Opis poszczególnych przedmiotów lub grup przedmiotów dla studiów podyplomowych pn. *Inżynieria Cyberbezpieczeństwa* prowadzonych na Wydziale Elektroniki i Technik Informacyjnych

1.	Nazwa przedmiotu lub grupy przedmiotów	Cyberbezpieczeństwo
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	stacjonarny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotów z przypisaną liczbą godzin	wykłady – 14 godz. zajęcia komputerowe – 24 godz.
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	

WYKŁADY

Budowa bezpieczeństwa w cyberprzestrzeni – (6h)

Cyberprzestrzeń; sieci, systemy i użytkownicy; systemy cyberfizyczne; współczesne sieci i systemy; wprowadzenie do dziedziny cyberbezpieczeństwa; pojęcia fundamentalne dla dziedziny – CIA (Confidentiality, Integrity, Availability); podatność, zagrożenie, skutek, ryzyko; budowa wielowarstwowego cyberbezpieczeństwa i programy; model dojrzałości i adekwatności środków cyberbezpieczeństwa; analiza ryzyka cyberzagrożeń i powiązanie z różnymi działaniami na rzecz podnoszenia cyberbezpieczeństwa; przegląd frameworków: NIST, ISO, CIS; problemy etyczne, prawne i ekonomiczne w cyberbezpieczeństwie; cyberatak; ataki na użytkowników; współczesny malware; case study różnych cyberataków i złośliwego oprogramowania; modelowanie cyberzagrożeń i ocena ryzyka; metodyki Cyber Kill Chain i MITRE ATT&CK; metody detekcji i analizy złośliwego oprogramowania; botnety i kanały Command&Control;

Poufność, integralność i dostępność (8h)

Ochrona poufności i integralności danych: kryptografia asymetryczna i symetryczna; kryptografia klucza publicznego; funkcje skrótu; certyfikaty; podpis cyfrowy; mechanizmy kontroli integralności danych; uwierzytelnienie i autoryzacja; ochrona dostępności danych: backupy, redundancja; strategie ochrony danych: klasyfikacja, dane wrażliwe; przegląd mechanizmów wbudowanych w systemy sieciowe, komputerowe, operacyjne oraz aplikacje i bazy danych pod kątem bezpieczeństwa danych;

ZAJĘCIA KOMPUTEROWE

Zajęcia wstępne (6h)

System operacyjny Windows i Linux; wirtualizacja i maszyny wirtualne; serwery i komunikacja zdalna – SSH; obsługa terminala Windows (PowerShell) i Linux (bash); komendy i działania z poziomu terminala; dystrybucje Linuxa dla cyberbezpieczeństwa: Kali Linux, Parrot, SIFT, Security Onion; Poznawanie pierwszych narzędzi: narzędzia wybranych dystrybucji Linuxa; Wireshark; CyberChef;

Wprowadzenie do programowania w języku Python (6h)

Środowisko pracy w języku Python: interpreter, środowisko wirtualne, instalowanie paczek; narzędzia do pracy z językiem Python: IDE (PyCharm), VSCode, JupyterLab / Jupyter Notebooks; wprowadzenie do języka Python; ładowanie modułów; zmienne; funkcje; liczby i operacje; pętle, wyrażenia logiczne; struktury danych: zbiór, lista, słownik; praca na plikach; manipulowanie łańcuchami znaków; strukturyzacja kodu Pythona: skrypty, moduły;

Zastosowanie Python do zadań IT, sieciowych i cyberbezpieczeństwa (6h)

Komunikacja sieciowa – CP, UDP, HTTP (REST API); obsługa protokołów zdalnego dostępu – SSH; Biblioteka scapy – obsługa ruchu sieciowego i ręczne generowanie pakietów; Moduł re – wyrażenia regularne;

Mechanizmy bezpieczeństwa danych (6h)

Konfiguracja infrastruktury klucza publicznego dla referencyjnej web aplikacji;
Konfiguracja mechanizmu kontroli dostępu (uwierzytelnienie, autoryzacja) – wybrane case study;

6.	Formy weryfikacji i oceny osiąganych efektów uczenia się (warunki i sposób zaliczenia)

kolokwium na zakończenie semestru: CYB_W01, CYB_W02, CYB_W03, CYB_W04, CYB_W05, CYB_W06, CYB_K01, CYB_K03, CYB_K04
zajęcia komputerowe (aktywność, sprawozdanie): CYB_U01, CYB_U02, CYB_U03, CYB_U04, CYB_U05, CYB_U06, CYB_U07, CYB_08, CYB_K01, CYB_K04
dyskusja na zajęciach: CYB_K01, CYB_K02, CYB_K04, CYB_U07, CYB_U08

7. Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych

Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Opis efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Wiedza		
CYB_W01	Ma wiedzę dotyczącą podstawowych pojęć z zakresu cyberbezpieczeństwa.	ICYB_W01
CYB_W02	Ma wiedzę z zakresu mechanizmów stosowanych w złośliwym oprogramowaniu	ICYB_W02
CYB_W03	Ma podstawową wiedzę dotyczącą środków technicznych zapewniających cyberbezpieczeństwo.	ICYB_W04
CYB_W04	Ma podstawową wiedzę z zakresu modelowania zagrożeń.	ICYB_W02
CYB_W05	ma podstawową wiedzę z zakresu metod ochrony danych, kryptografii i protokołów kryptograficznych.	ICYB_W04
CYB_W06	Ma podstawową wiedzę o języku programowania Python i możliwościach jego wykorzystania w rozwiązaniach dotyczących cyberbezpieczeństwa.	ICYB_W04
Umiejętności		
CYB_U01	Potrafi krytycznie analizować dostępną literaturę w zakresie podstaw cyberbezpieczeństwa	ICYB_U01
CYB_U02	Potrafi sformułować problemy dotyczące cyberbezpieczeństwa przy użyciu właściwej terminologi	ICYB_U07
CYB_U03	Potrafi opisać współczesne cyberzagrożenia posługując się wybranymi metodykami ich modelowania i w odniesieniu do podstawowych pojęć z zakresu cyberbezpieczeństwa.	ICYB_U02
CYB_U04	Potrafi tworzyć podstawowe skrypty narzędziowe w języku Python na podstawie zadanego problemu (specyfikacji), w szczególności dla zadań cyberbezpieczeństwa.	ICYB_U04
CYB_U05	Potrafi zaprojektować bezpieczną usługę sieciową obejmującą przechowywanie i przesyłanie danych oraz kontrolę dostępu.	ICYB_U04
CYB_U06	Potrafi zaprojektować i zrealizować proste rozwiązanie inżynierskie z zakresu bezpieczeństwa danych.	ICYB_U04
CYB_U07	Potrafi dokonać doboru i oceny adekwatności różnych mechanizmów cyberbezpieczeństwa w zależności	ICYB_U04

	od postawionych wymagań i następnie je zastosować.	
CYB_U08	Potrafi aktywnie uczestniczyć w dyskusji na tematy związane z cyberbezpieczeństwem, używając poprawnej terminologii i formułując trafne argumenty.	ICYB_U07
Kompetencje społeczne		
CYB_K01	Ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy.	ICYB_K03
CYB_K02	Ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności w zakresie inżynierii cyberbezpieczeństwa.	ICYB_K02
CYB_K03	Ma świadomość etyki cyberbezpieczeństwa, w tym odnajdowania podatności i obsługi incydentów cyberbezpieczeństwa.	ICYB_K01
CYB_K04	Rozumie konieczność wykorzystywania sprawdzonych metod i technologii zapewniania cyberbezpieczeństwa.	ICYB_K01

1.	Nazwa przedmiotu lub grupy przedmiotów	Bezpieczeństwo sieci
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	stacjonarny i zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4 (w tym do 2 – zdalnie)
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotów z przypisaną liczbą godzin	warsztaty – 20 godz. zajęcia komputerowe – 12 godz.
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	

ZAJĘCIA WARSZTATOWE

Wprowadzenie do komunikacji (2h)

Podstawy i taksonomie komunikacji. Modele warstwowe ISO/OSI i TCP/IP. Zadania warstw. Adresacja, enkapsulacja, multipleksacja.

Wprowadzenie do bezpieczeństwa komunikacji (2h)

Bezpieczeństwo komputerowe a bezpieczeństwo komunikacji. Podstawowe zagrożenia bezpieczeństwa. Pojęcia, mechanizmy i protokoły bezpieczeństwa. Źródła zagrożeń/podatności/luk. Rodzaje ataków sieciowych, ataki aktywne/pasywne, narzędzia i techniki. Bezpieczeństwo w relacji do modelu ISO/OSI. Charakterystyka głównych zagrożeń, np. skanowania, malware, sieci botnet (w tym IoT), ataki (D)DoS, ataki na DNS, spoofing, spam, phishing. Luki w TCP/IP. Fingerprinting. Prywatność. Ukrywanie informacji w ruchu sieciowym – metody, detekcja, przeciwdziałanie. Wpływ zagrożeń na polityki bezpieczeństwa.

Bezpieczeństwo w mediach bezprzewodowych (2h)

Bezpieczeństwo warstwy fizycznej. Modulacje cyfrowe. Techniki szerokopasmowe. Pseudolosowość, CDMA. MIMO, inteligentne anteny. Podstawowe zagrożenia w ujęciu użytkownika końcowego. Ataki na sieci bezprzewodowe. Błędy konfiguracji węzłów bezprzewodowych.

Systemy ochrony komunikacji (2h)

Zapory ogniowe, filtrowanie ingress/egress, rodzaje zapór ogniowych: filtry pakietów (pasywne/aktywne), bramy na poziomie sesji i aplikacji (proxy nieprzezroczyste/przezroczyste). Filtry. NAT/PAT. NGFW, WAF. NIDS/NIPS, komponenty NID/PS według Common Intrusion Detection Framework. Przykłady rozwiązań, np. Snort, Suricata, Bro. Systemy honeypot i honeynet.

Protokoły zabezpieczeń komunikacji: SSL/TLS/IPSec/VPN (2h)

Rola VPN w bezpieczeństwie i zapewnianiu usług poufności i integralności transmisji danych, a także uwierzytelnienia (serwera, klienta). IPSec. SSL/TLS.

Protokoły kontroli dostępu i uwierzytelnienia (2 h)

Sposoby realizacji usług kontroli dostępu i uwierzytelnienia, rola AAA, najważniejsze protokoły (RADIUS, TACACS+, DIAMETER). Uwierzytelnienie sieciowe (Kerberos), mobilne (OAuth, OpenID).

Bezpieczeństwo komunikacji w sieciach rozległych (2h)

Bezpieczeństwo routingu (RIP, OSPF, BGP). DNS, ataki (D)DoS.

Bezpieczeństwo komunikacji w sieciach lokalnych (2h)

MAC address spoofing, MAC address table overflow, ARP, DHCP, STP, VLAN, WLAN. Bezpieczeństwo urządzeń końcowych oraz bezpieczeństwo IoT.

Zabezpieczanie usług (4 h)

Sposoby zabezpieczania wybranych usług na przykładzie np. VoIP, PGP, S/MIME, WLAN. Zabezpieczanie aplikacji WWW, sesje HTTP, HTTP cookies, ataki SQL Injection (SQLi), Cross-Site Scripting, Cross-Site Request Forgery itp. Testowanie bezpieczeństwa aplikacji WWW. WAF.

ZAJĘCIA KOMPUTEROWE

L1 – Wprowadzenie do konfiguracji urządzeń sieciowych. Zapory ogniowe. (4h)

Wprowadzenie do Cisco IOS. Konfiguracja list ACL.

L2 – AAA i IDS. VPN. (4h)

Centralne uwierzytelnianie (RADIUS). IPSec VPN.

L3 – Zabezpieczanie sieci lokalnych (4h)

Port security, STP, DHCP, ARP.

6.	Formy weryfikacji i oceny osiąganych efektów uczenia się (warunki i sposób zaliczenia)
kolokwium na zakończenie semestru: BESI_W01, BESI_W02, BESI_W03, BESI_W04, BESI_W05, BESI_W06, BESI_W07, BESI_W08, BESI_W09 zajęcia warsztatowe (aktywność): BESI_U01, BESI_U02, BESI_U03, BESI_U07 zajęcia komputerowe (aktywność, sprawozdanie): BESI_U04, BESI_U05, BESI_U06, BESI_U08 dyskusja na zajęciach warsztatowych i komputerowych: BESI_U09, BESI_K01, BESI_K02	

7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych	
Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Opis efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Wiedza		
BESI_W01	Ma wiedzę dotyczącą podstawowych pojęć z zakresu bezpieczeństwa komunikacji w sieci teleinformatycznej.	ICYB_W01
BESI_W02	Ma podstawową wiedzę o głównych zagrożeniach w sieciach teleinformatycznych.	ICYB_W02
BESI_W03	Ma podstawową wiedzę z zakresu sposobu funkcjonowania systemów bezpieczeństwa sieciowego.	ICYB_W04
BESI_W04	Ma podstawową wiedzę z zakresu sposobu funkcjonowania protokołów bezpieczeństwa sieciowego.	ICYB_W04
BESI_W05	Ma wiedzę z zakresu analizy ruchu sieciowego pod kątem incydentów bezpieczeństwa.	ICYB_W03
BESI_W06	Ma podstawową wiedzę dotyczącą środków technicznych zapewniających bezpieczeństwo komunikacji w sieci.	ICYB_W04
BESI_W07	Ma podstawową wiedzę z zakresu zapewniania bezpieczeństwa w sieciach różnej skali (LAN, sieć operatora).	ICYB_W04
BESI_W08	Ma wiedzę z zakresu zapewniania prywatności w sieciach teleinformatycznych.	ICYB_W04
BESI_W09	Ma podstawową wiedzę z zakresu ukrywania informacji w ruchu sieciowym.	ICYB_W02
Umiejętności		
BESI_U01	Potrafi krytycznie analizować dostępne materiały źródłowe z zakresu bezpieczeństwa komunikacji w sieci.	ICYB_U01, ICYB_U09
BESI_U02	Potrafi w podstawowym zakresie definiować zagrożenia występujące w sieci teleinformatycznej.	ICYB_U02
BESI_U03	Potrafi stosować środki techniczne zapewniające bezpieczeństwo komunikacji w sieci.	ICYB_U04
BESI_U04	Potrafi w podstawowym zakresie wykorzystywać systemy i protokoły zabezpieczeń do zapewniania bezpieczeństwa w sieci teleinformatycznej.	ICYB_U04
BESI_U05	Potrafi przeprowadzić krytyczną ocenę bezpieczeństwa przykładowej sieci teleinformatycznej.	ICYB_U02

BESI_U06	Potrafi wykorzystywać podstawowe narzędzia do testowania zabezpieczeń sieci teleinformatycznych.	ICYB_U02
BESI_U07	Potrafi ocenić funkcjonowanie sieci w przypadku wystąpienia zagrożeń, przewidzieć ich skutki oraz zaproponować sposoby zabezpieczenia sieci.	ICYB_U02, ICYB_U04
BESI_U08	Potrafi stworzyć dokumentację przeprowadzonych badań, zgodnie z założoną metodyką i wymaganiami	ICYB_U05
BESI_U09	Potrafi aktywnie uczestniczyć w dyskusji na tematy związane z cyberbezpieczeństwem, w szczególności związane z bezpieczeństwem komunikacji w sieci, używając poprawnej terminologii i formułując trafne argumenty.	ICYB_U07
Kompetencje społeczne		
BESI_K01	Ma świadomość konieczności ciągłego uczenia się - doskonalenia swoich umiejętności i podnoszenia kompetencji w zakresie zapewniania bezpieczeństwa komunikacji.	ICYB_K02
BESI_K02	Ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy.	ICYB_K03

1.	Nazwa przedmiotu lub grupy przedmiotów	Bezpieczeństwo hostów i urządzeń końcowych
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	stacjonarny i zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4 (w tym do 2 – zdalnie)
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotów z przypisaną liczbą godzin	zajęcia komputerowe – 28 godz.
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	

ZAJĘCIA KOMPUTEROWE

Podstawy administrowania bezpieczeństwem systemów i środowisk Linux (6h)

Uwierzytelnienie. Model uprawnienń. Systemy plików. Limity dyskowe. Logowanie. Podstawowa i bezpieczna konfiguracja systemu – serwerowego i dla użytkownika końcowego. Terminal i skrypty w języku Bash w zarządzaniu systemami Linux.

Zaawansowane aspekty bezpieczeństwa systemów środowisk Linux (6h)

Zapora ogniowa (iptables). DAC vs. MAC. SELinux. LDAP. Logowanie i monitorowanie systemów Linux. Tworzenie kopii zapasowych i odtwarzanie z nich systemów.. Zarządzanie aktualizacjami systemów. Podatności systemów Linux.

Podstawy administrowania bezpieczeństwem systemów i środowisk Windows (6h)

Instalacja systemu Windows i Windows Server; podstawowa konfiguracja systemu Windows dla użytkownika, w szczególności w kontekście polityk bezpieczeństwa; podstawowa konfiguracja systemu Windows Server; PowerShell i podstawowe działania administracyjne w środowisku Windows, w tym pod kątem bezpieczeństwa; usługa aktualizacji i dystrybucji oprogramowania; zarządzanie flotą urządzeń Windows; wprowadzenie do Active Directory.

Zaawansowane aspekty bezpieczeństwa systemów środowisk Windows (8h)

Active Directory i zastosowanie do działań administracyjnych w zakresie bezpieczeństwa; logi systemu Windows – konfiguracja, kolekcjonowanie; przegląd wybranych rozwiązań Microsoft dla IT i bezpieczeństwa środowisk Windows. Oprogramowanie antywirusowe i systemy Endpoint Detection & Response. Tworzenie kopii zapasowych i odtwarzanie z nich systemów. Podatności systemów Windows.

6.	Formy weryfikacji i oceny osiąganych efektów uczenia się (warunki i sposób zaliczenia)

Kolokwium na zakończenie semestru: BHUK_W01, BHUK_W02, BHUK_W03, BHUK_W04, BHUK_W05, BHUK_W06, BHUK_W07, BHUK_W08, BHUK_U08, BHUK_K01
zajęcia komputerowe (aktywność, sprawozdanie): BHUK_U01, BHUK_U02, BHUK_U03, BHUK_U04, BHUK_U05, BHUK_U06, BHUK_U07, BHUK_U08
dyskusja na zajęciach: BHUK_U07, BHUK_U08, BHUK_K01, BHUK_K02, BHUK_K03

7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych

Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Opis efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
	Wiedza	
BHUK_W01	Ma wiedzę dotyczącą podstawowych pojęć z zakresu bezpieczeństwa systemów informacyjnych i oprogramowania.	ICYB_W01
BHUK_W02	Pa wiedzę dotyczącą podstawowych mechanizmów bezpieczeństwa w systemach operacyjnych Windows i Linux.	ICYB_W04

BHUK_W03	Ma podstawową wiedzę dotyczącą administrowania mechanizmami bezpieczeństwa w systemach operacyjnych Windows i Linux.	ICYB_W04
BHUK_W04	Ma wiedzę dotyczącą mechanizmów kontroli dostępu stosowaną w systemach operacyjnych i środowiskach teleinformatycznych.	ICYB_W04
BHUK_W05	Ma podstawową wiedzę z zakresu modelowania zagrożeń systemów informacyjnych i oprogramowania.	ICYB_W02
BHUK_W06	Ma podstawową wiedzę metodyki procesu zarządzania bezpieczeństwem systemów informacyjnych i oprogramowania.	ICYB_W04
BHUK_W07	Ma podstawową wiedzę z zakresu logowania, monitorowania i wykrywania cyberzagrożeń w systemach operacyjnych.	ICYB_W04
BHUK_W08	Ma podstawową wiedzę w zakresie tworzenia kopii zapasowych i odtwarzania z nich środowisk komputerowych.	ICYB_W04
Umiejętności		
BHUK_U01	Potrafi przygotować komputery i serwery z systemem Windows oraz Linux, uwzględniając podstawowe mechanizmy bezpieczeństwa.	ICYB_U04
BHUK_U02	Potrafi wykonywać czynności administracyjne w systemach Windows i Linux pod kątem bezpieczeństwa.	ICYB_U04
BHUK_U03	Potrafi skonfigurować podstawowe narzędzie katalogowe (Active Directory, LDAP) i wykorzystać je do scentralizowanego zarządzania bezpieczną konfiguracją systemów informacyjnych.	ICYB_U04
BHUK_U04	Potrafi skonfigurować podstawowe mechanizmy bezpieczeństwa w systemach operacyjnych Windows i Linux, m.in. kontrolę dostępu logowanie zdarzeń, antywirus, tworzenie kopii zapasowych.	ICYB_U04
BHUK_U05	Potrafi skonfigurować mechanizmy ochrony systemów operacyjnych na styku z sieciami teleinformatycznymi.	ICYB_U04
BHUK_U06	Potrafi stworzyć proste skrypty PowerShell (Windows) i Bash (Linux), automatyzujące konfigurację i zarządzanie	ICYB_U04

	bezpieczeństwem systemów operacyjnych.	
BHUK_U07	Potrafi aktywnie uczestniczyć w dyskusji na tematy związane z cyberbezpieczeństwem, w szczególności związane z bezpieczeństwem systemów operacyjnych i oprogramowania, używając poprawnej terminologii i formułując trafne argumenty.	ICYB_U07
BHUK_U08	Potrafi krytycznie analizować materiały źródłowe dotyczące systemów operacyjnych, administrowania nimi i ich bezpieczeństwem.	ICYB_U01, ICYB_U09
Kompetencje społeczne		
BHUK_K01	Ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy.	ICYB_K03
BHUK_K02	Ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności w zakresie inżynierii cyberbezpieczeństwa.	ICYB_K02
BHUK_K03	Rozumie konieczność wykorzystywania sprawdzonych metod i technologii zapewniania cyberbezpieczeństwa.	ICYB_K01

1.	Nazwa przedmiotu lub grupy przedmiotów	Ofensywne testowanie bezpieczeństwa
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	stacjonarny i zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4 (w tym do 2 – zdalnie)
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotów z przypisaną liczbą godzin	zajęcia komputerowe – 38 godz.
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	

ZAJĘCIA KOMPUTEROWE

Wstęp do testów penetracyjnych (6h)

Testy penetracyjne – wprowadzenie, planowanie testów – ustalenie zakresu i umowa (m.in. cele i obiekty testów); bezpieczne środowisko operacyjne i narzędzia wspierające gromadzenie danych podczas testów penetracyjnych; rekonesans (OSINT, rekonesans sieciowy); skanowanie sieciowe – część 1.

Skanowanie i wykorzystywanie podatności systemów (6h)

Skanowanie sieciowe – część 2 – enumeracja sieci i usług, automatyczne skanery podatności
Wykorzystywanie podatności – automatyzacja (na przykładzie Metasploit Framework); Ataki socjotechniczne.

Ataki na web aplikacje (6h)

Wykorzystywanie podatności - ataki na aplikacje WEB, ataki (D)DoS.

Zaawansowane techniki testowania systemów (6h)

Ataki na hasła (bruteforce, ataki słownikowe, tęczowe tablice); wykorzystywanie podatności – omijanie programów antywirusowych/obfuskacja; eskalacja uprawnień w systemach Windows i Linux; lateral movement i utrzymanie dostępu (w tym pivoting).

Eksploitacja systemów (6h)

Wykorzystywanie podatności – atak typu Buffer Overflow (pisanie własnego exploita)l Wykorzystywanie podatności – wyszukiwanie i modyfikacja istniejących exploitów – przykłady; Dokumentowanie testów penetracyjnych i sposoby dalszego rozwijania umiejętności.

Kompleksowe testy bezpieczeństwa (8h)

Testy kompleksowe - przeprowadzenie kompleksowych testów bezpieczeństwa w środowisku symulującym rzeczywistą infrastrukturę.

6.	Formy weryfikacji i oceny osiąganych efektów uczenia się (warunki i sposób zaliczenia)

Kolokwium na zakończenie semestru: OTEB_W01, OTEB_W02, OTEB_W03, OTEB_W04, OTEB_W05, OTEB_W06, OTEB_W07, OTEB_W08, OTEB_W09, OTEB_U09, OTEB_K01
zajęcia komputerowe (aktywność, sprawozdanie): OTEB_U01, OTEB_U02, OTEB_U03, OTEB_U04, OTEB_U05, OTEB_U06, OTEB_U07, OTEB_U08, OTEB_U09, OTEB_K01
dyskusja na zajęciach: OTEB_U08, OTEB_U09, OTEB_K02, OTEB_K03

7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych

Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Opis efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Wiedza		
OTEB_W01	Ma podstawową wiedzę z zakresu testów penetracyjnych i cyberbezpieczeństwa ofensywnego.	ICYB_W03
OTEB_W02	Ma podstawową wiedzę z zakresu narzędzi i technik testowania cyberbezpieczeństwa.	ICYB_W03
OTEB_W03	Ma podstawową wiedzę z zakresu modelowania zagrożeń systemów i oprogramowania.	ICYB_W02
OTEB_W04	Ma wiedzę dotyczącą podstawowych pojęć z zakresu bezpieczeństwa	ICYB_W01

	systemów informacyjnych, sieci i oprogramowania.	
OTEB_W05	Ma wiedzę dotyczącą podstawowych typów podatności występujących w systemach informacyjnych, sieciach i oprogramowaniu.	ICYB_W03
OTEB_W06	Ma wiedzę dotyczącą metodyk oceny podatności i szacowania na jej podstawie ryzyka.	ICYB_W02, ICYB_W03
OTEB_W07	Ma wiedzę o procesie zarządzania podatnościami w środowiskach teleinformatycznych.	ICYB_W07
OTEB_W08	Ma wiedzę o rozwoju kontekstu testowania bezpieczeństwa w organizacjach pod kątem budowy wielowymiarowej cyberodporności.	ICYB_W07
OTEB_W09	Ma wiedzę dotyczącą podstawowych technik atakowania użytkowników systemów teleinformatycznych (socjotechniki).	ICYB_W06
Umiejętności		
OTEB_U01	Potrafi przygotować środowisko pracy pentestera.	ICYB_U02
OTEB_U02	Potrafi wykorzystywać podstawowe narzędzia do realizacji testów penetracyjnych.	ICYB_U02
OTEB_U03	Potrafi przeprowadzić podstawowy test penetracyjny zgodnie z przyjętą metodyką.	ICYB_U02
OTEB_U04	Potrafi stworzyć dokumentację testów penetracyjnych zgodnie z przyjętą metodyką i wymaganiami.	ICYB_U05
OTEB_U05	Potrafi wykonać podstawowe sekwencje czynności testujących bezpieczeństwo systemów informacyjnych, sieci i oprogramowania.	ICYB_U02
OTEB_U06	Potrafi stosować techniki ofensywne w celu testowania różnych aspektów cyberbezpieczeństwa.	ICYB_U02
OTEB_U07	Potrafi dokonać oceny wykrytej podatności i oszacować na jej podstawie ryzyko.	ICYB_U02
OTEB_U08	Potrafi aktywnie uczestniczyć w dyskusji na tematy związane z cyberbezpieczeństwem, w szczególności związane z ofensywnym testowaniem bezpieczeństwa, używając poprawnej terminologii i formułując trafne argumenty.	ICYB_U07
OTEB_U09	Potrafi krytycznie analizować materiały źródłowe dotyczące cyberbezpieczeństwa ofensywnego.	ICYB_U01, ICYB_U09
Kompetencje społeczne		
OTEB_K01	Ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy.	ICYB_K03

OTEB_K02	Ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności w zakresie inżynierii cyberbezpieczeństwa.	ICYB_K02
OTEB_K03	Ma świadomość etyki cyberbezpieczeństwa, w tym odnajdowania podatności i obsługi incydentów cyberbezpieczeństwa.	ICYB_K01

1.	Nazwa przedmiotu lub grupy przedmiotów	Analiza cyberzagrożeń i incydentów
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	stacjonarny i zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4 (w tym do 2 – zdalnie)
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotów z przypisaną liczbą godzin	wykłady – 14 godz. zajęcia komputerowe – 12 godz.
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	

WYKŁADY

Wstęp do analizy cyberzagrożeń i incydentów (6h)

Współczesne zagadnienia analizy zagrożeń w cyberprzestrzeni, analiz powłamaniowych i zarządzania incydentami; metodyki modelowania cyberzagrożeń w zastosowaniu analitycznym; wstęp do budowy systemów detekcji cyberzagrożeń; przegląd typów systemów detekcji i reagowania - NIDS, HIDS/EDR/XDR, SIEM, SOAR, platformy DFIR; wstęp do inżynierii detekcji cyberzagrożeń; detekcje regułowe i analityczne; monitorowanie i logowanie zdarzeń.

OSINT, OpSec i bezpieczeństwo operacyjne (8h)

Biały wywiad i otwarte źródła informacji: wartość, źródła i filtrowanie OSInt; biały wywiad w wojskowości, organach ścigania, zastosowaniach cywilnych, biznesowych, prywatnych i przestępczych; analiza powiązań, relacji, tożsamości, przestrzenna i czasowa. Bezpieczeństwo operacyjne: projektowanie i wdrażanie strategii bezpieczeństwa operacyjnego (OpSec) na poziomie indywidualnym, organizacyjnym, korporacyjnym i instytucjonalnym; zarządzanie informacjami wrażliwymi i prywatnymi; bezpieczeństwo operacyjne w organizacji a zagrożenia dla instytucji publicznych i systemów infrastruktury krytycznej. Przestępstwa przyszłości: znaczenie interdyscyplinarnego planowania strategii bezpieczeństwa w związku z pojawianiem się, rosnącą dostępnością i malejącymi kosztami nowoczesnych technologii informacyjnych.

ZAJĘCIA KOMPUTEROWE

Inżynieria detekcji cyberzagrożeń (6h)

Systemy logowania zdarzeń; przeglądanie logów systemowych; praca z systemami detekcji zagrożeń w sieci (NIDS) i na hostach (HIDS, EDR); systemy SIEM, SOAR; popularne języki pisania reguł detekcji w różnych systemach; case study detekcji cyberzagrożeń (przykłady i ćwiczenia praktyczne).

Analiza powłamaniowa i zarządzanie incydentami (6h)

Planowanie działań i reakcji na wykryte cyberzagrożenia; pozyskanie materiału do analizy - obrazy dysków, zrzuty pamięci ulotnej, logi systemowe, logi z innych systemów cyberbezpieczeństwa i infrastruktury; dobór i zastosowanie narzędzi do pozyskanego materiału; analiza incydentu na podstawie zebranych danych; analiza złośliwych plików w specjalistycznych środowiskach; raportowanie; analiza powłamaniowana jako składnik zarządzania incydentami; case study incydentów (przykłady i ćwiczenia praktyczne).

6.	Formy weryfikacji i oceny osiąganych efektów uczenia się (warunki i sposób zaliczenia)

Kolokwium na zakończenie semestru: ANCI_W01, ANCI_W02, ANCI_W03, ANCI_W04, ANCI_W05, ANCI_W06, ANCI_W07, ANCI_W08, ANCI_U09, ANCI_K01, ANCI_K02
zajęcia komputerowe (aktywność, sprawozdanie): ANCI_U01, ANCI_U02, ANCI_U03, ANCI_U04, ANCI_U05, ANCI_U06, ANCI_U07, ANCI_U08, ANCI_U09
dyskusja na zajęciach: ANCI_U08, ANCI_U09, ANCI_K01, ANCI_K02

7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych

Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Opis efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Wiedza		
ANCI_W01	Ma wiedzę dotyczącą podstawowych pojęć z zakresu kryminalistyki cyfrowej, analizy oraz obsługi incydentów bezpieczeństwa komputerowego.	ICYB_W05
ANCI_W02	Ma podstawową wiedzę z zakresu uwarunkowań społeczno-ekonomiczno-prawnych przestępstw w cyberprzestrzeni.	ICYB_W06

ANCI_W03	Ma podstawową wiedzę z zakresu detekcji cyberzagrożeń i reakcji na nie.	ICYB_W04
ANCI_W04	Ma podstawową wiedzę z zakresu pozyskiwania i zabezpieczenia cyfrowego materiału dowodowego z różnych źródeł (systemy sprzętowo-programowe, sieci).	ICYB_W05
ANCI_W05	Ma wiedzę z zakresu analizowania cyfrowego materiału dowodowego.	ICYB_W05
ANCI_W06	Ma wiedzę z zakresu metod analitycznych stosowanych w kryminalistyce śledczej.	ICYB_W05
ANCI_W07	Ma wiedzę metodyki procesu zarządzania incydentami.	ICYB_W05
ANCI_W08	Ma podstawową wiedzę z zakresu modelowania zagrożeń.	ICYB_W02
Umiejętności		
ANCI_U01	Potrafi przygotować środowisko pracy analityka cyberzagrożeń i incydentów.	ICYB_U03
ANCI_U02	Potrafi formułować logikę detekcji cyberzagrożeń i odnieść ją do systemów monitorowania oraz detekcji.	ICYB_U02
ANCI_U03	Potrafi modelować zagrożenia z wykorzystaniem standardowych metodyk.	ICYB_U02
ANCI_U04	Potrafi obsłużyć zabezpieczony cyfrowy materiał dowodowy.	ICYB_U03
ANCI_U05	Potrafi stosować metody analityczne do pozyskanego cyfrowego materiału dowodowego.	ICYB_U03
ANCI_U06	Potrafi w podstawowym zakresie definiować procesy zarządzania incydentami naruszeń bezpieczeństwa komputerowego.	ICYB_U02
ANCI_U07	Potrafi aktywnie uczestniczyć w dyskusji na tematy związane z cyberbezpieczeństwem, w szczególności związane z cyberzagrożeniami i incydentami, używając poprawnej terminologii i formułując trafne argumenty.	ICYB_U07
ANCI_U08	Potrafi przygotować i przeprowadzić prezentację dotyczącą zagadnień technicznych związanych z cyberbezpieczeństwem.	ICYB_U07
ANCI_U09	Potrafi krytycznie analizować materiały źródłowe dotyczące cyberzagrożeń i incydentów.	ICYB_U01, ICYB_U09
Kompetencje społeczne		
ANCI_K01	Ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy.	ICYB_K03
ANCI_K02	Ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności w zakresie inżynierii cyberbezpieczeństwa.	ICYB_K02

1.	Nazwa przedmiotu lub grupy przedmiotów	Zarządzanie cyberbezpieczeństwem
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	4
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotów z przypisaną liczbą godzin	wykłady – 28 godz.
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	

WYKŁADY

Zarządzanie cyberbezpieczeństwem – kontekst dyrektora IT/CIO/CTO (6h)

Strategia zarządzania IT w nowoczesnym modelu; modele zarządzania IT – warstwa zarządcza (governance) i operacyjna (operations); zarządzanie infrastrukturą IT – działania operacyjne i długofalowe; zarządzanie projektami IT; zarządzanie problemami i incydentami; transformacja środowisk IT i zarządzanie długiem technologicznym; styk zadań z innymi interesariuszami, w tym z cyberbezpieczeństwem;

Zarządzanie cyberbezpieczeństwem – kontekst dyrektora cyberbezpieczeństwa/CISO (6h)

Strategie zarządzania cyberbezpieczeństwem; modele zarządzania cyberbezpieczeństwem - warstwa zarządcza (governance) i operacyjna (operations); wpływ typów środowisk na model działania CISO/dyrektora cyberbezpieczeństwa; programy cyberbezpieczeństwa – działania operacyjne i długofalowe, projekty z zakresu cyberbezpieczeństwa; zarządzanie problemami i incydentami; audyty i zgodność z wybranymi standardami oraz regulacjami prawnymi; styk i współpraca z interesariuszami z naciskiem na IT; zarządzanie ryzykiem cyberbezpieczeństwa; zarządzanie wiedzą o cyberzagrożeniach wewnętrznych i zewnętrznych; raportowanie i komunikacja nt. cyberbezpieczeństwa na poziomie zarządczym.

Zarządzanie cyberbezpieczeństwem – kontekst SOC/CERT/CSIRT managera (6h)

Działania operacyjne w cyberbezpieczeństwe; organizacje i zespoły operacyjne w cyberbezpieczeństwie: SOC, CERT, CSIRT; zarządzanie incydentami i reagowanie na zagrożenia - warstwa techniczna (narzędzia i systemy) oraz warstwa zarządcza (modele działania i frameworki, np. FIRST); styk SOC/CERT/CSIRT z innymi podmiotami – model wewnętrzny i zewnętrzny (usługowy); modele organizacji systemów cyberbezpieczeństwa na poziomach międzynarodowym, regionalnym i krajowym; Krajowy System Cyberbezpieczeństwa w Polsce.

Trendy i przyszłość cyberbezpieczeństwa (8h)

Historia rozwoju dziedziny w ostatnich 40+ latach; kamienie milowe i osiągnięcia w cyberbezpieczeństwie; filozofia pracy w cyberbezpieczeństwie; trendy i zagadnienia na nadchodzące lata i dekady w obszarze cyberbezpieczeństwa.

6.	Formy weryfikacji i oceny osiąganych efektów uczenia się (warunki i sposób zaliczenia)

Kolokwium na zakończenie semestru: ZACY_W01, ZACY_W02, ZACY_W03, ZACY_W04, ZACY_W05, ZACY_W06, ZACY_W07, ZACY_W08, ZACY_W09, ZACY_U07, ZACY_U08, ZACY_K01, ZACY_K02
praca w grupach i dyskusja na zajęciach: ZACY_U01, ZACY_U02, ZACY_U03, ZACY_U04, ZACY_U05, ZACY_U06, ZACY_U07, ZACY_U08, ZACY_K01, ZACY_K02

7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych

Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Opis efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Wiedza		
ZACY_W01	Ma wiedzę dotyczącą podstawowych pojęć z zakresu cyberbezpieczeństwa.	ICYB_W01
ZACY_W02	Ma wiedzę na temat cyberzagrożeń, ich źródeł i skali skutków.	ICYB_W02
ZACY_W03	Ma podstawową wiedzę dotyczącą specyfikacji celów i funkcji zapewniających cyberbezpieczeństwo.	ICYB_W01
ZACY_W04	Ma podstawową wiedzę dotyczącą aktów prawnych, norm, standardów i rekomendacji w obszarze cyberbezpieczeństwa.	ICYB_W03

ZACY_W05	Ma wiedzę z zakresu analizowania ryzyka systemów teleinformatycznych.	ICYB_W07
ZACY_W06	Ma podstawową wiedzę na temat mechanizmów cyberbezpieczeństwa, w szczególności ich stosowania w praktyce organizacyjnej i procesowej.	ICYB_W07
ZACY_W07	Ma podstawową wiedzę na temat tworzenia polityk bezpieczeństwa, ich wdrażania, tworzenia dokumentacji oraz formalnych i półformalnych metod dowodzenia poprawności systemów.	ICYB_W07
ZACY_W08	Rozumie aspekty dotyczące ochrony różnego typu infrastruktury teleinformatycznej, w szczególności sieci korporacyjnych i infrastruktury krytycznej.	ICYB_W07
ZACY_W09	Ma wiedzę dotyczącą podstawowych technik atakowania użytkowników systemów teleinformatycznych (socjotechniki).	ICYB_W06
Umiejętności		
ZACY_U01	Potrafi wykonać analizę możliwych cyberzagrożeń i oraz ocenić ich wpływ na zadane środowisko teleinformatyczne.	ICYB_U02, ICYB_U06
ZACY_U02	Potrafi wyspecyfikować cele i funkcje bezpieczeństwa dla systemu teleinformatycznego.	ICYB_U06
ZACY_U03	Potrafi stworzyć plany bezpieczeństwa i przygotować je wdrożenia.	ICYB_U06
ZACY_U04	Potrafi stosować środki techniczne zapewniające cyberbezpieczeństwo, adekwatnie do zadanego środowiska i otoczenia organizacyjnego.	ICYB_U06
ZACY_U05	Potrafi stworzyć plany, procesy i procedury operacyjne dla zadań cyberbezpieczeństwa.	ICYB_U06
ZACY_U06	Potrafi przeprowadzić analizę ryzyk dla bezpieczeństwa systemów teleinformatycznych.	ICYB_U02
ZACY_U07	Potrafi krytycznie analizować materiały źródłowe dotyczące zarządzania cyberbezpieczeństwem.	ICYB_U01, ICYB_U09
ZACY_U08	Potrafi aktywnie uczestniczyć w dyskusji na tematy związane z cyberbezpieczeństwem, w szczególności dotyczące zarządzania cyberbezpieczeństwem, używając poprawnej terminologii i formułując trafne argumenty.	ICYB_U07
Kompetencje społeczne		
ZACY_K01	Ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy.	ICYB_K03
ZACY_K02	Ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności w zakresie inżynierii cyberbezpieczeństwa.	ICYB_K02

1.	Nazwa przedmiotu lub grupy przedmiotów	Praca Końcowa z cyberbezpieczeństwa
2.	Tryb prowadzenia zajęć (zdalny/stacjonarny)	stacjonarny i zdalny
3.	Liczba punktów ECTS przypisana do przedmiotu lub grupy przedmiotów	6 (w tym do 5 – zdalnie)
4.	Formy prowadzenia zajęć dla przedmiotu lub grupy przedmiotów z przypisaną liczbą godzin	projekt – 92 godz.
5.	Treści programowe dla przedmiotu lub grupy przedmiotów	

PROJEKT
Projekt zespołowy (92h)
Projekt jest realizowany zgodnie z podejściem łączącym PBL (Project-based Learning) oraz pracę zespołową. Każdy zespół projektowy otrzymuje temat do realizacji. Tematy odnoszą się do zagadnień poruszanych w ramach przedmiotów tworzących program studiów podyplomowych Inżynieria Cyberbezpieczeństwa. Zadaniem każdego zespołu jest przeprowadzanie analizy teoretycznej i prac praktycznych w zakresie proponowanego tematu. Efektem końcowym prac jest raport oraz prezentacja podczas seminarium z udziałem innych uczestników studiów.

6.	Formy weryfikacji i oceny osiąganych efektów uczenia się (warunki i sposób zaliczenia)

Projekt (aktywność, sprawozdanie): PRAK_W01, PRAK_U01, PRAK_U02, PRAK_U03, PRAK_U05, PRAK_U06, PRAK_U08, PRAK_K01, PRAK_K02, PRAK_K03
dyskusja na zajęciach: PRAK_U07, PRAK_K01, PRAK_K02, PRAK_K03
projekt (prezentacja): PRAK_U07, PRAK_U08, PRAK_K01, PRAK_K03

7.	Efekty uczenia się przypisane do tych przedmiotów lub grup przedmiotów i ich odniesienie do efektów uczenia się dla programu studiów podyplomowych

Symbol efektu uczenia się dla przedmiotu lub grupy przedmiotów	Opis efektu uczenia się dla przedmiotu lub grupy przedmiotów	Symbol efektu uczenia się dla programu studiów podyplomowych
Wiedza		
PRAK_W01	ma podstawową wiedzę dotyczącą realizacji projektów w obszarze cyberbezpieczeństwa i IT.	ICYB_W01
Umiejętności		
PRAK_U01	Potrafi zrealizować złożone zadanie inżynierskie z zakresu cyberbezpieczeństwa.	ICYB_U04
PRAK_U02	Potrafi zastosować wiedzę i umiejętności z różnych obszarów cyberbezpieczeństwa, dostrzegając ich wzajemne oddziaływania.	ICYB_U04
PRAK_U03	Potrafi opracować plan projektu adekwatny do przedstawionych założeń i wymagań, aby osiągnąć zakładane rezultaty w określonym czasie.	ICYB_U08
PRAK_U04	Potrafi znaleźć i krytycznie analizować materiały źródłowe adekwatne do realizowanego zadania projektowego.	ICYB_U01, ICYB_U09
PRAK_U05	Potrafi przeprowadzić badania wybranego zagadnienia zgodnie z założoną metodyką i wymaganiami, a następnie udokumentować wyniki tych badań.	ICYB_U05
PRAK_U06	Potrafi opracować raport techniczny spełniający przyjęte w praktyce profesjonalnej cyberbezpieczeństwa wymagania dotyczące tego typu dokumentów.	ICYB_U05

PRAK_U07	Potrafi przygotować a następnie przeprowadzić prezentację, jasno formułując wnioski i opinie, stymulując dyskusję i w sposób przekonujący przedstawiając w niej swoje argumenty.	ICYB_U07
PRAK_U08	Potrafi planować i organizować pracę własną oraz współdziałać z innymi osobami w ramach prac w zespole.	ICYB_U08
Kompetencje społeczne		
PRAK_ K01	Ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy.	ICYB_K03
PRAK_ K02	Ma świadomość konieczności stałego aktualizowania i wzbogacania posiadanej wiedzy oraz zdobywania nowych umiejętności w zakresie inżynierii cyberbezpieczeństwa.	ICYB_K02
PRAK_K03	Ma świadomość konieczności pracy zespołowej i harmonijnej współpracy w celu osiągnięcia ważnych rezultatów w obszarze cyberbezpieczeństwa.	ICYB_K01