UCHWAŁA NR 447/XXV/XV/2019
Senatu Politechniki Białostockiej
z dnia 23 maja 2019 roku

- w sprawie ustalenia programu studiów podyplomowych Cyberbezpieczeństwo

Senat Politechniki Białostockiej, działając na podstawie art. 28 ust. 1 pkt 11 i 15 lit. a ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce (Dz. U. poz. 1668, z późn. zm.), postanawia:

§ 1

Ustalić program studiów podyplomowych Cyberbezpieczeństwo, stanowiący załącznik do niniejszej uchwały.

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

REKTOR

prof. dr hab. inż. Lech Dzienis

Politechnika Białostocka
Wydział Informatyki

PROGRAM STUDIÓW PODYPLOMOWYCH

Cyberbezpieczeństwo

Załącznik do Uchwały Nr 57/2019 Rady Wydziału Informatyki Politechniki Białostockiej z dnia 24.04.2019 r.

Program opracowany i realizowany we współpracy z:
Naukowa i Akademicka Sieć Komputerowa

NASK

Białystok 2019

Opracowanie:
dr inż. Ireneusz Mrozek (Politechnika Białostocka)
Agnieszka Wrońska (Naukowa i Akademicka Sieć Komputerowa)
Białystok, dn. 11.04.2019 r.

1. Nazwa studiów podyplomowych

Cyberbezpieczeństwo

2. Informacje ogólne

Program studiów został przygotowany we współpracy z Naukową i Akademicką Siecią Komputerową (NASK) na podstawie umowy zawartej z Politechniką Białostocką.
Zgodnie z umową, część zajęć będzie realizowana przez pracowników wydelegowanych przez NASK. Zajęcia będą się odbywały głównie na Wydziale Informatyki Politechniki Białostockiej, przy czym, jeden ze zjazdów może zostać zorganizowany w siedzibie NASK w Warszawie przy ul. Kolska 12, 01-045 Warszawa. Koszt dojazdu pokrywa Słuchacz we własnym zakresie.

3. Poziom Polskiej Ramy Kwalifikacji

Studia podyplomowe umożliwiają osiągnięcie kwalifikacji cząstkowych, uwzględniających charakterystyki drugiego stopnia Polskiej Ramy Kwalifikacji (PRK) na poziomie szóstym, określone w przepisach wydanych na podstawie art. 7 ust. 3 i 4 ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji.

4. Liczba semestrów i łączna liczba punktów ECTS

Studia podyplomowe *Cyberbezpieczeństwo* podzielone są na dwa etapy. Etap pierwszy o specjalności *Administrator Bezpieczeństwa Sieci* trwa 2 semestry. Po jego ukończeniu studia mogą być kontynuowane na 1-semestralnych specjalnościach: *Analityk Bezpieczeństwa Teleinformatycznego*.oraz *Inżynier Bezpieczeństwa Sieci*.

a) specjalność ***Administrator Bezpieczeństwa Sieci***
Liczba semestrów: 2
Liczba punktów ECTS konieczna do uzyskania kwalifikacji odpowiadających poziomowi studiów: 40

b) specjalność ***Analityk Bezpieczeństwa Teleinformatycznego***
Liczba semestrów: 3 (2+1)
Liczba punktów ECTS konieczna do uzyskania kwalifikacji odpowiadających poziomowi studiów: 55 (40 + 15)

c) specjalność ***Inżynier Bezpieczeństwa Sieci***
Liczba semestrów: 3 (2+1)
Liczba punktów ECTS konieczna do uzyskania kwalifikacji odpowiadających poziomowi studiów: 60 (40+20)

5. Łączna liczba godzin zajęć dydaktycznych

a) specjalność ***Administrator Bezpieczeństwa Sieci***

Zajęcia dydaktyczne obejmują łącznie 251 godzin, w tym 129 godzin na semestrze pierwszym i 122 godziny na semestrze drugim, zgodnie z podanym niżej planem studiów.

Lp.	Nazwa przedmiotu	Kod	Liczba ECTS			Liczba godzin w semestrze						Forma zaliczenia
			C	K	P	W	Ć	Ps	P	L	S	
SEMESTR 1												
1.1	Administracja systemami GNU Linux	CYB_LSA	3	1	2	10		10				Z
1.2	Koncepcje systemów operacyjnych	CYB_OSC	3	1	2,5	6		12				Z
1.3	Podstawy programowania skryptów	CYB_BSP	3	1	3	6		16				Z
1.4	Podstawy sieci komputerowych	CYB_BNW	4	1	3	12		12				Z
1.5	Podstawy kryptografii	CYB_BCY	3	0,5	2,5	10		4				Z
1.6	Zagrożenia w obszarze cyberbezpieczeństwa	CYB_CTH	1	0,4	0	10						Z
1.7	Podstawy bezpieczeństwa sieci i systemów IT	CYB_CSF	1	0,3	0	6						Z
1.8	Regulacyjne,strategiczne i etyczne aspekty cyberbezpieczeństwa	CYB_PLE	1	0,3	0	6						Z
1.9	Zarządzanie bezpieczeństwem informacji	CYB_MMS	1	0,4	0	9						Z
RAZEM W SEMESTRZE			**20**	5,9	13	75	54					Razem godz.:**129**
SEMESTR 2												
2.1	Ochrona sieci komputerowych	CYB_NDF	6	*2*	*5*	20		30				Z
2.2	Projekt zespołowy	CYB_IDR	4	*1*	4				20			Z
2.3	Technologie sieciowe i protokoły	CYB_NTP	4	*1*	*3*	10		10				Z
2.4	Bezpieczeństwo sieci bezprzewodowych	CYB_WSE	3	*0,5*	*2,5*	6		6				Z
2.5	Bezpieczeństwo w standardzie – normy w cyberbezpieczeństwie	CYB_IAS	3	*1*	2	10		10				Z
RAZEM W SEMESTRZE			**20**	*5,5*	*16,5*	46	76					Razem godz.:**122**
ŁĄCZNIE W TRAKCIE STUDIÓW			**40**	*11,4*	*29,5*	121 (48%)	130 (52%)					RAZEM GODZIN: **251**

Liczba ECTS: **C** - całkowita, **K** - "kontaktowych" (związanych z zajęciami wymagającymi bezpośredniego udziału nauczyciela), **P** - "praktycznych" (związanych z zajęciami o charakterze praktycznym)
Liczba godzin w semestrze: **W** - wykład, **Ć** - ćwiczenia, **Ps** - pracownia specjalistyczna, **P** - projekt, **L** - laboratorium, **S** - seminarium

b) specjalność ***Analityk Bezpieczeństwa Teleinformatycznego***

Zajęcia dydaktyczne obejmują łącznie 372 godziny, w tym 129 godzin na semestrze pierwszym, 122 godziny na semestrze drugim i 121 godzin na semestrze trzecim, zgodnie z podanym niżej planem studiów.

Lp.	Nazwa przedmiotu	Kod	Liczba ECTS			Liczba godzin w semestrze						Forma zaliczenia
			C	K	P	W	Ć	Ps	P	L	S	
SEMESTR 1												
1.1	Administracja systemami GNU Linux	CYB_LSA	3	1	2	10		10				Z
1.2	Koncepcje systemów operacyjnych	CYB_OSC	3	1	2,5	6		12				Z
1.3	Podstawy programowania skryptów	CYB_BSP	3	1	3	6		16				Z
1.4	Podstawy sieci komputerowych	CYB_BNW	4	1	3	12		12				Z
1.5	Podstawy kryptografii	CYB_BCY	3	0,5	2,5	10		4				Z
1.6	Zagrożenia w obszarze cyberbezpieczeństwa	CYB_CTH	1	0,4	0	10						Z
1.7	Podstawy bezpieczeństwa sieci i systemów IT	CYB_CSF	1	0,3	0	6						Z
1.8	Regulacyjne,strategiczne i etyczne aspekty cyberbezpieczeństwa	CYB_PLE	1	0,3	0	6						Z
1.9	Zarządzanie bezpieczeństwem informacji	CYB_MMS	1	0,4	0	9						Z
RAZEM W SEMESTRZE			**20**	5,9	13	75		54				Razem godz.:**129**
SEMESTR 2												
2.1	Ochrona sieci komputerowych	CYB_NDF	6	*2*	*5*	20		30				Z
2.2	Projekt zespołowy	CYB_IDR	4	*1*	4				20			Z
2.3	Technologie sieciowe i protokoły	CYB_NTP	4	*1*	*3*	10		10				Z
2.4	Bezpieczeństwo sieci bezprzewodowych	CYB_WSE	3	*0,5*	*2,5*	6		6				Z
2.5	Bezpieczeństwo w standardzie – normy w cyberbezpieczeństwie	CYB_IAS	3	*1*	2	10		10				Z
RAZEM W SEMESTRZE			**20**	*5,5*	*16,5*	46		76				Razem godz.:**122**
SEMESTR 3												
3.1	Zaawansowane technologie sieciowe i protokoły	CYB_ANT	3	1	2	10		15				Z
3.2	Analiza ogólnodostępnych źródeł informacji	CYB_OSI	3	1	2	8		12				Z
3.3	Analiza podatności	CYB_VLA	2	0,5	1	10		6				Z
3.4	Podstawy kryminalistyki cyfrowej	CYB_DFS	3	1	2	10		10				Z
3.5	Zaawansowane zagrożenia cybernetyczne	CYB_CTH	3	1,5	2	10		20				Z
3.6	Wprowadzenie do zarządzania incydentami	CYB_WZI	1	0,4	0	10						Z
RAZEM W SEMESTRZE			**15**	5,4	9	58		63				Razem godz.:**121**
ŁĄCZNIE W TRAKCIE STUDIÓW			**55**	*16,8*	*38,5*	179 (48%)		193 (52%)				RAZEM GODZIN**: 372**

Liczba ECTS: **C** - całkowita, **K** - "kontaktowych" (związanych z zajęciami wymagającymi bezpośredniego udziału nauczyciela), **P** - "praktycznych" (związanych z zajęciami o charakterze praktycznym)
Liczba godzin w semestrze: **W** - wykład, **Ć** - ćwiczenia, **Ps** - pracownia specjalistyczna, **P** - projekt, **L** - laboratorium, **S** - seminarium

c) specjalność ***Inżynier Bezpieczeństwa Sieci***

Zajęcia dydaktyczne obejmują łącznie 386 godzin, w tym 129 godzin na semestrze pierwszym, 122 godziny na semestrze drugim i 135 godzin na semestrze trzecim, zgodnie z podanym niżej planem studiów.

Lp.	Nazwa przedmiotu	Kod	Liczba ECTS			Liczba godzin w semestrze						Forma zaliczenia
			C	K	P	W	Ć	Ps	P	L	S	
SEMESTR 1												
1.1	Administracja systemami GNU Linux	CYB_LSA	3	1	2	10		10				Z
1.2	Koncepcje systemów operacyjnych	CYB_OSC	3	1	2,5	6		12				Z
1.3	Podstawy programowania skryptów	CYB_BSP	3	1	3	6		16				Z
1.4	Podstawy sieci komputerowych	CYB_BNW	4	1	3	12		12				Z
1.5	Podstawy kryptografii	CYB_BCY	3	0,5	2,5	10		4				Z
1.6	Zagrożenia w obszarze cyberbezpieczeństwa	CYB_CTH	1	0,4	0	10						Z
1.7	Podstawy bezpieczeństwa sieci i systemów IT	CYB_CSF	1	0,3	0	6						Z
1.8	Regulacyjne,strategiczne i etyczne aspekty cyberbezpieczeństwa	CYB_PLE	1	0,3	0	6						Z
1.9	Zarządzanie bezpieczeństwem informacji	CYB_MMS	1	0,4	0	9						Z
RAZEM W SEMESTRZE			**20**	5,9	13	75		54				Razem godz.:**129**
SEMESTR 2												
2.1	Ochrona sieci komputerowych	CYB_NDF	6	2	5	20		30				Z
2.2	Projekt zespołowy	CYB_IDR	4	1	4				20			Z
2.3	Technologie sieciowe i protokoły	CYB_NTP	4	1	3	10		10				Z
2.4	Bezpieczeństwo sieci bezprzewodowych	CYB_WSE	3	0,5	2,5	6		6				Z
2.5	Bezpieczeństwo w standardzie – normy w cyberbezpieczeństwie	CYB_IAS	3	1	2	10		10				Z
RAZEM W SEMESTRZE			**20**	5,5	16,5	46		76				Razem godz.:**122**
SEMESTR 3												
3.1	Administracja systemami Linux - LPIC-2	CYB_LP2	4	1,5	3	15		15				Z
3.2	Administracja systemami Windows	CYB_WAD	3	1	2	10		10				Z
3.3	Systemy IDS/IPS	CYB_IDS	3	0,5	2,5	5			10			Z
3.4	Testy penetracyjne	CYB_PTT	3	0,5	2,5	5			10			Z
3.5	Zaawansowana kryptografia	CYB_ACR	3	1	2	10		10				**E**
3.6	Zaawansowane technologie sieciowe i protokoły	CYB_ANT	3	1	2	10		15				Z
3.7	Analiza ryzyka w bezpieczeństwie informacji	CYB_SRA	1	0,3	0	10						Z
RAZEM W SEMESTRZE			**20**	5,8	14	65		70				Razem godz.:**135**
ŁĄCZNIE W TRAKCIE STUDIÓW			**60**	17,2	*43,5*	186 (48%)		200 (52%)				**RAZEM GODZIN: 386**

Liczba ECTS: **C** - całkowita, **K** - "kontaktowych" (związanych z zajęciami wymagającymi bezpośredniego udziału nauczyciela), **P** - "praktycznych" (związanych z zajęciami o charakterze praktycznym)
Liczba godzin w semestrze: **W** - wykład, **Ć** - ćwiczenia, **Ps** - pracownia specjalistyczna, **P** - projekt, **L** - laboratorium, **S** - seminarium

6. Opis kompetencji oczekiwanych od kandydata

Uczestnikiem studiów podyplomowych może być osoba, która posiada kwalifikację pełną co najmniej na poziomie 6 PRK, uzyskaną w systemie szkolnictwa wyższego i nauki (studia pierwszego stopnia, studia drugiego stopnia, jednolite studia magisterskie).

Naturalnymi kandydatami na studia podyplomowe *Cyberbezpieczeństwo* są absolwenci studiów z dyscypliny informatyki technicznej i telekomunikacji oraz informatyki.

Studia umożliwiają również rozwinięcie kompetencji absolwentom innych kierunków studiów posiadających wiedzę praktyczną z obszaru informatyki. W tym przypadku, kandydat będzie miał możliwość wypełnienia testu kompetencyjnego, sprawdzającego ogólną wiedzę niezbędną do rozpoczęcia studiów, którego wynik może mu pomóc w podjęciu decyzji o rozpoczęciu studiów. Test jest bezpłatny, dobrowolny i ma charakter anonimowy.

Słuchacze, którzy ukończą studia podyplomowe na kierunku *Cyberbezpieczeństwo* specjalność Administrator Bezpieczeństwa Sieci*,* w kolejnej edycji mogą się rejestrować i kontynuować naukę na dowolnej specjalności (Analityk Bezpieczeństwa Teleinformatycznego, Inżynier Bezpieczeństwa Sieci) z semestru trzeciego.

7. Sylwetka absolwenta

Cyberbezpieczeństwo jest dziedziną interdyscyplinarną wymagającą elastycznych ekspertów posiadających ugruntowaną wiedzę m.in. z zakresu: bezpieczeństwa systemów i sieci komputerowych, kryptografii, bieżących przepisów prawnych oraz posiadających wysokie kompetencje społeczne i komunikacyjne.

Program nauczania studiów podyplomowych *Cyberbezpieczeństwo* dostosowany jest do wymagań współczesności oraz kształtujących ją norm i trendów związanych z bezpieczeństwem informacji oraz systemów i sieci informatycznych.

Absolwent kierunku *Cyberbezpieczeństwo* (po ukończeniu specjalności ***Administrator Bezpieczeństwa Sieci***) posiada m.in.:

- wiedzę, umiejętności i kompetencje w zakresie ochrony i zabezpieczania danych oraz systemów i sieci komputerowych,
- niezbędne przygotowanie do pracy na stanowiskach związanych z ochroną danych cyfrowych i zabezpieczaniem systemów informatycznych,
- umiejętności z zakresu ochrony i bezpiecznego przetwarzania danych w formie cyfrowej, zabezpieczania sieci i systemów komputerowych, wykrywania nieautoryzowanego dostępu do chronionych danych,
- wiedzę w zakresie współczesnych technik zabezpieczania danych w formie cyfrowej, prawnych aspektów ochrony danych,

- umiejętności w zakresie stosowania współczesnych metod i środków zabezpieczania danych w formie cyfrowej oraz systemów do ich przetwarzania, przechowywania i transmisji.

Absolwent specjalności ***Analityk Bezpieczeństwa Teleinformatycznego*** uzyskuje dodatkowe kompetencje z zakresu:

- kryminalistyki cyfrowej,
- zarządzania incydentami,
- analizy podatności,
- zaawansowanych zagrożeń cybernetycznych,
- analizy ogólnodostępnych źródeł informacji,
- zaawansowanych protokołów sieciowych.

Absolwent specjalności ***Inżynier Bezpieczeństwa Sieci*** uzyskuje dodatkowe kompetencje z zakresu:

- przeprowadzania testów penetracyjnych,
- konfiguracji systemów IDS/IPS,
- technik sprawdzających poziom bezpieczeństwa systemów informatycznych,
- zaawansowanych protokołów sieciowych,
- zaawansowanych algorytmów kryptograficznych,
- proponowania rozwiązań technologicznych z obszaru bezpieczeństwa adekwatnych do istniejących potrzeb,
- administracji systemami Windows Serwer,
- zaawansowanej konfiguracji systemu Linux na poziomie LPIC-2.

8. Zestawienie tabelaryczne kierunkowych efektów uczenia się

Objaśnienia oznaczeń:
P6 – poziom 6 PRK (Polskie Ramy Kwalifikacji)
S – charakterystyka typowa dla kwalifikacji uzyskiwanych w ramach szkolnictwa wyższego
W – wiedza
T – teorie, zasady
Z – zjawiska i procesy
O – organizacja pracy
G – głębia i zakres
K – kontekst
U – umiejętności
I – informacje
W – wykorzystanie wiedzy
K – komunikowanie się
O – organizacja pracy
U – uczenie się
K – kompetencje społeczne
K – krytyczna ocena
O – odpowiedzialność
R – rola zawodowa
CYB – Cyberbezpieczeństwo
1, 2, 3 i kolejne – numery efektu kształcenia

Załącznik nr 1 do „Wytyczne do tworzenia programów studiów podyplomowych"

Symbol	**Efekty Uczenia się dla kierunku studiów**	**Odniesienie do charakterystyk drugiego stopnia określonych na podstawie art. 7 ust. 3 Ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji na poziomie 6 PRK**	**Odniesienie do charakterystyk drugiego stopnia określonych na podstawie art. 7 ust. 4 Ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji na poziomie 6 PRK**
Wiedza: absolwent zna i rozumie			
CYB_W01	pojęcia dotyczące bezpieczeństwa informacji (danych) oraz sieci komputerowych	P6S_WG	P6Z_WT
CYB_W02	mechanizmy oraz algorytmy zabezpieczania informacji cyfrowych (danych)	P6S_WG	P6Z_WT, P6Z_WO
CYB_W03	problemy bezpiecznej komunikacji poprzez publiczne kanały wymiany informacji	P6S_WG	P6Z_WT, P6Z_WO
CYB_W04	wybrane typy zagrożeń i ataków na systemy i sieci komputerowe	P6S_WG	P6Z_WT, P6Z_WZ
CYB_W05	protokoły transmisji w sieciach komputerowych	P6S_WG	P6Z_WT, P6Z_WO
CYB_W06	podstawowe mechanizmy zabezpieczeń wybranych systemów operacyjnych	P6S_WG	P6Z_WT

CYB_W07	metodyki, techniki i narzędzia niezbędne do implementacji skryptów	P6S_WG	P6Z_WT
CYB_W08	zasady tworzenia i wykorzystania polityki bezpieczeństwa	P6S_WG P6S_WK	P6Z_WT
CYB_W09	aspekty prawne związane z bezpieczeństwem informacji cyfrowych	P6S_WG	P6Z_WT
CYB_W10	wybrane metodyki zarządzania ryzykiem	P6S_WG	P6Z_WT
CYB_W11	wybrane narzędzia administratora systemów i sieci komputerowych	P6S_WG	P6Z_WT
Umiejętności: absolwent potrafi			
CYB_U01	wybrać oraz wykorzystać odpowiednie mechanizmy ochrony informacji cyfrowych w kontekście określonego problemu	P6S_UW	P6Z_UI P6Z_UO P6Z_UN
CYB_U02	skonfigurować i zabezpieczyć system operacyjny	P6S_UW	P6Z_UO
CYB_U03	zaprojektować, skonfigurować i zabezpieczyć prostą lokalną sieć komputerową	P6S_UW P6S_UU P6S_UO	P6Z_UO
CYB_U04	skonfigurować wybrane usługi w systemach i sieciach komputerowych	P6S_UW	PZ6_UO
CYB_U05	implementować proste skrypty powłoki systemów operacyjnych	P6S_UW	PZ6_UO
CYB_U06	zaproponować własną politykę bezpieczeństwa danej organizacji	P6S_UW P6S_UU	P6Z_UI P6Z_UO P6Z_UN
CYB_U07	przygotować dokumentację techniczną zrealizowanych rozwiązań	P6S_UW P6S_UK	P6Z_UO
CYB_U08	przygotować analizę ryzyka realizowanego przedsięwzięcia w kontekście bezpieczeństwa informacji w wybranej metodyce	P6S_UW P6S_UU	PZ6_UO
CYB_U09	wykrywać popularne ataki na systemy i sieci komputerowe oraz odpowiednio zareagować na zaistniały incydent	P6S_UW P6S_UU	PZ6_UI PZ6_UO
CYB_U10	używać wybranych narzędzi administratora systemów i sieci komputerowych	P6S_UW P6S_UU	PZ6_UO PZ6_UN
Kompetencje społeczne: absolwent jest gotów do			
CYB_K01	kierowania się w swojej pracy profesjonalizmem i etyką zawodową	P6S_KK P6S_KR	P6Z_KP, P6Z_KW, P6Z_KO
CYB_K02	realizacji swoich działań z uwzględnieniem aspektów ekonomicznych	P6S_KO	P6Z_KO

9. Matryca efektów uczenia się

				Nazwa studiów podyplomowych: Cyberbezpieczeństwo; Specjalność: Administrator Bezpieczeństwa Sieci																								
				MATRYCA POKRYCIA EFEKTÓW UCZENIA SIĘ																								
				WIEDZA												UMIEJĘTNOŚCI											K.S.		Kod przedmiotu
L.p.	Nazwa przedmiotu	Kod przedmiotu	semestr	CYB_W01	CYB_W02	CYB_W03	CYB_W04	CYB_W05	CYB_W06	CYB_W07	CYB_W08	CYB_W09	CYB_W10	CYB_W11	Kod przedmiotu	CYB_U01	CYB_U02	CYB_U03	CYB_U04	CYB_U05	CYB_U06	CYB_U07	CYB_U08	CYB_U09	CYB_U10	CYB_K01	CYB_K02	
1	Administracja systemami GNU Linux	CYB_LSA	SEM. 1						X	X				X	CYB_LSA		X	X		X					X			CYB_LSA
2	Koncepcje systemów operacyjnych	CYB_OSC		X	X		X							X	CYB_OSC	X	X	X	X	X	X	X				X		CYB_OSC
3	Podstawy programowania skryptów	CYB_BSP				X	X	X		X					CYB_BSP	X		X			X	X	X			X		CYB_BSP
4	Podstawy sieci komputerowych	CYB_BNW		X		X	X	X						X	CYB_BNW			X	X						X			CYB_BNW
5	Podstawy kryptografii	CYB_BCY		X	X		X								CYB_BCY	X												CYB_BCY
6	Zagrożenia w obszarze cyberbezpieczeństwa	CYB_CTH		X		X									CYB_CTH													CYB_CTH
7	Podstawy bezpieczeństwa sieci i systemów IT	CYB_CSF		X			X								CYB_CSF													CYB_CSF
8	Regulacyjne, strategiczne i etyczne aspekty cyberbezpieczeństwa	CYB_PLE										X	X		CYB_PLE													CYB_PLE
9	Zarządzanie bezpieczeństwem informacji	CYB_MMS					X				X	X	X		CYB_MMS													CYB_MMS
10	Ochrona sieci komputerowych	CYB_NDF	SEM. 2	X	X				X		X			X	CYB_NDF				X					X			CYB_NDF
11	Projekt zespołowy	CYB_IDR													CYB_IDR	X		X	X			X		X		X	CYB_IDR
12	Technologie sieciowe i protokoły	CYB_NTP				X	X	X							CYB_NTP									X	X			CYB_NTP
13	Bezpieczeństwo sieci bezprzewodowych	CYB_WSE		X	X	X	X	X	X						CYB_WSE			X						X				CYB_WSE
14	Bezpieczeństwo w standardzie – normy w cyberbezpieczeństwie	CYB_IAS		X								X	X		CYB_IAS	X							X			X	X	CYB_IAS
	SUMA			**8**	**4**	**5**	**8**	**4**	**3**	**2**	**2**	**3**	**3**	**4**		**5**	**2**	**6**	**4**	**2**	**2**	**3**	**2**	**2**	**5**	**3**	**2**	

				Nazwa studiów podyplomowych: Cyberbezpieczeństwo; Specjalność: Analityk Bezpieczeństwa Teleinformatycznego																										
				MATRYCA POKRYCIA EFEKTÓW UCZENIA SIĘ																									
				WIEDZA												UMIEJĘTNOŚCI											K.S.		Kod przedmiotu
L.p.	Nazwa przedmiotu	Kod przedmiotu	semestr	CYB_W01	CYB_W02	CYB_W03	CYB_W04	CYB_W05	CYB_W06	CYB_W07	CYB_W08	CYB_W09	CYB_W10	CYB_W11	Kod przedmiotu	CYB_U01	CYB_U02	CYB_U03	CYB_U04	CYB_U05	CYB_U06	CYB_U07	CYB_U08	CYB_U09	CYB_U10	CYB_K01	CYB_K02	
1	Administracja systemami GNU Linux	CYB_LSA	SEM. 1						X	X				X	CYB_LSA		X	X		X					X			CYB_LSA
2	Koncepcje systemów operacyjnych	CYB_OSC		X	X		X							X	CYB_OSC	X	X	X	X	X	X	X				X		CYB_OSC
3	Podstawy programowania skryptów	CYB_BSP				X	X	X		X					CYB_BSP	X		X			X	X	X			X		CYB_BSP
4	Podstawy sieci komputerowych	CYB_BNW		X		X	X	X						X	CYB_BNW			X	X						X			CYB_BNW
5	Podstawy kryptografii	CYB_BCY		X	X		X								CYB_BCY	X												CYB_BCY
6	Zagrożenia w obszarze cyberbezpieczeństwa	CYB_CTH		X		X									CYB_CTH													CYB_CTH
7	Podstawy bezpieczeństwa sieci i systemów IT	CYB_CSF		X			X								CYB_CSF													CYB_CSF
8	Regulacyjne, strategiczne i etyczne aspekty cyberbezpieczeństwa	CYB_PLE										X	X		CYB_PLE													CYB_PLE
9	Zarządzanie bezpieczeństwem informacji	CYB_MMS					X				X	X	X		CYB_MMS													CYB_MMS
10	Ochrona sieci komputerowych	CYB_NDF	SEM. 2	X	X				X		X			X	CYB_NDF				X					X			CYB_NDF
11	Projekt zespołowy	CYB_IDR													CYB_IDR	X		X	X			X			X		X	CYB_IDR
12	Technologie sieciowe i protokoły	CYB_NTP				X	X	X							CYB_NTP									X	X			CYB_NTP
13	Bezpieczeństwo sieci bezprzewodowych	CYB_WSE		X	X	X	X	X	X						CYB_WSE			X						X				CYB_WSE
14	Bezpieczeństwo w standardzie – normy w cyberbezpieczeństwie	CYB_IAS		X								X	X		CYB_IAS	X							X			X	X	CYB_IAS
15	Zaawansowane technologie sieciowe i protokoły	CYB_ANT	SEM. 3			X		X						X	CYB_ANT				X			X			X			CYB_ANT
16	Analiza ogólnodostępnych źródeł informacji	CYB_OSI		X	X	X						X			CYB_OSI	X						X						CYB_OSI
17	Analiza podatności	CYB_VLA		X			X		X					X	CYB_VLA										X			CYB_VLA
18	Podstawy kryminalistyki cyfrowej	CYB_DFS		X	X							X			CYB_DFS										X			CYB_DFS
19	Zaawansowane zagrożenia cybernetyczne	CYB_CTH		X			X			X		X			CYB_CTH		X							X	X			CYB_CTH
20	Wprowadzenie do zarządzania incydentami	CYB_WZI					X				X		X		CYB_WZI													CYB_WZI
	SUMA			**12**	**6**	**7**	**11**	**5**	**4**	**3**	**3**	**6**	**4**	**6**		**6**	**3**	**6**	**5**	**2**	**2**	**5**	**2**	**3**	**9**	**3**	**2**	

				Nazwa studiów podyplomowych: Cyberbezpieczeństwo; Specjalność: Inżynier Bezpieczeństwa Sieci																								
				MATRYCA POKRYCIA EFEKTÓW UCZENIA SIĘ																								
				WIEDZA												UMIEJETNOŚCI											K.S		Kod przedmiotu
L.p.	Nazwa przedmiotu	Kod przedmiotu	semestr	CYB_W01	CYB_W02	CYB_W03	CYB_W04	CYB_W05	CYB_W06	CYB_W07	CYB_W08	CYB_W09	CYB_W10	CYB_W11	Kod przedmiotu	CYB_U01	CYB_U02	CYB_U03	CYB_U04	CYB_U05	CYB_U06	CYB_U07	CYB_U08	CYB_U09	CYB_U10	CYB_K01	CYB_K02	
1	Administracja systemami GNU Linux	CYB_LSA	SEM. 1						X	X				X	CYB_LSA		X	X		X					X			CYB_LSA
2	Koncepcje systemów operacyjnych	CYB_OSC		X	X		X							X	CYB_OSC	X	X	X	X	X	X	X				X		CYB_OSC
3	Podstawy programowania skryptów	CYB_BSP				X	X	X		X					CYB_BSP	X		X			X	X	X			X		CYB_BSP
4	Podstawy sieci komputerowych	CYB_BNW		X		X	X	X						X	CYB_BNW			X	X						X			CYB_BNW
5	Podstawy kryptografii	CYB_BCY		X	X		X								CYB_BCY	X												CYB_BCY
6	Zagrożenia w obszarze cyberbezpieczeństwa	CYB_CTH		X		X									CYB_CTH													CYB_CTH
7	Podstawy bezpieczeństwa sieci i systemów IT	CYB_CSF		X			X								CYB_CSF													CYB_CSF
8	Regulacyjne, strategiczne i etyczne aspekty cyberbezpieczeństwa	CYB_PLE										X	X		CYB_PLE													CYB_PLE
9	Zarządzanie bezpieczeństwem informacji	CYB_MMS					X				X	X	X		CYB_MMS													CYB_MMS
10	Ochrona sieci komputerowych	CYB_NDF	SEM. 2	X	X				X		X			X	CYB_NDF				X						X			CYB_NDF
11	Projekt zespołowy	CYB_IDR													CYB_IDR	X		X	X			X			X		X	CYB_IDR
12	Technologie sieciowe i protokoły	CYB_NTP				X	X	X							CYB_NTP									X	X			CYB_NTP
13	Bezpieczeństwo sieci bezprzewodowych	CYB_WSE		X	X	X	X	X	X						CYB_WSE			X						X				CYB_WSE
14	Bezpieczeństwo w standardzie – normy w cyberbezpieczeństwie	CYB_IAS		X								X	X		CYB_IAS	X							X			X	X	CYB_IAS
15	Administracja systemami Linux - LPIC-2	CYB_LP2	SEM. 3						X					X	CYB_LP2		X											CYB_LP2
16	Administracja systemami Windows	CYB_WAD							X					X	CYB_WAD		X		X									CYB_WAD
17	Systemy IDS/IPS	CYB_IDS		X			X		X						CYB_IDS				X			X		X				CYB_IDS
18	Testy penetracyjne	CYB_PTT		X	X	X	X	X	X			X		X	CYB_PTT							X		X	X	X		CYB_PTT
19	Zaawansowana kryptografia	CYB_ACR			X			X							CYB_ACR	X									X			CYB_ACR
20	Zaawansowane technologie sieciowe i protokoły	CYB_ANT				X		X						X	CYB_ANT				X			X			X			CYB_ANT
21	Analiza ryzyka w bezpieczeństwie informacji	CYB_SRA											X		CYB_SRA													CYB_SRA
	SUMA			**10**	**6**	**7**	**10**	**7**	**7**	**2**	**2**	**4**	**4**	**8**		**6**	**4**	**6**	**7**	**2**	**2**	**6**	**2**	**4**	**8**	**4**	**2**	

10. Opis zasobów bibliotecznych oraz elektronicznych zasobów wiedzy obejmujących literaturę zalecaną, do których uczelnia zapewni dostęp

Biblioteka Politechniki Białostockiej zapewnia dostęp do zasobów bibliotecznych oraz elektronicznych zasobów wiedzy obejmujących literaturę zalecaną na Studiach Podyplomowych Cyberbezpieczeństwo.

Biblioteka Politechniki Białostockiej jest największą biblioteką naukowo-techniczną w regionie północno-wschodnim Polski. Biblioteka PB jest podstawą systemu biblioteczno-informacyjnego uczelni. W jej skład wchodzi Biblioteka Główna oraz Biblioteka Wydziału Architektury, Biblioteka Wydziału Inżynierii Zarządzania oraz Biblioteka Zamiejscowego Wydziału Leśnego w Hajnówce. Zadaniem Biblioteki Głównej jest zaspokajanie potrzeb wszystkich pracowników i studentów w zakresie dostępu do literatury naukowej i dydaktycznej. Biblioteki specjalistyczne obsługują zaś poszczególne jednostki organizacyjne uczelni (wydziały, instytuty) gromadzą i udostępniają księgozbiór ściśle związany z ich potrzebami.

Władze i nauczyciele akademiccy Wydziału Informatyki PB współpracują ściśle z Biblioteką PB w zakresie bieżącego gromadzenia zbiorów (książek oraz czasopism krajowych i zagranicznych), z wyspecjalizowanymi dokumentami włącznie. W procesie powiększania zbiorów uwzględniane są także potrzeby z zakresu zarządzania bezpieczeństwem systemów informatycznych, który jest skorelowany z realizowanymi kierunkami studiów. Bieżące zakupy krajowych i zagranicznych wydawnictw naukowych zapewniają dostęp studentom i nauczycieli akademickich Wydziału Informatyki do najnowszej literatury specjalistycznej.

Od 1951 roku Biblioteka PB zgromadziła ponad 406 tysięcy książek, czasopism, norm i literatury firmowej. Tematyka księgozbioru jest ściśle związana z potrzebami wydziałów i kierunkami studiów Politechniki Białostockiej. Wśród zgromadzonych materiałów bibliotecznych ważne miejsce zajmują wydawnictwa z zakresu: mechaniki; budowy, eksploatacji i technologii maszyn; biocybernetyki i inżynierii biomedycznej; automatyki i robotyki; elektrotechniki, elektroniki i telekomunikacji; informatyki; budownictwa; inżynierii i ochrony środowiska; zarządzania i marketingu; architektury; nauk matematyczno-przyrodniczych.

Tabela 1. Zbiory Biblioteki Politechniki Białostockiej w rozbiciu na kategorie

Lp.	Opis	Stan na 31.12.2017
1.	Łącznie zasoby (liczba woluminów), w tym:	406 331
	wydawnictwa zwarte	281 495
	wydawnictwa ciągłe	45 907
	zbiory specjalne (normy, literatura firmowa, dokumenty elektroniczne)	78 929
2.	Liczba czasopism prenumerowanych (dostępnych w formie papierowej), w tym:	419
	wydawnictwa polskie	389
	wydawnictwa zagraniczne	30
3.	Liczba wydawnictw zarejestrowanych (liczba woluminów), w tym:	6 821
	wydawnictwa zwarte	6 164
	wydawnictwa ciągłe	546
	zbiory specjalne (normy, literatura firmowa, dokumenty elektroniczne)	111

Źródło: dane z Biblioteki Głównej Politechniki Białostockiej.

Od 1995 roku w Bibliotece PB działa niezawodnie zintegrowany system biblioteczny ALEPH. Uruchomiona w 2009 roku 18 wersja ALEPH 500 zapewnia użytkownikom przyjazne środowisko pracy. Umożliwia korzystanie z nowych usług, np. automatycznej komunikacji za pomocą poczty elektronicznej dotyczącej wypożyczania książek oraz przesyłania zestawień tematycznych, a pracownikom biblioteki oferuje wiele nowych funkcji ułatwiających wprowadzanie danych. Zarejestrowani użytkownicy mogą zdalnie zamawiać książki, prolongować terminy ich zwrotu oraz kontrolować stan swojego konta. Obecnie wszystkie zbiory biblioteczne są widoczne w katalogu online.

Od października 2012 roku Biblioteka Główna funkcjonuje w gmachu Centrum Nowoczesnego Kształcenia. W nowoczesnych pomieszczeniach udostępniane są połączone zbiory Biblioteki Głównej oraz funkcjonujących dawniej bibliotek wydziałowych zlokalizowanych na terenie kampusu. Zgromadzenie w jednym miejscu bogatego księgozbioru pozwoliło na wyodrębnienie, na trzech kondygnacjach budynku, ogólnodostępnych, specjalistycznych czytelni:

- Czytelnia Wydawnictw Informacyjnych - 27 miejsc;
- Czytelnia Elektroniczna - 24 miejsca;
- Czytelnia Czasopism - 24 miejsca;
- Czytelnia Norm i Zbiorów Specjalnych - 10 miejsc;
- Czytelnia Książek - 81 miejsc.

Użytkownicy mogą korzystać również z 19 specjalnie zaprojektowanych i wyposażonych pomieszczeń do pracy indywidualnej i zbiorowej (72 miejsca). Dodatkowo na potrzeby szkoleń, prezentacji czy ćwiczeń dostępna jest sala multimedialna, w której są 32 stanowiska komputerowe. Łącznie Biblioteka PB dysponuje 378 miejscami dla czytelników (Biblioteka Główna - 270 oraz biblioteki specjalistyczne – 108). W 2015 roku na terenie Czytelni Książek utworzono stanowisko do pracy dla osób niepełnosprawnych ze specjalistycznym oprogramowaniem komputerowym.

Ponadto do dyspozycji użytkowników jest 108 stanowisk komputerowych z dostępem do Internetu. Na wybranych stanowiskach zainstalowano specjalistyczne oprogramowanie: Adobe AfterEffects CS6, Adobe Design & Web Premium CS6 (Photoshop, Illustrator, InDesign. Dreamweaver, Flash Professional, Fireworks, Acrobat X Pro, Bridge, Media Encoder), Adobe Photoshop CS6 Extended, Altium Designer 10 Academic, Android Studio, ArchiCAD 20 oraz 19, Autodesk Education Master Suite 2014 EDU (AutoCAD, Autodesk), Blender, Code Blocks Studio, Corel Designer Technical Suite X5, CorelDRAW Graphics Suite X6 (CorelDRAW, PHOTO-PAINT, PowerTRACE, CAPTURE, CONNECT), Dev-C++ , Embarcadero RAD Studio XE2 Professional (Delphi XE2, C++Builder XE2, Embarcadero Prism XE2, RadPHP XE2 & Android Platform, InterBase XE Developer Edition), Flash Builder Premium 4.5, GIMP, Microsoft Office 2010 oraz 2003, MikroMap, Netbeans IDE, Norma PRO EDU, proTeXtorazLEd - LaTeXEdytor, Solid Works 2017, Statistica 13.1, University Bundle V-Ray 2.0 for 3ds Max EDU + Pdplayer, Vensim PLE, Visual Studio Express 2012, WinKalk.

Użytkownicy mogą także korzystać z wysokiej klasy samoobsługowych skanerów (3 znajdują się w Bibliotece Głównej, 1 – w Bibliotece Wydziału Inżynierii Zarządzania) oraz skanerów płaskich dostępnych przy stanowiskach komputerowych.

Wychodząc naprzeciw potrzebom czytelników Biblioteka wprowadziła szereg rozwiązań podnoszących jakość świadczonych usług i komfort korzystania ze zbiorów. Przede wszystkim wolny, swobodny dostęp

do najnowszych zbiorów naukowych i dydaktycznych. Regulaminy czytelni zarówno Biblioteki Głównej jak i bibliotek specjalistycznych uwzględniają krótkoterminowe wypożyczenia zbiorów poza obręb czytelni na okres 7 dni lub na 3 godziny. Specjalne urządzenia (self-checki) pozwalają na samodzielne wypożyczenia i zwroty książek. Zamontowane na zewnątrz budynku CNK urządzenie „wrzutnia" umożliwia również zwrot książek w czasie zamknięcia biblioteki.

Istotnym uzupełnieniem księgozbioru bibliotecznego są zasoby elektroniczne. Dostęp do najnowszych osiągnięć nauki zapewniają tematyczne i wielodziedzinowe serwisy czasopism i książek elektronicznych. Biblioteka PB oferuje dostęp do następujących baz danych:

baz pełnotekstowych, m.in.:

- EBSCOhost (serwis interdyscyplinarny);
- Elsevier (baza interdyscyplinarna ScienceDirect);
- Emerald Engineering and Emerald Managament Journals (automatyka, robotyka, matematyka obliczeniowa, elektronika, inżynieria materiałowa, zarządzanie, marketing, finanse, logistyka, technika);
- Emerging Markets Information Service (EMIS) (biznes, zarządzanie i rachunkowość, ekonomia i finanse);
- IBUK libra (baza interdyscyplinarna książek polskich);
- IEEE Xplore Digital Library (technika);
- INFONA (interdyscyplinarna);
- Knovel Library (technika);
- Naukowa Akademicka Sieciowa Biblioteka Internetowa (NASBI) (baza interdyscyplinarna książek polskich);
- OECD iLibrary (interdyscyplinarna);
- ProQuest Ebook Central (interdyscyplinarna);
- SPRINGER (interdyscyplinarna);
- Wiley Online Library (interdyscyplinarna).

baz bibliograficzno-abstraktowych:

- ISI Web of Science (interdyscyplinarna);
- MathSciNet (matematyka, informatyka i dziedziny pokrewne);
- Scopus (interdyscyplinarna);
- Web of Science (interdyscyplinarna);

indywidualnych tytułów czasopism, m.in.:

- Building Services Engineering Research & Technology;
- Computer Methods in Material Science;

- Géotechnique;
- Journal of Landscape Architecture;
- LEUKOS;
- Lighting Research and Technology;
- Miesięcznik Hotelarz;
- Miesięcznik Rynek Turystyczny;
- Nature Publishing Group (interdyscyplinarna);
- Poradnik gospodarowania odpadami on-line;
- Science (nauki przyrodnicze i inne);
- Vademecum Bibliotekarza on-line.

oraz krajowych i zagranicznych baz ogólnodostępnych, jak:

- AGRO (nauki przyrodnicze, rolnicze i techniczne);
- BazEkon (ekonomia);
- BazTech (nauki techniczne oraz w wyborze nauki ścisłe i ochrona środowiska);
- Directory of Open Access Journals (multidyscyplinarna);
- ElektronischeZeitschriftenbibliothek (multidyscyplinarna).

W 2016 roku Biblioteka PB uruchomiła wyszukiwarkę naukową PRIMO – nowoczesne i uniwersalne narzędzie, służące do jednoczesnego przeszukiwania wszystkich zasobów bibliotecznych, zarówno tradycyjnych jak i elektronicznych. Dzięki niej przeszukiwanie zbiorów jest bardzo proste. Jedno okno wyszukiwawcze pozwala szybko i efektywnie dotrzeć do wszystkich lokalnych oraz zdalnych zasobów, a wyniki są pogrupowane wg indywidualnych potrzeb czytelnika.

W 2004 roku zostało zawarte „Porozumienie o utworzeniu Konsorcjum Bibliotek Naukowych Miasta Białegostoku". W ramach tego porozumienia w 2006 r. rozpoczęła działalność Podlaska Biblioteka Cyfrowa (dalej PBC). Biblioteka PB aktywnie uczestniczy w tworzeniu zasobu edukacyjnego poprzez rozwój Kolekcji Naukowo-Dydaktycznej. W jej skład wchodzą podręczniki dla studentów, monografie, skrypty i artykuły naukowe autorstwa pracowników Politechniki Białostockiej, w tym pracowników Wydziału Informatyki. W 2017 roku Biblioteka Politechniki Białostockiej zdigitalizowała 22 nowych publikacji, co łącznie daje 284 pozycji w zasobie PBC. Materiały te cieszą się dużym zainteresowaniem i zajmują czołowe miejsca wśród najbardziej poczytnych pozycji. W 2016 roku zarejestrowano 84 tys. wyświetleń publikacji zgromadzonych w PBC, a w 2017 roku było ich blisko 94 tys.

Zasoby biblioteczne są stale aktualizowane i wzbogacane z uwzględnieniem potrzeb nauczycieli akademickich i studentów poszczególnych wydziałów uczelni w tym Wydziału Informatyki. Władze i nauczyciele akademiccy Wydziału Informatyki współpracują ściśle z biblioteką w zakresie bieżącego gromadzenia zbiorów tradycyjnych i elektronicznych. Dotyczy to zarówno wydawnictw zwartych, prenumeraty czasopism w wersji papierowej i elektronicznej czy dostępu do elektronicznych baz danych.

Biblioteka Politechniki Białostockiej zapewnia dostęp między innymi do następujących zasobów bibliotecznych oraz elektronicznych zasobów wiedzy obejmujących literaturę zalecaną na Studiach Podyplomowych Cyberbezpieczeństwo:

I. Zasoby biblioteczne

1. A. Tanenbaum, Computer Networks, Prentice Hall, Indian International Ed.; 5th edition, 2010.
2. A. Silberschatz, P. B. Galvin, Podstawy systemów operacyjnych, wydanie 7, WNT, 2003.
3. A.S. Tanenbaum, Systemy Operacyjne, Wydanie III, Helion, 2010.
4. M. Mitchell, J. Oldham, A. Samuel, Linux - programowanie dla zaawansowanych, Wydawnictwo RM, 2002.
5. K. Wall, Linux : programowanie w przykładach, Mikom, 2000.
6. B. Eckel, Thinking in Java. Edycja Polska, wydanie 3, Helion, 2003.
7. J. Gręboszc, Opus Magnum C++ 11: programowanie w języku C++, Helion, 2017.
8. G. Coldwind, Zrozumieć programowanie, wydanie 1, PWN, 2015.
9. P. Barry, Python, Helion, 2017.
10. K. Rother, Python dla profesjonalistów : debugowanie, testowanie i utrzymywanie kodu, Helion, 2018.
11. K.M., Strothmann, Kryptografia: teoria i praktyka zabezpieczania systemów komputerowych, Wydawnictwo RM, 1999.
12. B. Schneier, Kryptografia dla praktyków, WNT, 2002.
13. D.L. Pipkin, Bezpieczeństwo informacji: ochrona globalnego przedsiębiorstwa, WNT, 2002.
14. N. Koblitz, Wykład z teorii liczb i kryptografii, WNT, 1995.
15. M. Wrona, Niebezpieczeństwo komputerowe, Wydawnictwo RM, 2000.
16. D.E Robling-Denning, Kryptografia i ochrona danych, Wyd. II, WNT, 1993.
17. E. Maiwald, Bezpieczeństwo w Sieci, Wydawnictwo Edition, 2000.
18. J. Stokłosa, T. Bilski, T. Pankowski, Bezpieczeństwo danych w systemach informatycznych, PWN, 2001.
19. H. Wells, Tłumaczenie: Piotr Rajca, Ajax. Bezpieczne aplikacje internetowe, O'Reilly, 2007.
20. P. Hope, B.Walther, Testowanie bezpieczeństwa aplikacji internetowych. Receptury, Helion, 2012.
21. R. Pejman, L. Jonathan, Bezprzewodowe sieci LAN 802.11. Podstawy, Mikom, 2007.
22. V. Ramachandran, Kali Linux: audyt bezpieczeństwa sieci Wi-Fi dla każdego, Helion, 2016.
23. J. Ross, Sieci bezprzewodowe. Przewodnik po sieciach WI-FI i szerokopasmowych sieciach bezprzewodowych, Helion, 2009.
24. D.E. Comer, Sieci komputerowe i intersieci: kompendium wiedzy każdego administratora, Helion, 2012.
25. A. Józefiok, CCNA 200-120. Zostań administratorem sieci komputerowych CISCO, Helion, 2015.
26. J. Muniz, A. Lakhani, Kali Linux. Testy penetracyjne, Helion, 2014.
27. J.P. Aumasson, Nowoczesna kryptografia: praktyczne wprowadzenie do szyfrowania, PWN, 2018.
28. M. Karbowski, Podstawy kryptografii, Helion, 2014.

II. Elektroniczne zasoby wiedzy

1. IEEE specifications 802.2, 802.3, 802.4, 802.5, 802.11: standards.ieee.org/getieee802/.
2. Request For Comments
3. Mikrotik documentation, http::/www.mikrotik.com
4. Dokumentacja pakietu Netfilter, http://www.netfilter.org
5. Dokumentacja serwera DHCP, https://www.isc.org/downloads/dhcp/
6. Apache project, http://www.apache.org
7. Dokumentacja pakietu OpenSSH, http://openssh.org
8. Podręcznik systemowy GNU Linux.
9. Materiały do kursu LPIC-1 oraz LPIC-2 (udostępniane studentom w formie elektronicznej).
10. Dokumentacja systemu Debian, http://www.debian.org/doc.
11. Dokumentacja systemu Fedora, http://docs.fedoraproject.org.
12. Dokumentacja systemu SuSe, http://en.opensuse.org/Documentation.

11. Karty przedmiotów

Karty są zamieszczone wg specjalności w następującej kolejności:

1. Administrator Bezpieczeństwa Sieci (przedmioty wspólne)
2. Administrator Bezpieczeństwa Teleinformatycznego
3. Inżynier Bezpieczeństwa Sieci

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Administracja systemami GNU Linux**							**Kod przedmiotu**	**CYB_LSA**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	1
	10				10			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest nabycie umiejętności wykonywania podstawowych operacji związanych z instalacją oraz podstawową administracją systemami Linux z poziomu konsoli.								
Treści programowe	Wykład: 1. Instalacja systemu operacyjnego. 2. Podstawowe polecenia wykonywane w oparciu o interfejs tekstowy. 3. Prawa dostępu po plików i katalogów. 4. Konfiguracja interfejsów sieciowych. 5. Zarządzanie kontami użytkowników (kontrola dostępu, polityka haseł, metody uwierzytelniania, polityka grupowa). 6. Aktualizacje oraz patchowanie. 7. Logowanie zdarzeń oraz audyt (pod kątem działania systemu oraz bezpieczeństwa). 8. System zarządzania usługami. 9. Wirtualizacja. 10. Kopie zapasowe oraz przywracanie danych. Pracownia specjalistyczna: 1. Instalacja systemu. 2. Podstawowe polecenia wykonywane w oparciu o interfejs tekstowy. 3. Konfiguracja interfejsów sieciowych. 4. Zarządzanie kontami użytkowników. 5. System zarządzania usługami.									
Metody dydaktyczne	programowanie z użyciem komputera, wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena zadań realizowanych w trakcie zajęć, ocena sprawozdań.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	potrafi zainstalować system dobierając odpowiednie parametry	CYB_U02
EU2	zna zasady zarządzania użytkownikami oraz potrafi zakładać im konta	CYB_W06 CYB_W11 CYB_U02 CYB_U10
EU3	zna polityki uwierzytelniania oraz potrafi je konfigurować	CYB_W06 CYB_W11 CYB_U02 CYB_U10
EU4	zna i konfiguruje funkcje kontroli	CYB_W06 CYB_W11 CYB_U03 CYB_U10
EU5	potrafi wykonywać kopie zapasowe oraz przywracać system z kopii zapasowej	CYB_W07 CYB_U05 CYB_U10
EU6	zna zasady aktualizacji systemu; potrafi aktualizować system oraz aplikować łatki	CYB_W06 CYB_W07 CYB_W11 CYB_U05 CYB_U10
EU7	zna strukturę plików z logami systemowymi oraz potrafi je analizować pod kątem bezpieczeństwa	CYB_W11 CYB_U10

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	ocena wykonanego zadania	Ps
EU2	kolokwium, sprawozdanie z wykonanego zadania	W, Ps
EU3	kolokwium, sprawozdanie z wykonanego zadania	W, Ps
EU4	kolokwium, sprawozdanie z wykonanego zadania	W, Ps
EU5	sprawozdanie z wykonanego zadania	Ps
EU6	kolokwium, sprawozdanie z wykonanego zadania	W, Ps
EU7	kolokwium, sprawozdanie z wykonanego zadania	W, Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach - 5x2h	10
2 - Udział w pracowni specjalistycznej - 5x2h	10
3 - Przygotowanie do pracowni specjalistycznej -	10
4 - Wykonanie zadań domowych (prac domowych) -	33
5 - Udział w konsultacjach -	2
6 - Przygotowanie do zaliczenia -	10
RAZEM:	**75**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	22 (1)+(2)+(5)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	53 (2)+(3)+(4)	2,0

Literatura podstawowa	1. Podręcznik systemowy GNU Linux. 2. Materiały do kursu LPIC-1 oraz LPIC-2 (udostępniane studentom w formie elektronicznej).	
Literatura uzupełniająca	1. Debian system documentation - http://www.debian.org/doc. 2. Fedora system documentation - http://docs.fedoraproject.org. 3. SuSe system documentation - http://en.opensuse.org/Documentation.	
Jednostka realizująca	Wydział Informatyki	**Data opracowania programu**
Program opracował(a)	dr inż. Ireneusz Mrozek	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Bezpieczeństwo sieci bezprzewodowych**							**Kod przedmiotu**	**CYB_WSE**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	2
	6				6			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zaznajomienie słuchaczy z problemami bezpieczeństwa sieci bezprzewodowych. Słuchacze poznają metody i algorytmy stosowane do zapewnienia bezpieczeństwa transmisji bezprzewodowej oraz zagrożenia w sieciach bezprzewodowych								
Treści programowe	Wykład: Protokół WEP. Protokół WPA. Protokół WPA2. EAP/802.11x. RADIUS. Zagrożenia i niedoskonałości protokołów WEP, WPA i WPA2. Pracownia specjalistyczna: Protokół WEP. Protokół WPA. Protokół WPA2. EAP/802.11x. RADIUS. Zagrożenia i niedoskonałości protokołów WEP, WPA i WPA2.								
Metody dydaktyczne	programowanie z użyciem komputera, wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium, pracownia specjalistyczna - sprawozdania z realizacji zadań.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna podstawy funkcjonowania sieci bezprzewodowych	CYB_W05
EU2	zna metody i algorytmy zapewniania bezpieczeństwa transmisji bezprzewodowej oraz implementuje je	CYB_W01 CYB_W02 CYB_W05 CYB_W06 CYB_U03
EU3	zna metody weryfikacji tożsamości i procesy asocjacji i uwierzytelniania oraz implementuje je	CYB_W02 CYB_W03 CYB_W06 CYB_U03
EU4	zna zagrożenia w sieciach bezprzewodowych i niedoskonałości stosowanych metod oraz potrafi im przeciwdziałać	CYB_W01 CYB_W02 CYB_W04 CYB_U09

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium, sprawozdania	W, Ps
EU3	kolokwium, sprawozdania	W, Ps
EU4	kolokwium, sprawozdania	W, Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach - 6h	6
2 - Udział w pracowni specjalistycznej - 6h	6
3 - Przygotowanie do pracowni specjalistycznej - 3x6h	18
4 - Opracowanie sprawozdań z pracowni specjalistycznej - 3x12h	36
5 - Przygotowanie do kolokwium zaliczającego - 8h	8
6 - Udział w konsultacjach -	2
RAZEM:	**76**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	14 (6)+(2)+(1)	0,5
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	60 (4)+(3)+(2)	2,5

Literatura podstawowa	1. R. Pejman, L. Jonathan, Bezprzewodowe sieci LAN 802.11. Podstawy, Mikom, 2007. 2. V. Ramachandran, Kali Linux: audyt bezpieczeństwa sieci Wi-Fi dla każdego, Helion, 2016. 3. J. Ross, Sieci bezprzewodowe. Przewodnik po sieciach WI-FI i szerokopasmowych sieciach bezprzewodowych, Helion, 2009.
Literatura uzupełniająca	1. Dokumenty RFC. 2. Dokumenty IEEE (standards.ieee.org).
Jednostka realizująca	Wydział Informatyki — **Data opracowania programu**
Program opracował(a)	dr inż. Tomasz Grześ — 17 lutego 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Bezpieczeństwo w standardzie – normy w cyberbezpieczeństwie**							**Kod przedmiotu**	**CYB_IAS**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	2
	10				10			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapoznanie słuchaczy z normami i wzorcami w zakresie projektowania i testowania cyberbezpieczeństwa.								
Treści programowe	Wykład: 1. „Security by design” – założenia projektowania i testowania w oparciu o normy i najlepsze praktyki 2. Normalizacja bezpieczeństwa teleinformatycznego – wprowadzenie: a. Normalizacja w Polsce, Europie i na świecie b. Wzajemna uznawalność i kompatybilność rozwiązań 3. Badania zgodności i certyfikacja – wprowadzenie: a. Zasady testowania i atestacji (certyfikacji) b. Uznawalność międzynarodowa certyfikatów i znaków 4. Omówienie praktycznego zastosowania norm w projektowaniu: a. Oprogramowania i urządzeń wg ISO15408 (Common Criteria) b. Systemów sterowania i kontroli w sieciach przemysłowych (OT, SCADA, Industrial Control Systems) wg IEC 62443 Pracownia specjalistyczna: Przygotowanie zarysu dokumentacji produktu (usługi) teleinformatycznego w odniesieniu do norm w obszarze cyberbezpieczeństwa.									
Metody dydaktyczne									
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena przygotowanej dokumentacji.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna polskie, europejskie i światowe organizacje normalizacyjne, ich relacje i zakres uznawania	CYB_W01 CYB_W09
EU2	zna zasady publikacji i stosowania norm w teleinformatyce i cyberbezpieczeństwie, potrafi rozpoznać normy niezbędne w projektowaniu i testowaniu	CYB_W09 CYB_U01 CYB_K01
EU3	zna i wybiera, właściwe dla danego kontekstu użycia, normy w obszarze projektowania i testowania cyberbezpieczeństwa	CYB_W01 CYB_W10 CYB_U01 CYB_K01 CYB_K02
EU4	potrafi przygotować zarys dokumentacji produktu (usług) teleinformatycznego w odniesieniu do norm w obszarze cyberbezpieczeństwa	CYB_U01 CYB_U08

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium, ocena przygotowanej dokumentacji	W, Ps
EU3	kolokwium, ocena przygotowanej dokumentacji	W, Ps
EU4	ocena przygotowanej dokumentacji	Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach - 5x2h	10
2 - Udział w pracowni specjalistycznej - 5x2h	10
3 - Przygotowanie do zaliczenia wykładu -	15
4 - Przygotowanie dokumentacji -	40
5 - Udział w konsultacjach -	2
RAZEM:	**77**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	22 (5)+(2)+(1)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	50 (4)+(2)	2,0

Literatura podstawowa	1. Norma Common Criteria (ISO15408) – część 1, 2, 3. 2. Norma IEC 62443.
Literatura uzupełniająca	1. Publikacja NIST 800-53, 800-37. 2. Uzgodnione profile zabezpieczeń (colaborative protection profiles) wg Common Criteria.
Jednostka realizująca	Naukowa i Akademicka Sieć Komputerowa (NASK) — **Data opracowania programu**
Program opracował(a)	Paweł Kostkiewicz — 11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Koncepcje systemów operacyjnych**							**Kod przedmiotu**	**CYB_OSC**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	1
	6				12			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Wprowadzenie słuchaczy do technik i metodyk skorelowanych z systemami operacyjnymi. Przedstawienie podstawowych funkcji systemu operacyjnego, wskazanie w jaki sposób one działają jak również wyjaśnienie jak systemy operacyjne współpracują ze sprzętem oraz z innymi aplikacjami uruchamianymi w ich środowisku. Słuchaczom zostaną także zaprezentowane sposoby zapewniania bezpieczeństwa w kontekście systemów operacyjnych.								
Treści programowe	Wykład: Koncepcja i zadania systemu operacyjnego. Zasady zarządzania zasobami sprzętowymi. Podstawy wirtualizacji i przykłady technologii wirtualizacyjnych. Kontrola dostępu do zasobów i tryby pracy zwykły oraz uprzywilejowany. Pracownia specjalistyczna: Podstawowe komendy w administracji systemami Linux i Windows. Wątki. Procesy. Zarządzanie pamięcią i użytkownikami. Wirtualizacja. Systemy plików. Zarządzanie bezpieczeństwem systemu operacyjnego. Kontrola dostępu.								
Metody dydaktyczne	programowanie z użyciem komputera, wykład informacyjny, ćwiczenia przedmiotowe, pokaz, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena zadań realizowanych w trakcie zajęć.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna podstawy budowy i działania systemów operacyjnych	CYB_W01 CYB_W02
EU2	potrafi zrealizować prostą synchronizację wątków w oparciu o semafory i monitory	CYB_U03 CYB_U04 CYB_U06
EU3	potrafi programować z wykorzystaniem środowiska dostarczonego przez system operacyjny	CYB_U01 CYB_U02 CYB_U06
EU4	potrafi zaplanować oraz przeprowadzić eksperymenty skorelowane z bezpieczeństwem systemu operacyjnego a następnie ocenić ich rezultaty	CYB_U03 CYB_U05 CYB_U07 CYB_K01
EU5	zna zasady wyboru systemu operacyjnego do realizowanego problemu	CYB_W04
EU6	potrafi zainstalować oraz skonfigurować wstępnie system operacyjny	CYB_W04 CYB_W11 CYB_U01

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	realizacja zadań na zajęciach	Ps
EU3	realizacja zadań na zajęciach	Ps
EU4	realizacja zadań na zajęciach	Ps
EU5	kolokwium	W
EU6	realizacja zadań na zajęciach	Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach - 3x2h	6
2 - Udział w zajęciach pracowni specjalistycznej - 6x2h	12
3 - Przygotowanie do pracowni specjalistycznej. Realizacja zadań. -	50
4 - Przygotowanie do zaliczenia wykładu -	5
5 - Udział w konsultacjach -	2
RAZEM:	**75**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	20 (5)+(2)+(1)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	62 (3)+(2)	2,5

Literatura podstawowa	1. A. Silberschatz, P. B. Galvin, Podstawy systemów operacyjnych, wydanie 7, WNT, 2003. 2. A.S. Tanenbaum, Systemy Operacyjne, Wydanie III, Helion, 2010. 3. W. Stallings, Systemy operacyjne. Architektura, funkcjonowanie i projektowanie. wydanie 9, Helion, 2018.
Literatura uzupełniająca	1. E. Nemeth, G. Snyder, T.R. Hein, B. Whaley, D.Mackin, Unix i Linux. Przewodnik administratora systemów, wydanie 5, Helion, 2018. 2. D.W. Jones, J. Hicks, Windows PowerShell w miesiąc, wydanie 3, Helion, 2018. 3. P.l Yosifovich, A. Ionescu, M.E. Russinovich, D.A. Solomon, Windows od środka. Architektura systemu, procesy, wątki, zarządzanie pamięcią i dużo więcej, wydanie 7, Helion, 2018. 4. M. Mitchell, J. Oldham, A. Samuel, Linux - programowanie dla zaawansowanych, Wydawnictwo RM, 2002. 5. K. Wall, Linux: programowanie w przykładach, Mikom, 2000.
Jednostka realizująca	Wydział Informatyki — **Data opracowania programu**
Program opracował(a)	dr inż. Mirosław Omieljanowicz,mgr inż. Maciej Szymkowski — 11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Ochrona sieci komputerowych**							**Kod przedmiotu**	**CYB_NDF**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	2
	20				30			**Punkty ECTS**	**6**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapoznanie z popularnymi koncepcjami ochrony sieci komputerowych (ochrona w głąb, minimalna ekspozycja, etc.) oraz narzędziami i usługami służącymi do zbudowania systemu ochrony.								
Treści programowe	Wykład: 1. Koncepcje ochrony systemów komputerowych: a. ochrona w głąb (ang. Defense in Depth) b. ataki sieciowe c. utwardzanie sieci d. minimalna ekspozycja (powierzchnie i wektory ataku) 2. Narzędzia ochrony i monitoringu sieci komputerowych: a. budowa firewalla b. strefy DMZ / Serwery Proxy c. serwery VPN d. urządzenia typu Honeypots oraz sieci Honeynets e. budowa systemów IDS/IPS 3. Operacje sieciowe: a. monitorowanie b. analiza ruchu 4. Polityka bezpieczeństwa sieci: a. kontrola dostępu do sieci (ang. Network Access Control) b. rozwijanie polityki bezpieczeństwa Pracownia specjalistyczna: 1. Konfiguracja serwera DNS 2. Konfiguracja serwera HTTP/HTTPS 3. Zaawansowana konfiguracja firewalla z wykorzystaniem pakietu netfilter 4. Utwardzanie systemu operacyjnego Linux 5. Konfiguracja serwera VPN 6. Konfiguracja sieci z wydzieloną strefą zdemilitaryzowaną (DMZ) oraz urządzeniem typu Honeypot								
Metody dydaktyczne	programowanie z użyciem komputera, wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena realizowanych zadań.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	opisuje kluczowe koncepcje w ochronie sieci komputerowych	CYB_W01 CYB_W08 CYB_W11
EU2	zna zasady działania oraz potrafi konfigurować wybrane systemy ochrony sieci komputerowych	CYB_W01 CYB_W02 CYB_W06 CYB_W08 CYB_W11 CYB_U04 CYB_U10
EU3	zna zasady analizowania, zastosowanej w danym systemie, polityki bezpieczeństwa do ochrony sieci komputerowej	CYB_W08
EU4	potrafi konfigurować podstawowe usługi zapewniające bezpieczeństwo transmisji danych	CYB_U04

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium, ocena realizowanych zadań i sprawozdań	W, Ps
EU3	kolokwium	W
EU4	ocena realizowanych zadań i sprawozdań	Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach - 10x2h	20
2 - Udział w pracowni specjalistycznej - 15x2h	30
3 - Przygotowanie sprawozdań z wykonywanych zadań -	30
4 - Przygotowanie do zaliczenia wykładu -	10
5 - Realizacja zadań domowych -	60
6 - Udział w konsultacjach -	2
RAZEM:	**152**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	52 (6)+(2)+(1)	2,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	120 (5)+(3)+(2)	5,0

Literatura podstawowa	1. S. Suehring, Zapory sieciowe w systemie Linux: kompendium wiedzy o nftables, Helion, 2015. 2. Dokumentacja pakietu netfilter, http://netfilter.org. 3. Dokumentacja serwera OpenVPN, http://openvpn.net. 4. Dokumentacja serwera Apache, http://www.apache.org.

Literatura uzupełniająca	1. W. Stallings, L. Brown, Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Helion, 2019. 2. E. Cole, R.L. Krutz, J. Conley, Bezpieczeństwo sieci. Biblia, Helion, 2005.	
Jednostka realizująca	Wydział Informatyki	**Data opracowania programu**
Program opracował(a)	dr inż. Andrzej Chmielewski	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Podstawy bezpieczeństwa sieci i systemów IT**							**Kod przedmiotu**	**CYB_CSF**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	1
	6							**Punkty ECTS**	**1**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapewnienie słuchaczom zrozumienia podstawowych koncepcji cyberbezpieczeństwa.								
Treści programowe	1. Podstawowe informacje, definicje i słownictwo dotyczące bezpieczeństwa sieci i systemów IT w kontekście cyberbezpieczeństwa. 2. Obraz tendencji w cyberzagrożeniach na świecie i w Polsce. 3. Omówienie typowych ataków na systemy informatyczne. 4. Wykrywanie złośliwej aktywności i detekcja formy ataku. 5. Podstawy zastosowań kryptografii i infrastruktury klucza publicznego.								
Metody dydaktyczne	wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Projekt zaliczeniowy.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	opisuje podstawowe pojęcia dotyczące dyscypliny bezpieczeństwa cybernetycznego i stosuje ją, aby zapewnić bezpieczeństwo systemu	CYB_W01 CYB_W04
EU2	opisuje potencjalne ataki systemowe i podmioty, które mogą je wykonać	CYB_W01 CYB_W04
EU3	opisuje narzędzia, metody i komponenty cyberobrony i stosuje metody cyberobrony, aby przygotować system do odpierania ataków	CYB_W04
EU4	opisuje odpowiednie środki, które należy podjąć w przypadku wystąpienia zagrożenia systemowego	CYB_W04
EU5	właściwie używa słownictwa związanego z cyberbezpieczeństwem	CYB_W01

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	projekt zaliczeniowy	W
EU2	projekt zaliczeniowy	W
EU3	projekt zaliczeniowy	W
EU4	projekt zaliczeniowy	W
EU5	projekt zaliczeniowy	W

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach. -	6
2 - Uczestnictwo w konsultacjach. -	2
3 - Przygotowanie do zaliczenia wykładu. -	17
RAZEM:	**25**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	8 (2)+(1)	0,3
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	0	0,0

Literatura podstawowa	1. Materiały podane przez prowadzącego.	
Literatura uzupełniająca	1. E. Maiwald, Bezpieczeństwo w Sieci, Wydawnictwo Edition, 2000. 2. J. Stokłosa, T. Bilski, T. Pankowski, Bezpieczeństwo danych w systemach informatycznych, Wydawnictwo Naukowe PWN, 2001. 3. C. Wells, Ajax. Bezpieczne aplikacje internetowe [Tłumaczenie: Piotr Rajca], O'Reilly, 2007. 4. P. Hope, B. Walther, Testowanie bezpieczeństwa aplikacji internetowych. Receptury, Helion, 2012.	
Jednostka realizująca	Naukowa i Akademicka Sieć Komputerowa (NASK)	**Data opracowania programu**
Program opracował(a)	Michał Leszczyński	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Podstawy kryptografii**							**Kod przedmiotu**	**CYB_BCY**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	1
	10				4			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapoznanie słuchaczy z podstawowymi wybranymi metodami zapewnienia poufności danych i sposobami ich wykorzystania.								
Treści programowe	Wykład: 1. Typowe zastosowania kryptografii a. funkcje bezpieczeństwa (bezpieczeństwo danych, integralność danych, uwierzytelnienie, niezaprzeczalność) b. różnica pomiędzy danymi blokowymi i strumieniem danych c. podpis cyfrowy. 2. Funkcje skrótu (MD4, MD5, SHA-1, SHA-2, SHA-3) a. integralność danych b. ochrona danych uwierzytelniających c. odporność na kolizje. 3. Kryptografia symetryczna (DES, Twofish). 4. Kryptografia klucza publicznego (Diffie-Hellman, RSA, ECC, ElGamal, DSA) a. infrastruktura klucza publicznego b. certyfikaty c. zarządzanie kluczami (tworzenie, wymiana/dystrybucja). 5. Praktyczne wykorzystanie kryptografii a. typowe protokoły kryptograficzne b. DES -> AES (rozwinięcie algorytmu DES) c. tryby pracy algorytmów kryptograficznych d. standardy kryptograficzne (FIPS 140 series). 6. Zagrożenia mechanizmów kryptograficznych a. typowe ataki b. błędy implementacyjne. Pracownia specjalistyczna: 1. Implementacja wybranego kryptosystemu symetrycznego. 2. Implementacja wybranego kryptosystemu asymetrycznego.									
Metody dydaktyczne	programowanie z użyciem komputera, ćwiczenia przedmiotowe, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena wykonywanych zadań praktycznych.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna zasady budowy systemów kryptograficznych	CYB_W01 CYB_W02
EU2	zna podstawowe architektury systemów kryptograficznych oraz dokonuje ich wyboru	CYB_W02 CYB_U01
EU3	umie wskazać różnice pomiędzy kryptografią symetryczną i asymetryczną	CYB_W02
EU4	zna zasady dobierania systemów kryptograficznych	CYB_W02
EU5	zna zagrożenia natury kryptograficznej	CYB_W02 CYB_W04

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium, ocena zadania praktycznego	W, Ps
EU3	kolokwium	W
EU4	kolokwium	W
EU5	kolokwium	W

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach -	10
2 - Udział w pracowni specjalistycznej -	4
3 - Udział w konsultacjach -	2
4 - Przygotowanie do pracowni specjalistycznej -	15
5 - Opracowanie sprawozdań z pracowni specjalistycznej i wykonanie zadań domowych (prac domowych) -	40
6 - Przygotowanie do zaliczenia wykładu -	10
RAZEM:	**81**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	16 (3)+(2)+(1)	0,5
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	59 (5)+(4)+(2)	2,5

Literatura podstawowa	1. J.P. Aumasson, Nowoczesna kryptografia: praktyczne wprowadzenie do szyfrowania, PWN, 2018. 2. M. Karbowski, Podstawy kryptografii, Helion, 2014. 3. B. Schneier, Kryptografia dla praktyków, WNT, 2002. 4. D.L. Pipkin, Bezpieczeństwo informacji: ochrona globalnego przedsiębiorstwa, WNT, 2002. 5. M. Kutyłowski, W. Strothmann, Kryptografia: teoria i praktyka zabezpieczania systemów komputerowych, Wydawnictwo RM, 1999.	
Literatura uzupełniająca	1. J. Kraft, An Introduction to Number Theory with Cryptography, Second Edition, CRC Press Inc, 2018. 2. M. Wrona, Niebezpieczeństwo komputerowe, Wydawnictwo RM, 2000. 3. D.R. Stinson, Cryptography. Theory And Practice, Springer-Verlag, 1995. 4. D.E. Robling-Denning, Kryptografia i ochrona danych, Wyd. II, WNT 1993. 5. N. Koblitz, Wykład z teorii liczb i kryptografii, WNT, 1995.	
Jednostka realizująca	Wydział Informatyki	**Data opracowania programu**
Program opracował(a)	dr inż. Ireneusz Mrozek	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Podstawy programowania skryptów**							**Kod przedmiotu**	**CYB_BSP**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	1
	6				16			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Zapoznanie słuchaczy ze zróżnicowanymi technikami pisania prostych skryptów, np. pozwalających na automatyzację części procesów administracyjnych. Przedstawienie sposobów na wykorzystanie zróżnicowanych struktur i technik programistycznych do pisania skryptów. Wykształcenie u słuchaczy biegłej znajomości tworzenia skryptów (w różnych językach programowania) z zachowaniem zasad bezpieczeństwa oraz wysokiej jakości kodu.								
Treści programowe	Wykład: Pojęcia związane z programowaniem. Struktura skryptu. Pojęcia związane z bezpieczeństwem. Zmienne. Parametry pozycyjne. Pętle. Instrukcje warunkowe. Operacje logiczne. Wyrażenia regularne. Pracownia specjalistyczna: Pisanie skryptów w środowiskach Windows oraz Linux. Wprowadzenie do implementacji prostych skryptów w różnych środowiskach programistycznych i różnych językach programowania. Implementacja podstawowych technik bezpieczeństwa w ramach programowania skryptów (m.in. analiza uprawnień, walidacja wprowadzonych danych). Wyrażenia regularne. Podstawowe operacje algebry Boole'a.								
Metody dydaktyczne	programowanie z użyciem komputera, wykład informacyjny, pokaz, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena dwóch projektów.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna i stosuje metodyki, techniki i narzędzia niezbędne do napisania skryptów	CYB_W07 CYB_U06 CYB_U08 CYB_K01
EU2	dobiera sposoby na zabezpieczenie implementowanych rozwiązań z zachowaniem ich wydajności	CYB_W03 CYB_W05 CYB_U03 CYB_U06
EU3	potrafi przetestować własne rozwiązanie zarówno pod kątem wydajności jak i bezpieczeństwa	CYB_W04 CYB_U06 CYB_U07 CYB_K01
EU4	zna zróżnicowane techniki programistyczne i potrafi uzasadnić konieczność użycia wybranych w ramach realizowanego projektu	CYB_W05 CYB_W07 CYB_U06 CYB_U08
EU5	umie wykorzystać biblioteki zewnętrzne do realizacji programów	CYB_U06
EU6	potrafi posłużyć się właściwie dobranymi środowiskami programistycznymi, systemami kontroli wersji oraz narzędziami dynamicznego testowania systemów informatycznych oraz ich komponentów	CYB_W05 CYB_U01 CYB_U06 CYB_K01

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium, ocena projektów zaliczeniowych	W, Ps
EU2	ocena projektów zaliczeniowych	Ps
EU3	ocena projektów zaliczeniowych	Ps
EU4	kolokwium, ocena projektów zaliczeniowych	W, Ps
EU5	ocena projektów zaliczeniowych	Ps
EU6	ocena projektów zaliczeniowych	Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach - 3x2h	6
2 - Udział w zajęciach pracowni specjalistycznej - 8x2h	16
3 - Realizacja zadań i projektów -	45
4 - Przygotowanie do kolokwium zaliczeniowego -	10
5 - Udział w konsultacjach -	2
RAZEM:	**79**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	24 (5)+(2)+(1)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	71 (4)+(3)+(2)	3,0

Literatura podstawowa	1. M. Ebrahimian, A. Mallett, Skrypty powłoki systemu Linux. Zagadnienia zaawansowane, Helion, 2019. 2. C. Flynt, S. Lakshman, S. Tushar, Skrypty powłoki systemu Linux. Receptury, Helion, Gliwice, 2019. 3. B. Eckel, Thinking in Java. Edycja Polska, wydanie 3, Helion, 2003. 4. J. Grębosz, Opus Magnum C++ 11: programowanie w języku C++, Helion, 2017. 5. G. Coldwind, Zrozumieć programowanie, wydanie 1, PWN, 2015.
Literatura uzupełniająca	1. E. Wilson, Tworzenie skryptów w Microsoft Windows. Podręcznik do samodzielnej nauki, Promise, 2016. 2. P. Barry, Python, Helion, 2017. 3. K. Rother, Python dla profesjonalistów: debugowanie, testowanie i utrzymywanie kodu, Helion, 2018.
Jednostka realizująca	Wydział Informatyki — **Data opracowania programu**
Program opracował(a)	dr inż. Tomasz Grześ,mgr inż. Maciej Szymkowski — 11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Podstawy sieci komputerowych**							**Kod przedmiotu**	**CYB_BNW**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	1
	12				12			**Punkty ECTS**	**4**
Przedmioty wprowadzające									
Cele przedmiotu	Zapoznanie słuchaczy z podstawowym modelem transmisji danych w sieciach komputerowych oraz realizacjami mechanizmów zdefiniowanych w takim modelu. Prezentacja przekroju zagadnień dotyczących sieci komputerowych. Zdobycie wiedzy dotyczącej problemów występujących w trakcie działania sieci oraz przyczyn ich powstawania. Znajomość zasad działania i korzystania z podstawowych usług dostępnych w Internecie.								
Treści programowe	Wykład: 1. Modele sieciowe (OSI i TCP/IP). 2. Media transmisyjne (przewodowe, optyczne i bezprzewodowe). 3. Architektury sieciowe i topologie (PAN, LAN / WAN, DMZ, enklawy, VLAN, NAT, podsieci, nadsieci). 4. Typowe urządzenia sieciowe i ich rola w sieci (rutery, przełączniki, hosty, VPN-y, firewalle). 5. Wprowadzenie do protokołów sieciowych (IP, TCP, UDP, ICMP). 6. Wprowadzenie do usług sieciowych i protokołów (DNS, NTP, VLAN itp.). 7. Wprowadzenie do aplikacji sieciowych i protokołów (SMTP, HTTP, VoIP, SSH itp.). 8. Korzystanie z podstawowych narzędzi do administrowania siecią. 9. Przegląd problemów związanych z bezpieczeństwem sieci. Pracownia specjalistyczna: 1. Kable sieciowe. 2. Konfiguracja VLAN-ów na przełącznikach. 3. Analiza pakietów sieciowych za pomocą aplikacji Wireshark. 4. Skanowanie portów. 5. Konfiguracja wybranych usług sieciowych, np.: a) Konfiguracja serwera DHCP. b) Konfiguracja serwera SSH.								
Metody dydaktyczne	wykład informacyjny, ćwiczenia laboratoryjne, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena sprawozdań z wykonywanych zadań praktycznych.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	opisuje podstawowe pojęcia, technologie, elementy i zagadnienia związane z komunikacją oraz transmisją danych	CYB_W01 CYB_W03
EU2	projektuje podstawowe architektury sieciowe, uwzględniając jego konkretne wymagania oraz zbiór hostów/klientów	CYB_U03 CYB_U04
EU3	potrafi śledzić oraz identyfikować pakiety biorące udział w prostym połączeniu TCP	CYB_W05 CYB_W11 CYB_U10
EU4	potrafi wykorzystywać analizatory sieciowe (np. Wiereshark) do obserwacji przesyłanych pakietów	CYB_W11 CYB_U10
EU5	potrafi wykryć urządzenia w sieci (np. za pomocą Nmap) oraz określić usługi sieciowe na nich działające	CYB_W11 CYB_U10
EU6	opisuje typowe luki w zabezpieczeniach sieci	CYB_W01 CYB_W04

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	sprawozdanie z wykonanego zadania	Ps
EU3	sprawozdanie z wykonanego zadania	Ps
EU4	sprawozdanie z wykonanego zadania	Ps
EU5	sprawozdanie z wykonanego zadania	Ps
EU6	kolokwium	W

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach - 6x2h	12
2 - Udział w pracowni specjalistycznej - 6x2h	12
3 - Udział w konsultacjach -	2
4 - Przygotowanie do pracowni specjalistycznej -	15
5 - Opracowanie sprawozdań i wykonanie zadań domowych -	50
6 - Przygotowanie do zaliczenia wykładu -	10
RAZEM:	**101**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	26 (3)+(2)+(1)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	77 (5)+(4)+(2)	3,0

Literatura podstawowa	1. D.E. Comer, Sieci komputerowe i intersieci: kompendium wiedzy każdego administratora, Helion, 2014. 2. A. Tanenbaum, Sieci komputerowe, Prentice Hall, Indian International Ed., 2010. 3. Dokumentacja pakietu Netfilter, http://www.netfilter.org. 4. Serwer DHCP, https://www.isc.org/downloads/dhcp/. 5. Apache project, http://www.apache.org. 6. Dokumentacja pakietu OpenSSH, http://openssh.org.

Literatura uzupełniająca	1. IEEE specifications 802.2, 802.3, 802.4, 802.5, 802.11: standards.ieee.org/getieee802/. 2. Request For Comments. 3. L.L. Peterson, B.S. Davie, Computer Networks: A Systems Approach, 5th edition, Elsevier, 2012. 4. Mikrotik - dokumentacja, http::/www.mikrotik.com.	
Jednostka realizująca	Wydział Informatyki	**Data opracowania programu**
Program opracował(a)	dr inż. Andrzej Chmielewski	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Projekt zespołowy**							**Kod przedmiotu**	**CYB_IDR**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	2
				20				**Punkty ECTS**	**4**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest praktyczna weryfikacja zdobytej wiedzy i umiejętności związanych z konfiguracją bezpiecznych sieci komputerowych zdobytych podczas studiów na bieżącym kierunku.								
Treści programowe	Zespołowa realizacja wybranego projektu zaproponowanego przez prowadzącego.								
Metody dydaktyczne	programowanie z użyciem komputera, metoda projektów,								
Forma zaliczenia	Sprawozdanie z wykonanego projektu.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	potrafi zaprojektować prostą i bezpieczną sieć komputerową	CYB_U03 CYB_K02
EU2	potrafi skonfigurować wybrane usługi sieciowe	CYB_U01 CYB_U03 CYB_U04 CYB_U10
EU3	potrafi przeskanować sieć pod kątem podatności i zrobić podstawową interpretację wyników skanów	CYB_U03 CYB_U10
EU4	potrafi przygotować dokumentację wykonanej sieci komputerowej	CYB_U07

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	sprawozdanie z wykonanego projektu	P
EU2	sprawozdanie z wykonanego projektu	P
EU3	sprawozdanie z wykonanego projektu	P
EU4	sprawozdanie z wykonanego projektu	P

Bilans nakładu pracy studenta (w godzinach)		**Liczba godz.**
Wyliczenie		
	1 - Udział w zajęciach -	20
	2 - Przygotowanie do realizacji projektu -	50
	3 - Przygotowanie sprawozdania ze zrealizowanego projektu -	30
	4 - Udział w konsultacjach -	2
	RAZEM:	**102**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	22 (4)+(1)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	102 (4)+(3)+(2)+(1)	4,0

Literatura podstawowa	1. Literatura do pozostałych przedmiotów z tego kierunku.	
Literatura uzupełniająca	1. Literatura do pozostałych przedmiotów z tego kierunku.	
Jednostka realizująca	Wydział Informatyki	**Data opracowania programu**
Program opracował(a)	dr inż. Maciej Brzozowski,dr inż. Eugenia Busłowska,dr inż. Andrzej Chmielewski,dr inż. Tomasz Grześ,dr inż. Ireneusz Mrozek,dr inż. Mirosław Omieljanowicz,mgr inż. Maciej Szymkowski	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Regulacyjne, strategiczne i etyczne aspekty cyberbezpieczeństwa**							**Kod przedmiotu**	**CYB_PLE**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	1
	6							**Punkty ECTS**	**1**
Przedmioty wprowadzające									
Cele przedmiotu	Wprowadzenie słuchaczy do tematyki strategicznych i regulacyjnych aspektów cyberbepzieczeństwa na poziomie krajowym i międzynarodowym (ze szczególnym naciskiem na regulacje na poziomie europejskim).								
Treści programowe	W ramach przedmiotu zostaną omówione najważniejsze kwestie z zakresu tworzenia strategii cyberbezpieczeństwa państw i tego jak wpływa ona na system cyberbezpieczeństwa na świecie. Zagadnienia te zostaną omówione na konkretnych przykładach (m.in. USA, UK, Niemcy, Francja, Izrael, Polska). Omówione zostaną najważniejsze instytucje, współpraca sektora prywatnego i publicznego oraz prawa i obowiązki poszczególnych organów wchodzących w skład systemu cyberbezpieczeństwa. Kolejne tematy będą ukierunkowane na podstawy prawne cyberbezpieczeństwa w Polsce. Przede wszystkim na kwestie związane ze Strategią Jednolitego Rynku Cyfrowego w Europie, Dyrektywą NIS oraz ustawą o krajowym systemie cyberbezpieczeństwa. Kolejnym poruszonym aspektem będzie zarządzanie kryzysowe w kontekście cyberbezpieczeństwa i współpraca pomiędzy poszczególnymi sektorami. Przedmiot zakończy się przeglądem działań jakie w zakresie cyberbezpieczeństwa prowadzą różne organizacje międzynarodowe i zastosowaniem prawa międzynarodowego w cyberprzestrzeni.								
Metody dydaktyczne	wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Kolokwium.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna prawne i strategiczne podstawy cyberbezpieczeństwa	CYB_W09
EU2	zna budowę systemu cyberbezpieczeństwa na poziomie kraju i na poziomie międzynarodowym	CYB_W09
EU3	zna zasady działania organizacji międzynarodowych w zakresie cyberbezpieczeństwa	CYB_W09
EU4	zna podstawowe zasady zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa	CYB_W09 CYB_W10
EU5	posiada wiedzę dotyczącą instytucji w Polsce odpowiadających za politykę cyberbezpieczeństwa	CYB_W09
EU6	posiada podstawową wiedzę z zakresu obowiązywania norm prawa międzynarodowego w cyberprzestrzeni	CYB_W09

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium	W
EU3	kolokwium	W
EU4	kolokwium	W
EU5	kolokwium	W
EU6	kolokwium	W

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
1 - Udział w wykładach -	6
2 - Przygotowanie do zaliczenia wykładu -	10
3 - Zapoznanie się z literaturą -	7
4 - Udział w konsultacjach -	2
RAZEM:	**25**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	8 (4)+(1)	0,3
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	0	0,0

Literatura podstawowa	1. Ustawa o krajowym systemie cyberbezpieczeństwa. 2. Ustawa o zarzadzaniu kryzysowym. 3. Dyrektywa NIS, czyli Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. 4. Rozporządzenie Ogólne o Ochronie Danych Osobowych - General Data Protection Regulation. 5. Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny. 6. Rozporządzenie Rady Ministrów w sprawie wykazu usług kluczowych oraz progów istotności skutku .zakłócającego incydentu dla świadczenia usług kluczowych. 7. ZALECENIE KOMISJI z dnia 13.9.2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę. 8. Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń. 9. Strategia Jednolitego Rynku Cyfrowego dla Europy (A Digital Single Market Strategy for Europe) - Strategia DSM. 10. Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022. 11. Diplomacy Toolbox. 12. Talin Mannual.
Literatura uzupełniająca	1. Raport Cyberbepzieczeńtrwo A.D., 2018. 2. Raporty ENISA, ONZ, NATO.
Jednostka realizująca	Naukowa i Akademicka Sieć Komputerowa (NASK)
Program opracował(a)	Magdalena Wrzosek
Data opracowania programu	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Technologie sieciowe i protokoły**							**Kod przedmiotu**	**CYB_NTP**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	2
	10				10			**Punkty ECTS**	**4**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapoznacznie słuchaczy z sieciami komputerowymi w zakresie zrozumienia funkcjonowania protokołów sieciowych, interakcji pomiędzy komponentami, czy aspektami bezpieczeństwa sieci. Jednocześnie słuchacze nabędą doświadczenia w zakresie używania narzędzi do monitorowania i analizowania sieci oraz zdobędą wiedzę na temat luk w sieci.								
Treści programowe	Wykład: Przełączanie w sieciach Ethernet. ARP i RARP. Bezpieczeństwo warstwy 2. Protokół IPv4. Adresacja IPv4, podsieci, VLSM. Protokół IPv6. Adresacja IPv6. Routing w protokołach IPv4 i IPv6. Tablice routingu i metryki. Bezpieczeństwo warstwy 3 i IPsec. Systemy nazw: DNS i NetBIOS. Analiza sieci. Rozwiązywanie problemów i narzędzie Netflow. Pracownia specjalistyczna: Przełączniki i przełączanie. ARP. Bezpieczeństwo warstwy 2. IPv4 i adresacja. IPv6 i adresacja. Routing. IPsec. Netwflow.								
Metody dydaktyczne	wykład problemowy, ćwiczenia laboratoryjne, pokaz, symulacja,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena realizacji zadań na podstawie sprawozdań.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	rozumie działanie warstwy 2 sieci (Ethernet)	CYB_W05
EU2	rozumie strukturę i zastosowanie kluczowych protokołów sieciowych (IPv4 i IPv6)	CYB_W05
EU3	zna, identyfikuje i opisuje różne najczęściej występujące zagrożenia w sieciach	CYB_W03 CYB_W04 CYB_U09
EU4	zna, identyfikuje i neutralizuje problemy dotyczące bezpieczeństwa w warstwie 2 i warstwie 3 sieci.	CYB_W04 CYB_U09
EU5	używa narzędzi do analizy i rozwiązywania problemów w sieciach	CYB_U10

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium	W
EU3	kolokwium, sprawozdania	W, Ps
EU4	kolokwium, sprawozdania	W, Ps
EU5	sprawozdania	Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Uczestnictwo w wykładach - 10h	10
2 - Uczestnictwo w pracowni specjalistycznej - 10h	10
3 - Przygotowanie do zajęć pracowni specjalistycznej - 8x4h	32
4 - Opracowanie sprawozdań - 8x4h	32
5 - Przygotowanie do kolokwium zaliczającego -	14
6 - Udział w konsultacjach -	2
RAZEM:	**100**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	22 (6)+(1)+(2)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	74 (2)+(3)+(4)	3,0

Literatura podstawowa	1. D.E. Comer, Sieci komputerowe i intersieci: kompendium wiedzy każdego administratora, Helion, 2012. 2. A. Tanenbaum, Computer Networks, Prentice Hall, Indian International Ed.; 5th edition, 2010. 3. A. Józefiok, CCNA 200-120. Zostań administratorem sieci komputerowych CISCO, Helion, 2015.
Literatura uzupełniająca	1. Dokumenty typu Request For Comments
Jednostka realizująca	Wydział Informatyki
Data opracowania programu	17 lutego 2019
Program opracował(a)	dr inż. Tomasz Grześ

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Zagrożenia w obszarze cyberbezpieczeństwa**							**Kod przedmiotu**	**CYB_CTH**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	1
	10							**Punkty ECTS**	**1**
Przedmioty wprowadzające									
Cele przedmiotu	Zapoznanie z kategoriami i rodzajami przestępstw oraz zagrożeń w cyberprzestrzeni. Opisanie różnych typów ataków i ich cech charakterystycznych.								
Treści programowe	Istota i określenie cyberterroryzmu. Motywacje i techniki. Model przeciwnika (zasoby, zdolności, zamiar, motywacja, awersja do ryzyka, dostęp). Rodzaje ataków i podatności, które je umożliwiają: łamanie haseł, backdoory, trojany, wirusy, ataki bezprzewodowe, sniffing, spoofing, przejęcie sesji, denial of service, BOTs, MAC spoofing, ataki na aplikacje internetowe, Advanced Persistent Threat (APT). Zdarzenia wskazujące na przeprowadzenie ataku. Czas ataku. Powierzchnia ataku. Ukryte kanały. Socjotechnika. Problem czynnika wewnętrznego w bezpieczeństwie. Źródła informacji o zagrożeniach. Zagadnienia prawne związane z zagrożeniami cybernetycznymi.								
Metody dydaktyczne	wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Kolokwium.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna istotę i określenie cyberterroryzmu	CYB_W03
EU2	zna kategorie i rodzaje przestępstw oraz zagrożeń w cyberprzestrzeni	CYB_W03
EU3	zna rodzaje ataków i podatności	CYB_W01 CYB_W03
EU4	wie na czym polega ochrona cyberprzestrzeni	CYB_W03

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium	W
EU3	kolokwium	W
EU4	kolokwium	W

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach -	10
2 - Przygotowanie do zaliczenia wykładu -	13
3 - Uczestnictwo w konsultacjach -	2
RAZEM:	**25**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	12 (3)+(1)	0,4
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	0	0,0

Literatura podstawowa	1. R.Maciejewski, Cyberbezpieczeństwo i bezpieczeństwo fizyczne obiektów w energetyce: wybrane aspekty badawcze, Fundacja na rzecz czystej energii, 2018 2. Opracowanie zbiorowe, Cyberbezpieczeństwo. Zarys wykładu, Wolters Kluwer, 2018	
Literatura uzupełniająca	1. Materiały podane przez prowadzącego.	
Jednostka realizująca	Wydział Informatyki	**Data opracowania programu**
Program opracował(a)	dr inż. Eugenia Busłowska	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Przedmiot wspólny**							**Profil kształcenia**	
Nazwa przedmiotu	**Zarządzanie bezpieczeństwem informacji**							**Kod przedmiotu**	**CYB_MMS**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	1
	9							**Punkty ECTS**	**1**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zdobycie podstawowych umiejętności pozwalających na zarządzanie bezpieczeństwem informacji w odniesieniu do wymagań normy ISO/IEC 27001:2014.								
Treści programowe	1. Zdobycie ogólnej wiedzy o relacjach i zawartości rodziny norm ISO/IEC 27xxx. 2. Zrozumienie znaczenia Systemu Zarządzania Bezpieczeństwem Informacji w Organizacji. 3. Wiedza umożliwiająca zaplanowanie wdrożenia SZBI w Organizacji.								
Metody dydaktyczne	wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Kolokwium.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna rodziny norm ISO/IEC 27xxxx oraz zachodzące między nimi relacje	CYB_W04 CYB_W08 CYB_W09
EU2	zna poszczególne obszary SZBI umożliwiające zarządzanie bezpieczeństwem	CYB_W08 CYB_W09 CYB_W10
EU3	zna podstawowe zasady opracowywania dokumentacji SZBI	CYB_W09
EU4	zna podstawową zasasy wykorzystywania zabezpieczeń organizacyjno proceduralnych na potrzeby innych wymagań prawnych np. KRI, KSC, RODO	CYB_W09

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium	W
EU3	kolokwium	W
EU4	kolokwium	W

Bilans nakładu pracy studenta (w godzinach)		**Liczba godz.**
Wyliczenie		
	1 - Udział w wykładach -	9
	2 - Przygotowanie do zaliczenia -	14
	3 - Udział w konsultacjach -	2
	RAZEM:	**25**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	11 (3)+(1)	0,4
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	0	0,0

Literatura podstawowa	1. PN-EN ISO/IEC 27000:2017 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia. 2. PN-EN ISO/IEC 27001:2017 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania . 3. PN-EN ISO/IEC 27002:2017 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji.
Literatura uzupełniająca	1. J. Krawiec, G. Ożarek, System Zarządzania Bezpieczeństwem Informacji w praktyce. Zabezpieczenia (Wydanie II zaktualizowane i rozszerzone), PKN, 2014.
Jednostka realizująca	Naukowa i Akademicka Sieć Komputerowa (NASK) — **Data opracowania programu**
Program opracował(a)	Dariusz Stefański — 11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Analityk Bezpieczeństwa Teleinformatycznego**							**Profil kształcenia**	
Nazwa przedmiotu	**Analiza ogólnodostępnych źródeł informacji**							**Kod przedmiotu**	**CYB_OSI**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	8				12			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapoznanie słuchaczy z metodami pozyskiwania informacji z ogólnodostępnych źródeł, w celu wykorzystania ich na potrzeby przeprowadzania białego wywiadu.								
Treści programowe	Wykład: 1. Bezpieczeństwo operacyjne podczas pozyskiwania danych z ogólnodostępnych źródeł 2. Wybrane ogólnodostępne źródła informacji 3. Metody analizy pozyskanych informacji Pracownia specjalistyczna: 1. Praktyczne wykorzystanie ogólnodostępnych źródeł informacji 2. Wykonanie analiz w ramach wybranego przypadku								
Metody dydaktyczne	wykład informacyjny, metoda przypadków, wykład problemowy,								
Forma zaliczenia	Wykład - test wielokrotnego wyboru; Pracownia specjalistyczna - prezentacja wyników przeprowadzonych analiz.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna i potrafi zastosować w praktyce metody zachowania bezpieczeństwa operacyjnego podczas procesu pozyskiwania i analizy informacji pochodzących z ogólnodostępnych źródeł	CYB_W02 CYB_W03 CYB_W09 CYB_U01 CYB_U07
EU2	zna zagrożenia wynikające z braku zastosowania środków zapewniających bezpieczeństwo operacyjne podczas procesu pozyskiwania i analizy informacji pochodzących z ogólnodostępnych źródeł	CYB_W03
EU3	zna wybrane ogólnodostępne źródła informacji i kategorie informacji, jakie można z nich pozyskać	CYB_W01
EU4	zna i potrafi zastosować w praktyce metody pozyskiwania i analizy informacji pochodzących z ogólnodostępnych źródeł	CYB_W01 CYB_U07

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	test wielokrotnego wyboru, prezentacja wyników przeprowadzonych analiz	W, PS
EU2	test wielokrotnego wyboru	W
EU3	test wielokrotnego wyboru	W
EU4	test wielokrotnego wyboru, prezentacja wyników przeprowadzonych analiz	W, Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach -	8
2 - Udział w pracowni specjalistycznej -	12
3 - Przygotowanie do zaliczenia wykladu -	10
4 - Przygotowanie analiz i prezentacji w ramach przydzielonego przypadku -	43
5 - Udział w konsultacjach -	2
RAZEM:	**75**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	22 (5)+(2)+(1)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	55 (4)+(2)	2,0

Literatura podstawowa	Materiały wskazane przez prowadzącego	
Literatura uzupełniająca	Materiały wskazane przez prowadzącego	
Jednostka realizująca	Naukowa i Akademicka Sieć Komputerowa (NASK)	**Data opracowania programu**
Program opracował(a)	Marcin Tunia	21 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Analityk Bezpieczeństwa Teleinformatycznego**							**Profil kształcenia**	
Nazwa przedmiotu	**Analiza podatności**							**Kod przedmiotu**	**CYB_VLA**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	10				6			**Punkty ECTS**	**2**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapewnienie słuchaczy zrozumienia metod analizy znalezionych podatności lub weryfikacji informacji o nich.								
Treści programowe	Wykład: 1. Najczęściej spotykane rodzaje podatności 2. Wprowadzenie do inżynierii wstecznej i debugowania kodu 3. Narzędzia wspierające analizę podatnego kodu 4. Środowisko Metasploit Framework i praca z nim Pracownia specjalistyczna: Przeprowadzanie testów bezpieczeństwa z wykorzystaniem środowiska Metasploit Framework.								
Metody dydaktyczne	wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena realizowanych zadań.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna rodzaje podatności w oprogramowaniu, scenariusze i następstwa ich wykorzystania	CYB_W01 CYB_W06
EU2	ma wiedzę o sposobach ochrony przed najpopularniejszymi rodzajami ataków oraz umie obsługiwać narzędzia wspomagające kategoryzację	CYB_W01 CYB_W04 CYB_U10
EU3	zna narzędzia i środowiska wspierające analizę podatności	CYB_W11
EU4	zna metody podstawowej inżynierii wstecznej, debugowania kodu i reprodukcji problemów	CYB_W11
EU5	posiada umiejętność samodzielnego poszukiwania informacji o podatnościach, testowania systemów pod kątem gotowych exploitów za pomocą środowiska Metasploit	CYB_U10

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium, ocena realizowanych zadań	W, Ps
EU3	kolokwium	W
EU4	kolokwium	W
EU5	ocena realizowanych zadań	Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach -	10
2 - Udział w pracowni specjalistycznej -	6
3 - Przygotowanie do zaliczenia wykładu -	10
4 - Realizacja zadań -	22
5 - Udział w konsultacjach -	2
RAZEM:	**50**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	18 (5)+(2)+(1)	0,5
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	28 (4)+(2)	1,0

Literatura podstawowa	Materiały podane przez prowadzącego.	
Literatura uzupełniająca	1. D. Kennedy, J. O'Gorman, D. Kearns, M. Aharoni, Metasploit. Przewodnik po testach penetracyjnych, Helion, 2013. 2. S. Davidoff, J. Ham, Network forensics: tracking hackers through cyberspace, Upper Saddle River: Prentice hall, 2012.	
Jednostka realizująca	Naukowa i Akademicka Sieć Komputerowa (NASK)	**Data opracowania programu**
Program opracował(a)	Kamil Frankowicz	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Analityk Bezpieczeństwa Teleinformatycznego**							**Profil kształcenia**	
Nazwa przedmiotu	**Podstawy kryminalistyki cyfrowej**							**Kod przedmiotu**	**CYB_DFS**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	10				10			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapewnienie słuchaczom umiejętności stosowania technik kryminalistycznych w całym cyklu życia dochodzenia, z naciskiem na przestrzeganie wymogów prawnych.								
Treści programowe	Wykład: 1. Zgodność z prawem a. Obowiązujące przepisy b. Oświadczenia c. Jak zeznawać d. Orzecznictwo e. Łańcuch dostaw 2. Dochodzenia cyfrowe a. E-Discovery b. Uwierzytelnienie dowodów c. Procedury kontroli pochodzenia produktu d. Metadane e. Analiza przyczyn źródłowych f. Korzystanie z maszyn wirtualnych do analizy Pracownia specjalistyczna: Praca z wykorzystaniem narzędzi DF, takich jak: EnCase, FTK, ProDiscover, Xways, SleuthKit.									
Metody dydaktyczne	wykład informacyjny, metoda przypadków, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena realizowanych zadań.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna zasady, prawa, polityki i procedury mające wpływ na kryminalistykę cyfrową	CYB_W09
EU2	potrafi użyć jednego lub więcej popularnych narzędzi DF, takich jak EnCase, FTK, ProDiscover, Xways, SleuthKit	CYB_U10
EU3	zna kolejne kroki w wykonywaniu kryminalistyki cyfrowej od początkowego rozpoznania incydentu poprzez etapy gromadzenia dowodów, ich przechowywania i analizy, poprzez zakończenie postępowania sądowego	CYB_W01 CYB_W02
EU4	zna prawne aspekty związane z bezpieczeństwem informacji	CYB_W09

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	ocena realizowanych zadań	Ps
EU3	kolokwium	W
EU4	kolokwium	W

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach -	10
2 - Udział w pracowni specjalistycznej -	10
3 - Wykonywanie zadań domowych -	38
4 - Przygotowanie do zaliczenia wykładu -	10
5 - Zapoznanie się z literaturą -	5
6 - Udział w konsutacjach -	2
RAZEM:	**75**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	22 (6)+(2)+(1)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	48 (3)+(2)	2,0

Literatura podstawowa	Materiały podane przez prowadzącego.	
Literatura uzupełniająca	1. W.A. Kasprzak, Ślady cyfrowe. Studium prawno-kryminalistyczne, Difin, 2015.	
Jednostka realizująca	Naukowa i Akademicka Sieć Komputerowa (NASK)	**Data opracowania programu**
Program opracował(a)	Agnieszka Wrońska	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Analityk Bezpieczeństwa Teleinformatycznego**							**Profil kształcenia**	
Nazwa przedmiotu	**Wprowadzenie do zarządzania incydentami**							**Kod przedmiotu**	**CYB_WZI**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	10							**Punkty ECTS**	**1**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapewnienie słuchaczom zrozumienia zagadnień i procesów obsługi incydentów cyberbezpieczeństwa.								
Treści programowe	1. Etapy zarządzania incydentem. 2. Procesy i procedury w reagowaniu na incydent. 3. Role i zadania podczas zarządzania incydentem. 4. Zarządzanie incydentem w kontekście procesów biznesowych firmy.								
Metody dydaktyczne	wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Kolokwium.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	opisuje etapy zarządzania incydentem	CYB_W04
EU2	wskazuje kluczowe czynności do wykonania podczas każdego z etapów zarządzania incydentem	CYB_W04
EU3	opisuje elementy dokumentacji w zakresie zarządzania incydentem	CYB_W04
EU4	wskazuje role i zadania w zespole reagującym na incydent	CYB_W08
EU5	opisuje relacje pomiędzy zarządzaniem incydentem a środowiskiem biznesowym	CYB_W10

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium	W
EU3	kolokwium	W
EU4	kolokwium	W
EU5	kolokwium	W

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach -	10
2 - Przygotowanie do zaliczenia -	8
3 - Zapoznanie z literaturą -	5
4 - Udział w konsultacjach -	2
RAZEM:	**25**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	12 (4)+(1)	0,4
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	0	0,0

Literatura podstawowa	Materiały podane przez prowadzącego.	
Literatura uzupełniająca	1. I. Tarnowski, Zarządzanie incydentami cyberbezpieczeństwa, PRESSCOM, 2019.	
Jednostka realizująca	Naukowa i Akademicka Sieć Komputerowa (NASK)	**Data opracowania programu**
Program opracował(a)	Przemysław Jaroszewski	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Analityk Bezpieczeństwa Teleinformatycznego**							**Profil kształcenia**	
Nazwa przedmiotu	**Zaawansowane technologie sieciowe i protokoły**							**Kod przedmiotu**	**CYB_ANT**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	10				15			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapoznanie z zaawansowanymi technologiami sieciowymi i protokołami oraz z zaawansowanymi koncepcjami sieciowymi. Przedstawione zostaną bardziej złożone problemy bezpieczeństwa związane z komunikacją sieciową.								
Treści programowe	Wykład: 1. Protokoły rutingu sieciowego (BGP, OSPF, MPLS) 2. Sieci definiowane programowo (SDN) 3. Bezpieczeństwo w protokole IPv6 4. Jakość usług (QoS) 5. Usługi sieciowe 6. Technologia VoIP 7. Multicasting 8. Zaawansowane zagadnienia bezpieczeństwa: a. bezpieczny serwer DNS b. głęboka inspekcja pakietów (ang. Deep Packet Inspection) c. protokół TLS (ang. Transport Layer Security) Pracownia specjalistyczna: 1. Konfiguracja wybranych protokołów rutingu 2. Konfiguracja wybranych usług i protokołów związanych z bezpieczeństwem								
Metody dydaktyczne	wykład problemowy, wykład informacyjny, programowanie z użyciem komputera,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena realizowanych zadań.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna i konfiguruje wybrane protokoły rutingu	CYB_W05 CYB_W11 CYB_U04 CYB_U07
EU2	zna zasady działania sieci definiowanych programowo	CYB_W05
EU3	zna zasady bezpiecznej transmisji w sieciach komputerowych z wykorzystaniem najnowszych protokołów	CYB_W03
EU4	potrafi konfigurować zaawansowane usługi podnoszące poziom bezpieczeństwa	CYB_U04 CYB_U07 CYB_U10

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium, sprawozdanie z wykonanego zadania	W, Ps
EU2	kolokwium	W
EU3	kolokwium	W
EU4	sprawozdanie z wykonanego zadania	Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach - 5x2h	10
2 - Udział w pracowni specjalistycznej - 5x3h	15
3 - Przygotowanie do zaliczenia wykładu -	10
4 - Realizacja zadań oraz przygotowywanie sprawozdań -	40
5 - Udział w konsultacjach -	2
RAZEM:	**77**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	27 (2)+(1)+(5)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	55 (4)+(2)	2,0

Literatura podstawowa	1. Dokumenty typu Request For Comments. 2. A. Tanenbaum, Computer Networks, Prentice Hall, Indian International Ed.; 5th edition, 2010. 3. D.E. Comer, Sieci komputerowe i intersieci: kompendium wiedzy każdego administratora, Helion, 2012.
Literatura uzupełniająca	1. A. Józefiok, CCNA 200-120. Zostań administratorem sieci komputerowych CISCO. Helion 2015. 2. M.A. Sportack, Routing Fundamentals, Cisco Press, 1999. 3. U. Black, IP Routing Protocols: RIP, OSPF, BGP, PNNI and Cisco Routing Protocols, Prentice Hall, 1999.

Jednostka realizująca	Wydział Informatyki	**Data opracowania programu**
Program opracował(a)	dr inż. Andrzej Chmielewski	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Analityk Bezpieczeństwa Teleinformatycznego**							**Profil kształcenia**	
Nazwa przedmiotu	**Zaawansowane zagrożenia cybernetyczne**							**Kod przedmiotu**	**CYB_CTH**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	10				20			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest wprowadzenie słuchaczy do zagadnień zaawansowanych ataków przeprowadzanych przez aktywnie działające grupy APT.								
Treści programowe	Wykład: 1. Wprowadzenie do problematyki APT, hackingu przeprowadzanego przez służby specjalne oraz cyberbroni. 2. Aktywne grupy APT i ich cele ataków. 3. Narzędzia i techniki wykorzystywane podczas ataków – backdoory, podatności 0-day, niestandardowe metody komunikacji z C&C. 4. Metody utwardzania systemów operacyjnych przed znanymi rodzajami narzędzi. 5. Wykrywanie ataków znanych grup APT. Pracownia specjalistyczna: 1. Utwardzanie systemów operacyjnych. Zabezpieczanie przed znanymi wektorami ataków grup APT. 2. Wykrywanie i identyfikowanie wykorzystywanych rozwiązań i technik podczas ataków.								
Metody dydaktyczne	programowanie z użyciem komputera, wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena realizowanych zadań.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	rozumie podstawowe zagadnienia związane z APT	CYB_W01 CYB_W09
EU2	zna aktywne grupy APT oraz ich powiązania	CYB_W01 CYB_W04
EU3	zna i stosuje narzędzia wykorzystywane przez aktorów oraz ich rodzaje	CYB_W07 CYB_U10
EU4	umie w podstawowym stopniu zabezpieczyć system operacyjny przed znanymi wektorami ataków grup APT	CYB_U02
EU5	umie w podstawowym stopniu wykrywać i identyfikować wykorzystywane rozwiązania i techniki podczas ataków	CYB_U09 CYB_U10

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium	W
EU3	kolokwium, ocena realizowanych zadań	W, Ps
EU4	ocena realizowanych zadań	Ps
EU5	ocena realizowanych zadań	Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach -	10
2 - Udział w pracowni specjalistycznej -	20
3 - Przygotowanie do zaliczenia wykładu -	10
4 - Realizacja zadań domowych -	33
5 - Udział w konsultacjach -	2
RAZEM:	**75**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	32 (5)+(1)+(2)	1,5
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	53 (2)+(4)	2,0

Literatura podstawowa	1. R. Maciejewski, Cyberbezpieczeństwo i bezpieczeństwo fizyczne obiektów w energetyce: wybrane aspekty badawcze, Fundacja na rzecz czystej energii, 2018. 2. Opracowanie zbiorowe, Cyberbezpieczeństwo. Zarys wykładu, Wolters Kluwer, 2018.
Literatura uzupełniająca	Materiały podane przez prowadzącego.
Jednostka realizująca	Naukowa i Akademicka Sieć Komputerowa (NASK)
Data opracowania programu	11 kwietnia 2019
Program opracował(a)	Kamil Frankowicz

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Inżynier Bezpieczeństwa Sieci**							**Profil kształcenia**	
Nazwa przedmiotu	**Administracja systemami Linux - LPIC-2**							**Kod przedmiotu**	**CYB_LP2**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	15				15			**Punkty ECTS**	**4**
Przedmioty wprowadzające	Koncepcje systemów operacyjnych (CYB_OSC), Podstawy programowania skryptów (CYB_BSP),								
Cele przedmiotu	Celem przedmiotu jest przygotowanie słuchaczy do administrowania systemami operacyjnymi Linux na poziomie LPIC-2.								
Treści programowe	Wykład i pracownia specjalistyczna: 1. Jądro systemu. 2. Edytory strumieniowe. 3. Zarządzanie procesami. 4. Cykliczne uruchamianie aplikacji (cron, job). 5. Zarządzanie pakietami. 6. Urządzenia w systemie Linux. 7. Zdalne systemy plików (NFS + automonter). 8. Macierze RAID. 9. Zarządzania przestrzenią pamięci masowej z wykorzystaniem LVM. 10. Konfiguracja serwera Samba. 11. SELinux. Szczegóły: https://www.lpi.org/study-resources/lpic-2-201-exam-objectives/ https://www.lpi.org/study-resources/lpic-2-202-exam-objectives/								
Metody dydaktyczne	programowanie z użyciem komputera, ćwiczenia laboratoryjne, wykład problemowy,								
Forma zaliczenia	Zaliczenie na podstawie realizowanych na zajęciach oraz w domu zadań praktycznych.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna i potrafi korzystać z funkcjonalności oferowanych przez jądro systemu	CYB_W11 CYB_U02
EU2	zna i potrafi zarządzać lokalnymi oraz zdalnymi systemami plików	CYB_W11 CYB_U02
EU3	zna zasady zabezpieczania sytemu operacyjnego Linux oraz potrafi go zabezpieczyć	CYB_W06 CYB_U02
EU4	zna i potrafi konfigurować usługi w systemie Linux	CYB_W06 CYB_U02

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium, realizacja zadań praktycznych	W, Ps
EU2	kolokwium, realizacja zadań praktycznych	W, Ps
EU3	kolokwium, realizacja zadań praktycznych	W, Ps
EU4	kolokwium, realizacja zadań praktycznych	W, Ps

Bilans nakładu pracy studenta (w godzinach)		**Liczba godz.**
Wyliczenie		
	1 - Udział w wykładach -	15
	2 - Udział w pracowni specjalistycznej -	15
	3 - Przygotowanie do zaliczenia wykładu -	10
	4 - Realizacja zadań domowych -	58
	5 - Udział w konsultacjach -	2
	RAZEM:	**100**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	32 (5)+(2)+(1)	1,5
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	73 (4)+(2)	3,0

Literatura podstawowa	1. Oficjalne materiały przygotowujące do certyfikatu LPIC-2 dostarczone przez prowadzącego. 2. Podręcznik systemowy GNU Linux.	
Literatura uzupełniająca	1. Dokumentacja systemu Debian - http://www.debian.org/doc. 2. Dokumentacja systemu Fedora - http://docs.fedoraproject.org. 3. Dokumentacja systemu SuSe - http://en.opensuse.org/Documentation.	
Jednostka realizująca	Wydział Informatyki	**Data opracowania programu**
Program opracował(a)	dr inż. Andrzej Chmielewski,mgr inż. Michał Czołombitko	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Inżynier Bezpieczeństwa Sieci**							**Profil kształcenia**	
Nazwa przedmiotu	**Administracja systemami Windows**							**Kod przedmiotu**	**CYB_WAD**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	10				10			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Słuchacz uzyskuje wiedzę i umiejętności potrzebne do wdrożenia podstawowej infrastruktury Windows Server w istniejącym środowisku przedsiębiorstwa. Przedmiot koncentruje się na zagadnieniach początkowej implementacji i konfiguracji podstawowych usług serwerowych takich jak: Active Directory Domain Services (AD DS).								
Treści programowe	Wykład i pracownia specjalistyczna: Instalacja i konfiguracja Windows Server. Infrastruktura AD DS - instalacja i konfiguracja kontrolerów domeny, - zarządzanie obiektami AD DS, - automatyzacja administracji AD DS. Implementacja opcji konfiguracyjnych magazynu w systemie Windows Server. Konfiguracja usług plikowych i drukowania w systemie Windows Server. Implementacja zasad grupy. Zabezpieczanie infrastruktury w systemie Windows Server przy użyciu obiektów zasad grupy; Technologie wirtualizacyjne Microsoft zawarte w Hyper-V.								
Metody dydaktyczne	programowanie z użyciem komputera, wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - realizacja zadań praktycznych.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	potrafi przeprowadzić instalację i konfigurację systemu operacyjnego Windows Server	CYB_U02
EU2	zna podstawowe usługi systemu operacyjnego Windows Server	CYB_W06 CYB_W11
EU3	potrafi obsługiwać system operacyjny w stopniu umożliwiającym jego nietrywialną konfigurację	CYB_U02
EU4	potrafi skonfigurować podstawowe usługi w systemie operacyjnym Windows Server	CYB_U04

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	ocena instalacji systemu	Ps
EU2	kolokwium	W
EU3	realizacja praktycznego zadania	Ps
EU4	realizacja praktycznego zadania	Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach -	10
2 - Udział w pracowni specjalistycznej -	10
3 - Realizacja zadań domowych -	43
4 - Przygotowanie do zaliczenia wykładu -	10
5 - Udział w konsultacjach -	2
RAZEM:	**75**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	22 (5)+(2)+(1)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	53 (3)+(2)	2,0

Literatura podstawowa	Dedykowania dokumentacja firmy Microsoft w języku angielskim dostępna w ramach IT Academy.
Literatura uzupełniająca	1. W. R. Stanek, Vademecum Administratora Windows Server 2012, Helion, 2012. 2. W. Stallings, Systemy operacyjne, Robomatic, 2004. 3. K. Wołk, Biblia Windows Server 2012. Podręcznik Administratora, Psychoskok, 2012. 4. A. Finn, M. Luescher, P. Lownds, Windows Server 2012 Hyper-V. Podręcznik instalacji i konfiguracji, Helion, 2012.
Jednostka realizująca	Wydział Informatyki — **Data opracowania programu**
Program opracował(a)	dr inż. Mirosław Omieljanowicz — 22 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Inżynier Bezpieczeństwa Sieci**							**Profil kształcenia**	
Nazwa przedmiotu	**Analiza ryzyka w bezpieczeństwie informacji**							**Kod przedmiotu**	**CYB_SRA**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	10							**Punkty ECTS**	**1**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zdobycie podstawowej wiedzy oraz umiejętności pozwalających na wykorzystywaniu analizy ryzyka w zarządzaniu bezpieczeństwem.								
Treści programowe	1. Zrozumienie, czym jest zarządzanie ryzykiem. 2. Poznanie poszczególnych elementów procesu zarządzania ryzykiem. 3. Umiejętność przeprowadzenia prostej analizy ryzyka.								
Metody dydaktyczne	wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Kolokwium.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna najpopularniejsze metodyki zarządzania ryzykiem	CYB_W10
EU2	zna poszczególne elementy procesu zarządzania ryzykiem	CYB_W10
EU3	zna podstawowe zasady oceny ryzyka	CYB_W10
EU4	zna podstawowe zasady wykorzystywania analizy ryzyka w zarządzaniu bezpieczeństwem np. KRI, KSC, RODO	CYB_W10

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium	W
EU2	kolokwium	W
EU3	kolokwium	W
EU4	kolokwium	W

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykladach -	6
2 - Przygotowanie do zaliczenia wykładu -	17
3 - Udział w konsultacjach -	2
RAZEM:	**25**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	8 (3)+(1)	0,3
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	0	0,0

Literatura podstawowa	1. PN-ISO/IEC 27005:2014 - Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji. 2. PN-ISO 31000:2012 Zarządzanie ryzykiem -- Zasady i wytyczne.
Literatura uzupełniająca	1. Zarządzanie ryzykiem. Przegląd wybranych metodyk (2015). Praca pod redakcją: dr inż. Dariusz Wróblewski ISBN: 978-83-61520-18-4. 2. Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych - Warszawa, 2015.
Jednostka realizująca	Naukowa i Akademicka Sieć Komputerowa (NASK) — **Data opracowania programu**
Program opracował(a)	Dariusz Stefański — 11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Inżynier Bezpieczeństwa Sieci**							**Profil kształcenia**	
Nazwa przedmiotu	**Systemy IDS/IPS**							**Kod przedmiotu**	**CYB_IDS**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	5			10				**Punkty ECTS**	**3**
Przedmioty wprowadzające	Ochrona sieci komputerowych (CYB_NDF), Podstawy bezpieczeństwa sieci i systemów IT (CYB_CSF), Podstawy kryptografii (CYB_BCY), Zagrożenia w obszarze cyberbezpieczeństwa (CYB_CTH),								
Cele przedmiotu	Celem jest zapoznanie z systemami IDS/IPS oraz nabycie umiejętności związanych z wykrywaniem i analizowaniem słabych punktów i zagrożeń oraz podejmowaniem kroków do złagodzenia powstałego ryzyka.								
Treści programowe	Wykład: 1. Dogłębna inspekcja pakietów 2. Analiza plików z logami 3. Agregacja plików z logami 4. Krzyżowe porównywanie oraz analiza plików z logami 5. Detekcja anomalii 6. Wykrywanie nadużyć w oparciu o sygnatury 7. Hostowy system wykrywania intruzów 8. Sieciowy system wykrywania intruzów 9. Rozproszona detekcja intruzów 10. Hierarchiczne systemy IDS 11. Przynęty (Honeynets/Honeypots) 12. Reakcja na intruzów Projekt: Konfiguracja wybranego systemu IDS/IPS dla zaprojektowanej sieci.									
Metody dydaktyczne	programowanie z użyciem komputera, metoda projektów, wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena sprawozdań z wykonywanych zadań praktycznych.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna i stosuje różne metody wykrywania intruzów stosowane w systemach IDS/IPS	CYB_W01 CYB_W04 CYB_U09
EU2	zna metody reakcji na wykrycie incydentów	CYB_W01 CYB_W04
EU3	potrafi skonfigurować wybrany system IDS/IPS	CYB_W04 CYB_W06 CYB_U04 CYB_U09
EU4	potrafi przygotować dokumentację techniczną wykonanego zadania	CYB_U07

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium, projekt	W, P
EU2	kolokwium	W
EU3	projekt	P
EU4	projekt	P

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
1 - Udział w wykładach -	5
2 - Udział w zajęciach projektowych -	10
3 - Realizacja projektu i przygotowanie raportu -	48
4 - Przygotowanie do zaliczenia wykładu -	10
5 - Udział w konsultacjach -	2
RAZEM:	**75**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	17 (5)+(1)+(2)	0,5
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	58 (3)+(2)	2,5

Literatura podstawowa	1. Dokumentacja pakietu Snort, https://www.snort.org. 2. Dokumentacja pakietu Suricata, https://suricata-ids.org.
Literatura uzupełniająca	1. Materiały udostępnione przez prowadzącego. 2. K.J. Cox, C. Gerg, Managing Security with Snort & IDS Tools, O'Reilly, 2009.
Jednostka realizująca	Wydział Informatyki — **Data opracowania programu**
Program opracował(a)	dr inż. Andrzej Chmielewski,dr hab. Piotr Hońko — 11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Inżynier Bezpieczeństwa Sieci**							**Profil kształcenia**	
Nazwa przedmiotu	**Testy penetracyjne**							**Kod przedmiotu**	**CYB_PTT**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	5			10				**Punkty ECTS**	**3**
Przedmioty wprowadzające	Ochrona sieci komputerowych (CYB_NDF), Podstawy bezpieczeństwa sieci i systemów IT (CYB_CSF), Podstawy kryptografii (CYB_BCY), Podstawy programowania skryptów (CYB_BSP), Podstawy sieci komputerowych (CYB_BNW), Zagrożenia w obszarze cyberbezpieczeństwa (CYB_CTH),								
Cele przedmiotu	Celem przedmiotu jest zapoznanie z metodami wykrywania różnego rodzaju podatności w celu przejęcia kontroli nad systemem.								
Treści programowe	Wykład: 1. Metodologia Flaw Hypothesis 2. Inne metodologie (np. OSSTMM) 3. Identyfikacja usterek w dokumentacji 4. Identyfikacja błędów wynikających z analizy kodu źródłowego 5. Skanowanie podatności 6. Zrozumienie rodzin ataków 7. Zrozumienie błędów, które prowadzą do luk w zabezpieczeniach 8. Rekonesans 9. Odkrywanie powierzchni ataków 10. Wektory ataków Projekt: Przeprowadzenie testów penetracyjnych dla zaprojektowanej (lub istniejącej) sieci komputerowej.								
Metody dydaktyczne	programowanie z użyciem komputera, metoda projektów, wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Projekt - przeprowadzenie testu penetracyjnego dla wybranej sieci.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna wybrane metodologie przeprowadzania testów penetracyjnych oraz potrafi je zaplanować, zorganizować i przeprowadzić w prostej sieci komputerowej	CYB_W01 CYB_W02 CYB_W03 CYB_W04 CYB_W05 CYB_W06 CYB_W09 CYB_W11 CYB_U09 CYB_U10 CYB_K01
EU2	zna podstawowe techniki socjotechniczne stosowane do pozyskiwania danych wrażliwych	CYB_W04
EU3	zna i korzysta z narzędzi stosowanych podczas testów penetracyjnych	CYB_W11 CYB_U10
EU4	potrafi przygotować raport z przeprowadzonych testów	CYB_U07

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	test zaliczeniowy, realizacja projektu	W, P
EU2	test zaliczeniowy	W
EU3	test zaliczeniowy, realizacja projektu	W, P
EU4	realizacja projektu	P

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach -	5
2 - Udział w pracowni specjalistycznej -	10
3 - Udział w konsultacjach -	2
4 - Realizacja zadań domowych oraz przygotowywanie sprawozdań -	48
5 - Przygotowanie do zaliczenia testu -	10
RAZEM:	**75**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	17 (3)+(2)+(1)	0,5
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	58 (4)+(2)	2,5

Literatura podstawowa	1. J. Muniz, A. Lakhani, Kali Linux. Testy penetracyjne, Helion 2014. 2. D. Kennedy, J. O'Gorman, D. Kearns, M. Aharoni, Metasploit. Przewodnik po testach penetracyjnych, Helion 2013. 3. Podręcznik systemowy GNU Linux.
Literatura uzupełniająca	1. Dokumentacja systemu Debian, http://www.debian.org/doc. 2. Dokumentacja systemu Fedora, http://docs.fedoraproject.org. 3. Dokumentacja systemu SuSe, http://en.opensuse.org/Documentation.

Jednostka realizująca	Wydział Informatyki	**Data opracowania programu**
Program opracował(a)	dr inż. Andrzej Chmielewski,mgr inż. Michał Czołombitko	17 lutego 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Inżynier Bezpieczeństwa Sieci**							**Profil kształcenia**	
Nazwa przedmiotu	**Zaawansowana kryptografia**							**Kod przedmiotu**	**CYB_ACR**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	10				10			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapoznanie słuchaczy z algorytmami, protokołami i ich wykorzystaniem w ochronie informacji.								
Treści programowe	Wykład: 1. Podstawy teorii liczb 2. Prawdopodobieństwo i statystyka 3. Podstawowe współczesne algorytmy kryptograficzne (AES, RSA, EC) 4. Algorytmy Suite B 5. Rodziny ataków (differential, man-in-the-middle) 6. Skróty i podpisy 7. Zarządzanie kluczami 8. Tryby działania algorytmów kryptograficznych i ich odpowiednie wykorzystanie 9. Klasyczna kryptoanaliza 10. Kryptografia oparta na identyfikacji tożsamości 11. Podpis cyfrowy 12. Wirtualne sieci prywatne 13. Kryptografia kwantowa Pracownia specjalistyczna: 1. Implementacja kryptosystemu asymetrycznego 2. Konfiguracja i wykorzystanie środowiska OpenPGP 3. Konfiguracja i wykorzystanie lokalnego ośrodka certyfikacyjnego (CA) w oparciu o narzędzia dostępne w systemie Linux									
Metody dydaktyczne	programowanie z użyciem komputera, wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Wykład: Kolokwium. Pracownia specjalistyczna - ocena wykonywanych zadań praktycznych.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna i stosuje wybrane algorytmy oraz protokoły kryptograficzne	CYB_W02 CYB_U10
EU2	zna i ocenia mechanizmy bezpieczeństwa z punktu widzenia kryptografii	CYB_W02 CYB_U01
EU3	rozumie mechanizmy kryptograficzne wykorzystywane np. w SSL, VPN czy secure storage	CYB_W02 CYB_W05
EU4	rozumie znaczenie problemu propagacji błędu w różnych trybach kryptograficznych	CYB_W02

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium, ocena realizacji zadań praktycznych	W, Ps
EU2	kolokwium, ocena realizacji zadań praktycznych	W, Ps
EU3	kolokwium	W
EU4	kolokwium	W

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
1 - Udział w wykładach -	10
2 - Udział w pracowni specjalistycznej -	10
3 - Udział w konsultacjach -	2
4 - Przygotowanie do pracowni specjalistycznej -	10
5 - Realizacja zadań domowych -	33
6 - Przygotowanie do testu zaliczeniowego -	10
RAZEM:	**75**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	22 (3)+(2)+(1)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	53 (5)+(4)+(2)	2,0

Literatura podstawowa	1. J.P. Aumasson, Nowoczesna kryptografia: praktyczne wprowadzenie do szyfrowania, PWN, 2018. 2. M. Karbowski, Podstawy kryptografii, Helion, 2014. 3. B. Schneier, Kryptografia dla praktyków, WNT, 2002. 4. D.L. Pipkin, Bezpieczeństwo informacji: ochrona globalnego przedsiębiorstwa, WNT, 2002. 5. M. Kutyłowski, W. Strothmann, Kryptografia: teoria i praktyka zabezpieczania systemów komputerowych, Wydawnictwo RM, 1999.
Literatura uzupełniająca	1. J. Kraft, An Introduction to Number Theory with Cryptography, Second Edition, CRC Press Inc, 2018. 2. M. Wrona, Niebezpieczeństwo komputerowe, Wydawnictwo RM, 2000. 3. D.R. Stinson, Cryptography. Theory And Practice, Springer-Verlag, 1995. 4. D.E. Robling-Denning, Kryptografia i ochrona danych, Wyd. II, WNT 1993. 5. N. Koblitz, Wykład z teorii liczb i kryptografii, WNT, 1995.

Jednostka realizująca	Wydział Informatyki	**Data opracowania programu**
Program opracował(a)	dr inż. Ireneusz Mrozek	11 kwietnia 2019

Wydział Informatyki									
Kierunek studiów	**Cyberbezpieczeństwo**							**Poziom i forma studiów**	**podyplomowe**
Specjalność / Ścieżka dyplomowania	**Inżynier Bezpieczeństwa Sieci**							**Profil kształcenia**	
Nazwa przedmiotu	**Zaawansowane technologie sieciowe i protokoły**							**Kod przedmiotu**	**CYB_ANT**
								Rodzaj przedmiotu	obowiązkowy
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	3
	10				15			**Punkty ECTS**	**3**
Przedmioty wprowadzające									
Cele przedmiotu	Celem przedmiotu jest zapoznanie z zaawansowanymi technologiami sieciowymi i protokołami oraz z zaawansowanymi koncepcjami sieciowymi. Przedstawione zostaną bardziej złożone problemy bezpieczeństwa związane z komunikacją sieciową.								
Treści programowe	Wykład: 1. Protokoły rutingu sieciowego (BGP, OSPF, MPLS) 2. Sieci definiowane programowo (SDN) 3. Bezpieczeństwo w protokole IPv6 4. Jakość usług (QoS) 5. Usługi sieciowe 6. Technologia VoIP 7. Multicasting 8. Zaawansowane zagadnienia bezpieczeństwa: a. bezpieczny serwer DNS b. głęboka inspekcja pakietów (ang. Deep Packet Inspection) c. protokół TLS (ang. Transport Layer Security) Pracownia specjalistyczna: 1. Konfiguracja wybranych protokołów rutingu 2. Konfiguracja wybranych usług i protokołów związanych z bezpieczeństwem									
Metody dydaktyczne	programowanie z użyciem komputera, wykład informacyjny, wykład problemowy,								
Forma zaliczenia	Wykład - kolokwium. Pracownia specjalistyczna - ocena realizowanych zadań.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna i konfiguruje wybrane protokoły rutingu	CYB_W05 CYB_W11 CYB_U04 CYB_U07
EU2	zna zasady działania sieci definiowanych programowo	CYB_W05
EU3	zna zasady bezpiecznej transmisji w sieciach komputerowych z wykorzystaniem najnowszych protokołów	CYB_W03
EU4	potrafi konfigurować zaawansowane usługi podnoszące poziom bezpieczeństwa	CYB_U04 CYB_U07 CYB_U10

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	kolokwium, sprawozdanie z wykonanego zadania	W, Ps
EU2	kolokwium	W
EU3	kolokwium	W
EU4	sprawozdanie z wykonanego zadania	Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach - 5x2h	10
2 - Udział w pracowni specjalistycznej - 5x3h	15
3 - Przygotowanie do zaliczenia wykładu -	10
4 - Realizacja zadań oraz przygotowywanie sprawozdań -	40
5 - Udział w konsultacjach -	2
RAZEM:	**77**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	27 (5)+(1)+(2)	1,0
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	55 (2)+(4)	2,0

Literatura podstawowa	1. Dokumenty typu Request For Comments. 2. A. Tanenbaum, Computer Networks, Prentice Hall, Indian International Ed.; 5th edition, 2010. 3. D.E. Comer, Sieci komputerowe i intersieci: kompendium wiedzy każdego administratora, Helion, 2012.
Literatura uzupełniająca	1. A. Józefiok, CCNA 200-120. Zostań administratorem sieci komputerowych CISCO. Helion 2015. 2. M.A. Sportack, Routing Fundamentals, Cisco Press, 1999. 3. U. Black, IP Routing Protocols: RIP, OSPF, BGP, PNNI and Cisco Routing Protocols, Prentice Hall, 1999.

Jednostka realizująca	Wydział Informatyki	**Data opracowania programu**
Program opracował(a)	dr inż. Ireneusz Mrozek	11 kwietnia 2019