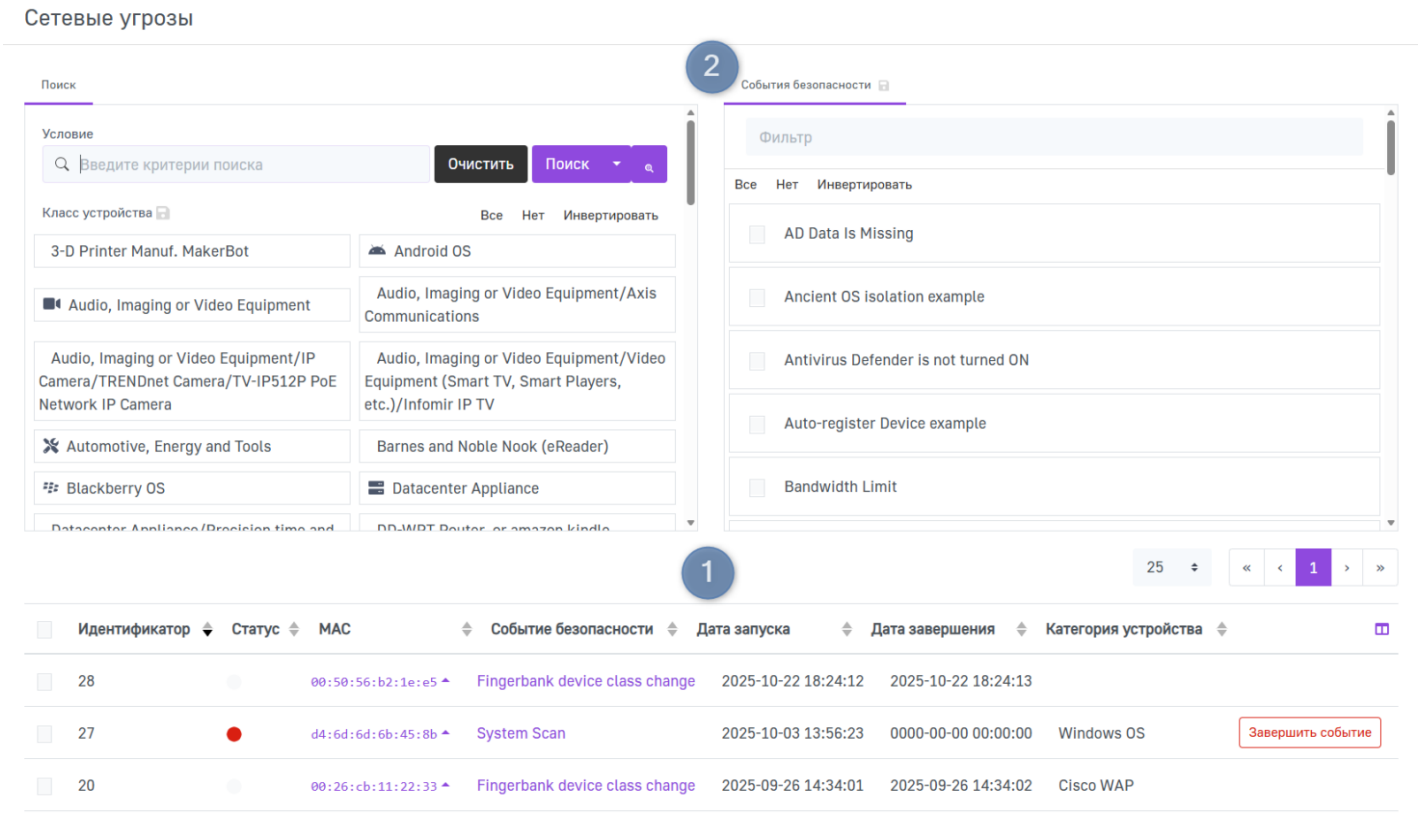
Страница «Сетевые угрозы»

Страница **Сетевые угрозы** предназначена для мониторинга и анализа сетевых угроз, обнаруженных системой AxelNAC. Здесь отображается вся информация об открытых и завершенных событиях безопасности, связанных с устройствами в сети.

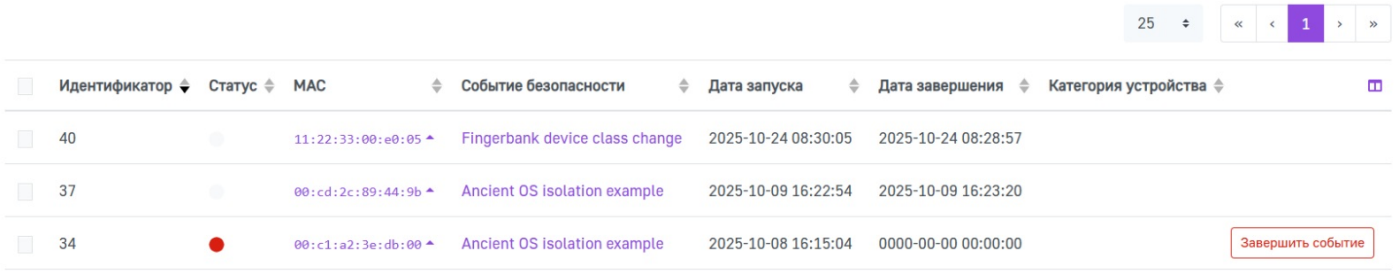
Страница включает в себя два основных блока:



1. **Таблица событий безопасности** — список отфильтрованной информация о событиях безопасности;
2. **Фильтрация данных** — используется для настройки фильтрации событий безопасности, отображаемых на таблице.

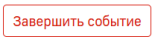
Таблица событий безопасности

На данной таблице отображается отфильтрованная информация о событиях безопасности.



По умолчанию таблице отображаются 7 столбцов:

- **Идентификатор** — уникальный идентификатор события безопасности;
- **Статус** — активность события безопасности: красный — открыто, серый — завершено;
- **MAC** — MAC-адрес устройства, на котором обнаружено событие безопасности;
- **Событие безопасности** — название события безопасности;
- **Дата запуска** — дата и время определения события безопасности;
- **Дата завершения** — дата и время завершения события безопасности;
- **Категория устройства** — определенный класс устройства.

Чтобы посмотреть подробную информацию о событии безопасности, нажмите на нужное событие. Для просмотра подробной информации об устройстве, нажмите на его **MAC-адрес**. При необходимости, вы можете завершить событие безопасности, для этого нажмите 

.

Управление таблицей

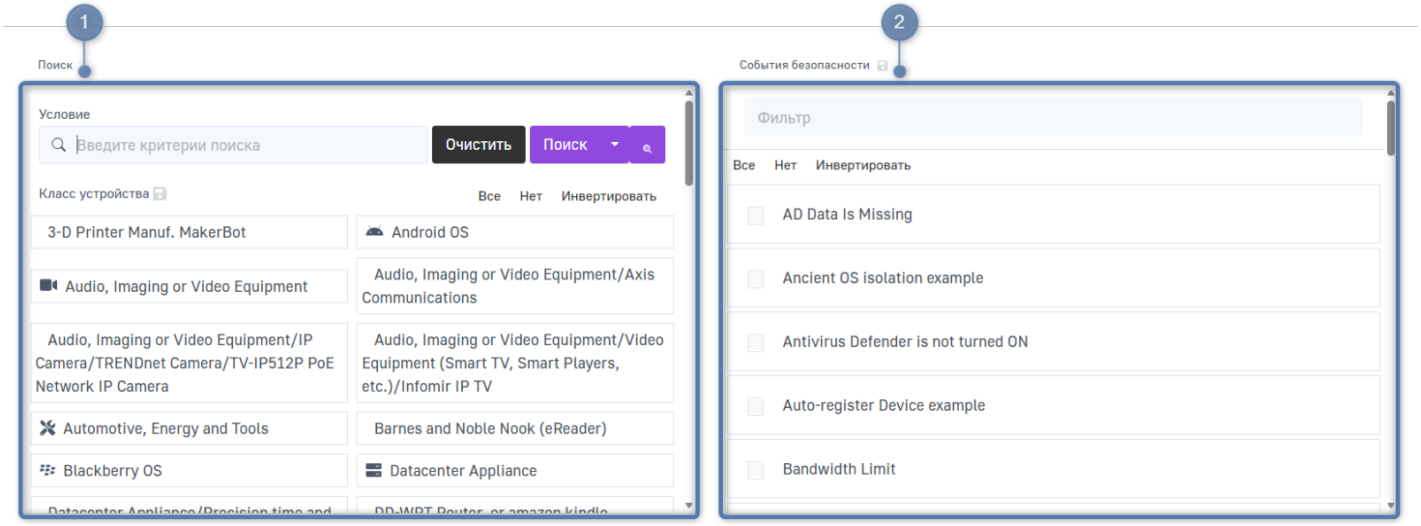
Набор отображаемых столбцов в таблице может быть изменен, для этого нажмите на иконку  . В выпадающем списке нажмите на название столбца, отображение которого в таблице необходимо изменить.

По умолчанию на странице отображается 25 записей, однако вы можете выбрать отображение 10, 50, 100, 200, 500 и 1000 записей на странице. Для этого нажмите на поле в правом верхнем углу списка и выберите в выпадающем списке необходимое количество для отображения.

Вы можете отсортировать таблицу по в порядке возрастания или убывания с помощью иконки . По умолчанию все записи в таблице отображаются в порядке алфавитного возрастания по столбцу **Идентификатор**.

Для переключения между страницами используйте блок в правом верхнем углу списка.

Фильтрация данных

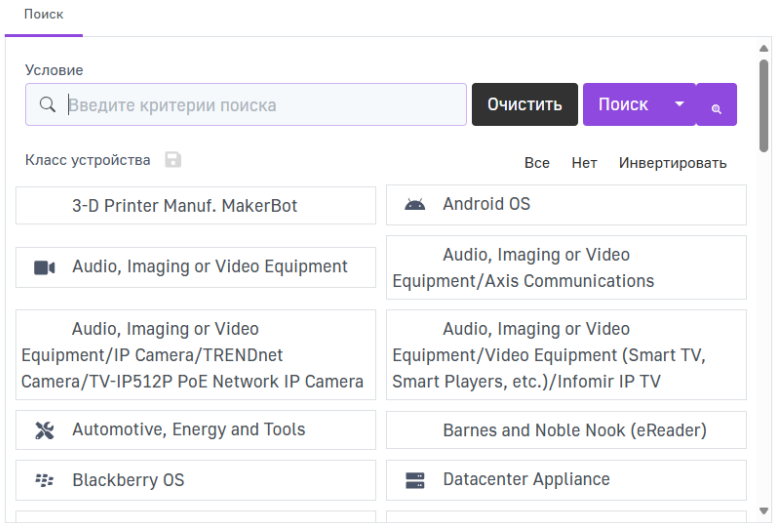


Фильтрация данных осуществляется с помощью блоков:

1. **Поиск** — фильтрация по параметрам события безопасности;
2. **События безопасности** — фильтрация по названию события безопасности.

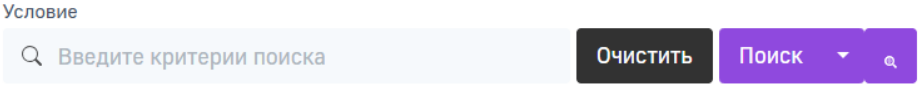
Поиск

Блок **Поиск** предназначен для настройки фильтрации событий безопасности, отображаемых в таблице, по их параметрам.



Поиск по условию

Условие позволяет отфильтровать события безопасности с помощью ввода конкретных критериев поиска.



Можно выполнить поиск по критериям: **Идентификатор**, **Статус**, **MAC**, **Дата запуска**, **Дата завершения**, **Ссылка на тикет**,

Примечания или **Категория устройства**. Введите интересующий критерий в поле поиска и нажмите **Поиск**. Нажмите **Очистить**, чтобы сбросить критерии поиска.

Также можно выполнять поиск по нескольким критериям. Для этого нажмите на иконку лупы справа от кнопки **Поиск**.

В меню расширенного поиска вы можете выбрать операторы **И** и **ИЛИ** и указать несколько критериев для поиска. Поиск можно вести по критериям:

- **Имя** — поиск по идентификатору события безопасности;
- **MAC-адрес** — поиск по MAC-адресу устройства, на котором обнаружено событие безопасности;
- **Дата запуска** — поиск по дате и времени определения события безопасности;
- **Дата завершения** — поиск дате и времени завершения события безопасности;
- **Ссылка на тикет** — поиск по ссылке на тикет;
- **Примечания** — поиск по дополнительной информации о событии безопасности.

Также вам доступны следующие операторы**:**

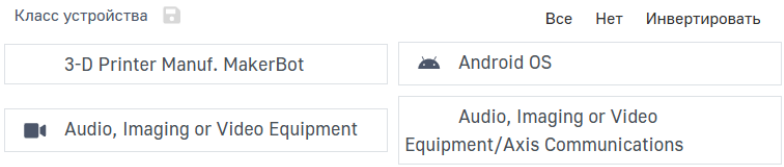
- **равно;**
- **не равно**;
- **начинается с**;
- **заканчивается на**;
- **содержит**;
- **больше чем** (доступно для критериев **Дата запуска, Дата завершения**);
- **меньше чем** (доступно для критериев **Дата запуска, Дата завершения**);
- **больше или равно** (доступно для критериев **Дата запуска, Дата завершения**);
- **меньше или равно** (доступно для критериев **Дата запуска, Дата завершения**).

Для того чтобы изменить порядок выражений, нажмите и удерживайте иконку и перетащите выражение. Чтобы удалить выражение, нажмите на иконку .

Вы можете сохранить и экспортировать существующий запрос, чтобы воспользоваться им позднее или импортировать уже существующий запрос. Все эти действия можно выбрать из выпадающего списка, нажав на иконку .

Поиск по классу устройства

Класс устройства позволяет отфильтровать события безопасности с помощью выбора определенного класса устройств, связанных с инцидентом.

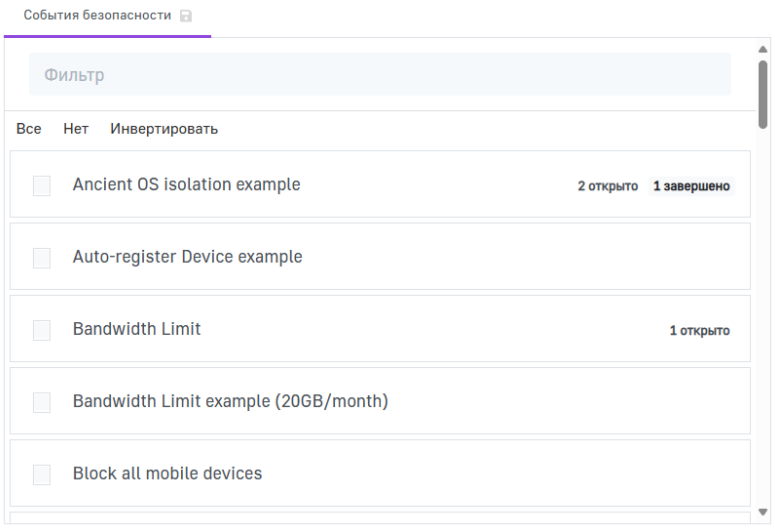


Нажмите на нужный класс устройств, чтобы сократить поиск и анализировать события безопасности только определенных классов устройств.

Для того чтобы выбрать все классы устройств, нажмите **Все**. Чтоб инвертировать выбранные классы, нажмите **Инвертировать**. Если необходимо отменить выбор, нажмите **Нет**.

События безопасности

Блок **События безопасности** позволяет отфильтровать события безопасности по их названию.



Нажмите на нужное событие безопасности, чтобы сократить поиск и анализировать только определенные события безопасности.

Для того чтобы выбрать все события безопасности, нажмите **Все**. Чтоб инвертировать выбранные события безопасности, нажмите **Инвертировать**. Если необходимо отменить выбор, нажмите **Нет**.

Групповые действия

Для того чтобы выполнить действия с несколькими событиями безопасности, отметьте необходимые события безопасности.

Чтобы выполнить действия со всеми событиями безопасности в списке, нажмите на селектор в шапке таблицы.

На данный момент единственное доступное групповое действие в системе — **Экспорт в CSV**. При его выборе, файл в формате **.csv**, содержащий записи таблицы, попадает в менеджер загрузки вашего браузера.

ID статьи: 1350
Последнее обновление: 29 окт., 2025
Обновлено от: Михалева А.
Ревизия: 6
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.0.1 -> AxelNAC. Руководство по использованию веб-интерфейса -> Меню «Статус» -> Страница «Сетевые угрозы» -> Страница «Сетевые угрозы»
https://docs.axel.pro/entry/1350/