Załącznik 2.11

Nazwa Wydziału prowadzącego kierunek studiów: ***Wydział Informatyki***
Nazwa kierunku studiów: ***cyberbezpieczeństwo***
Dyscyplina wiodąca: ***informatyka techniczna i telekomunikacja***
Profil kształcenia: ***ogólnoakademicki***
Poziom kształcenia: ***studia I stopnia***
uchwały Senatu* 46/2024/2025 z dnia 29 kwietnia 2025r.

Zajęcia	Kierunkowe efekty uczenia się	Treści programowe	Sposoby weryfikacji efektów uczenia się
1.Analiza matematyczna	K_W01 Ma szczegółową wiedzę z matematyki - obejmującą analizę matematyczną, algebrę, matematykę dyskretną, metody probabilistyczne, statystykę i metody numeryczne - przydatne do formułowania i rozwiązywania prostych zadań związanych z informatyką. K_U01 Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie K_U06 Ma umiejętność samokształcenia się, m.in. w celu podnoszenia kompetencji zawodowych	Przedmiot Analiza Matematyczna to tradycyjny element kształcenia na kierunkach technicznych. Zawiera on zagadnienia z rachunku różniczkowego funkcji jednej zmiennej, takie jak pochodne wyższych rzędów, wzór Taylora, oraz techniki badania przebiegu zmienności funkcji, co pozwala na zrozumienie ich zachowania i właściwości. Przedmiot obejmuje również całkę nieoznaczoną, nauczając technik całkowania przez podstawianie i przez części, a także sposoby obliczania całek pewnych funkcji wymiernych i niewymiernych. Ważną częścią jest całka oznaczona oraz jej zastosowania w geometrii, umożliwiające rozwiązanie problemów związanych z obliczaniem obszarów czy objętości.	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.Algebra liniowa	K_W01 Ma szczegółową wiedzę z matematyki - obejmującą analizę matematyczną, algebrę, matematykę dyskretną, metody probabilistyczne, statystykę i metody numeryczne - przydatne do formułowania i rozwiązywania prostych zadań związanych z informatyką. K_U01 Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Przedmiot Algebra liniowa obejmuje kompleksowe wprowadzenie do fundamentalnych zagadnień matematycznych. Rozpoczyna się od liczb zespolonych, prezentując ich podstawowe definicje, własności oraz różne formy: algebraiczną, trygonometryczną i wykładniczą, a także działania na nich. Następnie kurs koncentruje się na macierzach i wyznacznikach, omawiając podstawowe definicje, działania algebraiczne, macierz transponowaną, właściwości wyznacznika oraz jego obliczanie dla macierzy 2-go i 3-go stopnia, w tym rozwinięcie Laplace'a. Ważnym elementem jest nauka o macierzy odwrotnej i rzędzie macierzy. Kolejny blok tematyczny to układy równań	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

	K_U06 Ma umiejętność samokształcenia się, m.in. w celu podnoszenia kompetencji zawodowych	liniowych, ich zapis macierzowy, układy Cramera, twierdzenie Kroneckera-Capellego oraz metody rozwiązywania. Przedmiot także zagłębia się w przestrzeń liniową i jej bazy. Geometria analityczna jest omówiona poprzez wektory, iloczyny skalarne, wektorowe i mieszane, a także równania płaszczyzny, prostej oraz krzywych stożkowych takich jak okrąg, elipsa, hiperbola i parabola.	Na laboratorium zaliczenie może być realizowane w formie projektu.
3.Podstawy metod probabilistycznych i statystyki	K_W01 Ma szczegółową wiedzę z matematyki - obejmującą analizę matematyczną, algebrę, matematykę dyskretną, metody probabilistyczne, statystykę i metody numeryczne - przydatne do formułowania i rozwiązywania prostych zadań związanych z informatyką. K_U01 Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie K_K02 Ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera, w tym jej wpływ na środowisko, i związaną z tym odpowiedzialność za podejmowane decyzje	W ramach przedmiotu Podstawy metod probabilistycznych i statystyki studenci poznają rodzaje zdarzeń losowych oraz klasyczne i geometryczne definicje prawdopodobieństwa, które są kluczowe dla zrozumienia jego podstaw. Aksjomatyczna definicja prawdopodobieństwa i jej podstawowe własności umożliwiają dogłębne zrozumienie tej dziedziny. Przedmiot oferuje też wprowadzenie do kombinatoryki, niezbędnej w obliczeniach probabilistycznych. Omawiane są również prawdopodobieństwo warunkowe, zdarzenia niezależne, prawdopodobieństwo całkowite oraz twierdzenie Bayesa. Studenci uczą się schematu Bernoulliego, poznają zmienne losowe, dystrybuanty oraz wybrane rozkłady dyskretne i ciągłe. Przedmiot porusza także pojęcia wartości oczekiwanej, odchylenie standardowe i wariancję, a także wprowadza do statystyki opisowej i weryfikacji hipotez statystycznych.	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.Matematyka dyskretna	K_W01 Ma szczegółową wiedzę z matematyki - obejmującą analizę matematyczną, algebrę, matematykę dyskretną, metody probabilistyczne, statystykę i metody numeryczne - przydatne do formułowania i rozwiązywania prostych zadań związanych z informatyką. K_U01 Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie K_U06 Ma umiejętność samokształcenia się, m.in. w celu podnoszenia kompetencji zawodowych	Przedmiot Matematyka dyskretna obejmuje szeroki zakres tematów związanych z różnymi aspektami matematyki stosowanej i teoretycznej. Zajęcia rozpoczynają się od schematów kombinatorycznych, w tym wariacji, kombinacji, permutacji, oraz od podziałów zbiorów i liczb, które są kluczowe dla rozumienia podstaw kombinatoryki. Następnie kurs przechodzi do równań rekurencyjnych i funkcji tworzących, z przykładem problemu Fibonacciego, co umożliwia zrozumienie sekwencyjnych procesów. W ramach teorii grafów studenci poznają podstawowe pojęcia takie jak grafy i digrafy, stopnie wierzchołków oraz rodzaje grafów, w tym grafy dwudzielne i regularne. Omówiona jest również planarność grafu. Szczególną uwagę poświęca się drogom i cyklom, w tym cyklom Eulera oraz Hamiltona, z analizą problemu mostów królewieckich i	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.

		kryteriami hamiltonowskości grafów. Kurs kończy się na drzewach i lasach, w tym drzewach rozpinających, oraz omawia twierdzenia Cayleya i Kirchhoffa dotyczące zliczania drzew rozpinających.	
5. Systemy pomiarowe	K_W04 Ma szczegółową wiedzę w zakresie układów elektroniki, potrzebną do zrozumienia techniki cyfrowej i zasad funkcjonowania współczesnych komputerów K_U08 Potrofi programować układy akwizycji danych i ich dystrybucji K_U09 Potrafi wykorzystać do formułowania i rozwiązywania zadań informatycznych metody analityczne, symulacyjne i eksperymentalne	Przedmiot skupia się na metodach i narzędziach służących do przetwarzania, akwizycji oraz analizy danych pomiarowych w środowisku informatycznym. W ramach zajęć studenci zdobywają szczegółową wiedzę z zakresu układów elektroniki, dzięki czemu rozumieją technikę cyfrową. Ponadto uczą się programowania systemów akwizycji danych (m.in. czujników, modułów wejścia/wyjścia) i przygotowywania ich do wydajnej dystrybucji zebranych informacji. Wykorzystują przy tym analityczne, symulacyjne oraz eksperymentalne metody rozwiązywania problemów, co pozwala im skutecznie opracowywać i wdrażać rozwiązania w różnorodnych obszarach zastosowań inżynieryjnych oraz naukowo-badawczych.	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.Wprowadzenie do cyberbezpieczeństwa państw i jednostek	K_W15 Ma wiedzę nt. patentów, ustawy Prawo autorskie i prawa pokrewne oraz ustawy o ochronie danych osobowych K_W24 Zna i rozumie uwarunkowania i formy uczestnictwa w życiu społecznym i politycznym na różnych jego poziomach oraz w cyberprzestrzeni K_W25 Zna i potrafi scharakteryzować genezę, źródła , ewolucję i najważniejsze postaci dla rozwoju cyberbezpieczeństwa w wymiarze praktycznym i naukowym.	Definicje i podstawowe pojęcia: bezpieczeństwo jego poziomy, typy i wymiary, polityki bezpieczeństwa, cyberbezpieczeństwo, cyberprzestrzeń, cyberzagrożenia. Cyberbezpieczeństwo w systemie bezpieczeństwa państwa – znaczenie cyberbezpieczeństwa dla bezpieczeństwa narodowego Przegląd aktorów w cyberprzestrzeni: państwa, organizacje międzynarodowe, grupy hakerskie, jednostki. Cyberwojna i operacje w cyberprzestrzeni – podstawowe pojęcia i strategie. Polityka i strategia cyberbezpieczeństwa wybranych państw (np. Polska, USA, Rosja, Chiny, Państwa Nordyckie, Państwa Bałtyckie). Ewolucja zagrożeń cybernetycznych w kontekście nowych technologii. Cyberdyplomacja i globalna współpraca na rzecz bezpieczeństwa w cyberprzestrzeni. Perspektywy rozwoju kariery w dziedzinie cyberbezpieczeństwa – państwo, służby mundurowe, sektor prywatny. Znaczenie przepisów: prawo autorskie i ustawa o ochronie danych osobowych w kontekście 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.
7.Metody numeryczne	K_W01 Ma szczegółową wiedzę z matematyki - obejmującą analizę matematyczną, algebrę, matematykę dyskretną, metody probabilistyczne,	Przegląd tematyki w kontekście metod numerycznych: arytmetyka komputerowa, dokładność obliczeń, zbieżność metody numerycznej. Rozwiązywanie równań nieliniowych	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów.

	statystykę i metody numeryczne - przydatne do formułowania i rozwiązywania prostych zadań związanych z informatyką. K_W06 Ma w zaawansowanym stopniu, podbudowaną teoretycznie wiedzę ogólną w zakresie zastosowań wybranych algorytmów ich złożoności obliczeniowej, w szczególności w zakresie cyberbezpieczeństwa. K_U09 Potrafi wykorzystać do formułowania i rozwiązywania zadań informatycznych metody analityczne, symulacyjne i eksperymentalne, K_K03 Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania	Rozwiązywanie układów równań liniowych. Aproksymacja i interpolacja. Metody różniczkowania numerycznego. Kwadratury. Metody przybliżonego rozwiązywania równań różniczkowych	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 programowania	K_W03 Zna i rozumie algorytmy, języki i techniki programowania oraz tworzenia aplikacji. K_W07 Ma w zaawansowanym stopniu, podbudowaną teoretycznie wiedzę ogólną w zakresie języków i paradygmatów programowania, sztucznej inteligencji, baz danych. K_U11 Ma umiejętność formułowania algorytmów i ich programowania z użyciem przynajmniej jednego z popularnych środowisk programistycznych	Struktura programu w językach C pochodnych. Podstawowe biblioteki, sens ich stosowania. Wykorzystanie typów prostych Wykorzystanie typów tablicowych jedno i dwuwymiarowych. Definicja struktur. Instrukcje warunkowe (if, if-else, else-if). Instrukcje iteracyjne (for, while, do..while). Instrukcje wyboru (switch). Zastosowanie zmiennych plikowych. Wykorzystanie operatora new. Wykorzystanie zmiennych wskaźnikowych i referencyjnych. Definiowanie własnych funkcji.	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.Prawne podstawy cyberbezpieczeństwa	K_W12 Ma ogólną wiedzę dotyczącą zarządzania bezpieczeństwem informacji zgodnie z normami/regulacjami europejskimi i krajowymi. K_W17 Zna i rozumie podstawowe przepisy, pojęcia i zasady z zakresu cyberbezpieczeństwa, ochrony własności przemysłowej, intelektualnej i prawa autorskiego w sieci. K_U10 Potrafi – przy formułowaniu i rozwiązywaniu	Celem przedmiotu jest zapoznanie z podstawowymi pojęciami, źródłami i zasadami prawa dotyczącymi cyberbezpieczeństwa, ochrony danych i prywatności, wolności w cyberprzestrzeni oraz regulacjami międzynarodowymi i krajowymi w tym zakresie, z uwzględnieniem zagadnień cyberprzestępczości, sztucznej inteligencji i praw człowieka. Główne zagadnienia: Podstawowe wiadomości o prawie. Wyjaśnienie pojęć i definicje legalne. Cyberprzestrzeń, cyberbezpieczeństwo, bezpieczeństwo	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

	zadań inżynierskich z zakresu cyberbezpieczeństwa – dostrzegać ich aspekty systemowe, społeczne, ekonomiczne i prawne K_U23 Umie dokonać wstępnego przeglądu standardów ochrony informacji, potrafi przedstawić założenia poszczególnych dokumentów normatywnych i prawnych. Umie omówić niezbędne mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji oraz problem odpowiedzialności za naruszenie prawa chroniącego informację. K_U27 Potrafi przeprowadzić analizę i ocenę zagrożeń w cyberbezpieczeństwie, uwzględniając różnorodne wymiary bezpieczeństwa.	informacyjne, bezpieczeństwo teleinformacyjne, bezpieczeństwo teleinformatyczne. Bezpieczeństwo w cyberprzestrzeni w prawie międzynarodowym. Bezpieczeństwo w cyberprzestrzeni w prawie polskim. Cyberprzestępczość. przestępstwa stricte komputerowe. Próby regulacji prawnej sfery funkcjonowania sztucznej inteligencji. Prawa człowieka w cyberprzestrzeni. Prawo do prywatności w cyberprzestrzeni. Ochrona danych osobowych w cyberprzestrzeni. Wolność wypowiedzi w cyberprzestrzeni. Prawo do wolnych wyborów a cyberprzestrzeń.	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.Dostępność cyfrowa	K_W14 Ma wiedzę nt. kodeksów etycznych dotyczących informatyki, zna zasady etyki, rozumie zagrożenia związane z przestępczością elektroniczną i zna zasady ergonomii bezpieczeństwa i higieny pracy K_U02 Potrafi pracować indywidualnie i w zespole inżynierów; umie oszacować czas i dokonać wstępnej oceny ekonomicznej zleconego zadania; potrafi opracować i zrealizować harmonogram prac zapewniający dotrzymanie terminów	Wprowadzenie do dostępności cyfrowej. 2. Podstawy prawne wdrażania dostępności cyfrowej w Polsce, Europie i na świecie. 3. Standard WCAG. 4. Raport o stanie dostępności polskiej przestrzeni publicznej. 5. Dostępność cyfrowa przestrzeni biznesowej i korzyści z niej płynące. 6. Dostępność cyfrowa a inkluzywność i prawa człowieka. 7. Trzy poziomy dostępności cyfrowej dla stron internetowych, aplikacji mobilnych i zasobów cyfrowych - stan rzeczywisty i perspektywy zmian Dostępny dokument Word. 2. Dostępny arkusz kalkulacyjny. 3. Dostępna prezentacja multimedialna. 4. Zasady tworzenia tekstów alternatywnych. 5. Audiodeskrypcja. 6. Język prosty w rozumieniu i czytaniu. Planowanie (czasu, kosztów) i realizacja projektów związanych z produktami i usługami w zakresie dostępności.	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.Architektura systemów komputerowych	K_W04 Ma szczegółową wiedzę w zakresie układów elektroniki, potrzebną do zrozumienia techniki cyfrowej i zasad funkcjonowania współczesnych komputerów. K_U01 Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane	Systemy kodowania informacji i wartości liczbowych. Układy elektroniczne wykorzystywane w budowie komputera. Charakterystyka i analiza wybranych systemów komputerowych. Struktura procesora. Funkcjonowanie procesora i jego współdziałanie z pamięcią zewnętrzną. Struktura pamięci zewnętrznej. Reprezentacje instrukcji, danych i kodów, typy	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:

	informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	adresacji. Język maszynowy procesora. Realizacja operacji arytmetyczno-logicznych przez procesor w oparciu o elementy logiczne. Magistrale, interfejsy oraz urządzenia peryferyjne	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.
12. Systemy operacyjne	K_W19 Posiada wiedzę z zakresu budowy systemów operacyjnych, ich roli w zapewnieniu bezpieczeństwa informacji. K_U14 Ma umiejętność posługiwania się funkcjami systemu operacyjnego K_U20 Potrafi stosować mechanizmy synchronizacji procesów oraz programować komunikację sieciową w trybach klient-serwer i peer-to-peer	Historyczny rys rozwoju systemów operacyjnych. Rola i zadania systemu operacyjnego. Rodzaje systemów operacyjnych. Podstawy działania. Struktura systemu. Zasoby, procesy i wątki. Właściwości systemów operacyjnych. Planowanie przydziału procesora. Algorytmy planowania oraz kryteria oceny. Przykłady implementacja algorytmów planowania procesów i wątków. Mechanizmy synchronizacji procesów. Komunikacja i synchronizacja procesów – wzajemne wyłączanie, synchronizacja i blokada. Semafory - zasada działania, przykład implementacji. Zastosowanie semaforów w komunikacji międzyprocesowej. Hierarchia pamięci. Zarządzanie pamięcią operacyjną. Sterowania pamięcią, przydymiał pamięci. Pamięć wirtualna. System plików. Podstawowe operacje na plikach i folderach. Mechanizmy wejścia/wyjścia. Rodzaje urządzeń wejścia-wyjścia. Struktura mechanizmu wejścia wyjścia. Rola systemu operacyjnego w komunikacji poprzez sieci komp.	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.Sieci komputerowe	K_W05 Ma wiedzę w zaawansowanym stopniu zakresie telekomunikacji, potrzebną do zrozumienia zasad działania współczesnych sieci komputerowych, uwzględniając aspekty bezpieczeństwa. K_W18 Zna w zaawansowanym stopniu metody, techniki i narzędzia związane z przesyłaniem, przechowywaniem i przetwarzaniem danych w systemach informatycznych K_U09 Potrafi wykorzystać do formułowania i rozwiązywania zadań informatycznych metody analityczne, symulacyjne i eksperymentalne,	Historia sieci komputerowych. Zastosowania sieci komp. w rozwiązywaniu zadań informatycznych w tym symulacji i eksperymentu. Standardy sieciowe, model ISO/OSI, organizacje standaryzacyjne. Media transmisyjne i ich parametry. Technologia Ethernet, wykorzystywane media i rozwój, protokół ARP. Metody przełączania w sieci Ethernet, rodzaje i zastosowanie przełączników L2 i L3. Sieci bezprzewodowe, rodzina 802.11 (WiFi): dostęp do kanału, protokoły bezpieczeństwa. Protokół IP, komunikacja unicast/multicast, projektowanie schematu adresacji VLSM, istota routingu w sieciach. Charakterystyka protokołu IPv6, typy adresów oraz metody wdrażania. Warstwa transportowa sieci, protokoły TCP i UDP, segmentacja danych, multiplikacja połączeń i sesji na	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.

	K_U15 Ma umiejętność projektowania sieci komputerowych; potrafi pełnić funkcję administratora sieci komputerowej K_U20 Potrafi stosować mechanizmy synchronizacji procesów oraz programować komunikację sieciową w trybach klient-serwer i peerto-peer	hoście, realizacja niezawodności, połączenia między gniazdami, porty komunikacyjny i aspekt bezpieczeństwa. Podstawowe usługi sieciowe: warstwy aplikacji: poczta elektroniczna (SMTP, IMAP, POP, autoryzacja, zabezpieczenia), transfer danych (FTP, TFPT, SCP), zdalny dostęp (TELNET, SSH, usługi terminalowe), serwisy informacyjne (HTTP, HTTPS), rozproszony system nazw sieciowych (DNS). Konwergencja usług sieciowych, sieci SDN, SD-WAN, Kierunki rozwoju technologii sieciowych. Sieciowe usługi chmurowe.	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. Podstawy teleinformatyki	K_W03 Zna i rozumie algorytmy, języki i techniki programowania oraz tworzenia aplikacji. K_W05 Ma wiedzę w zaawansowanym stopniu zakresie telekomunikacji, potrzebną do zrozumienia zasad działania współczesnych sieci komputerowych, uwzględniając aspekty bezpieczeństwa. K_U15 Ma umiejętność projektowania sieci komputerowych; potrafi pełnić funkcję administratora sieci komputerowej	Sieci VLAN i łączy magistralnych. Routing między sieciami VLAN. Routing na przełączniku wielowarstwowym. Sieci bezprzewodowe WiFi (802.11). Protokół drzewa rozpinającego STP. Agregowanie łączy Ethernetowych. Zna i rozumie języki i techniki stosowane w konfiguracji i sterowaniu urządzeniami sieciowymi.	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.Programowanie obiektowe	K_W02 Ma w zaawansowanym stopniu wiedzę o cyklu życia systemów informatycznych K_W07 Ma w zaawansowanym stopniu, podbudowaną teoretycznie wiedzę ogólną w zakresie języków i paradygmatów programowania, sztucznej inteligencji, baz danych. K_U11 Ma umiejętność formułowania algorytmów i ich programowania z użyciem przynajmniej jednego z popularnych środowisk programistycznych	Elementy cyklu życia systemu informatycznego. Wprowadzenie do technik programowania obiektowego, Składnia wybranych języków obiektowych, Dziedziczenie, Enkapsulacja, Polimorfizm, Konstruktory, Destrutory, Funkcje zaprzyjaźnione, Interfejsy, Kontenery, Obsługa wyjkątków, Wielowątkowość.	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.Języki skryptowe	K_W03 Zna i rozumie algorytmy, języki i techniki programowania oraz tworzenia aplikacji. K_U11 Ma umiejętność formułowania algorytmów i ich programowania z użyciem przynajmniej jednego z popularnych środowisk programistycznych	Rola skryptów w administracji systemami i sieciami. Bash: zmienne, pętle, warunki — w kontekście automatyzacji zadań. Uruchamianie skryptów z crona i systemd. Obsługa procesów i ich monitorowanie. Skrypty do zarządzania użytkownikami, grupami i uprawnieniami. Parsowanie plików konfiguracyjnych (sed, awk, wyrażenia regularne). Podstawy komunikacji sieciowej (TCP/UDP, sockety). Pisanie prostych skryptów klienckich i serwerowych (Python, curl). Pobieranie danych z REST API. Obsługa błędów (try-except w Pythonie, set -e w Bashu). Narzędzia do debugowania: pdb, bash -x. Testy jednostkowe. Instalacja i konfiguracja Ansible. Pisanie playbooków do zarządzania systemami. Automatyczne wdrażanie konfiguracji sieci (np. ustawienia firewall, konfiguracja SSH). Integracja z Dockerem.	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.Kryptologia	K_W06 Ma w zaawansowanym stopniu, podbudowaną teoretycznie wiedzę ogólną w zakresie zastosowań wybranych algorytmów ich złożoności obliczeniowej, w szczególności w zakresie cyberbezpieczeństwa. K_W20 Ma w zaawansowanym stopniu wiedzę na temat algorytmów i protokołów kryptograficznych ich zastosowań w telekomunikacji oraz wiedzę umożliwiającą rozróżnianie metod szyfrowania informacji. K_W21 Ma w zaawansowanym stopniu wiedzę na temat metod i mechanizmów zapewniających bezpieczeństwo w sieciach komputerowych. Ma wiedzę o metodach uwierzytelniania i szyfrowania, wykrywania i przeciwdziałania atakom. K_U13 Potrafi, z wykorzystaniem metod z zakresu przedmiotów ścisłych rozwiązywać problemy w obszarze cyberbezpieczeństwa. K_K06 Ma świadomość roli społecznej absolwenta uczelni technicznej, a zwłaszcza rozumie potrzebę formułowania i przekazywania społeczeństwu —	Podstawy szyfrowania - realizacje praktyczne i zagadnienia teoretyczne, stanowiąc kluczowy element Cyberbezpieczeństwa. Studenci poznają szyfry klasyczne, algorytmy symetryczne (np. DES, AES), asymetryczne (np. RSA, ECC), funkcje skrótu oraz podpisy cyfrowe. Omawiana jest złożoność obliczeniowa algorytmów i jej znaczenie dla bezpieczeństwa. Analizowane są protokoły (np. SSL/TLS, SSH) i metody szyfrowania stosowane w telekomunikacji, a także porównywane ich zalety. Przedstawiane są techniki ochrony danych w sieciach, ataki na szyfry. Zadania praktyczne uwzględniają rozwiązywanie problemów cyberbezpieczeństwa przy użyciu narzędzi matematycznych (np. teoria liczb). Poruszane są też zagadnienia kryptanalizy i kryptografii kwantowej. Studenci uczą się również przekazywać wiedzę kryptologiczną w sposób zrozumiały.	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.

	m.in. poprzez środki masowego przekazu — informacji i opinii dotyczących osiągnięć informatyki i innych aspektów działalności inżyniera-informatyka; podejmuje starania, aby przekazać takie informacje i opinie w sposób powszechnie zrozumiały		
18.Wstęp do sztucznej inteligencji	K_W07 Ma w zaawansowanym stopniu, podbudowaną teoretycznie wiedzę ogólną w zakresie języków i paradygmatów programowania, sztucznej inteligencji, baz danych. K_W11 Zna metody, techniki i narzędzia, w tym AI, stosowane przy rozwiązywaniu złożonych zadań informatycznych związanych z bezpieczeństwem danych i infrastruktury sieciowej. K_U13 Potrafi, z wykorzystaniem metod z zakresu przedmiotów ścisłych rozwiązywać problemy w obszarze cyberbezpieczeństwa.	Algorytmy genetyczne, Perceptron, Sieci neuronowe, Automaty komórkowe, Zbiory przybliżone, Logika rozmyta, Skierowane liczby rozmyte, Automaty komórkowe, Wprowadzenie do Metaheurystyk, Algorytmy mrówkowe, Algorytmy pszczele, Poszukiwanie z tabu, Algorytm świetlików, Symulowane wyżarzanie	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.Bazy danych	K_W02 Ma w zaawansowanym stopniu wiedzę o cyklu życia systemów informatycznych K_W07 Ma w zaawansowanym stopniu, podbudowaną teoretycznie wiedzę ogólną w zakresie języków i paradygmatów programowania, sztucznej inteligencji, baz danych. K_W18 Zna w zaawansowanym stopniu metody, techniki i narzędzia związane z przesyłaniem, przechowywaniem i przetwarzaniem danych w systemach informatycznych K_U19 Ma umiejętność budowy systemów bazodanowych, wykorzystujących przynajmniej jeden z najbardziej popularnych systemów zarządzania bazą danych	Celem przedmiotu jest wprowadzenie studentów do modelowania baz danych (z uwzględnieniem kontekstu cyklu życia SI) z wykorzystaniem dwóch poziomów ogólności (model E-R oraz model relacyjny BD). Podejmowane aspekty zajęć to: zapoznanie sie z istotą relacji 1..1, 1..n, m..n oraz uzasadnione ich stosowanie. Wykorzystanie języka SQL do implementacji modelu baz danych z wykorzystaniem DDL, DML, DQL. Implementacja modelu baz danych będzie realizowana w DMBS Oracle oraz MySQL (lub innych równorzędnych).	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.Testy penetracyjne i kontrola zabezpieczeń	K_W10 Ma w zaawansowanym stopniu, wiedzę oraz zna narzędzia i techniki z zakresu testowania poziomu zabezpieczeń, zarówno w obszarze infrastruktury sieciowe jak i na poziomie aplikacji. K_U17 Umie zaimplementować narzędzia monitorujące bezpieczeństwo przetwarzanych danych K_U18 Potrafi dobrać i zastosować właściwe metod analizy danych w zadaniu analizy zagrożeń / wykrywania anomalii. K_U25 Potrafi zaplanować oraz przeprowadzić audyt bezpieczeństwa w tym testy penetracyjne.	Testy penetracyjne i kontrola zabezpieczeń stanowią kluczowy moduł kształcenia na kierunku cyberbezpieczeństwo, łączący zaawansowaną wiedzę techniczną z umiejętnościami praktycznymi. Program przedmiotu koncentruje się na następujących obszarach: Metodologie i narzędzia testów penetracyjnych: Studenci poznają frameworki, ucząc się planowania testów, modelowania zagrożeń oraz eksploatacji podatności w sieciach i aplikacjach. Wykorzystują narzędzia do analizy infrastruktury, testów aplikacji webowych czy automatyzacji ataków. Symulują ataki na systemy Windows/Linux, analizując m.in. podatności czy konfigurację firewalli. Poznają środowiska SIEM do detekcji anomalii. Uczą się wdrażać IDS/IPS oraz automatyzować analizę logów poprzez skrypty.	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.Bezpieczeństwo sieci korporacyjnych	K_W11 Zna metody, techniki i narzędzia, w tym AI, stosowane przy rozwiązywaniu złożonych zadań informatycznych związanych z bezpieczeństwem danych i infrastruktury sieciowej. K_U12 Potrafi planować, kontrolować i implementoać politykę bezpieczeństwa. K_U18 Potrafi dobrać i zastosować właściwe metod analizy danych w zadaniu analizy zagrożeń / wykrywania anomalii. K_U26 Potrafi skonfigurować i uruchomić mechanizmy bezpieczeństwa na ruterach i urządzeniach firewall, tunele szyfrowane i mechanizmy IDS.	Zabezpieczenie dostępu do urządzeń sieciowych, zarządzanie In-band vs OOB. Zabezpieczenie portów przełączników Ethernetowych przed atakami w L2, koncepcja inspekcji protokołu ARP oraz DHCP. Dystrybucja sygnatury czasu UTC, korekta związana z lokalizacją. Istota generowania logów oraz pułapek SNMP, centralizacja ich rejestracji. Centralizacja uwierzytelnienia, autoryzacji oraz rozliczeń – AAA. Architektura RADIUS: serwer, klient, użytkownicy. Kontrola dostępu do sieci 802.1X – bezpieczne uwierzytelnianie urządzeń sieci LAN. Monitorowanie ruchu przechodzące przez wybrane porty przełącznika. Segmentacja VLANów zwiększająca bezpieczeństwo sieci korporacyjnych, warianty implementacyjne PVLAN. Protokoły nadmiarowości pierwszego skoku jako mechanizm niezawodności sieci, porównanie standardów otwartych i zamkniętych. Bezpieczeństwo w sieciach bezprzewodowych – ewolucja standardów (m. in. WPA2-Enterprise, WPA3) segmentacja ruchu, topologia z kontrolerem WLC zarządzającym punktami dostępu. Bezpieczny backup konfiguracji oraz plików systemowych.	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.(Bezpieczne) Technologie internetowe	K_W17 Zna i rozumie podstawowe przepisy, pojęcia i zasady z zakresu cyberbezpieczeństwa, ochrony własności przemysłowej, intelektualnej i prawa	Moduł obejmuje techniki szyfrowania danych w ruchu (TLS 1.3, IPSec) i spoczynku (AES-256, VeraCrypt). Mechanizmy kontroli dostępu. Testy integralności danych z użyciem funkcji skrótu. Konfigurację bezpiecznych kanałów komunikacyjnych. Techniki	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów.

	autorskiego w sieci. K_W18 Zna w zaawansowanym stopniu metody, techniki i narzędzia związane z przesyłaniem, przechowywaniem i przetwarzaniem danych w systemach informatycznych K_W21 Ma w zaawansowanym stopniu wiedzę na temat metod i mechanizmów zapewniających bezpieczeństwo w sieciach komputerowych. Ma wiedzę o metodach uwierzytelniania i szyfrowania, wykrywania i przeciwdziałania atakom. K_U16 Potrafi zabezpieczyć przesyłane dane przed nieuprawnionym odczytem K_U19 Ma umiejętność budowy systemów bazodanowych, wykorzystujących przynajmniej jeden z najbardziej popularnych systemów zarządzania bazą danych	uwierzytelniania: infrastruktura PKI, protokoły RADIUS/TACACS+, biometria. Projektowanie bezpiecznych architektur baz danych.	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.Audyt systemów teleinformatycznych	K_W09 Ma wiedzę w zaawansowanym stopniu zakresie audytu systemów informatycznych oraz zna zagadnienia i metody stosowane w informatyce śledczej. K_W10 Ma w zaawansowanym stopniu, wiedzę oraz zna narzędzia i techniki z zakresu testowania poziomu zabezpieczeń, zarówno w obszarze infrastruktury sieciowe jak i na poziomie aplikacji. K_U21 Potrafi stosować techniki pozyskiwania dowodów cyfrowych zróżnych źródeł. Potrafi przeprowadzić i udokumentować analizę powłamaniową incydentu teleinformatycznego. K_U25 Potrafi zaplanować oraz przeprowadzić audyt bezpieczeństwa w tym testy penetracyjne. K_U23 Umie dokonać wstępnego przeglądu standardów ochrony informacji, potrafi przedstawić założenia poszczególnych dokumentów normatywnych i prawnych. Umie omówić niezbędne mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji oraz problem odpowiedzialności za naruszenie prawa chroniącego	Przeglądu standardów ochrony informacji. Metodyki audytu (np. LP-A8, TISM, COBIT). Zagadnienia informatyki śledczej: pozyskiwanie i analiza dowodów cyfrowych. Narzędzia audytowe: skanery podatności, systemy SIEM. Testowanie poziomu zabezpieczeń. Techniki testowania: BlackBox, WhiteBox, GreyBox. Narzędzia do testowania. Techniki pozyskiwania dowodów: z dysków twardych, pamięci RAM, urządzeń mobilnych. Analiza incydentów: tworzenie raportów z incydentów, dokumentacja procesu. Planowanie i przeprowadzanie audytu bezpieczeństwa. Etapy audytu: planowanie, zbieranie danych, ocena ryzyka, testy penetracyjne, raportowanie. Narzędzia audytowe: skanery podatności, systemy SIEM, oprogramowanie do analizy logów. Zarządzanie incydentami: procedury reagowania na incydenty, plany ciągłości działania.	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.

	informację		
24.Współpraca międzynarodowa na rzecz cyberbezpieczeństwa	K_W23 Zna i rozumie w zaawansowanym stopniu mechanizmy podejmowania decyzji politycznych na poziomie krajowym i międzynarodowym, a także wykorzystania narzędzi elektronicznych w administrowaniu państwem i jednostkami terytorialnymi. K_W24 Zna i rozumie uwarunkowania i formy uczestnictwa w życiu społecznym i politycznym na różnych jego poziomach oraz w cyberprzestrzeni K_U07 Potrafi analizować, wyciągać wniosku, z procesów decyzyjnych na szczeblu krajowym i międzynarodowym, uwzględniając kontekst cyberbezpieczeństwa. K_U27 Potrafi przeprowadzić analizę i ocenę zagrożeń w cyberbezpieczeństwie, uwzględniając różnorodne wymiary bezpieczeństwa. K_K04 Ma świadomość ważności zachowania w sposób profesjonalny, przestrzegania zasad etyki zawodowej i poszanowania różnorodności poglądów i kultur	Główne zagadnienia: Wprowadzenie do współpracy międzynarodowej w cyberbezpieczeństwie Strategie i polityki cyberbezpieczeństwa na poziomie globalnym Prawo międzynarodowe a cyberbezpieczeństwo Organizacje międzynarodowe w zakresie cyberbezpieczeństwa NATO i cyberobrona Unia Europejska i polityka cyberbezpieczeństwa Cyberterroryzm i zwalczanie cyberprzestępczości na arenie międzynarodowej Ataki na infrastrukturę krytyczną i reakcja międzynarodowa Cyberwojna i cyberkonflikty międzynarodowe Przeciwdziałanie dezinformacji i wojnie informacyjnej Studium przypadków – analiza największych incydentów cyberbezpieczeństwa Analiza strategii cyberbezpieczeństwa wybranych państw Tworzenie polityki bezpieczeństwa dla organizacji międzynarodowej Analiza międzynarodowych regulacji prawnych dotyczących cyberprzestępczości Warsztaty z zakresu cyberhigieny i ochrony danych osobowych Analiza przypadku cyberataków na infrastrukturę krytyczną Praktyczne aspekty wymiany informacji między krajami w ramach cyberobrony Analiza działań międzynarodowych organizacji w walce z cyberterroryzmem Scenariusze cyberwojny – role państw i organizacji międzynarodowych Wpływ dezinformacji na bezpieczeństwo międzynarodowe – analiza fake newsów Zaliczeniowe studium przypadku – opracowanie strategii międzynarodowej reakcji na cyberatak	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.Sieci sensorowe	K_W04 Ma szczegółową wiedzę w zakresie układów elektroniki, potrzebną do zrozumienia techniki cyfrowej i zasad funkcjonowania współczesnych komputerów K_U08 Potrafi programować układy akwizycji danych i ich dystrybucji K_U28 Potrafi ocenić przydatność rutynowych metod i narzędzi informatycznych oraz wybrać i zastosować właściwą metodę i narzędzia do zadań za zakresu cyberbezpieczeństwa	Inteligentne czujniki i systemy monitorujące wykorzystywane w różnych dziedzinach, takich jak IoT i sieci przemysłowe (OT). Zagrożenia związane z atakami na urządzenia IoT (m.in. infekcje malware, nieautoryzowany dostęp oraz fizyczne wtargnięcia). Metody zabezpieczania sieci IoT (VPN, szyfrowanie informacji i autentykacja urządzeń). Ocena przydatności metod i narzędzi informatycznych w celu zabezpieczenia sieci sensorowych. Narzędzia do monitorowania ruchu sieciowego. Techniki uwierzytelniania wieloskładnikowego (MFA) do zwiększenia bezpieczeństwa dostępu do sieci.	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.Bezpieczeństwo oprogramowania	K_W02 Ma w zaawansowanym stopniu wiedzę o cyklu życia systemów informatycznych K_W20 Ma w zaawansowanym stopniu wiedzę na temat algorytmów i protokołów kryptograficznych ich zastosowań w telekomunikacji oraz wiedzę umożliwiającą rozróżnianie metod szyfrowania informacji. K_U16 Potrafi zabezpieczyć przesyłane dane przed nieuprawnionym odczytem K_U17 Umie zaimplementować narzędzia monitorujące bezpieczeństwo przetwarzanych danych K_U26 Potrafi skonfigurować i uruchomić mechanizmy bezpieczeństwa na ruterach i urządzeniach firewall, tunele szyfrowane i mechanizmy IDS.	Projektowania bezpiecznych systemów informatycznych. Analiza wymagań i specyfikacji systemu z naciskiem na bezpieczeństwo i prywatność. Podstawy zarządzania ryzykiem oraz polityki bezpieczeństwa w organizacjach. Zaawansowane algorytmy szyfrowania oraz ich zastosowania w telekomunikacji. Narzędzia monitorujące bezpieczeństwo przetwarzanych danych. Analiza podatności w oprogramowaniu oraz metody ich przeciwdziałania. Systemy zabezpieczające oprogramowanie. Najlepsze praktyki w tworzeniu bezpiecznego oprogramowania.	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.Ochrona informacji niejawnych	K_W08 Ma wiedzę z zakresu zarządzania ryzykiem a także polityk bezpieczeństwa w różnych organizacjach. K_W12 Ma ogólną wiedzę dotyczącą zarządzania bezpieczeństwem informacji zgodnie z normami/regulacjami europejskimi i krajowymi. K_W15 Ma wiedzę nt. patentów, ustawy Prawo autorskie i prawa pokrewne oraz ustawy o ochronie danych osobowych	Zasady klasyfikacji informacji niejawnych. Kontrola dostępu oraz bezpieczne przechowywanie i przetwarzanie danych niejawnych. Normy i regulacje europejskie oraz krajowe. Analiza procesów decyzyjnych na szczeblu krajowym i międzynarodowym. Fizyczne aspekty ochrony informacji niejawnych, w tym środki techniczne i osobowe, takie jak systemy sygnalizacji zagrożeń, kontrola dostępu i nadzór wizyjny. Tworzenie Planu Ochrony Informacji Niejawnej.	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.Polityka i system cyberbezpieczeństwa RP	K_W12 Ma ogólną wiedzę dotyczącą zarządzania bezpieczeństwem informacji zgodnie z normami/regulacjami europejskimi i krajowymi. K_W23 Zna i rozumie w zaawansowanym stopniu mechanizmy podejmowania decyzji politycznych na poziomie krajowym i międzynarodowym, a także wykorzystania narzędzi elektronicznych w administrowaniu państwem i jednostkami terytorialnymi. K_W24 Zna i rozumie uwarunkowania i formy uczestnictwa w życiu społecznym i politycznym na różnych jego poziomach oraz w cyberprzestrzeni K_W25 Zna i potrafi scharakteryzować genezę, źródła , ewolucję i najważniejsze postaci dla rozwoju cyberbezpieczeństwa w wymiarze praktycznym i naukowym. K_U07 Potrafi analizować, wyciągać wniosku, z procesów decyzyjnych na szczeblu krajowym i międzynarodowym, uwzględniając kontekst cyberbezpieczeństwa.	Główne zagadnienia obejmują genezę cyberprzestrzeni, podstawowe pojęcia (sieci, systemy, użytkownicy) oraz regulacje bezpieczeństwa w prawie krajowym i międzynarodowym (ONZ, Rada Europy, UE). Dotyczą też polityki publicznej w zakresie cyberochrony (Strategia Cyfryzacji Polski 2035, polityka RP i państw członkowskich UE), zagadnień cyberbezpieczeństwa (istota, zagrożenia, system bezpieczeństwa narodowego, współpraca instytucji i sektora prywatnego), cyberwojny i cyberterroryzmu, a także cyberataków (rodzaje i obrona), cyberprzestępczości i szpiegostwa. Ważne są standardy i dobre praktyki ochrony sieci oraz badania naukowe w tym obszarze. Omówiono także strategię UE w zakresie cyberbezpieczeństwa, krajowy system cyberbezpieczeństwa, globalne zagrożenia w sieci, walkę informacyjną i dezinformację.	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.Praktyczne wykorzystanie informacji z otwartych źródeł	K_W08 Ma wiedzę z zakresu zarządzania ryzykiem a także polityk bezpieczeństwa w różnych organizacjach. K_U01 Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	Techniki pozyskiwania danych z mediów społecznościowych, blogów, forów dyskusyjnych, oraz innych internetowych źródeł, takich jak publikacje rządowe i artykuły naukowe. Wykorzystywanie zdobytych informacji (do monitorowania trendów rynkowych, oceny ryzyka biznesowego oraz identyfikacji potencjalnych zagrożeń bezpieczeństwa). Integracja i interpretacja uzyskanych informacji. Narzędzia do automatyzacji procesów pozyskiwania informacji. Analiza przypadków wykorzystania informacji z otwartych źródeł w służbach wywiadowczych, bezpieczeństwie korporacyjnym oraz w dziennikarstwie śledczym.	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.Informatyka śledcza	K_W09 Ma wiedzę w zaawansowanym stopniu zakresie audytu systemów informatycznych oraz zna zagadnienia i metody stosowane w informatyce śledczej. K_U21 Potrafi stosować techniki pozyskiwania dowodów cyfrowych zróżnych źródeł. Potrafi przeprowadzić i udokumentować analizę powłamaniową incydentu teleinformatycznego.	Audyt systemów informatycznych. Ocena infrastruktury IT, systemów bezpieczeństwa i zarządzania danymi. Techniki pozyskiwania dowodów cyfrowych z różnych źródeł. Narzędzia forenzyczne do analizy incydentów teleinformatycznych. Techniki analizy powłamaniowej, w tym tworzenie raportów z incydentów i dokumentacja procesu. Współpraca z organami ścigania. Procedury zabezpieczania dowodów cyfrowych. Symulacja incydentów bezpieczeństwa. Najlepsze praktyki w zarządzaniu incydentami bezpieczeństwa i współpracy z zespołami CSIRT.	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.Sieciowe systemy operacyjne	K_W19 Posiada wiedzę z zakresu budowy systemów operacyjnych, ich roli w zapewnieniu bezpieczeństwa informacji. K_U14 Ma umiejętność posługiwania się funkcjami systemu operacyjnego K_U15 Ma umiejętność projektowania sieci komputerowych; potrafi pełnić funkcję administratora sieci komputerowej	Routing statyczny IPv4. Standardowe listy kontroli dostępu ACL Rozszerzone listy kontroli dostępu ACL. Automatyczna konfiguracja adresów hosta DHCP. Statyczna translacja NAT + Port Forwarding. Dynamiczna translacja NAT (pula / PAT).	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.Zespołowy projekt informatyczny	K_W16 Ma wiedzę dotyczącą zarządzania i prowadzenia działalności gospodarczej, zna ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości K_U02 Potrafi pracować indywidualnie i w zespole inżynierów; umie oszacować czas i dokonać wstępnej	Przedmiot "Zespołowy projekt informatyczny" skupia się na praktycznym zastosowaniu wiedzy w projektach realizowanych w grupach. Zajęcia rozpoczynają się od omówienia zasad organizacji przedsięwzięć informatycznych, harmonogramowania oraz zarządzania jakością i ryzykiem. Kurs podkreśla znaczenie dokumentowania pracy i lokalizacji przechowywania kodu. Uczestnicy uczą się pracy zespołowej,	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

	oceny ekonomicznej zleconego zadania; potrafi opracować i zrealizować harmonogram prac zapewniający dotrzymanie terminów K_U04 Potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania, także z wykorzystaniem narzędzi informatycznych. K_U22 Potrafi wybrać i zastosować odpowiednią metodykę zarządzania projektami (w tym eksperymentalnymi) dla konkretnego zadania. Potrafi zdefiniować projekt i nim zarządzać. Umie zastosować podejście systemowe K_U24 Potrafi wykorzystać zasady bezpieczeństwa związane z pracą w środowisku przemysłowym K_K05 Potrafi myśleć i działać w sposób przedsiębiorczy	dzielą się na mniejsze grupy, ustalają liderów i metodyki pracy. Projektowanie, wdrażanie i prezentacja projektów są integralnymi częściami kursu, podobnie jak ocena postępów i zarządzanie problemami.	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. Zarządzanie projektami IT	K_W16 Ma wiedzę dotyczącą zarządzania i prowadzenia działalności gospodarczej, zna ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości K_U02 Potrafi pracować indywidualnie i w zespole inżynierów; umie oszacować czas i dokonać wstępnej oceny ekonomicznej zleconego zadania; potrafi opracować i zrealizować harmonogram prac zapewniający dotrzymanie terminów K_U22 Potrafi wybrać i zastosować odpowiednią metodykę zarządzania projektami (w tym eksperymentalnymi) dla konkretnego zadania. Potrafi zdefiniować projekt i nim zarządzać. Umie zastosować podejście systemowe. K_K03 Ma świadomość odpowiedzialności za pracę własną oraz gotowość podporządkowania się zasadom pracy w zespole i ponoszenia odpowiedzialności za wspólnie realizowane zadania	Wstęp do zarządzania projektem, definicje. Szacowanie czasu i ocena ekonomiczna. Metody zarządzania projektem. Zespół projektowy. Role w projekcie. Narzędzia kierownika projektu. Kompetencje w zespole projektowym w ICT. Specyfika projektów ICT ze specjalizacją w obszarze cyberbezpieczeństwa. Zarządzanie czasem, ryzykiem, jakością, budżetem i zmianą	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.Zagrożenia cywilizacyjne ery społeczeństwa cyfrowego	K_W13 Zna i rozumie w zaawansowanym stopniu różnorodne wymiary i uwarunkowania bezpieczeństwa, w tym zwłaszcza cyberbezpieczeństwa oraz związane z nimi zagrożenia. K_W22 Zna i rozumie fundamentalne dylematy współczesnej cywilizacji wynikające z postępu technologicznego. K_U10 Potrafi – przy formułowaniu i rozwiązywaniu zadań inżynierskich z zakresu cyberbezpieczeństwa – dostrzegać ich aspekty systemowe, społeczne, ekonomiczne i prawne K_U27 Potrafi przeprowadzić analizę i ocenę zagrożeń w cyberbezpieczeństwie, uwzględniając różnorodne wymiary bezpieczeństwa.	Paradygmat społeczeństwa ryzyka i permanentnej niepewności. - wojny i konflikty - kryzys ekologiczny - kryzys migracyjny - cofanie się demokracji - rozwój AI Transhumanizm jako ideologia czasów współczesnych - postulat nieśmiertelności - era postludzi - dylematy etyczne ery cyfrowej i transhumanizmu - bioinżynieria społeczna i biopolityka Jednostka w rzeczywistości cyfrowej: - uzależnienia cyfrowe - zachowania suicydalne - dezinformacja, fake news, propaganda- młodzież wobec zagrożeń w Internecie - seniorzy wobec zagrożeń cyfrowych - przestępczość zorganizowana w sieci. Weryfikacja umiejętności: dostrzeganie wybranych aspektów pozatechnicznych, analiza i ocena 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.
35.Edukacja na rzecz cyberbezpieczeństwa	K_W13 Zna i rozumie w zaawansowanym stopniu różnorodne wymiary i uwarunkowania bezpieczeństwa, w tym zwłaszcza cyberbezpieczeństwa oraz związane z nimi zagrożenia. K_U03 potrafi przygotować i przedstawić krótką prezentację poświęconą wynikom realizacji zadania inżynierskiego K_U06 Ma umiejętność samokształcenia się, m.in. w celu podnoszenia kompetencji zawodowych K_K02 Ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera, w tym jej wpływ na środowisko, i związaną z tym odpowiedzialność za podejmowane decyzje	Obszary poznawcze i empiryczne w edukacji na rzecz cyberbezpieczeństwa Podstawy wiedzy o kształceniu w zakresie bezpieczeństwa w cyberprzestrzeni Praktyczne aspekty wykorzystania technologii komputerowych w procesie kształcenia Specyfika zagrożeń w cyberprzestrzeni Środowisko szkół wokół bezpieczeństwa w cyberprzestrzeni System edukacji kadr administracji rządowej i samorządowej w zakresie cyberzagrożeń Szkolenie pracowników administracji państwowej do bezpiecznych zachowań w sieci Rola organizacji społecznych i mediów w edukacji na rzecz cyberbezpieczeństwa Teorie kształcenia w świecie cyfrowym Charakterystyka najważniejszych zagrożeń w cyberprzestrzeni Strategie ataków i obrony w cyberprzestrzeni-analiza przypadków Programy edukacyjne i prewencyjne realizowane na rzecz cyberbezpieczeństwa Badania naukowe realizowane na rzecz cyberbezpieczeństwa Edukacja na rzecz cyberbezpieczeństwa w Unii Europejskiej Edukacja na rzecz cyberbezpieczeństwa w wybranych państwach	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.

36.Polityki bezpieczeństwa	K_W08 Ma wiedzę z zakresu zarządzania ryzykiem a także polityk bezpieczeństwa w różnych organizacjach. K_W15 Ma wiedzę nt. patentów, ustawy Prawo autorskie i prawa pokrewne oraz ustawy o ochronie danych osobowych K_U12 Potrafi planować, kontrolować i implementować politykę bezpieczeństwa.	Elementy polityki bezpieczeństwa (w tym zarządzanie ryzykiem, kontrola dostępu, bezpieczeństwo fizyczne i sieciowe, oraz procedury reagowania na incydenty bezpieczeństwa). Planowanie, kontrola i implementacja polityk bezpieczeństwa, uwzględniając przepisy krajowe i międzynarodowe. Polityka informacyjna, ochrona informacji niejawnych i polityka bezpieczeństwa systemu teleinformatycznego. Tworzenie i wdrażanie polityki bezpieczeństwa w różnych organizacjach. Weryfikacja umiejętności - projekt.	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.
37.Seminarium dyplomowe	K_W17 Zna i rozumie podstawowe przepisy, pojęcia i zasady z zakresu cyberbezpieczeństwa, ochrony własności przemysłowej, intelektualnej i prawa autorskiego w sieci. K_U02 Potrafi pracować indywidualnie i w zespole inżynierów; umie oszacować czas i dokonać wstępnej oceny ekonomicznej zleconego zadania; potrafi opracować i zrealizować harmonogram prac zapewniający dotrzymanie terminów K_U03 potrafi przygotować i przedstawić krótką prezentację poświęconą wynikom realizacji zadania inżynierskiego K_U04 Potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania, także z wykorzystaniem narzędzi informatycznych. K_U05 Posługuje się językiem angielskim w stopniu (B2) wystarczającym do porozumiewania się, a także czytania ze zrozumieniem kart katalogowych, not aplikacyjnych, instrukcji obsługi urządzeń elektronicznych i narzędzi informatycznych oraz podobnych dokumentów	Przedmiot skupia się na realizacji pracy dyplomowej jako całości, dopracowanie części dokumentacyjnej i teoretycznej. Ważnym elementem jest rozwijanie umiejętności komunikacyjnych – oraz systemowe podejście do realizowanych zadań. Podczas seminarium studenci rozwijają swoje kompetencje techniczne i organizacyjne, ucząc się jednocześnie ciągłego podnoszenia kwalifikacji. Przygotowanie do obrany pracy.	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.

	K_U22 Potrafi wybrać i zastosować odpowiednią metodykę zarządzania projektami (w tym eksperymentalnymi) dla konkretnego zadania. Potrafi zdefiniować projekt i nim zarządzać. Umie zastosować podejście systemowe K_U28 Potrafi ocenić przydatność rutynowych metod i narzędzi informatycznych oraz wybrać i zastosować właściwą metodę i narzędzia do zadań za zakresu cyberbezpieczeństwa K_K01 Rozumie potrzebę i zna możliwości ciągłego dokształcania się, podnoszenia kompetencji zawodowych, osobistych i społecznych		
38.Wychowanie fizyczne		Zajęcia realizowane zgodnie z obowiązującym programem.	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.
39.Język obcy	K_U05 Posługuje się językiem angielskim w stopniu (B2) wystarczającym do porozumiewania się, a także czytania ze zrozumieniem kart katalogowych, not aplikacyjnych, instrukcji obsługi urządzeń elektronicznych i narzędzi informatycznych oraz podobnych dokumentów	Przedmiot język obcy skupia się na umiejętnościach komunikacyjnych potrzebnych inżynierom. Kurs umożliwia przygotowanie i prezentację wyników np. zadania inżynierskiego, a także rozwija zdolność czytania i rozumienia tekstów np. dokumentacji technicznej.	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.
1.Problemy społeczne i zawodowe informatyki	K_W14 Ma wiedzę nt. kodeksów etycznych dotyczących informatyki, zna zasady etyki, rozumie zagrożenia związane z przestępczością elektroniczną i zna zasady ergonomii bezpieczeństwa i higieny pracy K_W22 Zna i rozumie fundamentalne dylematy współczesnej cywilizacji wynikające z postępu technologicznego. K_K01 Rozumie potrzebę i zna możliwości ciągłego dokształcania się, podnoszenia kompetencji zawodowych, osobistych i społecznych K_K04 Ma świadomość ważności zachowania w sposób profesjonalny, przestrzegania zasad etyki zawodowej i poszanowania różnorodności poglądów i kultur K_K06 Ma świadomość roli społecznej absolwenta uczelni technicznej, a zwłaszcza rozumie potrzebę formułowania i przekazywania społeczeństwu — m.in. poprzez środki masowego przekazu — informacji i opinii dotyczących osiągnięć informatyki i innych aspektów działalności inżyniera-informatyka; podejmuje starania, aby przekazać takie informacje i opinie w sposób powszechnie zrozumiały	Przedmiot "Problemy społeczne i zawodowe informatyki" koncentruje się na analizie etycznych i prawnych aspektów działalności w branży IT. Kurs zaczyna się od omówienia kodeksów etycznych specyficznych dla informatyki, które kształtują odpowiedzialne postępowanie profesjonalistów. Zajęcia obejmują także zasady etyki w działalności gospodarczej, które są kluczowe dla utrzymania uczciwości i zaufania w relacjach biznesowych. Kolejnym istotnym tematem są zagrożenia wynikające z przestępczości elektronicznej, co podkreśla potrzebę świadomości i ochrony w cyfrowym środowisku. Przedmiot porusza również podstawowe zasady bezpieczeństwa i higieny pracy, niezbędne w zapewnieniu zdrowych i bezpiecznych warunków pracy. Ważnym aspektem są zasady ochrony własności intelektualnej.	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.Podstawy przedsiębiorczości	K_W16 Ma wiedzę dotyczącą zarządzania i prowadzenia działalności gospodarczej, zna ogólne zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości K_K05 Potrafi myśleć i działać w sposób przedsiębiorczy	Przedsiębiorczość w teoriach ekonomii i zarządzania Przedsiębiorczość i jej rodzaje Charakterystyka przedsiębiorcy Uwarunkowania rozwoju przedsiębiorczości Małe i średnie przedsiębiorstwa efektem zachowań przedsiębiorczych Przedsiębiorczość rodzinna Przedsiębiorczość kobiet Przedsiębiorczość społeczna	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.Elementy ergonomii i BHP	K_W14 Ma wiedzę nt. kodeksów etycznych dotyczących informatyki, zna zasady etyki, rozumie zagrożenia związane z przestępczością elektroniczną i zna zasady ergonomii bezpieczeństwa i higieny pracy K_U24 Potrafi wykorzystać zasady bezpieczeństwa związane z pracą w środowisku przemysłowym K_K02 Ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera, w tym jej wpływ na środowisko, i związaną z tym odpowiedzialność za podejmowane decyzje	Przedmiot „Elementy ergonomii i BHP" uczy zasad ergonomii, analizy ryzyka i technik tworzenia bezpiecznego środowiska pracy, poprawiając efektywność i komfort pracy.	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.Historia cybebezpieczeństwa	K_W22 Zna i rozumie fundamentalne dylematy współczesnej cywilizacji wynikające z postępu technologicznego. K_W25 Zna i potrafi scharakteryzować genezę, źródła , ewolucję i najważniejsze postaci dla rozwoju cyberbezpieczeństwa w wymiarze praktycznym i naukowym. K_K04 Ma świadomość ważności zachowania w sposób profesjonalny, przestrzegania zasad etyki zawodowej i poszanowania różnorodności poglądów i kultur	Rola mediów w życiu człowieka Komunikowanie masowe i środki komunikowania masowego – ogólna charakterystyka Historia rewolucji informatycznej Początki mediów, ich zadania, cywilizacja medialna System komputerowy - historia, podstawy i zasady działania Praktyczne podstawy sieci komputerowych. Usługi sieciowe i ich wpływ na życie społeczne Historia i rozwój Internetu Ocena i selekcja informacji pochodzącej z Internetu Internet jako nowa forma komunikacji: szanse i niebezpieczeństwa Konwergencja mediów i jej konsekwencje Media społecznościowe. Koncepcja wirtualnej społeczności Media mobilne – ich ewolucja i rola jako centrów komunikacyjnych Wyznaczniki jakości informacji w mediach	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.

		Rola mediów we współczesnych konfliktach zbrojnych i aktach terrorystycznych Cyberwalka. Militarny wymiar działań Usługi sieciowe i ich wpływ na życie współczesne Patologiczne formy korzystania z mediów Psychologiczne konteksty korzystania z mediów Systemy medialne w poszczególnych krajach	
1.Bezpieczenstwo usług sieciowych	K_W04 Ma szczegółową wiedzę w zakresie układów elektroniki, potrzebną do zrozumienia techniki cyfrowej i zasad funkcjonowania współczesnych komputerów. K_W11 Zna metody, techniki i narzędzia, w tym AI, stosowane przy rozwiązywaniu złożonych zadań informatycznych związanych z bezpieczeństwem danych i infrastruktury sieciowej. K_W21 Ma w zaawansowanym stopniu wiedzę na temat metod i mechanizmów zapewniających bezpieczeństwo w sieciach komputerowych. Ma wiedzę o metodach uwierzytelniania i szyfrowania, wykrywania i przeciwdziałania atakom. K_U15 Ma umiejętność projektowania sieci komputerowych; potrafi pełnić funkcję administratora sieci komputerowej	Metody, techniki i narzędzia w tym: układy techniki cyfrowej, sztuczna inteligencja (AI), stosowane do ochrony bezpieczeństwa usług sieciowych. Metody uwierzytelniania i szyfrowania usług sieciowych. Metody wykrywania i przeciwdziałania atakom na usługi. Systemy zabezpieczające usługi sieciowe. Oceną i poprawą bezpieczeństwa istniejących usług 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.
2.Ataki na sieci i metody obrony	K_W06 Ma w zaawansowanym stopniu, podbudowaną teoretycznie wiedzę ogólną w zakresie zastosowań wybranych algorytmów ich złożoności obliczeniowej, w szczególności w zakresie cyberbezpieczeństwa. K_W10 Ma w zaawansowanym stopniu, wiedzę oraz zna narzędzia i techniki z zakresu testowania poziomu zabezpieczeń, zarówno w obszarze infrastruktury sieciowe jak i na poziomie aplikacji K_U16 Potrafi zabezpieczyć przesyłane dane przed nieuprawnionym odczytem K_U27 Potrafi przeprowadzić analizę i ocenę zagrożeń w cyberbezpieczeństwie, uwzględniając różnorodne wymiary bezpieczeństwa.	Rodzaje zagrożeń i ataków skierowanych na warstwę aplikacji, protokołu lub sieci. Typy ataków (m.in. phishing, ataki na hasła i złośliwe oprogramowanie). Mechanizmy i skutki ataków. Metody obrony przed atakami. Filtracja ruchu, ograniczenie przepustowości, wykorzystanie usług zewnętrznych oraz monitorowanie i analiza ruchu.	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.Zarządzanie dostępem i kontrola tożsamości w sieci	K_W17 Zna i rozumie podstawowe przepisy, pojęcia i zasady z zakresu cyberbezpieczeństwa, ochrony własności przemysłowej, intelektualnej i prawa autorskiego w sieci. K_W19 Posiada wiedzę z zakresu budowy systemów operacyjnych, ich roli w zapewnieniu bezpieczeństwa informacji K_W21 Ma w zaawansowanym stopniu wiedzę na temat metod i mechanizmów zapewniających bezpieczeństwo w sieciach komputerowych. Ma wiedzę o metodach uwierzytelniania i szyfrowania, wykrywania i przeciwdziałania atakom. K_U12 Potrafi planować, kontrolować i implementować politykę bezpieczeństwa.	Określanie i kontrolowanie dostępu użytkowników lub systemów do zasobów sieciowych w oparciu o ich prawa dostępu. Techniki uwierzytelniania i autoryzacji do monitorowania tożsamości użytkowników i kierowania ich do przyznanych zasobów sieciowych. Metody uwierzytelniania (m.in. uwierzytelnianie wieloskładnikowe (MFA)). Protokoły szyfrowania. Kontrola dostępu oparta na rolach.	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.E-administracja	K_W22 Zna i rozumie fundamentalne dylematy współczesnej cywilizacji wynikające z postępu technologicznego. K_W23 Zna i rozumie w zaawansowanym stopniu mechanizmy podejmowania decyzji politycznych na poziomie krajowym i międzynarodowym, a także wykorzystania narzędzi elektronicznych w administrowaniu państwem i jednostkami terytorialnymi. K_W24 Zna i rozumie uwarunkowania i formy uczestnictwa w życiu społecznym i politycznym na różnych jego poziomach oraz w cyberprzestrzeni K_U07 Potrafi analizować, wyciągać wniosku, z procesów decyzyjnych na szczeblu krajowym i międzynarodowym, uwzględniając kontekst cyberbezpieczeństwa	Treści programowe realizowane na wykładach: Podstawowe pojęcia i istota e-administracji. E-administracja a e-demokracja. Koncepcje współczesnego governance a e-administracja. Struktura administracji publicznej w Polsce. Podstawy prawne cyfryzacji administracji publicznej w Polsce. Strategie rozwoju e-administracji w Europie. Otwarte dane publiczne: transparentność i odpowiedzialność w administracji publicznej. Współczesne wyzwania administracji elektronicznej i państwa cyfrowego. W ramach laboratorium realizowane są następujące zagadnienia: Rozwój polskiego społeczeństwa informacyjnego. Czynniki rozwoju e-administracji na szczeblu krajowym i lokalnym. BIP jako realizacja zasady dostępu do informacji publicznej. Dokument elektroniczny i podpis elektroniczny. Platforma ePUAP. E-usługi w administracji: sprawy obywatelskie, podatki i obsługa celna oraz działalność gospodarcza i zamówienia publiczne; wymiar sprawiedliwości; rynek pracy i zabezpieczenia społeczne; ochrona zdrowia oraz bezpieczeństwo i powiadamianie ratunkowe. E-administracja a rozwój inteligentnych aglomeracji. E-government na świecie – analiza porównawcza (EDGI). Cyfryzacja administracji publicznej państw europejskich – case studies. Głosowanie elektroniczne.	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.Projektowanie bezpiecznych sieci	K_W05 Ma wiedzę w zaawansowanym stopniu zakresie telekomunikacji, potrzebną do zrozumienia zasad działania współczesnych sieci komputerowych, uwzględniając aspekty bezpieczeństwa. K_W18 Zna w zaawansowanym stopniu metody, techniki i narzędzia związane z przesyłaniem, przechowywaniem i przetwarzaniem danych w systemach informatycznych K_U12 Potrafi planować, kontrolować i implementować politykę bezpieczeństwa.	Metody, techniki i narzędzia związane z przesyłaniem, przechowywaniem i przetwarzaniem danych w systemach informatycznych. Strategie projektowania sieci (m.in. podejście od góry do dołu). Identyfikacja i analiza ryzyka związanego z bezpieczeństwem sieci, w tym rozpoznanie potencjalnych zagrożeń i źródeł ataków. Planowanie, kontrola i implementacja polityki bezpieczeństwa. Architektury zabezpieczeń sieci. Strefy DMZ i ekranowane podsieci. Wdrażanie i konfiguracja systemów zabezpieczających sieci.	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.Bezpieczeństwo infrastruktury sieciowej	K_W04 Ma szczegółową wiedzę w zakresie układów elektroniki, potrzebną do zrozumienia techniki cyfrowej i zasad funkcjonowania współczesnych komputerów. K_W11 Zna metody, techniki i narzędzia, w tym AI, stosowane przy rozwiązywaniu złożonych zadań informatycznych związanych z bezpieczeństwem danych i infrastruktury sieciowej. K_W20 Ma w zaawansowanym stopniu wiedzę na temat algorytmów i protokołów kryptograficznych ich zastosowań w telekomunikacji oraz wiedzę umożliwiającą rozróżnianie metod szyfrowania informacji. K_U26 Potrafi skonfigurować i uruchomić mechanizmy bezpieczeństwa na ruterach i urządzeniach firewall, tunele szyfrowane i mechanizmy IDS.	Istota tunelowania ruchu w sieciach IP – protokół GRE. Framework IPsec, dostępne protokoły i algorytmy realizujące: uwierzytelnienie, integralność weryfikację nadawcy. VPN - zabezpieczanie transmisji danych przy użyciu algorytmów kryptograficznych. Bezpieczne tunele między oddziałami firmy, współpraca z protokołami routingu. Implementacja VPN na urządzeniach różnych dostawców VPN RA jako implementacja bezpiecznego dostępu do infrastruktury firmy przez telepracowników. Firewall CBAC – istota inspekcji ruchu. Zone-Based Firewall – granularne podejście do filtracji ruchu. Implementacja ZBF. Dostęp zdalny poprzez VPN terminowany na Firewallu, analiza rozwiązań, ograniczenia. Implementacje koncepcji DMZ.	Zaliczenie wykładu, test. 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: kolokwium w środowisku symulacyjnym Packet Tracer. Ocena zgodnie z punktami, jak wyżej.
7. Routing w sieciach IP	K_W05 Ma wiedzę w zaawansowanym stopniu zakresie telekomunikacji, potrzebną do zrozumienia zasad działania współczesnych sieci komputerowych, uwzględniając aspekty bezpieczeństwa. K_W18 Zna w zaawansowanym stopniu metody, techniki i narzędzia związane z przesyłaniem,	Routing dynamiczny RIPv2. Routing dynamiczny OSPF. Wieloobszarowy OSPF. Protokół EIGRP. Redystrybucja protokołów. Protokół bramy zewnętrznej BGP, iBGP. Tablice VRF.	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:

	przechowywaniem i przetwarzaniem danych w systemach informatycznych K_U15 Ma umiejętność projektowania sieci komputerowych; potrafi pełnić funkcję administratora sieci komputerowej		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.Bezpieczeństwo informacji i danych osobowych	K_W09 Ma wiedzę w zaawansowanym stopniu zakresie audytu systemów informatycznych oraz zna zagadnienia i metody stosowane w informatyce śledczej K_W20 Ma w zaawansowanym stopniu wiedzę na temat algorytmów i protokołów kryptograficznych ich zastosowań w telekomunikacji oraz wiedzę umożliwiającą rozróżnianie metod szyfrowania informacji. K_W21 Ma w zaawansowanym stopniu wiedzę na temat metod i mechanizmów zapewniających bezpieczeństwo w sieciach komputerowych. Ma wiedzę o metodach uwierzytelniania i szyfrowania, wykrywania i przeciwdziałania atakom.	Podstawy bezpieczeństwa informacji Ochrona danych osobowych – regulacje prawne Zagrożenia dla bezpieczeństwa informacji Metody zabezpieczania danych osobowych i informacji Bezpieczeństwo w sieci i mediach społecznościowych Polityka bezpieczeństwa w organizacji Bezpieczeństwo urządzeń mobilnych i IoT Ataki hakerskie i sposoby obrony Audyt w zakresie danych ochrony danych osobowych Odpowiedzialność prawna i konsekwencje naruszeń Przyszłość ochrony danych i nowych technologii	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.Systemy rozproszone	K_W11 Zna metody, techniki i narzędzia, w tym AI, stosowane przy rozwiązywaniu złożonych zadań informatycznych związanych z bezpieczeństwem danych i infrastruktury sieciowej. K_U11 Ma umiejętność formułowania algorytmów i ich programowania z użyciem przynajmniej jednego z popularnych środowisk programistycznych K_U24 Potrafi wykorzystać zasady bezpieczeństwa związane z pracą w środowisku przemysłowym	Wyzwania związane z bezpieczeństwem systemów rozproszonych: kontrola dostępu, autentykacja użytkowników, ustalenie regionów zaufania oraz zastosowanie kryptografii w przekazywaniu informacji. Zarządzanie kluczami kryptograficznymi i ich dystrybucja w systemie rozproszonym. Wykorzystanie zasad bezpieczeństwa w środowisku przemysłowym i infrastrukturze krytycznej. Identyfikacja i przeciwdziałanie zagrożeniom w systemach rozproszonych.	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.Technologia Firewalli	K_W11 Zna metody, techniki i narzędzia, w tym AI, stosowane przy rozwiązywaniu złożonych zadań informatycznych związanych z bezpieczeństwem danych i infrastruktury sieciowej. K_W18 Zna w zaawansowanym stopniu metody, techniki i narzędzia związane z przesyłaniem, przechowywaniem i przetwarzaniem danych w systemach informatycznych K_U15 Ma umiejętność projektowania sieci komputerowych; potrafi pełnić funkcję administratora sieci komputerowej	Historia i rozwój firewalli oraz wzrost potrzeb filtracji ruchu. Różnica między statyczną filtracją pakietów a inspekcją stanu połączenia (ACL vs SPI). Rola serów proxy w kontroli ruchu aplikacyjnego, filtrowaniu i buforowaniu treści. Warianty implementacji firewalli: sprzętowe, programowe, chmurowe w ujęciu skalowalności oraz integracji. Architektura i klasyfikacja firewalli: filtry pakietów, stanowe, aplikacyjne, NGFE, FWaaS. Modele wdrażania firewalla w organizacji: transparentne, routowane, DMZ. Firewalle w kontekście architektury bezpieczeństwa. Koncepcje raportowania, integracja z systemami SIEM. Automatyzacja reakcji na zagrożenia – systemy IDS/IPS. Koncepcja Zero Trust, polityka minimalizacji uprawnień oraz segmentacji sieci. Testy penetracyjne jako metoda przełamywania ochrony. Typowe błędy konfiguracyjne firewalli, znane metody omijania filtracji poprzez fragmentacje pakietów albo tunelowanie. Monitoring i logowanie zdarzeń w firewallach, polityka logowania, analiza logów oraz integracja z systemami analitycznymi. Trendy i przyszłość technologii firewalli: firewalle jako usługa w chmurze (FWaaS), sztuczna inteligencja i machine learning w ochronie sieci.	Zaliczenie wykładu: test. 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: zadanie praktyczne.
11.Uczenie maszynowe i LLM w cyberbezpieczeństwie	K_W07 Ma w zaawansowanym stopniu, podbudowaną teoretycznie wiedzę ogólną w zakresie języków i paradygmatów programowania, sztucznej inteligencji, baz danych. K_W11 Zna metody, techniki i narzędzia, w tym AI, stosowane przy rozwiązywaniu złożonych zadań informatycznych związanych z bezpieczeństwem danych i infrastruktury sieciowej. K_U13 Potrafi, z wykorzystaniem metod z zakresu przedmiotów ścisłych rozwiązywać problemy w obszarze cyberbezpieczeństwa.	Wykorzystanie algorytmów uczenia maszynowego do identyfikacji anomalii w ruchu sieciowym, wykrywania złośliwego oprogramowania i przewidywania potencjalnym atakom. Rodzaje uczenia maszynowego (nadzorowane i nienadzorowane) oraz ich zastosowania w cyberbezpieczeństwie. Analiza logów systemowych i identyfikacja podejrzanych aktywności. Automatyzacja procesów reagowania na incydenty bezpieczeństwa. Wykorzystywanie modeli językowych (LLM) w celu analizy treści (e-maili, stron internetowych) pod kątem charakterystycznych cech ataków phishingowych Detekcja zagrożeń, redukcja fałszywych alarmów i automatyzacja procesów bezpieczeństwa.	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.
12.Haktywizm i ruchy społeczne w Internecie	K_W13 Zna i rozumie w zaawansowanym stopniu różnorodne wymiary i uwarunkowania bezpieczeństwa, w tym zwłaszcza	Podstawowe definicje i pojęcia związane z ruchami społecznymi; teoria i geneza ruchów społecznych. Haktywizm jako zjawisko polityczne w cywilizacji informacyjnej	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów.

	cyberbezpieczeństwa oraz związane z nimi zagrożenia K_W24 Zna i rozumie uwarunkowania i formy uczestnictwa w życiu społecznym i politycznym na różnych jego poziomach oraz w cyberprzestrzeni K_U27 Potrafi przeprowadzić analizę i ocenę zagrożeń w cyberbezpieczeństwie, uwzględniając różnorodne wymiary bezpieczeństwa. K_K06 Ma świadomość roli społecznej absolwenta uczelni technicznej, a zwłaszcza rozumie potrzebę formułowania i przekazywania społeczeństwu — m.in. poprzez środki masowego przekazu — informacji i opinii dotyczących osiągnięć informatyki i innych aspektów działalności inżyniera-informatyka; podejmuje starania, aby przekazać takie informacje i opinie w sposób powszechnie zrozumiały	Grupa Annonymous: cyberprzestępcy czy rycerze wolności? Cyberpunks, WikiLeaks i widmo kryptograficznej anarchii Nowe ruchy religijne i ich działalność w cyberprzestrzeni Nowe ruchy ekologiczne i ich działalność w cyberprzestrzeni Rewolucja obyczajowa w latach 60. i 70. XX w. Slaktywizm – nowy ruch społeczny w internecie? Ruchy feministyczne Ruch społeczny LGBT* Ruchy sprzeciwiające się równouprawnieniu, m. in incele, femcelki, tradwives Nowe ruchy społeczne w kontekście procesów globalizacji	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.Pozyskiwanie i przetwarzanie danych w systemach IoT	K_W04 Ma szczegółową wiedzę w zakresie układów elektroniki, potrzebną do zrozumienia techniki cyfrowej i zasad funkcjonowania współczesnych komputerów. K_W05 Ma wiedzę w zaawansowanym stopniu zakresie telekomunikacji, potrzebną do zrozumienia zasad działania współczesnych sieci komputerowych, uwzględniając aspekty bezpieczeństwa. K_U08 Potrafi programować układy akwizycji danych i ich dystrybucji K_U09 Potrafi wykorzystać do formułowania i rozwiązywania zadań informatycznych metody analityczne, symulacyjne i eksperymentalne,	Techniki analityczne i symulacyjne do analizy danych IoT. Architektury rozwiązań IoT (m.in. Fog i Edge computing). Bezpieczeństwo danych IoT. Techniki szyfrowania i kontroli dostępu do urządzeń IoT. Bezpieczny przesył danych.	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.
14.Specjalnościowa pracownia dyplomowa	K_W17 Zna i rozumie podstawowe przepisy, pojęcia i zasady z zakresu cyberbezpieczeństwa, ochrony	Realizacja części praktycznej pracy dyplomowej, z uwzględnieniem dokumentacji i opisu tworzonego rozwiązania. Ogólne wymagania do pracy dyplomowej i podstawowe wytyczne. Technika pisania pracy dyplomowej. Formułowania	Kolokwium/egzamin oddzielnie z laboratoriów/ćwiczeń, oddzielnie z wykładu. Zgodnie z planem studiów.

	własności przemysłowej, intelektualnej i prawa autorskiego w sieci. K_U03 potrafi przygotować i przedstawić krótką prezentację poświęconą wynikom realizacji zadania inżynierskiego K_U04 Potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania, także z wykorzystaniem narzędzi informatycznych. K_U05 Posługuje się językiem angielskim w stopniu (B2) wystarczającym do porozumiewania się, a także czytania ze zrozumieniem kart katalogowych, not aplikacyjnych, instrukcji obsługi urządzeń elektronicznych i narzędzi informatycznych oraz podobnych dokumentów K_K06 Ma świadomość roli społecznej absolwenta uczelni technicznej, a zwłaszcza rozumie potrzebę formułowania i przekazywania społeczeństwu — m.in. poprzez środki masowego przekazu — informacji i opinii dotyczących osiągnięć informatyki i innych aspektów działalności inżyniera-informatyka; podejmuje starania, aby przekazać takie informacje i opinie w sposób powszechnie zrozumiały	tematu pracy. Sposoby poszukiwania literatury i źródeł danych do pracy. Napisanie wstępu. Definiowania celu pracy, formułowanie problemów badawczych, wniosków. Opracowanie wyników badań i ich analiza. Prezentacja zrealizowanych etapów pracy dyplomowej.	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.
1.Przetwarzanie równoległe i rozproszone	K_W06 Ma w zaawansowanym stopniu, podbudowaną teoretycznie wiedzę ogólną w zakresie zastosowań wybranych algorytmów ich złożoności obliczeniowej, w szczególności w zakresie cyberbezpieczeństwa. K_U11 Ma umiejętność formułowania algorytmów i ich programowania z użyciem przynajmniej jednego z popularnych środowisk programistycznych K_U13 Potrafi, z wykorzystaniem metod z zakresu przedmiotów ścisłych rozwiązywać problemy w obszarze cyberbezpieczeństwa.	Projektowanie i implementacja algorytmów równoległych i rozproszonych. Metody i techniki pracy równoległej i rozproszonej. Systemy wielowątkowe. Sterowanie systemami równoległymi i rozproszonymi. Sterowanie procesami współbieżnymi.	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.Przetwarzanie danych masowych	K_W18 Zna w zaawansowanym stopniu metody, techniki i narzędzia związane z przesyłaniem, przechowywaniem i przetwarzaniem danych w systemach informatycznych K_U09 Potrafi wykorzystać do formułowania i rozwiązywania zadań informatycznych metody analityczne, symulacyjne i eksperymentalne, K_U11 Ma umiejętność formułowania algorytmów i ich programowania z użyciem przynajmniej jednego z popularnych środowisk programistycznych	Zbieranie, przechowywanie i analiza zbiorów danych. Techniki efektywnego przetwarzania danych w środowiskach rozproszonych. Przetwarzanie strumieniowe. Analiza danych w czasie rzeczywistym. Data mining, analiza tekstowa i wizualizacja danych. Metody ETL (Extract, Transform, Load) wykorzystywane do wypełniania magazynów danych danymi z różnych źródeł. Czyszczenie danych: korekta błędów i nieprawidłowości w danych. Wdrażanie i konfiguracja systemów przetwarzania danych masowych.	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.Rozproszone systemy baz danych	K_W07 Ma w zaawansowanym stopniu, podbudowaną teoretycznie wiedzę ogólną w zakresie języków i paradygmatów programowania, sztucznej inteligencji, baz danych. K_W18 Zna w zaawansowanym stopniu metody, techniki i narzędzia związane z przesyłaniem, przechowywaniem i przetwarzaniem danych w systemach informatycznych K_U19 Ma umiejętność budowy systemów bazodanowych, wykorzystujących przynajmniej jeden z najbardziej popularnych systemów zarządzania bazą danych	1. Architektura systemów baz danych. Systemy scentralizowane a rozproszone. Pojęcie i cechy rozproszonej bazy danych. Rodzaje rozproszonych baz danych. 2. Modele danych. Podejście relacyjne. Obiektowość w bazach danych. Przechowywanie dużych obiektów. Multimedialne bazy danych Semistrukturalne bazy danych. XML - rozszerzalny język znaczników 3. Techniki replikacji i alokacji danych 4. Zarządzanie transakcjami w roproszonych bazach danych 5. Systemy NOSQL i big data.	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.Aplikacje w państwie cyfrowym	K_W23 Zna i rozumie w zaawansowanym stopniu mechanizmy podejmowania decyzji politycznych na poziomie krajowym i międzynarodowym, a także wykorzystania narzędzi elektronicznych w administrowaniu państwem i jednostkami terytorialnymi.	Treści programowe realizowane na wykładach: Podstawy państwa cyfrowego. Architektura systemów cyfrowych w administracji publicznej. E-usługi publiczne. Podstawy prawne cyfryzacji administracji publicznej w Polsce. Otwarte dane publiczne: transparentność i odpowiedzialność w administracji publicznej. Aplikacje w państwie cyfrowym. Bezpieczeństwo i	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

	K_W24 Zna i rozumie uwarunkowania i formy uczestnictwa w życiu społecznym i politycznym na różnych jego poziomach oraz w cyberprzestrzeni K_U07 Potrafi analizować, wyciągać wniosku, z procesów decyzyjnych na szczeblu krajowym i międzynarodowym, uwzględniając kontekst cyberbezpieczeństwa. K_U10 Potrafi – przy formułowaniu i rozwiązywaniu zadań inżynierskich z zakresu cyberbezpieczeństwa – dostrzegać ich aspekty systemowe, społeczne, ekonomiczne i prawne	ochrona danych. Współczesne wyzwania administracji elektronicznej i państwa cyfrowego. W ramach laboratorium realizowane są następujące zagadnienia: Tożsamość cyfrowa. Dokument elektroniczny i podpis elektroniczny. Platforma ePUAP. Aplikacja mObywatel. E-usługi w administracji: sprawy obywatelskie, podatki i obsługa celna oraz działalność gospodarcza i zamówienia publiczne; wymiar sprawiedliwości; rynek pracy i zabezpieczenia społeczne; ochrona zdrowia oraz bezpieczeństwo i powiadamianie ratunkowe. Aplikacje mobilne w inteligentnych aglomeracjach. E-government na świecie – analiza porównawcza (EDGI). Cyfryzacja administracji publicznej państw europejskich – case studies. Głosowanie elektroniczne – przykłady narzędzi.	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.Zabezpieczenia aplikacji webowych	K_W03 Zna i rozumie algorytmy, języki i techniki programowania oraz tworzenia aplikacji. K_W21 Ma w zaawansowanym stopniu wiedzę na temat metod i mechanizmów zapewniających bezpieczeństwo w sieciach komputerowych. Ma wiedzę o metodach uwierzytelniania i szyfrowania, wykrywania i przeciwdziałania atakom K_U25 Potrafi zaplanować oraz przeprowadzić audyt bezpieczeństwa w tym testy penetracyjne.	Zagrożenia dla aplikacji webowych. Ataki XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery) i SQL Injection. Techniki ochrony przed atakami. Walidacja i sanityzację danych wejściowych. Content Security Policy (CSP). Dynamiczne testy bezpieczeństwa aplikacji (DAST) i statyczna analiza kodu (SAST). Systemy zabezpieczające aplikacje webowe (zapory aplikacji internetowych (WAF) i mechanizmy uwierzytelniania wieloskładnikowego (MFA)).	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.Bezpieczeństwo aplikacji mobilnych	K_W05 Ma wiedzę w zaawansowanym stopniu zakresie telekomunikacji, potrzebną do zrozumienia zasad działania współczesnych sieci komputerowych, uwzględniając aspekty bezpieczeństwa K_W20 Ma w zaawansowanym stopniu wiedzę na temat algorytmów i protokołów kryptograficznych ich zastosowań w telekomunikacji oraz wiedzę umożliwiającą rozróżnianie metod szyfrowania informacji.	Treści przedmiotu dotycząc projektowania, implementacji, oraz testowania oprogramowania dla szerokorozumianych urządzeń mobilnych. Ze szczególnym uwzględnieniem zasad, narzędzi i metody z zakresu bezpieczeństwa informacji. Tematyka wykładów i laboratoriów dotyczy: wprowadzenie do środowiska pracy, budowa GUI, oprogramowanie zdarzeń. współpraca z bazami danych, korzystanie z kontrolek zewnętrznych, praca z Sensorami wielkości fizycznych, przetwarzanie danych pomiarowych, komunikacja ze sprzętem pomiarowym i	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

	K_U16 Potrafi zabezpieczyć przesyłane dane przed nieuprawnionym odczytem K_U28 Potrafi ocenić przydatność rutynowych metod i narzędzi informatycznych oraz wybrać i zastosować właściwą metodę i narzędzia do zadań za zakresu cyberbezpieczeństwa	wykonawczym, szyfrowanie danych, praktyczne zastosowania protokołów kryptograficznych, bezpieczna komunikacja poprzez Internet z systemami/aplikacjami zewnętrznymi, realizacja mini-projektów i realizacja testowania oprogramowania, korzystanie z dokumentacji.	90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
7.Audyt bezpieczeństwa aplikacji	K_W09 Ma wiedzę w zaawansowanym stopniu zakresie audytu systemów informatycznych oraz zna zagadnienia i metody stosowane w informatyce śledczej. K_U25 Potrafi zaplanować oraz przeprowadzić audyt bezpieczeństwa w tym testy penetracyjne. K_U27 Potrafi przeprowadzić analizę i ocenę zagrożeń w cyberbezpieczeństwie, uwzględniając różnorodne wymiary bezpieczeństwa. K_U28 Potrafi ocenić przydatność rutynowych metod i narzędzi informatycznych oraz wybrać i zastosować właściwą metodę i narzędzia do zadań za zakresu cyberbezpieczeństwa	Analiza polityk i procedur bezpieczeństwa. Metody audytu (m.in. testy białoskrzynkowe (white-box), czarnoskrzynkowe (black-box) i szaroskrzynkowe (grey-box)). Testy penetracyjne, skanowanie podatności i analiza kodu źródłowego. Identyfikacja podatności na ataki. Planowanie i przeprowadzanie audytu bezpieczeństwa.	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.Ochrona danych osobowych użykowników internetu/ dezinformacja	K_W12 Ma ogólną wiedzę dotyczącą zarządzania bezpieczeństwem informacji zgodnie z normami/regulacjami europejskimi i krajowymi. K_W15 Ma wiedzę nt. patentów, ustawy Prawo autorskie i prawa pokrewne oraz ustawy o ochronie danych osobowych K_U23 Umie dokonać wstępnego przeglądu standardów ochrony informacji, potrafi przedstawić założenia poszczególnych dokumentów normatywnych i prawnych. Umie omówić niezbędne mechanizmy prawne oraz zasady, metody i instrumenty ochrony informacji oraz problem odpowiedzialności za naruszenie prawa chroniącego informację.	Wprowadzenie do ochrony danych osobowych w internecie Podstawy prawne ochrony danych w internecie Polityki prywatności serwisów internetowych Cyberbezpieczeństwo i ochrona danych w urządzeniach mobilnych Metody śledzenia użytkowników w internecie Technologie ochrony danych osobowych Cyberprzestępczość i ochrona danych osobowych Deanonimizacja i analiza danych w internecie Etyka i odpowiedzialność w ochronie danych osobowych AI i ochrona prywatności w sieci Analiza przypadków największych naruszeń prywatności Rola państw w ochronie prywatności i regulacji internetu Społeczne i psychologiczne aspekty ochrony danych Przyszłość ochrony danych osobowych Wprowadzenie do dezinformacji Algorytmy a bańki informacyjne	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.

		Techniki manipulacji w internecie Rola mediów społecznościowych w dezinformacji Psychologia dezinformacji Boty i farmy trolli w internecie Weryfikacja informacji i krytyczne myślenie Studium przypadków znanych kampanii dezinformacyjnych Rola dziennikarstwa w walce z dezinformacją Przyszłość dezinformacji i cyfrowej manipulacji Analiza polityki prywatności serwisów internetowych Symulacja cyberataków i metod wyłudzania danych Praktyczne użycie narzędzi do anonimizacji Ćwiczenia z weryfikacji informacji Analiza treści dezinformacyjnych Projekt: kampania uświadamiająca o ochronie danych osobowych	
9.Zarządzanie tożsamością i dostępem w aplikacjach	K_W10 Ma w zaawansowanym stopniu, wiedzę oraz zna narzędzia i techniki z zakresu testowania poziomu zabezpieczeń, zarówno w obszarze infrastruktury sieciowe jak i na poziomie aplikacji. K_W17 Zna i rozumie podstawowe przepisy, pojęcia i zasady z zakresu cyberbezpieczeństwa, ochrony własności przemysłowej, intelektualnej i prawa autorskiego w sieci. K_U12 Potrafi planować, kontrolować i implementoać politykę bezpieczeństwa. K_U16 Potrafi zabezpieczyć przesyłane dane przed nieuprawnionym odczytem	Identyfikacja, uwierzytelnianie i zarządzanie tożsamościami użytkowników w organizacji. Bazy danych tożsamości. Przyznawanie i kontrola dostępu do aplikacji i danych na podstawie zasad autoryzacji. Kontrola dostępu oparta na rolach. Uwierzytelnianie wieloskładnikowe. Logowanie jednolite (SSO). Strategie zerowego zaufania.	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.Wprowadzenie do AI w cyberbezpieczeństwie	K_W06 Ma w zaawansowanym stopniu, podbudowaną teoretycznie wiedzę ogólną w zakresie zastosowań wybranych algorytmów ich złożoności obliczeniowej, w szczególności w zakresie cyberbezpieczeństwa. K_W11 Zna metody, techniki i narzędzia, w tym AI, stosowane przy rozwiązywaniu złożonych zadań informatycznych związanych z bezpieczeństwem	Metody, techniki i narzędzia AI do identyfikacji i przeciwdziałania cyberzagrożeniom. Zastosowania AI w cyberbezpieczeństwie, Wykrywanie zagrożeń. Automatyzacja reakcji na incydenty. Analiza danych. Możliwości AI w zakresie monitorowania ruchu sieciowego w czasie rzeczywistym, identyfikacji anomalii i podejrzanych zachowań. Wybrane algorytmy AI.	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

	danych i infrastruktury sieciowej. K_U18 Potrafi dobrać i zastosować właściwe metod analizy danych w zadaniu analizy zagrożeń / wykrywania anomalii. K_U27 Potrafi przeprowadzić analizę i ocenę zagrożeń w cyberbezpieczeństwie, uwzględniając różnorodne wymiary bezpieczeństwa.		80-89% - dobry 90-94% - dobry plus 95-100% - bardzo dobry Na laboratorium zaliczenie może być realizowane w formie projektu.
11.Technologie chmurowe i wirtualizacja	K_W19 Posiada wiedzę z zakresu budowy systemów operacyjnych, ich roli w zapewnieniu bezpieczeństwa informacji. K_U14 Ma umiejętność posługiwania się funkcjami systemu operacyjnego K_U20 Potrafi stosować mechanizmy synchronizacji procesów oraz programować komunikację sieciową w trybach klient-serwer i peerto-peer	Usługi IaaS, PaaS i SaaS. Współdzielenie zasobów obliczeniowych, magazynowych i aplikacyjnych. Wykorzystanie i techniki wirtualizacji sprzętu i oprogramowania. Technologie wirtualizacji.	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.
12.Studia nad społeczeństwem i technologią	K_W13 Zna i rozumie w zaawansowanym stopniu różnorodne wymiary i uwarunkowania bezpieczeństwa, w tym zwłaszcza cyberbezpieczeństwa oraz związane z nimi zagrożenia. K_W22 Zna i rozumie fundamentalne dylematy współczesnej cywilizacji wynikające z postępu technologicznego. K_U07 Potrafi analizować, wyciągać wniosku, z procesów decyzyjnych na szczeblu krajowym i międzynarodowym, uwzględniając kontekst cyberbezpieczeństwa. K_U10 Potrafi – przy formułowaniu i rozwiązywaniu zadań inżynierskich z zakresu cyberbezpieczeństwa – dostrzegać ich aspekty systemowe, społeczne,	STS – o relacjach między nauką, techniką i społeczeństwem Uwarunkowania rozwoju technicznego. Technonauka – nurty badań i różne koncepcje poznania Trywializowanie otoczenia i eksternalizacja zjawisk. Ryzyko jako cecha technonauki Technonauka jako element sieci społecznych. Socjologia przedmiotów Posthumanizm i transhumanizm – szansa czy zagrożenie? Neuronauka społeczna – czy istnieje mózg społeczny? O nowym wymiarze badań, jaki biologia może zaoferować humanistyce Współczesna technonauka – cechy, perspektywy i ograniczenia Wprowadzenie do SSnNiT. Kolektyw myślowy i różnice w postrzeganiu Demokracja przyszłości – perspektywy i wyzwania Feminizm a technika Koniec człowieka? O transhumanizmie i ludzkich cyborgach	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.

	ekonomiczne i prawne	Rozwój sztucznej inteligencji – szanse i zagrożenia Jak będą wyglądały miasta przyszłości? O idei smart cities Etyczny wymiar technonauki. Ocena technologii	
13.Zabezpieczenia aplikacji chmurowych	K_W10 Ma w zaawansowanym stopniu, wiedzę oraz zna narzędzia i techniki z zakresu testowania poziomu zabezpieczeń, zarówno w obszarze infrastruktury sieciowe jak i na poziomie aplikacji. K_U12 Potrafi planować, kontrolować i implementować politykę bezpieczeństwa. K_U16 Potrafi zabezpieczyć przesyłane dane przed nieuprawnionym odczytem	Ochrona zasobów wirtualnych. Zagrożenia współdzielenia zasobów. Metody zabezpieczeń aplikacji chmurowych. Audyt i kontrola dostępu w zakresie aplikacji chmurowych.	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.

…… ……..

data i podpis data i podpis

Zastępca ds. Kształcenia Dyrektora Kolegium