# Program studiów

**Kierunek studiów:** Bezpieczeństwo oraz cyberbezpieczeństwo instytucji finansowych i publicznych (AI)

**Rodzaj studiów:** studia podyplomowe

**Forma studiów:** stacjonarne / e-learning (online)

| Blok | | Opis | Kontent | Liczba godzin | ECTS |
|---|---|---|---|---|---|
| **Moduł I. Podstawy i teoria systemów bezpieczeństwa** | | | | | |
| **1.** | **Wprowadzenie do Bezpieczeństwa Informacji** | Ustawa o ochronie informacji niejawnych | Informacja niejawna w instytucjach państwowych | 8 | 3 |
| | | Kodeks pracy, ustawa o zwalczaniu nieuczciwej konkurencji, ustawa o ochronie danych osobowych, RODO, dyrektywa PE w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych | Tajemnica zawodowa w sektorze publicznym i prywatnym | | |
| **2.** | **Współczesne Zagrożenia Bezpieczeństwa** | Wszelkiego rodzaju klęski żywiołowe, katastrofy, wypadki, które wpływają na stan bezpieczeństwa informacyjnego organizacji (np. pożar budynku, w którym przechowywane są nośniki informacji) | Zagrożenia losowe | 12 | 5 |
| | | Szpiegostwo, działalność dywersyjna lub sabotażowa (ukierunkowana na zdobycie informacji, ofensywną dezinformację prowadzoną przez inne osoby, podmioty, organizacje) | Tradycyjne zagrożenia informacyjne | | |
| | | Zagrożenia związane z gromadzeniem, przechowywaniem, przetwarzaniem i przekazywaniem informacji w sieciach teleinformatycznych (do takich zagrożeń zaliczamy przestępstwa komputerowe, cyberterroryzm, walkę informacyjną) | Zagrożenia technologiczne | | |
| **3.** | **Technologie Ochrony Danych Finansowych** | Przekształcanie danych w kod, aby uniemożliwić nieautoryzowanym użytkownikom podgląd zawartości plików, nawet jeśli uzyskają dostęp do ich lokalizacji | Szyfrowanie danych | 16 | 7 |
| | | Zdefiniowana kontrola dostępu to podstawowy element zabezpieczeń, który determinuje, kto może uzyskać dostęp do określonych danych, aplikacji i zasobów oraz w jakich okolicznościach może to zrobić | Uwierzytelnianie i autoryzacja użytkownika | | |
| | | Tworzenie kopi danych, aby autoryzowani administratorzy mieli | Kopia zapasowa danych | | |

| | | | | | |
|---|---|---|---|---|---|
| | | sposób na ich przywracanie w przypadku awarii magazynu, naruszenia zabezpieczeń danych lub katastrofy dowolnego rodzaju | | | |
| | | Zautomatyzowany proces powiadomienia o potencjalnym niewłaściwym użyciu danych i możliwych problemach z zabezpieczeniami | Alerty w czasie rzeczywistym | | |
| **4.** | Bezpieczeństwo Sieci Komputerowych | Narzędzia i procesy mające na celu uniemożliwienie nieupoważnionym osobom fizycznego dotarcia do sieci (np. System Kontroli Dostępu) | Fizyczne bezpieczeństwo sieci | 12 | 5 |
| | | Uprawnienia regulujące, co konkretni użytkownicy mogą robić w sieci oraz szkolenia z zakresu cyberbezpieczeństwa | Administracyjne bezpieczeństwo sieci | | |
| | | Oprogramowanie i sprzęt, które monitorują procesy sieciowe w poszukiwaniu oznak włamania, poddają kwarantannie zidentyfikowane zagrożenia i powstrzymują nieautoryzowany ruch przed wejściem lub wyjściem z sieci | Techniczne bezpieczeństwo sieci | | |
| **5.** | **Audyt i Ocena Systemów Bezpieczeństwa** | Prowadzony jest przez pracowników danej instytucji w celu identyfikacji potencjalnych zagrożeń, luk w zabezpieczeniach i niezgodności z politykami bezpieczeństwa i procedurami wewnętrznymi | Audyt wewnętrzny | 12 | 5 |
| | | Wykonywany jest przez firmę zewnętrzną i jego celem jest identyfikacja potencjalnych zagrożeń i luk w zabezpieczeniach (łącznie z próbą ich przełamania) oraz ocena stopnia zgodności z przepisami prawnymi i standardami branżowymi | Audyt zewnętrzny | | |
| | | Zgodność systemów IT z przepisami RODO, wymaganiami ABW (Agencja Bezpieczeństwa Wewnętrznego), KNF (Komisja Nadzoru Finansowego), KRI (Krajowe Ramy Interoperacyjności), KSC (Krajowy System Cyberbezpieczeństwa) | Ocena zgodności | | |
| **6.** | **Ochrona Danych w Sektorze Publicznym** | Powinna określać zasady i wytyczne dotyczące zarządzania danymi, dostępu do nich, wymogi dotyczące haseł, kryptografii, procedur tworzenia kopii zapasowych, systemów it | Polityka bezpieczeństwa | 22 | 10 |
| | | Obejmują zastosowanie oprogramowania antywirusowego, zaporę sieciową, ochronę przed atakami DDoS, monitorowanie zdarzeń bezpieczeństwa (SIEM), kryptografię danych itp. | Systemy zabezpieczeń technologicznych | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Wdrożenie odpowiednich mechanizmów uwierzytelniania oraz ograniczenie dostępu do danych tylko dla upoważnionych użytkowników | Zarządzanie dostępem | | |
| | | OSINT | Nowoczesne techniki pozyskiwania informacji ze źródeł otwartych | | |
| | | Tworzenie kopi zapasowych na zewnętrznych nośnikach lub w chmurze, a także regularnie testowanie procesu przywracania danych, aby upewnić się, że są one skuteczne | Tworzenie kopii zapasowych danych | | |
| | | Szkolenia dotyczące zagrożeń związanych z phishingiem, atakami malware, ochroną haseł, poufnością danych oraz postępowaniem w przypadku podejrzenia naruszenia bezpieczeństwa | Szkolenia pracowników | | |
| **7.** | Polityka i Strategie Bezpieczeństwa Państwa | Polityka bezpieczeństwa (wojskowa, gospodarcza, energetyczna, informacyjna, ekologiczna), polityka bezpieczeństwa narodowego (wojskowa, zagraniczna). Strategia bezpieczeństwa publicznego, społecznego, informacyjnego, kulturowego, religijnego | Pojęcie polityki i strategii bezpieczeństwa | 28 | 12 |
| | | Obszar narodowy, regionalny i globalny. Elementy struktury bezpieczeństwa narodowego wynikające z celów wyznaczanych przez politykę | Obszar i zakres polityki i strategii bezpieczeństwa | | |
| | | Tworzenie aktów prawnych dotyczących bezpieczeństwa, kształtowanie postaw społecznych, zapewnienie poczucia bezpieczeństwa, rozwoju i sprawiedliwości, przewidywanie zagrożeń bezpieczeństwa państwa i sojuszy, współpraca międzynarodowa i zobowiązania sojusznicze, ochrona duchowego i materialnego dziedzictwa narodowego, ochrona środowiska naturalnego | Znaczenie polityki w bezpieczeństwie | | |
| | | Strategia bezpieczeństwa - działalność zmierzająca do realizacji (za pomocą odpowiednich narzędzi i rozwiązań) zasadniczych, długofalowych przedsięwzięć polityki bezpieczeństwa | Strategia w polityce bezpieczeństwa | | |
| | | Bankowość i system finansowy a bezpieczeństwo i wyzwania cyber | Bankowość i system finansowy w Polsce | | |
| | | Aspekty prawne bezpieczeństwa Państwa i jej instytucji | Konstytucyjne aspekty bezpieczeństwa instytucji Państwa | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Dokument opracowany przez zespół będący organem pomocniczym Rady Ministrów. Bezpieczeństwo państwa i obywateli, Polska w systemie bezpieczeństwa międzynarodowego, tożsamość i dziedzictwo narodowe, rozwój społeczny i gospodarczy, ochrona środowiska | Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020 | | |
| **8.** | **Polityka i Strategie Cyberbezpieczeństwa Państwa** | Rozwój krajowego systemu cyberbezpieczeństwa, zwiększenie odporności systemów informacyjnych administracji publicznej, zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa, budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa, zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa | Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 | 16 | 7 |
| | | Publiczne (organy państwa: władzy wykonawczej, ustawodawczej i sądowniczej, instytucje państwowe, agencje rządowe, samorząd terytorialny, aparat bezpieczeństwa państwa: wojsko, policja, służby) i prywatne (przedsiębiorcy, spółki, stowarzyszenia, fundacje, osoby fizyczne | Obszary występowania cyberzagrożeń | | |
| | | Ataki z użyciem szkodliwego oprogramowania (malware, wirusy), ataki socjotechniczne w celu wyłudzenia poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję (phishing), kradzieże tożsamości, spam, blokowanie dostępu do usług (mail bomb DDoS), ataki typu APT (advanced persistent threat), kradzieże, modyfikacje bądź niszczenie danych | Rodzaje zagrożeń cyberprzestrzeni | | |
| | | Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa. Celem ustawowym jest zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów | Krajowy system cyberbezpieczeństwa | | |
| **9.** | | SI może automatyzować wiele zadań, co przyspiesza procesy i zwiększa efektywność. SI może uczyć się na | Automatyzacja, uczenie maszynowe, rozpoznawanie wzorców, personalizacja | 8 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | **Sztuczna Inteligencja – Zagrożenia i Możliwości** | podstawie danych, co pozwala na tworzenie bardziej inteligentnych systemów. SI może analizować ogromne ilości danych i wykrywać ukryte wzorce, co ma zastosowanie w medycynie, finansach i innych dziedzinach. SI może dostosowywać się do indywidualnych potrzeb użytkowników, np. w rekomendacjach produktów czy treści | | | |
| | | SI może być wykorzystywana do ataków na prywatność i kradzieży danych. Automatyzacja może prowadzić do utraty miejsc pracy w niektórych sektorach. SI może popełniać błędy lub wykazywać uprzedzenia, jeśli nie jest odpowiednio zaprogramowana. Rozwój SI może prowadzić do zagrożeń dla ludzkości, np. w postaci superinteligencji | Bezpieczeństwo danych, bezrobocie, błędy i uprzedzenia, zagrożenie dla ludzkości | | |
| **10.** | **Instytucje odpowiedzialne za Bezpieczeństwo i Cyberbezpieczeństwo RP** | Utworzone na podstawie ustawy o obronie Ojczyzny z dnia 11 marca 2022 roku jako specjalistyczny komponent Sił Zbrojnych, właściwy do realizacji pełnego spektrum działań w cyberprzestrzeni, w szczególności w zakresie proaktywnej ochrony oraz aktywnej obrony elementów i zasobów cyberprzestrzeni kluczowych z punktu widzenia Sił Zbrojnych. WOC odpowiadają również w resorcie obrony narodowej za kluczowe obszary związane z kryptologią, cyberbezpieczeństwem oraz budową i eksploatacją systemów IT | Wojska Obrony Cyberprzestrzeni | 12 | 5 |
| | | Utworzone na podstawie ustawy z dnia 17 grudnia 2021 roku jako specjalistyczna jednostka organizacyjna Policji do której zadań należy rozpoznawanie i zwalczanie przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw oraz wspierania w tym zakresie innych jednostek organizacyjnych Policji | Centralne Biuro Zwalczania Cyberprzestępczości | | |
| | | Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Ministerstwo Obrony Narodowej, Ministerstwo Spraw Zagranicznych, Ministerstwo Finansów, Ministerstwo Sprawiedliwości, Prokuratura | Policja, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Krajowa, Rządowe Centrum Bezpieczeństwa | | | |
| **11.** | **Współpraca Międzynarodowa w Dziedzinie Cyberbezpieczeństwa** | Organizacje takie jak Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz inne instytucje międzynarodowe umożliwiają państwom współpracę w zakresie wymiany informacji na temat nowych zagrożeń, ataków i technik obronnych. To pozwala na szybsze reagowanie i dostosowywanie się do zmieniającego się krajobrazu cyberbezpieczeństwa | Współpraca i wymiana informacji | 16 | 7 |
| | | Współpraca w zakresie ustanawiania międzynarodowych standardów i ram prawnych jest kluczowa. Organizacje te mogą wypracowywać jednolite podejście do kwestii związanych z cyberbezpieczeństwem na arenie międzynarodowej. Przykładem jest Horyzontalna Grupa Robocza ds. Cyberbezpieczeństwa (HWP CI), która działa w Radzie UE | Standardy i ramy prawne | | |
| | | Organizowanie wspólnych ćwiczeń i symulacji pozwala na przetestowanie reakcji na różne scenariusze ataków. To pomaga w doskonaleniu umiejętności reagowania i koordynacji działań | Wspólne ćwiczenia i symulacje | | |
| | | Organizacje międzynarodowe wspierają państwa w ściganiu i zwalczaniu cyberprzestępczości. To obejmuje wymianę dowodów, śledzenie działań przestępczych i wspólne operacje | Wspólna walka z cyberprzestępczością | | |
| **12.** | **Egzamin sprawdzający wiedzę Moduł I** | Sesja egzaminacyjna nr 1 | | 4 | |
| **Moduł II. Praktyka działań w obszarze bezpieczeństwa** | | | | | |
| **13.** | **Wykład specjalistyczny eksperta – Bezpieczeństwo** | | | 4 | 3 |
| **14.** | **Wykład specjalistyczny eksperta – Cyberbezpieczeństwo** | | | 4 | 3 |
| **15.** | **Wykład specjalistyczny eksperta – Sztuczna Inteligencja** | | | 4 | 3 |
| **16.** | **Wykład specjalistyczny eksperta – Case Studies** | Zajęcia warsztatowe. | Faktyczne sytuacje zagrożenia bezpieczeństwa i cyberbezpieczeństwa wraz z przykładami właściwych oraz błędnych reakcji instytucji finansowych i publicznych. | 4 | 3 |
| **17.** | **Wykład specjalistyczny eksperta - Zagrożenia Kontrwywiadowcze** | Katalog współczesnych zagrożeń kontrwywiadowczych. Uwarunkowania krajowe i międzynarodowe aktywności wywiadowczej/kontrwywiadowczej. | Możliwości rozpoznawania, mitygacji i reakcji na zagrożenia kontrwywiadowcze. Przykłady spraw kontrwywiadowczych | 4 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | | | w kontekście wymiernych zagrożeń. | | |
| **18.** | **Wykład specjalistyczny eksperta – Sztuczna Inteligencja** | | | 4 | 3 |
| **19.** | **Wykład specjalistyczny - walka z fake newsami i komunikacja kryzysowa** | | | 4 | 3 |
| **20.** | **Egzamin sprawdzający wiedzę Moduł II** | Sesja egzaminacyjna nr 2 | | 4 | |
| **Moduł III. Geopolityka i skala globalna** | | | | | |
| **21.** | **Środowisko Bezpieczeństwa RP - Czynniki Zewnętrzne** | Udział RP w międzynarodowych organizacjach, jak NATO i UE. | Wpływ sojuszy dwustronnych, z sojuszem z USA na czele, jak też inicjatyw regionalnych na bezpieczeństwo Polski w kontekście zagrożeń zewnętrznych, szczególnie ze strony Rosji. | 4 | 3 |
| **22.** | **Podstawy Geopolityczne Bezpieczeństwa Międzynarodowego** | Doktryny geopolityki. | Wpływ doktryn na postrzeganie bezpieczeństwa międzynarodowego, ze szczególnym uwzględnieniem środowiska bezpieczeństwa UE/NATO oraz ich wschodniej flanki. | 4 | 3 |
| **23.** | **Wykład specjalistyczny eksperta - Dezinformacja** | Operacje dezinformacyjne Rosji wymierzone w Zachód. | Przykłady i podłoże teoretyczne. | 4 | 3 |
| **24.** | **Wykład specjalistyczny eksperta - Nielegałowie** | Skala zagrożenia bezpieczeństwa krajów Zachodu ze strony agentów obcego wywiadu wykorzystujących skradzioną tożsamość. | Przykłady. Warsztat służb. | 4 | 3 |
| **25.** | **Cyberaktywność Służb Specjalnych Rosji - Zagrożenia** | Grupy hakerów rosyjskich, ich aktywność i powiązania ze służbami. | Przykłady operacji. | 4 | 3 |
| **26.** | **Regionalne Konflikty, Globalne Zagrożenia - Case Studies** | Globalne skutki regionalnych konfliktów. | Jak wojny i rebelie w regionach Afryki i Bliskiego Wschodu wpływają na bezpieczeństwo Zachodu, Europy, Polski. | 4 | 3 |
| **27.** | **Prezentacja i obrona projektu - egzaminy końcowe** | Sesja egzaminacyjna nr 3 | | 4 | 3 |
| **28.** | **Wykład podsumowujący i wręczenie dyplomów** | | | 6 | |
| | | | Suma | 232 | 90 |