

Кар'єрне планування: Шлях у Cybersecurity

1. Точка А — Де я зараз:

- **Поточний статус:**
Початківець у сфері кібербезпеки, проходжу курси **GoIT**, **Google Cybersecurity (Coursera)** та інші безкоштовні курси, виконую практичні завдання, створюю GitHub-портфоліо.
- **Технічні навички:**
Базове знання **Linux**, **мереж**, **OWASP**, **NIST**, вмю користуватись терміналом, налаштовувати системи безпеки, працювати з CLI, знайомий із основами **SOC**, **SIEM**, **threat analysis**.
- **Мова програмування:**
Володію **Python**, **Bash**, почав вивчати **C/C++** для глибшого розуміння роботи пам'яті.
- **Кар'єрний фокус:**
Хочу стати **фахівцем із кібербезпеки**, який займається **аналітикою загроз**, **пентестом** або **SOC-аналітикою** в міжнародній компанії.

2. Точка В — Моя мета через 5+ років:

🔗 **Cybersecurity Specialist / SOC Analyst / Penetration Tester**

- Працюю у міжнародній компанії.
- Маю **сертифікації**: **CompTIA Security+**, **CySA+**, **СЕН**, або **OSCP**.
- Досконало володію **Linux**, **мережевою безпекою**, **SIEM-системами**, **пентест-інструментами**.
- Веду **блог / YouTube / GitHub-портфоліо** з власними кейсами.

3. Проміжні кар'єрні цілі (2–5):

◇ Ціль 1 (0–6 місяців):

- Завершити курс **Google Cybersecurity** на Coursera.
- Створити та наповнити **GitHub-портфоліо** (аудит безпеки, скрипти, звіти OWASP).
- Почати вести **документацію практичних навичок** (security audit, firewall config, Linux security).

◇ Ціль 2 (6–12 місяців):

- Отримати **CompTIA Security+** (перша базова сертифікація).
- Подати резюме на стажування або позицію **Junior SOC Analyst / IT Security Intern**.

- Навчитися працювати з **SIEM** (Splunk, Wazuh, Graylog), **Wireshark**, **Burp Suite**.

◇ **Ціль 3 (1–2 роки):**

- Отримати перший реальний досвід роботи / стажування в Cybersecurity.
- Пройти **CySA+** або почати підготовку до **CEH / OSCP**.
- Взяти участь у CTF, bug bounty, або відкритих проєктах.

◇ **Ціль 4 (2–4 роки):**

- Працювати у команді безпеки як **Mid-level Security Analyst / Pentester**.
- Поглибити знання у **reverse engineering, network forensics, cloud security** (AWS, Azure).

◇ **Альтернатива / резервна ціль:**

- Якщо не вдається одразу працевлаштуватися — створити власний **фриланс-профіль (Upwork, Fiverr)** для безпекових аудитів або консультацій малого бізнесу.