

# Cyber Security: Повний гід з кібербезпеки

## 1. Передісторія кібербезпеки

Кібербезпека почала активно розвиватися разом із розширенням комп'ютерних мереж у 1980–1990-х роках.

З розвитком інтернету та cloud з'явилися складні атаки: ransomware, phishing, APT.

## 2. Основні напрями

Мережева безпека: Firewall, IDS/IPS, VPN.

Безпека застосунків: secure coding.

Cloud Security: IAM, шифрування.

SOC та реагування на інциденти.

GRC (Governance, Risk, Compliance).

## 3. Як вивчати кібербезпеку

Крок 1. Освоїти networking та Linux.

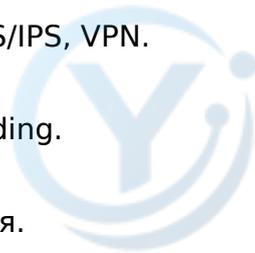
Крок 2. Вивчити типи атак.

Крок 3. Практикуватися у lab середовищах.

Крок 4. Освоїти security tools.

Крок 5. Вивчити стандарти безпеки (NIST, ISO).

Крок 6. Практикувати incident response.



## 4. Рівні знань

Початковий: базові поняття.

Середній: vulnerability scanning, SIEM.

Просунутий: penetration testing.

Архітектор: дизайн enterprise security.

## 5. Сертифікації

CompTIA Security+.

CEH.

CISSP.

CISM / CISA.

Cloud Security сертифікації.



## 6. Інструменти

Wireshark, Nmap.

Metasploit, Burp Suite.

Splunk, ELK.

Kali Linux.

## Висновок

Кібербезпека є критично важливою для сучасної ІТ-інфраструктури.  
Потрібна практика, лабораторії та постійне навчання.

