KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Krajowe zasoby informacyjne [S1Cybez1>KZI]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
2/3

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
16

Laboratorium
0

Inne
0

Ćwiczenia
0

Projekty/seminaria
24

Liczba punktów ECTS

3,00

Koordynatorzy

dr hab. inż. Mariusz Żal
mariusz.zal@put.poznan.pl

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

dr Renata Dąbrowska
renata.dabrowska@put.poznan.pl

Wykładowcy

Wymagania wstępne

• Podstawowa wiedza z zakresu cyberbezpieczeństwa. • Znajomość systemów informatycznych oraz podstawowych pojęć związanych z bezpieczeństwem informacji. • Umiejętność korzystania z narzędzi do analizy danych i systemów operacyjnych (Linux, Windows).

Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z pojęciem krajowych zasobów informacyjnych oraz ich znaczeniem w kontekście cyberbezpieczeństwa państwa. Studenci uzyskają wiedzę na temat systemów bazodanowych prowadzonych przez organy administracji publicznej oraz służby specjalne, ich podstaw prawnych, funkcjonalności oraz znaczenia dla bezpieczeństwa narodowego. Szczególny nacisk zostanie położony na zagadnienia ochrony informacji, koordynacji danych między instytucjami oraz reagowania na incydenty bezpieczeństwa. Przedmiot łączy elementy teoretyczne z praktycznymi ćwiczeniami dotyczącymi analizy, projektowania zabezpieczeń i reagowania na incydenty związane z krajowymi zasobami informacyjnymi.

Przedmiotowe efekty uczenia się

Wiedza:
• Zna podstawowe pojęcia związane z krajowymi zasobami informacyjnymi oraz ich rolą w systemie cyberbezpieczeństwa państwa. [K1_W21]
• Rozumie znaczenie infrastruktury krytycznej oraz kluczowych usług cyfrowych dla bezpieczeństwa państwa. [K1_W15]
• Zna regulacje prawne dotyczące ochrony zasobów informacyjnych w Polsce, w tym Ustawę o krajowym systemie cyberbezpieczeństwa (KSC), dyrektywę NIS2 oraz przepisy dotyczące ochrony informacji niejawnych. [K1_W21]
• Rozumie zasady funkcjonowania systemów bazodanowych prowadzonych przez organy administracji publicznej i służby specjalne. [K1_W21]
• Zna metody zabezpieczania danych i systemów informacyjnych oraz procedury reagowania na incydenty cyberbezpieczeństwa. [K1_W05]

Umiejętności:
• Potrafi identyfikować kluczowe krajowe zasoby informacyjne oraz oceniać ich znaczenie w kontekście bezpieczeństwa państwa. [K1_U15]
• Umie analizować i interpretować przepisy prawa oraz standardy dotyczące ochrony zasobów informacyjnych. [K1_U08]
• Potrafi wykorzystać narzędzia do analizy bezpieczeństwa systemów informacyjnych oraz oceny ryzyka.[K1_U06]
• Umie projektować podstawowe środki zabezpieczające oraz plany reakcji na incydenty dla krajowych zasobów informacyjnych. [K1_U07]
• Jest świadom konieczności planowania i realizowania własnego uczenia się przez całe życie [K1_U16]

Kompetencje społeczne:
• Rozumie znaczenie ochrony krajowych zasobów informacyjnych dla bezpieczeństwa narodowego. [K1_K05]
• Jest świadomy roli etycznej w pracy związanej z ochroną informacji publicznych i wrażliwych. [K1_K05]
• Potrafi podejmować odpowiedzialne decyzje w zakresie zarządzania ryzykiem związanym z ochroną zasobów informacyjnych. [K1_K02]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

1. Wiedza: test pisemny sprawdzający znajomość modeli kulturowych, etyki zawodowej i globalnych wyzwań technicznych.
2. Umiejętności: ocena realizacji projektu zespołowego oraz przygotowanej prezentacji wyników z uwzględnieniem aspektów międzykulturowych.
W każdej formie zaliczenia przedmiotu ocena zależy od liczby zdobytych przez studenta punktów w stosunku do maksymalnej liczby punktów obowiązkowych. Warunkiem pozytywnego zaliczenia jest otrzymanie co najmniej 50% punktów możliwych do zdobycia. Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

W ramach przedmiotu studenci zdobędą wiedzę na temat krajowych zasobów informacyjnych, ich

klasyfikacji oraz znaczenia dla cyberbezpieczeństwa państwa. Omówione zostaną podstawy prawne regulujące ochronę danych, w tym Ustawa o krajowym systemie cyberbezpieczeństwa, dyrektywy NIS oraz przepisy dotyczące ochrony informacji niejawnych. Studenci poznają wybrane systemy bazodanowe prowadzone przez administrację publiczną oraz służby specjalne, takie jak Krajowe Centrum Informacji Kryminalnych (KCIK). Zajęcia obejmą także tematykę dostępu do danych poufnych i tajnych, klauzul poufności oraz procedur uzyskiwania poświadczeń bezpieczeństwa wydawanych przez ABW. Szczególny nacisk zostanie położony na praktyczne aspekty ochrony informacji, w tym projektowanie zabezpieczeń, zarządzanie ryzykiem oraz reagowanie na incydenty bezpieczeństwa. Studenci będą mieli okazję zapoznać się z mechanizmami koordynacji informacji w Polsce oraz omówić rzeczywiste przypadki incydentów cyberbezpieczeństwa, analizując zastosowane środki ochrony i reakcje na zagrożenia. Kurs zakończy się projektem zespołowym, w którym uczestnicy zaprojektują kompleksowy plan zabezpieczenia wybranego zasobu informacyjnego.

Tematyka zajęć

Wykłady:
1. Wprowadzenie do informacji i krajowych zasobów informacyjnych:
• Definicja i znaczenie pojęcia "informacja" w kontekście bezpieczeństwa państwa.
• Społeczeństwo informacyjne - rola informacji w funkcjonowaniu państwa i obywateli.
• Klasyfikacja krajowych zasobów informacyjnych.
2. Podstawy prawne ochrony zasobów informacyjnych:
• Ustawa o krajowym systemie cyberbezpieczeństwa (KSC).
• Dyrektywa NIS i NIS2 oraz ich wpływ na krajowe regulacje prawne.
• RODO (GDPR) i przepisy dotyczące ochrony informacji niejawnych.
3. Systemy bazodanowe administracji publicznej i służb specjalnych:
• Omówienie wybranych systemów bazodanowych prowadzonych przez organy administracji publicznej (np. PESEL, CEIDG).
• Systemy bazodanowe służb specjalnych i "policyjnych" - Krajowe Centrum Informacji Kryminalnych (KCIK), systemy Policji i Straży Granicznej.
4. Bezpieczeństwo informacji i ochrona danych:
• Metody ochrony danych: szyfrowanie, uwierzytelnianie, kontrola dostępu.
• Organizacyjne środki ochrony informacji - procedury i dobre praktyki.
• Zagrożenia i błędy popełniane przez administratorów danych.
5. Dostęp do danych poufnych i tajnych:
• Zasady dostępu do danych poufnych i tajnych.
• Klauzula poufności w przedsiębiorstwach oraz wymogi bezpieczeństwa.
• Poświadczenia bezpieczeństwa wydawane przez Agencję Bezpieczeństwa Wewnętrznego (ABW).
6. Koordynacja informacji w Polsce:
• Mechanizmy koordynacji informacji między organami administracji publicznej a służbami specjalnymi.
• Kategorie przetwarzanych informacji i ich znaczenie dla bezpieczeństwa państwa.
• Mocne i słabe strony krajowego systemu koordynacji informacji.
7. Zarządzanie ryzykiem i reagowanie na incydenty:
• Metody oceny ryzyka dla zasobów informacyjnych.
• Proces zarządzania ryzykiem - identyfikacja, analiza, przeciwdziałanie.
• Procedury reagowania na incydenty - rola CERT, CSIRT, SOC.
• Planowanie ciągłości działania (BCP) i odtwarzania po awarii (DRP).
8. Studium przypadków:
• Analiza rzeczywistych incydentów związanych z krajowymi zasobami informacyjnymi.
• Dyskusja nad skutecznością podjętych środków ochrony i reakcji na incydenty.
Projekty:
Studenci w ramach przedmiotu będą realizować projekty zespołowe obejmujące następującą tematykę:
1. Opracowanie planu zabezpieczenia wybranego krajowego zasobu informacyjnego:
• Analiza ryzyka, projektowanie środków ochrony, planowanie reakcji na incydenty.
2. Symulacja incydentu bezpieczeństwa:
• Przygotowanie scenariusza incydentu, symulacja ataku oraz opracowanie raportu z działań w kontekście zasobów informacyjnych
3. Przegląd regulacji prawnych i opracowanie procedur zgodności:
• Przeanalizowanie obowiązujących przepisów prawa oraz opracowanie wewnętrznych procedur dotyczących ochrony danych i informacji niejawnych.
4. Analiza krajowych zasobów informacyjnych:

• Przygotowanie raportów z analizy wybranych elementów krajowych zasobów informacyjnych

Metody dydaktyczne

Wykłady: prezentacje multimedialne z elementami dyskusji i analiz studium przypadków.
Projekty zespołowe z zastosowaniem narzędzi informatycznych

Literatura

Podstawowa:
1. Ustawa o krajowym systemie cyberbezpieczeństwa, 2018 (z późniejszymi zmianami).
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS).
3. ISO/IEC 27001:2013 - Systemy zarządzania bezpieczeństwem informacji.
4. NIST Special Publication 800-37 - Risk Management Framework for Information Systems and Organizations.

Uzupełniająca:
1. Stallings, W. Network Security Essentials: Applications and Standards, Pearson, 2016.
2. Książki i raporty publikowane przez krajowe i międzynarodowe agencje ds. cyberbezpieczeństwa (np. CERT Polska, ENISA).
3. Materiały dostępne na stronach internetowych Narodowego Centrum Cyberbezpieczeństwa (NC Cyber).

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	80	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	40	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	40	1,50