

# Операционная инструкция Аудитора ИБ

## **1. Типовые операции, выполняемые Аудитором ИБ**

Аудитор ИБ участвует в следующих сценариях работы бизнес-системы Нетхаб:

1. «Контроль легитимности сетевых доступов»;

Аудитор ИБ управляет конфигурацией МСЭ и выполняет функции:

1. Выявление изменений настроек МСЭ, реализованных без запроса на управление сетевым доступом.
2. Принятие решения о необходимости регистрации инцидентов ИТ и ИБ в случае выявления

При осуществлении указанных функций Аудитор ИБ выполняет в НЕТХАБ следующие операции:

1. Сбор и анализ данных, формирование отчета об анализе изменений настроек конфигураций МСЭ;
2. Формирование отчета по закрытым запросам на управление сетевым доступом;
3. Анализ несоответствий изменений настроек МСЭ запросам на управление сетевым доступом;
4. Анализ отчета.

При выполнении указанных операций Аудитор ИБ руководствуется инструкциями, описанными в следующих разделах настоящего документа.

### **1.1. Сбор и анализ данных, формирование отчета об анализе изменений настроек конфигураций**

Сбор и анализ данных осуществляется системой Нетхаб автоматически.

#### **1.1.1. Условия выполнения операции**

Данная операция выполняется:

- Требуется проверка легитимности сетевого доступа (по расписанию или внепланово);

#### **1.1.2. Порядок выполнения операции**

##### **1.1.2.1. Подготовительные действия**

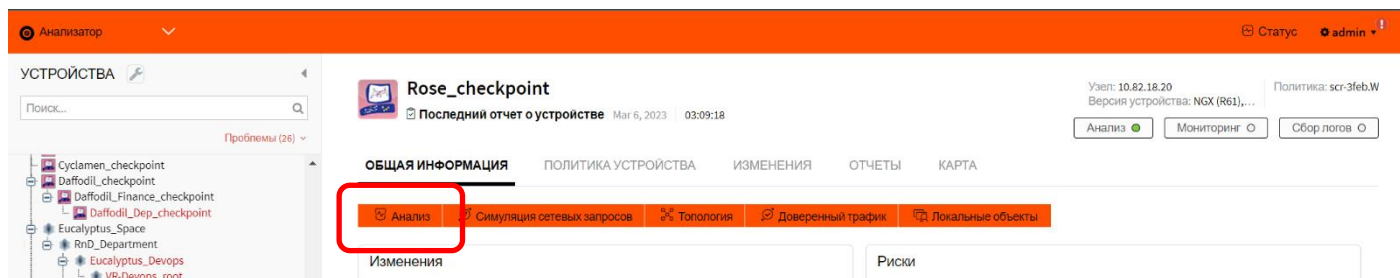
При выполнении операции в случае работы по инциденту проанализировать данные из карточки инцидента и определить идентификаторы связанных с ним МСЭ.

##### **1.1.2.2. Основные действия**

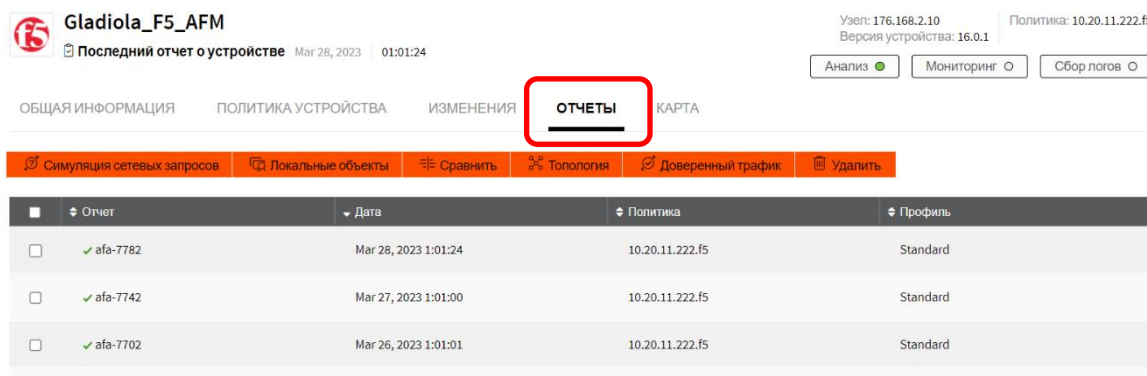
С помощью браузера подключиться к Web-интерфейсу системы Нетхаб.

Для формирования отчета по изменениям настроек МСЭ необходимо воспользоваться отчетом по анализу конфигурации устройств(а) – раздел ИЗМЕНЕНИЯ содержит информацию об обнаруженных системой Нетхаб изменениях.

Для этого необходимо в левом верхнем углу страницы перейти в модуль **Нетхаб Анализатор**, для этого надо нажать символ «V» и в выпадающем списке выбрать **Нетхаб Анализатор**. Перейти в раздел **УСТРОЙСТВА**, выбрать в дереве устройств МСЭ, для которого выполняется операция.



Для запуска анализа конфигурации устройства нажать кнопку **Анализ**, после чего убедиться, что система подготовила новый отчет по устройству – дата и время в поле **Последний отчет о устройстве** должна обновиться. Для просмотра или загрузки отчета необходимо перейти на вкладку **ОТЧЕТЫ** и выбрать интересующий отчет.



Для создания отчета по группе МСЭ необходимо выбрать раздел **ГРУППЫ** и выбрать интересующую группу МСЭ. Для запуска анализа конфигурации устройств группы нажать кнопку **Анализ**, после чего убедиться, что система подготовила новый отчет по устройству – дата и время в поле **Последний отчет о устройстве** должна обновиться. Для просмотра или загрузки отчета необходимо перейти на вкладку **ОТЧЕТЫ** и выбрать интересующий отчет.

### 1.1.2.3. Заключительные действия

Заключительные действия не требуются.

## 1.2. Формирование отчета по закрытым запросам на управление сетевым доступом

Сбор и анализ данных осуществляется системой Нетхаб автоматически.

### 1.2.1. Условия выполнения операции

Данная операция выполняется:

- Требуется проверка легитимности сетевого доступа (по расписанию или внепланово);
- Открыт инцидент, связанный с управлением сетевым доступом.

## 1.2.2. Порядок выполнения операции

### 1.2.2.1. Подготовительные действия

При выполнении операции в случае работы по инциденту ИТАТ проанализировать данные из карточки инцидента ИТАТ и определить идентификаторы связанных с ним запросов на управление сетевым доступом.

### 1.2.2.2. Основные действия

С помощью браузера подключиться к Web-интерфейсу системы Нетхаб. В левом верхнем углу страницы перейти в модуль **Нетхаб Менеджер**, для этого нужно нажать символ «V» и в выпадающем списке выбрать **Нетхаб Менеджер**.

Для формирования отчета по закрытым запросам на управление сетевым доступом необходимо перейти в режим поиска информации о запросах, для этого ввести данные для поиска в поле **Поиск ...** и нажать Enter или открыть страницу расширенного поиска перейдя по ссылке **Расширенный поиск**.

Идентификатор	Тема	Инициатор
29	Change Request to Allow Traffic	admin@netl
17	(Нет заголовка)	admin@netl
21	Change Request to Allow Traffic	admin@netl
4	Change Request to Block Traffic	admin@netl
5	Change Request to Block Traffic	admin@netl

На открывшейся странице выбрать необходимые поля для поиска и указать критерии поиска. При этом, возможно создание сложных конструкций с комбинацией различных условий по логическому AND и OR. Для отображения текущего запроса служит поле **Текущий поиск**. После заполнения поля

## Текущий поиск необходимыми условиями необходимо нажать кнопку

Добавление и поиск.

Добавление и поиск.

Если результат поиска не соответствует ожидаемому, то нужно нажать кнопку **Back** и отредактировать поисковый запрос, после чего выполнить повторный поиск.

Назад

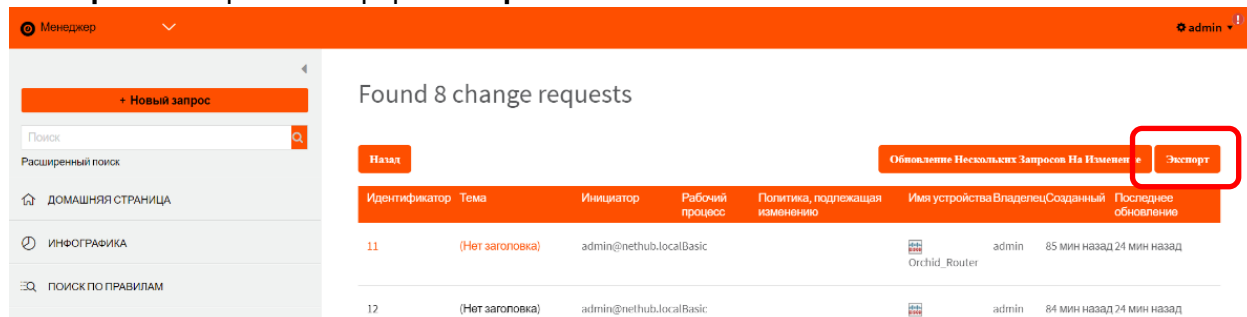
В случае, если планируется повторное использование поискового запроса рекомендуется сохранить сформированный отчет введя имя в поле **Описание**. Также имеется возможность загрузки ранее сохраненного поиска.

Операционная инструкция Аудитора ИБ

Поля для сохранения и загрузки отчетов расположены в нижней части страницы и отображаются после прокрутки содержимого страницы.

#### 1.2.2.1. Заключительные действия

Выгрузить результат выполненного поискового запроса для дальнейшего использования. Для этого на странице с результатами поискового запроса нажать кнопку **Export** и сохранить в формате **Spreadsheet**.



### 1.3. Анализ несоответствий изменений настроек МСЭ запросам на управление сетевым доступом

Данная операция предназначена для выявления несоответствий между внесенными изменениями в конфигурацию МСЭ и запросами на управление сетевым доступом.

#### 1.3.1. Условия выполнения операции

Данная операция выполняется:

- Требуется проверка легитимности сетевого доступа (по расписанию или внепланово);
- Открыт инцидент ИТАТ, связанный с управлением сетевым доступом.

#### 1.3.2. Порядок выполнения операции

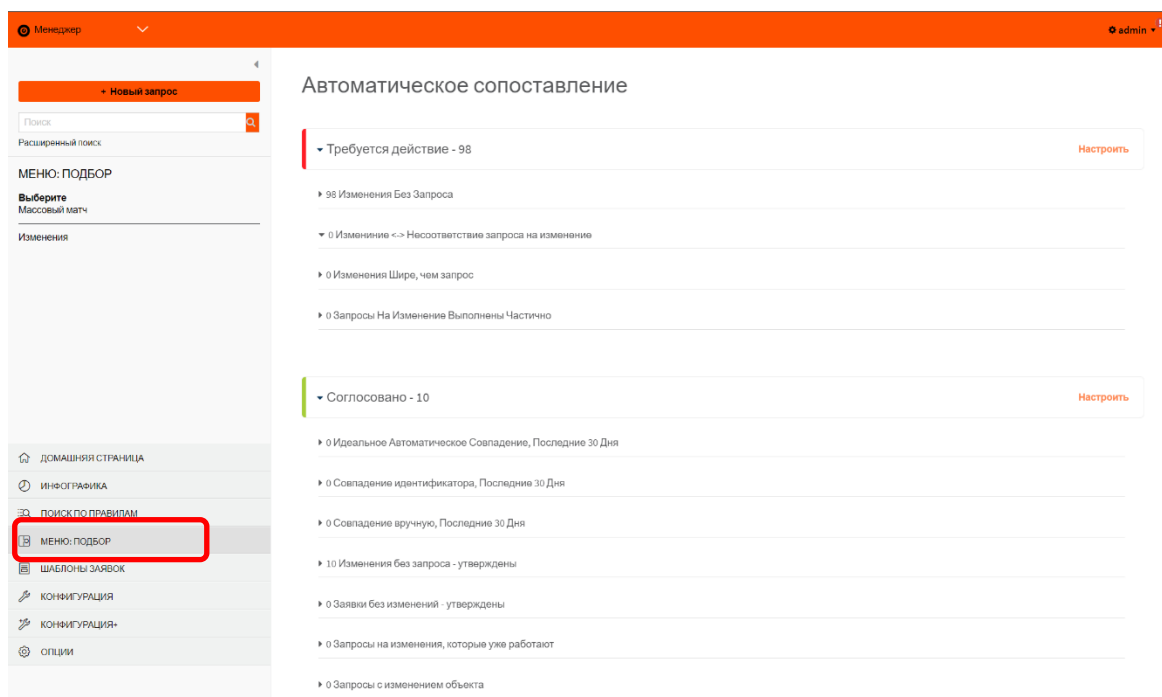
##### 1.3.2.1. Подготовительные действия

При выполнении операции определить идентификаторы связанных запросов на управление сетевым доступом.

##### 1.3.2.2. Основные действия

С помощью браузера подключиться к Web-интерфейсу системы Нетхаб. В левом верхнем углу страницы перейти в модуль **Нетхаб Менеджер**, для этого нужно нажать символ «V» и в выпадающем списке выбрать **Нетхаб Менеджер**.

Перейти в раздел меню **Auto Matching** и проанализировать список выявленных изменений, которые не удалось сопоставить с запросом в системе Нетхаб. Для этого необходимо развернуть список **Action Required**.



При наличии ненулевого количества запросов в следующих пунктах: **Изменения Без Запроса, Изменение <-> Несоответствие запроса на изменение, Изменения Шире, чем запрос**, направить по электронной почте Аналитика МСЭ оповещение о необходимости выполнения операции «Подтверждение легитимности изменения настроек конфигураций МСЭ».

### 1.3.2.3. Заключительные действия

Оповестить Координатора УСД и Аналитика МСЭ о выполнении операции.