

# MikroTik Certified Security Engineer

MTCSE

## *Chapter 1: Basic security*

Базовые  
понятия

Threats  
Угрозы

SECURITY  
DEPLOYMENT



**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-07

## Security basic 1 : **Confidentiality**

**Конфиденциальность** — необходимость предотвращения разглашения, утечки какой-либо информации.

**Конфиденциальная информация** — информация, являющаяся конфиденциальной, то есть «доверительной, не подлежащей огласке, секретной»; это понятие равнозначно с понятиями тайны или секрета

## Security basic 1 : **Integrity**

**Целостность информации** — условие того, что данные не были изменены при выполнении любой операции над ними, будь то передача, хранение или представление.

- статическая целостность (понимаемую как неизменность информационных объектов)
- динамическая целостность (относящуюся к корректному выполнению сложных действий)

## Security basic 1 : **Availability**

**Доступность** — обеспечение своевременного и надежного доступа к использованию информации

Информационные системы используются для получения определенных информационных услуг (сервисов). Если по тем или иным причинам получение этих услуг пользователями становится невозможным, это наносит ущерб всем субъектам информационных отношений

## Security basic 2 : **Prevention**

**Профилактика** — проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ, проведение разъяснительной работы по ИБ среди пользователей (обучение) и т.д.

Самое слабое звено в структуре информационной безопасности – это **человек**; можно создать надежную систему защиты и написать очень подробные инструкции по безопасности, однако халатное обращение сотрудников с важными сведениями, их доверчивость и беспечное поведение способны свести на нет все усилия

*Социальная инженерия в информационной безопасности\**

## Security basic 2 : **Detection**

**Обнаружение атак** — система мониторинга, учета событий и обнаружения потенциально возможных атак и аномалий.

Зачастую атаки на информационную систему (ИС) происходят постепенно: проникновение в обход политик информационной безопасности (ИБ), распространение в ИС с уничтожением следов своего присутствия и только потом непосредственно атака. Весь процесс может занять несколько месяцев, или даже лет. **Зачастую ни пользователь, ни администратор ИБ не подозревают об аномальных изменениях в системе и проводимой на нее атаке**

## Security basic 2 : **Reaction**

**Реакция** — факты об инциденте являются ключевой информацией для выбора ответной реакции и методов восстановления после инцидента

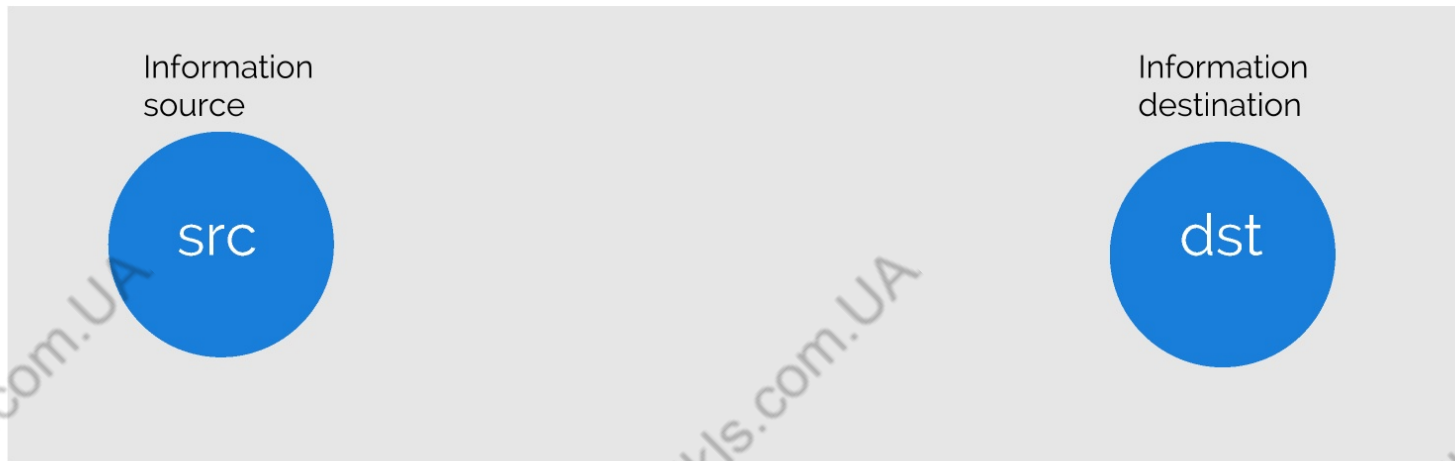
## Security basic 3 : **Attacks, Mechanisms & Services**

**Security Attack** : Any action that compromises the security of information

**Security Mechanism** : a process / device that is designed to detect, prevent or recover from a security attack.

**Security Service** : a service intended to counter security attacks, typically by implementing one or more mechanisms.

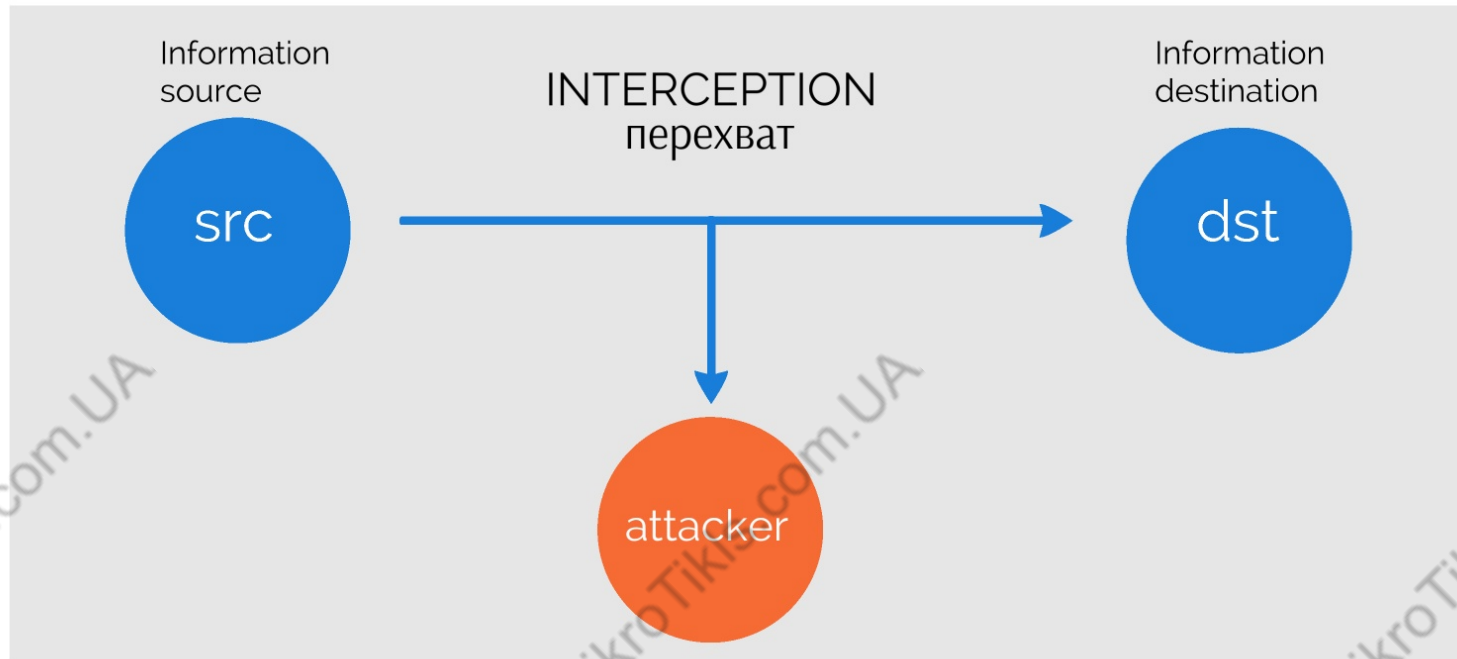
## Security basic: **Attacks**



## Security basic: **Attacks**

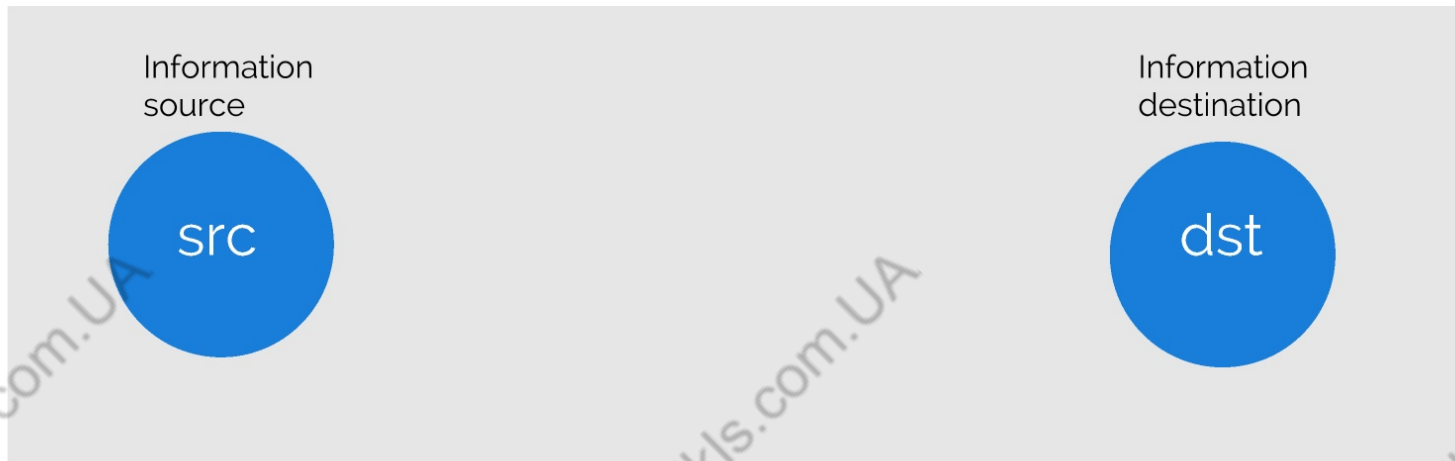


## Security basic: **INTERCEPTION**



«Несанкционированный субъект получил доступ к объекту, например, кража данных, подслушивающих чужое сообщение и т. д. »

## Security basic: **INTERRUPTION**



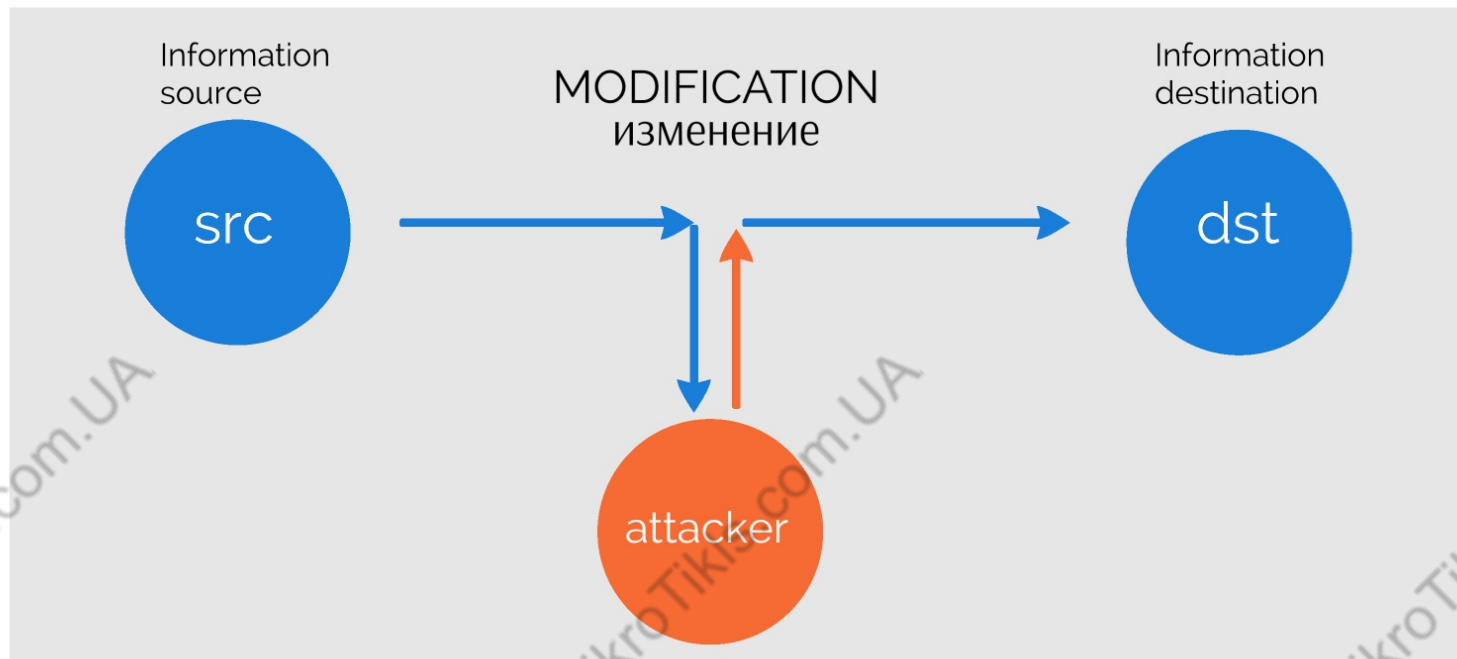
«Услуги или данные становятся недоступными, непригодными для использования, уничтожаются и т. д., Такие как потеря файла, отказ в обслуживании и т. д. »

## Security basic: **INTERRUPTION**



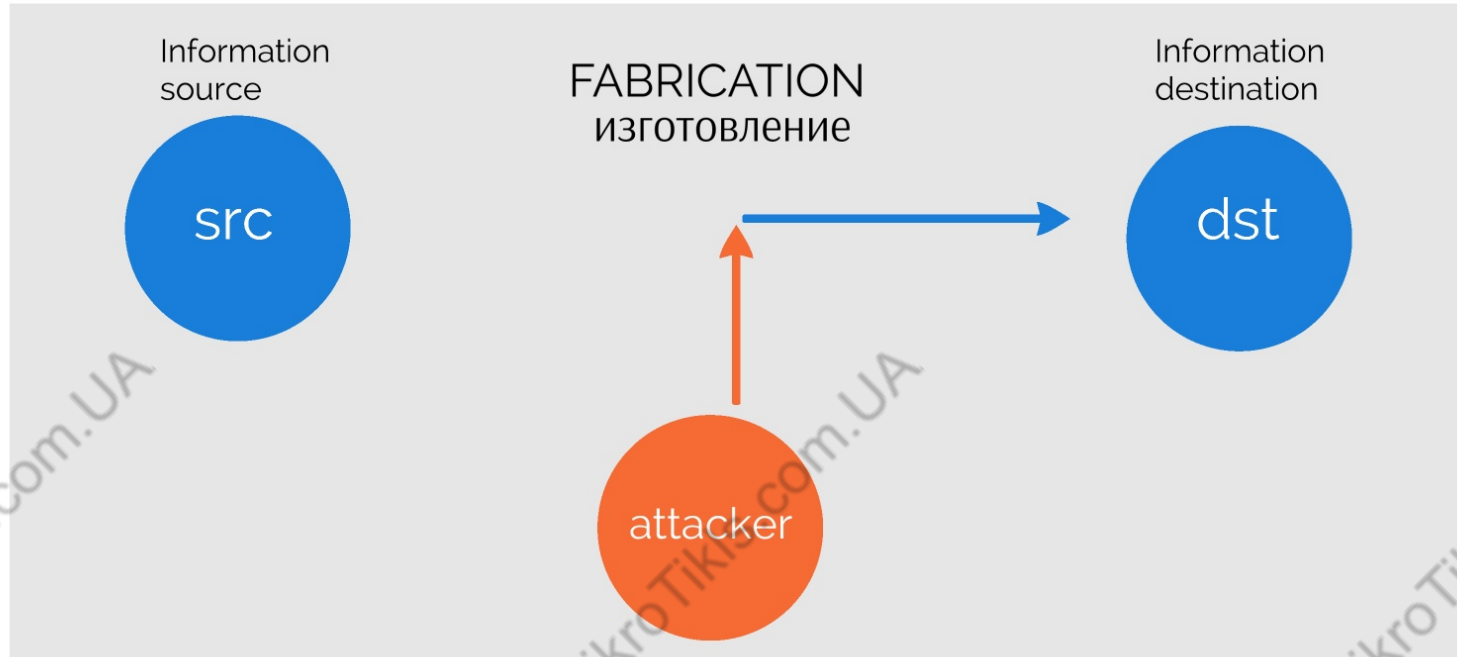
«Услуги или данные становятся недоступными, непригодными для использования, уничтожаются и т. д., Такие как потеря файла, отказ в обслуживании и т. д. »

## Security basic: **MODIFICATION**



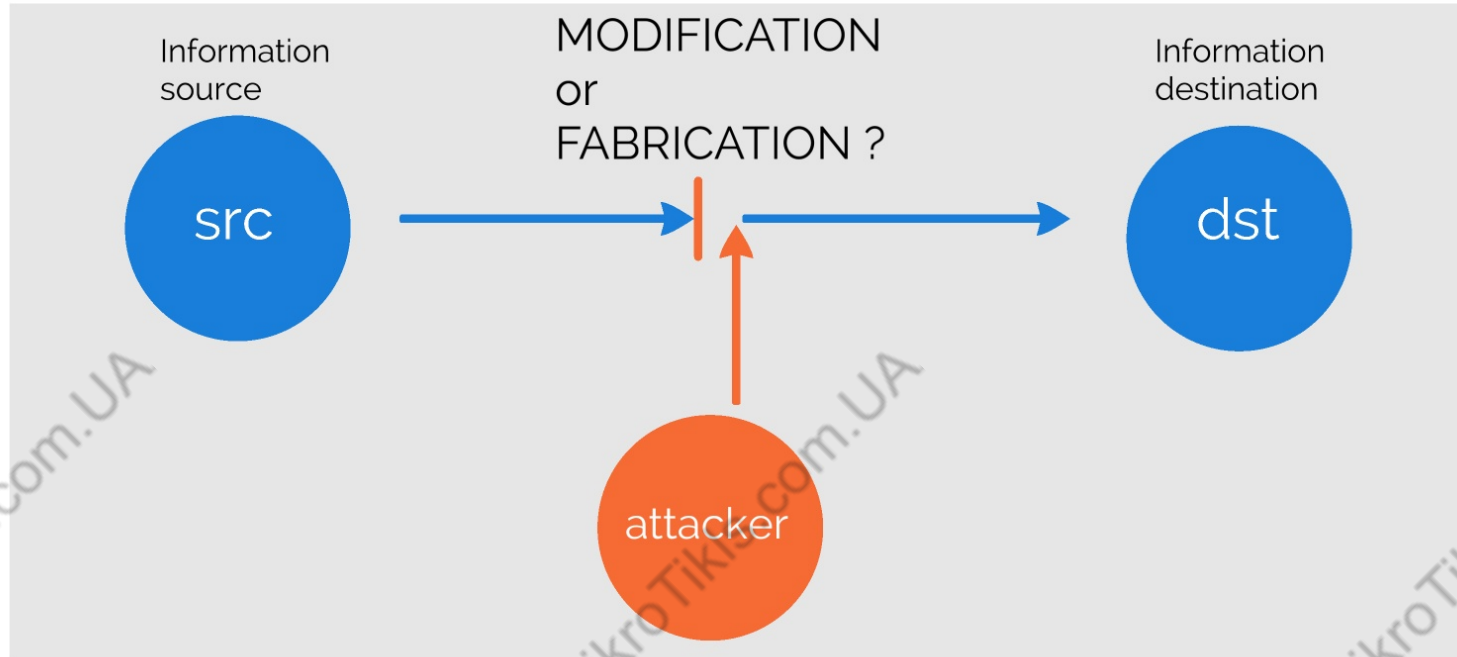
несанкционированное изменение данных

## Security basic: **FABRICATION**

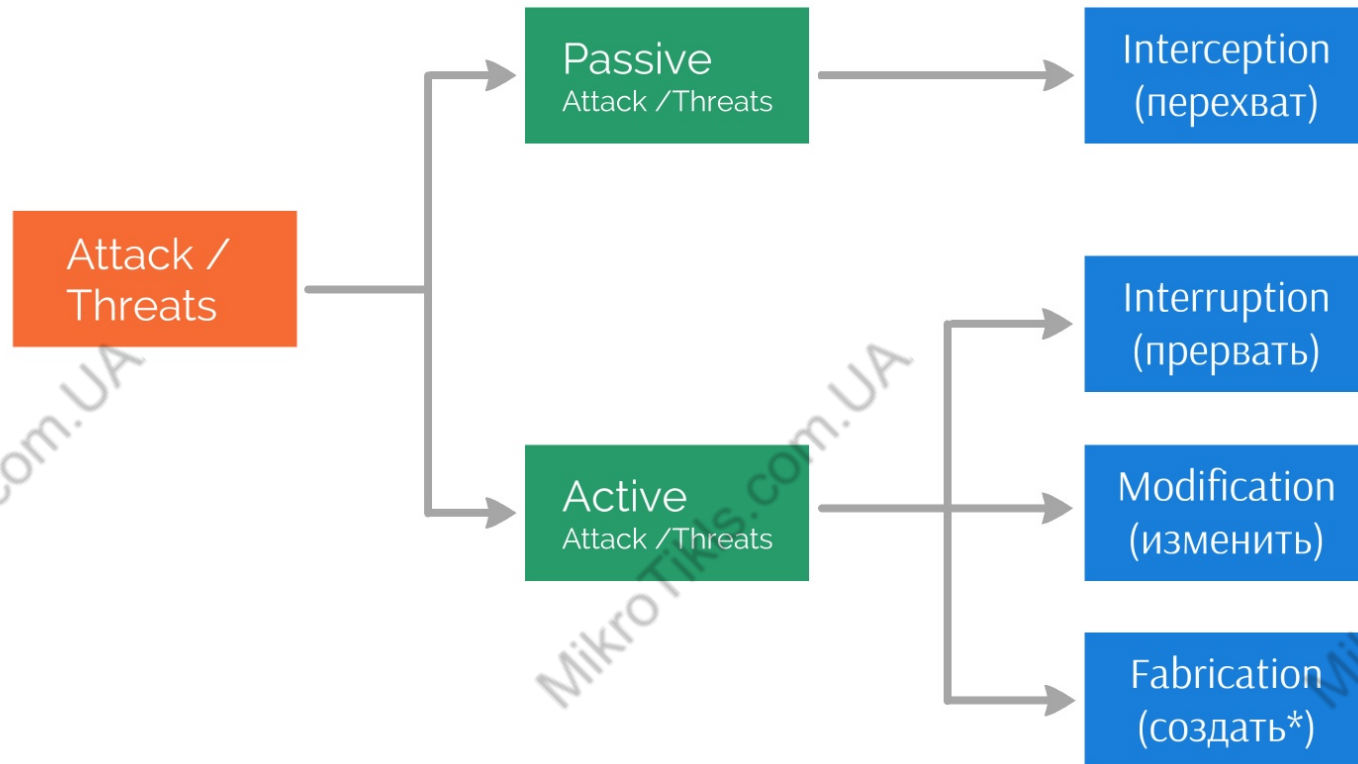


Генерируются дополнительные данные или действия, которые обычно не существуют

## Security basic: **MODIFICATION / FABRICATION**



## Security basic: **Attacks**



## Security basic: **Security Mechanisms**


- **Encryption** :преобразование данных в нечто, что злоумышленник не может понять (опционально - предоставление пользователю возможности проверить, были ли данные изменены)
- **Authentication** : процедура проверки подлинности, доказательство что пользователь именно тот, за кого себя выдает. пароль и т. д.
- **Authorization** : проверка, имеет ли субъект право на выполнение запрошенного действия(предоставление определённых прав.).
- **Auditing** : tracing which subjects accessed what, when, and which way. In general, auditing does not provide protection, but can be a tool for analysis of problems.

Идентификация, аутентификация и авторизация – три процесса - понимание

- **Идентификация** –
- **Аутентификация** –
- **Авторизация** –

Идентификация, аутентификация и авторизация – три процесса - понимание

- **Идентификация** – процесс распознавания пользователя по его идентификатору
- **Аутентификация** –
- **Авторизация** –

Идентификация: 

Это может быть логин,  
имя и фамилия, адрес  
электронной почты или  
номер мобильного  
телефона

Идентификация, аутентификация и авторизация – три процесса - понимание

- **Идентификация** – процесс распознавания пользователя по его идентификатору
- **Аутентификация** – процедура проверки подлинности, доказательство что пользователь именно тот, за кого себя выдает.
- **Авторизация** –

Идентификация:



Аутентификация:



Это может быть логин, имя и фамилия, адрес электронной почты или номер мобильного телефона

Нужно доказать, что он является человеком, который регистрировался под этим идентификатором

Идентификация, аутентификация и авторизация – три процесса - понимание

- **Идентификация** – процесс распознавания пользователя по его идентификатору
- **Аутентификация** – процедура проверки подлинности, доказательство что пользователь именно тот, за кого себя выдает.
- **Авторизация** – предоставление определённых прав.

Идентификация:



Аутентификация:



Авторизация:

Это может быть логин, имя и фамилия, адрес электронной почты или номер мобильного телефона

Нужно доказать, что он является человеком, который регистрировался под этим идентификатором

Если пара "логин-пароль" верны, то система предоставит пользователю доступ к его ресурсам, то есть произойдет авторизация.

# MikroTik Certified Security Engineer

MTCSE

## *Chapter 1: Basic security*

Базовые  
понятия

Threats  
Угрозы

SECURITY  
DEPLOYMENT



MTI-GROUP LLC / network academy

V.21-07

# COMMON THREATS

угрозы

## Security basic: **THREATS - Botnet**



Ботнет - группа компьютеров(устройств), которые были заражены вредоносным ПО и попали под контроль злоумышленника.

Термин «ботнет» - произошел от слов «робот и сеть», и каждое зараженное устройство называется ботом.

Ботнеты могут быть предназначены для выполнения незаконных или злонамеренных задач, включая рассылку спама, кражу данных, вымогателей, мошенническое нажатие на рекламу или распределенные атаки типа «отказ в обслуживании» (DDoS).

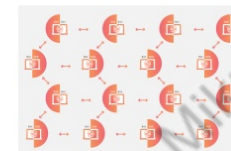
## Security basic: **THREATS - Botnet**

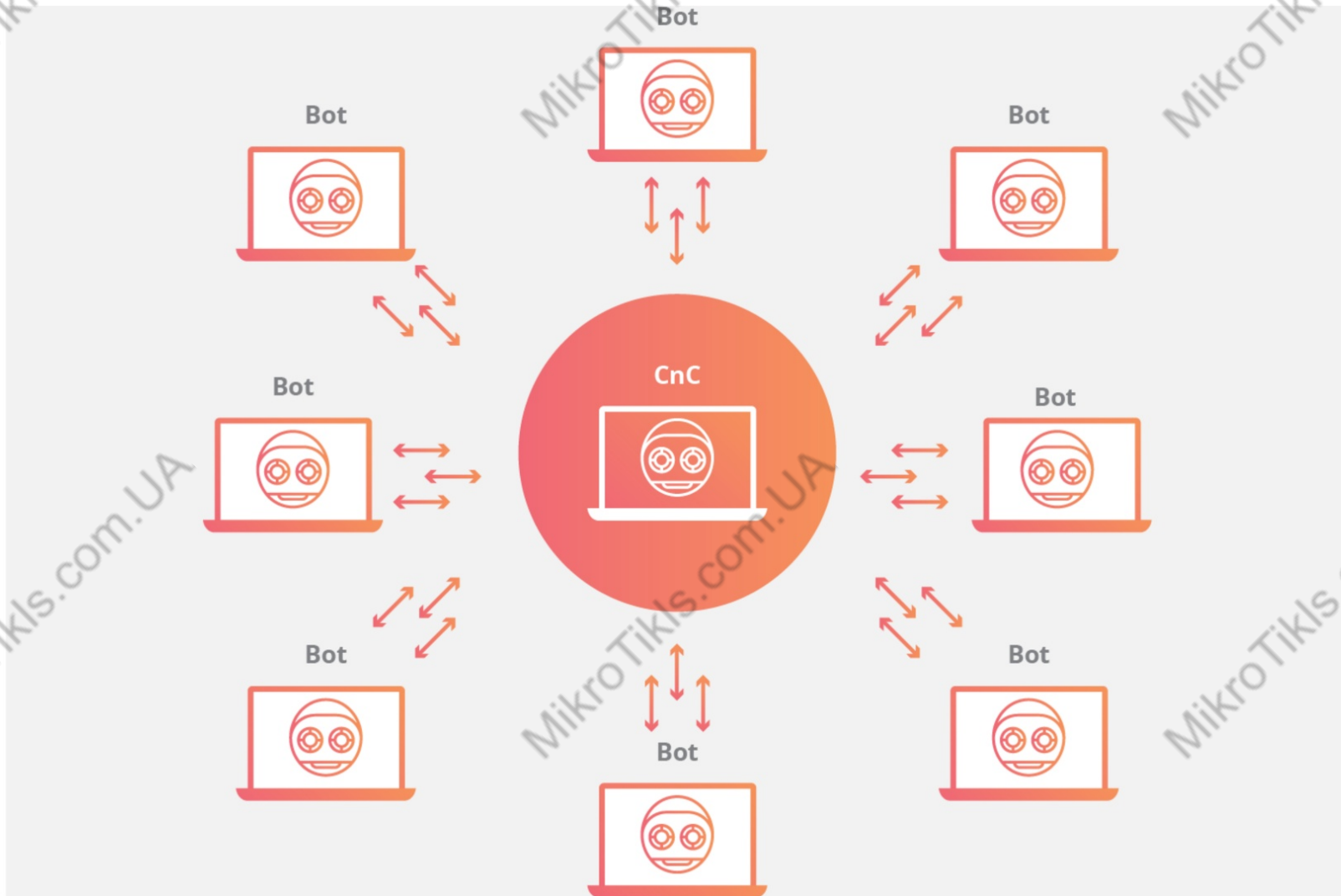
В то время, как некоторые вредоносные программы, такие как вымогатели, будут оказывать непосредственное влияние на владельца устройства, вредоносная программа DDoS-ботнета может иметь различные уровни видимости; некоторые вредоносные программы предназначены для полного контроля над устройством, в то время, как другие вредоносные программы выполняются в фоновом режиме, в режиме ожидания, в то время как они молча ожидают инструкций от злоумышленника или “bot herder”.

## Security basic: **THREATS - Botnet**

Конструкции ботнетов различны, но управляющие структуры можно разделить на две основные категории:

- The client/server botnet model
  - Star Network Topology
  - Multi Server Network Topology
  - Hierarchical Network Topology
- The peer-to-peer botnet model

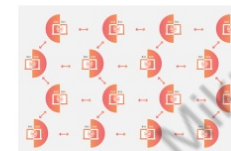


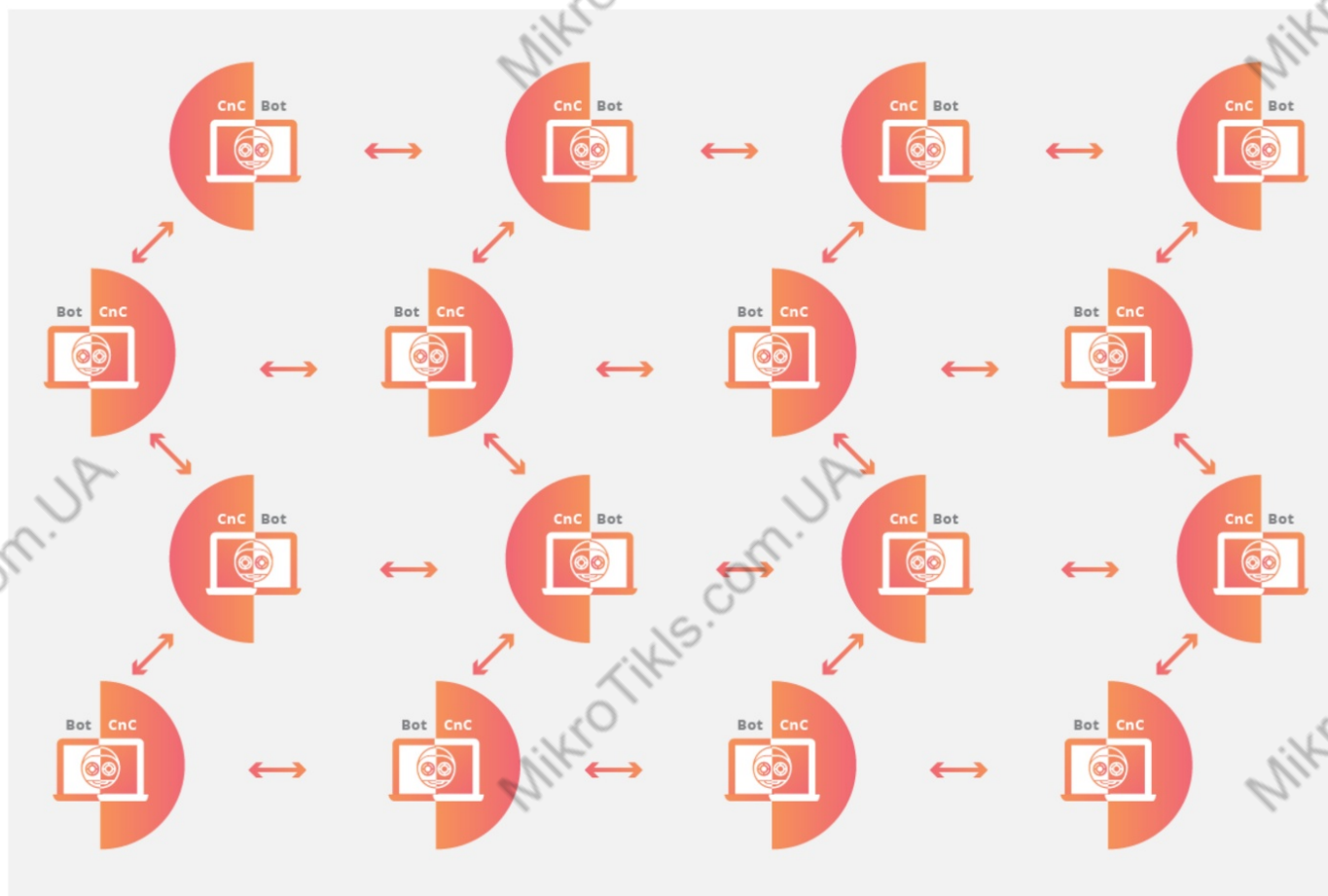


## Security basic: **THREATS - Botnet**

Конструкции ботнетов различны, но управляющие структуры можно разделить на две основные категории:

- The client/server botnet model
  - Star Network Topology
  - Multi Server Network Topology
  - Hierarchical Network Topology
- The peer-to-peer botnet model





## Security basic: **THREATS - Botnet**

Конструкции ботнетов различны, но управляющие структуры можно разделить на две основные категории:

- The client/server botnet model
  - Star Network Topology
  - Multi Server Network Topology
  - Hierarchical Network Topology
- The peer-to-peer botnet model



Security basic: **Distributed denial-of-service (DDoS)**



## Security basic: **Distributed denial-of-service (DDoS)**

Распределенная атака, типа «отказ в обслуживании» (DDoS) - это злонамеренная попытка нарушить нормальный трафик целевого сервера, службы или сети, перегружая цель или окружающую инфраструктуру потоком интернет-трафика\*.



DDoS-атаки достигают эффективности, используя несколько скомпрометированных компьютерных систем в качестве источников трафика атаки.

DDoS-атака может быть похожа на пробку, забивающую шоссе, препятствующую регулярному трафику прибыть в желаемое место назначения.

## Security basic: **Distributed denial-of-service (DDoS)**

Как работает DDoS-атака?

После того, как ботнет создан, злоумышленник может управлять машинами, отправляя обновленные инструкции каждому боту с помощью метода дистанционного управления. Когда ботнет использует целевой IP-адрес жертвы, каждый бот отвечает, отправляя запросы к цели, что может привести к переполнению целевого сервера или сети, что приведет к отказу в обслуживании нормальному трафику. Поскольку каждый бот является законным интернет-устройством, отделить трафик атаки от обычного трафика может быть сложно.

## Security basic: **Distributed denial-of-service (DDoS)**

Какие распространенные типы DDoS-атак?

Различные векторы DDoS-атак нацелены на различные компоненты сетевого подключения. Чтобы понять, как работают различные DDoS-атаки, необходимо знать, как осуществляется сетевое соединение.

В то время, как почти все DDoS-атаки связаны с перегрузкой целевого устройства или сети трафиком, атаки можно разделить на три категории.

- Application Layer Attacks
- Protocol Attacks
- Volumetric Attacks

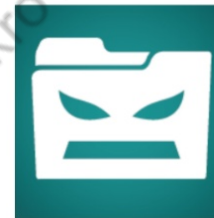
## Security basic: **Hacking**



«Взлом - это термин, используемый для описания действий, предпринятых кем-то, чтобы получить несанкционированный доступ к компьютеру(хосту)».

- Найти слабые места (или ранее существовавшие ошибки) в вашей безопасности настройки и использовать их для доступа к вашим ресурсам.
- Установить троянского коня, предоставляя хакерам "заднюю дверь" для поиска и доступа к вашей информации.

## Security basic: **Malware**



Malware, сокращенно от английского «malicious software» - вредоносное программное обеспечение, имеющее своей целью в той или иной форме нанести ущерб пользователю или компьютеру и его содержимому. Это общее название для всех видов кибер-угроз, таких как: вирусы, трояны, черви, шпионские программы, кейлоггеры, adware и др.

## Security basic: **Malware**

Какой вред может причинить Malware моему компьютеру?

- Меняют настройки браузера и не дают изменить их пользователю (например, устанавливает новую домашнюю страницу или поиск по умолчанию);
- Тратят ресурсы компьютера, тем самым снижают его быстродействие;
- Устанавливают рекламные программы на компьютер, такие как всплывающие окна и баннеры, которые работают даже без подключения к интернету;
- Используют компьютер и его ресурсы для DDoS-атак или майнинга криптовалют;
- Блокируют доступ к сайтам антивирусов и другим сайтам, содержащим инструменты для борьбы с вредоносным ПО;
- Собирают личные данные пользователя: логины, пароли, номера банковских карт и прочее;
- Без ведома пользователя могут скачивать с интернета и устанавливать другое вредоносное ПО.

## Security basic: **Phishing**



Фишинг - один из видов интернет-мошенничества, используется для того, чтобы вытянуть из пользователей личные данные, логины, пароли, номера банковских карт или другую важную информацию, злоумышленники создают поддельные страницы сайтов магазинов, банков, почтовых клиентов и соцсетей. Визуально они не отличаются от оригинальных, поэтому невнимательный посетитель вводит свои данные авторизации, после чего они попадают к мошенникам. Таким образом, мошенники могут взломать страницу вконтакте с помощью фишинга или получить доступ к банковскому аккаунту своей жертвы.

Как пользователь попадает на поддельную страницу?

## Security basic: **Phishing**

При фишинге сначала отправляется поддельное электронное письмо или другое электронное сообщение, составленное так, чтобы ввести жертву в заблуждение. Это сообщение выглядит так, как будто оно поступило от надежного отправителя.

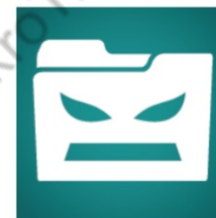
Типы:

- Фишинг с обманом
- «Гарпунный» фишинг
- «Охота на китов» (whaling)
- Фарминг

Фарминг - в данном случае жертвы могут попасть на сайт мошенников, даже не используя вредоносную ссылку.

Злоумышленник заражает компьютер пользователя либо DNS-сервер веб-сайта и перенаправляет пользователя на поддельный сайт даже в случае ввода правильного URL-адреса.

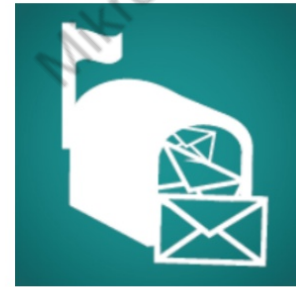
## Security basic: **Ransomware**



Программа-вымогатель – это разновидность вредоносного программного обеспечения. Она удерживает информацию жертвы в зашифрованном виде до получения злоумышленником определенного денежного выкупа. Обычно злоумышленник требует получение выкупа в виде криптовалюты, например, биткойнов. Только после этого он присылает ключ для дешифрования данных жертвы.

Обычно программы-вымогатели распространяются по нескольким каналам. Сюда входит фишинг с помощью электронной почты, вредоносная реклама и пакеты эксплойтов. После внедрения в систему программа-вымогатель зашифровывает отдельные файлы и уведомляет жертву о необходимости выкупа.

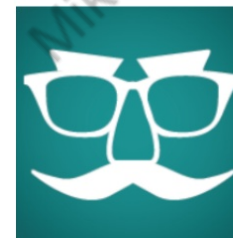
## Security basic: **Spam**



Спам - массовая рассылка корреспонденции рекламного характера(и не только) лицам, не выразившим желания её получать. Распространителей спама называют спамерами.

- Раздражать вас нежелательной почтой.
  - Использовать Фишинг (акции и т.д.)
  - Malware
- и т.д.

## Security basic: **Spoofing**



Подмена - ситуация, в которой один человек или программа успешно маскируется под другую путём фальсификации данных и позволяет получить незаконные преимущества

спуфинг IP (отправка сообщений на компьютеры с использованием IP-адреса доверенного источника), email спуфинг (подделка заголовка писем для маскировки истинного отправителя) и DNS спуфинг (изменение настроек сервера DNS для переадресации доменного имени на IP адрес злоумышленников).

## Security basic: **Spyware**



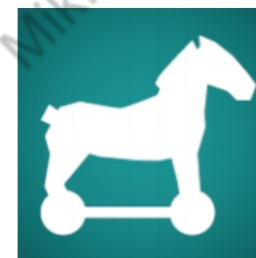
Spyware (программа-шпион) – программа, которая скрытным образом устанавливается на компьютер, смартфон, персональный цифровой помощник с целью сбора информации о конфигурации компьютера, копировании информации из памяти устройства, копировании данных пользователя, аудио/видео записи пользователя или пользовательской активности без согласия последнего.

## Security basic: **Adware**



Adware – это программы, которые предназначены для показа рекламы на вашем устройстве, перенаправления запросов поиска на рекламные веб-сайты и сбора маркетинговой информации о вас (например, какого рода сайты вы посещаете), чтобы реклама соответствовала вашим интересам.

## Security basic: **Trojan Horses**



Троянская программа (троянский конь) — разновидность вредоносной программы, проникающая в компьютер под видом легального программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно.

В данную категорию входят программы, осуществляющие различные неподтвержденные пользователем действия: сбор информации банковских карт ит. и её передачу злоумышленнику, её использование, удаление или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в целях майнинга, использование IP для нелегальной торговли

## Security basic: **Viruses**



Компьютерный вирус - это программа или часть программного кода, который загружается на компьютер без ведома и разрешения владельца. Присутствие в системе некоторых типов вирусов незаметно, однако некоторые из них разрушительны и предназначены для вторжения и овладения контролем над системой. Вирус может распространяться между компьютерами и даже сетями путем самовоспроизведения - так же, как биологический вирус переходит с одного носителя на другого.

## Security basic: **Worm**



Компьютерные черви - это тип вредоносного ПО, способного к самовоспроизведению и существенно снижающего скорость работы устройства

# MikroTik Certified Security Engineer

MTCSE

## *Chapter 1: Basic security*

Базовые  
понятия

Threats  
Угрозы

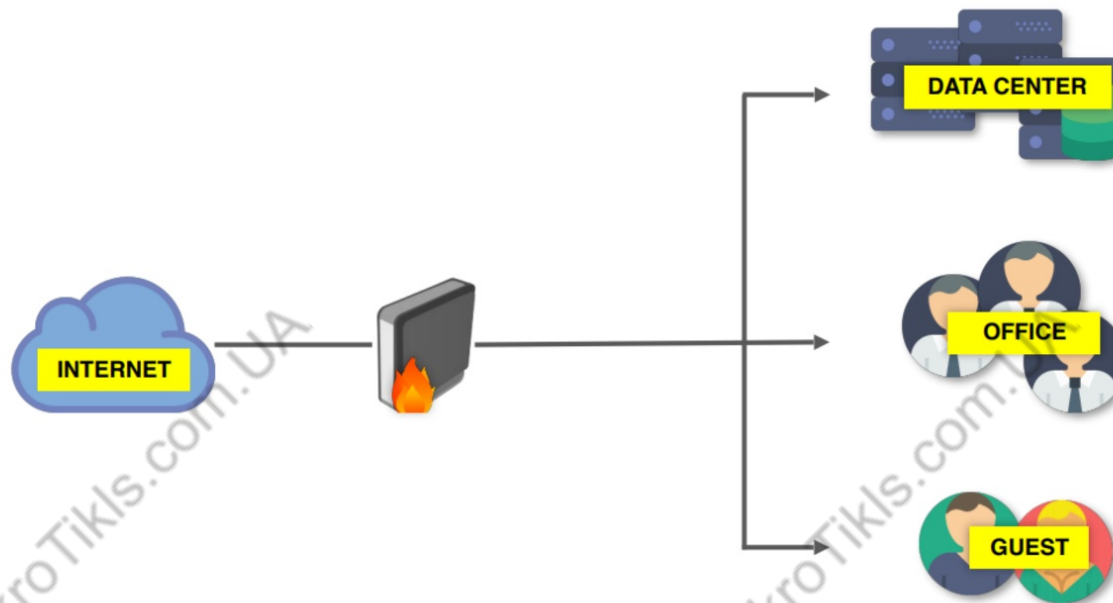
SECURITY  
DEPLOYMENT



MTI-GROUP LLC / network academy

V.21-07

## Security basic: **Global Firewall Router**



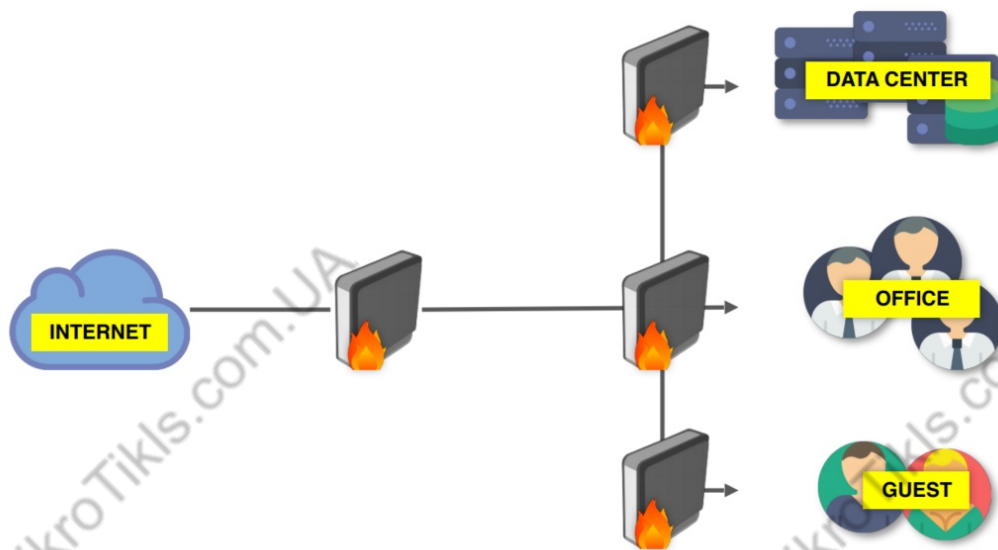
### плюсы

- простая топология
- легкость\* обслуживания

### минусы

- одна точка отказа
- высокая ресурсоемкость

## Security basic: **Specific Router Firewall**



### плюсы

- нагрузка распределяется между роутерами
- меньше правил на каждом роутере, тематические, упрощение.

### минусы

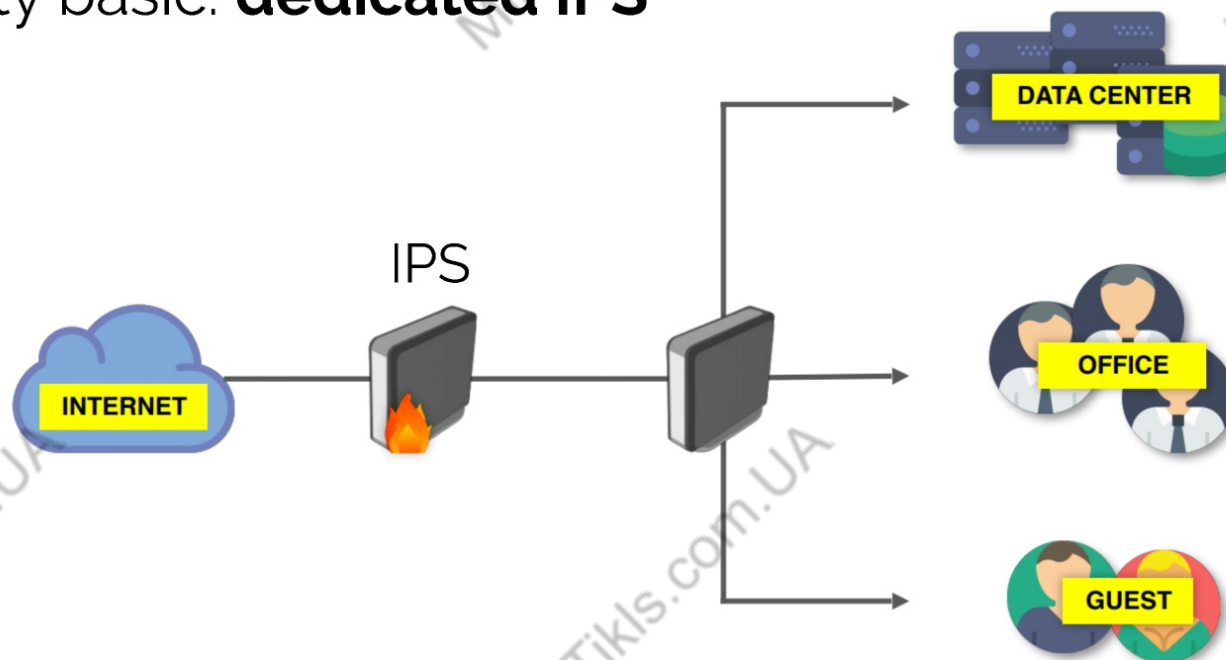
- больше оборудования - больше обслуживания
- актуализация (дублирование) настроек на каждом роутере

## Security basic: **dedicated IPS**

IPS (Intrusion Prevention System) – программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Системы IPS можно рассматривать как расширение Систем обнаружения вторжений (IDS), так как задача отслеживания атак остается одинаковой. Однако, они отличаются в том, что IPS должна отслеживать активность в реальном времени и быстро реализовывать действия по предотвращению атак.

## Security basic: **dedicated IPS**



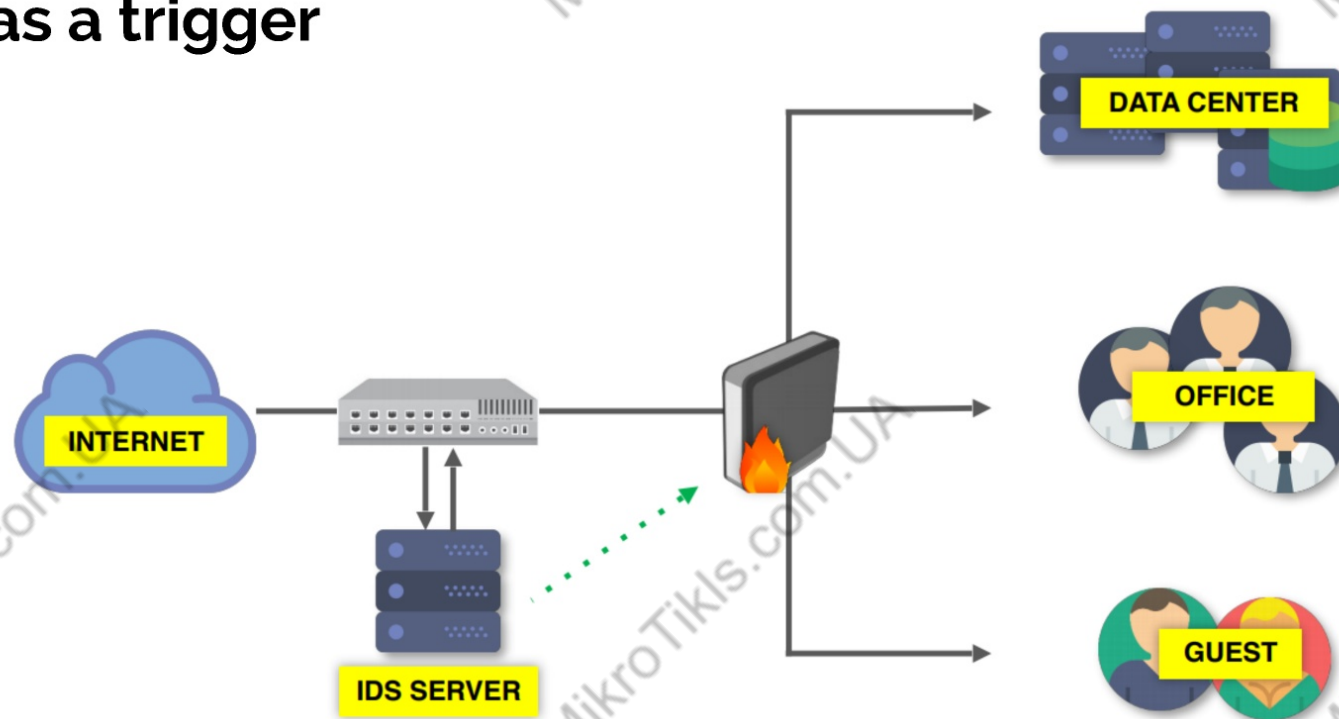
плюсы

- отдельно правила по защите ваших ресурсов от остальной конфигурации маршрутизатора, теперь они в IPS маршрутизаторе

минусы

- для IPS функций требуется мощный маршрутизатор

## Security basic: MikroTik with IDS as a trigger



## Security basic: **MikroTik with IDS as a trigger**

плюсы

- Все правила брандмауэра автоматически создаются при помощи API с IDS сервера

минусы

- Необходимо дополнительное устройство для triggering плохого трафика
- Необходимо мощное устройство для зеркалирования всего трафика в / из сети
- Необходимы специальные scripting для отправки информации на маршрутизатор
- дорого

# MikroTik Certified Security Engineer

MTCSE

## *Chapter 1: Basic security*

Базовые  
понятия

Threats  
Угрозы

SECURITY  
DEPLOYMENT



MTI-GROUP LLC / network academy

V.21-07