выбрать...". The right column has: "Дата начала" (Start date) with a red asterisk and a calendar icon, "Время начала" (Start time) with a red asterisk and a clock icon, and "Интервал повторений" (Repeat interval) with a red asterisk and a unit selector set to "сек.". At the bottom right are two buttons: "Сохранить" (Save) and "Отменить" (Cancel).

Рисунок 53. Создание расписания сканирования

Для редактирования расписания с помощью иконки «Редактировать» вызывается окно, в котором предоставляется возможность изменить название расписания и периодичность сканирования (Рисунок 54).



The screenshot shows the same "Расписание сканирования" (Scanning Schedule) form, but in edit mode. The "Название" (Name) field now contains the text "NetScan". The "Интервал повторений" (Repeat interval) field now contains the value "1 000 000". The "Сохранить" (Save) and "Отменить" (Cancel) buttons remain at the bottom right.

Рисунок 54. Редактирование расписания сканирования

Удаление расписания осуществляется с помощью иконки «Удалить».

Аналогичные операции могут быть проведены для расписаний работы ловушек и развертывания приманок в соответствующих вкладках.

При добавлении расписания работы ловушек во вкладке «Расписание ловушек» необходимо указать сенсор, на котором будет развернута ловушка, её тип (выбрать из выпадающего списка среди установленных на сенсоре), время включения и выключения, а также выбрать рабочие дни недели (Рисунки 55 - 56).

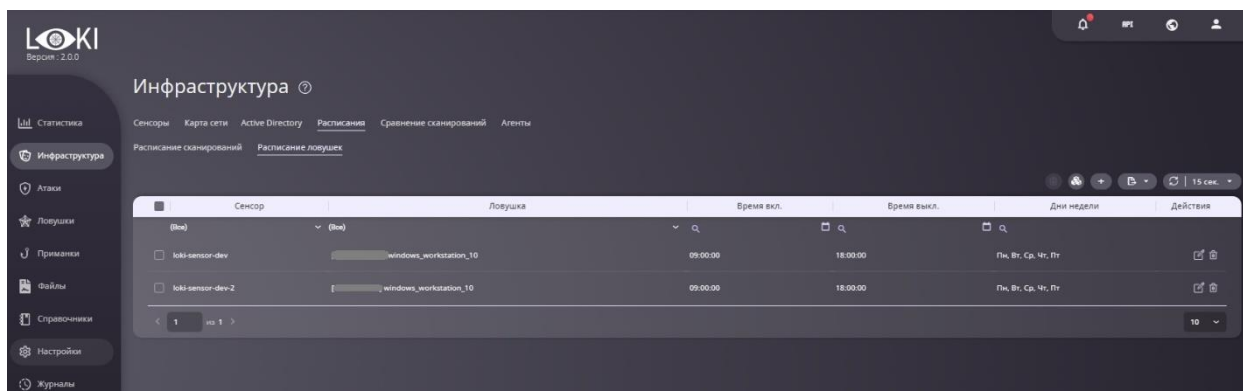


Рисунок 55. Вкладка «Расписание ловушек»

Расписания ловушек

Сенсор *

loki-sensor-17

Ловушка *

Время вкл. *

19:00:00

Время выкл. *

00:00:00

Дни недели *

☐ Пн

☒ Вт

☐ Ср

☒ Чт

☐ Пт

☒ Сб

☐ Вс

Сохранить

Отменить

Рисунок 56. Создание расписания работы ловушки

При добавлении расписания обновления приманок во вкладке «Расписание приманок» необходимо указать время и дни недели, в которые будет производится обновление (Рисунок 57).

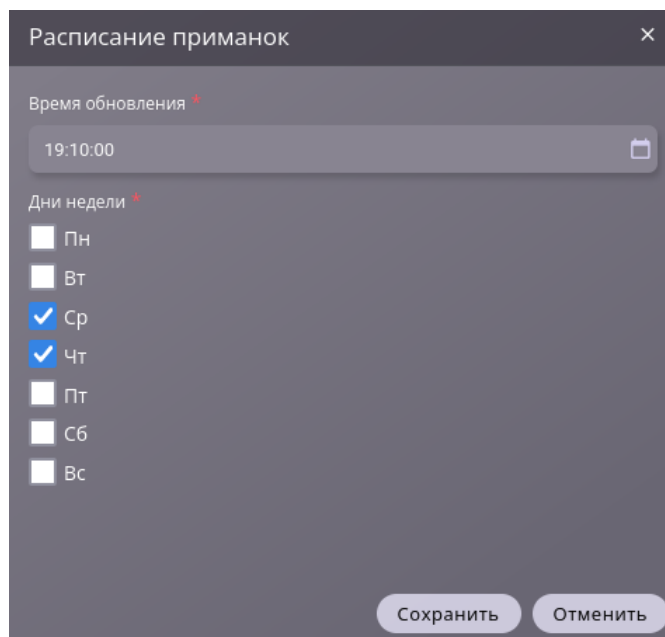


Рисунок 57. Создание расписания обновления приманок

После любых операций добавления и редактирования расписаний следует нажать кнопку «Сохранить» в соответствующем окне для успешного применения внесенных изменений.

5.9 Сравнение сканирований

Во вкладке «Сравнение сканирований» предоставляется возможность сравнить результаты предыдущих сканирований (Рисунок 58).

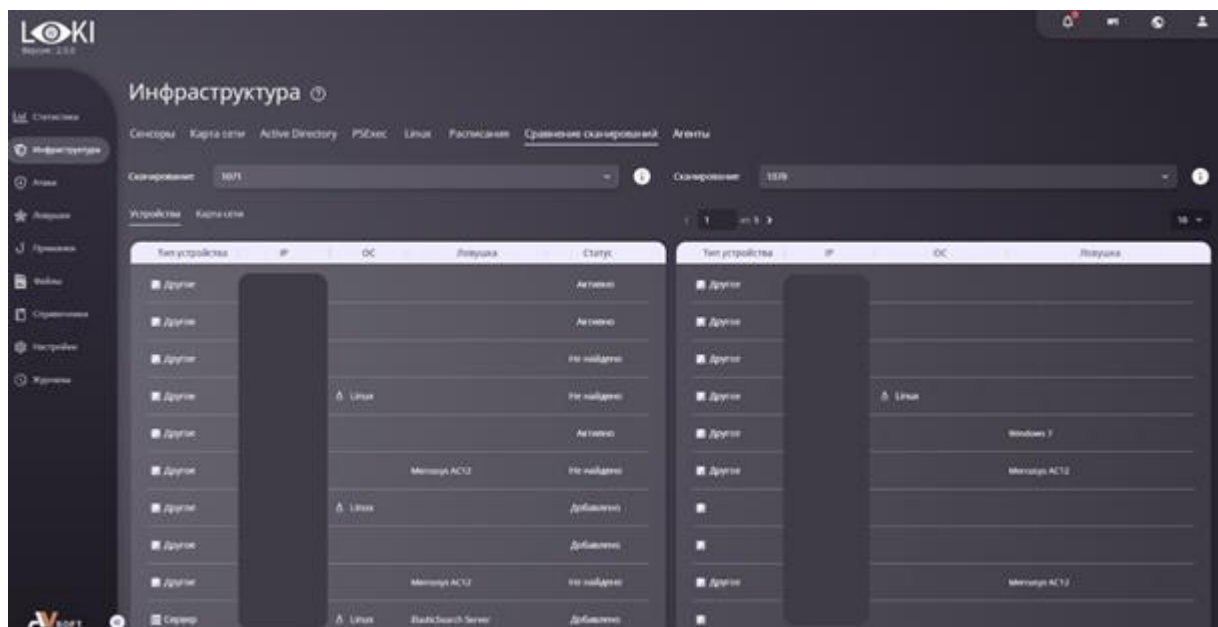


Рисунок 58. Вкладка «Сравнение сканирований»

При сравнении результатов сканирований имеется возможность переключить режим просмотра устройств в виде списков в режим интерактивных карт (Рисунок 59).

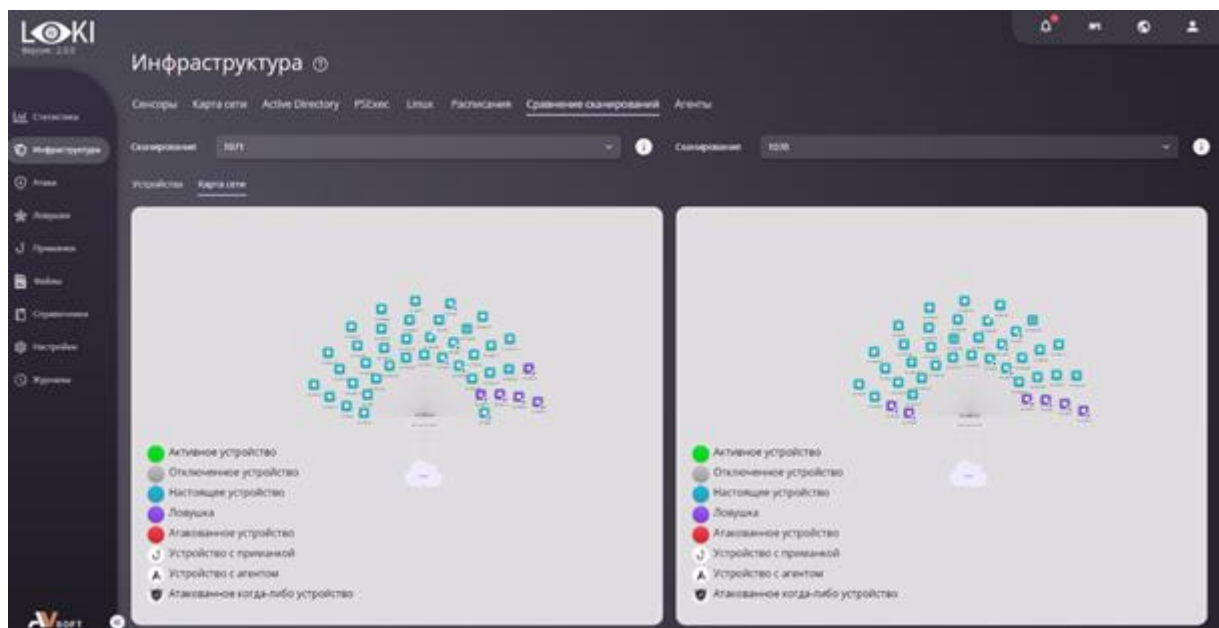


Рисунок 59. Интерактивные карты с результатами сканирования

5.10 Агенты

Агенты – программное обеспечение, устанавливаемое на реальные устройства для автоматической установки и обновления приманок. Также агенты позволяют осуществлять поиск уязвимостей в ПО, установленном в системе, и пресекать распространение атаки в сети.

Вкладка «Агенты» отображает информацию об агентах на рабочих местах (Рисунок 60).



Рисунок 60. Вкладка «Агенты»

Для обновления приманок на рабочих местах необходимо нажать на иконку «Обновить приманки». После нажатия на иконку система отобразит оповещение об успешности операции (Рисунок 61).

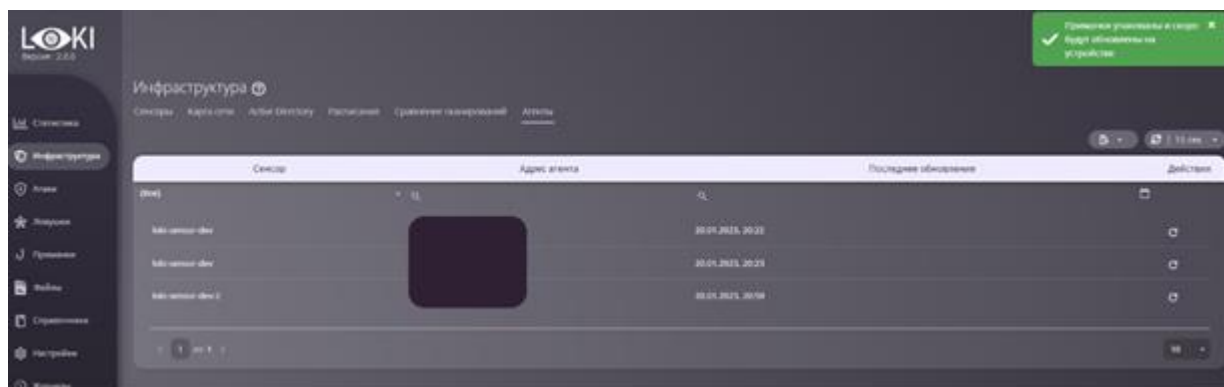


Рисунок 61. Уведомление об успешности операции

6 Раздел «Атаки»

6.1 Анализ атак

Раздел «Атаки» предназначен для офицеров безопасности, в котором они могут наблюдать карту сети с реальными устройствами, зафиксированными в организации по результатам сканирования, и развернутыми ловушками. Также здесь представлен полный список зафиксированных событий/инцидентов в результате атак на ловушки (Рисунок 62).

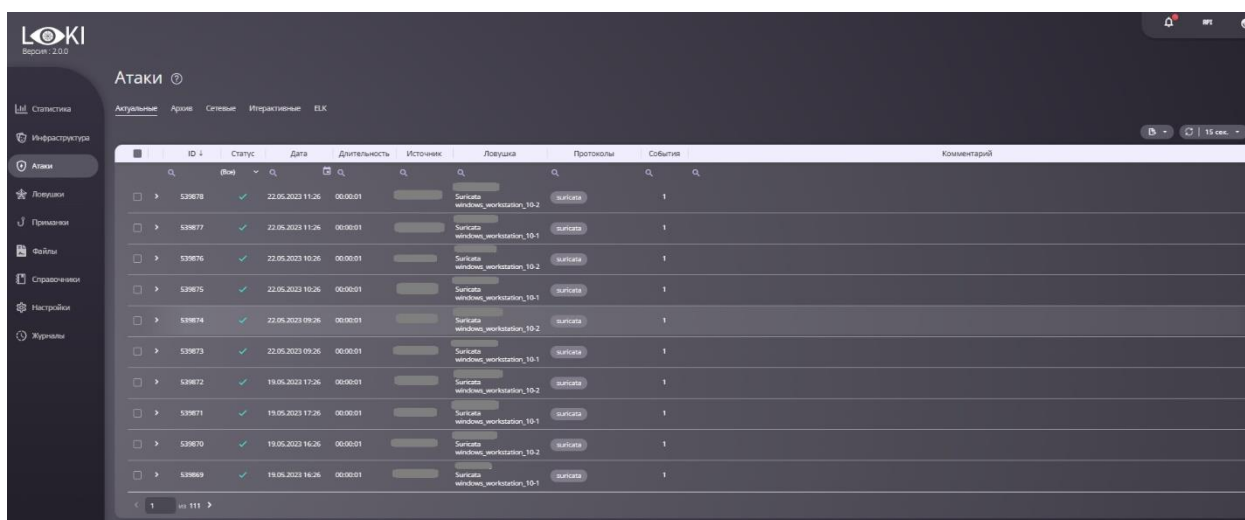


Рисунок 62. Раздел «Атаки»

Ловушки фиксируют несанкционированное подключение (в том числе сетевое сканирование портов) и поведение атакующего после успешной авторизации в имитируемой системе. Все действия злоумышленника группируются по временному интервалу в единый объект, который называется атака или сессия атак в зависимости от общего числа событий ИБ в рамках таймаута. За ограниченное время может быть совершено несколько атак на имитируемую систему, которые также автоматически объединяются в

отдельный объект. Как, например одно событие ИБ – это атака, несколько событий ИБ - сессия атак (т.е. объединенная атака). Сессия атак может быть возобновлена, если появилось новое событие ИБ, которое относится к данной атаке в рамках таймера атаки. Таким образом система LOKI автоматически группирует события ИБ в сессии для дальнейшего удобства при расследовании инцидента.

Помимо взаимодействия с ловушками система LOKI позволяет фиксировать случаи неудачных попыток авторизации на реальных устройствах организации с помощью службы каталогов Active Directory (в том числе с использованием ложных учётных записей). Данные случаи помечаются системой как атака и по ним также можно найти отчёт в общей таблице событий ИБ. Система LOKI обеспечивает интеграцию не менее, чем с 20 доменами Active Directory (в различных лесах) для получения событий АРМ и серверов организации.

Также система LOKI выявляет на АРМ и серверах с ОС Windows все локальные административные учетные записи. Причём на основании выявленных данных система обнаруживает АРМ и серверы, использующие локальные административные учетные записи с истекшими паролями, а также с паролями, неизменяемыми дольше определенного срока. Для реализации функционала контроля учетных записей система LOKI поддерживает интеграцию не менее, чем с 60 доменами Active Directory (в различных лесах), что в свою очередь позволяет обеспечить контроль учетных записей не менее, чем на 6500 АРМ и серверов.

В таблице атак присутствует возможность добавлять комментарии для зафиксированных событий с помощью иконки «Редактировать» напротив выбранной сессии атак (Рисунок 63).

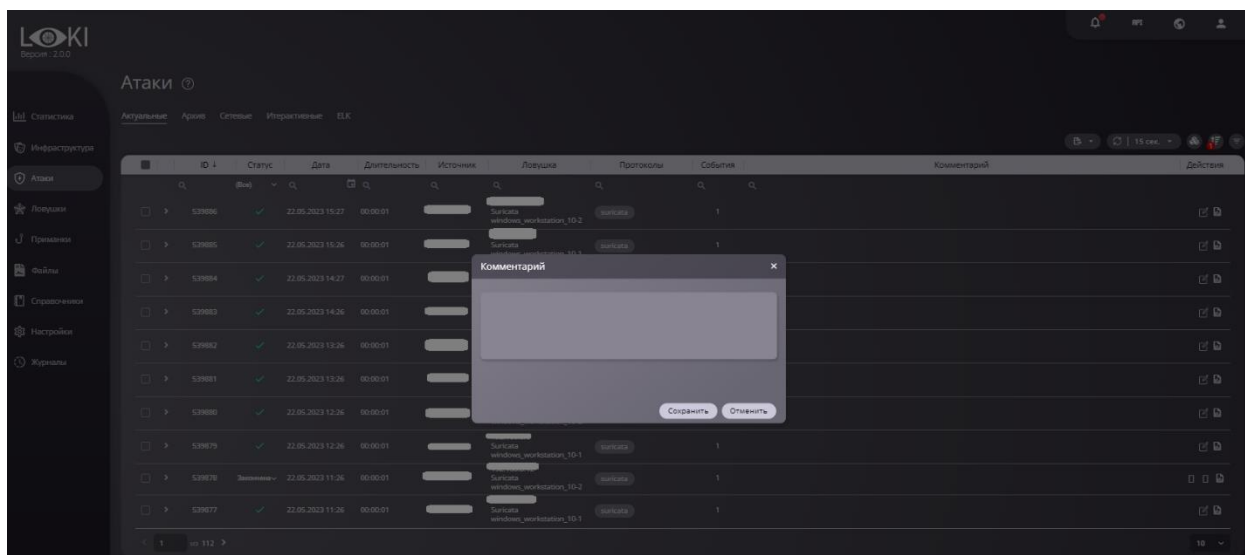


Рисунок 63. Добавление комментария к атаке

Для просмотра отчета по атаке или сессии атак необходимо нажать на иконку «Отчет» напротив выбранной атаки, после этого в новом окне будет предоставлен отчет по атаке (Рисунок 64).

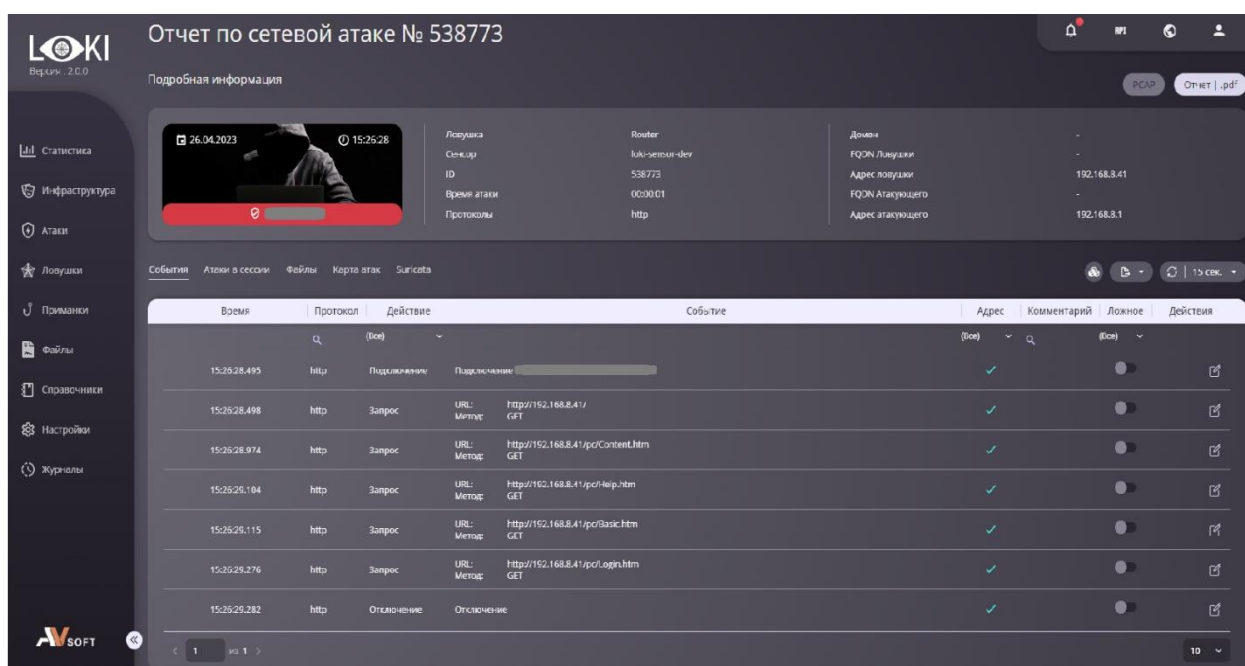


Рисунок 64. Отчет по сетевой атаке

Отчет предоставляет следующую информацию пользователю:

- адрес атакующего (IP-адрес и FQDN узла сети);
- адрес ловушки (IP-адрес и FQDN узла сети);
- протоколы, использованные для аутентификации или сетевого сканирования;
- список созданных файлов;

- Для экспорта данных отчета в структурированном виде следует воспользоваться иконкой «Экспортировать» (Рисунок 65). Система предоставляет возможность экспортировать данные в формате PDF и XLSX.



Во вкладке «Архив» отображается перечень всех совершенных атак на ловушки за все время (Рисунок 66). По истечении времени хранения актуальных атак система автоматически переносит данные из вкладки «Актуальные» во вкладку «Архив».



Во вкладке «Сетевые» отображается информация по всем зафиксированным сетевым атакам на ловушки (Рисунок 67).

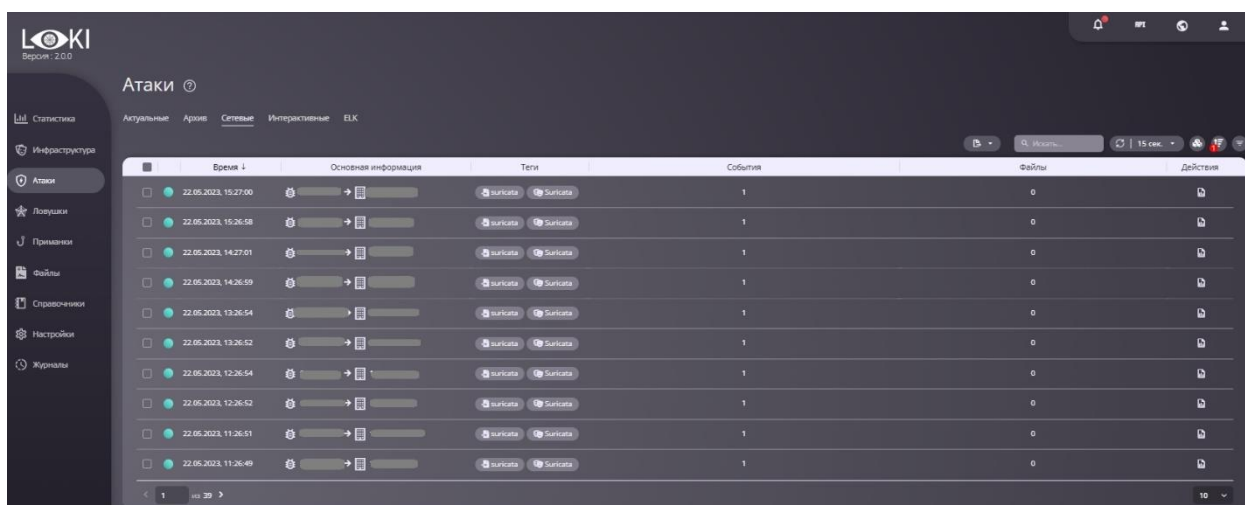


Рисунок 67. Вкладка «Сетевые»

С помощью иконок «Группировка», «Сортировка» и «Фильтрация» пользователь может осуществлять произвольную агрегацию зарегистрированных событий ИБ по различным параметрам.

В разделе «Интерактивные» отображаются атаки, которые были проведены на высокоинтерактивные ловушки.

В разделе «ELK» представлена статистика по учётным данным, используемым для подключения к ловушкам (Рисунок 68).

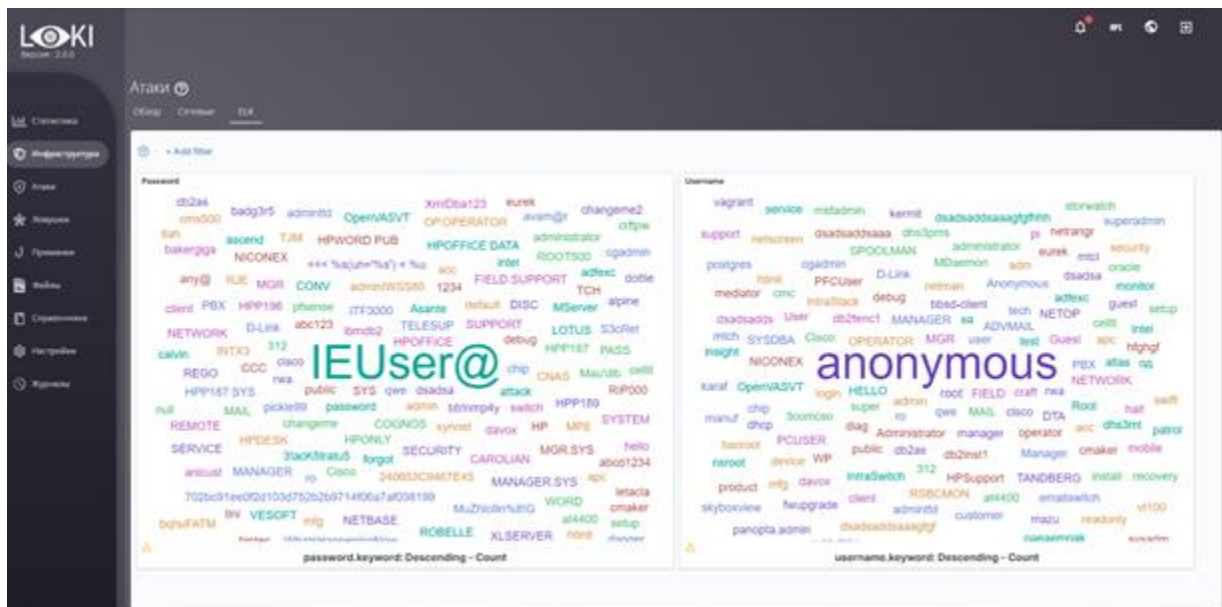


Рисунок 68. Вкладка «ELK»

6.2 Сценарии реагирования

Система детектирует присутствие злоумышленника в сети при компрометации учетных данных на приманке и подключении к ловушке. В таблице 6 описаны сценарии реагирования на действия злоумышленника для офицеров безопасности.

Таблица 6. Сценарии реагирования

№	Действия атакующего	Форензика	Сценарий реагирования
1.	Боковое перемещение в сети от скомпрометированного устройства к ловушке	Время подключения IP-адрес устройства IP-адрес ловушки	Изоляция устройства, с которого поступило подключение к ловушке Проверка запущенных процессов на устройстве Сбор списка уязвимостей на устройствах Восстановление данных из резервной копии при необходимости
2.	Авторизация на ловушке с помощью скомпрометированных учетных данных	Вводимые учетные данные Время ввода Результат авторизации (успешно / неуспешно) Протокол, используемый для подключения	Изоляция ловушки и скомпрометированного устройства в локальную подсеть Перенастройка правил маршрутизации таким образом, чтобы инфицированные машины не смогли коммуницировать с другими устройствами
3.	Взаимодействие с ловушкой (ввод команд)	Вводимые команды Время ввода Используемый	Сбор данных форензики, отправка их в SOC

№	Действия атакующего	Форензика	Сценарий реагирования
		протокол Результат ответа на команды	
4.	Взаимодействие с ловушкой (http(s)-запросы)	URL-адреса http(s)-запросов Используемые методы (например, GET, POST) Время запросов	Проверка URL-адресов на легитимность Сбор данных форензики, отправка их в SOC
5.	Загрузка файла на ловушку	Перехват файла Время загрузки Используемый протокол Отправка файла на статический и динамический анализ в песочницу Вердикт файла по результатам анализа Имя, контрольная сумма файла (SHA-256)	Обработка результатов анализа файла В случае присвоения файлу небезопасного вердикта отправка ИОС файла в SOC Направление в карантин файла с вредоносным содержимым
6.	Связь с C&C-сервером	IP-адрес C&C-сервера Время связи Используемый протокол Сетевые пакеты, отправляемые или	Отправка сработавших событий и других данных форензики в SOC

№	Действия атакующего	Форензика	Сценарий реагирования
		получаемые от С&С-сервера Анализ сетевого трафика Suricata Вердикт сетевого трафика от Suricata	
7.	Скачивание файла из ловушки (экспфильтрация)	Имя файла Время скачивания Используемый протокол	Сбор данных форензики, отправка их в SOC
8.	Отключение от ловушки	Время разрыва ТСР-сессии Используемый протокол	Сбор данных форензики, отправка их в SOC

7 Раздел «Ловушки»

В разделе «Ловушки» присутствует информация по всем ловушкам в системе (Рисунок 69).

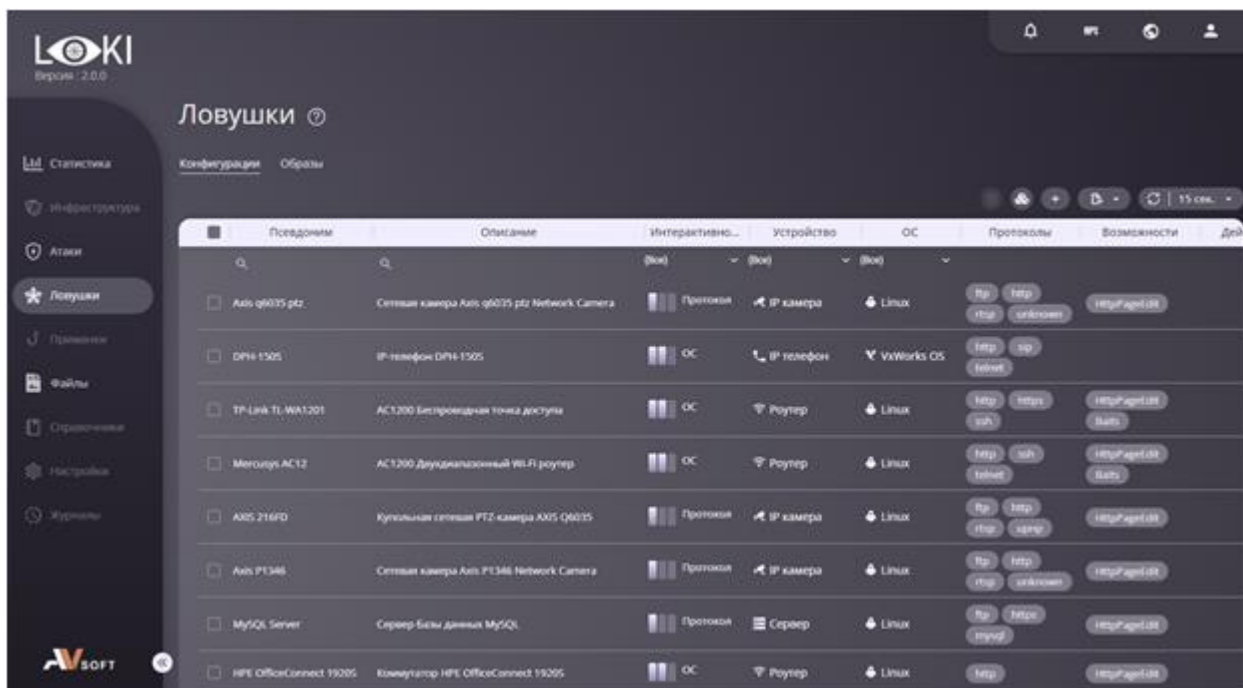


Рисунок 69. Вкладка «Конфигурации»

Во вкладке «Конфигурации» содержится следующая информация по настройке образов ловушек:

- Псевдоним;
- краткое описание;
- уровень интерактивности;
- тип имитируемого устройства;
- операционная система;
- поддерживаемые протоколы.
- возможности каждой ловушки

Все ловушки собирают сетевую телеметрию и дополнительные данные в соответствии с смоделированным протоколом:

- протокол;
- исходный порт;
- порт назначения;
- исходный IP-адрес;
- информация по электронной почте (адрес отправителя, адреса получателя, заголовок и тело письма, вложения);
- информация о соединениях HTTP/HTTPS (тип, адрес, user-agent,

данные запроса);

- информация о запросах к СУБД (текст запроса, ответ на запрос);
- учетные данные при наличии в соответствующем протоколе;
- ловушки также собирают собственный сетевой трафик для последующего анализа перехваченных сетевых атак.

В системе присутствуют ловушки низкого, среднего и высокого уровня интерактивности. У каждого уровня есть свои виды взаимодействия ловушки с атакующим, которые описаны в таблице 7. Уровень интерактивности ловушки зависит от используемого протокола. Все этапы взаимодействия ловушки и атакующего отображаются в отчете по атаке.

Таблица 7. Виды взаимодействия ловушек

Уровень интерактивности	Ловушка	Протокол	Собираемая информация
Высокий	Сервер <i>MongoDB</i> <i>Pure MySQL Server</i> <i>RDP Server</i>	mongod mysql rdp	Учетные данные авторизации Отправляемые команды и ответы на них Список системных событий Имена файлов и действия с ними
	Компьютер <i>Windows 10</i> <i>Debian 9</i>		
Средний	Сервер <i>OPC UA server</i> <i>Sinumerik (ACU TPI)</i>	opcua-tcp	Учетные данные авторизации Отправляемые команды и ответы на них Имена файлов и действия с ними Результаты просмотра содержимого сервера

Уровень интерактивности	Ловушка	Протокол	Собираемая информация
	Компьютер <i>Debian 10</i> <i>Debian 9</i> <i>Ubuntu 20.04</i>	ssh	Учетные данные авторизации Отправляемые команды и ответы на них Имена файлов и действия с ними
	Роутер <i>TP-Link TL-WA1201</i> <i>Mercusys AC12</i> <i>HPE OfficeConnect 1920S</i>	http https ssh telnet	Учетные данные авторизации Методы и URL-адреса http-запросов Отправляемые команды и ответы на них Имена файлов и действия с ними
	Телефон <i>DPH-150S</i>	http sip telnet	Учетные данные авторизации Методы и URL-адреса http-запросов Отправляемые команды и ответы на них
Низкий	Сервер <i>BACnet (ACU TII)</i> <i>Dovecot Mail Server</i> <i>ElasticSearch Server</i> <i>ENIP (ACU TII)</i>	bacnet enip ftp http https imap ipmi microsoft-ds/smb	Учетные данные авторизации Методы и URL-адреса http-запросов Отправляемые команды и ответы на них

Уровень интерактивности	Ловушка	Протокол	Собираемая информация
	<i>IPMI</i>	modbus	
	<i>Mail Server</i>	ms-wbt-server/rdp	
	<i>Modbus (ACU TII)</i>	msrpc	
	<i>MySQL Server</i>	mysql	
	<i>S7comm (ACU TII)</i>	netbios-ssn	
	<i>TFTP</i>	ntp	
	<i>Windows Server 2019</i>	pop3	
	<i>Windows Server 2016</i>	s7comm	
	<i>Windows Server 2012</i>	smtp	
	<i>Windows Server 2008</i>	ssl/imap	
		ssl/pop3	
		tftp	
	Компьютер	microsoft-ds/smb	Учетные данные авторизации Отправляемые команды и ответы на них
	<i>Windows 10</i>	ms-wbt-server/rdp	
	<i>Windows 7</i>	msrpc	
	<i>Windows XP</i>	netbios-ssn	
	Роутер	http	Учетные данные авторизации Методы и URL-адреса http-запросов
	<i>Cisco SG200-26</i>	https	
	Камера	ftp	Учетные данные авторизации Методы и URL-адреса http-запросов
	<i>AXIS 216FD</i>	hcnet	
	<i>AXIS</i>	http	
		https	

Уровень интерактивности	Ловушка	Протокол	Собираемая информация
	<i>M1065LW</i> <i>AXIS P1346</i> <i>AXIS P3384</i> <i>AXIS Q6035 PTZ</i> <i>Hikvision DS-2CD4125FWD-IZ</i>	rtsp upnp	
	Другое <i>FS-1125MFP</i> <i>IEC 61850</i> <i>Sauter EY-AS 525 (ACU TII)</i> <i>Suricata</i> <i>UPS AP9631</i>	bacnet ftp http iec61850 lpd pjl s7comm snmp telnet wsdapi	Учетные данные авторизации Отправляемые команды и ответы на них

Для анализа сетевых пакетов, поступающих на ловушку при взаимодействии с ней, используется система Suricata. Для включения анализа сетевого трафика необходимо добавить на сенсор ловушку с названием Suricata. Система Suricata позволяет выявлять сетевое сканирование устройств в инфраструктуре организации.

Работа высокоинтерактивных RDP и SSH ловушек осуществляется за счёт интеграции с системой ATHENA. Подробнее о настройке интеграции с системой ATHENA можно найти в Руководстве администратора системы LOKI в разделе 17.

При сканировании сетевых портов ловушки все эмулированные и доступные на ней из сети службы обеспечивают однозначную идентификацию ловушки в качестве одного из типов эмулируемых устройств.

При взаимодействии с ловушками средней и высокой интерактивности, эмулирующими службы для работы с файлами (сервисы удаленного доступа к файлам и сетевые файловые ресурсы) имеется возможность создания каталогов (директорий) с произвольным наименованием, в том числе на русском языке.

Во вкладке «Образы» содержатся сохраненные образы ловушек, которые можно использовать для развертывания и запуска (Рисунок 70).

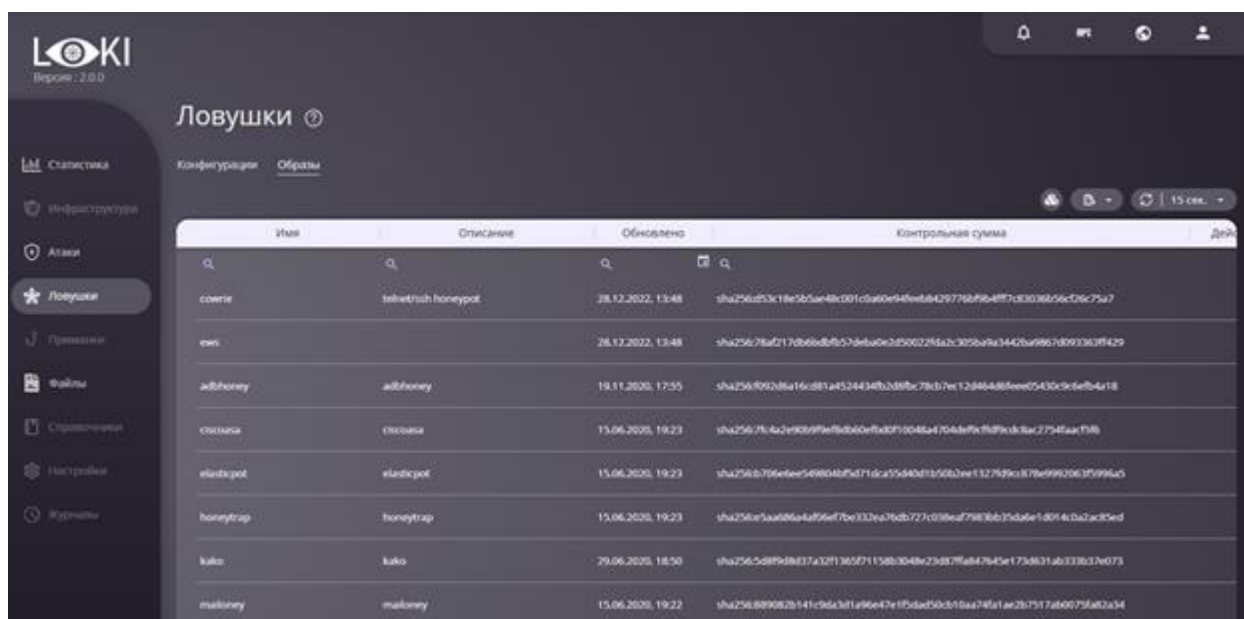


Рисунок 70. Вкладка «Образы»

8 Раздел «Приманки»

Приманки – значимые для злоумышленника данные на рабочих местах пользователей, которые могут быть применены к ловушкам.

Они представляют собой файлы, ключи реестра, конфигурации, данные авторизации, записи в базе данных и другие форматы, содержащие информацию, свидетельствующую о взаимодействии пользователя с сетевым устройством.

Приманки помогают увести злоумышленника на ложный след, сместив фокус с настоящей инфраструктуры на имитируемую (ловушки).

Вкладка «Приманки» отображает информацию об размещённых на рабочих местах приманках (Рисунок 71).

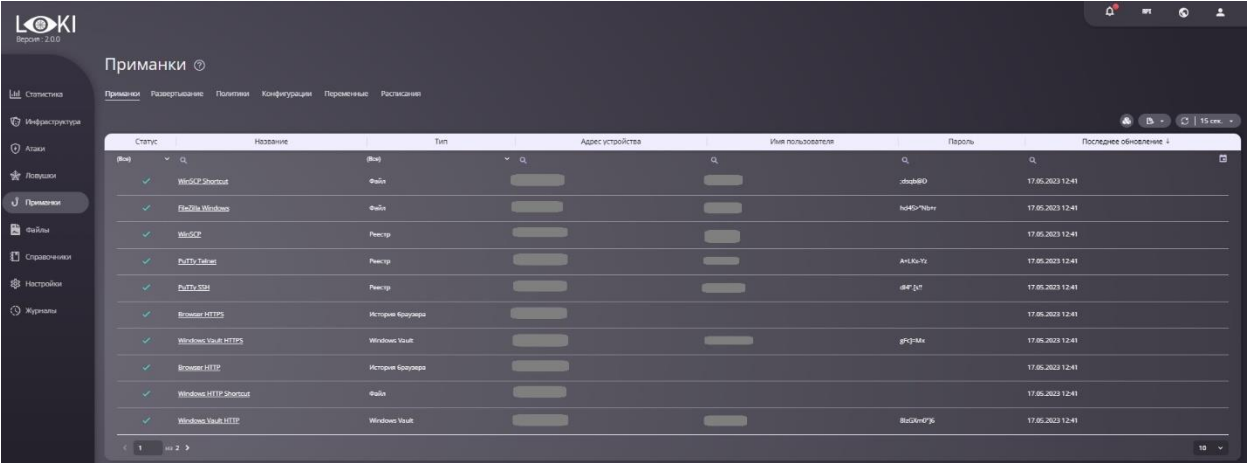


Рисунок 71. Вкладка «Приманки»

В таблице 8 представлен полный перечень приманок системы LOKI, доступных для установки на АРМ и сервера.

Таблица 8. Приманки

Протокол	Система	Описание
FTP	Windows	Конфигурационные данные утилиты WinSCP для подключений к удалённой машине по FTP (реестр Windows)
FTP	Windows	Конфигурационный файл с сохраненной историей подключений клиента FileZilla
FTP	Linux	Конфигурационный файл с сохраненной историей подключений клиента FileZilla
HTTP/HTTPS	Windows	История браузера
HTTP/HTTPS	Windows	Сохранённые данные авторизации для подключения по HTTP/HTTPS (Windows

Протокол	Система	Описание
		Vault)
Modbus	Windows	Конфигурационный файл с сохранёнными подключениями к промышленной системе S7-200
MySQL	Windows	Конфигурационные файлы клиента для подключения к базе данных MySQL
	Linux	
RDP	Windows	Конфигурационный файл с сохранёнными соединениями клиента Remote Desktop
RDP	Windows	Сохранённая сессия соединений клиента Remote Desktop (реестр Windows)
RDP	Windows	Сохранённые данные авторизации для подключения по RDP (Windows Vault)
MICROSOFT-DS/SMB	Linux	Скрипт для подключения по SMB протоколу
SSH	Linux	Конфигурационный файл с сохранённой историей соединений SSH
SSH	Windows	Сохранённая история подключений клиента

Протокол	Система	Описание
		PuTTY (реестр Windows)
SSH	Windows	Конфигурационные файлы с известными хостами, публичными ключами и настройками SSH соединения
	Linux	
TELNET	Windows	Сохранённая сессия клиента PuTTY (реестр Windows)

Также система LOKI позволяет размещать приманки на АРМ и серверах с ОС Windows в оперативной памяти системы (учетные данные в памяти процесса LSASS).

В разделе «Развертывание» во вкладке «PSEXec» представлен список устройств и их IP, для которых можно с помощью данной утилиты удаленно разместить приманки на АРМ и серверах с ОС Windows (Рисунок 72).

Более подробное описание так же представлено в данном документе чуть ниже (Рисунок 83).

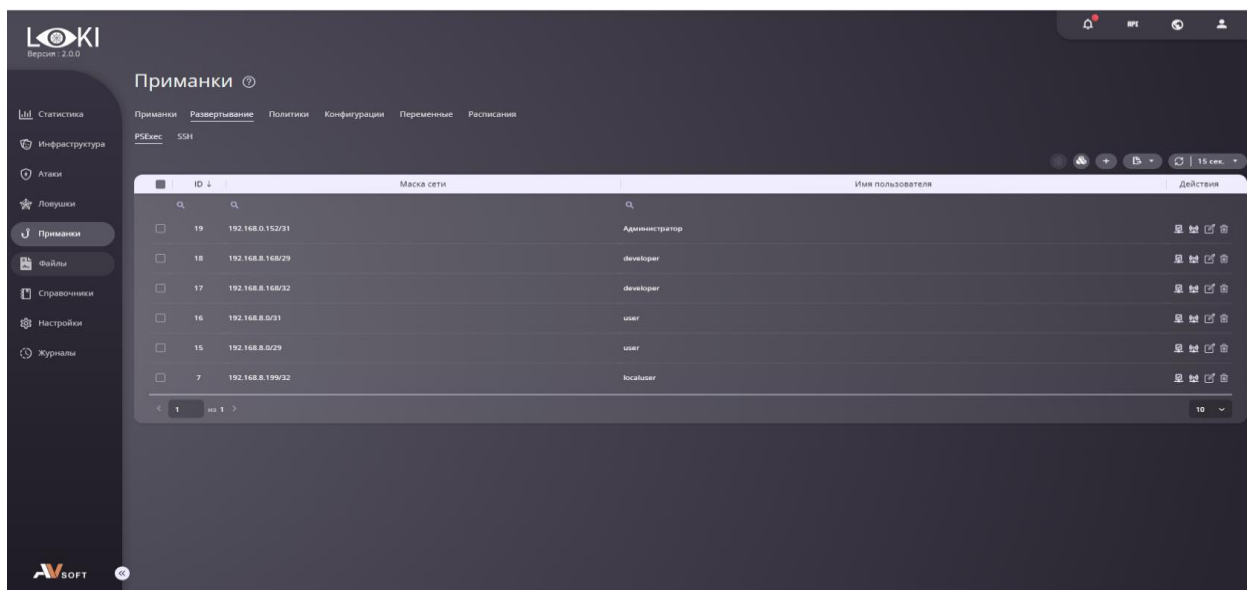


Рисунок 72 Вкладка «PSEXec»

В разделе «Развертывание» во вкладке «SSH» представлен список устройств и их адреса, для которых можно осуществить удаленную установку

приманок по протоколу SSH на устройства с ОС Linux (Рисунок 73).

Более подробное описание так же представлено в данном документе чуть ниже (Рисунок 85).

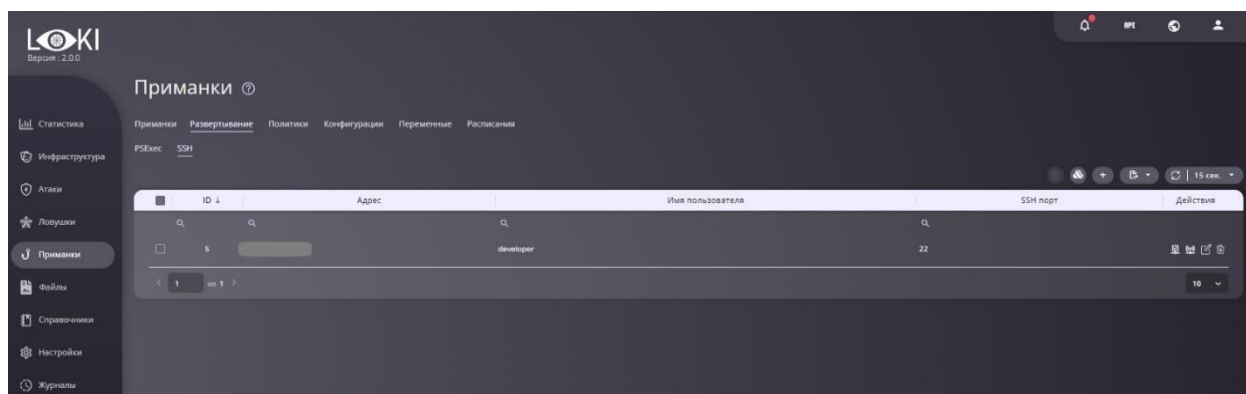


Рисунок 73 Вкладка «SSH»

Во вкладке «Политики» можно задавать политики для приманок и политики ПО для определённых приложений в ОС Windows и Linux. Например, для ПО «Mozilla Firefox» требуется установить http/http приманку (Рисунок 74).

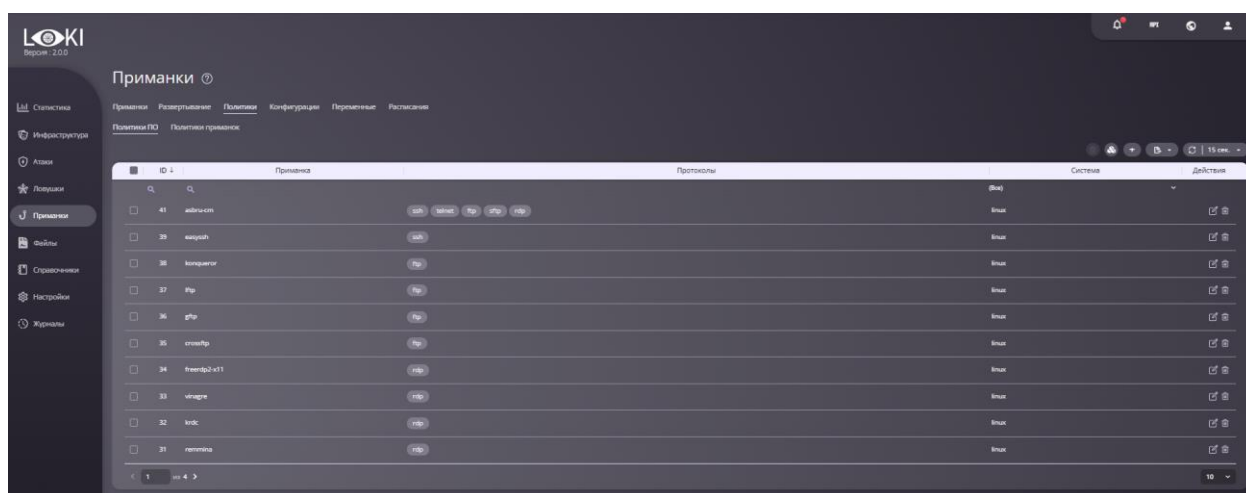


Рисунок 74. Вкладка «Политики ПО»

Во вкладке «Конфигурации» система предоставляет возможность именования ложных учетных записей в соответствии с определенными пользователем правилами наименования. Для этого необходимо нажать на стрелочку в левой части таблицы напротив выбранной приманки (Рисунок 75).

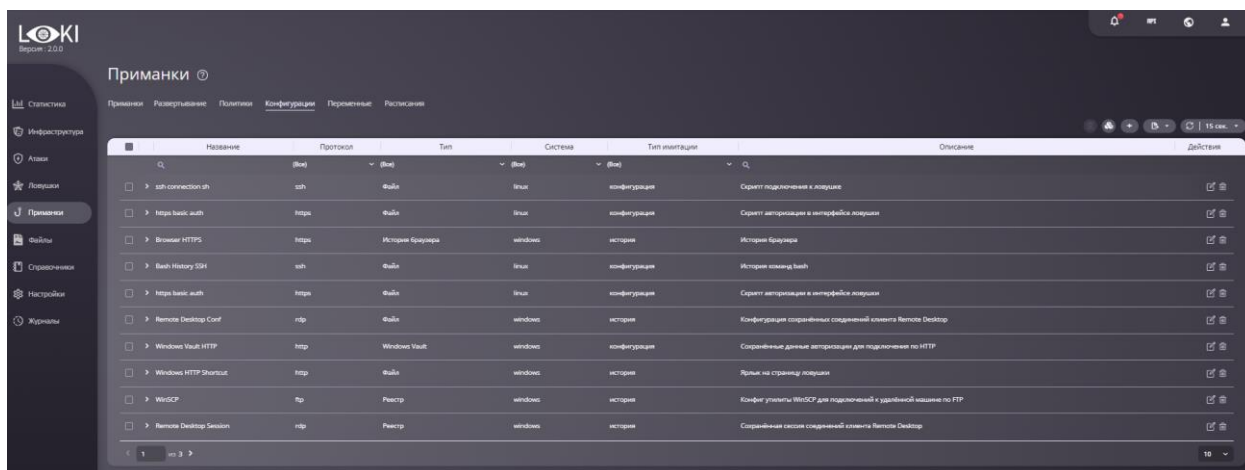


Рисунок 75. Подробная информация по приманке

Далее в раскрывшейся таблице необходимо нажать на иконку «Редактировать». В появившемся окне пользователь может внести изменения в настройки приманки в зависимости от её типа (Рисунок 76).

Приманка

Название:

Протокол:

Тип:

Система:

Тип имитации:

Описание:

Рисунок 76. Редактирование приманки

Во вкладке «Переменные» можно задать правила автоматического создания данных для ложных учетных записей приманки (Рисунок 77).

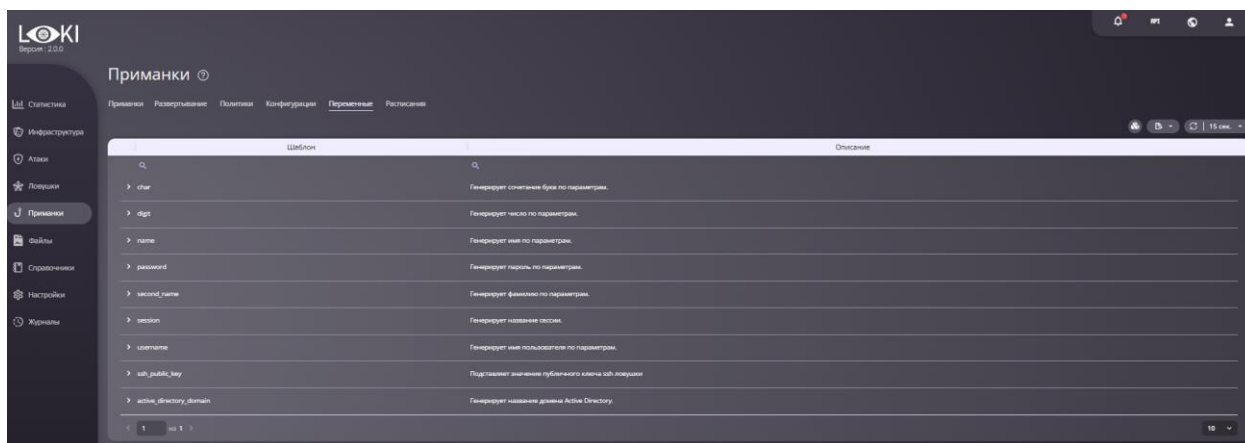


Рисунок 77. Раздел «Приманки», вкладка «Переменные»

В таблице представлены различные переменные и их возможные значения. Чтобы увидеть подробную информацию, нужно нажать на стрелочку около наименования переменной и появится полный список (Рисунок 78).

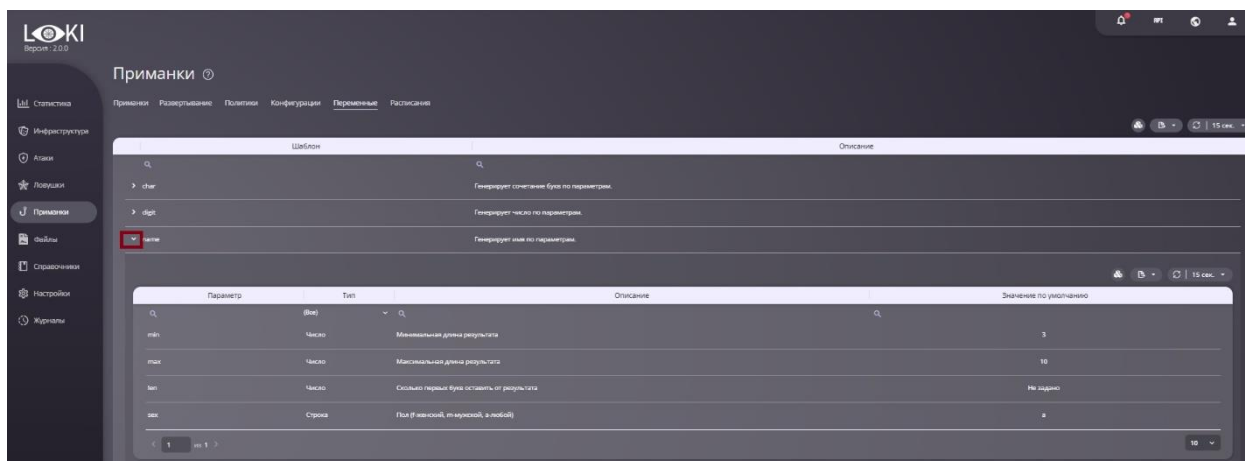


Рисунок 78. Полный список значений для переменных

Во вкладке «Расписания» система предоставляет возможность просмотреть время и последнее обновление приманок (Рисунок 79. Раздел «Приманки», вкладка «Расписания» Рисунок 79).

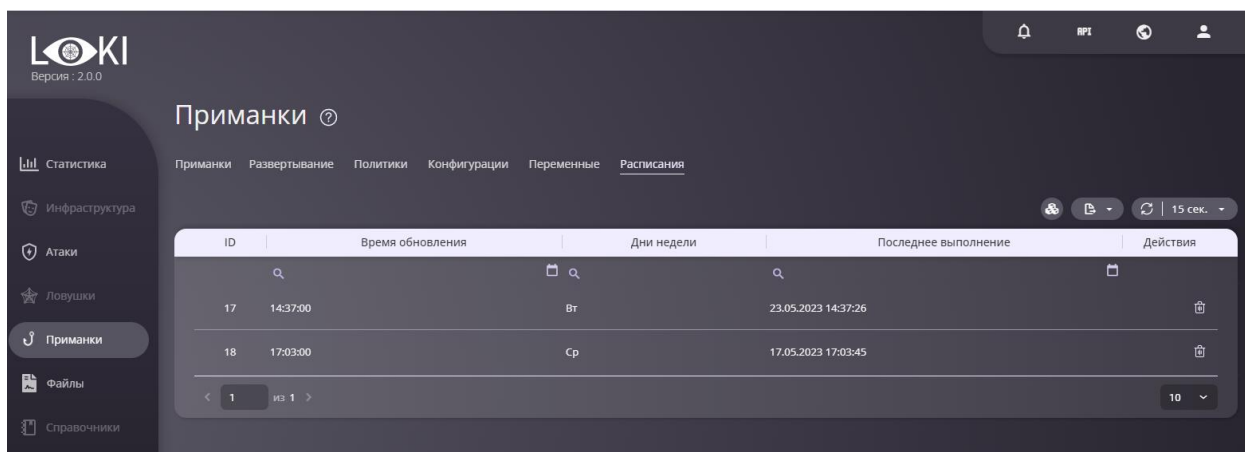


Рисунок 79. Раздел «Приманки», вкладка «Расписания»

9 Раздел «Файлы»

Раздел «Файлы» содержит перечень всех файлов, которые были отправлены или загружены на атакованные ловушки за все время (Рисунок 80).

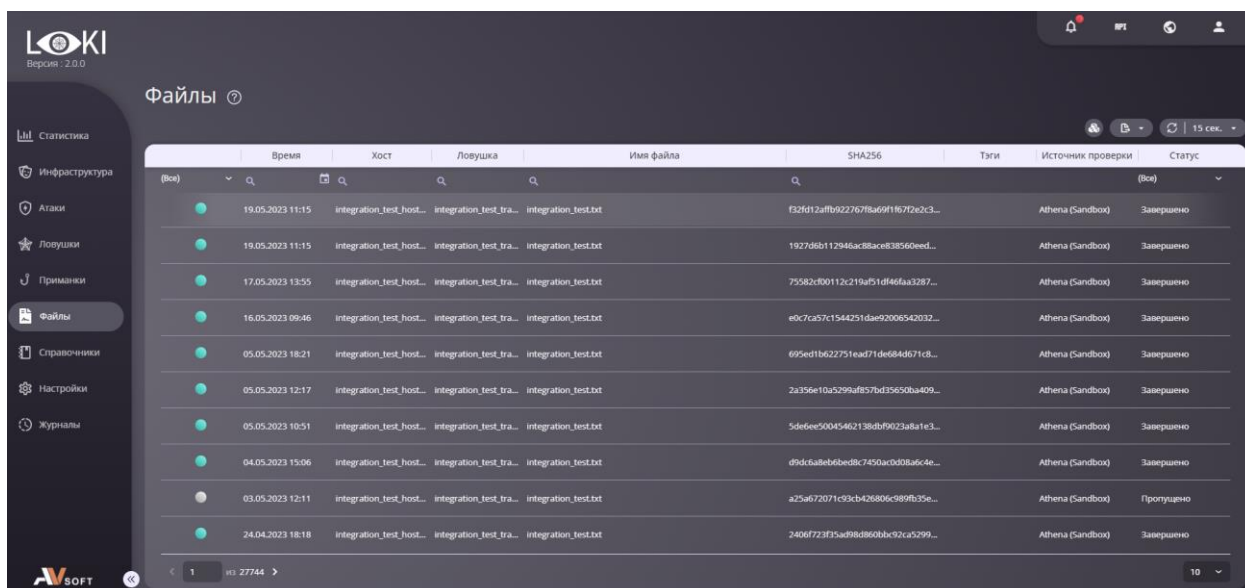


Рисунок 80. Раздел «Файлы»

10 Развертывание приманок

Список всех доступных приманок находится во вкладке «Приманки» раздела «Ловушки».

После любых операций с ловушками система автоматически генерирует новый набор приманок для их обновления на АРМ и серверах инфраструктуры. Система LOKI предусматривает как агентный, так и

безагентные способы развертывания и обновления приманок. Их подробное описание представлено в следующих трёх разделах.

Ловушки могут работать без приманок. Приманки генерируются под запущенные ловушки на сенсоре и помогают определить, какие устройства были задействованы при атаке. Например, атака на ловушку произошла с устройства 192.168.10.210, но при авторизации использовались данные с приманки на 192.168.10.200 – в отчёте об атаке это будет видно, и исходя из этого понятно, что злоумышленник перед атакой получил доступ не к одному устройству в сети, а к двум.

Приманки можно применить к любым ловушкам, но подходят они только в рамках подсети сенсора, для которого они были сгенерированы. Автоматического перенаправления с приманки на ловушку не происходит, злоумышленник или вирус самостоятельно добывает данные приманки в скомпрометированной системе и по «ложному следу» пытается подключиться к ловушке. Система LOKI отображает на карте, какие приманки и с какого рабочего места были использованы для атаки на ловушку, таким образом выявляя точку проникновения в инфраструктуру. При отсутствии приманок на рабочих местах нет возможности узнать, были ли скомпрометированы устройства инфраструктуры или нет, что значительно затрудняет реагирование на инцидент.

Установка приманок доступна только на те устройства, которые были обнаружены сенсором в рамках сканирования (если устройства нет в списке устройств сенсора, установка приманок на него не будет доступна) и которые находятся в обозреваемой подсети (имеют интерфейс) с ловушками – в подсети с сенсором. Установка приманок происходит с учетом операционной системы, которая была обнаружена при сканировании. Если фактическая операционная система отличается от обнаруженной, то ее нужно изменить у устройства в таблице устройств сенсора.

Для установки приманок на устройства с ОС Windows необходимы права администратора. Они нужны, чтобы создавать директории, файлы, записи в реестре и т.д. Для успешной установки приманок по SSH на

устройства с ОС Linux необходимо, чтобы пользователь имел sudo права (это нужно, чтобы была возможность создавать директории и файлы).

Приманки создаются под устройство и под запущенные ловушки сенсоров. Поэтому если запущенных ловушек на сенсоре нет, приманки не будут созданы.

Приманки системы LOKI могут быть установлены на следующие версии ОС Windows и Linux:

- Windows 7
- Windows 10
- Windows Server 2012R2
- Windows Server 2016
- Windows Server 2019
- Debian (от 9)
- Ubuntu (от 10.04)
- Astra Linux (от 1.7, Орел)

10.1 Развертывание приманок с использованием агента

В случае агентного способа управления приманками сначала необходимо провести установку агентов на конечных станциях. Скачивание установщиков агента под системы Windows и Linux доступно в веб-интерфейсе системы LOKI. Для этого необходимо перейти в раздел «Инфраструктура» во вкладку «Сенсоры» и нажать на иконку «Информация» напротив сенсора для нужной подсети. Далее следует перейти во вкладку «Агенты» и с помощью соответствующих кнопок скачать дистрибутив под системы Windows и Linux (Рисунок 81).

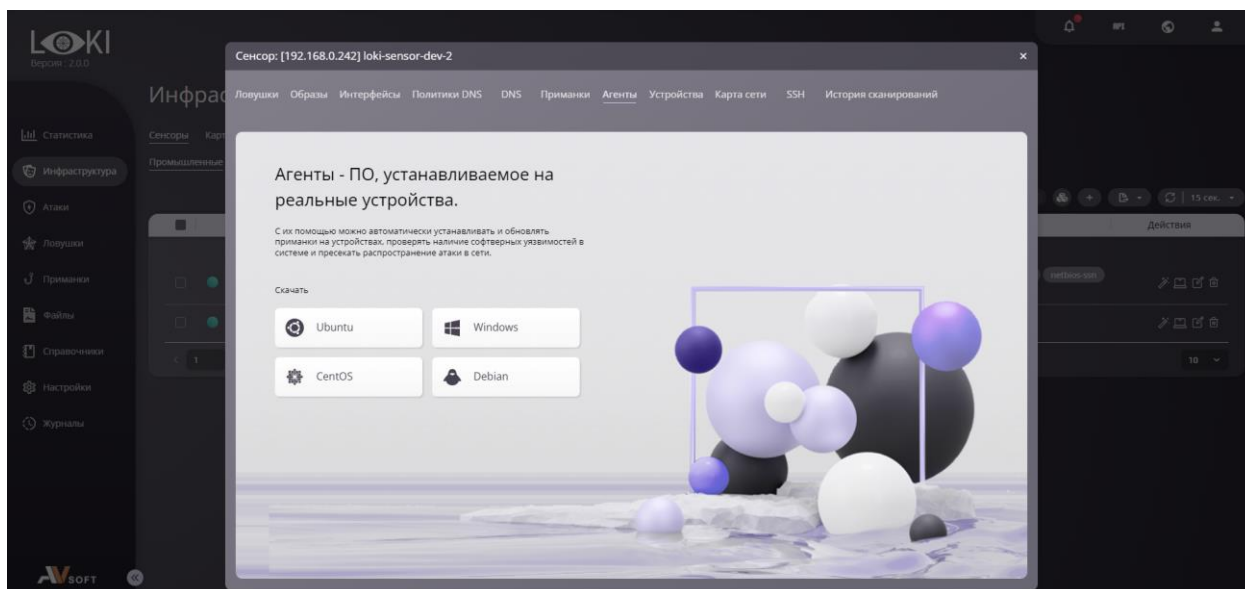


Рисунок 81. Скачивание дистрибутива агента

Важно отметить, что устройства, на которые планируется установить агенты, должны присутствовать в списке устройств сенсора (вкладка «Устройства» в диалоге сенсора).

С помощью полученных дистрибутивов необходимо провести установку агентов на устройствах с операционными системами Windows и Linux. Установщик для Windows представлен в виде файла EXE, для Linux – в виде DEB пакета.

После установки необходимо внести IP-адрес соответствующего сенсора в конфигурационный файл агента, который расположен в следующих директориях в зависимости от ОС:

Windows:

C:\ProgramData\AVSoft\LokiAgent\config.json

Linux:

/opt/LokiAgent/config.json

Адрес сенсора необходимо указать в поле “sensor”.

После установки агентов на АРМ и сервера инфраструктуры необходимо в веб-интерфейсе перейти в раздел «Инфраструктура» во вкладку «Агенты» и убедиться, что в таблице устройств с установленными агентами отобразилась соответствующая запись с корректным IP-адресом и названием сенсора (Рисунок 82). После проверки следует провести обновление приманок на рабочем месте с агентом, нажав на кнопку «Обновить приманки» напротив адреса выбранного устройства.

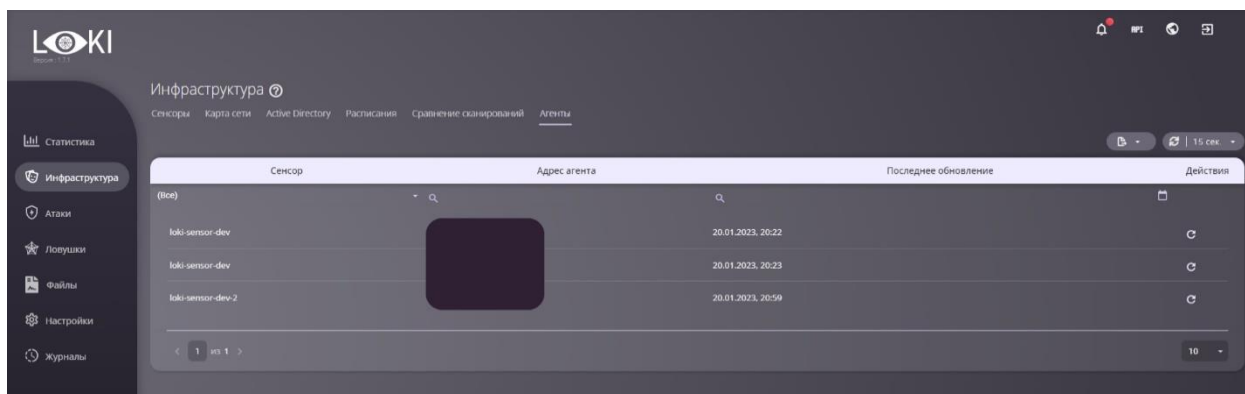


Рисунок 82. Вкладка «Агенты»

По умолчанию при установке приманок с использованием агентного способа приманки будут автоматически обновляться раз в сутки. Помимо этого, система предоставляет возможность настроить обновление приманок в соответствии с расписанием во вкладке «Инфраструктура» → «Расписания» → «Расписание приманок».

Агент работает только с одним сенсором. Подразумевается, что устройство (например, рабочая станция) не обязательно имеет доступ до сервера менеджмента, но обязательно имеет доступ до сенсора и подсети с ловушками.

10.2 Автоматическое развертывание приманок

Система LOKI предоставляет возможность безагентного распространения и обновления приманок на АРМ и серверах организации с ОС Windows и Linux.

Система LOKI использует утилиту PsExec для автоматического и удаленного размещения приманок на АРМ и серверах с ОС Windows. Для успешного автоматического развертывания приманок необходимо обеспечить наличие на устройствах с ОС Windows общей учетной записи локального администратора. Установка приманок осуществляется с правами данной «служебной» учетной записи.

Далее в интерфейсе системы LOKI необходимо перейти во вкладку «PsExec» в разделе «Приманки» → «Развертывание» (Рисунок 83).

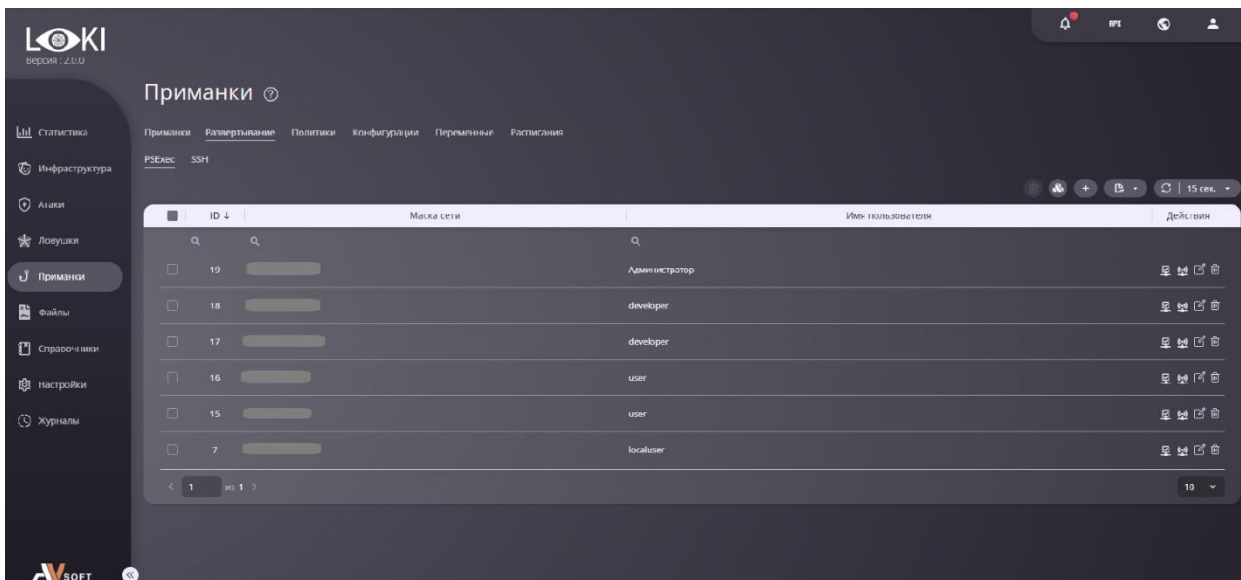


Рисунок 83. Вкладка «PsExec»

Для указания устройств, на которые необходимо установить приманки, следует нажать на иконку «Добавить» (Рисунок 84).

Рисунок 84. Окно «PsExec»

В появившемся окне необходимо заполнить поля, описанные в таблице 9.

Таблица 9. Форма «PsExec»

№	Поле	Описание поля
1.	Маска сети	Диапазон IP-адресов устройств, на которых необходимо разместить приманки
2.	Имя пользователя	

№	Поле	Описание поля
3.	Пароль	Имя и пароль «служебной» учетной записи локального администратора для авторизации в операционной системе

Для завершения процесса установки приманок на АРМ и сервера организации необходимо задать расписание обновления приманок во вкладке «Инфраструктура» → «Расписания» → «Расписание приманок». Согласно заданному расписанию система осуществит размещение приманок на указанные устройства с ОС Windows. Аналогично будет проводиться обновление приманок на данных устройствах.

На устройства с ОС Linux система LOKI осуществляет установку приманок по протоколу SSH. Для успешного автоматического развертывания приманок необходимо обеспечить наличие на устройствах с ОС Linux общей учетной записи с sudo правами.

Далее в интерфейсе системы LOKI необходимо перейти во вкладку «SSH» в разделе «Приманки» → «Развертывание» (Рисунок 85).

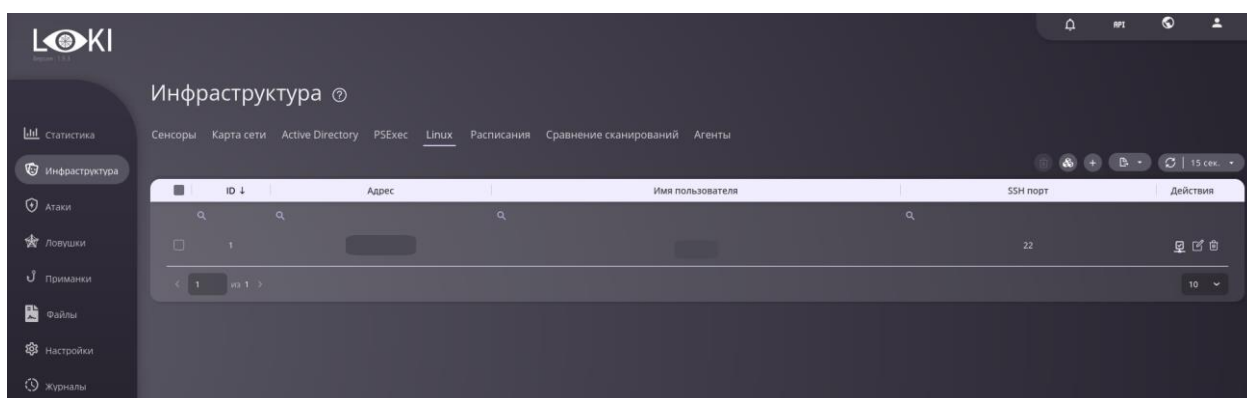


Рисунок 85. Вкладка «SSH»

Для указания устройств, на которые необходимо установить приманки, следует нажать на иконку «Добавить» (Рисунок 86).

Рисунок 86. Окно «Linux»

В появившемся окне необходимо заполнить поля, описанные в таблице 10.

Таблица 10. Форма «Linux»

№	Поле	Описание поля
1.	Адрес	IP-адрес устройства, на котором необходимо установить приманки
2.	Имя пользователя	Имя и пароль «служебной» учетной записи локального администратора для авторизации в операционной системе
3.	Пароль	
4.	SSH порт	Номер порта на устройстве для SSH подключения

По аналогии с ОС Windows после ввода данных для подключения к устройствам с ОС Linux необходимо задать расписание распространения и обновления приманок во вкладке «Инфраструктура» → «Расписания» → «Расписание приманок».

После установки описанными способами во вкладке «Приманки» в одноименном появятся записи с IP-адресами устройств, входящих в заданный при настройке диапазон. В данной вкладке отображается статус установки

приманки, крайняя дата обновления, ее тип, ложные учетные данные и адрес ловушки, на которую она ведёт (Рисунок 87).

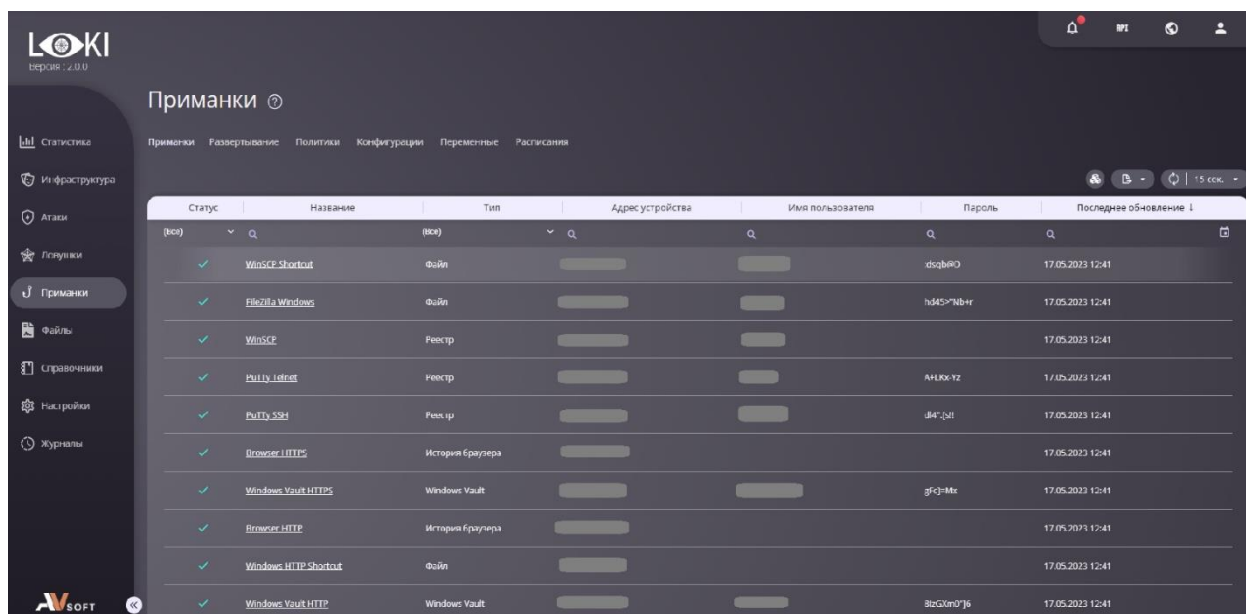


Рисунок 87. Вкладка «Приманки»

Описанные способы автоматического распространения приманок выполняются без разворачивания агентов на АРМ и серверах в качестве компонентов системы LOKI.

10.3 Ручное развертывание приманок

Также для случая безагентного распространения и обновления приманок система LOKI предоставляет возможность установить приманки вручную.

Для самостоятельной установки приманок необходимо предварительно скачать специальные установщики в веб-интерфейсе системы LOKI. Для этого необходимо перейти в раздел «Инфраструктура», нажать на иконку «Информация» напротив сенсора для нужной подсети. Далее следует перейти во вкладку «Приманки» и с помощью соответствующих кнопок скачать установщик приманок под системы Windows или Linux (Рисунок 88).

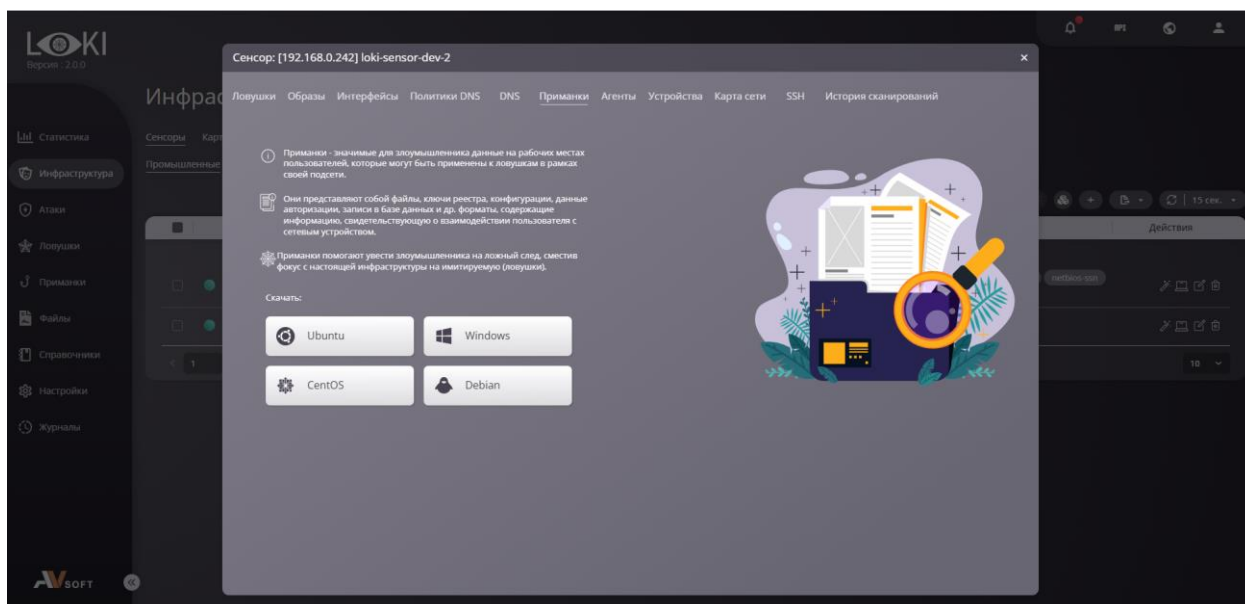


Рисунок 88. Скачивание установщика приманок

С помощью полученных установщиков можно провести установку приманок на устройствах с операционными системам Windows и Linux вручную.

После доставки установщика на целевой АРМ или сервере необходимо в командной строке перейти в директорию с файлом и запустить исполняемый файл со следующими параметрами:

```
baits_installer install <IP_адрес_сенсора>
```

При вводе команды указывается IP адрес сенсора, доступного в подсети устройства. Для того, чтобы узнать адрес сенсора в нужной подсети, можно воспользоваться консолью во вкладке «SSH» в диалоге сенсора («Инфраструктура» → «Сенсоры» → иконка «Информация» напротив соответствующего сенсора) и выполнить в ней следующую команду:

```
interface info
```

После ручного развертывания приманок на АРМ и сервера инфраструктуры необходимо в веб-интерфейсе перейти в раздел «Инфраструктура» во вкладку «Приманки» и убедиться, что в таблице устройств с установленными приманками отобразились соответствующие записи с корректными IP-адресами.

В отличие от вышеописанных способов ручной метод развертывания приманок не предполагает их автоматического обновления. Обновление приманок, как и их установка, осуществляется вручную.

Для ручного удаления приманок с АРМ или сервера необходимо выполнить следующую операцию в директории файла через командную строку:

```
baits_installer uninstall <IP_адрес_сенсора>
```

Описанный способ установки может быть применен при распространении приманок в домене Active Directory с помощью настройки соответствующей политики в SCCM системе.

Как и предыдущий способ описанный метод разворачивания приманок выполняется без разворачивания агентов на АРМ и серверах в качестве компонентов системы LOKI.