

Операционная инструкция аналитика ИБ

1. Типовые операции, выполняемые Аналитиком ИБ

Аналитик ИБ управляет конфигурацией МСЭ и выполняет функции:

1. Проведение оценки опасности маршрута прохождения трафика согласно запросу на изменение сетевого доступа;
2. Принятие решения о возможности изменения сетевого доступа с учетом Профиля риска изменения сетевого доступа.

При осуществлении указанных функций Аналитик ИБ выполняет следующие операции:

1. Оценка опасности маршрута прохождения трафика и согласование.
2. Согласование отклонений реализованных изменений от запрошенных

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

1.1. Оценка опасности маршрута прохождения трафика и согласование

Данная операция предназначена для осуществления оценки опасности запрошенных изменений сетевого доступа и принятия решения о возможности изменения сетевого доступа с точки зрения обеспечения ИБ на уровне сети.

Цель – недопущение внесения изменений в конфигурацию МСЭ, противоречащих принятым в организации правилам, сформулированным в Профиле оценки рисков.

1.1.1. Условия выполнения операции

Данная операция выполняется если:

- Для запроса на управление сетевыми доступами подтвержден маршрут прохождения трафика.

1.1.2. Порядок выполнения операции

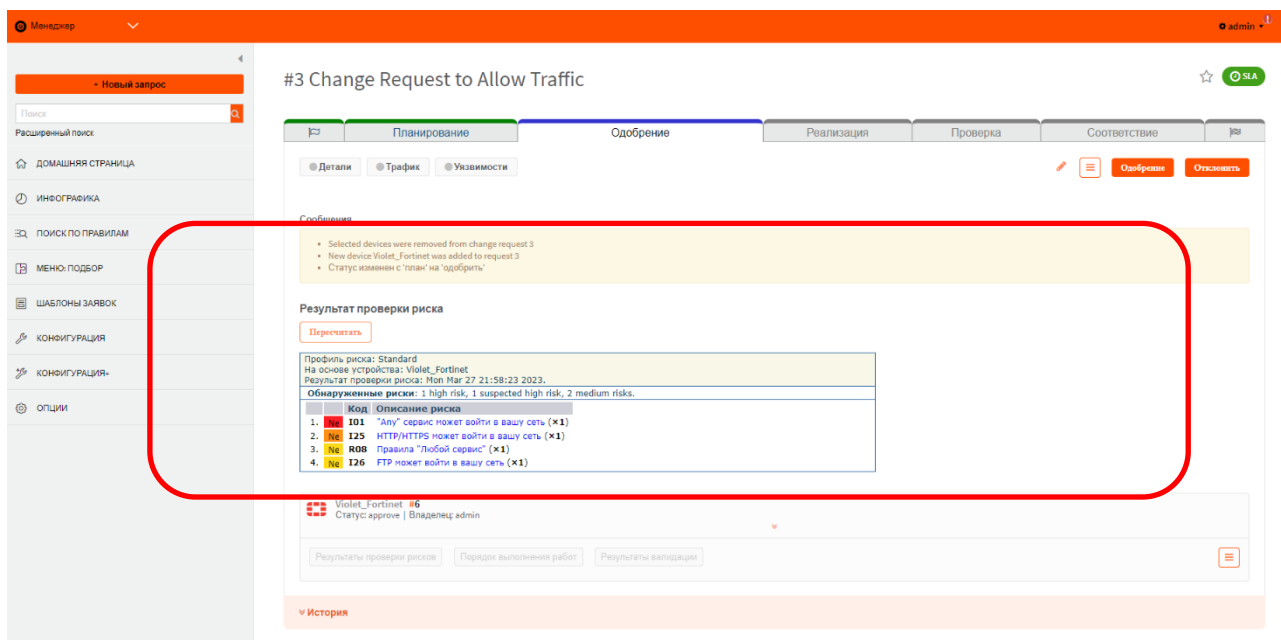
1.1.2.1. Подготовительные действия

Определить идентификатор запроса в НЕТХАБ на основе ранее сохраненных данных или данных из заявки.

1.1.2.2. 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 выполнения операции необходимо перейти по ссылке в карточку запроса или ввести его номер в поле **Поиск**, убедиться, что запрос находится на стадии **Одобрение** и в карточке запроса отображаются созданные подзапросы для внесения изменений на каждом устройстве. Проанализировать заключение системы Нетхаб об опасности маршрута в поле **Результат проверки риска**.



В зависимости от уровня опасности принять решение о возможности выполнения запрошенных изменений:

- Если система Нетхаб пришла к заключению об отсутствии опасности запрошенных изменений, то в поле **Результат проверки риска** отображается вердикт **No risks were found**. В этом случае для согласования запрошенных изменений необходимо нажать кнопку **Одобрение**;
- Если система Нетхаб пришла к заключению о наличии низкого уровня опасности запрошенных изменений, то в поле **Результат проверки риска** отображается вердикт **Обнаруженные риски: low risk** и имеются записи с бежевым цветовым кодом. При необходимости, перейдя по ссылке соответствующего правила в поле **Risk Description**, возможно выполнить более детальный анализ. В этом случае для согласования запрошенных изменений необходимо нажать кнопку **Одобрение**;
- Если система Нетхаб пришла к заключению о наличии среднего уровня опасности запрошенных изменений, то в поле **Результат проверки риска** отображается вердикт **Обнаруженные риски: medium risk** и имеются записи с желтым цветовым кодом. В этом случае необходимо проанализировать причины такого заключения, перейдя по ссылке соответствующего правила в поле **Risk Description**. Далее необходимо направить Инициатору запроса сообщение о необходимости корректировки данных запроса на изменение для соответствия Профилю оценки опасности. Для этого необходимо нажать кнопку **Перепланировка** и указать причины перевода запроса на уточнение, а также требования, которым не соответствуют запрошенные изменения;

- Если система Нетхаб пришла к заключению о наличии высокого уровня опасности запрошенных изменений, то в поле **Результат проверки риска** отображается вердикт **Обнаруженные риски: high risk** или **suspected high risk** и имеются записи с красным или оранжевым цветовым кодом. В этом случае необходимо проанализировать причины такого заключения, перейдя по ссылке соответствующего правила в поле **Risk Description**. Далее необходимо отклонить запрос. Для этого необходимо нажать кнопку **Отклонить** и указать причины отклонения запроса, а также требования, которым не соответствуют запрошенные изменения.

Если в поле **Результат проверки риска** не отображается вердикт системы Нетхаб или Профиль оценки опасности был изменен с момента формирования оценки, то необходимо инициировать повторную оценку путем нажатия на кнопку **Пересчитать**. После чего выполнить повторный анализ заключения системы Нетхаб.

1.1.2.3. Заключительные действия

Проинформировать Администратора ГУСД о завершении выполнения операции

1.2. Согласование отклонений реализованных изменений от запрошенных

В рамках данной операции выполняется согласование отклонений внесенных изменений от согласованных в рамках согласования запроса на изменения сетевого доступа. Согласование выполняется по электронной почте и с использованием НЕТХАБ.

1.2.1. Условия выполнения операции

Данная операция выполняется если:

- Запрос был переведен в статус Validate.

1.2.1.1. Подготовительные действия

Определить идентификатор запроса в НЕТХАБ на основе ранее сохраненных данных или данных из заявки.

1.2.1.2. 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 **Менеджер**.

Для выполнения операции необходимо перейти по ссылке в карточку запроса или ввести его номер в поле **Поиск**. Проанализировать карточку запроса и, если отображается статус **Проверка не удалась** необходимо из данных страницы определить причины такого статуса, после чего принять решение о допустимости отклонения и по электронной почте сообщить о принятом решении Администратору ГУСД.

В случае принятия решения о возможности согласования отклонений в карточке запроса необходимо нажать кнопку **Утвердить**.

В случае принятия решения о недопустимости отклонений в карточке запроса необходимо нажать кнопку **Отклонить** для возврата запроса на стадию Реализация и повторного выполнения изменений.

1.2.1.3. Заключительные действия

Заключительных действий не требуется.