ІНФОРМАТИКА


# Виявлення атак. Захист периметра комп'ютерних мереж

За навчальною програмою 2018 року

**Урок 9**

Розділ 2
§ 9

# Виявлення атак


***Виявлення атак** – це процес ідентифікації та регулювання на підозрілу діяльність, направлену на обчислювальні чи мережні ресурси*

***Усі існуючі технології виявлення мережевих атак можна розділити на два типи:***

| | |
|---|---|
| ***методи на основі сигнатур (зразків і правил)*** | ***методи на основі аномалій*** |

Розділ 2
§ 9

# Виявлення атак


## Класифікації систем виявлення атак

### За способом виявлення атаки

- Виявлення аномального поводження (anomaly-based)
- Виявлення зловживань (misuse detection або signature-based

### За способом збору інформації про атаку

- Пасивні просто фіксують факт атаки, записують дані у файл журналу й видають попередження
- Активні намагаються протидіяти атаці

### За способом реагування

Розділ 2
§ 9

# Виявлення атак


## Аналіз активності атак

| Статичні системи виявлення атак | Динамічні системи виявлення атак |
| --- | --- |
| Статичні засоби роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе програмне забезпечення, помилки в конфігураціях і т. д. Виявляють сліди вторгнення. | здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережні пакети, що передаються за певний проміжок часу. Постійно стежать за безпекою системи |

Розділ 2
§ 9

# Виявлення атак


## (Продовження...) Аналіз активності атак

| **Мережеві системи виявлення атак** | **Хостові системи виявлення атак** |
| --- | --- |
| Здійснюють контроль усього трафіку даних всієї підмережі та порівнюють трафік, який передається у підмережі з бібліотекою відомих атак. Як тільки розпізнана атака або визначено відхилення у поведінці, відразу відсилається попередження адміністратору | Встановлюються на хості і виявляють зловмисні дії на ньому |

Розділ 2
§ 9

# Виявлення атак


***Реалізація більшості мережевих атак здійснюються в три етапи.***

***Перший, підготовчий, етап полягає в пошуку передумов для здійснення атаки***

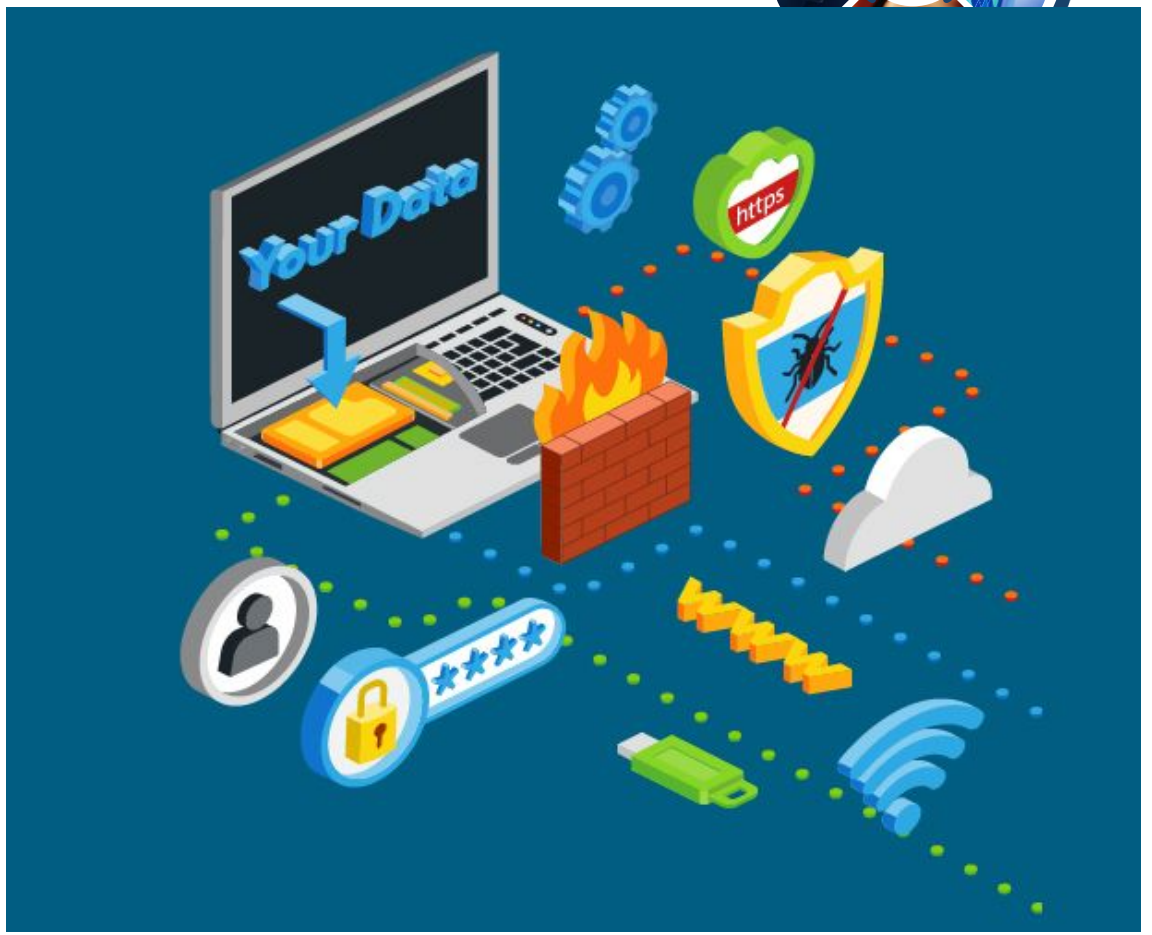
***Пошук вразливостей, використання яких робить можливим реалізацію атаки***

***На третьому етапі атака завершується, «заметено» сліди і т.д.***

Розділ 2
§ 9

# Захист периметра комп’ютерних мереж


***Безпека мережі*** — *заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів.*



Розділ 2
§ 9

# Захист периметра комп’ютерних мереж

10
11

## *Безпека інформаційної мережі включає захист:*

- *обладнання*
- *програмного забезпечення*
- *даних*
- *персоналу*

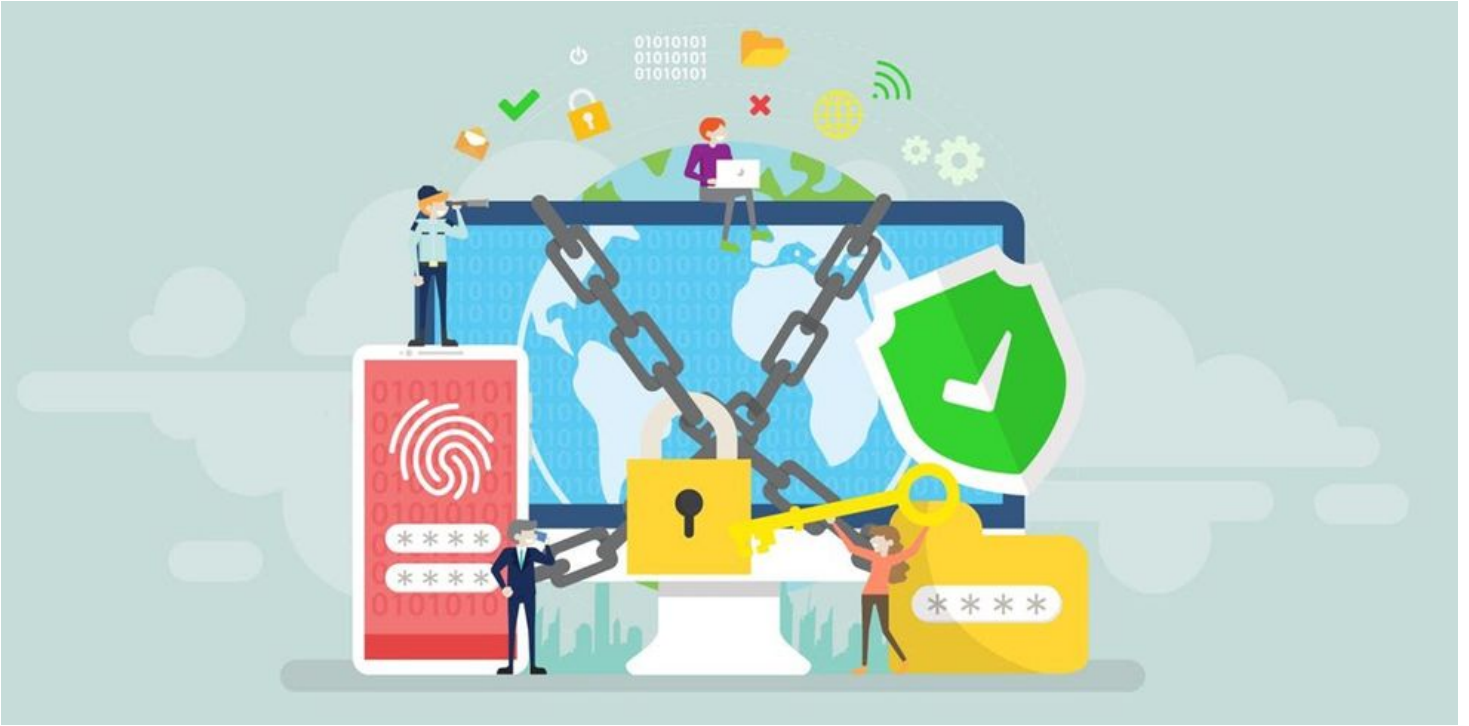
Розділ 2
§ 9

# Захист периметра комп’ютерних мереж

**Мережева безпека** охоплює різні комп'ютерні мережі:

| приватні | державні |
| --- | --- |

**Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю.**



Розділ 2
§ 9

# Захист периметра комп'ютерних мереж


## *Система безпеки мережі:*

- *Захищає від внутрішніх та зовнішніх мережних атак.*
- *Забезпечує конфіденційність обміну інформацією з будь-якого місця та в будь-який час.*
- *Контролює доступ до інформації, ідентифікуючи користувачів та їхні системи.*
- *Забезпечує надійність системи.*

Розділ 2
§ 9

# Захист периметра комп'ютерних мереж

10
11

## *Ключові елементи захищених мережних служб:*

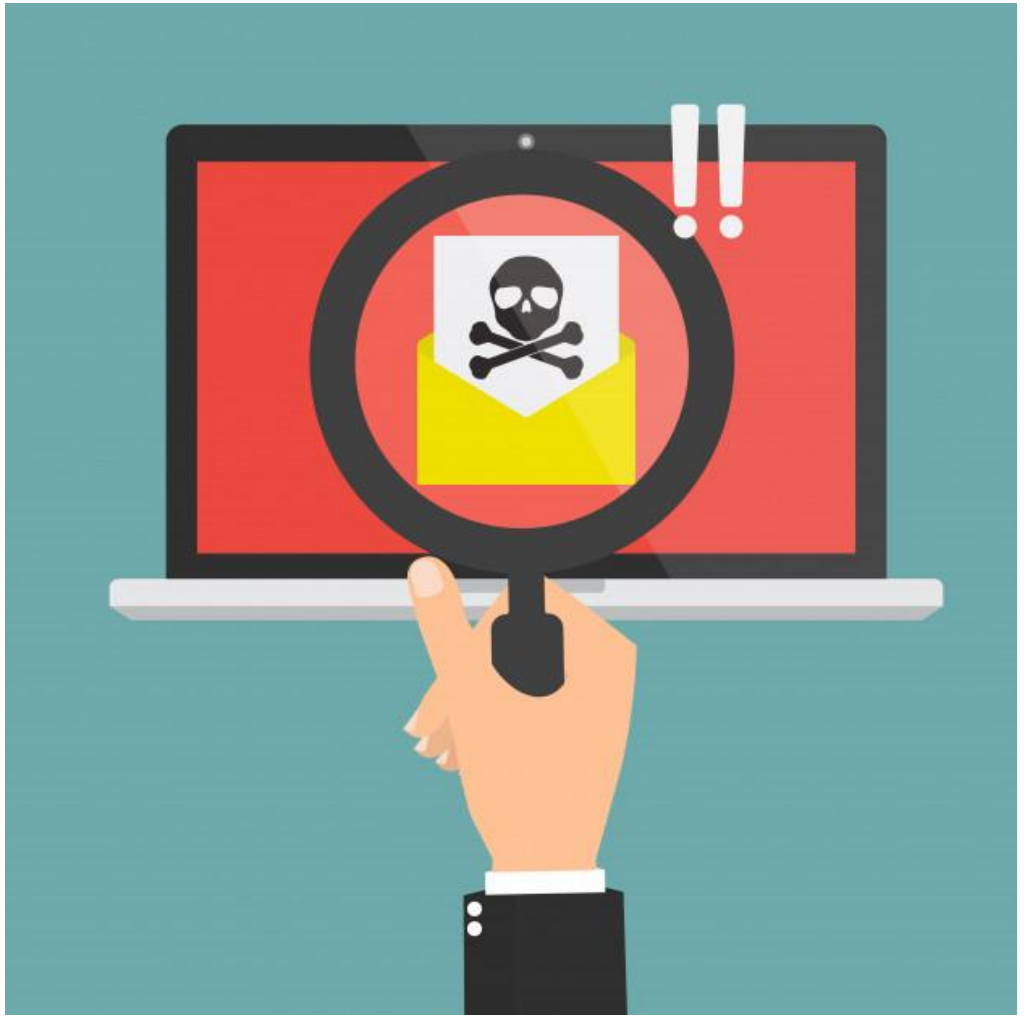
- *Брандмауери*
- *Антивірусні засоби*
- *Знаряддя, які відстежують стан мережі, грають важливу роль під час визначення мережних загроз*
- *Захищений віддалений доступ і обмін даними*

Розділ 2
§ 9

# Захист периметра комп'ютерних мереж

## Методи обмеження доступу в мережі:

- ✔ Фільтрація MAC-адреси
- ✔ Режим прихованого ідентифікатора SSID
- ✔ Методи аутентифікації
- ✔ Методи шифрування



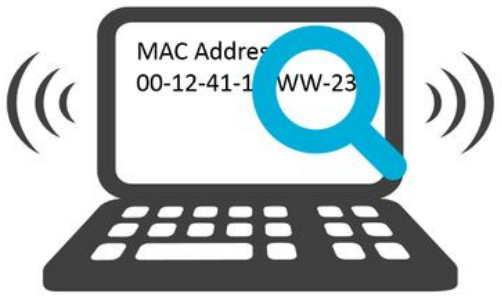
Розділ 2
§ 9

# Захист периметра комп'ютерних мереж

## Фільтрація MAC-адреси

Фільтрацію можна здійснювати такими трьома способами:

- Точка доступу дозволяє отримати доступ станціям з будь-якою MAC-адресою;
- Точка доступу дозволяє отримати доступ тільки станціям, чиї MAC-адреси є в довіреному списку;
- Точка доступу забороняє доступ станціям, чиї MAC-адреси є в "чорному списку";



Розділ 2
§ 9

# Захист периметра комп'ютерних мереж

## Режим прихованого ідентифікатора SSID

**Ідентифікатор SSID – назва бездротової мережі**

**У разі прихованого SSID виявлення бездротової мережі є неможливим і не можна до неї підключитися, не знаючи значення SSID.**

Розділ 2
§ 9

# Захист периметра комп'ютерних мереж

## Методи аутентифікації

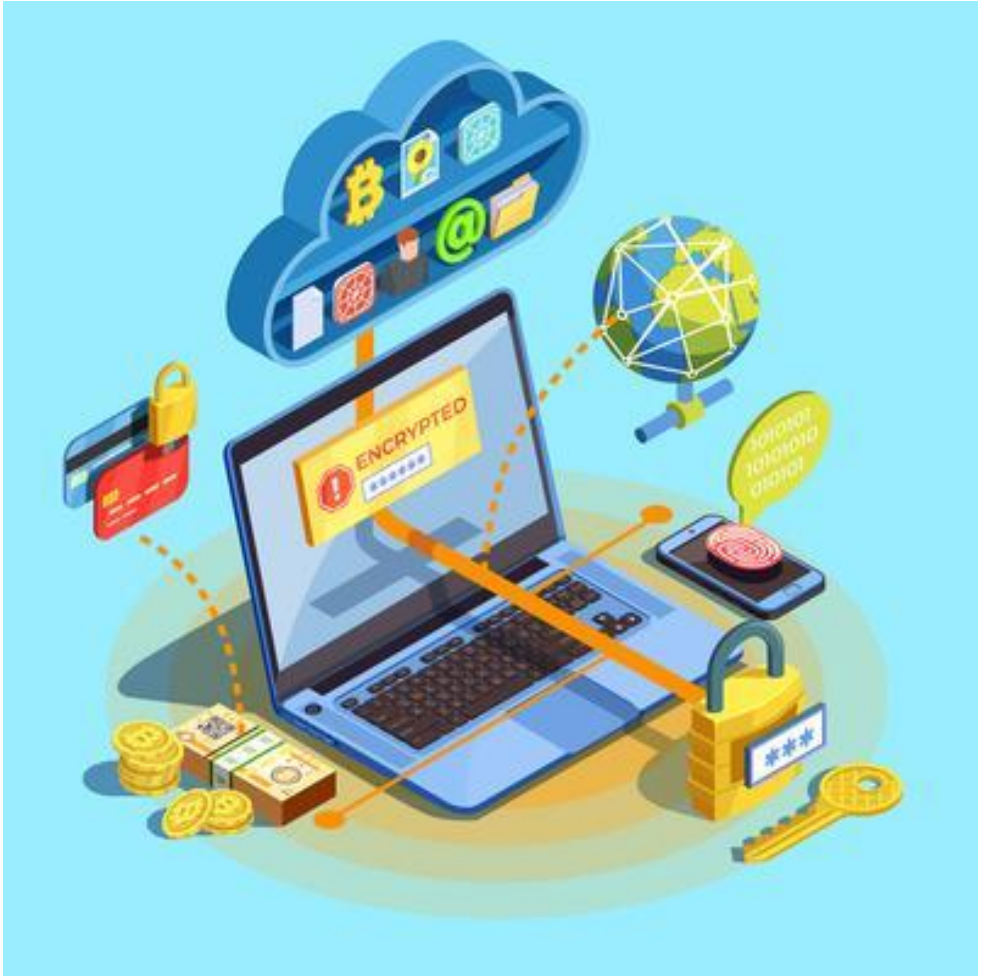
***Аутентифікація** – видача певних прав доступу абоненту на основі наявного в нього ідентифікатора.*

- Відкрита аутентифікація
- Аутентифікація із загальним ключем
- Аутентифікація за допомогою наданого ключа WPA-PSK
- Аутентифікація за допомогою RADIUS-сервера

Розділ 2
§ 9

# Захист периметра комп'ютерних мереж

## Методи шифрування




- WEP-шифрування
- TKIP-шифрування
- CKIP-шифрування
- WPA-шифрування
- WPA2-шифрування

Розділ 2
§ 9

# Керування механізмами захисту

***Захист периметра комп’ютерних мереж.*** *Цілісність периметра комп’ютерної мережі забезпечується використанням певних базових технологій міжмережевого екранування в точці підключення мережі, що захищається, до зовнішньої неконтрольованої мережі.*

Розділ 2
§ 9

# Керування механізмами захисту

***Керування механізмами захисту.***

***Налаштування захисних механізмів може виконуватися засобами:***

***локального управління***

***централізованого управління***

***в мережевому режимі функціонування системи***

Розділ 2
§ 9

# Запитання для рефлексії

1. *Чи встиг я у повному обсязі здійснити заплановане на цьому уроці?*
2. *Що потрібно зробити, щоб результат роботи був кращим?*
3. *Яких знань я набув на уроці?*
4. *Чи досяг я мети, яку ставив собі на початку уроку?*

Розділ 2
§ 9

# Домашнє завдання


***Зробити пост у соціальних мережах про захист периметра комп'ютерних мереж і керування механізмів захисту***

Розділ 2
§ 9

# Працюємо за комп’ютером


***Створіть презентацію “Які є види мережевих атак?”***

***1. Розмісіть роботу на Google-диску, надайте доступ, для перегляду і редагування учителю і 2 однокласникам.***

***2. Перегляньте проектну роботу своїх друзів. Додайте коментарі. Порівняйте змістовну частину і оформлення.***

***3. Оцініть власну роботу і переглянуті роботи.***

# ІНФОРМАТИКА


**Урок 9**

# Дякую за увагу!

За навчальною програмою 2018 року