# UserGate Log Analyzer

## Руководство администратора

# Оглавление

# 1 ВВЕДЕНИЕ

UserGate Log Analyzer (UserGate LogAn, LogAn) - это решение, реализующее функции систем SIEM (Security Information and Event Management) и IRP (Incident Response Platform).

SIEM - система управления информацией о безопасности и событиями информационной безопасности. UserGate LogAn собирает в себе данные, получаемые из различных источников (сенсоров), например, таких как, межсетевые экраны UserGate, системы управления и контроля конечных устройств UserGate, сенсоры SNMP, сенсоры WMI. Результат обработки данных предоставляется в едином интерфейсе, доступном для аналитиков безопасности, что облегчает изучение характерных особенностей, соответствующих инцидентам безопасности. На основе получаемых данных (событий) LogAn в реальном времени с помощью правил аналитики осуществляет агрегацию повторяющихся событий и их корреляцию (связывание разрозненных событий между собой), создавая инциденты кибербезопасности. Правила реагирования позволяют автоматически определить методы реагирования на инциденты информационной безопасности.

Для проведения расследований инцидентов кибербезопасности используется встроенная в UserGate LogAn система IRP. IRP - это платформа управления процессами реагирования на инциденты информационной безопасности. UserGate LogAn позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании.

LogAn поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде.

# 2 ЛИЦЕНЗИРОВАНИЕ USERGATE LOGAN

UserGate LogAn лицензируется по количеству настроенных сенсоров, с которых он собирает информацию. В качестве сенсора может выступать шлюз UserGate, либо любое другое устройство, которое может отправлять информацию по протоколу SNMP на сервер LogAn.

Лицензия на UserGate LogAn дает право бессрочного пользования продуктом.

Дополнительно лицензируются следующие модули:

| Наименование | Описание |
|---|---|
| **Модуль Security Update (SU)** | Модуль SU дает право на получение:<br>• обновлений ПО UserGate LogAn<br>• технической поддержки.<br><br>Модуль выписывается на 1 год, по истечении данного срока для получения обновлений ПО и технической поддержки необходимо приобрести продление лицензии. |
| **Сенсоры** | Данный модуль определяет количество сенсоров, с которых LogAn может собирать информацию. Данный модуль выписывается сроком на 1 год и требует ежегодного продления. |

Для регистрации продукта необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Перейти в Дашборд | Нажать на пиктограмму **Дашборд** в правом верхнем углу. |
| **Шаг 2.** В разделе **Информация о лицензии** зарегистрировать продукт | В разделе **Информация о лицензии** нажать на ссылку **Зарегистрированная версия**, ввести ПИН-код и заполнить регистрационную форму. |

Посмотреть статус установленной лицензии можно в разделе **Дашборд** в виджете **Лицензия**.

# 3 ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА

UserGate LogAn поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде. В случае виртуальной машины UserGate LogAn поставляется с двумя Ethernet-интерфейсами. В случае поставки в виде ПАК UserGate LogAn может содержать 8 или более Ethernet-портов.

## 3.1 Развертывание программно-аппаратного комплекса

В случае поставки решения в виде ПАК, программное обеспечение уже загружено и готово к первоначальной настройке. Перейдите к главе Подключение к UserGate LogAn для дальнейшей настройки.

## 3.2 Развертывание виртуального образа

UserGate LogAn Virtual Appliance позволяет быстро развернуть виртуальную машину, с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают такие вендоры как VMWare, Oracle VirtualBox. Для Microsoft Hyper-v и KVM поставляются образы дисков виртуальной машины.

**Примечание**

Для корректной работы виртуальной машины рекомендуется использовать минимум 8 Гб оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.

Для начала работы с виртуальным образом, выполните следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Скачайте образ и распакуйте | Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru. |
| **Шаг 2.** Импортируйте образ в свою систему виртуализации | Инструкцию по импорту образа вы можете посмотреть на сайтах VirtualBox и VMWare. Для Microsoft Hyper-v и KVM необходимо создать виртуальную машину и указать в качестве диска скачанный образ, **после чего отключить службы интеграции** в настройках созданной виртуальной машины. |
| **Шаг 3.** Настройте параметры виртуальной машины | Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb. |
| **Шаг 4.** Важно! Увеличьте размер диска виртуальной машины | Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите размер диска в 300Gb или более. Рекомендованный размер - 1000Gb или более. |

| | |
|---|---|
| **Шаг 5.** Настройте виртуальные сети | UserGate LogAn поставляется с двумя интерфейсами, назначенными в зоны:<br>• Management - первый интерфейс виртуальной машины.<br>• Trusted - второй интерфейс виртуальной машины. |
| **Шаг 6.** Выполните сброс к заводским настройкам | Запустите виртуальную машину UserGate LogAn.<br><br>Во время загрузки выберите **Support Menu** и выполните **Factory reset**. **Этот шаг крайне важен**. Во время этого шага настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного в 4-м пункте. |

## 3.3 Подключение к UserGate LogAn

Интерфейс port0 настроен на получение IP-адреса в автоматическом режиме (DHCP) и назначен в зону **Management**. Первоначальная настройка осуществляется через подключение администратора к веб-консоли через интерфейс port0.

Если нет возможности назначить адрес для Management-интерфейса в автоматическом режиме с помощью DHCP, то его можно явно задать, используя CLI (Command Line Interface). Более подробно об использовании CLI смотрите в главе Интерфейс командной строки (CLI).

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Подключиться к интерфейсу управления | **При наличии DHCP-сервера**<br>Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить UserGate LogAn. После загрузки UserGate LogAn укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта.<br><br>**Статический IP-адрес**<br>Включить UserGate LogAn. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI)**.** Подключиться к веб-консоли UserGate LogAn по указанному адресу, он должен выглядеть примерно следующим образом: https://UserGate_LogAn_IP_address:8010. |
| **Шаг 2.** Выбрать язык | Выбрать язык, на котором будет продолжена первоначальная настройка. |
| **Шаг 3.** Задать пароль | Задать логин и пароль для входа в веб-интерфейс управления. |
| **Шаг 4.** Зарегистрировать систему | Ввести ПИН-код для активации продукта и заполнить регистрационную форму. Для активации системы необходим доступ UserGate LogAn в интернет. Если на данном этапе выполнить регистрацию не удается, то ее следует повторить после настройки сетевых интерфейсов на шаге 8. |
| **Шаг 5.** Настроить зоны, IP-адреса интерфейсов, | В разделе **Интерфейсы** включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим |

| | |
|---|---|
| подключить UserGate LogAn в сеть предприятия | зонам. Подробно об управлении интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами:<br>• Зона Management (сеть управления), интерфейс port0.<br>• Зона Trusted (LAN). Предполагается, что через зону Trusted LogAn будет подключен в сеть, через которую шлюзы UserGate будут отсылать на него журналы, а также через которую LogAn получит доступ в интернет.<br><br>Для работы UserGate LogAn достаточно одного настроенного интерфейса. Разделение функций управления устройством и сбора данных на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием. |
| **Шаг 6.** Настроить шлюз в интернет | В разделе **Шлюзы** указать IP-адрес шлюза в интернет на интерфейсе, имеющим доступ в интернет, как правило, это зона **Trusted**. Подробно о настройке шлюзов в интернет читайте в главе Настройка шлюзов. |
| **Шаг 7.** Указать системные DNS-серверы | В разделе **DNS** укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации. Подробно об управлении DNS читайте в главе Раздел настройки. |
| **Шаг 8.** Зарегистрировать продукт (если не был зарегистрирован на шаге 4) | Зарегистрировать продукт с помощью ПИН-кода. Для успешной регистрации необходимо подключение к интернету и выполнение предыдущих шагов. Более подробно о лицензировании продукта читайте в главе Лицензирование UserGate LogAn. |
| **Шаг 9.** Создать дополнительных администраторов (опционально) | В разделе **Администраторы** создать дополнительных администраторов системы, наделить их необходимыми полномочиями (ролями). |

После выполнения вышеперечисленных действий UserGate LogAn готов к работе. Для более детальной настройки обратитесь к необходимым главам справочного руководства.

# 4 НАСТРОЙКА USERGATE LOGAN

## 4.1 Раздел настройки

Раздел **Настройки** определяет базовые установки UserGate LogAn:

| Наименование | Описание |
|---|---|
| **Часовой пояс** | Часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т.п. |
| **Язык интерфейса по умолчанию** | Язык, который будет использоваться по умолчанию в консоли. |
| **Настройка времени сервера** | Настройка параметров установки точного времени.<br>**Использовать NTP –** использовать сервера NTP из указанного списка для синхронизации времени.<br>**Основной сервер NTP** – адрес основного сервера точного времени. Значение по умолчанию - pool.ntp.org<br>**Запасной сервер NTP** – адрес запасного сервера точного времени.<br>**Время на сервере** – позволяет установить время на сервере. Время должно быть указано в часовом поясе UTC. |
| **Системные DNS-серверы** | Укажите корректные IP-адреса серверов DNS в настройках. |
| **Состояние Log Analyzer** | Отображается текущее состояние сервера Log Analyzer:<br>• **Состояние** - показывает текущее состояние сервиса статистики.<br>• Порт - TCP порт, на котором сервер LogAn слушает входящие соединения от серверов UserGate. |
| **Версия устройства** | Версия ПО UserGate Log Analyzer. |
| **Агент UserGate Management Center** | Настройки для подключения устройства к центральной консоли управления, позволяющей управлять парком устройств UserGate LogAn из одной точки.<br>• **Включен/Выключен** - включение или отключение управления с помощью UserGate Management Center.<br>• **Адрес UserGate Management Center** – адрес сервера.<br>• **Код устройства** – токен, требуемый для подключения к UserGate Management Center. |

## 4.2 Управление устройством

Раздел **Управление устройством** определяет следующие установки UserGate LogAn:

- Настройки диагностики.
- Операции с сервером.
- Экспорт настроек.

### 4.2.1 Диагностика

В данном разделе задаются параметры диагностики сервера, необходимые службе технической поддержки UserGate LogAn при решении возможных проблем.

| Наименование | Описание |
|---|---|
| **Детализация диагностики** | • **Off** - ведение журналов диагностики отключено.<br>• **Error** - журналировать только ошибки работы сервера.<br>• **Warning** - журналировать только ошибки и предупреждения.<br>• **Info** - журналировать только ошибки, предупреждения и дополнительную информацию.<br>• **Debug** - максимум детализации.<br><br>Рекомендуется установить значение параметра **Детализация диагностики** в **Error** (только ошибки) или **Off** (Отключено), если техническая поддержка UserGate не попросила вас установить иные значения. Любые значения, отличные от Error (только ошибки) или Off (Отключено), негативно влияют на производительность UserGate LogAn. |
| **Журналы диагностики** | • **Скачать журналы** - скачать диагностические журналы для передачи их в службу поддержки UserGate.<br>• **Очистить журналы** - очистить содержимое журналов. |
| **Удаленный помощник** | • **Вкл/Выкл** - включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к серверу UserGate LogAn для диагностики и решения проблем. Для успешной активации удаленного помощника UserGate LogAn должен иметь доступ к серверу удаленного помощника компании UserGate по протоколу SSH.<br>• **Идентификатор удаленного помощника** - полученное случайным образом значение. Уникально для каждого включения удаленного помощника.<br>• **Токен удаленного помощника** - полученное случайным образом значение токена. Уникально для каждого включения удаленного помощника. |

### 4.2.2 Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

| Наименование | Описание |
|---|---|
| **Операции с сервером** | • **Перезагрузить** - перезагрузка сервера UserGate LogAn. |

| | |
|---|---|
| | • **Выключить** - выключение сервера UserGate LogAn. |
| **Обновления** | Выбор канала обновлений ПО UserGate LogAn:<br>• **Стабильные** - проверка наличия стабильных обновлений ПО.<br>• **Бета** - проверка наличия экспериментальных обновлений. |

Компания UserGate постоянно работает над улучшением качества своего программного обеспечения и предлагает обновления продукта UserGate LogAn в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе Лицензирование UserGate LogAn). При наличии обновлений в разделе **Управление продуктом** отобразится соответствующее оповещение. Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя UserGate LogAn.

Для установки обновлений необходимо выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать файл резервного копирования | Создать резервную копию состояния UserGate LogAn, как это описано в разделе **Управление устройством --> Резервное копирование и восстановление первоначальных настроек**. Данный шаг рекомендуется всегда выполнять перед применением обновлений, поскольку он позволит восстановить предыдущее состояние устройства в случае возникновения каких-либо проблем во время применения обновлений. |
| **Шаг 2.** Установить обновления | В разделе **Управление устройством** при наличии оповещения **Доступны новые обновления** нажать на ссылку **Установить сейчас**. Система установит скачанные обновления, по окончании установки UserGate LogAn будет перезагружен. |

### 4.2.3 Экспорт настроек

Администратор имеет возможность сохранить текущие настройки UserGate LogAn в файл и впоследствии восстановить эти настройки на этом же или другом сервере UserGate LogAn. В отличие от резервного копирования, экспорт/импорт настроек не сохраняет текущее состояние всех компонентов комплекса, сохраняются только текущие настройки.

**Примечание**

Экспорт/импорт настроек не восстанавливает состояние интерфейсов и информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать UserGate LogAn с помощью имеющегося ПИН-кода и настроить интерфейсы.

Для экспорта настроек необходимо выполнить следующие действия:

| Наименование | Описание |
|---|---|

| | |
|---|---|
| **Шаг 1.** Экспорт настроек | В разделе **Управление устройством --> Экспорт настроек** нажмите **Экспорт** и выберите **Экспортировать все настройки** или **Экспортировать сетевые настройки**. Система сохранит:<br>• текущие настройки сервера под именем: logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin<br>• сетевые настройки под именем: network-logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin<br><br>nodename – имя узла UserGate LogAn.<br><br>version – версия UserGate LogAn.<br><br>YYYYMMDD_HHMMSS – дата и время выгрузки настроек в часовом поясе UTC.<br><br>Например, logan_core-logan_core@ranreahattha_6.2.0.13494RS-1_20211227_091350.bin или network-logan_core-logan_core@ranreahattha_6.2.0.13494RS-1_20211227_091407.bin. |

Для применения созданных ранее настроек необходимо выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Импорт настроек | В разделе **Управление устройством** нажать на ссылку **Экспорт настроек --> Импорт** и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен |

Дополнительно администратор может настроить сохранение настроек на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать правило экспорта | В разделе **Управление устройством --> Экспорт настроек** нажать кнопку **Добавить**, указать имя и описание правила. |
| **Шаг 2.** Указать параметры удаленного сервера | Во вкладке правила **Удаленный сервер** указать параметры удаленного сервера:<br>• **Тип сервера** - FTP или SSH.<br>• **Адрес сервера** - IP-адрес сервера.<br>• **Порт** - порт сервера.<br>• **Логин** - учетная запись на удаленном сервере.<br>• Пароль/Подтверждение пароля - пароль учетной записи.<br>• **Путь на сервере** - путь на сервере, куда будут выгружены настройки. |
| **Шаг 3.** Выбрать расписание выгрузки | Во вкладке правила **Расписание** указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его в следующем виде:<br><br>(минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье)<br><br>Каждое из первых пяти полей может быть задано следующим образом:<br>• Звездочка (*) - обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) - обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, |

| | |
|---|---|
| | "1,5,10,11" или "1-11,19-23".<br>• Звездочка и тире используются для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа. |

## 4.3 Администраторы

Доступ к веб-консоли UserGate LogAn регулируется с помощью создания дополнительных учетных записей администраторов, назначения им профилей доступа, создания политики управления паролями администраторов и настройки доступа к веб-консоли на уровне разрешения сервиса в свойствах зоны сети.

**Примечание**

При первоначальной настройкеUserGate LogAn создается локальный суперпользователь Admin.

Для создания дополнительных учетных записей администраторов устройства необходимо выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать профиль доступа администратора | В разделе **Администраторы --> Профили администраторов** нажать кнопку **Добавить** и указать необходимые настройки. |
| **Шаг 2.** Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора | В разделе **Администраторы** нажать кнопку **Добавить** и выбрать необходимый вариант:<br>• **Добавить локального администратора** - создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа.<br>• **Добавить пользователя LDAP** - добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы авторизации**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль.<br>• **Добавить группу LDAP** - добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе **Серверы авторизации**. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. |

При создании профиля доступа администратора необходимо указать следующие параметры:

| Наименование | Описание |
|---|---|

| | |
|---|---|
| **Название** | Название профиля. |
| **Описание** | Описание профиля. |
| **Права доступа** | Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать:<br>• Нет доступа.<br>• Чтение.<br>• Чтение и запись. |
| **Пользовательские роли** | Определяет роли пользователя для действия над инцидентами и правилами аналитики, назначаемые администраторам данного профиля. Более подробно о ролях смотрите в разделах Роли и ролевые разрешения пользователей. |

### Примечание

Не следует путать роли и ролевые разрешения с правами доступа на определенные объекты в консоли управления. Права доступа дают возможность просматривать или изменять определенные объекты, например, инциденты, а роли и ролевые разрешения позволяют пользователю производить определенные действия с элементами объектов, например, создать инцидент, назначить ему исполнителя и т.п. Для полноценной работы пользователя в системе, как правило, требуется делегирование ему прав доступа и определенных ролевых разрешений.

Администратор UserGate LogAn может настроить дополнительные параметры защиты учетных записей администраторов, такие, как сложность пароля и блокировку учетной записи на определенное время при превышении количества неудачных попыток авторизации.

Для настройки этих параметров необходимо:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Настроить политику паролей | В разделе **Администраторы --> Администраторы** нажать кнопку **Настроить**. |
| **Шаг 2.** Заполнить необходимые поля | Указать значения следующих полей:<br>• **Сложный пароль** - включает дополнительные параметры сложности пароля, задаваемые ниже, такие как - минимальная длина, минимальное число символов в верхнем регистре, минимальное число символов в нижнем регистре, минимальное число цифр, минимальное число специальных символов, максимальная длина блока из одного и того же символа.<br>• **Число неверных попыток аутентификации** - количество неудачных попыток аутентификации администратора, после которых учетная запись заблокируется на **Время блокировки**. |

| | |
|---|---|
| | • **Время блокировки** - время, на которое блокируется учетная запись. |

В разделе **Администраторы --> Сессии администраторов** отображаются все администраторы, выполнившие вход в веб-консоль администрирования UserGate LogAn. При необходимости любую из сессий администраторов можно закрыть (сбросить).

Администратор может указать зоны, с которых будет возможен доступ к сервису веб-консоли (порт TCP 8010).

**Примечание**

Не рекомендуется разрешать доступ к веб-консоли для зон, подключенных к неконтролируемым сетям, например, к сети интернет.

Для разрешения сервиса веб-консоли для определенной зоны необходимо в свойствах зоны в разделе контроль доступа разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе Настройка зон.

## 4.4 Управление сертификатами

UserGate LogAn использует защищенный протокол HTTPS для управления устройством. Для выполнения данной функции UserGate LogAn использует сертификат типа **SSL веб-консоли**.

Для того чтобы создать новый сертификат, необходимо выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать сертификат | Нажать на кнопку **Создать** в разделе **Сертификаты**. |
| **Шаг 2.** Заполнить необходимые поля | Указать значения следующих полей:<br>• **Название** - название сертификата, под которым он будет отображен в списке сертификатов.<br>• **Описание** - описание сертификата.<br>• **Страна** - страна, в которой выписывается сертификат.<br>• **Область или штат** - область или штат, в котором выписывается сертификат.<br>• **Город** - город, в котором выписывается сертификат.<br>• **Название организации** - название организации, для которой выписывается сертификат.<br>• **Common name** - имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров.<br>• **E-mail** - e-mail вашей компании. |
| **Шаг 3.** Указать, для чего будет использован данный сертификат | После создания сертификата необходимо указать его роль в UserGate LogAn. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку **Редактировать** и указать тип сертификата - SSL веб-консоли. После этого UserGate LogAn |

| | |
|---|---|
| | перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата. |

UserGate LogAn позволяет экспортировать созданные сертификаты и импортировать сертификаты, созданные на других системах, например, сертификат, выписанный доверенным удостоверяющим центром вашей организации.

Для экспорта сертификата необходимо:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Выбрать сертификат для экспорта | Выделить необходимый сертификат в списке сертификатов. |
| **Шаг 2.** Экспортировать сертификат | Выбрать тип экспорта:<br>• **Экспорт сертификата** - экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для инспектирования SSL, для установки его в качестве локального удостоверяющего центра на компьютеры пользователей.<br>• **Экспорт CSR** - экспортирует CSR сертификата, например, для подписи его удостоверяющим центром. |

**Примечание**

Рекомендуется сохранять сертификат для возможности его последующего восстановления.

**Примечание**

В целях безопасностиUserGate LogAn не разрешает экспорт приватных ключей сертификатов.

Для импорта сертификата необходимо иметь файлы сертификата и - опционально - приватного ключа сертификата и выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Начать импорт | Нажать на кнопку **Импорт**. |
| **Шаг 2.** Заполнить необходимые поля | Указать значения следующих полей:<br>• Название - название сертификата, под которым он будет отображен в списке |

| | |
|---|---|
| | сертификатов.<br>• Описание - описание сертификата.<br>• Загрузите файл, содержащий данные сертификата.<br>• Загрузите файл, содержащий приватный ключ сертификата.<br>• Пароль для приватного ключа, если таковой требуется.<br>• Цепочка сертификатов – файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата. Необязательное поле. |

## 4.5 Серверы авторизации

Серверы авторизации - это внешние источники учетных записей пользователей для авторизации в веб-консоли управления LogAn. LogAn поддерживает только сервер авторизации LDAP-коннектор. LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA.
- Осуществлять авторизацию пользователей через домены Active Directory/FreeIPA.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

| Наименование | Описание |
|---|---|
| **Вкл** | Включает или отключает использование данного сервера авторизации. |
| **Название** | Название сервера авторизации. |
| **SSL** | Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу. |
| **Доменное имя LDAP или IP-адрес** | IP-адрес контроллера домена или название домена LDAP. Если указано доменное имя, то UserGate получит адрес сервера LDAP с помощью DNS-запроса. |
| **Bind DN («login»)** | Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене. |
| **Пароль** | Пароль пользователя для подключения к домену. |
| **Домены LDAP** | Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. |
| **Пути поиска** | Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com. |

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Настройка LDAP-коннектора завершена.

## 4.6 Роли и ролевые разрешения пользователей

Роль пользователя - это набор ролевых разрешений. Ролевое разрешение - это возможность администратору совершать определенные действия, например, добавлять или удалять вложение из созданного инцидента, создавать правило срабатывания, создать или закрыть инцидент и т.д. Роли назначаются профилям администраторов, которые присваиваются администраторам. Подробно о создании администраторов и их профилей смотрите в разделе Администраторы.

Что бы создать роль и назначить ей определенные разрешения необходимо выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать роль | В разделе **Роли пользователей** нажать на кнопку **Добавить**, дать название и описание создаваемой роли. |
| **Шаг 2.** Добавить в созданную роль необходимые разрешения | В разделе **Ролевые разрешения** выбрать необходимое разрешение и с помощью кнопки **Добавить** добавить в него созданную ранее роль. |

Для пользователей могут быть указаны следующие ролевые разрешения.

| Наименование | Описание |
|---|---|
| **Назначаемый пользователь** | Пользователь с этим разрешением может быть назначен на инцидент.<br><br>Ответственный за инцидент может быть указан при создании или редактировании инцидента. |
| **Назначение инцидентов** | Возможность назначать пользователей на инциденты.<br><br>Указать ответственного можно при создании или редактировании инцидента. |
| **Закрытие инцидентов** | Возможность закрыть инцидент. Часто бывает полезно, когда разработчики разрешают инциденты, а тестировщики закрывают их.<br><br>Закрыть инцидент можно во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента). Закрытие инцидента возможно только из состояний, для которых в схеме инцидента настроен переход в состояние Закрыт. Подробнее читайте в Настройки инцидентов. |
| **Создание инцидентов** | Возможность создавать инциденты.<br><br>Инциденты могут быть созданы во вкладке **Инциденты --> Журнал инцидентов** или автоматически при срабатывании правила аналитики. О создании инцидентов |

| | |
|---|---|
| | подробнее читайте в разделе Создание инцидентов безопасности. |
| **Изменение инцидентов** | Возможность изменять инциденты.<br><br>Редактирование инцидентов доступно во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента). Подробнее читайте в разделе Подробности инцидента. |
| **Переоткрытие инцидентов** | Возможность переоткрывать инциденты.<br><br>Заново открыть инцидент можно во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента). |
| **Редактирование наблюдателей** | Возможность добавлять и удалять наблюдателей.<br><br>Пользователи для наблюдения за инцидентом могут быть указаны при создании или редактировании инцидента. |
| **Оставление комментариев** | Возможность комментировать инциденты.<br><br>Комментирование инцидентов возможно во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в разделе **Активность**. |
| **Удаление любых комментариев** | Возможность удалять любые комментарии к инцидентам.<br><br>Комментарии к инциденту можно посмотреть во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в разделе **Активность**. |
| **Удаление собственных комментариев** | Возможность удалять собственные комментарии к инцидентам.<br><br>Комментарии к инциденту можно посмотреть во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в разделе **Активность**. |
| **Редактирование любых комментариев** | Возможность редактировать любые комментарии к инцидентам.<br><br>Комментарии к инциденту можно посмотреть во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в разделе **Активность**. |
| **Редактирование своих комментариев** | Возможность редактировать свои комментарии к инцидентам.<br><br>Комментарии к инциденту можно посмотреть во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в разделе **Активность**. |
| **Создание вложений** | Возможность добавлять вложения к инцидентам.<br><br>Вложения к инциденту можно добавить во вкладке **Инциденты** при создании инцидента или его редактировании. Вложения отображены во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в разделе **Вложения**. |

| | |
|---|---|
| **Удаление любых вложений** | Возможность удалять любые вложения.<br><br>Вложения к инциденту отображены во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в разделе **Вложения**. |
| **Удаление своих вложений** | Возможность удалять свои вложения.<br><br>Вложения к инциденту отображены во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в разделе **Вложения**. |
| **Редактирование улик** | Возможность создания и редактирования улик.<br><br>Улики могут быть добавлены во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в разделе **Улики**. Подробнее об уликах читайте в разделе Подробности инцидента. |
| **Обновление обогащений** | Возможность обновлять/запрашивать обогащения улик.<br><br>Список внешних сервисов обогащений доступен во вкладке **Настройки** в разделе **Библиотеки --> Внешние сервисы обогащений**. Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений. |
| **Создание отчёта** | Возможность создавать, загружать и посылать отчёты инцидентов.<br><br>Создание отчётов инцидентов доступно во вкладке **Инциденты --> INC-N:Название инцидента** (где N – порядковый номер инцидента). Подробнее читайте в разделе Подробности инцидента. |
| **Добавление журналов к инциденту** | Возможность добавлять журналы к инциденту.<br><br>Журналы могут быть добавлены во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в разделе **Журналы**. Подробнее о журналах читайте в разделе Поиск; о срабатываниях – в разделе Срабатывания. |
| **Удалить все срабатывания/журналы из инцидента** | Возможность удаления всех срабатываний/журналов из инцидента.<br><br>Срабатывания и журналы отображены во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в соответствующих разделах **Срабатывания** и **Журналы**. Подробнее о журналах читайте в разделе Поиск; о срабатываниях – в разделе Срабатывания. |
| **Удаление собственных срабатываний, журналов к инцидентам** | Возможность удалять собственные срабатывания/журналы к инцидентам.<br><br>Срабатывания и журналы отображены во вкладке **Инциденты --> <INC-N:Название инцидента>** (где N – порядковый номер инцидента) в соответствующих разделах **Срабатывания** и **Журналы**. Подробнее о журналах читайте в разделе Поиск; о срабатываниях – в разделе Срабатывания. |
| **Создание схемы инцидента** | Возможность создавать схемы инцидентов.<br><br>Схемы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов --> Схема инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |

| | |
|---|---|
| **Редактирование схемы инцидента** | Возможность редактировать схемы инцидентов.<br><br>Схемы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов --> Схема инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Удаление схемы инцидента** | Возможность удалять схемы инцидентов.<br><br>Схемы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов --> Схема инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Установка схемы инцидентов по умолчанию** | Возможность установки схем инцидентов по умолчанию.<br><br>В UserGate LogAn создана одна схема инцидента по умолчанию; доступна во вкладке **Настройки** в разделе **Настройка инцидентов --> Схема инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Создание состояния инцидента** | Возможность создавать состояния инцидентов.<br><br>Список состояний инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов --> Состояния инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Редактирование состояния инцидента** | Возможность редактировать состояния инцидентов.<br><br>Список состояний инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов --> Состояния инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Удаление состояния инцидента** | Возможность удалять состояния инцидентов.<br><br>Список состояний инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов --> Состояния инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Создание типа инцидента** | Возможность создавать типы инцидентов.<br><br>Типы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов --> Типы инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Редактирование типа инцидента** | Возможность редактировать типы инцидентов.<br><br>Типы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов --> Типы инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Удаление типа инцидента** | Возможность удалять типы инцидентов.<br><br>Типы инцидентов доступны во вкладке **Настройки** в разделе **Настройка инцидентов --> Типы инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |

| | |
|---|---|
| **Создание решения инцидента** | Возможность создавать решения инцидентов.<br><br>Список решений инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов --> Решения инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Редактирование решения инцидентов** | Возможность редактировать решения инцидентов.<br><br>Список решений инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов --> Решения инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Удаление решения инцидентов** | Возможность удалять решения инцидентов.<br><br>Список решений инцидентов отображён во вкладке **Настройки** в разделе **Настройка инцидентов --> Решения инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Создание действия реагирования** | Возможность создавать действия реагирования.<br><br>Действия реагирования могут быть созданы во вкладке **Аналитика --> Действия реагирования**. Подробнее читайте в разделе Действия реагирования. |
| **Редактирование действия реагирования** | Возможность редактировать действия реагирования.<br><br>Действия реагирования отображены во вкладке **Аналитика --> Действия реагирования**. Подробнее читайте в разделе Действия реагирования. |
| **Удаление действия реагирования** | Возможность удалять действия реагирования.<br><br>Действия реагирования отображены во вкладке **Аналитика --> Действия реагирования**. Подробнее читайте в разделе Действия реагирования. |
| **Включение/выключение действия реагирования** | Возможность включать/выключать действия реагирования.<br><br>Действия реагирования отображены во вкладке **Аналитика --> Действия реагирования**. Подробнее читайте в разделе Действия реагирования. |
| **Создание сенсора** | Возможность создавать сенсоры.<br><br>Сенсоры UserGate, SNMP, SNMP MIB и WMI могут быть созданы во вкладке **Настройки** в разделе **Сенсоры**. Подробнее читайте в разделе Сенсоры. |
| **Редактирование сенсора** | Возможность редактировать сенсоры.<br><br>Сенсоры UserGate, SNMP, SNMP MIB и WMI доступны во вкладке **Настройки** в разделе **Сенсоры**. Подробнее читайте в разделе Сенсоры. |
| **Включение/выключение сенсора** | Возможность включать/выключать сенсоры.<br><br>Сенсоры UserGate, SNMP, SNMP MIB и WMI доступны во вкладке **Настройки** в разделе **Сенсоры**. Подробнее читайте в разделе Сенсоры. |
| **Создание правила syslog** | Возможность создавать правила syslog. |

| | |
|---|---|
| | Правила syslog могут быть созданы во вкладке **Настройки** в разделе **Библиотеки --> Приложения syslog**. |
| **Редактирование правила syslog** | Возможность редактировать правила syslog.<br><br>Созданные правила syslog доступны во вкладке **Настройки** в разделе **Библиотеки --> Приложения syslog**. |
| **Включение/выключение правила syslog** | Возможность включать/выключать правила syslog.<br><br>Правила syslog доступны во вкладке **Настройки** в разделе **Библиотеки --> Приложения syslog**. |
| **Создание группы email** | Возможность создавать почтовые адреса/почтовые группы.<br><br>Почтовые адреса и группы почтовых адресов могут быть созданы во вкладке **Настройки** в разделе **Библиотеки --> Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса. |
| **Редактирование группы email** | Возможность редактировать почтовые адреса/почтовые группы.<br><br>Почтовые адреса и группы почтовых адресов доступны во вкладке **Настройки** в разделе **Библиотеки --> Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса. |
| **Удаление группы email** | Возможность удалять почтовые адреса/почтовые группы.<br><br>Почтовые адреса и группы почтовых адресов доступны во вкладке **Настройки** в разделе **Библиотеки --> Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса. |
| **Создание группы номеров телефонов** | Возможность создавать номера телефонов/группы телефонных номеров.<br><br>Номера телефонов и группы телефонных адресов могут быть созданы во вкладке **Настройки** в разделе **Библиотеки --> Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса. |
| **Редактирование группы номеров телефонов** | Возможность редактировать номера телефонов/группы телефонных номеров.<br><br>Номера телефонов и группы телефонных адресов могут доступны во вкладке **Настройки** в разделе **Библиотеки --> Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса. |
| **Удаление группы номеров телефонов** | Возможность удалять номера телефонов/группы телефонных номеров.<br><br>Номера телефонов и группы телефонных адресов могут доступны во вкладке **Настройки** в разделе **Библиотеки --> Почтовые адреса**. Подробнее читайте в разделе Почтовые адреса. |
| **Создание профиля оповещения** | Возможность создавать профиль оповещения.<br><br>Во вкладке **Настройки** в разделе **Библиотеки --> Профили оповещений** могут быть созданы два типа профилей: SMPP и SMTP. Подробнее о профилях оповещений читайте в разделе Профили оповещений. |

| | |
|---|---|
| **Редактирование профиля оповещения** | Возможность редактировать профиль оповещения.<br><br>Список профилей доступен во вкладке **Настройки** в разделе **Библиотеки --> Профили оповещений**. Подробнее о профилях оповещений читайте в разделе Профили оповещений. |
| **Удаление профиля оповещения** | Возможность редактировать профиль оповещения.<br><br>Список профилей доступен во вкладке **Настройки** в разделе **Библиотеки --> Профили оповещений**. Подробнее о профилях оповещений читайте в разделе Профили оповещений. |
| **Создание категории срабатывания** | Возможность создавать категории срабатывания.<br><br>Категории срабатываний могут быть созданы во вкладке **Настройки** в разделе **Библиотеки --> Категории срабатываний**. Подробнее о категориях срабатываний читайте в разделе Категории срабатываний. |
| **Редактирование категории срабатывания** | Возможность редактировать категории срабатывания.<br><br>Список категорий срабатываний доступен во вкладке **Настройки** в разделе **Библиотеки --> Категории срабатываний**. Подробнее о категориях срабатываний читайте в разделе Категории срабатываний. |
| **Удаление категории срабатывания** | Возможность удалять категории срабатывания.<br><br>Список категорий срабатываний доступен во вкладке **Настройки** в разделе **Библиотеки --> Категории срабатываний**. Подробнее о категориях срабатываний читайте в разделе Категории срабатываний. |
| **Редактирование внешнего сервиса обогащения** | Возможность редактировать внешний сервис обогащения.<br><br>Список внешних сервисов обогащения доступен во вкладке **Настройки** в разделе **Библиотеки --> Внешние сервисы обогащений**. Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений. |
| **Включение/выключение внешнего сервиса обогащения** | Возможность включать/выключать внешний сервис обогащения.<br><br>Список внешних сервисов обогащения доступен во вкладке **Настройки** в разделе **Библиотеки --> Внешние сервисы обогащений**. Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений. |

После создания роли, она может быть использована для назначения в профили администраторов.

# 5 ОФЛАЙН ОПЕРАЦИИ С СЕРВЕРОМ

Некоторые операции с сервером проводятся, когда сервер не выполняет свою функцию и находится в офлайн режиме. Для выполнения таких операций необходимо во время загрузки сервера выбрать раздел меню **Support menu** и затем одну из требуемых операций. Для получения доступа к этому меню необходимо подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB (при наличии соответствующих разъемов на устройстве) или используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UserGate LogAn. Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.

Во время загрузки администратор может выбрать один из нескольких пунктов загрузки в boot-меню:

| Наименование | Описание |
|---|---|
| **UGOS LOGAN** | Загрузка UserGate с выводом диагностической информации о загрузке в последовательный порт. |
| **UGOS LOGAN (failsafe)** | Загрузка UserGate в упрощённом видеорежиме. |
| **Support menu** | Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор). |
| **Restore previous version** | Раздел доступен после обновления или создания резервной копии. |

Раздел системных утилит (**Support menu**) позволяет выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Check filesystems** | Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление. |
| **Expand data partition** | Увеличение раздела для хранения данных на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UserGate. Данные и настройки UserGate не сбрасываются. |
| **Create backup** | Создать полную копию диска UserGate на внешний USB носитель. Все данные на внешнем носителе будут удалены. |
| **Restore from backup** | Восстановление UserGate с внешнего USB носителя. |
| **Factory reset** | Сброс состояния UserGate к первоначальному состоянию системы. Все данные и настройки будут утеряны. |
| **Exit** | Выход и перезагрузка устройства. |

# 6 НАСТРОЙКА СЕТИ

В данном разделе описаны сетевые настройки UserGate LogAn.

## 6.1 Настройка зон

Зона в UserGate LogAn - это логическое объединение сетевых интерфейсов. Политики безопасности UserGate LogAn используют зоны интерфейсов, а не непосредственно интерфейсы.

Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например, зона LAN-интерфейсов, зона интернет-интерфейсов, зона интерфейсов управления.

По умолчанию UserGate LogAn поставляется со следующими зонами:

| Наименование | Описание |
|---|---|
| **Management** | Зона для подключения доверенных сетей, из которых разрешено управление UserGate LogAn. |
| **Trusted** | Зона для подключения доверенных сетей, например, LAN-сетей. Предполагается, что через зону Trusted LogAn будет подключен в сеть, через которую шлюзы UserGate будут отсылать на него журналы, а также через которую LogAn получит доступ в интернет. |

Для работы UserGate LogAn достаточно одного настроенного интерфейса. Разделение функций управления устройством и сбора данных на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.

Администраторы UserGate LogAn могут изменять настройки зон, созданных по умолчанию, а также создавать дополнительные зоны.

**Примечание**

Можно создать не более 255 зон.

Для создания зоны необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать зону | Нажать на кнопку **Добавить** и дать название зоне. |
| **Шаг 2.** Настроить параметры защиты зоны от DoS (опционально) | Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP:<br>• **Порог уведомления** - при превышении количества запросов с одного IP-адреса над указанным значением происходит запись события в системный журнал.<br>• **Порог отбрасывания пакетов** - при превышении количества запросов с одного IP-адреса над указанным значением UserGate LogAn начинает |

| | |
|---|---|
| | отбрасывать пакеты, поступившие с этого IP-адреса, и записывает данное событие в системный журнал.<br><br>Рекомендованные значения для порога уведомления - 300 запросов в секунду, для порога отбрасывания пакетов - 600 запросов в секунду.<br><br>**Исключения защиты от DoS** - позволяет указать список IP-адресов серверов, которые необходимо исключить из защиты. Это может быть полезно, например, для шлюзов UserGate, которые могут слать большой объем данных на сервера LogAn. |
| **Шаг 3.** Настроить параметры контроля доступа зоны (опционально) | Указать предоставляемые UserGate LogAn сервисы, которые будут доступны клиентам, подключенным к данной зоне. Для зон, подключенных к неконтролируемым сетям, таким, как интернет, рекомендуется отключить все сервисы.<br><br>Сервисы:<br>• **Ping** - позволяет пинговать UserGate LogAn.<br>• **SNMP** – доступ к UserGate LogAn по протоколу SNMP (UDP 161).<br>• **XML-RPC** для управления - позволяет управлять продуктом по API (TCP 4040).<br>• **Консоль администрирования** - доступ к веб-консоли управления (TCP 8010).<br>• **CLI по SSH** - доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200.<br>• **Log Analyzer** – сервис анализатора журналов Log Analyzer. Необходимо разрешить на зонах, с которых LogAn будет получать данные от серверов UserGate (TCP 22699 – для серверов UserGate версии 6.1.x; TCP 22711 - для серверов UserGate версии 7.0.x, использующих SSL для передачи данных).<br>• **Сборщик логов** - сервис для разрешения сбора информации с удалённых устройств по протоколу Syslog (по умолчанию используется порт 514). |
| **Шаг 4.** Настроить параметры защиты от IP-спуфинг атак (опционально) | Атаки на основе IP-спуфинга позволяют передать пакет из одной сети, например, из **Trusted**, в другую, например, в **Management**. Для этого атакующий подменяет IP-адрес источника на предполагаемый адрес необходимой сети. В таком случае ответы на этот пакет будут пересылаться на внутренний адрес.<br><br>Для защиты от подобных атак администратор может указать диапазоны IP-адресов, адреса источников которых допустимы в выбранной зоне. Сетевые пакеты с адресами источников, отличными от указанных, будут отброшены.<br><br>С помощью чекбокса **Инвертировать** администратор может указать адреса источников, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными диапазонами IP-адресов источников. Например, можно указать диапазоны "серых" IP-адресов 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0./16 и включить опцию **Инвертировать**. |

## 6.2 Настройка интерфейсов

Раздел **Интерфейсы** отображает все физические и виртуальные интерфейсы, имеющиеся в системе, позволяет менять их настройки и добавлять VLAN и бонд-интерфейсы.

Кнопка **Редактировать** позволяет изменять параметры сетевого интерфейса:

- Включить или отключить интерфейс.

- Указать тип интерфейса - Layer 3.
- Назначить зону интерфейсу.
- Изменить физические параметры интерфейса - MAC-адрес и размер MTU.
- Выбрать тип присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:

- VLAN.
- Бонд.

### 6.2.1 Объединение интерфейсов в бонд

С помощью кнопки **Добавить бонд-интерфейс** администратор может объединить несколько физических интерфейсов в один логический агрегированный интерфейс для повышения пропускной способности или для отказоустойчивости канала. При создании бонда необходимо указать следующие параметры:

| Наименование | Описание |
|---|---|
| **Вкл** | Включает бонд. |
| **Название** | Название бонда. |
| **Зона** | Зона, к которой принадлежит бонд. |
| **Интерфейсы** | Один или более интерфейсов, которые будут использованы для построения бонда. |
| **Режим** | Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть:<br>• **Round robin.** Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости.<br>• **Active backup**. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости.<br>• **XOR.** Передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и отказоустойчивости.<br>• **Broadcast.** Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости.<br>• **IEEE 802.3ad** - режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику. |

| | |
|---|---|
| | • **Adaptive transmit load balancing.** Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты.<br>• **Adaptive load balancing.** Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами. |
| **MII monitoring period (мсек)** | Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию - 0 - отключает MII-мониторинг. |
| **Down delay (мсек)** | Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0. |
| **Up delay (мсек)** | Задает время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0. |
| **LACP rate** | Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения:<br>• **Slow** - запрос партнера на передачу LACPDU-пакетов каждые 30 секунд.<br>• **Fast** - запрос партнера на передачу LACPDU-пакетов каждую 1 секунду. |
| **Failover MAC** | Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. Возможные значения:<br>• **Отключено** - устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения.<br>• **Active** - MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа.<br>• **Follow** - MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном. |
| **Xmit hash policy** | Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или |

| | |
|---|---|
| | IEEE 802.3ad. Возможные значения:<br>• **Layer 2** - использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad.<br>• **Layer 2+3** - использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad.<br>• **Layer 3+4** - используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут дойти до получателя не в том порядке, так как отправляются через разные интерфейсы. |
| **Сеть** | Способ присвоения IP-адреса - без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. |

## 6.3 Настройка шлюзов

Для подключения UserGate LogAn к интернету необходимо указать IP-адрес одного или нескольких шлюзов.

Можно указать несколько шлюзов, если для подключения к интернету используется несколько провайдеров. Пример настройки сети с двумя провайдерами:

- Интерфейс port1 с IP-адресом 192.168.11.2 подключен к интернет-провайдеру 1. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.11.1.
- Интерфейс port2 с IP-адресом 192.168.12.2 подключен к интернет-провайдеру 2. Для выхода в интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.12.1.

При наличии двух или более шлюзов возможны 2 варианта работы:

| Наименование | Описание |
|---|---|
| **Балансировка трафика между шлюзами** | Установить флажок **Балансировка** и указать **Вес** каждого шлюза. В этом случае весь трафик в интернет будет распределен между шлюзами в соответствии с указанными весами (чем больше вес, тем большая доля трафика идет через шлюз). |
| **Основной шлюз с переключением на запасной** | Выбрать один из шлюзов в качестве основного и настроить **Проверку сети**, нажав на одноименную кнопку в интерфейсе. Проверка сети проверяет доступность хоста в интернет с указанной в настройках периодичностью, и в случае, если хост перестает быть доступен, переводит весь трафик на запасные шлюзы в порядке их расположения в консоли. |

По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8), но может быть изменена на любой другой хост по желанию администратора.

## 6.4 Маршруты

Данный раздел позволяет указать маршрут в сеть, доступную за определенным маршрутизатором. Например, в локальной сети может быть маршрутизатор, который объединяет несколько IP-подсетей.

Для добавления маршрута необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Задать название и описание данного маршрута | В разделе **Сеть** выберите в меню **Маршруты**, нажмите кнопку **Добавить**. Укажите имя для данного маршрута. Опционально можно задать описание маршрута. |
| **Шаг 2.** Указать адрес назначения | Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172 .16.20.5/32. |
| **Шаг 3.** Указать шлюз | Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера UserGate LogAn. |
| **Шаг 4.** Указать интерфейс | Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение **Автоматически**, то UserGate LogAn сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов. |
| **Шаг 5.** Указать метрику | Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут, если маршрутов несколько в данную сеть несколько. |

# 7 ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ (CLI)

UserGate LogAn позволяет создавать базовые настройки устройства с помощью интерфейса командной строки, или CLI (command line interface). С помощью CLI администратор может выполнить ряд диагностирующих команд, таких, как ping, nslookup, traceroute, осуществить настройку сетевых интерфейсов и зон, а также перезагрузить или выключить устройство.

CLI полезно использовать для диагностики сетевых проблем или в случае, когда доступ к веб-консоли утерян, например, некорректно указан IP-адрес интерфейса или ошибочно установлены параметры контроля доступа для зоны, запрещающие подключение к веб-интерфейсу.

Подключение к CLI можно выполнить через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании UserGate LogAn), через последовательный порт или с помощью SSH по сети.

Для подключения к CLI с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Подключить монитор и клавиатуру к UserGate LogAn | Подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB. |
| **Шаг 2.** Войти в CLI | Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство UserGate LogAn не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля - utm. |

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Подключиться к UserGate LogAn | Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к UserGate LogAn. |
| **Шаг 2.** Запустить терминал | Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows или minicom для Linux. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1. |
| **Шаг 3.** Войти в CLI | Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство UserGate LogAn не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля - utm. |

Для подключения к CLI по сети с использованием протокола SSH необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|

| | |
|---|---|
| **Шаг 1.** Разрешить доступ к CLI (SSH) для выбранной зоны | Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200. |
| **Шаг 2.** Запустить SSH-терминал | Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес UserGate LogAn, в качестве порта подключения - 2200, в качестве имени пользователя - имя пользователя с правами Full administrator (по умолчанию Admin). Для Linux команда на подключение должна выглядеть так:<br><br>ssh Admin@IPUserGateLogAn -p 2200 |
| **Шаг 3.** Войти в CLI | Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство UserGate LogAn не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля - utm. |

После успешного входа в CLI можно посмотреть список возможных команд с помощью команды **help**. Для подробного описания любой команды необходимо использовать синтаксис
**help command.**

Например, для получения подробной справки по использованию команды настройки сетевого интерфейса iface необходимо выполнить
**help Iface**

Полный список команд:

| Наименование | Описание |
|---|---|
| **help** | Показывает список доступных команд. |
| **exit quit Ctrl+D** | Выйти из CLI. |
| **date** | Посмотреть текущее время на сервере. |
| **gateway** | Посмотреть или задать значения шлюза. Смотрите gateway help для детальной информации. |
| **iface** | Набор команд для просмотра и настройки параметров сетевого интерфейса. Смотрите iface help для детальной информации. |
| **license** | Посмотреть информацию о лицензии. |
| **netcheck** | Проверить доступность стороннего HTTP/HTTPS-сервера.<br><br>**netcheck [-t TIMEOUT] [-d] URL**<br><br>Опции:<br><br>-t – максимальный таймаут ожидания ответа от веб-сервера.<br><br>-d – запросить содержание сайта. По умолчанию запрашиваются только заголовки. |

| | |
|---|---|
| **nslookup** | Выполнить определение IP-адреса по имени хоста. |
| **ping** | Выполнить ping определенного хоста. |
| **radmin** | Включить или отключить удаленный доступ к серверу для технической поддержки UserGate LogAn. |
| **radmin_e** | Включить или отключить удаленный доступ к серверу для технической поддержки UserGate LogAn, в случаях, когда сервер UserGate LogAn завис. |
| **reboot** | Перезагрузить сервер UserGate LogAn. |
| **route** | Создать, изменить, удалить маршрут. |
| **shutdown** | Выключить сервер UserGate LogAn. |
| **traceroute** | Выполнить трассировку соединения до определенного хоста. |
| **zone** | Набор команд для просмотра и настройки параметров зоны. Смотрите zone help для детальной информации. |

# 8 СЕНСОРЫ

Для сбора информации с различных устройств и последующего ее анализа UserGate LogAn использует сенсоры. Сенсор - это совместимое с LogAn устройство, которое может передавать определенные данные на сервер LogAn. Сенсорами могут выступать шлюзы UserGate, а также любые другие сетевые устройства, способные передавать данные по протоколу SNMP.

## 8.1 Сенсоры UserGate

Сенсор UserGate подключает одно устройство типа шлюз безопасности UserGate к серверу LogAn. Для подключения сенсора UserGate необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** На сервере UserGate разрешить сервисы **Log Analyzer** и **SNMP** на требуемой зоне | На сервере UserGate, который вы хотите добавить в качестве сенсора, в разделе **Сеть --> Зоны** выберите зону, через интерфейсы которой будет происходить сетевой обмен с сервером LogAn, и разрешите сервисы **Log Analyzer** и **SNMP**. |
| **Шаг 2.** На сервере UserGate скопируйте токен в буфер обмена | На сервере UserGate, который вы хотите добавить в качестве сенсора, в разделе **Настройки --> Log Analyzer** скопируйте значение токена в буфер обмена. Он понадобится на шаге 4. |
| **Шаг 3.** На сервере LogAn разрешить сервис Log Analyzer на требуемой зоне | На сервере LogAn в разделе **Сеть --> Зоны** выберите зону, через интерфейсы которой будет происходить сетевой обмен с сервером UserGate, и разрешите сервис Log Analyzer. |
| **Шаг 4.** Создайте сенсор UserGate | На сервере LogAn в разделе **Сенсоры --> Сенсоры UserGate** нажмите кнопку **Добавить** и заполните необходимые поля. |

При создании сенсора UserGate необходимо заполнить следующие поля:

| Наименование | Описание |
|---|---|
| **Включено** | Включает или выключает данный сенсор UserGate. |
| **Название** | Название сенсора UserGate. |
| **Описание** | Опциональное описание сенсора UserGate. |
| **Адрес сервера** | IP-адрес сервера UserGate, для которого создается данный сенсор. |
| **Log Analyzer адрес** | IP-адрес сервера LogAn, который будет использоваться на сервере UserGate, в качестве назначения для отсылки журналов. Для выбора отображаются только те адреса, на интерфейсах зон которых разрешен сервис Log Analyzer. |

| | |
|---|---|
| **Токен** | Токен, полученный на сервере UserGate. |

После создания сенсора, сервер UserGate начинает отсылать данные на сервер LogAn.

На сервере UserGate произошли следующие изменения конфигурации:

- В разделе Настройки--Log Analyzer изменился адрес сервера Log Analyzer на адрес, указанный при создании сенсора UserGate.
- В разделе Диагностика и мониторинг--SNMP добавилось правило SNMP, разрешающее серверу Log Analyzer получать информацию по протоколу SNMP.

На сервере LogAn добавились следующие элементы:

- В разделе Журналы и отчеты--Журналы появились записи с созданного UserGate сенсора.
- В Дашборде появилась возможность добавить новый виджет - График сенсора UserGate, содержащий информацию, полученную с сенсора UserGate.

**Примечание**

В случае изменения администратором правила SNMP на сервереUserGate, LogAn вернет настройки или пересоздаст правило при включении/отключении сенсора на сервере LogAn.

## 8.2 Сенсоры SNMP

С помощью сенсора SNMP администратор может подключить SNMP-совместимое сетевое устройство к серверу UserGate LogAn для сбора и анализа его метрик. UserGate LogAn может отображать любые счетчики, полученные по SNMP с помощью запросов SNMP. Для настройки сенсора SNMP необходимо иметь базы MIB (Management Information Base) на управляемое устройство. Подробнее об управлении базами MIB смотрите раздел данного руководства Управление SNMP MIB.

Для настройки сенсора SNMP необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Загрузите базу MIB того устройства, которое хотите добавить для мониторинга. | На сервере LogAn в разделе **Сенсоры--Управление SNMP MIB** загрузите файл с MIB. |
| **Шаг 2.** Создайте сенсор SNMP | На сервере LogAn в разделе **Сенсоры--Сенсоры SNMP** нажмите кнопку **Добавить** и заполните необходимые поля. |

При создании сенсора SNMP необходимо заполнить следующие поля:

| Наименование | Описание |
|---|---|
| **Вкл** | Включает или выключает данный сенсор SNMP. |

| | |
|---|---|
| **Название** | Название сенсора SNMP. |
| **Описание** | Опциональное описание сенсора SNMP. |
| **Адрес сервера** | IP-адрес сенсора SNMP. |
| **Порт** | Порт сенсора SNMP. Обычно для запросов данных по протоколу SNMP используется порт TCP 161. |
| **Версия** | Указывает версию протокола SNMP, которая будет использоваться в данном сенсоре. Возможны варианты SNMP v2c и SNMP v3. |
| **Community** | SNMP community - строка для идентификации сервера LogAn и сетевого устройства для версии SNMP v2c. Используйте только латинские буквы и цифры. |
| **Интервал опроса (сек)** | Интервал, через который сервер LogAn будет инициировать получение данных с сетевого устройства. |
| **Пользователь** | Только для SNMP v3. Имя пользователя для авторизации сетевом устройстве. |
| **Тип аутентификации** | Выбор режима аутентификации. Возможны варианты:<br>• Без аутентификации, без шифрования (noAuthNoPriv).<br>• С аутентификацией, без шифрования (authNoPriv).<br>• С аутентификацией, с шифрованием (authPriv).<br><br>Наиболее безопасным считается режим работы authPriv. |
| **Алгоритм аутентификации** | Алгоритм, используемый для аутентификации. |
| **Пароль аутентификации** | Пароль, используемый для аутентификации. |
| **Алгоритм шифрования** | Алгоритм, используемый для шифрования. Возможно использовать DES и AES. |
| **Пароль шифрования** | Пароль, используемый для шифрования. |
| **Счетчики** | Укажите здесь все требуемые данные, которые LogAn будет запрашивать на сетевом устройстве. Счетчики выбираются из баз MIB, которые загружены на устройство.<br><br>Выберите в дереве SNMP необходимый раздел и добавьте соответствующий счетчик либо укажите в строке SNMP OID счетчика и его тип. |

После успешного добавления сенсора в разделе Дашборд появилась возможность добавить виджет с графиками данных SNMP, полученными с данного сенсора.

## 8.3 Управление SNMP MIB

В данном разделе администратор может добавлять и удалять базы MIB (Management Information Base) на сервере UserGate LogAn.

Для получения специфических MIB обратитесь к производителю вашего устройства. UserGate LogAn уже содержит наиболее популярные базы сетевых устройств.

## 8.4 Сенсоры WMI

С помощью сенсора WMI администратор может подключить WMI-совместимое сетевое устройство (компьютер под управлением ОС WIndows) к серверу UserGate LogAn для сбора и анализа его метрик.

# 9 СБОРЩИК ЛОГОВ

Сборщик логов предназначен для централизованного сбора информации с сетевых устройств, что помогает облегчить мониторинг сети, виртуальных машин, серверов, пользовательских устройств, приложений.

## 9.1 Syslog

В данном разделе настраиваются правила сбора событий системных журналов Unix-систем (syslog), которые содержат информацию о работе системы, её состоянии и безопасности, наличии ошибок, сбоях в работе. Правила syslog позволяют осуществлять фильтрацию записей событий (по времени, критичности событий, объектам, названию устройств, приложениям), упрощая поиск необходимой информации.

Для работы сборщика логов необходимо настроить сервер, с которого будет происходить сбор информации, и правила syslog.

Настройка сервера производится в разделе **Сборщик логов --> Syslog** во вкладке **Настройки** веб-интерфейса UserGate Log Analyzer; необходимо указать следующие данные:

| Наименование | Описание |
|---|---|
| **Включено** | Включение/отключение приёма syslog событий. |
| **Протокол** | Сетевой протокол, использующийся для сбора информации:<br>• TCP.<br>• UDP. |
| **Порт** | Номер порта, использующегося для сбора syslog событий. По умолчанию – порт 514. |
| **Максимальное количество сессий** | Максимальное количество устройств, подключённых одновременно с целью отправки сообщений. |
| **Безопасное соединение** | Включение/отключение шифрования потока данных.<br>Подробнее об использовании TLS в Syslog читайте в соответствующей документации. |
| **Файл сертификата ЦС** | Сертификат удостоверяющего центра (центра сертификации), который используется для установления безопасного соединения. |
| **Файл сертификата** | Сертификат, сгенерированный пользователем и подписанный центром сертификации (ЦС); необходимо указать при настройке безопасного соединения. |
| **Разрешённые соседи** | Список устройств, с которых UserGate LogAn будет получать информацию в случае использования безопасного соединения. |

Для настройки правил фильтрации записей событий syslog необходимо указать следующие данные:

| Наименование | Описание |
| --- | --- |
| **Включено** | Включение/отключение правила syslog. |
| **Название** | Название правила syslog. |
| **Описание** | Описание правила syslog (опционально). |
| **Действие** | Действие:<br>• **Разрешить** – разрешение приёма сообщений, подходящих под условия правила.<br>• **Запретить** – блокировка приёма сообщений, подходящих под условия правила. |
| **Часовой пояс** | Часовой пояс, настроенный на удалённых устройствах. Приём сообщений будет разрешён или запрещён с устройств, у которых сохранение записей происходит в указанном часовом поясе. |
| **Вставить** | Место вставки создаваемого правила в списке правил: наверх, вниз или выше выбранного существующего правила. |
| **Критичность** | Критичность событий syslog:<br>• **Экстренная**: критическое состояние, которое сказывается на работоспособности системы.<br>• **Тревога**: состояние, требующее незамедлительного вмешательства.<br>• **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе.<br>• **Ошибки**: сообщения о сбоях в системе.<br>• **Предупреждения**: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия.<br>• **Уведомительная**: события, которые относятся к необычному поведению системы, но не являются ошибками.<br>• **Информативная**: информационные уведомления.<br>• **Отладочная**: информация, полезная разработчикам для отладки приложений. |
| **Объект** | Категория события:<br>• **Сообщения ядра**.<br>• **Сообщения пользовательские**.<br>• **Почтовая система**.<br>• **Системный сервис**.<br>• **Безопасность/авторизация**.<br>• **Сообщения syslog**.<br>• **Система печати LPR**.<br>• **Система сетевых новостей**.<br>• **Подсистема UUCP**.<br>• **Сервис времени**.<br>• **Безопасность/аутентификация**.<br>• **FTP сервис**.<br>• **Система NTP**.<br>• **Аудит**. |

| | |
|---|---|
| | • **Тревога**.<br>• **Сервис времени 2**.<br>• **Local 0 - Local 7**. |
| **Имя хоста** | Название устройства. |
| **Название приложения** | Название приложения, сбор информации о котором необходимо разрешить/запретить.<br><br>Подробнее читайте в разделе Приложения syslog. |

Записи событий будут отображены в журнале **Syslog**, подробнее читайте в разделе Системный журнал.

# 10 БИБЛИОТЕКИ

## 10.1 Почтовые адреса

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в правилах фильтрации почтового трафика и для использования в оповещениях.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать группу почтовых адресов | В панели **Группы почтовых адресов** нажать на кнопку **Добавить**, дать название группе. |
| **Шаг 2.** Добавить почтовые адреса в группу | Выделить созданную группу, нажать на кнопку **Добавить** на панели **Почтовые адреса** и добавить необходимые почтовые адреса. |

## 10.2 Номера телефонов

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать группу телефонных номеров | В панели **Группы телефонных номеров** нажать на кнопку **Добавить**, дать название группе. |
| **Шаг 2.** Добавить номера телефонов в группу | Выделить созданную группу, нажать на кнопку **Добавить** на панели **Группа телефонных номеров** и добавить необходимые номера. |

## 10.3 Профили оповещений

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP, доставка сообщений с помощью e-mail
- SMPP, доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки

Для создания профиля сообщений SMTP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

| Наименование | Описание |
|---|---|
| **Название** | Название профиля. |
| **Описание** | Описание профиля. |
| **Хост** | IP-адрес сервера SMTP, который будет использоваться для отсылки почтовых сообщений. |
| **Порт** | Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера. |
| **Безопасность** | Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL. |
| **Авторизация** | Включает авторизацию при подключении к SMTP-серверу. |
| **Логин** | Имя учетной записи для подключения к SMTP-серверу. |
| **Пароль** | Пароль учетной записи для подключения к SMTP-серверу. |

Для создания профиля сообщений SMPP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

| Наименование | Описание |
|---|---|
| **Название** | Название профиля. |
| **Описание** | Описание профиля. |
| **Хост** | IP-адрес сервера SMPP, который будет использоваться для отсылки SMS сообщений. |
| **Порт** | Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL – 3550. |
| **SSL** | Использовать или нет шифрацию с помощью SSL. |
| **Авторизация** | Включает авторизацию при подключении к SMPP-серверу. |
| **Логин** | Имя учетной записи для подключения к SMPP-серверу. |
| **Пароль** | Пароль учетной записи для подключения к SMPP-серверу. |
| **Правила трансляции номеров** | В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8. |

## 10.4 Категории срабатываний

Элемент библиотеки **Категории срабатываний** позволяет создать категории, по которым можно группировать определенные срабатывания правил аналитики, применяемые к событиям. Более подробно о правилах аналитики смотрите в разделе Аналитика. По умолчанию создаются категории:

- Availability - правила аналитики, определяющие инциденты, приводящие к ухудшению доступности информационных систем.
- Performance - правила аналитики, определяющие инциденты, приводящие к ухудшению производительности информационных систем.
- Security - правила аналитики, определяющие инциденты, приводящие к ухудшению безопасности информационных систем.

## 10.5 Внешние сервисы обогащений

В данном элементе библиотеки представлены ресурсы, с помощью которых происходит дополнительный сбор информации об угрозах. С данных источников приходят фиды – структурированные проанализированные данные об IP-адресах и доменах, с которых происходит распространение вредоносных файлов, их сэмплы и хэши; списки фишинговых сайтов, почтовые адреса отправителей фишинговых писем; адреса, с которых происходит сканирование сетей с целью обнаружения уязвимостей; IP-адреса, с которых проводятся атаки типа брутфорс; сигнатуры для обнаружения вредоносного программного обеспечения.

Чтобы использовать сервисы обогащения их необходимо включить. Для использования некоторых сервисов обогащения необходимо прохождение регистрации и предоставление ключа доступа.

| Наименование | Описание |
|---|---|
| **dnsgoogle** | Интернет-сервис компании Google, представляющий собой общедоступные DNS-серверы.<br>Подробнее: https://dns.google.<br>Предназначен для типов улик: IP. |
| **urlhaus** | Проект abuse.ch. Целью проекта является сбор, отслеживание и обмен URL-адресами вредоносных программ.<br>Подробнее: https://urlhaus.abuse.ch/.<br>Предназначен для типов улик: Домен, Хэш, Имя хоста, IP, URL. |
| **dshield** | Система корреляции журналов межсетевого экрана для совместной работы. Система получает журналы от добровольцев со всего мира и использует их для анализа тенденций атак.<br>Подробнее: https://www.dshield.org/xml.html.<br>Предназначен для типов улик: Домен, FQDN, IP. |
| **fortiguard** | Аналитическая и научно-исследовательская организация в сфере угроз компании Fortinet.<br>Подробнее: https://www.fortiguard.com/webfilter.<br>Предназначен для типов улик: Домен, FQDN, URL. |

| | |
|---|---|
| **cybercrime** | Сервис предоставляет информацию об уровнях угрозы разных объектов.<br><br>Подробнее: http://cybercrime-tracker.net.<br><br>Предназначен для типов улик: Домен, FQDN, IP, URL, Другое. |
| **cyberprotect** | Сервис предоставляет информацию об уровнях угрозы разных объектов.<br><br>Подробнее: https://console.threatscore.cyberprotect.cloud/.<br><br>Предназначен для типов улик: Домен, Хэш, IP, URL, Агент пользователя. |
| **unshorten** | Сервис предоставляет возможности предварительного просмотра целевого URL для любого короткого URL и проверки безопасности на вредоносные ссылки. Сервис не использует внешний ресурс; анализирует ответ на запрос по тестируемому URL.<br><br>Предназначен для типов улик: URL. |
| **ipwhois** | Сервис позволяет получить информацию об IP-адресах.<br><br>Подробнее: https://ipwhois.io/.<br><br>Предназначен для типов улик: IP. |
| **ipinfo** | Инструмент для определения владельца, интернет-провайдера и местонахождения веб-сайта, домена или IP-адреса.<br><br>Подробнее: https://ipinfo.io/.<br><br>Предназначен для типов улик: IP.<br><br>Для использования сервиса необходимо ввести реквизиты. |
| **hashdd** | Сервис предоставляет базу вредоносных хэшей файлов и различные проверки для получения полного представления об угрозе.<br><br>Подробнее: https://hashdd.com/.<br><br>Предназначен для типов улик: Хэш.<br><br>Для использования сервиса необходимо ввести реквизиты. |
| **urlscan** | Сервис для получения информации о подозрительных, вредоносных и фишинговых URL.<br><br>Подробнее: https://urlscan.io/.<br><br>Предназначен для типов улик: Домен, FQDN, Хэш, IP, URL.<br><br>Для использования сервиса необходимо ввести реквизиты. |
| **emailrep** | Система, которая собирает данные об адресах электронной почты, доменах и пользователях.<br><br>Подробнее: https://emailrep.io/.<br><br>Предназначен для типов улик: Почта.<br><br>Для использования сервиса необходимо ввести реквизиты. |

| | |
|---|---|
| **greynoise** | Компания занимается анализом фонового шума Интернета (пакеты данных, адресованные IP-адресам или портам, где нет сетевого устройства, настроенного для их приёма). Благодаря такой фильтрации снижается количество ложных срабатываний.<br>Подробнее: https://www.greynoise.io/.<br>Предназначен для типов улик: IP.<br>Для использования сервиса необходимо ввести реквизиты. |
| **abuseip** | Проект, который занимается борьбой со злоумышленной деятельностью.<br>Подробнее: https://www.abuseipdb.com/.<br>Предназначен для типов улик: IP.<br>Для использования сервиса необходимо ввести реквизиты. |
| **hybridanalysis** | Сервис проверки файлов на вредоносность.<br>Подробнее: https://www.hybrid-analysis.com/.<br>Предназначен для типов улик: Хэш.<br>Для использования сервиса необходимо ввести реквизиты. |

## 10.6 Приложения syslog

Данный раздел содержит приложения, которые могут быть использованы в правилах syslog для сбора информации.

Чтобы добавить приложение необходимо выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Шаг 1**. Создать приложение. | Нажать кнопку **Добавить** и указать название и описание приложения. |
| **Шаг 2**. Указать приложение. | Указать название приложения, для которого будут применены правила syslog. |

# 11 ДАШБОРД

Данный раздел позволяет посмотреть текущее состояние сервера и серверов, которые подключены к нему для отправки логов, их загрузку, статус лицензии и так далее.

Отчеты предоставлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице **Дашборд**. По умолчанию созданы страницы с виджетами Log Analyzer (отображение состояния сервера Log Analyzer), NOC (Network Operation Center) и SOC (Security Operation Center).

Некоторые виджеты позволяют настроить отображение, указать фильтрацию данных и настроить прочие параметры. Для настройки виджета необходимо кликнуть по символу шестеренки в правом верхнем углу. Не все параметры, перечисленные ниже, доступны для каждого типа виджетов.

| Наименование | Описание |
|---|---|
| **Название** | Название виджета, которое будет отображаться в Дашборд. |
| **Описание** | Опциональное описание виджета. |
| **Количество записей** | Максимальное количество записей для отображения. |
| **Группировать по** | Поле данных, по которому будут сгруппированы данные в виджете. |
| **Диаграмма** | Выбор типа представления данных. Доступны значения:<br>• Число.<br>• Круговая диаграмма.<br>• Вертикальная гистограмма.<br>• Горизонтальная гистограмма.<br>• Таблица.<br>• График.<br>• Карта мира. |
| **Запрос фильтра** | SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных. |
| **Сенсор** | Сенсор, данные с которого используются для данного виджета. |

# 12 ЖУРНАЛЫ И ОТЧЕТЫ

## 12.1 Журналы

UserGate LogAn журналирует все события, которые происходят во время его работы и работы подключенных к нему серверов, и записывает их в следующие журналы:

- **Журнал событий** – события, связанные с изменением настроек сервера UserGate LogAn, авторизация пользователей, администраторов, обновлений различных списков и т.п.
- **Журнал веб-доступа** – подробный журнал всех веб-запросов, обработанных UserGate LogAn.
- **Журнал трафика** – подробный журнал срабатывания правил межсетевого экрана, NAT, DNAT, Port forwarding, Policy based routing. Для регистрации данных событий необходимо включить журналирование в необходимых правилах межсетевого экрана, NAT, DNAT, Port forwarding, Policy based routing.
- **Журнал СОВ** – события, регистрируемые системой обнаружения и предотвращения событий.
- **Журнал АСУ ТП** – события, регистрируемые правилами контроля систем АСУ ТП.
- **Журнал инспектирования SSH** – журнал срабатывания правил инспектирования SSH. Для регистрации данных событий необходимо включить журналирование.
- **История поиска** – поисковые запросы пользователей в популярных поисковых системах.
- **Журнал событий конечных устройств** – отображает события, получаемые от контроллируемых с помощью программного обеспечения UserGate Endpoint конечных устройств.
- **Журнал правил конечных устройств** – события срабатывания правил межсетевого экрана конечных устройств, в настройках которых включено логирование.
- **Приложения конечных устройств** – отображает приложения, которые когда-либо запускались на конечных устройствах.
- **Аппаратура конечных устройств** – содержит информацию об устройствах, подключённых к конечным устройствам.
- **Системный журнал** – отображены записи сообщений о событиях удалённых Unix-систем, полученные по протоколу Syslog.

### 12.1.1 Журнал событий

Журнал событий отображает события, связанные с изменением настроек сервера UserGate LogAn, например, добавление/удаление/изменение данных учетной записи, правила или любого другого элемента. Здесь же отображаются все события входа в веб-консоль, авторизации пользователей через Captive-портал и другие.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, компоненте, важности, типу события.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить отмеченными только те столбцы, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

### 12.1.2 Журнал веб-доступа

Журнал веб-доступа отображает все запросы пользователей в интернет по протоколам HTTP и HTTPS. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время события.
- Пользователь.
- Действия.
- Правило.
- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- IP назначения.
- Порт назначения.
- Категории.
- Протокол (HTTP).
- Метод (HTTP).
- Код ответа (HTTP).
- MIME (если присутствует).
- Байт передано/получено.
- Пакетов отправлено.
- Реферер (при наличии).
- Операционная система.
- Браузер.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить отмеченными только те столбцы, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

### 12.1.3 Журнал трафика

Журнал трафика отображает события срабатывания правил межсетевого экрана или правил NAT, в настройках которых включено логирование пакетов. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время события.
- Пользователь.
- Действие.
- Правило.
- Приложение.
- Протокол.
- Зона источника.
- Адрес источника.
- Порт источника.
- IP-назначения.

- Порт назначения.
- NAT IP-источника (если это правило NAT).
- NAT порт источника (если это правило NAT).
- NAT IP назначения (если это правило NAT).
- NAT порт назначения (если это правило NAT).
- Байт отправлено/получено.
- Пакетов.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить отмеченными только те столбцы, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

### 12.1.4 Журнал СОВ

Журнал системы обнаружения вторжений отображает сработавшие сигнатуры СОВ, для которых установлено действие журналировать или блокировать. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время.
- Действие.
- Сигнатура.
- Класс - класс сигнатуры.
- CVE - номер уязвимости по базе CVE.
- Bugtrack - номер уязвимости по базе Bugtrack.
- Nessus - номер уязвимости по базе Nessus.
- Протокол.
- IP источника.
- Порт источника.
- IP назначения.
- Порт назначения.
- Подробности срабатывания сигнатуры.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить отмеченными только те столбцы, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

### 12.1.5 Журнал АСУ ТП

Журнал АСУ ТП отображает сработавшие правила АСУ ТП, для которых включена функция записи в журнал правил. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время.
- Действие.
- Правило.
- Зона источника.
- IP источника.
- IP назначения.
- Порт назначения.
- Протокол.
- Команда АСУ ТП.
- Адрес регистра.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить отмеченными только те столбцы, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

### 12.1.6 Журнал испектирования SSH

Журнал инспектирования SSH отображает сработавшие правила инспектирования SSH, для которых включено журналирование. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время.
- Пользователь.
- Действие.
- Правило.
- Команда.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC-адрес источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить отмеченными только те столбцы, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

### 12.1.7 История поиска

В разделе **История поиска** отображаются все поисковые запросы пользователей, для которых настроено журналирование в политиках веб-безопасности. Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить отмеченными только те столбцы, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как пользователи, диапазон дат, поисковые системы и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

### 12.1.8 Журнал событий конечных устройств

Журнал событий конечных устройств отображает события, получаемые от контроллируемых с помощью программного обеспечения UserGate Endpoint конечных устройств. Программное обеспечение UserGate Endpoint собирает и передает на UserGate LogAnalyzer журналы операционной системы, журналы различного установленного программного обеспечения, антивирусного программного обеспечения и других приложений.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как конечное устройство, диапазон дат, компоненте, важности, типу события и другим.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить отмеченными только те столбцы, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

### 12.1.9 Журнал правил конечных устройств

Журнал правил конечных устройств отображает события срабатывания правил межсетевого экрана конечных устройств, в настройках которых включено логирование.

### 12.1.10 Приложения конечных устройств

Журнал приложения конечных устройств отображает приложения, которые когда-либо запускались на конечных устройствах. Для каждого приложения отображается дополнительная информация, какая как SHA-1 хеш сумма исполняемого файла, версия приложения, электронная подпись приложения и другие параметры.

### 12.1.11 Системный журнал

В системном журнале (syslog) отображены записи сообщений о событиях, происходящих в системе.

Для удобства формирования журнала записи могут быть отфильтрованы по различным критериям.

В UserGate LogAn также представлен режим расширенного поиска для формирования сложных фильтров поиска с использованием специального языка запросов, синтаксис которого рассмотрен далее в разделе Поиск и фильтрация данных.

После настройки фильтра его можно сохранить, нажав кнопку **Сохранить как**. После сохранения фильтр будет доступен во вкладке **Популярные фильтры**.

Администратор может сам выбрать столбцы, которые будут отражаться в журнале. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

В журнале представлена следующая информация:

- Название узла UserGate.
- Время.
- Критичность событий.
- Объект.
- Имя компьютера.
- Приложение, о котором была получена информация.
- Идентификатор процесса (PID).
- Данные события.

Нажатие кнопки **Показать** позволяет открыть окно с информацией о записи журнала приложений.

Запись журнала может быть добавлена к сведениям об инциденте нажатием кнопки **Добавить в инцидент**.

С помощью кнопки Экспортировать в CSV администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

### 12.1.12 Поиск и фильтрация данных

Количество записей, регистрируемых в журналах, как правило, очень велико, и UserGate LogAn предоставляет удобные способы поиска и фильтрации необходимой информации. Администратор может использовать простой и расширенный поиск по содержимому журналов.

При использовании простого поиска администратор использует графический интерфейс, чтобы задать фильтрацию по значениям требуемых полей журналов, отфильтровывая таким образом ненужную информацию. Например, администратор может задать интересующий его диапазон времени, список пользователей, категорий и т.п. Задание критериев поиска интуитивно понятно и не требует специальных знаний.

Построение более сложных фильтров возможно в режиме расширенного поиска с использованием специального языка запросов. В режиме расширенного поиска можно строить запросы с использованием полей журналов, которые недоступны в базовом режиме. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Значения полей могут быть введены с использованием одинарных или двойных кавычек, или без них, если значения не содержат пробелов. Для группировки нескольких условий можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

| Наименование | Описание |
|---|---|
| **AND или and** | Логическое И, требует выполнения всех условий, заданных в запросе. |

| | |
|---|---|
| **OR или or** | Логическое ИЛИ, достаточно выполнения одного из условий запроса. |

Операторы определяют условия фильтра и могут быть следующими:

| Наименование | Описание |
|---|---|
| **=** | Равно. Требует полного совпадения значения поля указанному значению, например, ip=172.16.31.1 будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1. |
| **!=** | Не равно. Значение указанного поля не должно совпадать с указанным значением, например, ip!=172.16.31 будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1. |
| **<=** | Меньше либо равно. Значение поля должно быть меньше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например,<br><br>date <= '2019-03-28T20:59:59' AND statusCode=303. |
| **>=** | Больше либо равно. Значение поля должно быть больше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например,<br><br>date >= "2019-03-13T21:00:00" AND statusCode=200. |
| **<** | Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например,<br><br>date < '2019-03-28T20:59:59' AND statusCode=404. |
| **>** | Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например,<br><br>(statusCode>200 AND statusCode <300) OR (statusCode=404). |
| **IN** | Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например, например,<br><br>category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category'). |
| **NOT IN** | Позволяет указать несколько значений поля в запросе; будут отображены записи, несодержащие указанные значения. Список значений необходимо указывать в круглых скобках, например,<br><br>category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category'). |
| **~** | Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например, |

| | |
|---|---|
| | browser ~ "Mozilla/5.0".<br><br>Данный оператор может быть применен только к полям, в которых хранятся строковые данные. |
| **!~** | Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например,<br><br>browser !~ "Mozilla/5.0".<br><br>Данный оператор может быть применен только к полям, в которых хранятся строковые данные. |
| **MATCH** | При использовании оператора MATCH подстрока, которая должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например,<br><br>details MATCH '\"module\":\"threats\"'.<br><br>Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax. |
| **NOT MATCH** | При использовании оператора NOT MATCH подстрока, которая не должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например,<br><br>details NOT MATCH '\"module\":\"threats\"'.<br><br>Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax. |

При составлении расширенного запроса UserGate LogAn показывает возможные варианты названия полей, применимых к ним операторов и возможных значений, облегчая оператору системы формирование сложных запросов. При переключении режима поиска с основного на расширенный UserGate LogAn автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме поиска.

### 12.1.13 Экспорт журналов

Функция экспортирования журналов UserGate LogAn позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate LogAn поддерживает выгрузку следующих журналов:

- Журнал DNS.
- Журнал событий.
- Журнал веб-доступа.
- Журнал СОВ.
- Журнал АСУ ТП.
- Журнал трафика.
- Журнал инспектирования SSH.
- Журнал событий конечных устройств.
- Журнал правил конечных устройств.
- Приложения конечных устройств.
- Аппаратура конечных устройств.

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию. Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо создать конфигурации экспорта журналов в разделе **Экспорт журналов**.

При создании конфигурации требуется указать следующие параметры:

| Наименование | Описание |
|---|---|
| **Название правила** | Название правила экспорта журналов. |
| **Описание** | Опциональное поле для описания правила. |
| **Журналы для экспорта** | Выбор файлов журналов, которые необходимо экспортировать:<br>• Журнал DNS.<br>• Журнал событий.<br>• Журнал веб-доступа.<br>• Журнал СОВ.<br>• Журнал АСУ ТП.<br>• Журнал трафика.<br>• Журнал инспектирования SSH.<br>• Журнал событий конечных устройств.<br>• Журнал правил конечных устройств.<br>• Приложения конечных устройств.<br>• Аппаратура конечных устройств.<br><br>Для каждого из журналов возможно указать синтаксис выгрузки:<br>• CEF – Common Event Format (ArcSight).<br>• JSON – JSON format.<br>• @CEE: JSON - CEE Log Syntax (CLS) Encoding JSON.<br><br>Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов. |
| **Тип сервера** | SSH (SFTP), FTP, Syslog. |
| **Адрес сервера** | IP-адрес или доменное имя сервера. |
| **Транспорт** | Только для типа серверов Syslog - TCP или UDP. |
| **Порт** | Порт сервера, на который следует отправлять данные. |
| **Протокол** | Только для типа серверов Syslog – RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM. |
| **Критичность** | Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: |

| | |
|---|---|
| | • **Тревога**: состояние, требующее незамедлительного вмешательства.<br>• **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе.<br>• **Ошибки**: в системе возникли ошибки.<br>• **Предупреждения**: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия.<br>• **Уведомительная**: события, которые относятся к необычному поведению системы, но не являются ошибками.<br>• **Информативная**: информационные сообщения. |
| **Facility** | Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения:<br>• **Сообщения пользовательские**.<br>• **Системный сервис**.<br>• **Безопасность/авторизация**.<br>• **Аудит**.<br>• **Тревога**.<br>• **Local 0**.<br>• **Local 1**.<br>• **Local 2**.<br>• **Local 3**.<br>• **Local 4**.<br>• **Local 5**.<br>• **Local 6**.<br>• **Local 7**. |
| **Имя хоста** | Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN). |
| **App-Name** | Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog. |
| **Логин** | Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog. |
| **Пароль** | Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog. |
| **Повторите пароль** | Подтверждение пароля учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog. |
| **Путь на сервере** | Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog. |
| **Расписание** | Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты:<br>• Ежедневно.<br>• Еженедельно.<br>• Ежемесячно.<br>• Каждые ... часов.<br>• Каждые ... минут. |

| | |
|---|---|
| | • Задать вручную.<br><br>При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом:<br>• Звездочка (*) - обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) - обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br>• Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа." |

## 12.2 Отчеты

С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

Раздел отчеты состоит из трех подразделов - шаблоны, правила и созданные отчеты. Что бы создать отчет необходимо выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создать правило создания отчета | Создать правило создания отчета, в котором указать необходимые параметры создания отчета. |
| **Шаг 2.** Запустить отчет | Запустить отчет в ручном режиме или дождаться времени, когда он запустится в автоматическом режиме по указанному в правиле расписанию. |
| **Шаг 3.** Получить отчет | Получить отчет по почте, если в правиле была настроена отправка отчета по почте, или скачать полученный отчет в разделе **Созданные отчеты.** |

**Примечание**

Процесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов.

### 12.2.1 Шаблоны

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией разработчиком UserGate.

Список возможных шаблонов отчетов, сгруппированных по категориям:

- События - группа шаблонов по событиям, регистрируемым в журнале событий.
- СОВ - группа шаблонов по событиям, регистрируемым в журнале СОВ.
- Сетевая активность - группа шаблонов по событиям, регистрируемым в журнале трафика.
- Трафик - группа шаблонов по событиям, регистрируемым в журнале трафика и относящимся к объему потребленного трафика пользователями, приложениями и т.п.
- Веб-активность - группа шаблонов по событиям, регистрируемым в журнале веб-доступа.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).

### 12.2.2 Пользовательские шаблоны

В отличии от обычных шаблонов, предоставляемых производителем решения, пользовательские шаблоны позволяют создать отчет по тем критериям, которые необходимо пользователю. Администратор может выбрать необходимые поля для отображения, задать условия и возможные группировки. Созданные пользовательские отчеты могут быть использованы в правилах построения отчетов наряду с обычными предопределенными отчетами. Для создания пользовательского шаблона необходимо в разделе **Отчеты--Пользовательские отчеты** нажать на кнопку **Добавить** и заполнить следующие параметры:

| Наименование | Описание |
|---|---|
| **Название** | Название пользовательского шаблона. |
| **Описание** | Опциональное поле для описания пользовательского шаблона. |
| **Категория** | Выбор источника данных для данного шаблона. Доступны значения:<br>• Журнал событий.<br>• Журнал веб-доступа.<br>• Журнал трафика.<br>• Журнал СОВ.<br>• Журнал инспектирования SSH.<br>• Срабатывания.<br>• Журнал событий конечных устройств.<br>• Журнал правил конечных устройств.<br>• Приложения конечных устройств. |
| **Запрос фильтра** | SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении отчета по данному шаблону. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. В качестве полей данных можно использовать столбцы, перечисленные ниже в поле **Столбцы.** Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных. |
| **Сортировать по** | Укажите поле данных, по которому будут отсортированы данные в отчете. Сортировку можно указать по возрастанию и по убыванию. |
| **Группировать по** | Укажите поле данных, по которому будут сгруппированы данные в отчете. |

| | |
|---|---|
| **Столбцы** | Список столбцов, доступных для конкретного источника данных. |
| **Выбранные** | Список столбцов, выбранных для отображения в отчете. |

### 12.2.3 Правила отчетов

Правило отчета задает параметры создаваемого отчета, а также расписание запуска отчетов и способы доставки отчета пользователям. При создании правила отчета администратор указывает следующие параметры:

| Наименование | Описание |
|---|---|
| **Вкл** | Включение/отключения отчета. |
| **Название** | Название правила. |
| **Описание** | Опциональное поле для описания правила. |
| **Язык отчета** | Выбор языка, который будет использован в отчете. |
| **Диапазон** | Диапазон времени, за который необходимо подготовить отчет. |
| **Формат отчета** | Формат отчета (PDF, HTML, XML, CSV), в котором будет создаваться данный отчет.<br><br>В ажно! Создание отчета в формате PDF создает высокую нагрузку на процессор и память. Чем объемнее отчет, тем более высокая нагрузка. Не используйте формат отчета PDF для пользовательских шаблонов. Для шаблонов **Подробный список всех посещенных URL** и **Подробный список всех посещенных сайтов** автоматически используется формат CSV, независимо от выбранного формата. |
| **Количество записей** | Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству топ записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль. |
| **Количество в группировке (если применимо)** | Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству сгруппированных записей, например, топ 10 пользователей по категориям - для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчетов, которые содержат группирование. |
| **Пользователи** | Задает пользователей или группы пользователей, для которых будет создаваться отчет. Если оставить поле пустым, то отчет будет создаваться для всех пользователей. |
| **Шаблоны** | Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон. |
| **Расписание** | Выбор расписания для создания отчетов. Возможны варианты:<br>• Ежедневно. |

| | |
|---|---|
| | • Еженедельно.<br>• Ежемесячно.<br>• Каждые ... часов.<br>• Каждые ... минут.<br>• Задать вручную.<br><br>При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом:<br><br>• Звездочка (*) - обозначает весь диапазон (от первого до последнего).<br>• Дефис (-) - обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7.<br>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".<br><br>Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа. |
| **Доставка** | Возможность задать опциональную отправку созданного отчета получателям по протоколу SMTP. Необходимо задать:<br><br>• Профиль SMTP, который будет использован для отправки отчетов. Подробно о настройке профилей SMTP смотрите в главе **Оповещения.**<br>• От - имя отправителя письма.<br>• Тема письма - тема письма (subject).<br>• Тело письма - содержимое письма.<br>• Получатели - список получателей письма. Получатели должны быть добавлены в списки библиотеки **Почтовые адреса.** |

### Примечание

Процесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов. Особенно важно учитывать загрузку ресурсов при запуске отчетов за большой диапазон времени.

### Примечание

Для того, чтобы запустить правило отчета не обязательно включать его и указывать время запуска правила. В ручном режиме можно запустить любой, в том числе отключенный отчет, для этого в списке правил необходимо выбрать требуемое правило и нажать накнопкуЗапустить сейчас. Готовый отчет после создания будет доступен в разделе Созданные отчеты.

### 12.2.4 Созданные отчеты

В разделе **Созданные отчеты** хранятся все полученные отчеты. Отчеты создаются в формате pdf или csv. Для каждого отчета указывается название отчета, которое совпадает с названием правила отчета, которое было использовано для создания данного отчета, время создания отчета и размер отчета.

Для скачивания отчета необходимо использовать кнопку **Скачать**, для удаления - **Удалить**.

Время хранения готовых отчетов (ротация) настраивается по нажатию на кнопку **Настроить**. Значение по умолчанию - 60 дней.

# 13 АНАЛИТИКА

Раздел **Аналитика** UserGate Log Analyzer предоставляет функционал SIEM – системы управления информацией о безопасности и событиями информационной безопасности. UserGate Log Analyzer предоставляет возможность проведения анализа журналов событий безопасности, получаемых с настроенных сенсоров, таких как МЭ UserGate, конечные устройства UserGate Client, сторонние сетевые устройства, поддерживающие передачу данных по протоколу SNMP, сенсоры WMI. Все данные хранятся в одной базе данных, что даёт возможность осуществлять сложный поиск, корреляцию повторяющихся событий, их агрегацию, создавая инциденты безопасности, и упростить процесс изучения особенностей инцидентов.

Первоначальной единицей информации, которая поступает в UserGate Log Analyzer, является событие. **Событие** - это одна запись в журнале, например, единичное срабатывание правила СОВ на МЭ UserGate, блокировка доступа к запрещенному ресурсу (срабатывание блокирующего правила контентной фильтрации), успешная или неуспешная попытка доступа в консоль управления и другие подобные события, которые регистрируются на устройствах, подключенных к UserGate Log Analyzer. Отдельное событие может не нести достаточно информации об угрозе ИБ, но несколько однотипных событий (например, неуспешных попыток доступа в консоль управления) или разных событий, зарегистрированных в определенной последовательности и поступивших из разных источников, могут представлять ценность в идентификации угрозы. Этот процесс называется корреляция событий. Группа событий, объединенная правилом аналитики (корреляции), представляет собой **Срабатывание**. Инженер безопасности проводит анализ срабатывания, изучает входящие в срабатывание события и при необходимости может создавать **Инцидент** компьютерной безопасности на основе одного или нескольких срабатываний.

С помощью правил аналитики инженер безопасности может автоматизировать процесс корреляции событий и создание срабатываний, а также назначить определенные **Действия реагирования** (реакцию) системы на создаваемые срабатывания. Все это позволяет облегчить процесс изучения регистрируемых событий и сократить время между обнаружением проблемы и ее решением.

Настройка данной функции доступна во вкладке **Аналитика**, где можно настроить правила аналитики, создать действия реагирования, просмотреть журнал срабатывания правил и подробности срабатывания.

Данные функции будут рассмотрены далее в соответствующих разделах: **Ошибка! Недопустимый объект гиперссылки.**, Действия реагирования, Срабатывания и Подробности срабатывания. Правила аналитики

Во вкладке **Правила аналитики** можно создавать правила обработки событий журналов. Настройка правил аналитики позволяет производить сложный поиск среди событий информационной безопасности. Срабатывание правила происходит при выявлении корреляции событий с разных источников. Правила могут работать в двух режимах: исторический режим (анализ событий за выбранный период) и режим реального времени.

Правила создаются нажатием кнопки **Добавить**. Далее во вкладке **Общие** необходимо указать свойства правила.

| Наименование | Описание |
|---|---|
| **Включено** | Включает/отключает правило аналитики для работы в режиме реального времени. |
| **Название** | Отображает название правила аналитики. |

| | |
|---|---|
| **Описание** | Описывает правила аналитики. Данное поле необязательно для заполнения. |
| **Уровень угрозы** | Показывает уровень угрозы, который будет отображаться при срабатывании правила.<br><br>Для выбора доступны следующие уровни:<br>• **Очень низкий**: события, сформировавшие срабатывание правила аналитики, представляют очень низкий уровень угрозы, и администратор может не предпринимать никаких действий.<br>• **Низкий**: события, сформировавшие срабатывание правила аналитики, представляют низкий уровень угрозы, и администратор может не предпринимать никаких действий.<br>• **Средний**: необходимо обратить внимание на события, попавшие под срабатывание правила аналитики.<br>• **Высокий**: события, требующие исследования и принятия мер.<br>• **Очень высокий**: события, требующие исследования и срочного принятия мер. |
| **Приоритет** | Показывает приоритет, установленный для срабатывания правила аналитики:<br>• **Низкий**: срабатывания данных правил обладают низким приоритетом реагирования.<br>• **Нормальный**: на срабатывания данных правил необходимо обратить внимание и, возможно, предпринять меры.<br>• **Важный**: на срабатывания данных правил необходимо обратить внимание и предпринять меры.<br>• **Критический**: срабатывания данных правил требуют незамедлительного реагирования.<br><br>При срабатывании правила установленный приоритет будет указывать на важность срабатывания правила аналитики. |
| **Категория** | Отображает категорию, к которой относится срабатывание.<br><br>По умолчанию для выбора доступны следующие категории:<br>• **Security**: правила данной категории определяют инциденты, приводящие к ухудшению безопасности информационных систем.<br>• **Availability**: правила данной категории определяют инциденты, которые приводят к ухудшению доступности информационных систем.<br>• **Performance**: правила данной категории определяют инциденты, которые приводят к ухудшению производительности информационных систем.<br><br>Дополнительные категории срабатываний могут быть созданы в разделе во вкладке **Настройки --> Библиотеки --> Категории срабатываний**. |
| **Часовой пояс** | Указывает на часовой пояс, по времени которого будут работать правила аналитики, т.к. сервер может собирать данные с источников, находящихся в различных часовых поясах. |

Во вкладке **Условия** необходимо указать условие/условия срабатывания правила. Если условий несколько, то они связаны между собой логическим «И» и выполняются сверху вниз. Т.е. правило сработает только в том случае, если будут выполнены все условия. Условие можно создать нажатием кнопки **Создать**. Далее необходимо указать следующие параметры.

| Наименование | Описание |
|---|---|

| | |
|---|---|
| **Название** | Отображает название условия правила аналитики. |
| **Описание** | Описывает условие правила аналитики. Данное поле необязательно для заполнения. |
| **Ограничить время выполнения условия** | Включить/отключить ограничение времени выполнения условия.<br><br>При включении ограничения времени правило аналитики сработает, только в том случае, когда за указанный отрезок времени условие выполнится заданное количество раз. |
| **Время выполнения условия** | Указывает на отрезок времени, за который условие должно выполнится заданное количество раз, чтобы произошло срабатывание правила аналитики. Время указывается в секундах.<br><br>Указание времени выполнения условия доступно при включённом чекбоксе **Ограничить время выполнения условия**. |
| **Запрос фильтра** | Отображает SQL-подобный поисковый запрос условия, который пишется по базе журналов. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы.<br><br>Синтаксис написания запроса можно просмотреть в разделе Поиск и фильтрация данных.<br><br>Запрос также может быть написан с использованием синтаксиса Google/RE2 в операторе MATCH.<br><br>**Например**. Поисковый запрос:<br><br>source = 'wmi log' and logFile = 'Microsoft-Windows-Sysmon/Operational' and logEventId = 1 and data MATCH 'ParentCommandLine:(.*)cmd.exe' and data ~ 'CertReq -Post -config'.<br><br>Данный запрос производит поиск в журнале событий конечных устройств, который берёт данные из журнала Microsoft-Windows-Sysmon/Operational. При нахождении события, которое соответствует созданию нового процесса, запускается поиск родительского процесса (т.е. процесса, который вызвал создание нового процесса) и поиск вызова команды certreq с параметрами. Часть запроса с оператором MATCH позволяет определить, что certreq запустили из cmd (командной строки). Таким образом определяется то, что у текущего процесса родительским был cmd.exe.<br><br>Подробнее о синтаксисе Google/RE2 в операторе MATCH: https://github.com/google/re2/wiki/Syntax. |
| **Группировать по** | Отображает список параметров, по которым могут быть сгруппированы правила в результате срабатывания. Поля будут отображены при просмотре карточки срабатывания.<br><br>О параметрах, по которым возможна группировка, читайте в разделе .<br><br>При указании категорий для группировки правило аналитики сработает только в том случае, если условие выполнится именно для выбранной категории заданное количество раз, указанное в поле параметра **Повторений шаблона**. |
| **Повторений шаблона** | Показывает количество выполнений условия, необходимое для срабатывания правила. Данный параметр может быть использован вместе с параметром **Ограничить время выполнения условия** или без него. |
| **Запустить сейчас** | Производит запуск анализа событий за определённый период времени (работа в историческом |

| | |
|---|---|
| | режиме).<br><br>Далее необходимо задать временной диапазон. Если чекбокс **Указать диапазон времени** не активен, то анализ по созданному правилу аналитики проводится по всей базе событий за всё время. После завершения анализа, нажав кнопку **Показать срабатывания** в окне **Запуск правила аналитики**, можно перейти в журнал срабатываний и просмотреть информацию о срабатывании этого правила.<br><br>Также правило можно запустить без записи в журнал срабатывания, т.е. для проверки работоспособности правила или просмотра количества срабатываний. Для этого необходимо включить чекбокс **Тестовый запуск**. |

Во вкладке **Действия реагирования** могут быть добавлены действия, которые будут выполнены автоматически при срабатывании правила аналитики. Действия реагирования могут быть созданы нажатием кнопки **Создать и добавить новый объект** или добавлены из списка существующих действий. Подробнее о действиях реагирования и их настройке читайте в разделе Действия реагирования.

Чтобы запустить правило в режиме реального времени необходимо нажать кнопку **Включить**. Кнопка **Отключить** завершает выполнение выбранного правила аналитики.

Созданные правила можно редактировать, удалять и копировать. Кнопка **Показать срабатывания** отобразит журнал с краткой информацией о всех срабатываниях выбранного правила. Также можно настроить отображение списка правил: отображать все правила, только включённые/выключенные правила.

При настройке условий правил аналитики возможно производить группировку событий по параметрам, представленным в записях журналов LogAn, NGFW и конечных устройств. Список параметров, по которым возможна группировка событий, смотрите в таблице раздела Поиск.

## 13.1 Пример настройки правила аналитики

В качестве примера рассмотрим настройку правила аналитики, направленную на поиск попыток брутфорса.

Брутфорс (Brute force) – метод взлома учётных записей путём подбора паролей к ним. Суть подхода заключается в последовательном автоматизированном переборе всех возможных комбинаций символов с целью определения правильной.

После задания общих настроек, таких как название правила, описание, уровень угрозы, приоритет, категория срабатывания и часовой пояс, были заданы несколько условий.

- **source = 'endpoint events log' AND logEventId = 4625 AND data MATCH 'Failure Reason:(\s*)Unknown user name or bad password.'**

  В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4625. Данный идентификатор события соответствует неудачной попытке авторизации учётной записи. Часть условия с оператором MATCH позволяет определить причину отказа в авторизации: неправильный логин или пароль.

Подробнее о событии 4625 читайте в соответствующей документации: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4625.

- **source = 'endpoint events log' AND logEventId = 4672**

В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4672. Данный идентификатор события соответствует успешной авторизации с назначением специальных привилегий текущему сеансу.

Подробнее о событии 4672 читайте в соответствующей документации: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4672.

- **source ='endpoint events log' AND logEventId = 4624**

В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4624. Данный идентификатор события соответствует успешному входу пользователя в систему.

Подробнее о событии 4624 читайте в соответствующей документации: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4624.

## 13.2 Поиск

Во вкладке **Поиск** отражён список всех событий журналов подключённых сенсоров и событий журналов Log Analyzer. С использованием строки поиска можно производить поиск нужных событий. Строка поиска использует SQL-подобный поисковый запрос. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы. Синтаксис написания запроса можно просмотреть в разделе Поиск и фильтрация данных. Запрос также может быть написан с использованием синтаксиса Google/RE2 в операторе MATCH.

С использованием кнопки **Добавить правило**, можно добавить новое правило аналитики, в котором в качестве запроса фильтра будет указан введённый поисковый запрос. Подробнее о правилах аналитики смотрите в разделе **Ошибка! Недопустимый объект гиперссылки.**.

Также, нажатием кнопки **Добавить условие**, по введённому поисковому запросу можно сформировать условие и добавить его в созданное ранее правило аналитики. При добавлении необходимо указать правило аналитики и имя условия.

Выбранное событие можно добавить в инцидент нажатием кнопки **Добавить в инцидент**. Подробнее об инцидентах читайте в главе Настройки инцидентов.

Существует 2 режима представления данных о событиях: табличный вид и текстовый вид. Для перехода в выбранный режим используются кнопки **Переключить в текстовый вид** или **Переключить в табличный вид**.

Во вкладке **Поиск** можно увидеть следующую информацию о событиях.

| Наименование в базе данных | Наименование в поисковом запросе | Описание |
|---|---|---|
| **Узел** | node | Показано имя узла устройства NGFW или LogAn. |
| **Время** | date | Указано время события или срабатывания правила аналитики. Отображается в часовом поясе, настроенном на UserGate LogAn. |
| **Время первого события** | triggeredAlertFirstEventDate | Для журнала срабатываний: отображено время первого события, попавшего под срабатывание правила аналитики. |

| | | |
|---|---|---|
| **Время последнего события** | triggeredAlertLastEventDate | Для журнала срабатываний: отображено время последнего события, попавшего под срабатывание правила аналитики. |
| **Источник** | source | Показан журнал, в который записано событие: журналы LogAn, NGFW, конечных устройств, срабатываний. |
| **Важность** | severity | Отражена категория события журналов событий NGFW, LogAn:<br>• **Информационные**: как правило, не требуют внимания администратора.<br>• **Предупреждение**: предупреждают о возможных проблемах.<br>• **Ошибка**: сообщают об ошибках.<br>• **Критические**: сообщают о серьёзных ошибках, которые могут повлиять на функциональность. |
| **Компонент** | component | Отражён компонент, в котором произошло событие (например: обновления, настройки, консольная авторизация, аналитика и т.п.). Относится к записям журнала событий NGFW и LogAn. |
| **Тип события** | event | Отображён тип события из журнала событий NGFW, LogAn (например: проверка, скачивание, установка обновлений, успешная/неуспешная авторизация, поиск параметров и т.п.). |
| **Пользователь** | user | Показано имя пользователя, с учётной записи которого был совершён вход в систему NGFW, LogAn, конечного устройства. Относится к записям журналов событий NGFW, LogAn и конечных устройств, веб доступа, трафика, СОВ, срабатываний. |
| **Модуль** | module | Указан модуль, в котором произошло событие (например: Web console, Core, VPN сервер и т.п.). Относится к записям журнала событий NGFW, LogAn. |
| **Учёт изменений** | changeTracker | Указан тип изменений (журнал событий LogAn, NGFW). Возможные типы изменений пользователь может задать самостоятельно. |
| **Данные** | data | Представлена подробная информация о событии. Относится к записям журналов событий конечных устройств и syslog. |
| **Информация** | details | Представлена подробная информация о событии из журнала событий Log Analyzer и NGFW. |
| **Правило** | rule | Отображено название правила аналитики, межсетевого экрана, контентной фильтрации, АСУ ТП или СОВ. |
| **Действие** | action | Отображено действие, настроенное в правилах межсетевого экрана, контентной фильтрации, АСУ ТП или СОВ:<br>• **Разрешить** (allow/pass/allow_webaccess): действие, настроенное в правилах межсетевого экрана, СОВ |

| | | |
|---|---|---|
| | | или контентной фильтрации.<br>• **Безопасный поиск** ('safe browsing').<br>• **Captive-портал** ('captive portal').<br>• **Предупредить** (warning): действие, настроенное в правилах контентной фильтрации.<br>• **Уведомление** (alert): относится к DoS защите на зоне.<br>• **NAT** (nat).<br>• **DNAT** (dnat).<br>• **Порт-форвардинг** ('port forwarding').<br>• **Policy-based routing** ('policy based routing').<br>• **Network mapping** ('network mapping').<br>• **Запретить** (deny/drop/deny_webaccess): действие, настроенное в правилах межсетевого экрана, СОВ или контентной фильтрации.<br>• **Расшифровать** (decrypt): действие, настроенное в правилах инспектирования.<br>• **Журналировать** (log): действие, настроенное в правилах СОВ.<br>• **Пропускать** (pass): действие, настроенное в правилах АСУ ТП.<br>• **Блокировать** (drop): действие, настроенное в правилах АСУ ТП. |
| **Приложение** | application | Название приложения. Относится к записям журнала трафика, СОВ, syslog, журналов правил и приложений конечных устройств. |
| **Сетевой протокол** | networkProtocol | Показан транспортный протокол подключения, использующийся для доступа к ресурсу. Относится к записям журналов трафика, СОВ, журнала правил конечных устройств. |
| **HTTP протокол** | httpProtocol | Указана версия HTTP протокола. Относится к записям журнала веб-доступа. |
| **Категории сайтов** | urlCategory | Отображены категории, к которым относится сайт. Относится к записям журнала веб-доступа и журнала правил конечных устройств. |
| **Причины** | | Отображены причины из журнала веб-доступа (например: причина блокировки). |
| **Метод** | method | Отображен метод HTTP (основная операция над ресурсом).<br>• **OPTIONS**: используется для определения возможностей веб-сервера или параметров соединения для конкретного ресурса.<br>• **GET**: используется для запроса содержимого указанного ресурса.<br>• **HEAD**: аналогичен методу GET, за исключением того, что в ответе сервера отсутствует тело.<br>• **POST**: применяется для передачи пользовательских данных заданному ресурсу. |

| | | |
|---|---|---|
| | | • **PUT**: используется для загрузки содержимого запроса на указанный в запросе URI.<br>• **PATCH**: аналогично PUT, но применяется только к фрагменту ресурса.<br>• **DELETE**: удаляет указанный ресурс.<br>• **TRACE**: возвращает полученный запрос так, что клиент может увидеть, какую информацию промежуточные серверы добавляют или изменяют в запросе.<br>• **CONNECT**: преобразует соединение запроса в прозрачный TCP/IP-туннель.<br><br>Относится к записям журнала веб-доступа. |
| **Код ответа HTTP** | statusCode | Отображён код состояния, являющийся частью первой строки ответа от сервера при запросах по протоколу HTTP. Относится к записям журнала веб-доступа. |
| **Тип контента** | mime | Показан тип контента. Является записью журнала веб-доступа и журнала правил конечных устройств. |
| **URL** | url | URL-адрес ресурса, к которому было выполнено обращение. Относится к записям журнала веб-доступа. |
| **Реферер** | referer | Отображён URL-адрес предыдущей страницы (если есть). Относится к записям журнала веб-доступа. |
| **Операционная система** | operatingSystem | Отображён тип операционной системы устройства пользователя. Относится к записям журнала веб-доступа и СОВ. |
| **User-agent** | userAgent | Useragent пользовательского браузера. Относится к записям журнала веб-доступа. |
| **Сигнатуры** | signature | Отображено имя сработавшей сигнатуры системы обнаружения вторжений (СОВ). Является параметром журнала СОВ. |
| **Зона источника** | zoneSource | Указана зона источника. Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ. |
| **IP источника** | ipSource | Показан IP-адрес источника трафика. Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ, журнала правил конечных устройств. |
| **Порт источника** | portSource | Отображён номер порта источника, через который осуществляется подключение. Относится к записям журналов веб-доступа, трафика, СОВ, журнала правил конечных устройств. |
| **MAC источника** | macSource | MAC-адрес источника. Относится к записям журналов трафика |

| | | |
|---|---|---|
| | | и СОВ. |
| **Зона назначения** | zoneDest | Отображена зона назначения. Относится к записям журналов веб-доступа, трафика, СОВ, журнала правил конечных устройств. |
| **IP назначения** | ipDest | Показан IP-адрес назначения трафика. Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ, журнала правил конечных устройств. |
| **Порт назначения** | portDest | Указан номер порта назначения, используемый транспортным протоколом. Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ, журнала правил конечных устройств. |
| **MAC назначения** | macDest | MAC-адрес назначения. Относится к записям журналов трафика и СОВ. |
| **NAT адрес источника** | natIpSource | Отображён NAT IP-адрес источника (если настроены правила NAT). Относится к записям журнала трафика. |
| **NAT порт источника** | natPortSource | Отображён NAT порт источника (если настроены правила NAT). Относится к записям журнала трафика. |
| **NAT адрес назначения** | natIpDest | Отображён NAT IP-адрес назначения (если настроены правила NAT). Относится к записям журнала трафика. |
| **NAT порт назначения** | natPortDest | Отображён NAT порт назначения (если настроены правила NAT). Относится к записям журнала трафика. |
| **Байт отправлено/получено** | bytesSent/bytesRecv | Отображён отправленный/полученный объём информации. Относится к записям журналов трафика и веб-доступа. |
| **Пакетов отправлено/получено** | packetSent/packetRecv | Показано количество отправленных/полученных пакетов. Относится к записям журналов трафика и веб-доступа. |
| **Конечное устройство/сенсор** | sensor | Отображено имя конечного устройства/сенсора. Относится к записям журнала событий конечных устройств. |
| **Счётчик** | counter | Название счётчика, добавленного в WMI и SNMP сенсор. Относится к записям журнала событий конечных устройств. |
| **Объект SNMP** | snmpObject | Указан идентификатор SNMP объекта (SNMP OID). Относится к записям журнала событий конечных устройств. |
| **Тип SNMP объекта** | snmpObjectType | Указан тип SNMP объекта. Относится к записям журнала событий конечных устройств. |
| **Статус** | status | Отображён результат выполнения WMI или SNMP запроса (OK или Error). Относится к записям журнала событий конечных устройств. |

| | | |
|---|---|---|
| **Ошибка** | error | Показана ошибка WMI или SNMP, возникшая в результате выполнения запроса. Относится к записям журнала событий конечных устройств. |
| **Протокол АСУТП** | scadaProtocol | Указан протокол SCADA (Supervisory Control And Data Acquisition – диспетчерское управление и сбор данных).<br>• **IEC 104** (ГОСТ Р МЭК 60870-5-104).<br>• **Modbus**.<br>• **DNP3** (Distributed Network Protocol).<br>• **MMS** (Manufacturing Message Specification).<br>• **OPC UA** (Open Platform Communications Unified Architecture).<br><br>Относится к записям журнала АСУ ТП. |
| **Уровень лога** | logLevel | Указан тип события:<br>• **Audit Success** (успешный аудит): событие журнала безопасности, которое происходит при успешном обращении к аудируемым ресурсам.<br>• **Audit Failure** (неуспешный аудит): событие журнала безопасности, которое происходит при неуспешном обращении к аудируемым ресурсам.<br>• **Error** (ошибка): событие указывает на существенные проблемы, которые могут стать причиной потери функциональности или данных.<br>• **Information** (сведения): информационные события, которые, как правило, не требуют внимания администратора.<br>• **Warning** (предупреждение): события указывают на проблемы, которые не требуют немедленного исправления, однако могут привести к ошибкам в будущем.<br><br>Относится к записям журнала событий конечных устройств. |
| **Источник журнала событий** | logEventSource | Название программного обеспечения, которое сформировало запись события в журнал. Относится к записям журнала событий конечных устройств. |
| **Категория лога** | logCategory | Категория лога, необходимая для упорядочивания событий. Данные берутся из Windows EventLog. Каждый источник может определять свои идентификаторы категорий. Относится к записям журнала событий конечных устройств. |
| **Категория задачи** | taskCategory | Показана категория задачи. Является записью журнала событий конечных устройств. |
| **Имя компьютера** | computerName | Представлено полное имя конечного устройства. Относится к записям журналов событий конечных устройств, syslog. |

| | | |
|---|---|---|
| **Код события лога** | logEventCode | Отображён код события лога, соответствующий определённому событию. Является записью журнала событий конечных устройств. |
| **Идентификатор события лога** | logEventId | Показан идентификатор события лога, который определяет первичный идентификатор события. Относится к записям журнала событий конечных устройств. |
| **Тип события лога** | logEventType | Отображён тип события лога. Он представлен параметрами, каждый из которых соответствует уровню лога:<br>• 1 - уровень лога: error.<br>• 2 - уровень лога: warning.<br>• 3 - уровень лога: information.<br>• 4 - уровень лога: audit success.<br>• 5 - уровень лога: audit failure.<br><br>Относится к записям журнала событий конечных устройств. |
| **Строка вставки** | insertionString | Отображены данные блока EventData события Windows. Относится к записям журнала событий конечных устройств. |
| **Файл журнала лога** | logFile | Показана информация из журнала событий конечных устройств, т.е. информация о важных программных и аппаратных событиях. Типы журналов:<br>• **Application** (файл журнала приложений): для событий приложений и служб.<br>• **Security** (файл журнала безопасности): для событий системы аудита.<br>• **System** (файл системного журнала): для событий драйверов устройств.<br>• **CustomLog**: журнал содержит события, регистрируемые приложениями, которые создают пользовательский журнал. Использование пользовательского журнала позволяет приложению управлять размером журнала или присоединять списки управления доступом в целях безопасности, не затрагивая другие приложения.<br><br>Относится к записям журнала событий конечных устройств. |
| **Команда** | scadaCommand | Отображена команда управления АСУ ТП (например: чтение или запись). Относится к записям журнала АСУ ТП. |
| **Адрес регистра** | scadaAddress | Адрес регистра, с которым необходимо провести операцию (запись или чтение). Относится к записям журнала АСУ ТП. |
| **Номер ASDU** | scadaAsdu | Показан адрес ASDU (COA – Common Object Address). Параметр относится к протоколу IEC-104. Относится к записям журнала АСУ ТП. |

| | | |
|---|---|---|
| **Идентификатор устройства** | scadaDevice | Указан уникальный номер устройства, содержащийся в базе данных OPC-сервера. Параметр относится к протоколу OPC UA. Относится к записям журнала АСУ ТП. |
| **Имя переменной** | scadaVarname | Отображено имя переменной. Параметр, в основном, используется для обмена данными в режиме реального времени. Параметр относится к протоколу MMS. Относится к записям журнала АСУ ТП. |
| **Хэш** | hash | Показан хэш приложения. Является параметром журнала приложений конечных устройств. |
| **Объект** | facility | Категория события. Относится к записям журнала syslog. Возможны следующие значения:<br>• Сообщения ядра.<br>• Сообщения пользовательские.<br>• Почтовая система.<br>• Системный сервис.<br>• Безопасность/авторизация.<br>• Сообщения syslog.<br>• Система печати LPR.<br>• Система сетевых новостей.<br>• Подсистема UUCP.<br>• Сервис времени.<br>• Безопасность/аутентификация.<br>• FTP сервис.<br>• Система NTP.<br>• Аудит.<br>• Тревога.<br>• Сервис времени 2.<br>• Local 0 - Local7. |
| **Критичность** | syslogSeverity | Указана критичность событий журнала syslog.<br>• **Экстренная**: критическое состояние, которое сказывается на работоспособности системы.<br>• **Тревога**: состояние, требующее незамедлительного вмешательства.<br>• **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе.<br>• **Ошибки**: несрочные сбои в системе.<br>• **Предупреждения**: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия.<br>• **Уведомительная**: события, которые относятся к необычному поведению системы, но не являются ошибками.<br>• **Информативная**: информационные уведомления.<br>• **Отладочная**: информация, полезная разработчикам для отладки приложений. |

| | | |
|---|---|---|
| **Идентификатор процесса** | processId | Указан идентификатор процесса. Относится к записям журнала syslog. |

Администратор может выбрать для показа только те столбцы, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

## 13.3 Действия реагирования

Действия реагирования позволяют определить методы реагирования при срабатывании правил аналитики информационной безопасности. Действия могут быть созданы во вкладке **Аналитика --> Действия реагирования**. При добавлении действия необходимо указать следующие параметры.

| Наименование | Описание |
|---|---|
| **Включено** | Включает/отключает правило реагирования. |
| **Название** | Отображает название правила реагирования. |
| **Описание** | Описывает правила реагирования. Данное поле необязательно для заполнения. |
| **Действие** | Показывает действие, выбранное для исполнения в случае срабатывания правила аналитики. Действие реагирования выполнится, если оно указано в свойствах правила аналитики.<br><br>Для выбора доступны следующие виды реагирования:<br>• **Отправить email**: отправка письма на выбранные почтовые адреса. Настройка действия **Отправить email** будет рассмотрена далее в разделе Действие типа отправить email.<br>• **Отправить сообщение**: отправка сообщения на указанные номера телефонов. Настройка действия **Отправить сообщение** будет рассмотрена далее в разделе Действие типа отправить сообщение.<br>• **Webhook**: получение уведомления о срабатывании правила на веб-странице, адрес которой был указан при настройке действия. Настройка действия **Webhook** будет рассмотрена далее в разделе Действие типа webhook.<br>• **Создать инцидент**: автоматическое создание инцидента в результате срабатывания правил аналитики. О настройке действия **Создать инцидент** читайте в разделе Настройки инцидентов. |
| **Записывать в журнал правил** | Включает/отключает журналирование данных о срабатывании действия реагирования. Данные записываются в журнал событий Log Analyzer, который можно просмотреть во вкладке **Журналы и отчёты --> Журналы Log Analyzer --> Журнал событий**. |
| **Группировать похожие срабатывания** | Для удобства при настройке действий реагирования возможно использование функции группировки срабатываний.<br><br>Группировка возможна по следующим параметрам:<br>• **Никогда**. |

| | |
|---|---|
| | • **За период времени**. При настройке группировки срабатываний правила аналитики за период времени действие реагирования выполнится, если в течении указанного времени произошло хотя бы одно срабатывание.<br>• **По количеству срабатываний**. При настройке группировки по количеству срабатываний правила аналитики действие реагирования выполнится только после указанного количества срабатываний. |
| **Период группировки** | Отображает период группировки в минутах. Задание параметра возможно только при выборе группировки похожих срабатываний за период времени. |
| **Количество срабатываний** | Отображает заданное количество срабатываний. Задание параметра возможно только при выборе группировки похожих срабатываний по количеству срабатываний. |

Созданные действия реагирования можно редактировать, удалять, копировать, включать, отключать. Также в списке действий реагирования можно отображать все действия, только включённые или только выключенные.

### 13.3.1 Действие типа отправить email

Если в качестве действия реагирования была выбрана отправка email, то в свойствах правила реагирования необходимо указать следующие параметры.

| Наименование | Описание |
|---|---|
| **Профиль оповещения** | Профиль оповещения SMTP, который будет использован для отправки email.<br>Подробнее о настройке профилей SMTP читайте в главе Профили оповещений. |
| **От** | Имя отправителя письма. |
| **Тема** | Тема письма. |
| **Почтовые адреса** | Список почтовых адресов получателей. Получатели должны быть добавлены в списки в разделе **Настройки --> Библиотеки --> Почтовые адреса**. О добавлении почтовых адресов читайте в разделе Почтовые адреса. |
| **Шаблон** | Шаблон письма уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию.<br>Подробнее читайте в разделе Шаблон уведомлений. |

### 13.3.2 Действие типа отправить сообщение

Если в качестве действия реагирования была выбрана отправка сообщения, то в свойствах правила реагирования необходимо указать следующие параметры.

| Наименование | Описание |
|---|---|

| | |
|---|---|
| **Профиль оповещения** | Профиль оповещения SMPP, который будет использован для отправки сообщения.<br><br>Подробнее о настройке профилей SMPP читайте в главе Профили оповещений. |
| **От** | Имя отправителя письма. |
| **Номера телефонов** | Список номеров телефонов получателей. Получатели должны быть добавлены в списки в разделе **Настройки --> Библиотеки --> Номера телефонов**. О добавлении телефонных номеров читайте в разделе Номера телефонов. |
| **Шаблон** | Шаблон сообщения с возможностью передачи значений различных переменных, относящихся к срабатыванию.<br><br>Подробнее читайте в разделе Шаблон уведомлений. |

### 13.3.3 Действие типа webhook

Для настройки webhook в свойствах правила реагирования необходимо указать следующие параметры.

| Наименование | Описание |
|---|---|
| **URL** | Адрес веб-сайта, на котором будут отображаться оповещения о срабатывании правила. |
| **Шаблон** | Шаблон уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию.<br><br>Подробнее читайте в разделе Шаблон уведомлений. |

Для тестирования webhook можно воспользоваться сервисом https://webhook.site. Для этого необходимо перейти на сайт Webhook.site и скопировать сгенерированную ссылку. Далее её необходимо указать в свойствах правила реагирования в поле **URL** во вкладке **Действия**.

### 13.3.4 Шаблон уведомлений

Во вкладке **Шаблон** необходимо указать текст уведомления. Можно передавать не только фиксированный текст, но и данные, относящиеся к срабатыванию или его записям в журнале.

| Наименование | Описание |
|---|---|
| **{ANALYTICS_RULE_NAME}** | Название правила аналитики. |
| **{ANALYTICS_RULE_DESCRIPTION}** | Описание правила аналитики. |
| **{NAME}** | Название определённого срабатывания. |
| **{TIME}** | Время срабатывания правила аналитики. |

| | |
|---|---|
| **{TRIGGERED_ALERTS_NUMBER}** | Количество срабатываний. |
| **{FIRST_TRIGGERED_ALERT_TIME}** | Время первого срабатывания. |
| **{LAST_TRIGGERED_ALERT_TIME}** | Время последнего срабатывания. |
| **{TRIGGERED_ALERTS_NAMES}** | Список названий срабатываний, если используется группировка. |
| **{FIRST_EVENT_TIME}** | Время первого события, попавшего под срабатывание правила аналитики. |
| **{LAST_EVENT_TIME}** | Время последнего события, попавшего под срабатывания правила аналитики. |
| **{THREAT_LEVEL}** | Указанный уровень угрозы. |
| **{CATEGORY}** | Категория, к которой относится срабатывание. |
| **{PRIORITY}** | Приоритет срабатывания правила аналитики. |
| **{ADMINISTRATOR_NAME}** | Имя администратора, которым было создано правило аналитики. |
| **{USER_NAME}** | Имя пользователя. |
| **{SOURCE_ZONE}** | Зона источника. |
| **{DESTINATION_ZONE}** | Зона назначения. |
| **{SOURCE_COUNTRY}** | Страна источника. |
| **{DESTINATION_COUNTRY}** | Страна назначения. |
| **{SOURCE_IP}** | IP-адрес источника. |
| **{SOURCE_PORT}** | Порт источника. |
| **{DESTINATION_IP}** | IP-адрес назначения. |
| **{DESTINATION_PORT}** | Порт назначения. |
| **{SOURCE_ZONE_ALL}** | Зоны источников всех событий, сформировавших срабатывание. |
| **{DESTINATION_ZONE_ALL}** | Зоны назначения всех событий, сформировавших срабатывание. |
| **{SOURCE_COUNTRY_ALL}** | Страны источников всех событий, сформировавших срабатывание. |
| **{DESTINATION_COUNTRY_ALL}** | Страны назначения всех событий, сформировавших срабатывание. |
| **{SOURCE_IP_ALL}** | IP-адреса источников всех событий, сформировавших срабатывание. |

| | |
|---|---|
| **{SOURCE_PORT_ALL}** | Порты источников всех событий, сформировавших срабатывание. |
| **{DESTINATION_IP_ALL}** | IP-адреса назначения всех событий, сформировавших срабатывание. |
| **{DESTINATION_PORT_ALL}** | Порты назначения всех событий, сформировавших срабатывание. |

**Примечание**

Поле чувствительно к регистру букв. Название параметров необходимо вводить прописными буквами в фигурных скобках (как представлено в таблице).

Чтобы передать данные, относящиеся к срабатыванию, необходимо в поле во вкладке **Шаблон** ввести название одного из параметров, представленных в таблице. Например, если ввести **{ANALYTICS_RULE_NAME}**, то в тексте уведомления, настроенном как отправка e-mail, SMS или webhook, будет отражено название правила аналитики, которое сработало. Если заполнить шаблон при настройке действия **Создать инцидент**, то текст будет отображён в описании инцидента.

## 13.4 Срабатывания

Во вкладке **Срабатывания** показан список срабатываний правил аналитики и отображена краткая информация о них. Срабатывание - это набор событий, объединенных правилом аналитики.

Можно увидеть следующую информацию о срабатываниях.

| Наименование | Описание |
|---|---|
| **Узел** | Показано имя узла LogAn. |
| **Время** | Указаны дата и время срабатывания правила аналитики. |
| **ID** | Отображен идентификатор срабатывания. |
| **Время первого события** | Показано время первого события, попавшего под срабатывание правила аналитики. |
| **Время последнего события** | Показано время последнего события, попавшего под срабатывание правила аналитики. |
| **Количество событий** | Показано количество событий, попавших под срабатывание правила аналитики. |
| **Правило** | Отображено название правила аналитики, которое сработало. |
| **Категория** | Отображена категория, к которой относится срабатывание. По умолчанию для выбора |

| | |
|---|---|
| | доступны следующие категории:<br>• **Security**: правила данной категории определяют инциденты, приводящие к ухудшению безопасности информационных систем.<br>• **Availability**: правила данной категории определяют инциденты, которые приводят к ухудшению доступности информационных систем.<br>• **Performance**: правила данной категории определяют инциденты, которые приводят к ухудшению производительности информационных систем.<br><br>Дополнительные категории срабатываний правил аналитики могут быть созданы в разделе во вкладке **Настройки --> Библиотеки --> Категории срабатываний**. |
| **Приоритет** | Показан приоритет срабатывания, указанный при настройке правила аналитики:<br>• **Низкий**: данные правила обладают низким приоритетом реагирования.<br>• **Нормальный**: на данные правила необходимо обратить внимание и, возможно, предпринять меры.<br>• **Важный**: на данные правила необходимо обратить внимание и предпринять меры.<br>• **Критический**: данные правила требуют незамедлительного реагирования.<br><br>Установленный приоритет указывает на важность срабатывания. |
| **Пользователь** | Указано имя пользователя. |
| **Сигнатуры** | Отображено имя сработавшей сигнатуры СОВ. |
| **Зона источника** | Отображена зона, из которой происходит подключение. |
| **IP источника** | Показан IP-адрес источника. |
| **Порт источника** | Указан порт источника. |
| **Зона назначения** | Отображена зона назначения. |
| **IP назначения** | Показан IP-адрес назначения. |
| **Порт назначения** | Указан порт назначения. |

Администратор может выбрать для показа только те столбцы, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Доступны два режима поиска: простой и расширенный. Простой режим использует графический интерфейс; расширенный поиск предназначен для формирования более сложных фильтров поиска с использованием специального языка запросов, о синтаксисе которого написано в разделе Поиск и фильтрация данных.

Нажатием кнопки **Сохранить как** можно сохранить настроенный фильтр. Список сохранённых фильтров поиска можно просмотреть, нажав на кнопку **Популярные фильтры**.

Чтобы посмотреть карточку срабатывания (краткую информацию о выбранном срабатывании), необходимо нажать кнопку **Показать**.

Нажатие кнопки **Показать подробно** произведёт перевод на вкладку Подробности срабатывания, где отображена подробная информации о выбранном срабатывании. О вкладке **Подробности срабатывания** читайте в соответствующей главе Подробности срабатывания.

Выбранное срабатывание правила аналитики можно добавить в инцидент нажатием одноимённой кнопки **Добавить в инцидент**.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

## 13.5 Подробности срабатывания

На данной вкладке отображена подробная информация о срабатывании правила аналитики и отображаются все события, попавшие в данное срабатывание.

Данные могут быть представлены в табличном или текстовом виде. Переключение между режимами осуществляется нажатием кнопок **Переключить в текстовый вид** или **Переключить в табличный вид**, находящихся внизу экрана.

Представлена следующая информация о срабатывании.

| Наименование | Описание |
|---|---|
| **Срабатывание** | Показан идентификатор срабатывания. |
| **Время** | Указано время срабатывания правила аналитики. Отображается в часовом поясе, настроенном на UserGate LogAn. |
| **Приоритет** | Отображён установленный при настройке приоритет срабатывания.<br>• **Низкий**: данные правила обладают низким приоритетом реагирования.<br>• **Нормальный**: на данные правила необходимо обратить внимание и, возможно, предпринять меры.<br>• **Важный**: на данные правила необходимо обратить внимание и предпринять меры.<br>• **Критический**: данные правила требуют незамедлительного реагирования. |
| **Правило** | Показано название правила аналитики, которое сработало. |
| **Поиск инцидента** | Нажатие данной кнопки производит поиск инцидента, в котором используется данное срабатывание. |
| **Список событий** | Показаны события, которые попали в данное срабатывание. |

Нажатие кнопки **Показать срабатывания** произведёт перевод на вкладку **Срабатывания**, где будет отображён список срабатываний выбранного правила аналитики.

# 14 ИНЦИДЕНТЫ

Раздел **Инциденты** предоставляет функционал встроенной в UserGate Log Analyzer системы IRP – платформы управления процессами реагирования на инциденты информационной безопасности. Инцидентом считается событие или набор событий информационной безопасности, которые подлежат расследованию. UserGate LogAn позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании (подробнее читайте разделе Настройки инцидентов).

IRP система плотно интегрирована с системой SIEM, функционал которой представлен разделом Аналитика. Раздел **Аналитика** позволяет задать создание инцидента в качестве действия реагирования, тем самым автоматизируя процесс создания инцидентов информационной безопасности (подробнее о настройке действий реагирования читайте в разделе Действия реагирования).

Также, помимо автоматического создания, инциденты могут быть созданы вручную инженером информационной безопасности (подробнее читайте в разделе Создание инцидентов безопасности).

## 14.1 Настройки инцидентов

Процесс расследования инцидента проходит в несколько этапов, на каждом из которых инциденту присваивается определенный статус или **Состояние**, например, Открыт --> Сбор данных --> В работе --> Закрыт. Переход между состояниями возможен по определенным правилам, определяемыми администратором, например, нельзя перейти из состояния Открыт сразу в состояние Закрыт. Возможные переходы между состояниями инцидентов описываются в **Схеме инцидентов**.

По окончании расследования каждому инциденту присваивается **Решение**, например, ложная атака, подтвержденная атака, выполнено и т.п.

**Тип инцидента** выбирается на этапе создания инцидента и определяет назначение инцидента. Например, типом инцидента может быть Инцидент безопасности, Задача и т.п.

**Схема инцидента** связывает воедино состояния, возможные переходы между состояниями, решения и типы инцидентов, формируя процесс расследования инцидента информационной безопасности.

UserGate LogAn позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании. После первоначальной установки решения создается схема расследования по умолчанию с названием Incident. Администратор системы может изменить существующую схему или создать свою собственную схему. Можно создать несколько схем расследования инцидентов, но использоваться может только одна схема, которая является активной.

Что бы создать свою собственную схему расследования инцидентов необходимо выполнить следующие действия:

| Наименование | Описание |
|---|---|
| **Шаг 1.** Создайте необходимые решения инцидентов | В разделе **Настройки инцидентов --> Решения инцидентов** нажмите добавить, укажите название и описание создаваемого решения и нажмите кнопку **Сохранить**. |
| **Шаг 2.** Создайте типы инцидентов | В разделе **Настройки инцидентов --> Типы инцидентов** нажмите добавить, укажите название и описание создаваемого типа и нажмите кнопку **Сохранить**. |

| | |
|---|---|
| **Шаг 3.** Создайте состояния инцидентов | В разделе **Настройки инцидентов --> Состояния инцидентов** нажмите добавить, укажите название, описание и группу создаваемого состояния. Группа состояние определяет положение данного состояние в схеме состояний. Возможно 3 варианта:<br>• **Открыто** - данная группа назначается состояниям инцидентов, по которым еще не начата работа или она приостановлена. Как правило, это начальные состояния инцидентов, например Создан. Все состояния данной группы помечаются синим цветом в веб-консоли.<br>• **В работе** - данная группа назначается состояниям инцидентов, по которым ведется, но еще не завершена работа. Это промежуточные состояния инцидентов, например, В работе, Расследование. Все состояния данной группы помечаются желтым цветом в веб-консоли.<br>• **Закрыто** - данная группа назначается состояниям инцидентов, по которым завершена работа. Это конечные состояния инцидентов, например, Завершено, Закрыто. При переходе в состояние этой группы необходимо обязательно указать решение инцидента, например, Ложная атака, Подтвержденная атака, Выполнено. Все состояния данной группы помечаются зеленым цветом в веб-консоли.<br><br>После определения всех полей нажмите кнопку **Сохранить**. |
| **Шаг 4.** Создайте схему инцидентов | В разделе **Настройки инцидентов --> Схемы инцидентов** нажмите добавить и укажите следующие параметры:<br>• Сделать активной - делает данную схему активной. Только одна схема может быть активной, если была активна другая схема, то данное действие сделает ее не активной, и все новые и существующие инциденты перейдут на работу по новой схеме.<br>• Схема - название схемы.<br>• Префикс - префикс, который будет использован при назначении идентификаторов создаваемым инцидентам. Идентификатор будет иметь вид Префикс – порядковый номер, например INC-99.<br>• Описание - необязательное описание данной схемы.<br>• Состояния рабочего процесса - описывает все состояния, которые может принимать инцидент в своем жизненном цикле. Добавьте сюда все состояния инцидентов, созданные на предыдущем шаге.<br>• Начальное состояние - указывает начальное состояние, которое принимает инцидент при его создании.<br>• Переходы - необходимо указать все возможные переходы между состояниями и дать им названия. Например, создать переход под названием **Взять в работу** для перехода из состояния **Открыто** в состояние **В работе**. Перевод инцидента между состояниями возможен только для тех состояний, между которыми определены переходы.<br>• Решения инцидентов - указывает список возможных решений инцидентов. Решение является обязательным при завершении работы по расследованию тикета, то есть при переводе его в состояние, относящееся к группе **закрыто**. Выберите все необходимые решения, которые были созданы ранее.<br>• Типы инцидентов - укажите типы инцидентов, которые могут быть использованы в этой схеме. |
| **Шаг 5.** Активируйте схему инцидентов | После создания схемы инцидентов ее необходимо активировать. Для этого активируйте чекбокс **Сделать активной** в настройках схемы инцидентов. |

## 14.2 Дашборд по инцидентам

В данной вкладке можно просмотреть текущее состояние инцидентов информационной безопасности, созданных на LogAn. Отчеты представлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице Дашборд.

Некоторые виджеты позволяют настроить отображение, указать фильтрацию данных и настроить прочие параметры. Для настройки виджета необходимо кликнуть по символу шестеренки в правом верхнем углу. Не все параметры, перечисленные ниже, доступны для каждого типа виджетов.

| Наименование | Описание |
|---|---|
| **Название** | Название виджета, которое будет отображено в Дашборд. |
| **Диаграмма** | Тип представления данных:<br>• Число.<br>• Вертикальная гистограмма.<br>• Таблица. |
| **Запрос фильтра** | SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета. |
| **Описание** | Описание виджета. |
| **Количество записей** | Максимальное количество записей для отображения. |

## 14.3 Журнал инцидентов

Во вкладке **Журнал инцидентов** представлен список созданных инцидентов информационной безопасности. В таблице отражена следующая информация об инцидентах.

| Наименование в базе данных | Наименование в поисковом запросе | Описание |
|---|---|---|
| **Создан** | date | Дата и время создания инцидента. |
| **Изменён** | updateDate | Дата и время последнего изменения. |
| **Индекс** | incidentPrefix | Префикс инцидента (INC-N, где N – порядковый номер инцидента; нумерация начинается с 0). |
| **Имя** | incidentName | Название инцидента. |

| | | |
|---|---|---|
| **Правило** | rule | Название правила аналитики, в результате срабатывания которого автоматически был создан инцидент, т.е. при настройке правила аналитики было задано действие реагирования **Создать инцидент**. |
| **Статус** | status | Статус инцидента.<br><br>Существует 3 группы состояний, которые определяют положение данного состояние в схеме состояний:<br><br>• **Открыто** - данная группа назначается состояниям инцидентов, по которым еще не начата работа или она приостановлена. Как правило, это начальные состояния инцидентов, например Создан. Все состояния данной группы помечаются синим цветом в веб-консоли.<br>• **В работе** - данная группа назначается состояниям инцидентов, по которым ведется, но еще не завершена работа. Это промежуточные состояния инцидентов, например, В работе, Расследование. Все состояния данной группы помечаются желтым цветом в веб-консоли.<br>• **Закрыто** - данная группа назначается состояниям инцидентов, по которым завершена работа. Это конечные состояния инцидентов, например, Завершено, Закрыто. При переходе в состояние этой группы необходимо обязательно указать решение инцидента, например, Ложная атака, Подтвержденная атака, Выполнено. Все состояния данной группы помечаются зеленым цветом в веб-консоли.<br><br>По умолчанию в UserGate создана схема Incident, которая содержит переходы между всеми состояниями. Схемы инцидентов можно добавить в разделе **Настройки --> Настройка инцидентов --> Схема инцидентов**.<br><br>Дополнительные состояния инцидентов можно задать во вкладке **Настройки --> Настройка инцидентов --> Состояния инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Решение** | resolution | Решение инцидента. По умолчанию созданы:<br><br>• **False positive**: ложная атака.<br>• **True positive**: подтверждённая атака.<br>• **Duplicate**: проблема повторяет другую проблему.<br>• **Won't do**: задача не выполнима.<br>• **Done**: проблема решена.<br><br>Дополнительные решения инцидентов можно создать во вкладке **Настройки --> Настройка инцидентов --> Решения инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Тип** | type | Тип инцидента. По умолчанию доступны 2 типа: инцидент безопасности и задача. Дополнительно типы инцидентов можно создать в разделе **Настройки --> Настройка инцидентов --> Типы инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |
| **Приоритет** | priority | Приоритет инцидента: |

| | | |
|---|---|---|
| | | • Низкий.<br>• Нормальный.<br>• Важный.<br>• Критический. |
| **Инициатор** | reporter | Имя администратора, который создал инцидент. |
| **Последнее изменение** | lastChangeBy | Имя администратора, который внёс последнее изменение. |
| **Назначен** | assignee | Имя администратора, назначенного на инцидент. |
| **Активность** | | Количество комментариев, срабатываний правил аналитики и журналов событий, добавленных в инцидент. |

Администратор может выбрать для показа только те столбцы, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Возможно производить фильтрацию инцидентов по параметрам, представленным в таблице. Фильтрация доступна в двух режимах: простой и расширенный (подробнее о синтаксисе расширенного поиска читайте в разделе Поиск и фильтрация данных).

Настроенные фильтры можно сохранять, нажав кнопку **Сохранить как**. Сохранённые фильтры можно просмотреть с использованием кнопки **Популярные фильтры**.

Нажатием кнопки **Экспортировать в CSV** администратор может скачать отфильтрованный список инцидентов в csv-файл для дальнейшего анализа.

## 14.4 Создание инцидентов безопасности

Во вкладке **Журнал инцидентов** также можно создавать инциденты информационной безопасности. Для создания и работы с инцидентами информационной безопасности пользователь должен обладать определёнными ролевыми разрешениями (подробнее читайте в разделе Роли и ролевые разрешения пользователей).

Инциденты создаются нажатием кнопки **Создать инцидент**. Далее необходимо указать следующие параметры.

| Наименование | Описание |
|---|---|
| **Имя** | Указать название инцидента информационной безопасности. |
| **Тип** | Указать тип инцидента.<br><br>По умолчанию созданы 2 типа инцидентов: инцидент безопасности и задача. Дополнительно типы инцидентов могут быть созданы в разделе **Настройки --> Настройка инцидентов --> Типы инцидентов**. Подробнее читайте в разделе Настройки инцидентов. |

| | |
|---|---|
| **Приоритет** | Назначить приоритет<br>• Низкий.<br>• Нормальный.<br>• Важный.<br>• Критический. |
| **Назначен** | Назначить ответственного на инцидент. |
| **Наблюдатели** | Указать список сотрудников для наблюдения за инцидентом. При любых изменениях инцидента они будут получать уведомление. |
| **Вложения** | Прикрепить файлы, относящиеся к инциденту. |
| **Описание** | Ввести описание инцидента. |

## 14.5 Подробности инцидента

Выбор инцидента и нажатие кнопки **Показать** произведет перевод на новую вкладку (название вкладки формируется из индекса и заданного имени инцидента), где будет отображена подробная информация о выбранном инциденте. На данной вкладке также можно редактировать (кнопка **Редактировать**) и комментировать (кнопка **Комментировать**) инцидент, изменять ответственного за инцидент (кнопка **Назначить**), и статус рабочего процесса (кнопка **Рабочий процесс**). Помимо информации об инциденте, отображённой во вкладке **Журнал инцидентов** (подробнее читайте в разделе Журнал инцидентов), можно увидеть следующую информацию.

В разделе **Срабатывания** отражена информация о срабатываниях правил аналитики, добавленных в инцидент. Подробнее читайте в разделе Срабатывания. Добавить срабатывания в инцидент можно нажатием кнопки **Добавить срабатывания**. Далее необходимо выбрать срабатывания, которые необходимо добавить в инцидент. Чтобы просмотреть подробности срабатывания выделите нужное срабатывание правила аналитики и нажмите кнопку **Показать подробно**. Также можно просмотреть краткую информацию о срабатывании нажав на кнопку **Показать**. Нажатием на кнопку **Удалить из инцидента** можно удалить запись о срабатывании правила аналитики из инцидента. Список срабатываний правил аналитики, добавленный в инциденты, можно скачать в csv-файл для дальнейшего анализа нажатием кнопки **Экспортировать в CSV**.

В разделе **Журналы** отображена подробная информация о событиях всех журналов (подробнее о записях журналов читайте в разделе Поиск). Чтобы добавить события в инцидент нажмите **Добавить в инцидент** и выберите события для добавления. Нажатие кнопки **Удалить из инцидента** позволяет удалить ненужные события.

В разделе **Улики** отображены записи о наблюдениях за объектами, указанными при настройке. Улики необходимы для упрощения анализа инцидента информационной безопасности, принятия верного решения и уменьшения затраченного на инцидент времени. Для получения информации используются ресурсы для обогащения (подробнее читайте в разделе Внешние сервисы обогащений). Подробную информацию, предоставленную сервисом, можно увидеть в настройках обогащения, нажав на обогащение.

Улики можно создать нажатием кнопки **Добавить**. Далее необходимо указать параметры, которые будут отражены в таблице раздела.

| Наименование | Описание |
|---|---|
| **Тип улики** | Возможен выбор одного из следующих типов улик:<br>• **Автономная система**: система IP-сетей и маршрутизаторов, находящихся под единым управлением.<br>• **Домен**: имя сайта в Интернете.<br>• **Файл**: файл, который может быть для сбора информации о нём.<br>• **Имя файла**: название файла, о котором необходимо собрать информацию.<br>• **FQDN**: полное доменное имя.<br>• **Хэш**: хэш какого-либо файла, например, добавленного в инцидент.<br>• **Имя хоста**: метка устройства, подключённого к компьютерной сети и использующаяся для идентификации устройства.<br>• **IP**: уникальный адрес, идентифицирующий устройство в компьютерной сети.<br>• **Почта**: адрес электронной почты.<br>• **Тема письма**: часть письма, указанная в поле subject.<br>• **Реестр**: ключ реестра Microsoft Windows – каталог, в котором хранятся настройки и параметры операционной системы.<br>• **Путь URI**: последовательность символов, идентифицирующая абстрактный или физический ресурс.<br>• **URL**: индивидуальный адрес ресурса в сети Интернет.<br>• **Агент пользователя**: буквенно-цифровая строка, идентифицирующая программу, которая отправляет запрос на сервер и одновременно запрашивает доступ к web-сайту.<br>• **Другое**. |
| **Значение** | Необходимо указать объект, с которым будет производиться работа: IP-адрес, домен, и т.п. |
| **Тип атаки** | Для указания доступны следующие типы атаки:<br>• **Ботнет** - сеть заражённых компьютеров, удалённо управляемых преступниками.<br>• **Фишинг** - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.<br>• **Вредоносное ПО** - любое программное обеспечение, которое пытается заразить компьютер или мобильное устройство.<br>• **DDoS** - способ заблокировать работу сайта путем подачи большого количества запросов, превышающих пропускную способность сети.<br>• **Угон трафика** – злоумышленное перенаправление трафика.<br>• **Сетевое сканирование** – сканирование узлов сети для определения уязвимостей.<br>• **Брутфорс** - метод взлома учётных записей путём подбора паролей к ним.<br>• **Компроментация** - факт несанкционированного доступа к защищенной информации, а также подозрение осуществления такого доступа.<br>• **Спам** - массовая рассылка с использованием специальных программ, коммерческой, политической и иной рекламы или иного вида сообщений людям, не выразившим желания их получать.<br>• **Другое**. |
| **TLP** | Отображена маркировка конфиденциальной информации (Traffic Light Protocol). Возможны следующие маркировки: |

| | |
|---|---|
| | • **RED**: информация является крайне конфиденциальной.<br>• **AMBER**: информацией можно поделиться в рамках своей организации, при условии, что этой информацией нужно поделиться.<br>• **GREEN**: информация может быть широко распространена в пределах определённого сообщества.<br>• **WHITE**: информация в свободном распространении, но не нарушает авторские права. |
| **Индикатор компроментации?** | Чекбокс необходимо отметить, если объект является потенциальным индикатором компроментации. |
| **Сервисы** | Отображён список сервисов, которые используются для получения дополнительной информации об объектах наблюдения. Список сервисов отображается автоматически после выбора типа улики. Список сервисов доступен в разделе **Настройки --> Библиотеки --> Внешние сервисы обогащений**. Подробнее читайте в разделе Внешние сервисы обогащений. |
| **Обновлено** | Показаны дата и время последнего обновления сервиса. |

С использованием соответствующих кнопок **Редактировать** и **Удалить** улики можно редактировать или удалять.

В разделе **Активность** можно просмотреть комментарии по инциденту и историю внесения изменений (добавление наблюдателей, изменение статуса рабочего процесса и т.д.).

С использованием кнопки **Создать отчёт** можно создать отчёт об инциденте:

- **Incident report**: пользовательский отчёт, который может быть создан на английском или русском языках в формате PDF или HTML. При создании отчёта возможно использование шаблонов, список которых доступен в разделе **Журналы и отчёты --> Отчёты инцидентов --> Правила отчётов инцидентов**.
- **GOSSOPKA report**: для создания отчёта используется шаблон **Форма для ГОССОПКА**, который соответствует требованиям к отчётам ГОССОПКА. Отчёт можно просто скачать (кнопка **Создать файл**) или сразу сформировать в требуемом формате и отправить в систему личных кабинетов ГОССОПКА (кнопка **Послать через сеть**). Для автоматической отправки отчёта пользователю необходимо предоставить учётную запись для входа в личный кабинет на сайте ГОССОПКА и защищённый канал передачи. Подробнее читайте в разделе Передача отчётов об инцидентах информационной безопасности в ГосСОПКА.

## 14.6 Передача отчётов об инцидентах информационной безопасности в ГосСОПКА

ГосСОПКА – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Целью создания ГосСОПКА является защита критической информационной инфраструктуры (КИИ), владельцы объектов которой должны подключиться к ГосСОПКА. Также к ГосСОПКА можно подключиться и на добровольной основе для обеспечения более высокого уровня информационной безопасности и улучшения методов выявления и реагирования на инциденты.

В UserGate Log Ananlyzer реализована возможность передачи отчётов о компьютерных атаках, инцидентах и уязвимостях в стандартизированном формате через личный кабинет ГосСОПКА.

Для отправки отчётов необходимо:

1. Самостоятельно подключиться к системе личных кабинетов ГосСОПКА.

Подключение необходимо для взаимодействия и автоматизации обмена информацией о зафиксированных инцидентах информационной безопасности и методах их предотвращения с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак.

2. Добавить криптографический шлюз для организации межсетевого взаимодействия с сетью НКЦКИ (Национальный координационный центр по компьютерным инцидентам; главный центр ГосСОПКА).

Для самостоятельного подключения к ГосСОПКА используются аппаратно-программные комплексы компаний Инфотекс (ViPNet), Код безопасности (Континент), С-Терра (С-Терра Шлюз).

**Примечание**

Не указывайте криптографический шлюз в качестве шлюза по умолчанию.

3. Добавить DNS-серверы для определения адреса системы личных кабинетов ГосСОПКА.

Для определения адреса системы личных кабинетов ГосСОПКА необходимо добавить серверы с адресами 10.0.100.49 и 10.0.100.50.

**Примечание**

В список системных DNS-серверов можно добавить не более трёх серверов. Серверы ГосСОПКА не могут быть использованы для преобразования доменных имён в сети Интернет.

4. Настроить статический маршрут в сеть ГосСОПКА для обеспечения доступности DNS-серверов, указанных в пункте 3.

Для обеспечения доступности серверов ГосСОПКА необходимо добавить статический маршрут с адресом назначения: 10.0.100.0/24. Подробнее о настройке маршрутов читайте в разделе Маршруты.

5. Настроить подключение к личному кабинету ГосСОПКА с UserGate LogAn для возможности отправки отчёта.

В UserGate Log Analyzer по умолчанию создан коннектор **Gossopka**, предназначенный для взаимодействия с ГосСОПКА. При настройке коннектора необходимо указать

Для настройки коннектора перейдите во вкладку **Настройки** в раздел **Сенсоры --> Коннектор**. Используйте коннектор **Gossopka**, созданный в UserGate Log Analyzer по умолчанию; необходимо указать: FQDN личного кабинета, вместо указанного по умолчанию (значение по умолчанию отображает формат, в котором должно быть указано значение поля), логин/пароль и ключ API, который добавляется в поле HTTP заголовки.

6. Настроить шаблон отчёта.

По молчанию создан шаблон **Форма для ГОССОПКА**, соответствующий требованиям ГосСОПКА к отчётам. Заполните поля формы; данная форма будет использоваться при формировании отчёта.

| Наименование | Описание |
| --- | --- |
| **Организация** | Название организации. |
| **Категория** | Категория уведомления:<br>• Уведомление о компьютерном инциденте.<br>• Уведомление о компьютерной атаке.<br>• Уведомление о наличии уязвимости. |
| **Тип события ИБ** | Тип события информационной безопасности:<br>• Вовлечение контролируемого ресурса в инфраструктуру ВПО.<br>• Замедление работы ресурса в результате DDoS-атаки.<br>• Заражение ВПО.<br>• Захват сетевого трафика.<br>• Использование контролируемого ресурса для фишинга.<br>• Компрометация учётной записи.<br>• Несанкционированное изменение информации.<br>• Несанкционированное разглашение информации.<br>• Публикация на ресурсе запрещённой законодательством РФ информации.<br>• Рассылка спам-сообщений с контролируемого ресурса.<br>• Успешная эксплуатация уязвимости. |
| **Статус реагирования на инцидент** | Статус реагирования на инцидент:<br>• Меры приняты.<br>• Проводятся мероприятия по реагированию.<br>• Возобновлены мероприятия по реагированию. |
| **Необходимость привлечения сил ГосСОПКА** | Отметьте чекбокс в случае необходимости привлечения сил ГосСОПКА. |
| **Краткое описание события ИБ** | Описание события информационной безопасности. |
| **Сведения о средстве или способе выявления инцидента** | Информация о способе и устройстве/ПО, посредством которого был выявлен инцидент. |
| **Дата и время выявления инцидента** | Дата и время выявления инцидента заполняются автоматически. |
| **Дата и время завершения инцидента** | Дата и время завершения инцидента заполняются автоматически. |

| | |
|---|---|
| **Ограничительный маркер TLP** | Маркировка конфиденциальной информации (Traffic Light Protocol). Возможны следующие маркировки:<br>• **RED**: информация является крайне конфиденциальной.<br>• **AMBER**: информацией можно поделиться в рамках своей организации, при условии, что этой информацией нужно поделиться.<br>• **GREEN**: информация может быть широко распространена в пределах определённого сообщества.<br>• **WHITE**: информация в свободном распространении, но не нарушает авторские права. |
| **Влияние на доступность** | Потенциальное влияние на доступность информационных ресурсов:<br>• Отсутствует.<br>• Низкое.<br>• Высокое. |
| **Влияние на целостность** | Потенциальное влияние на целостность ресурсов информационной системы:<br>• Отсутствует.<br>• Низкое.<br>• Высокое. |
| **Влияние на конфиденциальность** | Потенциальное влияние на конфиденциальность (ограничение доступа к информационным ресурсам, разрешения доступа к системе только авторизованным пользователям, предотвращение раскрытия информации неуполномоченным лицам):<br>• Отсутствует.<br>• Низкое.<br>• Высокое. |
| **Краткое описание иной формы последствий компьютерного инцидента** | Описание последствий инцидента, кроме тех, что были указаны ранее. |
| **Наименование контролируемого ресурса, на котором был выявлен компьютерный инцидент** | Наименование контролируемого информационного ресурса объекта КИИ, на котором выявлен компьютерный инцидент, компьютерная атака или уязвимость. |
| **Информация о категорировании ОКИИ** | Присвоенная объекту КИИ категория значимости:<br>• Информационный ресурс не является объектом КИИ.<br>• Объект КИИ без категории значимости (объект признан незначимым).<br>• Объект КИИ третьей категории значимости (самая низкая). |

| | |
|---|---|
| | • Объект КИИ второй категории значимости.<br>• Объект КИИ первой категории значимости (самая высокая). |
| **Сфера функционирования субъекта** | Сфера функционирования объекта КИИ (например, банковская сфера, здравоохранение и т.п.). |
| **Наличие подключения к сети Интернет** | Наличие подключения к сети Интернет:<br>• **Да**.<br>• **Нет**. |
| **Страна/регион** | Код в соответствии с ISO-3166-2 (https://en.wikipedia.org/wiki/ISO_3166-2). |
| **Населенный пункт или геокоординаты** | Название населённого пункта или его географические координаты.<br>Географические координаты указываются в формате: *широта* – С.Ш, *долгота* – В.Д. |

7. Сформировать и отправить отчёт об инциденте информационной безопасности.

Формирование отчёта доступно во вкладке с подробностями об инциденте нажатием кнопки **Создать отчёт --> GOSSOPKA report**. Для отправки отчёта необходимо указать коннектор, настроенный ранее и нажать **Послать через сеть**.

Далее нужно заполнить необходимые поля формы (большинство поле заполнено в соответствии с шаблоном **Форма для ГОССОПКА**) и нажать **ОК**. В случае успешного соединения сервер UserGate Log Analyzer отправит отчёт на коннектор (в систему личных кабинетов ГосСОПКА).

Запись об отправке отчёта будет отображена в журнале событий Log Analyzer.

# 15 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Раздел технической поддержки на сайте компании https://www.usergate.com/ru/support содержит дополнительную информацию по настройке UserGate LogAn. Кроме этого, здесь же вы можете оставить заявку на решение вашей проблемы.