



Akademia Nauk Stosowanych
im. Hipolita Cegielskiego w Gnieźnie Uczelnia Państwowa

SYLABUS

Pozycja przedmiotu w planie:		R.II / S.III
1. OGÓLNY OPIS PRZEDMIOTU		
1	Nazwa modułu	Moduł zajęć specjalnościowych
2	Nazwa przedmiotu	Techniki zabezpieczania (OPSEC) i pozyskiwania (OSINT) informacji
3	Kierunek studiów	Bezpieczeństwo wewnętrzne
4	Poziom studiów	Licencjackie
5	Forma studiów	Stacjonarne
6	Profil studiów	Praktyczny
7	Rok studiów	Drugi
8	Semestr przedmiotu	Trzeci
9	Jednostka prowadząca kierunek studiów	Instytut Nauk o Bezpieczeństwie
10	Liczba punktów ECTS	2
11	Sposób zaliczenia:	Zaliczenie z oceną
12	Imię i nazwisko nauczyciela (li) akademickiego (ich), stopień lub tytuł naukowy, adres e-mail	Dr Leonard Dajerling Mgr Karol Geppert
13	Imię i nazwisko koordynatora(ów) przedmiotu, stopień lub tytuł naukowy, adres e-mail	Dr Leonard Dajerling
14	Język wykładowy	Polski
15	Tryb prowadzenia zajęć	Mieszany
16	Sposób prowadzenia zajęć	Synchroniczny
17	Narzędzia informatyczne wykorzystywane do prowadzenia zajęć, udostępniania materiałów i komunikacji ze studentami	Platforma Microsoft Teams/Patforma Moodle
15	Przedmioty wprowadzające	Metodologia badań, Logika
16	Wymagania wstępne	Umiejętność logicznego myślenia
17	Cele przedmiotu:	
C1	Celem zajęć jest zapoznanie studentów z metodami i narzędziami pozyskiwania, analizowania oraz wykorzystywania informacji dostępnych w otwartych źródłach (OSINT – Open Source Intelligence).	
C2	Studenci poznają etyczne i prawne aspekty OSINT oraz sposoby zabezpieczenia własnej aktywności podczas prowadzenia działań wywiadowczych OPSEC	
C3	Celem jest zapoznanie studentów z nowoczesnymi technologiami cyfrowymi stosowanymi do pozyskiwania, przetwarzania i analizy informacji w różnych kontekstach, w tym w zarządzaniu, bezpieczeństwie i naukach społecznych.	
18	Forma zajęć, liczba godzin wymagająca bezpośredniego udziału nauczyciela akademickiego, liczba godzin nakładu pracy studenta	
Forma zajęć		Liczba godzin
Wykład		15
Zajęcia: projektowe		45
Suma godzin		60
Ip.	Całkowity nakład pracy studenta	

	Nakład pracy związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela akademickiego wynosi:	Godzinowe obciążenie studenta
	Wykład	60 godzin
	Ćwiczenia	
	Nakład pracy związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela akademickiego wynosi 45 godzin, co odpowiada 1,5 punktom ECTS.	
2	Bilans nakładu pracy studenta: 1. przygotowanie do ćwiczeń 2. praca własna studenta Łączny nakład pracy studenta wynosi 25 godzin, co odpowiada 1 punktom ECTS.	25 godzin
3	Łączny nakład pracy studenta	95 godzin
4	Punkty ECTS za przedmiot	2 ECTS
5	Liczba punktów ECTS, którą student musi osiągnąć w ramach zajęć o charakterze praktycznym w tym zajęć laboratoryjnych, warsztatowych, projektowych	1 ECTS
Efekty uczenia się - wiedza		[BW1_W02] Zna podstawowe terminy, definicje i typologie z zakresu bezpieczeństwa wewnętrznego, w tym filozofii bezpieczeństwa i etyki zawodowej [P6U_W] [PS6_WK] [BW1_W01] Wie czym jest wiedza naukowa oraz posiada podstawową wiedzę z zakresu nauk o bezpieczeństwie, ich miejscu w systemie nauk i roli jaką odgrywają one w naukach społecznych w odniesieniu do współczesnej filozofii nauki [P6U_W] [PS6_WG] [BW1_W04] Rozumie filozofię bezpieczeństwa jako wiedzę o jednej z podstawowych potrzeb człowieka (poczucie bezpieczeństwa) w skali jednostkowej, lokalnej, krajowej, subregionalnej i globalnej. Potrafi zdefiniować terroryzm, zna problemy związane z zagrożeniem terrorystycznym oraz uwarunkowania bezpieczeństwa na wszystkich tych poziomach. [P6U_W] [PS6_WG] [PS6_WK]
Efekty uczenia się - umiejętności		[BW1_U06] Posiada umiejętność jasnego formułowania poleceń i komunikowania się w sposób klarowny i zwięzły, zna reguły komunikacji i zagrożenia w procesie komunikowania się szczególnie przy rozwiązywaniu konfliktów. [P6U_U] [PS6_UK] [PS6_UW] [BW1_U07] Posiada umiejętność dokonania analizy problemu, klarownego wyłożenia swoich racji i zaproponowania rozwiązania. [P6U_UU] [PS6_UK] [PS6_UW]
Efekty uczenia się – kompetencje społeczne		[BW1_K04] Posiada umiejętności negocjacyjne, potrafi rozwiązywać konflikty w dążeniu do realizacji nadrzędnego celu. [P6U_K] [PS6_KK] [PS6_KO] [BW1_K05] Potrafi podnosić swoje kwalifikacje i kompetencje rozumie konieczność permanentnego doskonalenia się. [P6U_K] [PS6_KK] [BW1_K06] Jest świadom ograniczeń własnej wiedzy i umiejętności, potrafi krytycznie spojrzeć na efekty własnej pracy i podnosić jej efektywność, jest gotów do ponoszenia odpowiedzialności za przydzielony odcinek zadań. [P6U_K] [PS6_KK] [PS6_KO] [PS6_KR]

2. TREŚCI PROGRAMOWE ODNIESIONE DO EFEKTÓW UCZENIA SIĘ		
Forma zajęć	Treści programowe	liczba godzin
Forma:		
W	Wykład: 1. Wprowadzenie do OSINT - Definicja i znaczenie białego wywiadu - Historia i rozwój OSINT - Zastosowanie OSINT w sektorze publicznym i prywatnym - OSINT a inne formy wywiadu (HUMINT, SIGINT, IMINT) - Przegląd narzędzi wykorzystywanych w OSINT Źródła: M. Bazzell, <i>Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information</i>, 10th Edition, 2023. R. Hopton, <i>Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence</i>, 2021.	15

	• Artykuły na stronie Bellingcat (https://www.bellingcat.com/) 2. Prawne i etyczne aspekty OSINT • Prawo międzynarodowe i krajowe dotyczące wywiadu jawnoźródłowego • Granice etyczne i moralne w OSINT • Problematyka prywatności i ochrona danych osobowych • RODO i OSINT – aspekty praktyczne • Case study: głośne przypadki naruszeń etyki w OSINT Źródła: • K. Vermeulen, <i>OSINT Techniques and Ethics: Open Source Intelligence in a Digital World</i>, 2022. • R. A. Clarke, <i>Cyber War: The Next Threat to National Security and What to Do About It</i>, 2012. • Strona Electronic Frontier Foundation (https://www.eff.org/) 3. Narzędzia i techniki OSINT • Wyszukiwanie informacji w Google – zaawansowane operatory • Meta-wyszukiwarki i alternatywne sposoby zdobywania informacji • Analiza zasobów dostępnych w social media • Dark Web i Deep Web – legalność i metody eksploracji • Automatyzacja procesów OSINT Źródła: • H. Bergman, <i>Google Hacking for Penetration Testers</i>, 3rd Edition, 2016. • Strona OSINT Techniques (https://osintcurio.us/) • Narzędzia OSINT na Intel Techniques (https://inteltechniques.com/) 4. Analiza, weryfikacja i raportowanie w OSINT • Weryfikacja źródeł i analiza wiarygodności • Metody rozpoznawania dezinformacji • Narzędzia do analizy danych wizualnych (fotografii, wideo, metadanych) • Tworzenie raportów wywiadowczych • Przykłady raportów OSINT Źródła: • B. Buchanan, <i>The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics</i>, 2020. • Artykuły i raporty na First Draft News (https://www.firstdraftnews.org/) • Narzędzia do analizy zdjęć i wideo: InVID, ExifTool, Google Reverse Image Search 5. Wprowadzenie do OPSEC • Definicja i geneza OPSEC (program <i>Purple Dragon</i>, doświadczenia wojskowe i cywilne). • Rola OPSEC w bezpieczeństwie wewnętrznym, militarnym i cyberbezpieczeństwie. • Podstawowe pojęcia: zagrożenie, luka informacyjna, wskaźnik (indicator), środek przeciwdziałania. Źródła: • U.S. Joint Chiefs of Staff, <i>Joint Publication 3-13.3: Operations Security (OPSEC)</i>, 2020. • DOE, <i>Operations Security (OPSEC) Program Manual</i>, DOE M 471.6-1, 2011. • J. C. Wentz, <i>Cybersecurity and Operations Security in the Modern Era</i>, CRC Press, 2022. 6. Proces OPSEC – pięć kroków • Identyfikacja krytycznych informacji. • Analiza zagrożeń (threat assessment). • Analiza podatności (vulnerability assessment). • Ocena ryzyka i dobór środków przeciwdziałania. • Wdrażanie i monitorowanie środków OPSEC. Źródła: • U.S. Army, <i>FM 3-13: Information Operations</i>, 2016. • M. J. Kowalski, <i>Bezpieczeństwo informacyjne organizacji</i>, Difin, 2020. • N. Kshetri, <i>Cybersecurity and Cyberwarfare: Introduction and Perspectives</i>, Springer, 2019. 7. Narzędzia i techniki OPSEC • Środki organizacyjne, techniczne i proceduralne. • OPSEC w cyberprzestrzeni – anonimizacja, ochrona metadanych, bezpieczne korzystanie z social media. • Studia przypadków naruszeń OPSEC (np. Snowden, wycieki z operacji NATO).	
--	---	--

	Źródła: • B. Szafranski, <i>Ochrona informacji niejawnych i bezpieczeństwo informacyjne</i>, Wolters Kluwer, 2018. • C. Hadnagy, <i>Social Engineering: The Science of Human Hacking</i>, Wiley, 2018. • CERT Polska, Raporty roczne o stanie bezpieczeństwa w cyberprzestrzeni (https://cert.pl/raporty). 8. Aspekty prawne i etyczne OPSEC • OPSEC a prawo do informacji i wolność słowa. • Balans między bezpieczeństwem organizacji a prawami jednostki. • Regulacje krajowe i międzynarodowe dotyczące ochrony informacji (m.in. RODO, ustawa o ochronie informacji niejawnych). Źródła: • Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. • Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). • R. A. Clarke, <i>Cyber War: The Next Threat to National Security and What to Do About It</i>, HarperCollins, 2012.	
Ć	Ćwiczenia: 1. Praktyczne zastosowanie Google Hacking i meta-wyszukiwarek • Ćwiczenia z wykorzystaniem operatorów Google (site:, filetype:, intitle:) • Analiza ukrytych informacji w dokumentach dostępnych online • Poszukiwanie informacji w archiwach internetowych (np. Wayback Machine) Źródła: • Strona Google Hacking Database (https://www.exploit-db.com/google-hacking-database) 2. OSINT w social media • Wyszukiwanie danych na Facebooku, Twitterze, Instagramie, LinkedIn • Narzędzia do analizy kont społecznościowych (np. Maltego, Social Mapper) • Analiza sieci społecznych – praktyczne przykłady Źródła: • OSINT Techniques Blog (https://osintcurio.us/) • Narzędzia: Tinfoleak, Twint, SocioSpyder 3. Geolokalizacja i analiza zdjęć • Weryfikacja zdjęć i materiałów wideo (ExifTool, InVID) • Narzędzia do geolokalizacji: Google Earth Pro, Mapillary, Wikimapia • Praktyczne zadania – odnajdywanie miejsc na podstawie zdjęć Źródła: • Bellingcat's Online Investigation Toolkit (https://www.bellingcat.com/resources/) 4. Automatyzacja OSINT • Scraping danych z internetu (np. BeautifulSoup, Selenium) • Tworzenie alertów w OSINT (Google Alerts, Tweetdeck) • Wprowadzenie do skryptów OSINT w Pythonie Źródła: • Python for OSINT Practitioners (https://github.com/jivoi/awesome-osint) 5. Tworzenie raportu OSINT – studium przypadku • Zastosowanie zdobytych umiejętności do analizy rzeczywistego zagadnienia • Weryfikacja informacji i prezentacja raportu • Dyskusja nad wynikami i wnioskami Źródła: • OSINT Framework (https://osintframework.com/) • The Verification Handbook (https://verificationhandbook.com/) 6. Identyfikacja informacji krytycznych • Ćwiczenie: analiza fikcyjnej organizacji i wskazanie informacji krytycznych, które mogą być wykorzystane przez przeciwnika. Źródła: • U.S. Joint Chiefs of Staff, <i>JP 3-13.3 OPSEC</i>, 2020. • DOE, <i>Operations Security Program Manual</i>, 2011. 7. Analiza podatności • Warsztaty: symulacja ataku przeciwnika (red teaming) i ocena, jakie informacje można pozyskać z niechronionych źródeł. Źródła:	45

	- Red Team Journal (https://redteamjournal.com/). J. W. Baggett, <i>Red Teaming: Transform Your Business by Thinking Like the Enemy</i>, HarperBusiness, 2013. 8. Środki przeciwdziałania - Projekt grupowy: opracowanie planu OPSEC dla instytucji publicznej (np. policja, administracja). Źródła: B. Szafrński, <i>Ochrona informacji niejawnych i bezpieczeństwo informacyjne</i>, Wolters Kluwer, 2018. - NIST, <i>Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)</i>, 2010. 9. OPSEC w mediach społecznościowych - Studium przypadku: analiza profili w social media i wskazanie zagrożeń wynikających z nadmiernego ujawniania informacji. Źródła: C. Hadnagy, <i>Social Engineering: The Science of Human Hacking</i>, Wiley, 2018. - OSINTCurio.us (https://osintcurio.us/). - Raporty Bellingcat (https://www.bellingcat.com/).	
--	--	--

3. Literatura	
Literatura podstawowa	Podana w treści programowej
Literatura uzupełniająca	Provost, F., & Fawcett, T. (2013). <i>Data Science for Business: What You Need to Know About Data Mining and Data-Analytic Thinking</i> . O'Reilly Media. Zeng, D., Chen, H., Lusch, R., & Li, S. H. (2010). <i>Social Media Analytics and Intelligence</i> . IEEE Intelligent Systems. Howard, P. N., & Hussain, M. M. (2013). <i>Democracy's Fourth Wave? Digital Media and the Arab Spring</i> . Oxford University Press.

4. Metody dydaktyczne	
Forma	Metody dydaktyczne
Wykład	Metody podające - wykład informacyjny, wykład konwersatoryjny, opowiadanie, opis Metody eksponujące (pokaz, prezentacja multimedialna, pomoce dydaktyczne, symulacja).
Ćwiczenia	Metody poszukujące- problemowe – sytuacyjna, burza mózgowa, metody ćwiczeniowo-praktyczne – projekt, studium przypadku, laboratoryjna, doświadczeń, obserwacji, dyskusja – panelowa, okrągłego stołu, punktowana, referatu

5. Metody i kryteria oceniania	
Forma zajęć: Wykład	Forma zaliczenia: Zaliczenie
Uzyskane punkty są przeliczane na oceny według następującej skali: Procent punktów Ocena 91-100% Bardzo dobry 85-90% Dobry plus 76-84% Dobry 66-75% Dostateczny plus 51-65% Dostateczny 0-50% Niedostateczny	
Opis: Rozwiązanie zadań	
Warunkiem zaliczenia przedmiotu jest uzyskanie powyżej 51% punktów	
Forma zajęć: Zajęcia: projektowe	Forma zaliczenia: Zaliczenie z oceną

Uzyskane punkty są przeliczane na oceny według następującej skali:	
Procent punktów	Ocena
91-100%	Bardzo dobry
85-90%	Dobry plus
76-84%	Dobry
66-75%	Dostateczny plus
51-65%	Dostateczny
0-50%	Niedostateczny
Opis: Odpowiedź ustna za pytania problemowe	
Warunkiem zaliczenia przedmiotu jest uzyskanie powyżej 51% punktów	

	Zatwierdzenie karty opisu zajęć	
	Stanowisko Tytuł/stopień naukowy, imię nazwisko	Podpis
Opracował	Dr Leonard Dajerling mgr Karol Geppert	
Zatwierdził	Dyrektor Instytutu p.o. mgr K. Geppert	