

Program studiów podyplomowych

Cyberbezpieczeństwo

rok akademicki 2026/2027

100% on line

Nazwa modułu	Liczba godzin
Cyberbezpieczeństwo - dziś i jutro	20
<ol style="list-style-type: none"> 1. Wstęp. definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne, aktualne trendy na świecie. <ol style="list-style-type: none"> a. Polityka bezpieczeństwa - czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola. b. Incydenty bezpieczeństwa - co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować. c. Studia przypadków oraz wpływ cyberataków na organizację. d. Współczesne strategie bezpieczeństw 2. Typy ataków hackerskich- demonstracje wraz z objaśnieniem metod ochrony. <ol style="list-style-type: none"> a. Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących. b. Ścieżka ataku (kill-chain) zasady- rozpoznanie i zasady postępowania c. Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC) d. Ataki przez pocztę e-mail (fałszywe e-maile) e. Ataki przez strony WWW - jak nie dać się zainfekować, fałszywe strony f. Ataki przez komunikatory (Skype, Facebook) g. Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.) h. Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam 3. Dobre praktyki, formy obrony przed atakami. 4. Rozwój Kompetencji z zakresu bezpieczeństwa. 5. Dlaczego bezpieczeństwo to nie tylko Departament Bezpieczeństwa. 	
Cyberbezpieczeństwo w systemach operacyjnych	10
<ol style="list-style-type: none"> 1. Wprowadzenie do bezpieczeństwa systemów operacyjnych <ol style="list-style-type: none"> a. Najczęściej występujące zagrożenia b. Podstawowe pojęcia bezpieczeństwa: poufność, dostępność, integralność 2. Bezpieczeństwo systemu Windows <ol style="list-style-type: none"> a. Rodzaje kont b. Zabezpieczenia kont użytkowników c. Uprawnienia i zasady dostępu d. Zabezpieczenia systemowe (UAC, BitLocker etc) e. Zapora ogniowa 	

<ul style="list-style-type: none"> f. Aktualizacje g. Monitorowanie i analiza logów h. Dobre praktyki <p>3. Bezpieczeństwo systemu Linux</p> <ul style="list-style-type: none"> a. Zarządzanie kontami użytkowników i grupami b. Uprawnienia plików i zarządzanie dostępem c. Mechanizmy bezpieczeństwa systemowego (SELinux, AppArmor) d. Aktualizacje i zarządzanie pakietami e. Zapora ogniowa f. Monitorowanie systemu i analiza logów <p>4. Bezpieczeństwo w systemie MacOS</p> <ul style="list-style-type: none"> a. Konta użytkowników i role b. Mechanizmy uwierzytelniania c. System plików APFS d. Kontrola prywatności i uprawnień aplikacji e. Mechanizmy zabezpieczeń systemu (XProtect, Gatekeeper, SIP) f. Szyfrowanie dysków za pomocą FileVault g. Aktualizacje i zarządzanie bezpieczeństwem <p>5. Dobre praktyki bezpieczeństwa</p> <ul style="list-style-type: none"> a. Silne hasła b. Uwierzytelnianie wieloskładnikowe c. Kopie zapasowe 	
Informatyka śledcza	30
<p>1. Teoria (Podstawy i Proces Informatyki Śledczej)</p> <ul style="list-style-type: none"> a. Definicje i podstawowe pojęcia b. Historia i rozwój informatyki śledczej c. Znaczenie informatyki śledczej w cyberbezpieczeństwie <p>2. Przegląd aktów prawnych i standardów dotyczących informatyki śledczej</p> <ul style="list-style-type: none"> a. Kluczowe przepisy prawne b. Międzynarodowe standardy i regulacje c. Przypadki prawne związane z informatyką śledczą <p>3. Proces Informatyki Śledczej</p> <ul style="list-style-type: none"> a. Fazy procesu śledczego (identyfikacja, zabezpieczenie, analiza, raportowanie) b. Zasady zachowania integralności dowodów cyfrowych c. Dokumentacja i raportowanie wyników <p>4. Zabezpieczanie Dowodów Cyfrowych</p> <ul style="list-style-type: none"> a. Techniki zabezpieczania miejsca zdarzenia b. Narzędzia i metody zbierania dowodów z komputerów c. Metody zabezpieczania dowodów z urządzeń mobilnych <p>5. Analiza Danych Cyfrowych</p> <ul style="list-style-type: none"> a. Podstawy analizy danych b. Narzędzia do analizy dysków twardych i systemów plików 	

<ul style="list-style-type: none"> c. Techniki odzyskiwania skasowanych i ukrytych danych 6. Analiza Sieciowa <ul style="list-style-type: none"> a. Zbieranie i analiza danych sieciowych b. Monitorowanie ruchu sieciowego c. Analiza logów systemowych i sieciowych 7. Analiza Malware <ul style="list-style-type: none"> a. Identyfikacja i klasyfikacja złośliwego oprogramowania b. Techniki analizy malware (statyczna i dynamiczna) c. Narzędzia do analizy złośliwego oprogramowania 8. Informatyka Śledcza w Chmurze <ul style="list-style-type: none"> a. Zbieranie dowodów w środowiskach chmurowych b. Wyzwania związane z infrastrukturą chmurową c. Narzędzia do śledztwa w chmurze 9. Śledztwa w Mediach Społecznościowych - OSINT <ul style="list-style-type: none"> a. Techniki zbierania dowodów z mediów społecznościowych b. Anonimowość i prywatność w mediach społecznościowych c. Analiza profili i aktywności w mediach społecznościowych 10. Warsztaty - Symulacja Zabezpieczania Miejsca Zdarzenia <ul style="list-style-type: none"> a. Praktyczne ćwiczenia w zabezpieczaniu dowodów b. Użycie narzędzi do zbierania dowodów c. Przechowywanie i transport dowodów 11. Warsztaty - Analiza Danych Cyfrowych <ul style="list-style-type: none"> a. Praktyczne ćwiczenia z użyciem narzędzi do analizy danych b. Odzyskiwanie skasowanych i ukrytych danych c. Tworzenie raportów z analizy danych 12. Warsztaty - Analiza Sieciowa i Malware <ul style="list-style-type: none"> a. Praktyczne ćwiczenia w analizie logów sieciowych b. Analiza przykładowego złośliwego oprogramowania c. Dokumentacja wyników analizy 13. Analiza rzeczowych przypadków śledczych 	
Warsztaty z CompTIA Security+	40
<ul style="list-style-type: none"> 1. Podstawowe koncepcje bezpieczeństwa <ul style="list-style-type: none"> a. Terminologia, koncepcje b. Mechanizmy kontrolne bezpieczeństwa 2. Porównanie różnych typów zagrożeń <ul style="list-style-type: none"> a. Aktorzy-zagrozenia b. Przestrzenie ataku c. Inżynieria społeczna 3. Omówienie podstawowych pojęć kryptografii <ul style="list-style-type: none"> a. Algorytmy kryptograficzne, b. Infrastruktura PKI c. Rozwiązania kryptograficzne 	

- | | |
|--|--|
| <ol style="list-style-type: none">4. Wdrażanie zarządzania tożsamością i kontrolą dostępu<ol style="list-style-type: none">a. Uwierzytelnianieb. Autoryzacjac. Zarządzanie tożsamością5. Zabezpieczanie architektury sieci korporacyjnej<ol style="list-style-type: none">a. Architektura sieci korporacyjnejb. Urządzenia zabezpieczające siećc. Bezpieczna komunikacja6. Zabezpieczanie architektury sieci w usługach chmurowych<ol style="list-style-type: none">a. Infrastruktura chmurowab. Systemy wbudowanec. Architektura Zero Trust7. Omówienie koncepcji odporności<ol style="list-style-type: none">a. Zarządzanie aktywamib. Strategie redundancjic. Bezpieczeństwo fizyczne8. Zarządzanie podatnościami<ol style="list-style-type: none">a. Podatności w urządzeniach i systemach operacyjnychb. Luki w oprogramowaniu i usługach chmurowychc. Metody identyfikacji luk w zabezpieczeniachd. Analiza i usuwanie luk w zabezpieczeniach9. Bezpieczeństwo sieciowe<ol style="list-style-type: none">a. Podstawowe założenia dotyczące bezpieczeństwa siecib. Podnoszenie poziomu bezpieczeństwa sieci10. Ocena bezpieczeństwa punktów końcowych<ol style="list-style-type: none">a. Wdrażanie zabezpieczeń punktów końcowychb. Wdrażanie zabezpieczeń urządzeń mobilnych11. Wdrażanie zabezpieczeń aplikacji<ol style="list-style-type: none">a. Wytyczne dla zabezpieczania aplikacjib. Koncepcje bezpieczeństwa aplikacji w chmurze i sieci Web12. Zarządzanie incydentami i monitorowanie środowiska<ol style="list-style-type: none">a. Reagowanie na incydentyb. Informatyka śledczac. Narzędzia do monitorowania13. Po czym rozpoznać atak – wskaźniki kompromitacji<ol style="list-style-type: none">a. Ataki złośliwym oprogramowaniemb. Ataki fizyczne i sieciowec. Ataki na aplikacje14. Zarządzania bezpieczeństwem w organizacji poprzez polityki, standardy i procedury<ol style="list-style-type: none">a. Polityki, standardy i proceduryb. Zarządzanie zmianamic. Automatyzacja i orkiestracja15. Podstawowe pojęcia związane zarządzania ryzykiem | |
|--|--|

<ul style="list-style-type: none"> a. Koncepcje zarządzania ryzykiem. b. Audyty i ocena ryzyka <p>16. Ochrona danych i dbałość o ich zgodność w organizacji</p> <ul style="list-style-type: none"> a. Klasyfikacja danych i zgodność b. Polityki personalne 	
Introduction to Microsoft Security, Compliance, and Identity. Przygotowanie do egzaminu	30
<ul style="list-style-type: none"> 1. Podstawowe pojęcia dotyczące bezpieczeństwa, zgodności i tożsamości <ul style="list-style-type: none"> a. Koncepcje i metodologie bezpieczeństwa b. Zasady bezpieczeństwa i zgodności firmy Microsoft 2. Koncepcje i możliwości rozwiązań firmy Microsoft do zarządzania tożsamością i dostępem <ul style="list-style-type: none"> a. Koncepcje tożsamości b. Podstawowe usługi i typy tożsamości usługi Azure AD c. Możliwości uwierzytelniania w usłudze Azure AD d. Możliwości zarządzania dostępem w usłudze Azure AD e. Możliwości ochrony tożsamości i zarządzania w usłudze Azure AD 3. Możliwości rozwiązań zabezpieczających firmy Microsoft <ul style="list-style-type: none"> a. Podstawowe funkcje zabezpieczeń na platformie Azure b. Możliwości zarządzania zabezpieczeniami platformy Azure c. Możliwości zabezpieczeń platformy Azure Sentinel d. Możliwości ochrony przed zagrożeniami platformy Microsoft 365 e. Możliwości zarządzania zabezpieczeniami platformy Microsoft 365 f. Zabezpieczenia punktów końcowych za pomocą usługi Microsoft Intune 4. Możliwości rozwiązań Microsoft zapewniających zgodność <ul style="list-style-type: none"> a. Możliwości zarządzania zgodnością w Microsoft b. Możliwości ochrony informacji i ładu korporacyjnego platformy Microsoft 365 c. Możliwości związane z ryzykiem wewnętrznym na platformie Microsoft 365 d. Możliwości eDiscovery platformy Microsoft 365 e. Możliwości audytu platformy Microsoft 365 f. Możliwości zarządzania zasobami na platformie Azure 5. Warsztat przygotowujący do egzaminu 	
Microsoft Security Operations Analyst	30
<ul style="list-style-type: none"> 1. Ograniczanie zagrożenia za pomocą usługi Microsoft 365 Defender 2. Ograniczanie zagrożenia za pomocą usługi Microsoft Defender dla punktów końcowych 3. Ograniczanie zagrożenia za pomocą usługi Microsoft Defender for Cloud 4. Tworzenie zapytań dla Microsoft Sentinel przy użyciu języka Kusto Query Language 5. Konfiguracja środowiska Microsoft Sentinel 6. Łączenie dzienników z Microsoft Sentinel 7. Wykrywanie i prowadzenie dochodzenia przy użyciu programu Microsoft Sentinel 8. Polowanie na zagrożenia w Microsoft Sentinel 	

RODO	10
<ol style="list-style-type: none"> 1. Wprowadzenie do RODO (GDPR) i jego znaczenie w cyberbezpieczeństwie. 2. Przetwarzanie danych osobowych i odpowiedzialność w kontekście technologicznym. 3. Zabezpieczenia techniczne i organizacyjne zgodnie z RODO. 4. Zarządzanie incydentami naruszenia danych i informatyka śledcza. 5. Zgodność z RODO w systemach AI i automatyzacji procesów. 6. Podsumowanie, sesja pytań i odpowiedzi oraz quiz sprawdzający. 	
Bezpieczeństwo aplikacji webowych	20
<ol style="list-style-type: none"> 1. Wprowadzenie do bezpieczeństwa aplikacji webowych. 2. Bezpieczeństwo ruchu sieciowego (TLS/SSL; Nagłówki HTTP, Same-Origin Policy i Cross-Origin Resource Sharing). 3. Narzędzia (Analiza ruchu sieciowego, manipulacja zapytaniami HTTP, tworzenie własnych skryptów, skanery podatności). 4. Analiza podatności (atak, obrona, przykład) 5. Bezpieczeństwo API 6. Czarnoskrzynkowy test penetracyjny (CTF) 	
Bezpieczeństwo Copilot	10
<ol style="list-style-type: none"> 1. Badanie projektu Copilot dla Microsoft 365 2. Wdrażanie Copilot dla Microsoft 365 3. Badanie bezpieczeństwa danych i zgodności w Copilot dla Microsoft 365 4. Zarządzanie bezpiecznym dostępem użytkowników w Microsoft 365 5. Zarządzanie rolami i grupami ról w Microsoft 365 6. Eksploracja wywiadu zagrożeń w Microsoft Defender XDR 	
Suma godzin	200