



Петербургский
международный
образовательный
форум



«Интеграция развития инженерных и предпринимательских компетенций школьников: формат, содержание, перспективы»

Мастер-класс

Государственное бюджетное общеобразовательное учреждение лицей №373 Московского района Санкт-Петербурга «Экономический лицей»





XIII Петербургский
международный
образовательный
форум

XIII St. Petersburg
International
Educational Forum



Обучение школьников информационной безопасности с помощью настольного сетевого тренажера НаСТя

Докладчик

Личман Татьяна Борисовна

*учитель информатики
ГБОУ лицей №373
Московского района
Санкт-Петербурга*

28.03.2023 г.



XIII Петербургский
международный
образовательный
форум

XIII St. Petersburg
International
Educational Forum

Особенности обеспечения информационной безопасности в компьютерных сетях

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве

Связь между компонентами осуществляется физически, при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно) и программно, при помощи механизма сообщений.

Обе эти взаимосвязи наглядно представлены в сетевом настольном тренажере НаСТя



XIII Петербургский
международный
образовательный
форум

XIII St. Petersburg
International
Educational
Forum

Знакомимся с настольным сетевым тренажером НаСТя





XIII Петербургский
международный
образовательный
форум

XIII St. Petersburg
International
Educational Forum

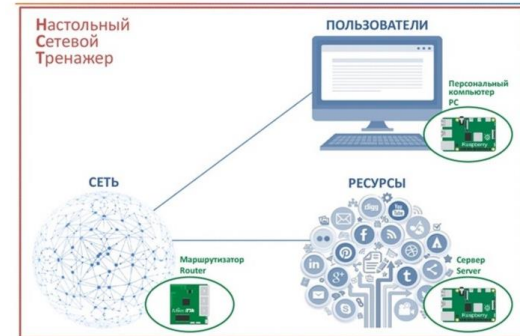
Начинаем работу



Для того чтобы начать работу, надо просто подключить к тренажеру монитор, клавиатуру и мышь.

На корпусе НаСтИ предусмотрены тумблеры подачи/выключения электропитания отдельных сетевых элементов: ПК, маршрутизатор, сервер.

Интернет на столе



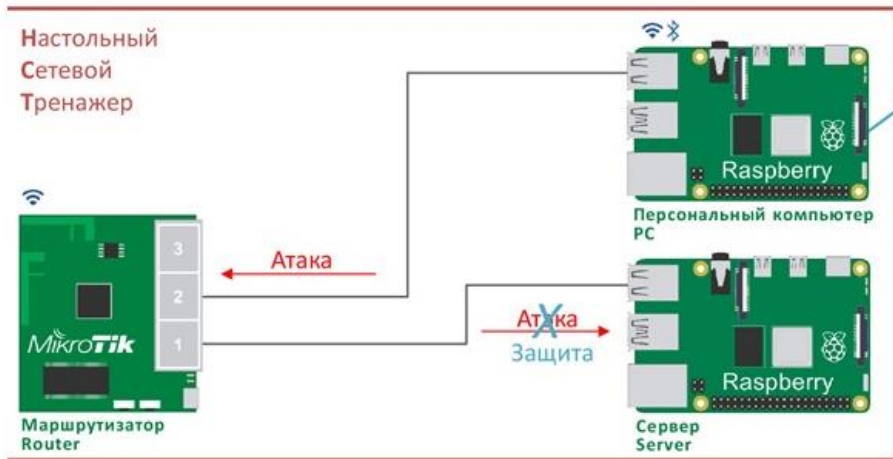
В качестве ПК и сервера используются платы микрокомпьютеров Raspberry Pi 3 Model B+, маршрутизатор – MikroTik hAP mini.

Все элементы сети соединены между собой кабелями для передачи данных по технологии Ethernet.



XIII Петербургский
международный
образовательный
форум

XIII St. Petersburg
International
Educational Forum



*Лабораторные работы
проводятся в замкнутой
контролируемой среде, без
доступа к другим сетям*

Безопасность

- Защита инфокоммуникационных сетей
- Системы обнаружения вторжений
- Имитация сетевых атак различных типов
- Методы защиты от атак

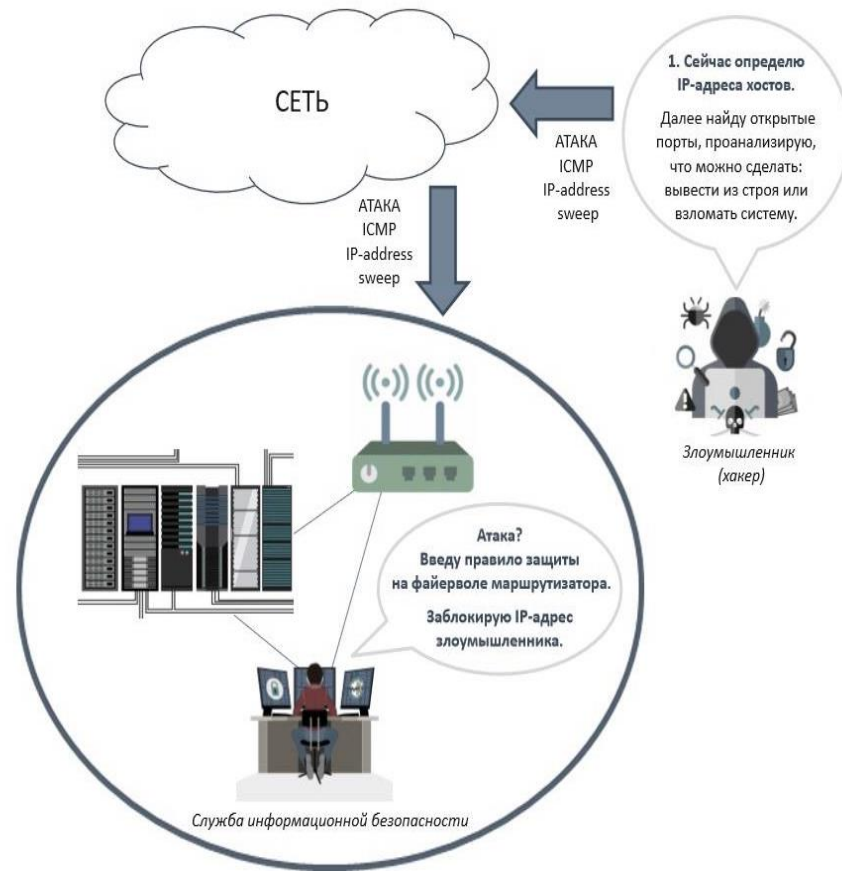


XIII Петербургский
международный
образовательный
форум

XIII St. Petersburg
International
Educational Forum

ЗАЩИТА ОТ АТАКИ ICMP

Лабораторная работа





XIII Петербургский
международный
образовательный
форум

XIII St. Petersburg
International
Educational Forum

Ход проведения лабораторной работы

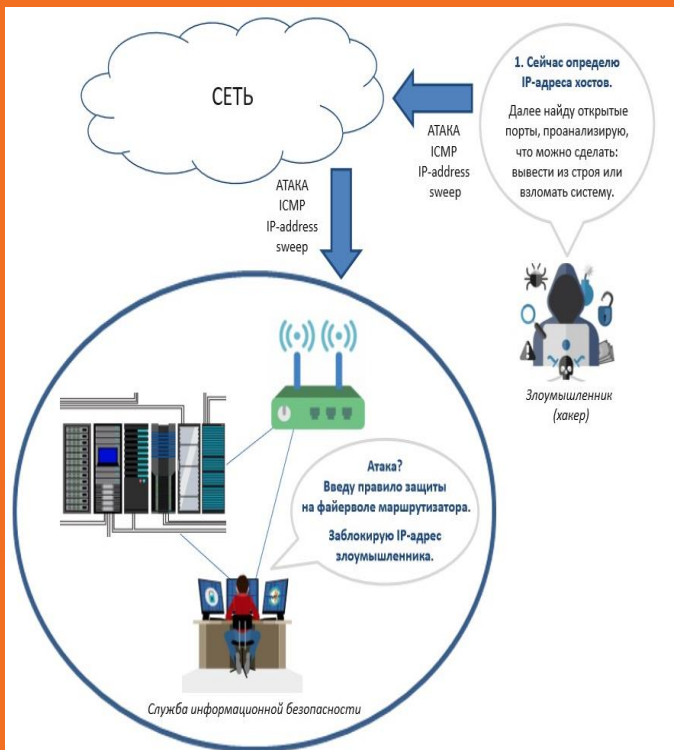


1. Подготовка: убедиться, что на маршрутизаторе и сервере не настроена защита от атаки.
 2. Запустить сканирование сети (злоумышленник).
 3. Проанализировать обнаруженные устройства в сети (злоумышленник).
 4. Обнаружить атаку, настроить защиту на файрволе маршрутизатора Mikrotik от ICMP сканирования сети (сотрудник ИБ).
 5. Проверить (сотрудник ИБ) :
 - Был ли заблокирован злоумышленник? Файервол маршрутизатора внес IP-адрес злоумышленника в черный список?
 - Заблокирован только IP- адрес злоумышленника?
- Если п.5 выполнен, защита проведена верно.



XIII Петербургский
международный
образовательный
форум

XIII St. Petersburg
International
Educational Forum



Самостоятельно:

Проверить наличие доступа в сеть
(используя встроенный браузер)

Повторить п.1,2,3 из лабораторной работы

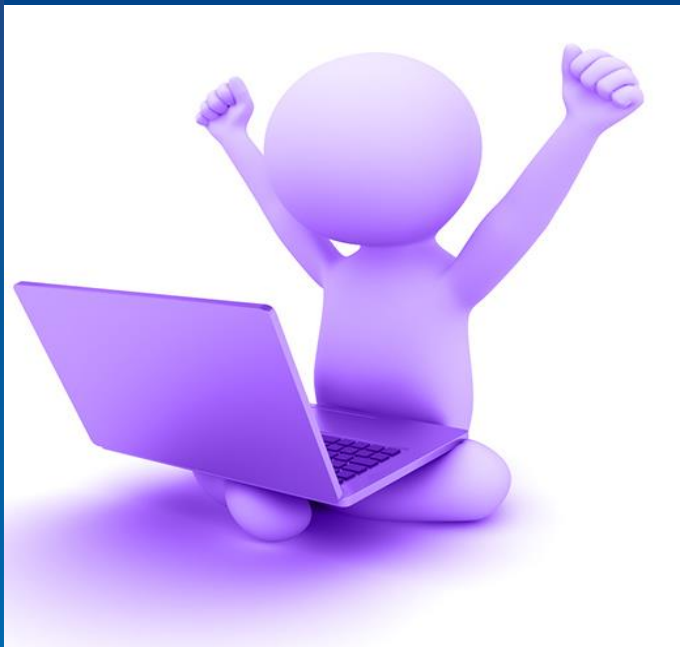
Обнаружить атаку, настроить защиту на
фаерволе маршрутизатора Mikrotik от
ICMP сканирования сети таким образом,
чтобы полностью блокировать доступ в сеть

Проверить (сотрудник ИБ) : Был ли
заблокирован доступ в сеть?



ХIII Петербургский
международный
образовательный
форум

XIII St. Petersburg
International
Educational Forum



Спасибо за внимание!

