Politechnika Białostocka									
Kierunek studiów	**Matematyka Stosowana**							**Poziom i forma studiów**	**pierwszego stopnia inżynierskie stacjonarne**
Specjalność / Ścieżka dyplomowania	**Matematyka nowoczesnych technologii**							**Profil kształcenia**	praktyczny
Nazwa przedmiotu	**Bezpieczeństwo i integralność danych**							**Kod przedmiotu**	**MAT1BID**
								Rodzaj przedmiotu	obieralny
Forma zajęć i liczba godzin	W	Ć	L	P	Ps	T	S	**Semestr**	5
	30				30			**Punkty ECTS**	**5**
Przedmioty wprowadzające									
Cele przedmiotu	Zapoznanie studentów z podstawowymi metodami i technikami oraz zasadami, standardami i normami zabezpieczeń różnorodnych baz danych przed niepowołanym dostępem do ich zasobów, w tym ich integralności.								
Treści programowe	Wykład i pracownia specjalistyczna: Podstawowe problemy bezpieczeństwa zasobów baz danych, przestępstwa komputerowe; normy, zalecenia i certyfikaty, środki ostrożności i mechanizmy ochrony. Typowe, elementarne zagrożenia baz danych: podatność na zagrożenia systemu operacyjnego serwera bazodanowego, aplikacji komunikującej się z bazą, oprogramowania bazodanowego, problemy z kontami umożliwiającymi dostęp do bazy. Mechanizmy i techniki uwierzytelniania, autoryzacja, kontrola dostępu. Elementy kryptografii: szyfry symetryczne, szyfry asymetryczne, standardy szyfrowania, zarządzanie kluczami, funkcje skrótu, podpis cyfrowy, standardy podpisu cyfrowego, prawne aspekty wykorzystania kryptografii Mechanizmy zabezpieczeń systemów operacyjnych i typowe naruszenia ich bezpieczeństwa, Mechanizmy zabezpieczeń infrastruktury sieciowej: bezpieczeństwo podstawowych protokołów, narzędzia podnoszące poziom bezpieczeństwa sieci. Bezpieczeństwo aplikacji użytkowych i usług: ochrona popularnych usług aplikacyjnych (WWW, poczta elektroniczna, komunikatory internetowe). Środowiska o podwyższonym bezpieczeństwie: interfejs usług bezpieczeństwa, bazy danych o podwyższonym bezpieczeństwie.								
Metody dydaktyczne	programowanie z użyciem komputera, wykład informacyjny, klasyczna metoda problemowa, wykład problemowy,								
Forma zaliczenia	Wykład - egzamin pisemny; Pracownia specjalistyczna - ocena wykonanych projektów i aktywności na zajęciach.								

Symbol efektu uczenia się	**Zakładane efekty uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**
EU1	zna podstawowe zagrożenia dla bezpieczeństwa baz danych oraz metody i techniki ich zabezpieczeń	K_W10 K_W12
EU2	zna standardy rozwiązań kryptograficznych służących zabezpieczeniom zasobów komputerowych	K_W11 K_W14
EU3	potrafi zaprojektować, wdrożyć i przetestować zabezpieczenia sieci i danych	K_U10 K_U14 K_U17
EU4	rozpoznaje zagrożenia dla bezpieczeństwa konkretnych zasobów bazodanowych	K_U10 K_U17

Symbol efektu uczenia się	**Sposób weryfikacji efektu uczenia się**	**Forma zajęć na której zachodzi weryfikacja**
EU1	egzamin	W
EU2	egzamin	W
EU3	ocena projektów w ramach pracowni specjalistycznej	Ps
EU4	ocena projektów w ramach pracowni specjalistycznej	Ps

Bilans nakładu pracy studenta (w godzinach)	**Liczba godz.**
Wyliczenie	
1 - Udział w wykładach -	15
2 - Udział w pracowni specjalistycznej -	45
3 - Realizacja zadań domowych -	45
4 - Udział w konsultacjach -	5
5 - Przygotowanie do egzaminu -	14
6 - Obecność na egzaminie -	2
RAZEM:	**126**

Wskaźniki ilościowe	**GODZINY**	**ECTS**
Nakład pracy studenta związany z zajęciami wymagającymi bezpośredniego udziału nauczyciela	67 (6)+(4)+(2)+(1)	2,7
Nakład pracy studenta związany z zajęciami o charakterze praktycznym	90 (3)+(2)	3,6

Literatura podstawowa	1. J. Stokłosa, T. Bilski, T. Pankowski, Bezpieczeństwo danych w systemach informatycznych, Wydaw. Naukowe PWN , Warszawa 2001. 2. K. Kenan, Kryptografia w bazach danych. Ostatnia linia obrony, Wydaw. Naukowe PWN, Warszawa 2007. 3. A. J. Menezes, P. C. Oorschot, S.A. Vanstone, Kryptografia stosowana, WNT, Warszawa 2009. 4. J. Pieprzyk, T. Hardjono, J. Seberry, Teoria bezpieczeństwa systemów komputerowych, Wydawnictwo Helion, Warszawa 2006.
Literatura uzupełniająca	1. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Matematyka szyfrów i techniki kryptologii, Wydawnictwo Helion, Warszawa 2013. 2. N. Koblitz, Algebraiczne aspekty kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 2000. 3. N. Koblitz, Wykład z teorii liczb i kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 2006. 4. D. R. Stinson, Kryptografia w teorii i w praktyce, Wydawnictwa Naukowo-Techniczne, Warszawa 2005.

Jednostka realizująca	Katedra Informatyki Teoretycznej	**Data opracowania programu**
Program opracował(a)	dr hab. Czesław Bagiński	5 kwietnia 2019