Курс з кібербезпеки, що охоплює різні аспекти – від базових концепцій до практичних навичок. Цей курс розрахований як на початківців, так і на тих, хто вже має певний досвід і хоче систематизувати свої знання.

Курс з Кібербезпеки: Захисти свій цифровий світ

Ціль курсу: Надати всебічні знання та практичні навички, необхідні для розуміння сучасних загроз кібербезпеці, їх запобігання, виявлення та реагування.

Для кого цей курс:

* Будь-яка людина, яка бажає покращити свій рівень цифрової гігієни.
* IT-спеціалісти, які хочуть розширити свої знання в області безпеки.
* Менеджери, які приймають рішення щодо інформаційної безпеки в компаніях.
* Студенти та всі, хто цікавиться кар'єрою в кібербезпеці.

Тривалість курсу: Може бути адаптована (наприклад, 12-16 тижнів, по 2-4 години на тиждень лекцій/практики + самостійна робота).

Модуль 1: Вступ до Кібербезпеки та Основи

Тиждень 1: Що таке Кібербезпека?

* Визначення та значення: Чому кібербезпека важлива у сучасному світі?
* Історія кібербезпеки: Еволюція загроз та захисту.
* Основні принципи безпеки (тріада CIA): Конфіденційність, Цілісність, Доступність (Confidentiality, Integrity, Availability).
* Ключові терміни та поняття: Вразливість, загроза, ризик, атака, експлойт, патч.
* Ролі та кар'єрні шляхи в кібербезпеці: Аналітик безпеки, інженер безпеки, пентестер, спеціаліст з реагування на інциденти, аудитор тощо.

Тиждень 2: Основи комп'ютерних мереж та операційних систем для кібербезпеки

* Огляд мережевих протоколів: TCP/IP, DNS, HTTP/HTTPS, FTP, SSH.
* Модель OSI та TCP/IP: Їх значення для розуміння мережевих атак.
* Мережеві пристрої: Маршрутизатори, світчі, фаєрволи.
* Основи операційних систем: Windows, Linux, macOS (особливості безпеки, управління користувачами та правами, файлова система).
* Концепції віртуалізації та хмарних обчислень: Вступ.

Модуль 2: Загрози, Вразливості та Атаки

Тиждень 3: Види шкідливого програмного забезпечення (Malware)

* Віруси, хробаки, трояни: Різниця та механізми поширення.
* Рансомвер (Ransomware): Як працює, запобігання та дії при зараженні.
* Шпигунське ПЗ (Spyware), рекламні програми (Adware), руткіти (Rootkits), ботнети (Botnets).
* Практика: Використання антивірусних програм, аналіз зразків malware (у безпечному середовищі).

Тиждень 4: Соціальна інженерія та Фішинг

* Що таке соціальна інженерія: Методи маніпуляції та психологічного впливу.
* Види фішингу: Спірфішинг, вейлінг, смишинг, вішинг.
* Розпізнавання фішингових листів та сайтів: Практичні поради.
* Запобігання та навчання: Як захистити себе та своїх співробітників.

Тиждень 5: Веб-вразливості та Атаки

* OWASP Top 10: Найбільш поширені веб-вразливості.
* SQL-ін'єкції (SQL Injection): Принципи та запобігання.
* Міжсайтовий скриптинг (XSS - Cross-Site Scripting): Типи та захист.
* Підробка міжсайтових запитів (CSRF - Cross-Site Request Forgery).
* Вразливості аутентифікації та контролю доступу.

* DDoS-атаки (Distributed Denial of Service): Механізми та методи протидії.

Тиждень 6: Мережеві атаки та Загрози

* Сканування портів та мережеві розвідки.
* Атаки типу "людина посередині" (Man-in-the-Middle - MitM).
* Підбір паролів (Brute-Force) та атаки за словником.
* ARP Spoofing, DNS Spoofing.
* Вразливості Wi-Fi мереж (WEP, WPA/WPA2, WPA3).

Модуль 3: Захист та Запобігання

Тиждень 7: Захист кінцевих точок (Endpoint Security)

* Антивірусні та антивредоносні програми: Еволюція та сучасні рішення (EDR, XDR).
* Мережеві екрани (Firewalls): Персональні та корпоративні.
* Системи виявлення та запобігання вторгнень (IDS/IPS).
* Управління патчами та оновленнями: Важливість своєчасного оновлення ПЗ.
* Базові конфігурації безпеки для ОС.

Тиждень 8: Управління ідентифікацією та доступом (Identity and Access Management - IAM)

* Концепції IAM: Аутентифікація, авторизація, облік.
* Надійні паролі: Створення та управління.
* Багатофакторна аутентифікація (MFA/2FA): Типи та переваги.
* Управління привілейованим доступом (Privileged Access Management - PAM).
* Рольова модель доступу (Role-Based Access Control - RBAC).

Тиждень 9: Шифрування та Криптографія

* Основні принципи криптографії: Симетричне та асиметричне шифрування.
* Хеш-функції: Призначення та використання (перевірка цілісності, зберігання паролів).
* Цифрові підписи та сертифікати: Принцип роботи, інфраструктура відкритих ключів (PKI).
* SSL/TLS: Забезпечення безпеки веб-з'єднань.
* Шифрування дисків та даних: BitLocker, VeraCrypt.

Тиждень 10: Безпека мережі та Хмарна безпека

* Сегментація мережі: VLAN, мережеві зони (DMZ).
* VPN (Virtual Private Network): Призначення та використання.
* Безпека бездротових мереж: Захист Wi-Fi.
* Безпека хмарних обчислень: IaaS, PaaS, SaaS – відповідальність та загрози.
* Концепція "Нульової довіри" (Zero Trust).

Модуль 4: Регулювання, Реагування та Практика

Тиждень 11: Законодавство та Регулювання в Кібербезпеці

* Міжнародні та національні стандарти: ISO 27001, NIST Cybersecurity Framework.
* Закони про захист даних: GDPR (Загальний регламент про захист даних), HIPAA (для охорони здоров'я).
* Нормативні акти в Україні: Закон України "Про основні засади забезпечення кібербезпеки України".
* Етичні аспекти кібербезпеки.

Тиждень 12: Реагування на інциденти та Відновлення після катастроф (Disaster Recovery)

* Життєвий цикл реагування на інциденти: Підготовка, виявлення та аналіз, стримування, викорінення, відновлення, післяінцидентний аналіз.
* План реагування на інциденти (Incident Response Plan).
* Криміналістична експертиза (Digital Forensics): Збір та аналіз доказів.

* Плани безперервності бізнесу (Business Continuity Planning - BCP).
* Резервне копіювання та відновлення даних.

Тиждень 13: Оцінка вразливостей та Тестування на проникнення (Penetration Testing)

* Різниця між оцінкою вразливостей та пентестом.
* Методології пентесту: OSSTMM, PTES.
* Етапи пентесту: Розвідка, сканування, експлуатація, підтримка доступу, приховування слідів.
* Інструменти для пентесту: Nmap, Wireshark, Metasploit, Burp Suite, Kali Linux.
* Практикум: Проведення простого пентесту (на тестовому середовищі).

Тиждень 14: Моніторинг та Аналіз безпеки (SOC, SIEM)

* Центр операцій з безпеки (Security Operations Center - SOC): Функції та ролі.
* Системи управління інформацією та подіями безпеки (SIEM): Призначення, збір та аналіз логів.
* Системи оркестрації, автоматизації та реагування на безпекові події (SOAR).
* Загрози intelligence (Threat Intelligence): Використання даних про загрози.
* Машинне навчання в кібербезпеці.

Додаткові Модулі / Поглиблене вивчення (за бажанням)

* Безпека мобільних пристроїв: iOS, Android.
* IoT (Internet of Things) безпека.
* Операційна безпека (OpSec).
* DevSecOps: Інтеграція безпеки в розробку програмного забезпечення.
* Аудит інформаційної безпеки.
* Захист критичної інфраструктури.

Методологія навчання

* Лекції: Теоретичні основи, пояснення концепцій.
* Практичні заняття/Лабораторні роботи: Використання інструментів, симуляція атак, налаштування захисту.
* Домашні завдання: Закріплення матеріалу.
* Кейс-стаді: Розбір реальних інцидентів кібербезпеки.
* Проєкти: Індивідуальні або групові проєкти з розробки плану безпеки, проведення міні-пентесту тощо.
* Обговорення та Q&A сесії.

Рекомендовані ресурси

* Онлайн-платформи: Coursera, Udemy, edX, Cybrary, TryHackMe, Hack The Box.
* Книги: "The Phoenix Project", "Hacking: The Art of Exploitation", "CompTIA Security+ Study Guide".
* Офіційні документації: NIST, ISO, OWASP.
* Новинні сайти та блоги з кібербезпеки: KrebsOnSecurity, BleepingComputer, The Hacker News.
* Сертифікації: CompTIA Security+, Certified Ethical Hacker (CEH), CISSP (для досвідчених).

Завершення курсу: Успішне завершення курсу передбачає не тільки отримання теоретичних знань, а й здатність застосовувати їх на практиці для забезпечення ефективного рівня кібербезпеки у повсякденному житті та професійній діяльності.

Цей курс може бути адаптований під конкретні потреби та рівень підготовки слухачів.

Успіхів у вивченні кібербезпеки!