Журнал событий

Все события в сети НЕЙРОСС регистрируются и передаются другим узлам сети. Журнал событий Платформы НЕЙРОСС позволяет хранить записи обо всех событиях в системе за последние 5 лет. Журнал событий контроллера БОРЕЙ позволяет хранить до 1000 событий.

Переход к функционалу: Рабочий стол НЕЙРОСС > События

Содержание:

- Отличие журнала событий от системного журнала
- Окно раздела
- Фильтрация событий
- Лента событий
- Экспорт событий
- Примеры отбора событий
- Особые условия

Общие сведения

Журнал событий позволяет просматривать вновь возникающие события в режиме реального времени, а также выполнять расширенный поиск архивных событий. Результаты поиска можно отфильтровать по временному интервалу, источнику события (конкретному элементу, например, — от точки доступа), узлу системы, пропуску и другим критериям и выгрузить в файл формата CSV для последующего просмотра и редактирования в программах Microsoft Excel, Libre Office и других. При необходимости вывода событий в виде стандартных отчётов рекомендуется использовать приложение АРМ НЕЙРОСС Отчёты.

Для получения событий в реальном времени используйте вкладку **Живой журнал** , для поиска прошедших событий используйте вкладку **История**.

В версии 20,6 Платформы НЕЙРОСС мы полностью мы полностью переработали интерфейс приложения журнала событий, добавив возможность вывода событий всех узлов сети с функцией фильтрации по домену и по меткам (по принципу включает/исключает), также остались доступны фильтры по названию события, источнику, и выбранным пропускам. Теперь это по настоящему мощный инструмент просмотра событий узлов НЕЙРОСС. Вы можете видеть все события от всех узлов НЕЙРОСС, а также отслеживать события ONVIF ip-видеокамер, в том числе, — события встроенной в камеру видеоаналитики. Любую выборку событий вы можете экспортировать в файл формата CSV и превратить в полноценный отчёт, добавив оформление в выбранном вами редакторе.

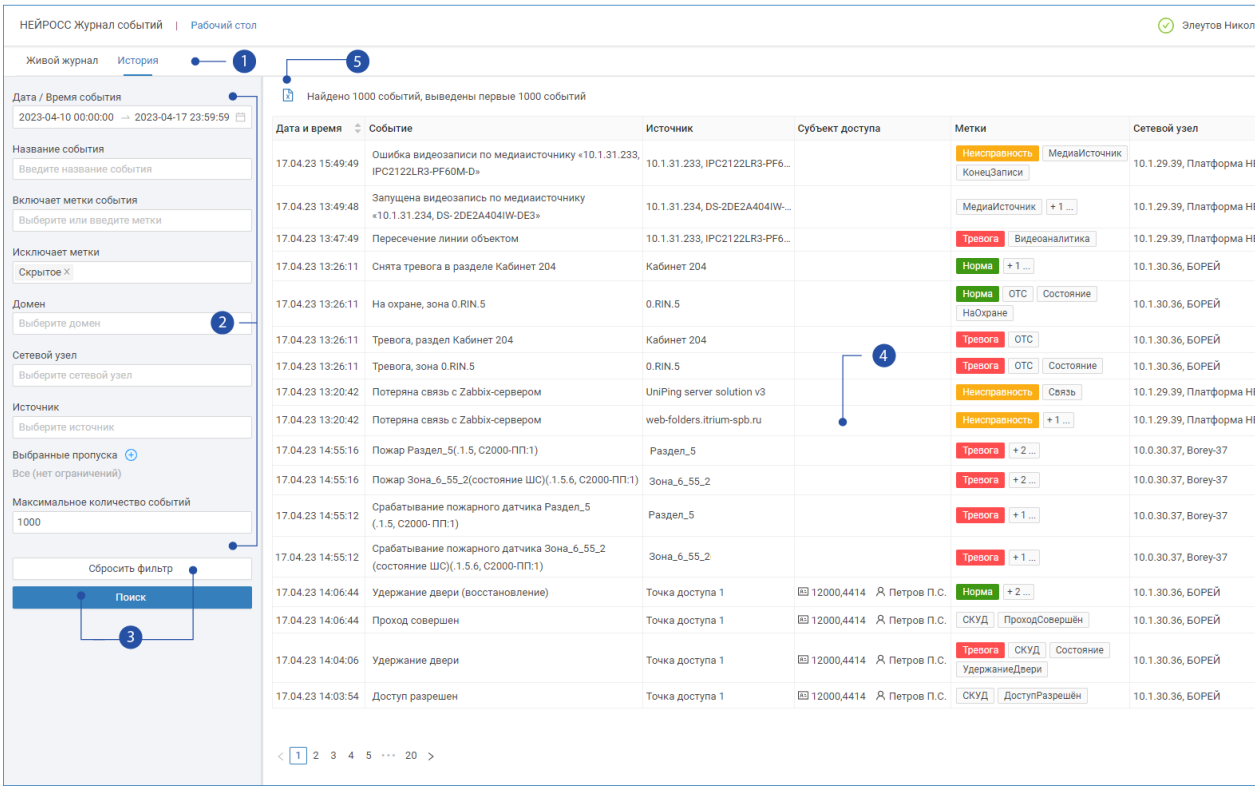
Под учётной записью **root** возможен поиск только событий текущего узла (узла, под IP-адресом которого выполнен вход в интерфейс). Для поиска среди всех событий сети НЕЙРОСС выполните авторизацию под «облачной» учётной записью с правами общего конфигурирования [Пользователи, роли и права].

Отличие журнала событий от системного журнала

Журнал событий — универсальное средство поиска событий узлов НЕЙРОСС и их дочерних элементов: точек доступа, разделов сигнализации, помещений, планов, позволяет отслеживать события доступа (в том числе по конкретному пропуску), тревоги, неисправности и другие события, которыми обмениваются узлы НЕЙРОСС и ONVIF-камеры.

Системный журнал — универсальное средство диагностики проблем Платформы НЕЙРОСС, которое предназначено для отслеживания системных событий и действий пользователей (в том числе, — операторов АРМ НЕЙРОСС).

Окно раздела



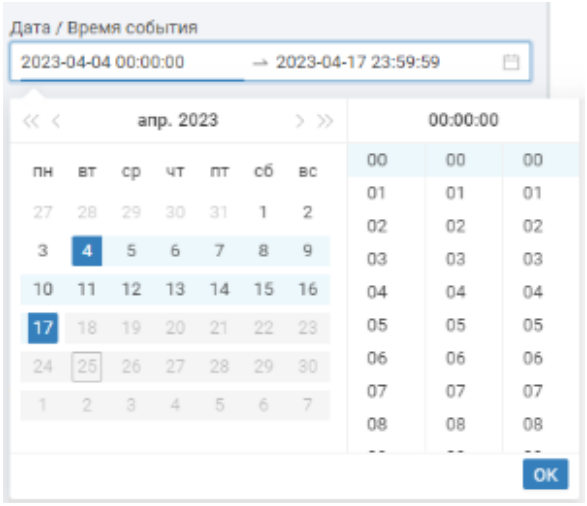
1. **Вкладки переключения**: вкладка Живой журнал предназначена для получения событий в режиме реального времени, вкладка **История** предназначена для поиска по всем событиям.
2. **Фильтр журнала событий**: [Фильтрация событий]
3. **Кнопки управления**: Сбросить фильтр — очистить поля фильтра, Поиск — запустить поиск по заданному фильтру.
4. **Список событий**: события, удовлетворяющие фильтру

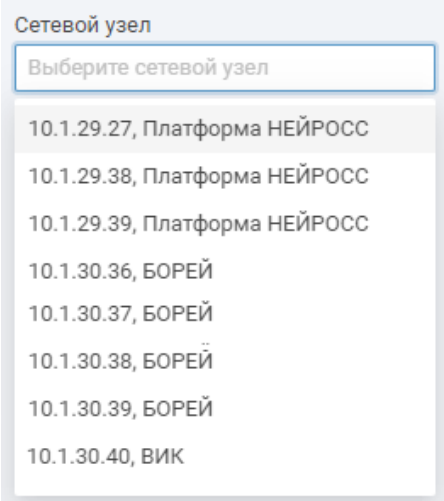
> Полный JSON события вы можете просмотреть в поле **Дополнительная информация о событии**. Нажмите на кнопку .

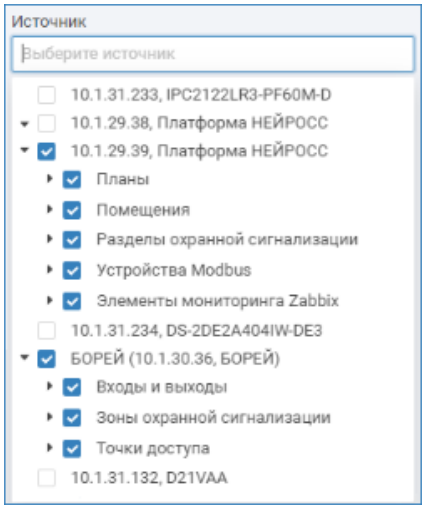
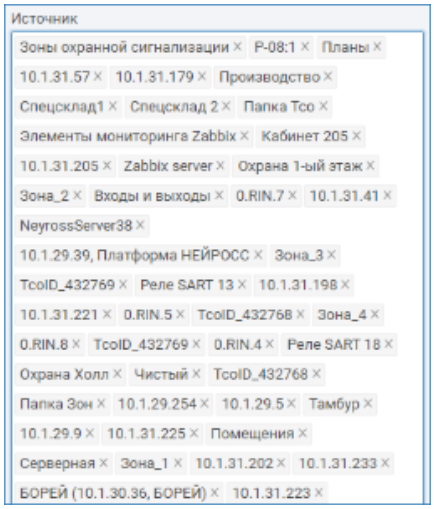
5. **Экспорт событий**: данные по событиям, отображённым в окне в текущее время будут выгружены в файл в формата CSV.

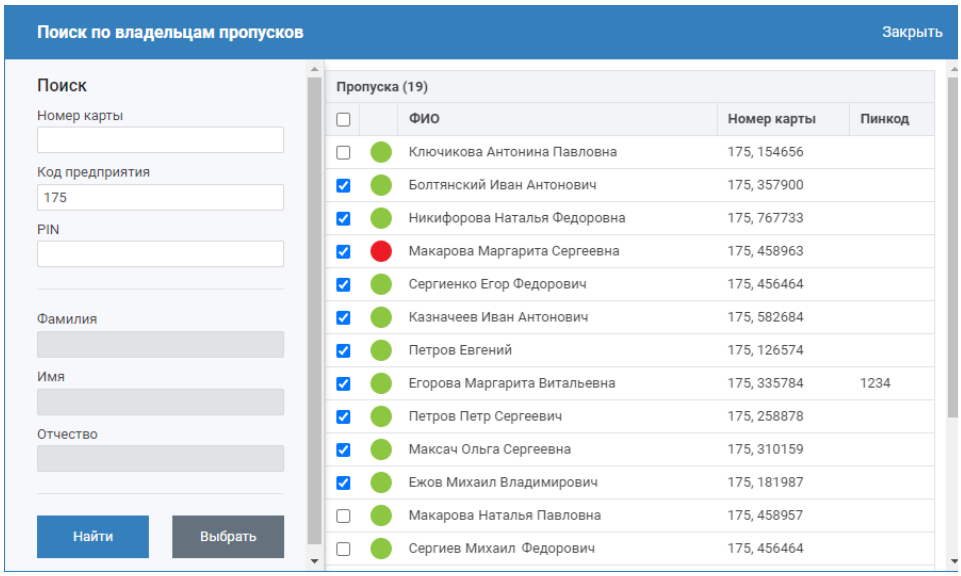
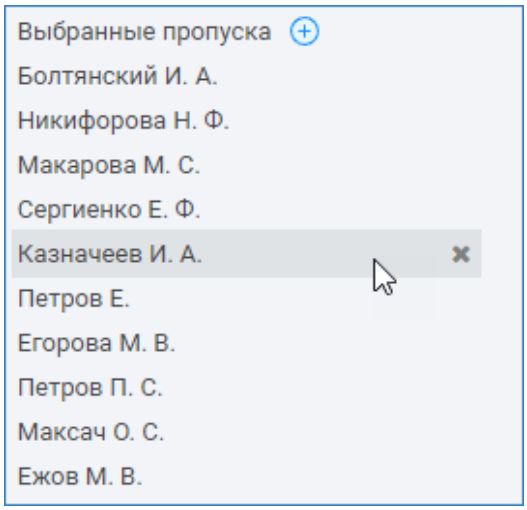
Фильтрация событий

Перечень полей фильтра приведён в таблице ниже.

Поле фильтра	Комментарий
Дата/время события	Необходимо указать начальную и конечную дату/время интервала. Вы можете ввести значение вручную в формате ГГГ ММ-ДД ЧЧ:ММ:СС или воспользоваться элементом **Календарь**. Чтобы открыть календарь щелкните левой клавиши мыши в пол Задайте дату и время точки начала и окончания интервала, затем нажмите на кнопку **ОК**. 
Название события	Поиск по любому слову сообщения о событии (не зависит от регистра символов).
Включает метки события, множественный выбор	Поиск по стандартным и пользовательским меткам события. Обратите внимание, что наборы меток элементов, состояний и событий отличаются! Если вам требуются найти события какого то типа, найдите одно такое событие, просмотрите метки и задайте их в данном поле. Если задано несколько меток, будут выведены только события, содержащие каждую из указанных меток. Примеры меток событий: ОТС (события охранно-тревожной сигнализации), СКУД (события контроля и управления доступом Видеоаналитика (события видеоаналитики), МедиаИсточник (события начала/остановки записи и проч).
Исключает метки, множественный выбор	Исключение событий с указанными метками (как стандартными так и пользовательскими). Если задано несколько меток, отбрасываются события, содержащие хотя бы одну из указанны меток.

Домен, множественный выбор	Домены — объединение нескольких узлов в группу, устанавливающую правило фильтрации (отбрасывания) сетевь сообщений. Благодаря этому узел обменивается событиями только от узлов в том же домене, что и он сам, а остальные игнорирует. Это позволяет поддерживать несколько независим и несвязанных групп контроллеров в одной подсети, и распределять информационную нагрузку на узлы. При необходимости вывода событий только от узлов в подгрупп объединённой доменом, укажите имя домена. **ВАЖНО** Текущий узел (узел, с IP-адреса которого выполнен вход в приложение) должен принадлежать данному домену [Что такое Сеть НЕЙРОСС, узел НЕЙРОСС?].
Сетевой узел	Поиск событий по сетевому узлу (в поле **DEVICE** и **NETWORKNODE** JSON события указан узел). **Важно** Источником события может быть не сам узел, а его дочерний элемент, например, — раздел сигнализации, помещение или элемент Zabbix, например, — узел Платформа НЕЙРОСС является источником событий потери связи, конфликтов ресурсов, ошибок лицензии, ошибок видеозаписи, событий видеоаналитики и проч. В этом случае воспользуйтесь фильтром по источнику. 

Источник	Поиск событий по источнику (в поле **SOURCE** и **ONVIFSOURCE** JSON события указан выбранный источник). При выборе выбор элемента, автоматически выбираются все его дочерние элементы. Вы можете откорректировать список, удалив лишние  

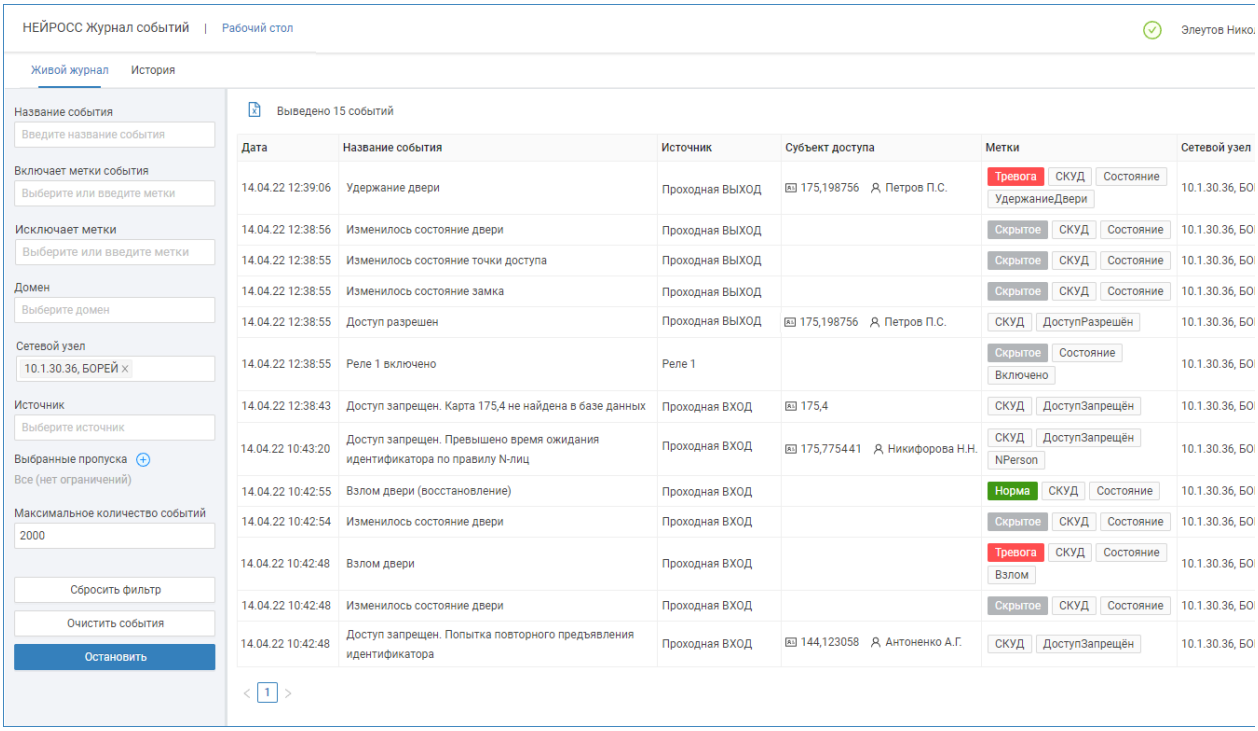
Выбранные пропуска, множественный выбор	Поиск событий доступа по одному или нескольким пропускам. Нажмите на кнопку ⊕ **Добавить пропуска**. Возможен поиск по карте или по владельцу. Задайте фильтр, нажмите **Найти**. Выберите требуемые пропуска и нажмите на кнопку **Выбрать**.  Выбранные пропуска отобразятся в окне фильтра. Вы можете откорректировать список, удалив лишние. 
Максимальное количество событий	Целое число. По умолчанию отображается последние 100 событий. При необходимости отображения большего количеств — увеличьте значение в поле.

Лента событий

На вкладке **Живой журнал** события отображаются в режиме реального времени и могут быть отфильтрованы по названию, меткам, узлу, источнику и/или пропуску.

ВАЖНО

Фильтры применяются немедленно. Если вы не видите каких-то событий, проверьте параметры фильтрации. Кнопка **Очистить** позволяет очистить экран для более удобного просмотра поступающих событий (при этом события не удаляются, их можно отобразить с помощью инструментов вкладки **Поиск**). Для спокойного анализа уже полученных событий используйте кнопку **Остановить**, при этом вывод новых событий будет прекращён.



Кнопки управления: **Сбросить фильтр** — удалить данные в полях всех фильтров, **Очистить события** — очистить окно вывода событий (при этом события не удаляются, их можно отобразить с помощью инструментов вкладки **История**), **Остановить** — прекратить вывод новых событий.

Экспорт событий

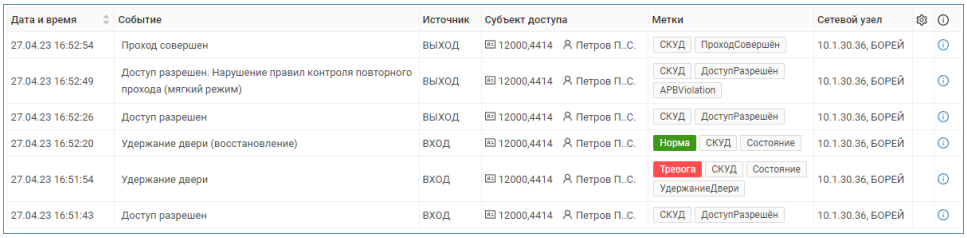
При необходимости экспорта результатов поиска в файл формата CSV для последующего редактирования в MS Excel и др. программах, нажмите на кнопку .

Файл будет сформирован и выгружен в папку загрузок браузера.

Примеры отбора событий

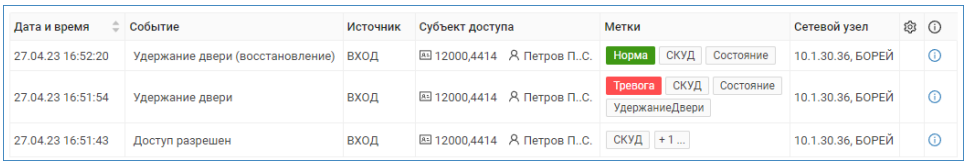
Тема

События доступа по конкретному пропуску



Дата и время	Событие	Источник	Субъект доступа	Метки	Сетевой узел
27.04.23 16:52:54	Проход совершен	ВЫХОД	12000,4414 Петров П..С.	СКУД ПроходСовершён	10.1.30.36, БОРЕЙ
27.04.23 16:52:49	Доступ разрешен. Нарушение правил контроля повторного прохода (мягкий режим)	ВЫХОД	12000,4414 Петров П..С.	СКУД ДоступРазрешён APBViolation	10.1.30.36, БОРЕЙ
27.04.23 16:52:26	Доступ разрешен	ВЫХОД	12000,4414 Петров П..С.	СКУД ДоступРазрешён	10.1.30.36, БОРЕЙ
27.04.23 16:52:20	Удержание двери (восстановление)	ВХОД	12000,4414 Петров П..С.	Норма СКУД Состояние	10.1.30.36, БОРЕЙ
27.04.23 16:51:54	Удержание двери	ВХОД	12000,4414 Петров П..С.	Тревога СКУД Состояние УдержаниеДвери	10.1.30.36, БОРЕЙ
27.04.23 16:51:43	Доступ разрешен	ВХОД	12000,4414 Петров П..С.	СКУД ДоступРазрешён	10.1.30.36, БОРЕЙ

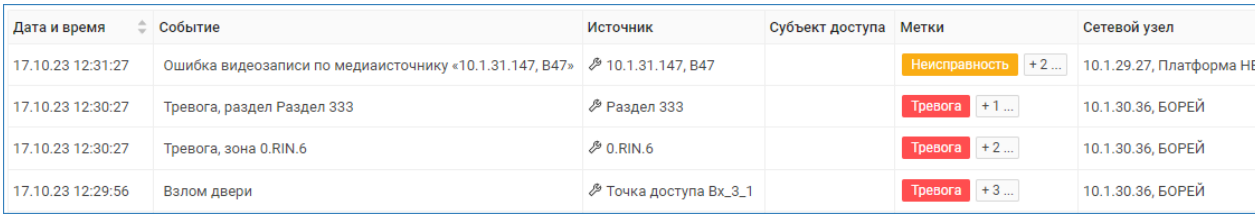
События доступа по конкретному пропуску через заданную точку доступа



Дата и время	Событие	Источник	Субъект доступа	Метки	Сетевой узел
27.04.23 16:52:20	Удержание двери (восстановление)	ВХОД	12000,4414 Петров П..С.	Норма СКУД Состояние	10.1.30.36, БОРЕЙ
27.04.23 16:51:54	Удержание двери	ВХОД	12000,4414 Петров П..С.	Тревога СКУД Состояние УдержаниеДвери	10.1.30.36, БОРЕЙ
27.04.23 16:51:43	Доступ разрешен	ВХОД	12000,4414 Петров П..С.	СКУД +1 ...	10.1.30.36, БОРЕЙ

Особые условия

Если источник события находится в режиме техобслуживания, он помечается значком [Перевод в режим техобслуживания].



Дата и время	Событие	Источник	Субъект доступа	Метки	Сетевой узел
17.10.23 12:31:27	Ошибка видеозаписи по медиаисточнику «10.1.31.147, B47»	10.1.31.147, B47		Неисправность +2 ...	10.1.29.27, Платформа НЕ
17.10.23 12:30:27	Тревога, раздел Раздел 333	Раздел 333		Тревога +1 ...	10.1.30.36, БОРЕЙ
17.10.23 12:30:27	Тревога, зона 0.RIN.6	0.RIN.6		Тревога +2 ...	10.1.30.36, БОРЕЙ
17.10.23 12:29:56	Взлом двери	Точка доступа Вх_3_1		Тревога +3 ...	10.1.30.36, БОРЕЙ