Załącznik Nr 2.10

Wydział/~~Instytut~~ Informatyki

kierunek studiów: Cyberbezpieczeństwo

dyscyplina wiodąca: informatyka techniczna i telekomunikacja

profil kształcenia: ogólnoakademicki

poziom kształcenia: studia II stopnia

numer uchwały Senatu* 49/2025/2026 z dnia 28 kwietnia 2026 r.

Lp.	Zajęcia	Kierunkowe efekty uczenia się	Treści programowe	Sposoby weryfikacji efektów uczenia się
1	Zaawansowane metody programistyczne	K_W04 Zna zaawansowane mechanizmy i standardy bezpieczeństwa stosowane w systemach rozproszonych, sieciach i systemach Internetu Rzeczy. K_W05 Zna i rozumie, w pogłębionym stopniu, cykl życia systemów informatycznych z uwzględnieniem procesów projektowania, wdrażania, testowania, utrzymania i zapewnienie cyberbezpieczeństwa. K_K01 Rozumie dynamikę zmian, w zakresie wiedzy i umiejętności, charakterystyczną dla cyberbezpieczeństwa, jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści, uznaje znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięganie opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu. K_U12 Potrafi wykonać typowe dla cyberbezpieczeństwa proste systemy, narzędzia lub konfiguracje zabezpieczeń zgodnie z określoną specyfikacją, dobierając właściwe metody, techniki i środowiska, a także poprawnie realizując proces implementacji i testowania.	Przedmiot ma na celu ukazanie studentom, jak różne obszary informatyki są ze sobą powiązane w kontekście tworzenia i testowania bezpiecznego oprogramowania w tym z modułami sprzętowymi (bazy danych, sieci komputerowe, systemy wbudowane). Zajęcia mają również na celu przygotowanie studentów do zrozumienia wymagań dotyczących biegłości programistycznej i praktycznej znajomości takich dziedzin jak sieci komputerowe czy bazy danych, które będą rozwijane w dalszej części studiów.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
2	Bezpieczeństwo ofensywne infrastruktury IT	K_W01 Ma pogłębioną i uporządkowaną wiedzę z zakresu informatyki technicznej i telekomunikacji oraz procesów zachodzących w systemach i sieciach teleinformatycznych, istotnych dla zapewniania bezpieczeństwa ich działania. K_K04 Jest gotów do inicjowania działań na rzecz bezpieczeństwa w cyberprzestrzeni oraz popularyzowania wiedzy o zagrożeniach i dobrych praktykach wśród społeczeństwa.	1. Wektory ataków na tle modelu IOS/OSI; 2. Narzędzia ataków w warstwie L2/L3. Metody zaburzania sesji TCP; 3. Wektory ataków w warstwie sesji; 4. Wektory ataków na protokoły warstwy aplikacji (HTTP, DNS, SSH, SMB, RDP, SMTP, TLS); 5.Struktura domen, DNS footprinting, WHOIS; 6. Metodyka rozpoznawania usług – nmap, dig, Shodan; 7. Pasywna analiza środowiska sieciowego - rozpoznanie typu Reconnaissance, skanowanie hostów - Nmap; 8. Aktywna analiza środowiska sieciowego - budowa własnych pakietów - scapy; 9. Unikanie wykrycie skanowania zasobów.; 10. Kontrola dostępu vs błędy autoryzacji: analiza logów prób logowania, OWASP; 11. Podatności - baza CVE. 12. Inżynieria społeczna: Social Engineer Toolkit (SET), rubby duck."	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
3	Kryptografia kwantowa i postkwantowa	K_W03 Ma pogłębioną wiedzę o faktach, metodach i narzędziach analizy danych w kryptografii i systemach bezpieczeństwa oraz zna główne trendy, kierunki badań i nowe technologie w cyberbezpieczeństwie wraz z ich wpływem na gospodarkę i społeczeństwo, co umożliwia rozwiązywanie złożonych problemów tego obszaru. K_U02 Potrafi wykorzystywać metody analityczne, symulacyjne i eksperymentalne w analizie i ocenie bezpieczeństwa systemów informatycznych oraz do definiowania i rozwiązywania zadań inżynierskich w tym problemów badawczych K_U03 Potrafi wykrywać podatności i ataki, analizować i oceniać ryzyko w systemach teleinformatycznych oraz opracowywać i wdrażać procedury i strategie ochrony, w tym dla sieci bezprzewodowych i IoT, a także oceniać przydatność nowych rozwiązań technicznych i proponować ich ulepszenia. K_U05 Potrafi oszacować przydatność, aspekt ekonomiczny i posługiwać się zaawansowanymi metodami i narzędziami informatycznymi, analitycznymi i diagnostycznymi w zadaniach inżynierskich i naukowych, dotyczących cyberbezpieczeństwa, łącząc wiedzę z różnych obszarów informatyki i innych dyscyplin.	Podstawy mechaniki kwantowej i komputerów kwantowych. Protokoły dystrybucji klucza kwantowego (QKD). Zagrożenia wynikające z algorytmów Shora i Grovera dla tradycyjnych systemów kryptograficznych. Algorytmy postkwantowe, w tym kratowe. Podpisy postkwantowe. Kryptografia kodowa. Standaryzacja kryptografii postkwantowej wg NIST (ML-KEM). Ochrona infrastruktury cyfrowej, danych i komunikacji. Praktyczne aspekty implementacji kryptografii kwantowej i postkwantowej. Przygotowanie i przeprowadzenie migracji do kwantoodpornej infrastruktury kryptograficznej. Kierunki badań i rozwoju technologii postkwantowych.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
4	Zwinne metodyki zarządzania projektami	K_W05 Zna i rozumie, w pogłębionym stopniu, cykl życia systemów informatycznych z uwzględnieniem procesów projektowania, wdrażania, testowania, utrzymania i zapewnienie cyberbezpieczeństwa. K_W07 Ma wiedzę o zasadach tworzenia i prowadzenia działalności gospodarczej, w tym startupów technologicznych w obszarze IT i cyberbezpieczeństwa. K_U07 Potrafi pracować indywidualnie i w zespole (także kierując jego pracą), biorąc odpowiedzialność za jej wyniki, oraz samodzielnie określać kierunki rozwoju zawodowego i naukowego, planować i realizować samokształcenie, a także ukierunkowywać w nim innych. K_K03 Jest gotów do pełnienia ról zawodowych i społecznych wymagających odpowiedzialności, przywództwa i współpracy w zespołach interdyscyplinarnych.	Wprowadzenie do zwinnego zarządzania projektami z uwzględnieniem i odniesieniu do cyklu życia systemów informatycznych. Filozofia, pryncypia i zmienne projektowe. Czynniki wpływające na sukces w Agile. Proces w zwinnym zarządzaniu projektem. Role i odpowiedzialność w metodykach AgilePM i Scrum. Współpraca w zespole projektowym. Definiowanie wymaga. Szacowanie w zwinnym zarządzaniu. Komunikacja w zespole projektowym. Konflikt w zespole projektowym. Dekalog dobrych praktyk. Związek z właściwym zarządzaniem a sukcesem gospodarczym podmiotu.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.

5	Metodologia badań naukowych	K_W02 Zna metodologiczne podstawy prowadzenia badań naukowych oraz ma wiedzę dotyczącą metodyki prowadzenia prac badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa. K_U01 Potrafi samodzielnie pozyskiwać informacje z różnych źródeł, krytycznie je analizować i twórczo interpretować oraz formułować i testować hipotezy, prowadzić eksperymenty i symulacje oraz prezentować ich wyniki, stosując właściwe metody do rozwiązywania złożonych problemów bezpieczeństwa IT K_U09 posiada praktyczne umiejętności posługiwania się językiem angielskim na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego K_U11 Potrafi odpowiednio dobierać źródła i selekcjonować informacje, dokonywać ich krytycznej analizy, syntezy i oceny w celu prognozowania, wyjaśnienia i rozwiązania problemów w obszarze cyberbezpieczeństwa	Pojęcie i istota badań naukowych; Dziedziny i dyscypliny naukowe; Charakterystyka problemów badawczych; Rodzaje metod badawczych (obserwacje, eksperymenty, badania dokumentów, sondaż, metody statystyczne, symulacja komputerowa, metody heurystyczne);Pomiar w badaniach naukowych, niepewność pomiarowa; Matematyka i narzędzia informatyczne w nauce (identyfikacja modeli i parametrów);Rodzaje, charakterystyka i narzędzia pisania prac naukowych; Analiza przykładów. Etyka pracy badawczej. Praca z publikacjami naukowymi w tym w języku angielskim.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
6	Inteligentne zapory sieciowe	K_W04 Zna zaawansowane mechanizmy i standardy bezpieczeństwa stosowane w systemach rozproszonych, sieciach i systemach Internetu Rzeczy. K_U03 Potrafi wykrywać podatności i ataki, analizować i oceniać ryzyko w systemach teleinformatycznych oraz opracowywać i wdrażać procedury i strategie ochrony, w tym dla sieci bezprzewodowych i IoT, a także oceniać przydatność nowych rozwiązań technicznych i proponować ich ulepszenia.	1.Uruchomienie i wstępna konfiguracja firewalli wiodących dostawców na rynku; 2. Konfiguracja protokołów routingu i podstawowych mechanizmów bezpieczeństwa; 3.Koncepcja firewalla, strefowego. Domyślna polityka tranzytu ruchu firewalla stanowego; 4.Implementacja list kontroli dostępu – selektywne blokowanie / zezwalania na ruch; 5.Granularne podejście do ruchu IP: security levels (ASA), security flow (SRX), session (PA); 6. Zaawansowane polityki filtracji ruchu, polityki graniczne; 7. NAT jako mechanizm ukrywania adresacji; 8. Inspekcja protokołów i kontrola ruchu L7 – porównanie implementacji; 9. Mechanizmy identyfikacji aplikacji zwiększające widoczność w sieci; 10. Systemy detekcji zagrożeń (IDS/IPS); 11. Mechanizmy ochrony przed: skanowaniem, zalewaniem ruchem oraz anomaliami protokołów; 12.Monitoring bezpieczeństwa sieci - analiza logów; 13. Zewnętrzny analizator logów i system zbierania incydentów (syslog/SIEM); 14. Filtracja i kontrola usługi DNS.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
7	Modelowanie i organizacja procesów biznesowych	K_W08 Rozumie znaczenie i konsekwencje pozatechnicznych (społecznych, etycznych i środowiskowych) uwarunkowań działalności zawodowej w zakresie technologii informatycznych i zabezpieczeń cyfrowych. K_K05 Jest gotów do podejmowania inicjatyw przedsiębiorczych oraz działalności innowacyjnej w obszarze technologii informatycznych i bezpieczeństwa cyfrowego.	Celem przedmiotu jest przekazanie studentom wiedzy i umiejętności związanej z dziedziną zarządzania procesami biznesowymi, zarówno modelowaniem jak i organizacją tych procesów. Studenci poznają podstawowe notacje procesów biznesowych z rozwinięciem tematu notacji BPMN. Zostanie im przedstawiona organizacja procesów biznesowych na tle przedsiębiorstwa. Organizacja procesów biznesowych zostanie zilustrowana przy użyciu systemu zarządzania przedsiębiorstwem klasy ERP.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
8	Podstawy Analizy Danych w Cyberbezpieczeństwie	K_W03 Ma pogłębioną wiedzę o faktach, metodach i narzędziach analizy danych w kryptografii i systemach bezpieczeństwa oraz zna główne trendy, kierunki badań i nowe technologie w cyberbezpieczeństwie wraz z ich wpływem na gospodarkę i społeczeństwo, co umożliwia rozwiązywanie złożonych problemów tego obszaru. K_U02 Potrafi wykorzystywać metody analityczne, symulacyjne i eksperymentalne w analizie i ocenie bezpieczeństwa systemów informatycznych oraz do definiowania i rozwiązywania zadań inżynierskich w tym problemów badawczych K_U05 Potrafi oszacować przydatność, aspekt ekonomiczny i posługiwać się zaawansowanymi metodami i narzędziami informatycznymi, analitycznymi i diagnostycznymi w zadaniach inżynierskich i naukowych, dotyczących cyberbezpieczeństwa, łącząc wiedzę z różnych obszarów informatyki i innych dyscyplin.	1.Wprowadzenie do roli i źródeł danych w cyberbezpieczeństwie oraz przegląd współczesnych trendów analitycznych. 2.Podstawy eksploracji danych. 3.Narzędzia i metody analityczne w cyberbezpieczeństwie: Python, środowiska SIEM, IDS/IPS i platformy Threat Intelligence. 4. Analiza ruchu sieciowego z wykorzystaniem danych PCAP, NetFlow i logów systemów detekcji. 5.Analiza logów systemowych, aplikacyjnych i sieciowych oraz korelacja zdarzeń w kontekście wykrywania ataków. 6.Wprowadzenie do metod uczenia maszynowego stosowanych w detekcji zagrożeń i analizie behawioralnej. 7.Analiza danych kryptograficznych oraz ocena konfiguracji i bezpieczeństwa rozwiązań kryptograficznych. 8. Metody i narzędzia analizy incydentów bezpieczeństwa, w tym korelacja wielośródłowa i raportowanie.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.

9	Projektowanie i Realizacja Systemów Cyberbezpieczeństwa	K_W01 Ma pogłębioną i uporządkowaną wiedzę z zakresu informatyki technicznej i telekomunikacji oraz procesów zachodzących w systemach i sieciach teleinformatycznych, istotnych dla zapewniania bezpieczeństwa ich działania. K_U04 Potrafi zaprojektować i zrealizować projekt inżynierski lub badawczy z zakresu cyberbezpieczeństwa, zgodny ze specyfikacją i zapewniający bezpieczeństwo informacji, wykorzystując odpowiednie techniki i narzędzia (potrafi również opracować nowe lub dostosować istniejące), uwzględniając przy tym aspekty etyczne, prawne, organizacyjne, ekonomiczne oraz elementy innowacyjności. K_U12 Potrafi wykonać typowe dla cyberbezpieczeństwa proste systemy, narzędzia lub konfiguracje zabezpieczeń zgodnie z określoną specyfikacją, dobierając właściwe metody, techniki i środowiska, a także poprawnie realizując proces implementacji i testowania. K_K02 Jest gotów do przestrzegania zasad etyki zawodowej, działania na rzecz przestrzegania tych zasad oraz jest świadomy potrzeby i znaczenia rozwoju dorobku zawodowego. K_K03 Jest gotów do pełnienia ról zawodowych i społecznych wymagających odpowiedzialności, przywództwa i współpracy w zespołach interdyscyplinarnych.	Zasady projektowania bezpiecznego oprogramowania. Analiza podatności i błędów programistycznych prowadzących do zagrożeń. Biblioteki z obszaru cyberbezpieczeństwa (C#, Java, Python, PHP). Implementacja mechanizmów uwierzytelniania i autoryzacji. Programowanie systemów monitorowania i detekcji incydentów (IDS/IPS). Tworzenie i integracja modułów kryptograficznych. Systemy kontroli dostępu i analizy zdarzeń. Automatyzacja zadań cyberbezpieczeństwa, w tym w oparciu o sztuczną inteligencję. Architektury systemów odporne na ataki. Wdrażanie procedur bezpieczeństwa w systemach lokalnych i chmurowych. Testowanie bezpieczeństwa aplikacji. Zasady szkolenia administratorów i użytkowników systemów z cyberhigieny i cyberbezpieczeństwa. Zarządzanie administratorami.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
10	Język obcy specjalistyczny	K_U06 Potrafi skutecznie komunikować się na tematy specjalistyczne w środowisku zawodowym i naukowym, w języku polskim i angielskim, właściwie dobierając i stosując techniki informacyjno-komunikacyjne, w tym przygotować opracowanie naukowe lub raport techniczny z zakresu cyberbezpieczeństwa oraz zaprezentować jego wyniki K_U09 posiada praktyczne umiejętności posługiwania się językiem angielskim na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego	Zajęcia obejmują naukę specjalistycznego języka obcego związanego z informatyką, pomagając w zrozumieniu terminologii branżowej oraz rozwijając umiejętności komunikacji pisemnej i ustnej. Studenci uczą się efektywnie korzystać z języka w kontekście zawodowym.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
11	Seminarium dyplomowe	K_W02 Zna metodologiczne podstawy prowadzenia badań naukowych oraz ma wiedzę dotyczącą metodyki prowadzenia prac badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa. K_W06 Zna i rozumie uwarunkowania prawne, ekonomiczne, organizacyjne i etyczne działalności zawodowej i naukowej w obszarze cyberbezpieczeństwa, w tym regulacje dotyczące ochrony danych, własności intelektualnej i odpowiedzialności prawnej. K_W08 Rozumie znaczenie i konsekwencje pozatechnicznych (społecznych, etycznych i środowiskowych) uwarunkowań działalności zawodowej w zakresie technologii informatycznych i zabezpieczeń cyfrowych. K_U01 Potrafi samodzielnie pozyskiwać informacje z różnych źródeł, krytycznie je analizować i twórczo interpretować oraz formułować i testować hipotezy, prowadzić eksperymenty i symulacje oraz prezentować ich wyniki, stosując właściwe metody do rozwiązywania złożonych problemów bezpieczeństwa IT K_U04 Potrafi zaprojektować i zrealizować projekt inżynierski lub badawczy z zakresu cyberbezpieczeństwa, zgodny ze specyfikacją i zapewniający bezpieczeństwo informacji, wykorzystując odpowiednie techniki i narzędzia (potrafi również opracować nowe lub dostosować istniejące), uwzględniając przy tym aspekty etyczne, prawne, organizacyjne, ekonomiczne oraz elementy innowacyjności. K_U06 Potrafi skutecznie komunikować się na tematy specjalistyczne w środowisku zawodowym i naukowym, w języku polskim i angielskim, właściwie dobierając i stosując techniki informacyjno-komunikacyjne, w tym przygotować opracowanie naukowe lub raport techniczny z zakresu cyberbezpieczeństwa oraz zaprezentować jego wyniki K_U08 Potrafi stosować zasady etyki zawodowej, ochrony informacji i odpowiedzialnego wykorzystania technologii informatycznych. K_K01 Rozumie dynamikę zmian, w zakresie wiedzy i umiejętno, ścicharakterystyczną dla cyberbezpieczeństwa, jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści, uznaje znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięganie opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu.	Ogólne wymagania do pracy dyplomowej i podstawowe wytyczne. Technika pisania pracy naukowej. Formułowania tematu pracy. Sposoby poszukiwania literatury i źródeł danych do pracy. Definiowania celu badań, formułowanie problemów badawczych, wniosków. Opracowanie wyników badań i ich analiza. Prezentowanie wyników prac.	I semestr opracowanie 50% pracy. II semestr zatwierdzenie pracy przez promotora.
12	Wojna informacyjna i geopolityka w XXI wieku	K_W09 Posiada świadomość problemów współczesnej cywilizacji wynikających z rozwoju nauk technicznych i inżynieryjnych, zwłaszcza informatyki i telekomunikacji, a także z wykorzystania najnowszych osiągnięć nauki i technologii. Rozumie zagrożenia z tym związane, w tym osobiste i społeczne dylematy wynikające z działań mogących naruszać bezpieczeństwo systemów teleinformatycznych. K_U10 Potrafi analizować, odpowiednio dobierać i stosować a także przystosowywać i opracowywać metody oraz narzędzia działania w celu prognozowania, wyjaśniania i rozwiązywania problemów w obszarze cyberbezpieczeństwa	Geopolityka w XXI wieku -dynamika i uwarunkowania Podstawowe pojęcia: wojna informacyjna, cyberwojna i propaganda, konflikty w infosferze i ich specyfika Główne doktryny i aktorzy w wojnie informacyjnej Rola danych i technologii cyfrowych we współczesnej rywalizacji na arenie międzynarodowej Techniczne i informacyjne środki cyberwojny; Rola algorytmów rekomendacji, bańki informacyjne, polaryzacja i radykalizacja online; Komunikowanie jako źródło budowania odporności na cyberzagrożenia w państwie – case studies	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.

13	Systemy cyberbezpieczeństwa na świecie	K_W09 Posiada świadomość problemów współczesnej cywilizacji wynikających z rozwoju nauk technicznych i inżynieryjnych, zwłaszcza informatyki i telekomunikacji, a także z wykorzystania najnowszych osiągnięć nauki i technologii. Rozumie zagrożenia z tym związane, w tym osobiste i społeczne dylematy wynikające z działań mogących naruszać bezpieczeństwo systemów teleinformatycznych. K_W10 Ma pogłębioną wiedzę o państwowych i międzynarodowych systemach zarządzania cyberbezpieczeństwem oraz o źródłach i konsekwencjach zagrożeń na poziomie krajowym i globalnym, w tym o roli władz i organizacji międzynarodowych oraz możliwościach przeciwdziałania i łagodzenia skutków tych zagrożeń. K_U10 Potrafi analizować, odpowiednio dobierać i stosować a także przystosowywać i opracowywać metody oraz narzędzia działania w celu prognozowania, wyjaśniania i rozwiązywania problemów w obszarze cyberbezpieczeństwa K_U11 Potrafi odpowiednio dobierać źródła i selekcjonować informacje, dokonywać ich krytycznej analizy, syntezy i oceny w celu prognozowania, wyjaśnienia i rozwiązania problemów w obszarze cyberbezpieczeństwa	Globalne fora i organizacje współpracy w cyberbezpieczeństwie (m. in. ONZ, NATO, UE, fora regionalne); Modele narodowych systemów cyberbezpieczeństwa – porównanie struktur instytucjonalnych; Normy i standardy cyberbezpieczeństwa w systemach prawnych wybranych państw na świecie; Infrastruktura krytyczna i jej ochrona na przykładzie wybranych krajów; Programy budowy odporności społecznej na cyberzagrożenia i dezinformację – case studies; Między kontrolą, cenzurą a ofensywą – systemy cyberbezpieczeństwa w państwach autorytarnych; Nordycki model cyberodporności; Cyberbezpieczeństwo a sektor prywatny: Big Tech, małe i średnie przedsiębiorstwa, sektor finansowy- wymagania dotyczące certyfikacji, monitorowanie oraz zapobieganie nieprawodłowościom	Egzamin weryfikujący wiedzę potwierdzającą osiągnięcie założonych efektów uczenia. Forma pisemna 6 pytań opisowych / obliczeniowych, każde po 4 punkty: Zaliczenie od 13 pkt. 13,0 - 15,0 - ocena 3.0 16,0 - 17,0 - ocena 3.5 18,0 - 19,0 - ocena 4.0 20,0 - 21,0 - ocena 4.5 22,0 - 24,0 - ocena 5.0 Na początku ćwiczeń przewidziane są wejściówki. Zaliczenie przedmiotu na podstawie sumy uzyskanych punktów w wejściówek. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry
14	Cyberterroryzm i podstawy systemu zwalczania terroryzmu	K_W06 Zna i rozumie uwarunkowania prawne, ekonomiczne, organizacyjne i etyczne działalności zawodowej i naukowej w obszarze cyberbezpieczeństwa, w tym regulacje dotyczące ochrony danych, własności intelektualnej i odpowiedzialności prawnej. K_W10 Ma pogłębioną wiedzę o państwowych i międzynarodowych systemach zarządzania cyberbezpieczeństwem oraz o źródłach i konsekwencjach zagrożeń na poziomie krajowym i globalnym, w tym o roli władz i organizacji międzynarodowych oraz możliwościach przeciwdziałania i łagodzenia skutków tych zagrożeń. K_U11 Potrafi odpowiednio dobierać źródła i selekcjonować informacje, dokonywać ich krytycznej analizy, syntezy i oceny w celu prognozowania, wyjaśnienia i rozwiązania problemów w obszarze cyberbezpieczeństwa	Terroryzm jako forma przemocy; Geneza cyberterroryzmu; Określenia i istota cyberterroryzmu; Rola i znaczenie cyberterroryzmu w świecie ; Cyberterroryzm polityczny, religijny, gospodarczy, kryminalny, państwowy; Obszary zagrożeń cyberterrorystycznych - cele i obiekty ataków cyberterrorystycznych; Scenariusze ataków w cyberprzestrzeni; Technologiczne, edukacyjne i strategiczne zwalczanie cyberterroryzmu; Przykłady cyberataków i sposobów ich zwalczania	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
15	Innowacyjność i kreatywne myślenie	K_W07 Ma wiedzę o zasadach tworzenia i prowadzenia działalności gospodarczej, w tym startupów technologicznych w obszarze IT i cyberbezpieczeństwa. K_U07 Potrafi pracować indywidualnie i w zespole (także kierując jego pracą), biorąc odpowiedzialność za jej wyniki, oraz samodzielnie określać kierunki rozwoju zawodowego i naukowego, planować i realizować samokształcenie, a także ukierunkowywać w nim innych. K_U08 Potrafi stosować zasady etyki zawodowej, ochrony informacji i odpowiedzialnego wykorzystania technologii informatycznych. K_K05 Jest gotów do podejmowania inicjatyw przedsiębiorczych oraz działalności innowacyjnej w obszarze technologii informatycznych i bezpieczeństwa cyfrowego.	Wprowadzenie do Design Thinking (DT) z uwzględnieniem uwarunkowań i prowadzenia biznesu w IT i cyberbezpieczeństwie, Etapy Procesu Design Thinking, Model pracy twórczej w ramach metodologii DT , Mapa empatii, Mapa Interesariuszy, wywiady indywidualne/warsztat badawczy/ obserwacja uczestnicząca, Projektowe Techniki Badawcze, Wywiady Indywidualne Jakościowe, Burza mózgów, Idea card, Metody prototypowania. Modele Biznesowe, Inspiratory do budowania zespołów. Praca indywidualna i zespołowa w procesie DT z elementami odpowiedzialnego przywództwa i planowania rozwoju kompetencji projektowych. Zasady etyki, ochrony informacji i odpowiedzialnego wykorzystania technologii w tworzeniu innowacyjnych rozwiązań oraz rozwijaniu postaw przedsiębiorczych w obszarze IT i cyberbezpieczeństwa.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
16	Przedmiot obieralny - nauki humanistyczne	K_K02 Jest gotów do przestrzegania zasad etyki zawodowej, działania na rzecz przestrzegania tych zasad oraz jest świadomy potrzeby i znaczenia rozwoju dorobku zawodowego. K_K04 Jest gotów do inicjowania działań na rzecz bezpieczeństwa w cyberprzestrzeni oraz popularyzowania wiedzy o zagrożeniach i dobrych praktykach wśród społeczeństwa.	Przedmiot o charakterze humanistycznym rozwija zdolność zdobywania i analizowania informacji z różnych źródeł. Akcentuje konieczność formułowania i argumentowania opinii na podstawie wiedzy z dziedziny nauk humanistycznych. Zajęcia te zwiększają świadomość etycznych aspektów, odpowiedzialności za dziedzictwo kulturowe oraz szacunku dla różnorodności kulturowej.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.

17	Rozwój kompetencji społecznych	K_U08 Potrafi stosować zasady etyki zawodowej, ochrony informacji i odpowiedzialnego wykorzystania technologii informatycznych. K_K02 Jest gotów do przestrzegania zasad etyki zawodowej, działania na rzecz przestrzegania tych zasad oraz jest świadomy potrzeby i znaczenia rozwoju dorobku zawodowego. K_K03 Jest gotów do pełnienia ról zawodowych i społecznych wymagających odpowiedzialności, przywództwa i współpracy w zespołach interdyscyplinarnych. K_K04 Jest gotów do inicjowania działań na rzecz bezpieczeństwa w cyberprzestrzeni oraz popularyzowania wiedzy o zagrożeniach i dobrych praktykach wśród społeczeństwa.	Naukowe sekrety motywacji, Dialog motywujący - wyznaczanie celów strategicznych, Inteligencja emocjonalna, inteligencja społeczna - wybrane zagadnienia Koszty analfabetyzmu emocjonalnego. Autentyczność, czytelność, empatia – inteligencja społeczna w środowisku pracy Społeczna odpowiedzialność biznesu Etyka wobec zmian technologicznych Trening umiejętności społecznych Efektywny trening antystresowy Ocena i rozwój inteligencji społecznej Skuteczne przywództwo Wystąpienia publiczne. Rozwijanie umiejętności skutecznej komunikacji, empatii i współpracy w zespole, wspierających odpowiedzialne działanie, rozwiązywanie konfliktów oraz budowanie pozytywnych relacji w środowisku zawodowym.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
18	Język obcy	K_U09 posiada praktyczne umiejętności posługiwania się językiem angielskim na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego	Przedmiot język obcy skupia się na umiejętnościach komunikacyjnych potrzebnych w branż nowoczesnych technologii. Kurs umożliwia przygotowanie i prezentację wyników np. zadania inżynierskiego, a także rozwija zdolność czytania i rozumienia tekstów np. dokumentacji technicznej i naukowej.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
19	Automatyzacja procesów sieciowych	K_W01 Ma pogłębioną i uporządkowaną wiedzę z zakresu informatyki technicznej i telekomunikacji oraz procesów zachodzących w systemach i sieciach teleinformatycznych, istotnych dla zapewniania bezpieczeństwa ich działania. K_U04 Potrafi zaprojektować i zrealizować projekt inżynierski lub badawczy z zakresu cyberbezpieczeństwa, zgodny ze specyfikacją i zapewniający bezpieczeństwo informacji, wykorzystując odpowiednie techniki i narzędzia (potrafi również opracować nowe lub dostosować istniejące), uwzględniając przy tym aspekty etyczne, prawne, organizacyjne, ekonomiczne oraz elementy innowacyjności. K_U05 Potrafi oszacować przydatność, aspekt ekonomiczny i posługiwać się zaawansowanymi metodami i narzędziami informatycznymi, analitycznymi i diagnostycznymi w zadaniach inżynierskich i naukowych, dotyczących cyberbezpieczeństwa, łącząc wiedzę z różnych obszarów informatyki i innych dyscyplin. K_U12 Potrafi wykonać typowe dla cyberbezpieczeństwa proste systemy, narzędzia lub konfiguracje zabezpieczeń zgodnie z określoną specyfikacją, dobierając właściwe metody, techniki i środowiska, a także poprawnie realizując proces implementacji i testowania. K_K01 Rozumie dynamikę zmian, w zakresie wiedzy i umiejętności charakterystyczną dla cyberbezpieczeństwa, jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści, uznaje znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięganie opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu.	Architektura współczesnych sieci komputerowych oraz systemów zabezpieczeń sieciowych. Automatyzacja zarządzania infrastrukturą sieciową w środowiskach korporacyjnych. Koncepcje NetDevOps i DevSecOps w administracji siecią i bezpieczeństwem. Konteneryzacja jako środowisko uruchamiania narzędzi do automatyzacji i testów sieciowych. Interfejsy programistyczne API w urządzeniach sieciowych i zaporach sieciowych nowej generacji. Formaty danych JSON i XML w komunikacji z urządzeniami sieciowymi. Modele danych YANG oraz ich zastosowanie w konfiguracji i monitorowaniu sieci. Mechanizmy REST, RESTCONF i NETCONF w automatycznym zarządzaniu urządzeniami sieciowymi. Pobieranie konfiguracji urządzeń sieciowych oraz ich archiwizacja. Analiza zmian konfiguracji i kontrola spójności ustawień sieciowych. Ruch syntetyczny jako narzędzie testowania połączeń i polityk bezpieczeństwa. Generowanie ruchu syntetycznego w środowiskach testowych. Testowanie reguł zapór sieciowych oraz dostępności usług sieciowych. Skrypty programistyczne do automatyzacji zadań sieciowych. Integracja narzędzi testowych z kontenerami Docker. Monitorowanie stanu urządzeń sieciowych z wykorzystaniem interfejsów API. Automatyczne raportowanie wyników testów i kontroli konfiguracji sieciowych.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
20	Zaawansowana analiza danych	K_W03 Ma pogłębioną wiedzę o faktach, metodach i narzędziach analizy danych w kryptografii i systemach bezpieczeństwa oraz zna główne trendy, kierunki badań i nowe technologie w cyberbezpieczeństwie wraz z ich wpływem na gospodarkę i społeczeństwo, co umożliwia rozwiązywanie złożonych problemów tego obszaru. K_U01 Potrafi samodzielnie pozyskiwać informacje z różnych źródeł, krytycznie je analizować i twórczo interpretować oraz formułować i testować hipotezy, prowadzić eksperymenty i symulacje oraz prezentować ich wyniki, stosując właściwe metody do rozwiązywania złożonych problemów bezpieczeństwa IT K_U02 Potrafi wykorzystywać metody analityczne, symulacyjne i eksperymentalne w analizie i ocenie bezpieczeństwa systemów informatycznych oraz do definiowania i rozwiązywania zadań inżynierskich w tym problemów badawczych	1. Zaawansowane metody przetwarzania, integrowania i analizy danych złożonych oraz heterogenicznych w cyberbezpieczeństwie. 2. Techniki modelowania statystycznego, probabilistycznego i predykcyjnego do badania złożonych zjawisk oraz oceny ryzyka. 3. Projektowanie, trenowanie i ocena zaawansowanych modeli uczenia maszynowego i głębokiego stosowanych do detekcji zagrożeń i analizy behawioralnej. 4. Analiza wielowymiarowa i redukcja wymiarowości w celu identyfikacji nieoczywistych wzorców, anomalii i kampanii ataków. 5. Wykorzystanie symulacji, eksperymentów oraz metod danych do testowania hipotez, walidacji rozwiązań i modelowania odporności systemów. 6. Zaawansowana korelacja międzydomenowa obejmująca logi, ruch sieciowy, dane kryptograficzne, artefakty forensyczne i Threat Intelligence.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.

21	Ukrywanie i ochrona informacji w sieciach i systemach	K_W04 Zna zaawansowane mechanizmy i standardy bezpieczeństwa stosowane w systemach rozproszonych, sieciach i systemach Internetu Rzeczy. K_W08 Rozumie znaczenie i konsekwencje pozatechnicznych (społecznych, etycznych i środowiskowych) uwarunkowań działalności zawodowej w zakresie technologii informatycznych i zabezpieczeń cyfrowych. K_U05 Potrafi oszacować przydatność, aspekt ekonomiczny i posługiwać się zaawansowanymi metodami i narzędziami informatycznymi, analitycznymi i diagnostycznymi w zadaniach inżynierskich i naukowych, dotyczących cyberbezpieczeństwa, łącząc wiedzę z różnych obszarów informatyki i innych dyscyplin. K_K02 Jest gotów do przestrzegania zasad etyki zawodowej, działania na rzecz przestrzegania tych zasad oraz jest świadomy potrzeby i znaczenia rozwoju dorobku zawodowego.	Treści kształcenia obejmują zastosowanie zaawansowanych metod i narzędzi do analizy zagrożeń, ochrony informacji, anonimizacji, wykrywania steganografii oraz zabezpieczania danych w systemach rozproszonych i chmurowych, z uwzględnieniem etycznych standardów pracy i potrzeby ciągłego rozwoju zawodowego w obszarze cyberbezpieczeństwa. Wymagania ochrony infoprmacji. Modele zagrożeń. Techniki anonimizacji i ochrony prywatności. Zabezpieczenie danych i usług przed podsłuchem i manipulacją. Steganografia i ukrywanie danych w różnych formatach i na różnych nośnikach. Metody detekcji i analizy steganografii. Ochrona informacji w systemach rozproszonych i chmurowych. Monitorowania i analiza incydentów ochrony poufności. Aktualne trendy i wyzwania (bieżące case studies).	Egzamin w wykładu, zaliczenie gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Zaliczenie laboratorium: dwa kolokwia w środowisku symulacyjnym Packet Tracer. Wymagane jest zaliczenie obu, ocena zgodnie z punktami, jak wyżej.
22	Środowiska wirtualne	K_W05 Zna i rozumie, w pogłębionym stopniu, cykl życia systemów informatycznych z uwzględnieniem procesów projektowania, wdrażania, testowania, utrzymania i zapewnienie cyberbezpieczeństwa. K_U02 Potrafi wykorzystywać metody analityczne, symulacyjne i eksperymentalne w analizie i ocenie bezpieczeństwa systemów informatycznych oraz do definiowania i rozwiązywania zadań inżynierskich w tym problemów badawczych K_U05 Potrafi oszacować przydatność, aspekt ekonomiczny i posługiwać się zaawansowanymi metodami i narzędziami informatycznymi, analitycznymi i diagnostycznymi w zadaniach inżynierskich i naukowych, dotyczących cyberbezpieczeństwa, łącząc wiedzę z różnych obszarów informatyki i innych dyscyplin. K_U07 Potrafi pracować indywidualnie i w zespole (także kierując jego pracą), biorąc odpowiedzialność za jej wyniki, oraz samodzielnie określać kierunki rozwoju zawodowego i naukowego, planować i realizować samokształcenie, a także ukierunkowywać w nim innych.	Treści obejmują architektury i techniki wirtualizacji, konteneryzację i orkiestrację (Docker, Kubernetes), sieci SDN, infrastrukturę oraz wdrożenia w chmurach publicznych, rozwijając umiejętność analizy, projektowania i bezpiecznego utrzymania systemów informatycznych z wykorzystaniem zaawansowanych narzędzi oraz pracy indywidualnej i zespołowej. W szczeg.: 1. Podstawy i architektury wirtualizacji. odstawy i architektury wirtualizacji.; 2.Typy wirtualizacji (pełna, parawirtualizacja, wirtualizacja sprzętowa); 3.Wirtualizacja zasobów: CPU, pamięci operacyjnej / masowej; 4.Konteneryzacja - Idea kontenerów i porównanie z VM; 5.Docker – architektura, obrazy, sieci, wolumeny; 6.Docker – automatyzacja środowiska, skalowalność infrastruktury. Kubernetes: pody, deployments, serwisy, ingress, skalowanie, Helm i zarządzanie aplikacjami. 7.Wprowadzenie do sieci definiowanych programowo - SDN (Software Defined Networking); 8.Terraform: tworzenie i zarządzanie infrastrukturą; 9.Wirtualizacja w chmurach publicznych; 10.Wdrożenia w Amazon EC2, Google Compute Engine, Azure VM.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
23	Informatyka śledcza	K_W04 Zna zaawansowane mechanizmy i standardy bezpieczeństwa stosowane w systemach rozproszonych, sieciach i systemach Internetu Rzeczy. K_W06 Zna i rozumie uwarunkowania prawne, ekonomiczne, organizacyjne i etyczne działalności zawodowej i naukowej w obszarze cyberbezpieczeństwa, w tym regulacje dotyczące ochrony danych, własności intelektualnej i odpowiedzialności prawnej. K_U02 Potrafi wykorzystywać metody analityczne, symulacyjne i eksperymentalne w analizie i ocenie bezpieczeństwa systemów informatycznych oraz do definiowania i rozwiązywania zadań inżynierskich w tym problemów badawczych K_U03 Potrafi wykrywać podatności i ataki, analizować i oceniać ryzyko w systemach teleinformatycznych oraz opracowywać i wdrażać procedury i strategie ochrony, w tym dla sieci bezprzewodowych i IoT, a także oceniać przydatność nowych rozwiązań technicznych i proponować ich ulepszenia.	Treści kształcenia obejmują podstawy informatyki śledczej, analizę artefaktów w systemach rozproszonych i IoT, identyfikację zdarzeń naruszających bezpieczeństwo z wykorzystaniem metod analitycznych i symulacyjnych oraz omówienie prawnych, organizacyjnych i etycznych uwarunkowań prowadzenia analiz, rozwijając umiejętność oceny ryzyka, wykrywania podatności i formułowania procedur ochronnych. W szczeg.: 1. Podstawy informatyki śledczej, w tym proces zabezpieczania, pozyskiwania, analizy i raportowania dowodów cyfrowych zgodnie z obowiązującymi standardami i zasadami integralności danych. 2. Analiza artefaktów systemowych i sieciowych w systemach rozproszonych oraz środowiskach IoT, z uwzględnieniem specyfiki ich architektury i mechanizmów bezpieczeństwa. 3. Metody identyfikacji zdarzeń naruszających bezpieczeństwo, w tym analiza logów, rekonstrukcja incydentów oraz ocena podatności bez wykonywania technik ofensywnych. 4. Wykorzystanie metod analitycznych, eksperymentalnych i symulacyjnych do oceny ryzyka, badania zachowania systemów oraz walidacji scenariuszy incydentów. 5. Uwarunkowania prawne, organizacyjne i etyczne prowadzenia analiz śledczych, obejmujące ochronę danych, prywatność, własność intelektualna oraz zasady odpowiedzialności prawnej.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
24	Uczenie maszynowe w identyfikacji zagrożeń	K_W02 Zna metodologiczne podstawy prowadzenia badań naukowych oraz ma wiedzę dotyczącą metodyki prowadzenia prac badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa. K_W03 Ma pogłębioną wiedzę o faktach, metodach i narzędziach analizy danych w kryptografii i systemach bezpieczeństwa oraz zna główne trendy, kierunki badań i nowe technologie w cyberbezpieczeństwie wraz z ich wpływem na gospodarkę i społeczeństwo, co umożliwia rozwiązywanie złożonych problemów tego obszaru. K_U02 Potrafi wykorzystywać metody analityczne, symulacyjne i eksperymentalne w analizie i ocenie bezpieczeństwa systemów informatycznych oraz do definiowania i rozwiązywania zadań inżynierskich w tym problemów badawczych K_U03 Potrafi wykrywać podatności i ataki, analizować i oceniać ryzyko w systemach teleinformatycznych oraz opracowywać i wdrażać procedury i strategie ochrony, w tym dla sieci bezprzewodowych i IoT, a także oceniać przydatność nowych rozwiązań technicznych i proponować ich ulepszenia.	Podstawy zastosowań uczenia maszynowego w identyfikacji zagrożeń. Techniki przygotowania danych i inzynierii cech dla danych sieciowych i systemowych. Wykrywanie anomalii (metody nadzorowane i nienadzorowane). Klasyfikacja anomalii, w tym ataków. Modele sekwencyjne do analizy logów i zdarzeń. Systemy wykrywania intruzów oparte na uczelniu maszynowym. Analiza statyczna i dynamiczna w wykrywaniu szkodliwego oprogramowania. Ocena skuteczności modeli i metryk cyberbezpieczeństwa. Odporność modeli uczenia maszynowego na ataki typu adversarial. Implementacja i modernizacja (wzmacnianie odporności) modeli uczenia maszynowego w cyberbezpieczeństwie	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.

25	E-governence przywództwo cyfrowe	K_W09 Posiada świadomość problemów współczesnej cywilizacji wynikających z rozwoju nauk technicznych i inżynieryjnych, zwłaszcza informatyki i telekomunikacji, a także z wykorzystania najnowszych osiągnięć nauki i technologii. Rozumie zagrożenia z tym związane, w tym osobiste i społeczne dylematy wynikające z działań mogących naruszać bezpieczeństwo systemów teleinformatycznych. K_U10 Potrafi analizować, odpowiednio dobierać i stosować a także przystosowywać i opracowywać metody oraz narzędzia działania w celu prognozowania, wyjaśniania i rozwiązywania problemów w obszarze cyberbezpieczeństwa K_U11 Potrafi odpowiednio dobierać źródła i selekcjonować informacje, dokonywać ich krytycznej analizy, syntezy i oceny w celu prognozowania, wyjaśnienia i rozwiązania problemów w obszarze cyberbezpieczeństwa K_K03 Jest gotów do pełnienia ról zawodowych i społecznych wymagających odpowiedzialności, przywództwa i współpracy w zespołach interdyscyplinarnych.	Modele e-governance w Polsce i na świecie; Przywództwo cyfrowe w administracji publicznej: kompetencje i style zarządzania; Transformacja cyfrowa państwa: strategie, roadmapy i governance projektów IT; E-usługi publiczne: typy i wyzwania oraz bariery związane z wdrażaniem; dane cyfrowe w administracji (open data, big data) a podejmowanie decyzji publicznych; Marginalizacja i wykluczenie cyfrowe: rola liderów publicznych w wyrównywaniu szans; Zaufanie obywateli do cyfrowych usług państwa; Etyka, odpowiedzialność a przywództwo cyfrowe	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
26	E-partycypacja i usługi w administracji	K_W10 Ma pogłębioną wiedzę o państwowych i międzynarodowych systemach zarządzania cyberbezpieczeństwem oraz o źródłach i konsekwencjach zagrożeń na poziomie krajowym i globalnym, w tym o roli władz i organizacji międzynarodowych oraz możliwościach przeciwdziałania i łagodzenia skutków tych zagrożeń. K_U10 Potrafi analizować, odpowiednio dobierać i stosować a także przystosowywać i opracowywać metody oraz narzędzia działania w celu prognozowania, wyjaśniania i rozwiązywania problemów w obszarze cyberbezpieczeństwa K_U11 Potrafi odpowiednio dobierać źródła i selekcjonować informacje, dokonywać ich krytycznej analizy, syntezy i oceny w celu prognozowania, wyjaśnienia i rozwiązania problemów w obszarze cyberbezpieczeństwa K_K04 Jest gotów do inicjowania działań na rzecz bezpieczeństwa w cyberprzestrzeni oraz popularyzowania wiedzy o zagrożeniach i dobrych praktykach wśród społeczeństwa.	Ewolucja demokracji: demokracja klasyczna, demokracja przedstawicielska, kryzys de-mokracji, e-demokracja; Pojęcie demokracji uczestniczącej i elektronicznej; Partycypacja obywatelska i elektroniczna partycypacja obywatelska – definicja i typologie; Nowe ruchy społeczne – rola narzędzi sieciowych w podejmowaniu aktywności obywatelskiej; Formy, narzędzia i modele e-partycypacji – konsultacje online, współdecydowanie, petycje elektroniczne, budżety obywatelskie; E-partycypacja w perspektywie porównawczej – analiza wybranych raportów E-partycypacja na szczeblu lokalnym (budżet partycypacyjny w Polsce i na świecie, partycypacja miejska w sieci). E-partycypacja na szczeblu krajowym i międzynarodowym. Projektowanie cyfrowych usług publicznych z udziałem obywateli; Standardy, jakość i etyka e-usług w administracji (m. in. dostępność, użyteczność, „podróż użytkownika” obywatela); Bariery i wykluczenie w e-partycypacji – kompetencje cyfrowe, zaufanie, dostęp do Internetu, język administracji; E-partycypacja w planowaniu przestrzennym i politykach lokalnych (interaktywne narzędzia planowania, e-mapy etc.); Bezpieczeństwo i ochrona danych w e-partycypacji oraz e-usługach administracji	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
27	Technologie Internetu rzeczy	K_W01 Ma pogłębioną i uporządkowaną wiedzę z zakresu informatyki technicznej i telekomunikacji oraz procesów zachodzących w systemach i sieciach teleinformatycznych, istotnych dla zapewniania bezpieczeństwa ich działania. K_U04 Potrafi zaprojektować i zrealizować projekt inżynierski lub badawczy z zakresu cyberbezpieczeństwa, zgodny ze specyfikacją i zapewniający bezpieczeństwo informacji, wykorzystując odpowiednie techniki i narzędzia (potrafi również opracować nowe lub dostosować istniejące), uwzględniając przy tym aspekty etyczne, prawne, organizacyjne, ekonomiczne oraz elementy innowacyjności. K_U12 Potrafi wykonać typowe dla cyberbezpieczeństwa proste systemy, narzędzia lub konfiguracje zabezpieczeń zgodnie z określoną specyfikacją, dobierając właściwe metody, techniki i środowiska, a także poprawnie realizując proces implementacji i testowania.	Treści obejmują architekturę systemów IoT, modele komunikacji i protokoły transmisji danych w sieciach urządzeń inteligentnych, a także zasady projektowania i integracji komponentów sprzętowych oraz programowych, ukierunkowane na zapewnienie bezpieczeństwa działania systemów teleinformatycznych. Treści kształcenia obejmują również projektowanie i realizację złożonych projektów IoT z uwzględnieniem mechanizmów ochrony informacji, analizy ryzyka, doboru odpowiednich narzędzi i technik inżynierskich oraz adaptacji istniejących rozwiązań do specyficznych wymagań bezpieczeństwa, przy równoczesnym uwzględnieniu aspektów etycznych, prawnych, organizacyjnych, ekonomicznych oraz innowacyjności.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
28	Pentesty	K_W04 Zna zaawansowane mechanizmy i standardy bezpieczeństwa stosowane w systemach rozproszonych, sieciach i systemach Internetu Rzeczy. K_W06 Zna i rozumie uwarunkowania prawne, ekonomiczne, organizacyjne i etyczne działalności zawodowej i naukowej w obszarze cyberbezpieczeństwa, w tym regulacje dotyczące ochrony danych, własności intelektualnej i odpowiedzialności prawnej. K_U03 Potrafi wykrywać podatności i ataki, analizować i oceniać ryzyko w systemach teleinformatycznych oraz opracowywać i wdrażać procedury i strategie ochrony, w tym dla sieci bezprzewodowych i IoT, a także oceniać przydatność nowych rozwiązań technicznych i proponować ich ulepszenia. K_K01 Rozumie dynamikę zmian, w zakresie wiedzy i umiejętno, ścicharakterystyczną dla cyberbezpieczeństwa, jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści, uznaje znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięganie opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu.	Modele oceny bezpieczeństwa. Metodologia testów penetracyjnych. Zalecenia etyczne, prawne i dobre praktyki przy testach penetracyjnych. Informacja o celu. Rekonesans pasywny i aktywny. Testy socjotechniczne. Identyfikacja podatności w sieciach, systemach i usługach. Ocena konfiguracji sieci, systemów i usług. Testowanie bezpieczeństwa. Analiza zabezpieczeń środowisk Internetu Rzeczy, chmurowych i konteneryzacji. Raportowanie. Priorytetowanie zagrożeń. Zalecenia naprawcze.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.

29	Cyberbezpieczeństwo w przemyśle (IIoT)	K_W08 Rozumie znaczenie i konsekwencje pozatechnicznych (społecznych, etycznych i środowiskowych) uwarunkowań działalności zawodowej w zakresie technologii informatycznych i zabezpieczeń cyfrowych. K_U04 Potrafi zaprojektować i zrealizować projekt inżynierski lub badawczy z zakresu cyberbezpieczeństwa, zgodny ze specyfikacją i zapewniający bezpieczeństwo informacji, wykorzystując odpowiednie techniki i narzędzia (potrafi również opracować nowe lub dostosować istniejące), uwzględniając przy tym aspekty etyczne, prawne, organizacyjne, ekonomiczne oraz elementy innowacyjności. K_U05 Potrafi oszacować przydatność, aspekt ekonomiczny i posługiwać się zaawansowanymi metodami i narzędziami informatycznymi, analitycznymi i diagnostycznymi w zadaniach inżynierskich i naukowych, dotyczących cyberbezpieczeństwa, łącząc wiedzę z różnych obszarów informatyki i innych dyscyplin. K_K02 Jest gotów do przestrzegania zasad etyki zawodowej, działania na rzecz przestrzegania tych zasad oraz jest świadomy potrzeby i znaczenia rozwoju dorobku zawodowego.	Architektura systemów przemysłowych oraz przemysłowego Internetu Rzeczy (IIoT). Integracja systemów OT i IT w środowiskach przemysłowych. Modele komunikacji i przetwarzania danych w systemach automatyki przemysłowej. Architektura zdarzeniowa w systemach IIoT i jej wpływ na bezpieczeństwo procesów przemysłowych. Zagrożenia cybernetyczne w sieciach przemysłowych i systemach sterowania. Bezpieczeństwo komunikacji w protokołach przemysłowych i systemach telemetrycznych. Segmentacja i izolacja sieci przemysłowych. Zapory sieciowe i systemy bezpieczeństwa dedykowane środowiskom przemysłowym. Monitorowanie i detekcja zdarzeń bezpieczeństwa w systemach IIoT. Analiza ruchu sieciowego oraz zdarzeń w środowiskach przemysłowych. Automatyzacja reakcji na incydenty w systemach przemysłowych. Zarządzanie cyklem życia urządzeń IIoT z perspektywy bezpieczeństwa. Regułowe i politykowe podejście do ochrony systemów przemysłowych. Integracja systemów monitorowania, detekcji i raportowania zdarzeń bezpieczeństwa. Odporność systemów przemysłowych na awarie oraz zakłócenia cybernetyczne. Zasady projektowania bezpiecznych systemów IIoT.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
30	Automatyzacja w IoT	K_W03 Ma pogłębioną wiedzę o faktach, metodach i narzędziach analizy danych w kryptografii i systemach bezpieczeństwa oraz zna główne trendy, kierunki badań i nowe technologie w cyberbezpieczeństwie wraz z ich wpływem na gospodarkę i społeczeństwo, co umożliwia rozwiązywanie złożonych problemów tego obszaru. K_U02 Potrafi wykorzystywać metody analityczne, symulacyjne i eksperymentalne w analizie i ocenie bezpieczeństwa systemów informatycznych oraz do definiowania i rozwiązywania zadań inżynierskich w tym problemów badawczych K_U05 Potrafi oszacować przydatność, aspekt ekonomiczny i posługiwać się zaawansowanymi metodami i narzędziami informatycznymi, analitycznymi i diagnostycznymi w zadaniach inżynierskich i naukowych, dotyczących cyberbezpieczeństwa, łącząc wiedzę z różnych obszarów informatyki i innych dyscyplin.	Architektura systemów Internetu Rzeczy z uwzględnieniem warstwy urządzeń, sieci i aplikacji. Architektura zdarzeniowa w systemach IoT jako podstawa automatyzacji przetwarzania danych. Przetwarzanie strumieni danych IoT w modelu potoków danych od urządzenia do aplikacji. Automatyzacja reakcji systemów IoT na zdarzenia generowane przez urządzenia końcowe. Sieci LoRaWAN oraz komunikacja urządzeń niskoemisyjnych z infrastrukturą sieciową. Automatyzacja cyklu życia urządzeń IoT: rejestracja, aktywacja, monitorowanie i dezaktywacja. Formaty przesyłania danych pomiarowych oraz automatyczne dekodowanie i walidacja danych IoT. Integracja urządzeń IoT z platformami sieciowymi i aplikacyjnymi. Interfejsy programistyczne API w systemach i platformach IoT. Regułowe przetwarzanie danych IoT oraz automatyzacja decyzji na podstawie polityk i zdarzeń. Konteneryzacja jako środowisko realizacji i wdrażania potoków przetwarzania danych IoT. Automatyzacja testów komunikacji i poprawności działania urządzeń oraz systemów IoT. Monitorowanie stanu urządzeń IoT oraz jakości transmisji danych. Wersjonowanie i automatyzacja konfiguracji systemów IoT w podejściu infrastruktury i aplikacji jako kodu.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
31	Programowanie systemów mobilnych	K_W04 Zna zaawansowane mechanizmy i standardy bezpieczeństwa stosowane w systemach rozproszonych, sieciach i systemach Internetu Rzeczy. K_W05 Zna i rozumie, w pogłębionym stopniu, cykl życia systemów informatycznych z uwzględnieniem procesów projektowania, wdrażania, testowania, utrzymania i zapewnienie cyberbezpieczeństwa. K_U01 Potrafi samodzielnie pozyskiwać informacje z różnych źródeł, krytycznie je analizować i twórczo interpretować oraz formułować i testować hipotezy, prowadzić eksperymenty i symulacje oraz prezentować ich wyniki, stosując właściwe metody do rozwiązywania złożonych problemów bezpieczeństwa IT K_U07 Potrafi pracować indywidualnie i w zespole (także kierując jego pracą), biorąc odpowiedzialność za jej wyniki, oraz samodzielnie określać kierunki rozwoju zawodowego i naukowego, planować i realizować samokształcenie, a także ukierunkowywać w nim innych.	Treści obejmują architekturę nowoczesnych systemów mobilnych, modele komunikacji z usługami sieciowymi i systemami rozproszonymi oraz standardy bezpieczeństwa stosowane w aplikacjach mobilnych, w tym mechanizmy szyfrowania, autoryzacji, ochrony danych i integracji z usługami IoT. Omawiany jest pełny cykl życia aplikacji mobilnych — od projektowania interfejsów i logiki biznesowej, poprzez implementację, testowanie funkcjonalne i bezpieczeństwa, aż po wdrażanie, utrzymanie i monitorowanie zagrożeń. Studenci realizują zadania projektowe obejmujące analizę problemów, samodzielne wyszukiwanie i krytyczną ocenę informacji, projektowanie i eksperymentowanie z rozwiązaniami programistycznymi oraz prezentowanie wyników badań i symulacji. Zajęcia rozwijają kompetencje pracy indywidualnej i zespołowej, w tym prowadzenia zespołu projektowego, odpowiedzialnego podejmowania decyzji oraz planowania i realizacji samokształcenia w dynamicznie zmieniającym się obszarze technologii mobilnych i cyberbezpieczeństwa.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.

32	Sztucznointeligentne narzędzia cyberoborony	K_W02 Zna metodologiczne podstawy prowadzenia badań naukowych oraz ma wiedzę dotyczącą metodyki prowadzenia prac badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa. K_W03 Ma pogłębioną wiedzę o faktach, metodach i narzędziach analizy danych w kryptografii i systemach bezpieczeństwa oraz zna główne trendy, kierunki badań i nowe technologie w cyberbezpieczeństwie wraz z ich wpływem na gospodarkę i społeczeństwo, co umożliwia rozwiązywanie złożonych problemów tego obszaru. K_U01 Potrafi samodzielnie pozyskiwać informacje z różnych źródeł, krytycznie je analizować i twórczo interpretować oraz formułować i testować hipotezy, prowadzić eksperymenty i symulacje oraz prezentować ich wyniki, stosując właściwe metody do rozwiązywania złożonych problemów bezpieczeństwa IT K_U02 Potrafi wykorzystywać metody analityczne, symulacyjne i eksperymentalne w analizie i ocenie bezpieczeństwa systemów informatycznych oraz do definiowania i rozwiązywania zadań inżynierskich w tym problemów badawczych	Przedmiot wprowadza w zagadnienia wykorzystania sztucznej inteligencji w cyberobronie, obejmując metodologiczne podstawy badań, analizę i interpretację danych bezpieczeństwa oraz projektowanie i ocenę eksperymentów. Studenci uczą się samodzielnie pozyskiwać i krytycznie analizować informacje, stosować metody analityczne, symulacyjne i eksperymentalne oraz interpretować wyniki badań nad inteligentnymi systemami zabezpieczeń. 1. Zastosowania sztucznej inteligencji i uczenia maszynowego w systemach cyberobrony. 2. Metody analizy danych wykorzystywane do wykrywania zagrożeń i anomalii w środowiskach bezpieczeństwa. 3. Architektury i funkcje inteligentnych systemów obronnych. 4. Metodologia badań naukowych i eksperymentów nad AI w cyberbezpieczeństwie. 5. Zastosowanie analiz, symulacji i eksperymentów do oceny skuteczności narzędzi cyberobrony.	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
33	Bezpieczeństwo dzieci, młodzieży i seniorów online	K_W09 Posiada świadomość problemów współczesnej cywilizacji wynikających z rozwoju nauk technicznych i inżynieryjnych, zwłaszcza informatyki i telekomunikacji, a także z wykorzystania najnowszych osiągnięć nauki i technologii. Rozumie zagrożenia z tym związane, w tym osobiste i społeczne dylematy wynikające z działań mogących naruszać bezpieczeństwo systemów teleinformatycznych. K_U10 Potrafi analizować, odpowiednio dobierać i stosować a także przystosowywać i opracowywać metody oraz narzędzia działania w celu prognozowania, wyjaśniania i rozwiązywania problemów w obszarze cyberbezpieczeństwa K_U11 Potrafi odpowiednio dobierać źródła i selekcjonować informacje, dokonywać ich krytycznej analizy, syntezy i oceny w celu prognozowania, wyjaśnienia i rozwiązania problemów w obszarze cyberbezpieczeństwa K_K03 Jest gotów do pełnienia ról zawodowych i społecznych wymagających odpowiedzialności, przywództwa i współpracy w zespołach interdyscyplinarnych.	Dzieci i seniorzy jako szczególne grupy narażone na cyberzagrożenia oraz typy tych zagrożeń; Rola edukacji cyfrowej w budowaniu bezpieczeństwa najmłodszych i starszych użytkowników internetu; Rola rodziny, szkoły i pozostałych instytucji w monitorowaniu i wspieraniu bezpiecznych nawyków cyfrowych – kampanie, szkolenia, wsparcia wspólnoty. Uzależnienia cyfrowe i ich społeczne konsekwencje wśród dzieci, młodzieży i seniorów; Oszustwa internetowe i sposoby ich rozpoznawania, cyberprzemoc i wsparcie ofiar, rozrywka online jako źródło zagrożeń,	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
34	Odporność cyfrowa samorządów i społeczności lokalnych	K_W10 Ma pogłębioną wiedzę o państwowych i międzynarodowych systemach zarządzania cyberbezpieczeństwem oraz o źródłach i konsekwencjach zagrożeń na poziomie krajowym i globalnym, w tym o roli władz i organizacji międzynarodowych oraz możliwościach przeciwdziałania i łagodzenia skutków tych zagrożeń. K_U10 Potrafi analizować, odpowiednio dobierać i stosować a także przystosowywać i opracowywać metody oraz narzędzia działania w celu prognozowania, wyjaśniania i rozwiązywania problemów w obszarze cyberbezpieczeństwa K_U11 Potrafi odpowiednio dobierać źródła i selekcjonować informacje, dokonywać ich krytycznej analizy, syntezy i oceny w celu prognozowania, wyjaśnienia i rozwiązania problemów w obszarze cyberbezpieczeństwa K_K04 Jest gotów do inicjowania działań na rzecz bezpieczeństwa w cyberprzestrzeni oraz popularyzowania wiedzy o zagrożeniach i dobrych praktykach wśród społeczeństwa.	Rewolucja cyfrowa – wyzwania i szanse dla samorządów; Cyberbezpieczeństwo jednostek samorządu terytorialnego – uwarunkowania prawno-normatywne; Lokalne centra cyberbezpieczeństwa; Infrastruktura krytyczna i jej ochrona na poziomie lokalnym przed cyberatakami; ISAC (ang. Information Sharing and Analysis Centre) – JST – jako forum budowania cyberodporności samorządów; Wdrażanie polityk bezpieczeństwa informacji i zarządzanie ryzykiem w samorządach; Tworzenie i testowanie planów reagowania na incydenty cybernetyczne w JST; Omówienie wybranych technologii zabezpieczających; Edukacja na rzecz kształtowania kompetencji cyfrowych wśród mieszkańców i pracowników administracji	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów. Egzamin/kolokwium jest zaliczone, gdy student uzyska min 51% punktów. Skala ocen: do 50% - niedostateczna 51-69% - dostateczna 70-79% - dostateczny plus 80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.

* Wypełnia DJiOK

……
data i podpis
Zastępca ds. Kształcenia

……
data i podpis
Dyrektora Kolegium