Grupa efektów kierunkowych: - (od April 28, 2026) Cyberbezpieczeństwo pierwszego stopnia inżynierskie spec. --- stacjonarne 2026/2027Z -- 2030/2031L

Efekty kierunkowe: Wiedza

CYB1_W01	metody matematyczne, statystyczne i sztucznej inteligencji, stosowane w informatyce, w szczególności w cyberbezpieczeństwie	P6S_WG
CYB1_W02	budowę i zasady działania systemów komputerowych, w tym architekturę komputerów, systemy operacyjne oraz sposoby reprezentacji i przetwarzania informacji	P6S_WG
CYB1_W03	zasady programowania, w tym zasady wytwarzania bezpiecznego kodu i obsługi błędów	P6S_WG
CYB1_W04	w zaawansowanym stopniu zasady działania sieci komputerowych oraz specyfiki bezpieczeństwa środowisk wirtualnych, kontenerowych i chmurowych	P6S_WG
CYB1_W05	architekturę i specyfikę bezpieczeństwa systemów ICT, w tym internetu rzeczy	P6S_WG
CYB1_W06	podatności systemów ICT, w tym aplikacji, systemów operacyjnych i sieci, oraz mechanizmy ich powstawania	P6S_WG
CYB1_W07	w zaawansowanym stopniu techniki i rodzaje ataków, w tym socjotechnicznych, metody analizy zagrożeń, w tym modele opisujące techniki i taktyki atakujących	P6S_WG
CYB1_W08	specyfikę zaawansowanych ataków na urządzenia i systemy ICT	P6S_WG
CYB1_W09	w zaawansowanym stopniu mechanizmy, techniki zabezpieczania systemów ICT, ich metody weryfikacji, z uwzględnieniem cyklu życia systemu	P6S_WG
CYB1_W10	podstawy kryptografii stosowanej oraz mechanizmy uwierzytelniania, autoryzacji i kontroli dostępu	P6S_WG
CYB1_W11	zasady monitorowania bezpieczeństwa systemów ICT oraz podstawy wykrywania i obsługi incydentów	P6S_WG
CYB1_W12	metody audytu bezpieczeństwa systemów ICT, oceny ryzyka oraz zasady zarządzania bezpieczeństwem informacji, w tym standardy i normy stosowane w cyberbezpieczeństwie	P6S_WK
CYB1_W13	regulacje prawne związane z cyberbezpieczeństwem i zarządzaniem bezpieczeństwem informacji, w tym kluczowe akty prawne UE, oraz zasady podejścia GRC	P6S_WK
CYB1_W14	wybrane narzędzia, technologie oraz podejścia stosowane w cyberbezpieczeństwie, w tym ich zastosowania, ograniczenia oraz rolę w zapewnianiu bezpieczeństwa systemów ICT	P6S_WG
CYB1_W15	zasady tworzenia, prowadzenia i utrzymania dokumentacji technicznej oraz bezpieczeństwa systemów ICT, w tym raportów, procedur i polityk	P6S_WG
CYB1_W16	uwarunkowania społeczne, ekonomiczne i środowiskowe projektowania oraz eksploatacji systemów ICT, w tym zasady zrównoważonego rozwoju oraz projektowania uniwersalnego i ich znaczenie dla cyberbezpieczeństwa	P6S_WK
CYB1_W17	zasady security-by-design, privacy-by-design oraz modelowania zagrożeń w cyklu życia systemów ICT	P6S_WG
H1_W01	fundamentalne dylematy współczesnej cywilizacji	P6S_WK

H1_W02	podstawowe ekonomiczne, prawne, etyczne i inne uwarunkowania różnych rodzajów działalności zawodowej, w tym podstawowe pojęcia i zasady z ochrony własności przemysłowej i prawa autorskiego	P6S_WK
H1_W03	podstawowe zasady tworzenia i rozwoju różnych form przedsiębiorczości	P6S_WK

Efekty kierunkowe: Umiejętności

CYB1_U01	stosować metody matematyczne oraz narzędzia statystyczne i informatyczne, w tym elementy sztucznej inteligencji, do zapewnienia bezpieczeństwa w systemach ICT	P6S_UW
CYB1_U02	analizować działanie systemów komputerowych oraz rozwiązywać problemy związane z funkcjonowaniem systemów operacyjnych i zarządzaniem zasobami	P6S_UW
CYB1_U03	tworzyć i analizować programy komputerowe oraz dobierać odpowiednie techniki i narzędzia do rozwiązywania problemów informatycznych	P6S_UW
CYB1_U04	analizować działanie sieci komputerowych oraz identyfikować złożone i nietypowe problemy i zagrożenia w komunikacji sieciowej	P6S_UW
CYB1_U05	zarządzać podstawowymi elementami infrastruktury ICT oraz przeprowadzać podstawową konfigurację bezpiecznych środowisk chmurowych i kontenerowych	P6S_UW
CYB1_U06	identyfikować podatności systemów ICT, stosować techniki testowania zabezpieczeń oraz dobierać odpowiednie mechanizmy ochrony, również w warunkach nie w pełni przewidywalnych	P6S_UW
CYB1_U07	analizować techniki ataków oraz identyfikować i modelować złożone i nietypowe zagrożenia w systemach ICT z wykorzystaniem ustrukturyzowanych metod analizy	P6S_UW
CYB1_U08	stosować mechanizmy kryptograficzne oraz uwierzytelniania, autoryzacji i kontroli dostępu	P6S_UW
CYB1_U09	analizować złożone i nietypowe incydenty bezpieczeństwa oraz wspierać proces wykrywania i reagowania, z uwzględnieniem kontekstu organizacyjnego, również w warunkach nie w pełni przewidywalnych	P6S_UW
CYB1_U10	zabezpieczać cyfrowy materiał dowodowy oraz przeprowadzać podstawową analizę powłamaniową i analizę złośliwego oprogramowania w celu odtworzenia przebiegu incydentu	P6S_UW
CYB1_U11	identyfikować, analizować i oceniać ryzyko związane z bezpieczeństwem informacji i systemów ICT oraz uczestniczyć w procesach audytu i stosować adekwatne środki ochrony zgodnie z wymaganiami prawnymi i organizacyjnymi oraz z uwzględnieniem aspektów etycznych	P6S_UW
CYB1_U12	dobierać i wykorzystywać narzędzia oraz techniki z zakresu cyberbezpieczeństwa do analizy, wykrywania i ograniczania złożonych i nietypowych zagrożeń, również w warunkach nie w pełni przewidywalnych	P6S_UO
CYB1_U13	projektować architekturę bezpiecznych systemów ICT oraz integrować mechanizmy bezpieczeństwa w cyklu ich projektowania i wdrażania, a także dokonywać krytycznej analizy sposobu funkcjonowania oraz oceny proponowanych i istniejących rozwiązań technicznych	P6S_UW
CYB1_U14	wykorzystywać techniki pozyskiwania, krytycznej analizy i syntezy informacji, w tym z otwartych źródeł (OSINT), do identyfikowania zagrożeń oraz potencjalnych wektorów ataku	P6S_UW
CYB1_U15	komunikować się i debatować w języku polskim i obcym (na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego), zarówno z informatykami jak i osobami bez wiedzy informatycznej, przy użyciu najnowszych technik informacyjno-komunikacyjnych, w ramach realizacji projektów informatycznych, przy użyciu specjalistycznej terminologii	P6S_UK
CYB1_U16	prezentować, korzystając z najnowszych technik informacyjno-komunikacyjnych, zagadnienia techniczne z dziedziny informatyki i jej zastosowań w sposób zrozumiały dla osób nieposiadających wykształcenia inżynierskiego	P6S_UK

CYB1_U17	samodzielnie planować i realizować własne uczenie się przez całe życie w celu podnoszenia swoich kompetencji zawodowych	P6S_UU
CYB1_U18	rozwiązywać praktyczne zadania inżynierskie z zakresu informatyki, w tym związane z utrzymaniem systemów ICT, wykorzystując standardy, normy oraz doświadczenie zdobyte w środowisku zawodowym	P6S_UW
CYB1_U19	dokumentować przebieg działań związanych z bezpieczeństwem systemów ICT, w tym sporządzać raporty z incydentów, audytów i testów bezpieczeństwa oraz tworzyć i aktualizować procedury i dokumentację techniczną zgodnie ze standardami, z zachowaniem wymagań dotyczących integralności i łańcucha dowodowego tam, gdzie jest to wymagane	P6S_UW
CYB1_U20	uwzględniać uwarunkowania środowiskowe, ekonomiczne i społeczne oraz aspekty etyczne w projektowaniu, wdrażaniu i eksploatacji systemów ICT oraz dokonywać wstępnej oceny ekonomicznej proponowanych rozwiązań, w tym dobierać rozwiązania sprzyjające efektywnemu i odpowiedzialnemu wykorzystaniu zasobów	P6S_UW
CYB1_U21	projektować i oceniać rozwiązania informatyczne z uwzględnieniem zasad projektowania uniwersalnego, dostrzegając i uwzględniając aspekty etyczne i społeczne	P6S_UW
H1_U01	brać udział w debacie przedstawiając i oceniając różne stanowisk	P6S_UK
H1_U02	planować i organizować pracę indywidualną i w zespole, współdziałać w ramach prac zespołowych	P6S_UO

Efekty kierunkowe: Kompetencje społeczne

CYB1_K01	krytycznej oceny posiadanej wiedzy i jej źródeł, rozpoznawania ograniczeń własnych kompetencji, inicjowania i podejmowania działań na rzecz ciągłego aktualizowania wiedzy w tym dynamicznie rozwijającym się obszarze, a także do zasięgania opinii ekspertów w sytuacjach przekraczających jego samodzielne możliwości rozwiązania problemu	P6S_KK
CYB1_K02	zachowania w sposób profesjonalny, przyjmowania odpowiedzialności za własną pracę, dbałości o dorobek i tradycję zawodu inżyniera oraz poszanowania różnorodności poglądów	P6S_KR
CYB1_K03	działania w sytuacjach wymagających szybkiego podejmowania decyzji, w tym pod presją czasu i w warunkach stresu, typowych dla obsługi incydentów bezpieczeństwa, testów penetracyjnych oraz sytuacji kryzysowych w systemach ICT	P6S_KK
CYB1_K04	współpracy z interesariuszami organizacyjnymi, prawnymi i technicznymi w zakresie identyfikowania i ograniczania ryzyk cyberbezpieczeństwa, z poszanowaniem różnorodności kompetencji	P6S_KO
H1_K01	przestrzegania zasad etyki zawodowej i wymagania tego od innych	P6S_KR
H1_K02	wypełniania zobowiązań społecznych, działania na rzecz środowiska społecznego	P6S_KO
H1_K03	myślenia i działania w sposób przedsiębiorczy, propagowania i wdrażania polityki zrównoważonego rozwoju	P6S_KO