Cyberbezpieczeństwo: Ochrona danych i systemów informatycznych (40 godzin)

Sposób organizacji szkoleń: 40 godzin w formule online

Liczba uczestników: 10 osób

Program szkolenia:

Zagrożenia bezpieczeństwa informatycznego i metody ataku (8 godzin)

• Wprowadzenie do cyberzagrożeń i podstawowe rodzaje ataków.

• Metody ataku: phishing, malware, ataki typu DDoS.

• Sposoby identyfikacji i klasyfikacji zagrożeń.

Podstawy kryptografii i bezpieczeństwa sieci (8 godzin)

• Podstawowe pojęcia z zakresu kryptografii: szyfrowanie, deszyfrowanie, podpis cyfrowy.

• Bezpieczne protokoły komunikacyjne: SSL/TLS.

• Sieci VPN (Virtual Private Network) jako narzędzie zapewnienia bezpieczeństwa komunikacji.

Zarządzanie ryzykiem cyberbezpieczeństwa (8 godzin)

• Analiza ryzyka: identyfikacja, ocena, kontrola i monitorowanie.

• Metody zarządzania ryzykiem: minimalizacja, przenoszenie, akceptacja, unikanie.

• Planowanie i wdrażanie strategii bezpieczeństwa w organizacji.

Testowanie penetracyjne i audyt bezpieczeństwa (8 godzin)

• Testy penetracyjne: cel, proces przeprowadzania, raportowanie wyników.

• Audyt bezpieczeństwa: metody, narzędzia, zasady przeprowadzania.

• Ocena podatności systemów i sieci komputerowych.

Prawo i zasady regulujące cyberbezpieczeństwo (8 godzin)

• Międzynarodowe i krajowe regulacje dotyczące bezpieczeństwa IT.

• Prywatność danych osobowych: ogólne rozporządzenie o ochronie danych osobowych (RODO).

• Etyka w cyberprzestrzeni i odpowiedzialność prawna za naruszenia bezpieczeństwa.

Efekty kształcenia: Po ukończeniu kursu uczestnicy będą mogli:

• Zidentyfikować różnorodne rodzaje zagrożeń bezpieczeństwa informatycznego i zastosować odpowiednie metody ochrony.

• Zrozumieć zasady działania kryptografii i stosować je do zapewnienia bezpieczeństwa danych i komunikacji sieciowej.

• Przeprowadzać analizę ryzyka cyberbezpieczeństwa i wdrażać odpowiednie strategie zarządzania ryzykiem.

• Wykorzystywać techniki testowania penetracyjnego i audytu bezpieczeństwa do identyfikacji słabych punktów systemów informatycznych.

• Rozumieć obowiązujące przepisy prawne i zasady regulujące cyberbezpieczeństwo oraz stosować je w praktyce.