

Страница «Сетевые угрозы»

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

Страница включает в себя два основных блока:

Сетевые угрозы

The screenshot shows the 'Network Threats' page with two main sections. On the left, there is a search/filter interface with a search bar, a 'Класс устройства' (Device Class) dropdown, and a table of device categories. On the right, there is a table of security events with columns for ID, Status, MAC, Event, Start Date, End Date, and Device Category. A red box highlights the 'Завершить событие' (End event) button for event 27.

Идентификатор	Статус	MAC	Событие безопасности	Дата запуска	Дата завершения	Категория устройства
28		00:50:56:b2:1e:e5	Fingerbank device class change	2025-10-22 18:24:12	2025-10-22 18:24:13	
27	●	d4:6d:6d:6b:45:8b	System Scan	2025-10-03 13:56:23	0000-00-00 00:00:00	Windows OS
20		00:26:cb:11:22:33	Fingerbank device class change	2025-09-26 14:34:01	2025-09-26 14:34:02	Cisco WAP

1. **Таблица событий безопасности** — список отфильтрованной информации 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.

The screenshot shows a table of security events with columns for ID, Status, MAC, Event, Start Date, End Date, and Device Category. A red box highlights the 'Завершить событие' (End event) button for event 34.

Идентификатор	Статус	MAC	Событие безопасности	Дата запуска	Дата завершения	Категория устройства
40		11:22:33:00:e0:05	Fingerbank device class change	2025-10-24 08:30:05	2025-10-24 08:28:57	
37		00:cd:2c:89:44:9b	Ancient OS Isolation example	2025-10-09 16:22:54	2025-10-09 16:23:20	
34	●	00:c1:a2:3e:db:00	Ancient OS Isolation example	2025-10-08 16:15:04	0000-00-00 00:00:00	

По умолчанию таблице отображаются 7 столбцов:

- **Идентификатор** — уникальный идентификатор события безопасности;
- **Статус** — активность события безопасности: красный — открыто, серый — завершено;
- **МАС** — 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 **МАС-адрес**. При необходимости, вы можете завершить событие безопасности, для этого нажмите **Завершить событие**.

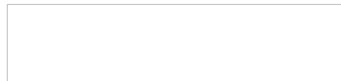
Управление таблицей

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

The screenshot shows two separate search/filtering blocks. The left block, labeled '1', is titled 'Search' and contains a search input field with placeholder 'Введите критерии поиска' and a purple 'Search' button. Below it is a 'Device class' dropdown with several options like '3-D Printer Manuf. MakerBot', 'Android OS', etc. The right block, labeled '2', is titled 'Filter' and contains a 'Safety events' dropdown. Below it is a list of filter criteria with checkboxes: 'AD Data Is Missing', 'Ancient OS isolation example', 'Antivirus Defender is not turned ON', 'Auto-register Device example', and 'Bandwidth Limit'. Both blocks have a 'Clear' button and a 'Search' dropdown.

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.

The screenshot shows the 'Search' block. It has a 'Search' tab selected. Below it is a 'Search conditions' section with a search input field containing placeholder 'Введите критерии поиска' and a purple 'Search' button. To the right of the input field are three buttons: 'Clear', 'Search', and a dropdown menu. Below this is a 'Device class' dropdown with several options like '3-D Printer Manuf. MakerBot', 'Android OS', etc. The interface is identical to the one shown in the 'Filtering data' section.

Поиск по условию

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

The screenshot shows the 'Search by condition' block. It has a 'Search conditions' section with a search input field containing placeholder 'Введите критерии поиска' and a purple 'Search' button. To the right of the input field are three buttons: 'Clear', 'Search', and a dropdown menu.

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 критерий 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:

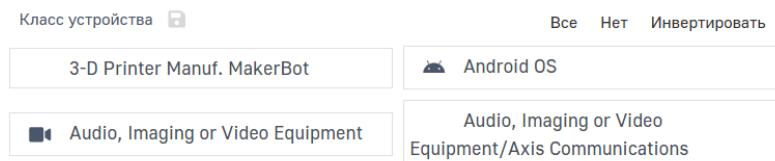
- **равно**;
- **не равно**;
- **начинается с**;
- **заканчивается на**;
- **содержит**;
- **больше чем** (доступно для критериев **Дата запуска**, **Дата завершения**);
- **меньше чем** (доступно для критериев **Дата запуска**, **Дата завершения**);
- **больше или равно** (доступно для критериев **Дата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



Класс устройства 

Все Нет Инвертировать

3-D Printer Manuf. MakerBot

Android OS

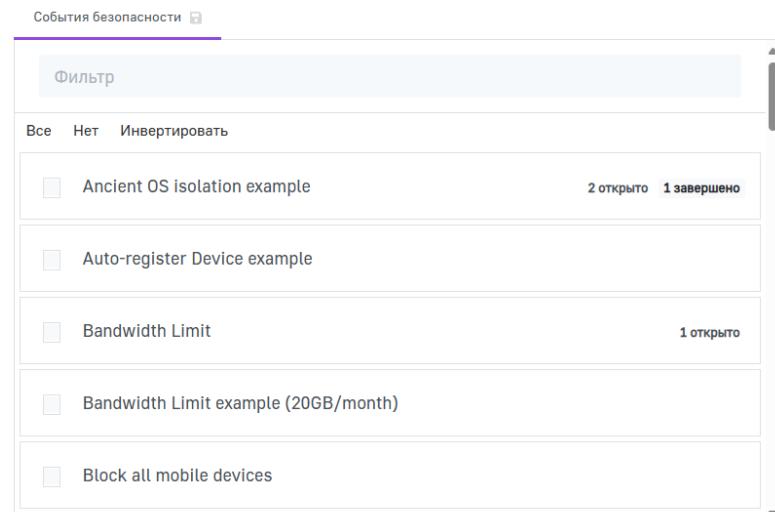
Audio, Imaging or Video Equipment/Axis Communications

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**. Чтобы инвертировать выбранные классы, нажмите **Инвертировать**. Если необходимо отменить выбор, нажмите **Нет**.

События безопасности

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



События безопасности 

Фильтр

Все Нет Инвертировать

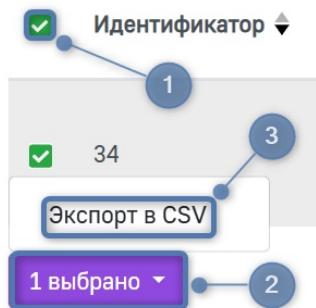
Название	Статус
Ancient OS isolation example	2 открыто 1 завершено
Auto-register Device example	
Bandwidth Limit	1 открыто
Bandwidth Limit example (20GB/month)	
Block all mobile devices	

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

Для того чтобы выбрать все события безопасности, нажмите **Все**. Чтобы 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/>