Uniwersytet Gdański

Karta przedmiotu

Nazwa i kod przedmiotu	Bezpieczeństwo informacyjne (Ćw. audytoryjne), PG_00205615		
Kierunek studiów	Bezpieczeństwo narodowe (P)		
Data rozpoczęcia studiów	październik 2026 r.	Rok akademicki realizacji przedmiotu	2026/2027
Poziom kształcenia	I stopnia - licencjackie	Grupa zajęć	Grupa zajęć obowiązkowych z zakresu kierunku studiów Grupa zajęć powiązanych z praktycznym przygotowaniem zawodowym - profil praktyczny
Forma studiów	stacjonarne	Sposób realizacji	na uczelni
Rok studiów	1	Język wykładowy	polski
Semestr studiów	2	Liczba punktów ECTS	2.0
Profil kształcenia	praktyczny	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Rada Uczelni		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr Konrad Ćwikliński	
	Prowadzący zajęcia z przedmiotu		

Formy zajęć

Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
Liczba godzin zajęć	0.0	30.0	0.0	0.0	0.0	30

W tym liczba godzin zajęć na odległość: 0.0

Aktywność studenta i liczba godzin pracy

Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów	Udział w konsultacjach	Praca własna studenta	RAZEM
Liczba godzin pracy studenta	30	0.0	20.0	50

Cel przedmiotu

Celem przedmiotu Bezpieczeństwo informacyjne w formie ćwiczeń audytoryjnych jest przygotowanie studentów do rozumienia, analizowania i praktycznego rozwiązywania problemów związanych z bezpieczeństwem informacji w kontekście funkcjonowania państwa, instytucji publicznych oraz podmiotów prywatnych. Przedmiot ma na celu wykształcenie umiejętności identyfikacji zagrożeń informacyjnych, oceny ryzyka oraz stosowania środków zaradczych, w tym organizacyjnych, technicznych i prawnych. Szczególny nacisk położony zostanie na rozwijanie kompetencji w zakresie ochrony danych, cyberbezpieczeństwa, zarządzania incydentami bezpieczeństwa oraz analizowania współczesnych zagrożeń hybrydowych i dezinformacyjnych. W ramach ćwiczeń studenci zapoznają się z praktycznymi aspektami bezpieczeństwa informacyjnego od podstaw analizy informacji i oceny wiarygodności źródeł, przez modelowanie zagrożeń, po opracowanie procedur reagowania i zabezpieczania systemów informacyjnych. Ćwiczenia obejmują analizę rzeczywistych przypadków naruszeń bezpieczeństwa, tworzenie planów bezpieczeństwa informacyjnego, a także rozwiązywanie zadań symulacyjnych i problemowych.

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[BNL3_U07] Aktywnie uczestniczy w życiu społeczno-politycznym oraz podejmuje próby uczestnictwa w dyskursie publicznym. Kieruje procesem samokształcenia rozwija swój warsztat pracy oraz nowe umiejętności poznawcze. Planuje i organizuje pracę swoją i zespołu, przygotowując projekty społeczne, polityczne, ekonomiczne, obywatelskie (także te, które polegają na współdziałaniu z innymi osobami), korzystając z różnych źródeł i możliwości technologicznych.	Uczestniczy w projektach dotyczących bezpieczeństwa informacyjnego, wykorzystując źródła cyfrowe i narzędzia technologiczne.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU2] prezentacja/projekt/referat/ raport
[BNL3_U05] Wskazuje i wyjaśnia rolę państwa demokratycznego, a także społeczeństwa obywatelskiego w obszarze bezpieczeństwa.	Wyjaśnia rolę instytucji demokratycznych w zapewnianiu bezpieczeństwa informacyjnego.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU2] prezentacja/projekt/referat/ raport
[BNL3_U02] Analizuje przyczyny i przebieg procesów oraz ich ewolucji odnoszących się do społecznych, politycznych, ekonomicznych, prawnych, etycznych i kulturowych aspektów bezpieczeństwa.	Analizuje przyczyny i skutki procesów zagrożeń informacyjnych w kontekście społecznym, politycznym i prawnym.	[SU1] wypowiedź ustna/rozmowa/ dyskusja [SU2] prezentacja/projekt/referat/ raport
[BNL3_K04] Jest przygotowana do aktywności na rynku pracy, ma świadomość konieczności podnoszenia kwalifikacji odpowiedzialnego pełnienia ról zawodowych.	Jest przygotowany do pracy w sektorze ochrony informacji i rozumie potrzebę ciągłego doskonalenia zawodowego.	[SK1] wypowiedź ustna/rozmowa/ dyskusja [SK2] prezentacja/projekt/referat/ raport
[BNL3_W13] Posiada wiedzę z zakresu prawa własności intelektualnej, obejmującą ochronę praw autorskich oraz własności przemysłowej.	Student zna i rozumie zasady prawa autorskiego oraz ochrony własności intelektualnej w systemach informacyjnych.	[SW1] wypowiedź ustna/rozmowa/ dyskusja [SW2] prezentacja/projekt/referat/ raport
[BNL3_W08] W zaawansowanym stopniu wie jakie są mechanizmy w zarządzaniu ryzykiem i podejmowaniu decyzji w instytucjach bezpieczeństwa narodowego.	Posiada wiedzę o funkcjonowaniu państwa i społeczeństwa w kontekście ochrony informacji i cyberbezpieczeństwa	[SW1] wypowiedź ustna/rozmowa/ dyskusja [SW2] prezentacja/projekt/referat/ raport

Treści przedmiotu

Ramowy program przedmiotu (ćwiczenia audytoryjne)

1. Wprowadzenie do przedmiotu. Podstawowe pojęcia bezpieczeństwa informacji.
2. Klasyfikacja informacji. Ochrona informacji niejawnych i wrażliwych.
3. Źródła i typy zagrożeń informacyjnych. Przykłady cyberataków.
4. Analiza ryzyka. Metody i matryce oceny ryzyka.
5. Zarządzanie incydentami. Reagowanie i raportowanie.
6. Polityka bezpieczeństwa informacji. Tworzenie dokumentu.
7. Ochrona danych osobowych. Prawo autorskie i IP.
8. Audyt bezpieczeństwa informacji zasady i etapy.
9. Narzędzia audytorskie. Praca z checklistą i dokumentacją.
10. Systemy ISMS. Norma ISO/IEC 27001.
11. Inżynieria społeczna. Czynniki ludzkie w zagrożeniach.
12. Cyberbezpieczeństwo a bezpieczeństwo informacyjne.
13. Etyka i odpowiedzialność. Rola sygnalistów (whistleblowing).
14. Projekt audytu praca zespołowa.
15. Prezentacja projektów.. Podsumowanie.

Wymagania wstępne i dodatkowe

<table>
<tr><td>Sposoby i kryteria oceniania osiąganych efektów uczenia się</td><td colspan="2"><table>
<tr><th>Sposób oceniania (składowe)</th><th>Próg zaliczeniowy</th><th>Składowa oceny końcowej</th></tr>
<tr><td>Aktywność w zajęciach</td><td>50.0%</td><td>65.0%</td></tr>
<tr><td>Praca w grupach</td><td>50.0%</td><td>35.0%</td></tr>
</table></td></tr>
<tr><td rowspan="3">Zalecana lista lektur</td><td>Podstawowa lista lektur</td><td>1. Gajewski J., Bezpieczeństwo informacji i usług w systemach teleinformatycznych, Wydawnictwo PJWSTK, Warszawa, 2021.
2. Polański P., Bezpieczeństwo informacji w praktyce, Wolters Kluwer, Warszawa, 2020.
3. Górski J., Systemy zarządzania bezpieczeństwem informacji według ISO/IEC 27001, PWN, Warszawa, 2019.
4. Tadeusiewicz R., Bezpieczeństwo informacji. Wprowadzenie do ochrony danych i informacji w systemach informatycznych, Wydawnictwa AGH, Kraków, 2020.
5. Chmielarz W., Zarządzanie bezpieczeństwem informacji w organizacjach, Wydawnictwo Naukowe WZ UW, Warszawa, 2022.
6. Solms R. von, van Niekerk J., Information Security Context and Techniques, Routledge, London, 2017.
7. Harris S., CISSP All-in-One Exam Guide, McGraw-Hill, New York, 2022.
8. Smith R.E., Elementary Information Security, Jones & Bartlett Learning, Burlington, 2021.
9. ISO/IEC 27001:2022 Information Security Management Systems Requirements, ISO, Geneva, 2022.
10. Peltier T.R., Information Security Policies, Procedures, and Standards, Auerbach Publications, Boca Raton, 2021.</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td>1. Grzelak M., Zarządzanie ryzykiem w cyberbezpieczeństwie, Difin, Warszawa, 2021.
2. Gąsiorowska A., Bezpieczeństwo informacji i ochrona danych osobowych, Poltext, Warszawa, 2020.
3. Bidziński K., Zarządzanie bezpieczeństwem informacji w administracji publicznej, CeDeWu, Warszawa, 2019.
4. Calder A., IT Governance: An International Guide to Data Security and ISO27001/ISO27002, Kogan Page, London, 2021.
5. Tipton H.F., Krause M., Information Security Management Handbook, Auerbach Publications, Boca Raton, 2021.
6. Andress J., The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Syngress, Oxford, 2020.
7. Greengard S., Cybersecurity and Privacy: Issues in the Age of Digital Transformation, MIT Press, Cambridge, 2021.
8. NIST SP 800-30, Guide for Conducting Risk Assessments, National Institute of Standards and Technology, Gaithersburg, 2012.
9. Białek R., Bezpieczeństwo informacji w systemach informatycznych, PWN, Warszawa, 2018.
10. Disterer G., ISO/IEC 27000, 27001 and 27002 for Information Security Management, Journal of Information Security, 2013.</td></tr>
<tr><td>Adresy eZasobów</td><td></td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td colspan="2">1. Co to jest analiza ryzyka w bezpieczeństwie informacji?
2. Jakie są różnice między polityką bezpieczeństwa a procedurami operacyjnymi?
3. Wymień podstawowe elementy systemu zarządzania bezpieczeństwem informacji zgodnego z ISO/IEC 27001.
4. Jakie są typowe zagrożenia w systemach informacyjnych?
5. Jakie znaczenie ma człowiek w systemie bezpieczeństwa informacji?</td></tr>
<tr><td>Praktyki zawodowe w ramach przedmiotu</td><td colspan="2">Nie dotyczy</td></tr>
</table>