

CYBERBEZPIECZEŃSTWO – studia stacjonarne I stopnia

PROGRAM STUDIÓW WYŻSZYCH ROZPOCZYNAJĄCYCH SIĘ W ROKU AKADEMICKIM 2023/2024

data zatwierdzenia przez Radę Instytutu

pieczęć i podpis Dyrektora

.....

Studia wyższe na kierunku	Cyberbezpieczeństwo
Dziedzina/y	Nauk ścisłych i przyrodniczych, nauk inżynieryjno-technicznych, nauk społecznych
Dyscyplina wiodąca (% udział)	Informatyka techniczna i telekomunikacja (55%)
Pozostałe dyscypliny (% udział)	Nauki o bezpieczeństwie (30%), Informatyka (10%), Matematyka (5%),
Poziom	PIERWSZY (studia inżynierskie I stopnia)
Profil	praktyczny
Forma prowadzenia	STUDIA stacjonarne
Specjalności	–
Punkty ECTS	210
Czas realizacji (liczba semestrów)	7
Uzyskiwany tytuł zawodowy	inżynier
Warunki przyjęcia na studia	<p>Kryteria przyjęć na studia dla kandydatów z „nową maturą”:</p> <p>Dla nowej matury: 1% = 1 punkt. O miejscu na liście rankingowej decyduje większa z liczb:</p> <ul style="list-style-type: none">• wynik (w punktach) egzaminu maturalnego z matematyki lub informatyki – poziom podstawowy, część pisemna• 2 x wynik (w punktach) egzaminu maturalnego z matematyki lub informatyki – poziom rozszerzony, część pisemna. <p>Kryteria przyjęć na studia dla kandydatów ze „starą maturą”:</p> <p>o miejscu na liście rankingowej decyduje większa z liczb:</p> <ul style="list-style-type: none">• przeliczona na punkty (według podanego poniżej przelicznika) ocena z pisemnego egzaminu dojrzałości z matematyki lub informatyki,• przeliczona na punkty (według podanego poniżej przelicznika) ocena z ustnego

CYBERBEZPIECZEŃSTWO – studia stacjonarne I stopnia

	<p>egzaminu dojrzałości z matematyki lub informatyki,</p> <ul style="list-style-type: none"> • 0,75 x przeliczona na punkty (według podanego poniżej przelicznika) ocena z egzaminu dojrzałości z jednego z przedmiotów: fizyka, chemia, – część pisemna. <p>Przelicznik ocen ze świadectw starej matury na punkty:</p> <p>Mierny- 30 punktów Dostateczny - 50 punktów Dobry - 70 punktów Bardzo dobry - 90 punktów Celujący - 100 punktów</p> <p>UWAGA: Laureaci i finaliści olimpiad stopnia centralnego będą przyjmowani na studia według obowiązującej w czasie postępowania kwalifikacyjnego Uchwały Senatu Uniwersytetu Pedagogicznego w Krakowie.</p>
--	---

Efekty uczenia się

Symbol efektu kierunkowego	Kierunkowe efekty uczenia się	Odniesienie do efektów uczenia się zgodnych z Polską Ramą Kwalifikacji	
		Symbol charakterystyk uniwersalnych I stopnia ¹	Symbol charakterystyk II stopnia ²
WIEDZA: ABSOLWENT zna i rozumie:			
K_W01	w zaawansowanym stopniu fakty i teorie stanowiące wiedzę z przedmiotów ścisłych, zwłaszcza matematyki i fizyki, niezbędną do opisu i analizy działania sieci komputerowych i urządzeń sieciowych, a także innych urządzeń zakresu technik komputerowych oraz algorytmów ich funkcjonowania	P6U_W	P6S_WG
K_W02	w zaawansowanym stopniu fakty i teorie stanowiące wiedzę w zakresie zabezpieczania architektury systemów komputerowych i urządzeń sieciowych w lokalnych i rozległych sieciach komputerowych	P6U_W	P6S_WG
K_W03	elementarne algorytmy, języki i techniki programowania oraz zasady projektowania systemów baz danych w kontekście wymagań bezpieczeństwa	P6U_W	P6S_WG
K_W04	zagadnienia dotyczące systemów informatycznych i sieci komputerowych oraz zasady ich organizacji i administracji	P6U_W	P6S_WG
K_W05	zasady działania podstawowych narzędzi kryptograficznych w kontekście zapewnienia optymalnego zabezpieczenia struktur lokalnych i sieciowych	P6U_W	P6S_WG
K_W06	zasady działania aplikacji i usług elektronicznych w Internecie i w sieciach lokalnych ze szczególnym uwzględnieniem aspektów bezpieczeństwa	P6U_W	P6S_WG
K_W07	w zaawansowanym stopniu pojęcia, struktury i procesy z zakresu cyberbezpieczeństwa (w tym zagrożenia i szanse wynikające z funkcjonowania w świecie cyfrowym wpływające na współczesne państwa, społeczeństwa, podmioty prywatne), jak również przykłady je ilustrujące oraz zależności występujące	P6U_W	P6S_WG

¹ Zgodnie z załącznikiem do ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz. U. z 2016, poz.64).

² Zgodnie z załącznikiem do rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 14 listopada 2018 r. w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji (Dz. U. z 2018 r., poz. 2218).

CYBERBEZPIECZEŃSTWO – studia stacjonarne I stopnia

	w obrębie wiedzy dotyczącej bezpieczeństwa w cyberprzestrzeni		
K_W08	w zaawansowanym stopniu prawne, techniczne, ekonomiczno-społeczne i inne uwarunkowania cyberbezpieczeństwa oraz polityki przeciwdziałania przestępczości w cyberprzestrzeni (w tym zaawansowane zasady tworzenia i rozwoju polityki bezpieczeństwa informacyjnego)	P6U_W	P6S_WK
K_W09	istotę człowieka jako podmiotu kształtującego współczesne struktury i procesy w środowisku bezpieczeństwa narodowego i międzynarodowego oraz cyberbezpieczeństwa, generującym szanse i zagrożenia dla jego przyszłości	P6U_W	P6S_WK
K_W10	główne tendencje rozwojowe, najistotniejsze nowe osiągnięcia oraz dylematy etyczne w obszarze cyberbezpieczeństwa	P6U_W	P6S_WK
UMIEJĘTNOŚCI			
ABSOLWENT potrafi:			
K_U01	korzystać z nowoczesnych narzędzi IT w zakresie planowania, budowania i eksploatacji sieci komputerowych o lokalnym i rozszerzonym zasięgu w oparciu o zasady bezpieczeństwa funkcjonowania tych struktur	P6U_U	P6S_UW
K_U02	wykorzystywać nowoczesne narzędzia technologii informacyjno-komunikacyjnych w zakresie obsługi (instalacji, konfiguracji i eksploatacji) systemów operacyjnych	P6U_U	P6S_UW
K_U03	używać dedykowanych środowisk programistycznych wraz z wybranymi bibliotekami w celu efektywnego i bezpiecznego tworzenia aplikacji desktopowych, mobilnych czy internetowych	P6U_U	P6S_UW
K_U04	konstruować algorytmy i pisać pojedyncze aplikacje oraz większe projekty programistyczne, w oparciu o języki programowania niskiego i wysokiego poziomu, z uwzględnieniem zasad bezpieczeństwa	P6U_U	P6S_UW
K_U05	indywidualnie lub w zespole pracować (m.in. opracować dokumentację, przedstawić prezentację i prowadzić dyskusję na temat zadania, projektu lub zagadnień w szczególności zw. z cyberbezpieczeństwem, również w jęz. obcym) lub planować pracę, a także komunikować się przy użyciu technik właściwych dla branży IT	P6U_U	P6S_UO
K_U06	zaplanować i przeprowadzać testy, eksperymenty i badania z dziedziny telekomunikacji i informatyki, w szczególności związane z cyberbezpieczeństwem	P6U_U	P6S_UO
K_U07	analizować i projektować protokoły, sieci i systemy teleinformatyczne, stosując właściwe metody, techniki i narzędzia oraz biorąc pod uwagę aspekty związane z bezpieczeństwem ich użytkowania	P6U_U	P6S_UW
K_U08	konfigurować urządzenia i protokoły sieciowe oraz nimi zarządzać, mając na uwadze bezpieczeństwo danych	P6U_U	P6S_UW
K_U09	dokonać analizy pod kątem bezpieczeństwa struktur krytycznych z zakresu sieci komputerowych i systemów operacyjnych	P6U_U	P6S_UW
K_U10	formułować i rozwiązywać złożone, typowe i nietypowe problemy zw. z bezpieczeństwem w cyberprzestrzeni, dobierając odpowiednie źródła informacji (również w języku obcym) oraz krytycznie je analizując i syntetyzując, a także wybierając stosowne narzędzia programistyczne, sprzętowe i sieciowe	P6U_U	P6S_UW
K_U11	prawidłowo dostrzec, ocenić i interpretować zjawiska w zakresie cyberbezpieczeństwa oraz rozwoju nowych technologii w ujęciu historycznym, politycznym, społecznym, gospodarczym, militarnym, prawnym (w tym w zakresie ochrony własności intelektualnej) i etycznym.	P6U_U	P6S_UW
K_U12	posługiwać się co najmniej jednym językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego oraz	P6U_U	P6S_UK

CYBERBEZPIECZEŃSTWO – studia stacjonarne I stopnia

	terminologią w zakresie cyberbezpieczeństwa		
K_U13	samodzielnie planować i realizować własne uczenie się oraz swój dalszy rozwój zawodowy w branży IT, w szczególności w sektorze cyberbezpieczeństwa.	P6U_U	P6S_UU
KOMPETENCJE SPOŁECZNE ABSOLWENT jest gotów do:			
K_K01	inicjowania działań na rzecz współdziałania z innymi osobami w ramach prac zespołowych i podejmowania różnych wiodących ról w interdyscyplinarnych zespołach zajmujących się analizowaniem cyberbezpieczeństwa oraz myślenia i działania w sposób przedsiębiorczy	P6U_K	P6S_KO
K_K02	krytycznej oceny poziomu swojej wiedzy oraz ciągłego dokształcania się i konsultacji z innymi ekspertami z branży IT w szczególności związanej z cyberbezpieczeństwem, a także planowania własnego rozwoju zawodowego	P6U_K	P6S_KK
K_K03	respektowania zasad etycznych i prawnych w cyberprzestrzeni oraz zobowiązań płynących z wykonywanego zawodu (w tym poszanowania prawa własności intelektualnej)	P6U_K	P6S_KR
K_K04	uznawania znaczenia tworzenia i wdrażania rozwiązań z obszaru cyberbezpieczeństwa w podnoszeniu jakości życia na świecie (na poziomie jednostki oraz zbiorowości)	P6U_K	P6S_KO
K_K05	inicjowania działań w złożonym ekosystemie podmiotów związanych z zapewnianiem cyberbezpieczeństwa – zarówno z punktu widzenia sektora prywatnego jak i publicznego	P6U_K	P6S_KO

Sylwetka absolwenta	<p>Absolwent kierunku <i>cyberbezpieczeństwo</i> uczestnicząc w procesie dydaktycznym, realizowanym za pomocą innowacyjnych metod kształcenia posiada interdyscyplinarną wiedzę z zakresu nauk inżynieryjno-technicznych, ścisłych i przyrodniczych oraz społecznych w zakresie cyberbezpieczeństwa, jak również rozumie i potrafi efektywnie analizować procesy zachodzące w środowisku cyfrowym w biznesie i podmiotach publicznych oraz osób fizycznych. Ma wiedzę z zakresu:</p> <ul style="list-style-type: none"> • kryptografii, • tworzenia, konfiguracji i wykorzystania narzędzi oraz technologii związanych z bezpieczeństwem systemów oraz sieci komputerowych lokalnych i rozległych (w celu zabezpieczania ich funkcjonowania w instytucjach publicznych oraz u wszelkiego rodzaju podmiotów prowadzących działalność gospodarczą), • działania aplikacji i usług elektronicznych w Internecie (a także w sieciach o mniejszym zasięgu, w tym lokalnych), • dostępnych rozwiązań w obszarze zabezpieczeń sieci teleinformatycznych, systemów komputerowych, aplikacji oraz projektowania tego typu systemów. <p>Ponadto zna zagrożenia cyberprzestrzeni i świata wirtualnego, w tym m.in.:</p> <ul style="list-style-type: none"> • aspekty prawne, kryminologiczne i techniczne cyberprzestępczości, • patologiczne formy korzystania z mediów i cyberprzemocy, • zagrożenia bezpieczeństwa informacyjnego. <p>Absolwent kierunku cyberbezpieczeństwo posiada umiejętności i kompetencje w zakresie:</p> <ul style="list-style-type: none"> • wykorzystania nowoczesnych narzędzi technologii informacyjno-komunikacyjnych w ramach sieci teleinformatycznych, systemów operacyjnych i technik tworzenia aplikacji, • pracy w różnego typu środowiskach programistycznych, • doboru, konfiguracji i eksploatacji specjalistycznego sprzętu sieciowego (szczególnie w zastosowaniach dotyczących projektowania i integracji systemów bezpieczeństwa), • zabezpieczania systemów teleinformatycznych przed atakami oraz dokonywania analizy struktur wrażliwych, w tym sieci komputerowych,
---------------------	---

CYBERBEZPIECZEŃSTWO – studia stacjonarne I stopnia

	<p>w kontekście ich podatności na ataki,</p> <ul style="list-style-type: none">kształtowania kultury bezpieczeństwa współczesnego człowieka, minimalizacji zagrożeń w celu zapewnienia ochrony danych osobowych, finansów, tożsamości i prywatności, zwalczania cyberprzestępczości, jak również zapobiegania patologiom cyfrowym.
Uzyskiwane kwalifikacje oraz uprawnienia zawodowe	<p>Absolwenci tego kierunku studiów mogą podjąć pracę w obszarach związanych z bezpieczeństwem w cyberprzestrzeni (sektor prywatny/publiczny), w tym:</p> <ul style="list-style-type: none">podmiotach tworzących krajowy system cyberbezpieczeństwa,w policyjnych wydziałach do walki z cyberprzestępczością, <p>jak również jako eksperci działów IT ds. bezpieczeństwa m.in. jako:</p> <ul style="list-style-type: none">administratorzy sieci komputerowych,specjaliści ds. bezpieczeństwa,analitycy i konsultanci ds. cyberbezpieczeństwa,inżynierowie bezpieczeństwa,pentesterzy,Security Software Developerzy – programiści z wiedzą nt. cyberbezpieczeństwa), <p>a także jako:</p> <ul style="list-style-type: none">edukatorzy kompetencji cyfrowych,pracownicy instytucji publicznych odpowiedzialni za cyberbezpieczeństwo oraz szkolenia w tym obszarze,pracownicy organizacji fact-checkingowych.
Dostęp do dalszych studiów	<p>Absolwenci studiów I stopnia uzyskują przygotowanie do pracy zawodowej, a także możliwość kontynuowania kształcenia na studiach II stopnia na kierunku <i>cyberbezpieczeństwo</i>, jak również pokrewnych kierunkach studiów oraz na studiach podyplomowych.</p>

Jednostka badawczo-dydaktyczna właściwa merytorycznie dla tych studiów

Instytut Bezpieczeństwa i Informatyki

CYBERBEZPIECZEŃSTWO

PLAN STUDIÓW STACJONARNYCH INŻYNIERSKICH 1-go STOPNIA 2023-2027

STUDIA ROZPOCZYNAJĄCE SIĘ W ROKU AKADEMICKIM 2023/2024

Semestr I

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Matematyka 1		30						30	zal z oc.	3
Organizacja i architektura komputerów	30			30				60	E	4
Podstawy programowania	20			30				50	E	4
Teoretyczne podstawy informatyki	25	30						55	E	6
Teoria bezpieczeństwa	15	15						30	zal	2
Ochrona własności intelektualnej							15	15	zal	1
Technologie informacyjne				30				30	zal z oc.	3
	90	75		90			15	270	3	23

Kursy do wyboru

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
<i>Języki hipertekstowe i tworzenie stron WWW*</i>	10			30				40	zal z oc.	2
<i>Systemy CMS*</i>										
<i>Przedmioty z zakresu nauk humanistycznych**</i>	30	30						60	zal z oc.	5
	40	30		30				100	0	7

Pozostałe zajęcia

rodzaj zajęć	godz.	forma zaliczenia	punkty ECTS
Szkolenie biblioteczne (e-learning)	2	zal	0
Szkolenie BHK (e-learning)	4	zal	0
	6		0

CYBERBEZPIECZEŃSTWO

Semestr II

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe							forma zaliczenia	punkty ECTS	
	W	zajęć w grupach					e-learning			razem
		A	K	L	S	P				
Matematyka 2	30	30						60	E	5
Algorytmy i struktury danych	30			30				60	zal z oc.	6
Wprowadzenie do sieci komputerowych	10			20				30	zal z oc.	3
Bazy danych 1	10			30				40	zal z oc.	2
Języki i narzędzia programowania obiektowego	10			30				40	zal z oc.	2
Środowisko cyberbezpieczeństwa	30	15						45	E	4
Teoria organizacji i zarządzania	15	15						30	zal	2
	135	60		110				305	2	24

Kursy do wyboru

nazwa kursu	godziny kontaktowe							forma zaliczenia	punkty ECTS	
	W	zajęć w grupach					e-learning			razem
		A	K	L	S	P				
Zarządzanie bezpieczeństwem informacji*	10	15						25	zal	3
Zarządzanie ryzykiem cyberbezpieczeństwa*										
Język obcy (min. poziom B2)**			40					40	zal	3
	10	15	40					65	0	6

CYBERBEZPIECZEŃSTWO

Semestr III

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe							forma zaliczenia	punkty ECTS	
	W	zajęć w grupach					e-learning			razem
		A	K	L	S	P				
Matematyka cz. III	30	30						60	E	5
Wprowadzenie do systemów operacyjnych	30			30				60	E	4
Bezpieczeństwo aplikacji internetowych 1	20			30				50	E	3
Bezpieczeństwo sieci komputerowych 1	20			30				50	E	3
Bezpieczeństwo systemów operacyjnych 1	20			30				50	zal z oc.	3
Nowe technologie w cyberprzestrzeni	20	15						35	zal	3
Ochrona danych osobowych	15	15						30	zal	3
	155	60		120				335	4	24

Kursy do wyboru

nazwa kursu	godziny kontaktowe							forma zaliczenia	punkty ECTS	
	W	zajęć w grupach					e-learning			razem
		A	K	L	S	P				
<i>Język obcy (minimum poziom B2)**</i>			40					40	zal	3
<i>Patologie w cyberprzestrzeni*</i>	15	15						30	zal	3
<i>Cyberzagrożenia*</i>										
<i>Kultura fizyczna**</i>		30						30	zal	0
	15	45	40					100	0	6

CYBERBEZPIECZEŃSTWO

Semestr IV

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe							forma zaliczenia	punkty ECTS	
	W	zajęć w grupach					e-learning			razem
		A	K	L	S	P				
Fizyczne podstawy działania urządzeń informatycznych	30							30	E	3
Bazy danych 2				30				30	zal z oc.	3
Bezpieczeństwo aplikacji internetowych 2				30				30	zal z oc.	2
Bezpieczeństwo sieci komputerowych 2				30				30	zal z oc.	3
Programowanie niskopoziomowe	15			15				30	zal z oc.	2
Programowanie skryptowe	10			30				40	zal z oc.	3
Kryptografia	30			15				45	zal z oc.	2
Zarządzanie kryzysowe w cyberbezpieczeństwie	15	20						35	E	4
Biały wywiad		20						20	zal	2
	100	40		150				290	2	24

Kursy do wyboru

nazwa kursu	godziny kontaktowe							forma zaliczenia	punkty ECTS	
	W	zajęć w grupach					e-learning			razem
		A	K	L	S	P				
Język obcy (minimum poziom B2)**			30					30	E	4
Manipulacja informacją*										
Kultura informacyjna w cyberbezpieczeństwie*		20						20	zal	2
Kultura fizyczna**		30						30	zal	0
		50	30					80	1	6

CYBERBEZPIECZEŃSTWO

Semestr V

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Bezpieczeństwo infrastruktury krytycznej i systemów sterowania przemysłowego i IoT	10			30				40	zal z oc.	3
Metodyki testów penetracyjnych 1	20			30				50	zal z oc.	3
Sprzętowe aspekty cyberbezpieczeństwa	10			20				30	zal z oc.	2
Inżynieria oprogramowania	10			20				30	zal z oc.	2
Wykrywanie anomalii sieciowych z użyciem uczenia maszynowego	10			30				40	zal z oc.	3
Wojny informacyjne	15	15						30	zal	2
Podstawy prawne cyberbezpieczeństwa	20	15						35	E	4
Zarządzanie strategiczne w cyberbezpieczeństwie	15	20						35	E	4
	110	50		130				290	2	23

Kursy do wyboru

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
<i>Komunikacja i zarządzanie projektami *</i>	15	15						30	zal z oc.	3
<i>Metody badawcze w informatyce i projektach inżynierskich*</i>										
<i>Programowanie aplikacji mobilnych*</i>	20			30				50	zal z oc.	4
<i>Tworzenie aplikacji internetowych*</i>										
	35	15		30				80	0	7

Semestr VI

Praktyki

nazwa praktyki	godz.	tyg.	forma zaliczenia	punkty ECTS
PRAKTYKA ZAWODOWA w instytucjach/firmach realizujących projekty informatyczne i z zakresu cyberbezpieczeństwa, dobranych pod kątem realizowanego kierunku. Zasady odbywania praktyk normuje Regulamin praktyk zawodowych (niepedagogicznych) Studentów Uniwersytetu Pedagogicznego im. KEN oraz Regulamin Studenckich Praktyk Zawodowych.	720	15	zal	30
	720	15		30

CYBERBEZPIECZEŃSTWO

Semestr VII

Zajęcia dydaktyczne - obligatoryjne

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
Analiza malware	10			20				30	zal z oc.	2
Analiza powłamaniowa	10			25				35	zal z oc.	2
Bezpieczeństwo sieci komputerowych 3				30				30	zal z oc.	2
Bezpieczeństwo systemów operacyjnych 2				30				30	zal z oc.	3
Metodyki testów penetracyjnych 2				30				30	zal z oc.	2
Wykrywanie incydentów				20				20	zal z oc.	2
Militarny wymiar cyberbezpieczeństwa	20	15						35	E	4
	40	15		155				210	1	17

Kursy do wyboru

nazwa kursu	godziny kontaktowe								forma zaliczenia	punkty ECTS
	W	zajęć w grupach					e-learning	razem		
		A	K	L	S	P				
<i>Analiza informacji*</i>	10			20				30	zal z oc.	2
<i>Metody eksploracji danych*</i>										
<i>Projekt inżynierski**</i>					40			40	zal z oc.	6
	10			20	40			70	0	8

Egzamin dyplomowy inżynierski

Tematyka	ECTS
Egzamin inżynierski jest pisemnym i ustnym sprawdzianem potwierdzającym osiągnięcie wybranych efektów kształcenia w zakresie wiedzy i umiejętności, realizowanych w ramach studiów. Zakres egzaminu inżynierskiego obejmuje treści przedmiotów z grupy zajęć kierunkowych.	5

^zPrzedmiot prowadzony w formie zdalnej

EN - kurs prowadzony w języku angielskim

*Kurs do wyboru – wybór z koszyka instytutowego

**Zaznaczono kursy obowiązkowe, których tematyka jest do wyboru