

Sylabus przedmiotu / modułu kształcenia		
Nazwa przedmiotu/modułu kształcenia:		Bezpieczeństwo i zarządzanie bazami danych
Nazwa w języku angielskim:	Security and database management	
Język wykładowy:	polski	
Kierunek studiów, dla którego przedmiot jest oferowany:		Bezpieczeństwo informacyjne
Jednostka realizująca:	Wydział Nauk Społecznych	
Rodzaj przedmiotu/modułu kształcenia (obowiązkowy/fakultatywny):		obowiązkowy
Poziom modułu kształcenia (np. pierwszego lub drugiego stopnia):		pierwszego stopnia
Rok studiów:	drugi	
Semestr:	trzeci	
Liczba punktów ECTS:	2	
Imię i nazwisko koordynatora przedmiotu:		dr Piotr Świtalski
Imię i nazwisko prowadzących zajęcia:		dr Piotr Świtalski
Założenia i cele przedmiotu:		Celem przedmiotu jest zaznajomienie studentów z problematyką bezpieczeństwa baz danych w systemach informatycznych. W założeniach do tego przedmiotu przewiduje się zajęcia praktyczne z użyciem komputerów, podczas których studenci nabędą umiejętności z zabezpieczeniem systemów baz danych oraz ich zarządzaniem. Ma również usystematyzować wiedzę w zakresie standardów bezpieczeństwa.
Symbol efektu	Efekt uczenia się: WIEDZA	Symbol efektu kierunkowego
W_01	Zna i rozumie zagadnienia z zakresu bezpieczeństwa systemów komputerowych w zakresie zarządzania bazami danych	K_W01
W_02	Zna i rozumie sposoby gromadzenia i przechowywania danych w bazach danych. Zna różne rodzaje systemów baz danych i sposoby ich zabezpieczeń.	K_W09
W_03	Zna i rozumie techniki związane z atakami na systemy komputerowe w tym na bazy danych i potrafi im przeciwdziałać	K_W05
Symbol efektu	Efekt uczenia się: UMIEJĘTNOŚCI	Symbol efektu kierunkowego
U_01	Potrafi zidentyfikować zagrożenia skutkujące utratą integralności i spójności bazy danych.	K_U03

U_02	Potrafi sprawnie wykorzystać narzędzia bezpieczeństwa systemów komputerowych w zakresie baz danych.	K_U04
U_03	Potrafi dobrać adekwatne zabezpieczenia w stosunku do zagrożenia w systemie komputerowym.	K_U04
Forma i typy zajęć:		studia stacjonarne: ćwiczenia laboratoryjne (30 godz.) studia niestacjonarne: ćwiczenia laboratoryjne (18 godz.)
Wymagania wstępne i dodatkowe:		
Warunkiem uczestnictwa w zajęciach jest podstawowa znajomość systemów operacyjnych Windows oraz Linuks.		
Treści modułu kształcenia:		
Wstęp do relacyjnych baz danych. Pojęcie relacji. Typy relacji. Projektowanie bazy danych. Typy danych. Normalizacja bazy danych. Pojęcie integralności oraz spójności bazy danych. Podstawy relacyjnych baz danych cz. 1. Język SQL. Tworzenie bazy danych. Klauzula CREATE. Atrybuty. Wprowadzanie danych do bazy danych. Typowe błędy popełniane przy tworzeniu bazy danych. Podstawy relacyjnych baz danych cz. 2. Wybieranie danych z bazy danych. Klauzula WHERE. Modyfikacja danych. Modyfikacja struktury bazy danych. Klauzula ALTER. Zarządzanie relacyjną bazą danych. Mechanizmy uwierzytelniania w systemach baz danych. Zarządzanie użytkownikami w bazach danych i konfiguracja dostępu do danych. Poufność danych w bazach danych. Monitorowanie aktywności w bazach danych. Wstęp do nierelacyjnych baz danych. Rodzaje nierelacyjnych baz danych. Typowe różnice między relacyjnymi oraz nierelacyjnymi bazami danych. Modelowanie nierelacyjnych baz danych. Bazy danych dokumentowe i bazy danych grafowe. Nierelacyjne bazy danych: MongoDB cz. 1. Powłoka MongoDB, import danych, zapytania, skrypty powłoki. Wybieranie danych z bazy danych. Typowe operatory. Nierelacyjne bazy danych: MongoDB cz. 2. Operacje CRUD. Modelowanie danych w bazie MongoDB. Przykłady relacji w MongoDB. Modyfikacja danych w kolekcji. Nierelacyjne bazy danych: MongoDB cz. 3. Metody agregacji danych. Potok agregacji. Operatory potoku agregacji. Operatory akumulujące. Operatory łańcuchowe. Nierelacyjne bazy danych: Neo4J cz. 1. Definiowanie modelu danych w Neo4J. Tworzenie węzłów oraz relacji. Wyszukiwanie danych. Modyfikacja danych. Modyfikacja węzłów i relacji. Import danych. Nierelacyjne bazy danych: Neo4J cz. 2. Klauzule MATCH i WHERE. Wyszukiwanie najkrótszej ścieżki. Klauzula RETURN i funkcje agregujące. Podśluchiwanie ruchu sieciowego. Metody podsłuchiwania ruchu sieciowego. Narzędzia do realizacji podsłuchu ruchu sieciowego. Przykładowe realizacje podsłuchu. Łamanie haseł. Programy wykorzystywane do łamania haseł. Łamanie haseł systemu Linuks. Łamanie haszy w programie hashcat. Ataki na bazy danych. Wykonanie ataków wstrzykiwania złośliwego kodu do aplikacji internetowych. Atak SQL Injection. Atak Blind SQL Injection. Atak trwały XSS. Atak odbity XSS. Zapory sieciowe. Zasady tworzenia reguł firewalla iptables. Przykładowe reguły. Konfiguracja zapory sieciowej. Filtrowanie ruchu sieciowego. Blokowanie portów serwera bazy danych. Kopie bezpieczeństwa baz danych. Metody tworzenia kopii bezpieczeństwa w systemach komputerowych. Metody automatyzacji procesu tworzenia kopii bezpieczeństwa. Program rsync. Zrzuty bazy danych. Przywracanie zawartości bazy danych.		

Literatura podstawowa:	
1. Vinicius M. Grippa, Sergey Kuzmichev, MySQL. Jak zaprojektować i wdrożyć wydajną bazę danych. Wydanie II. Wyd. Helion, Gliwice, 2022. 2. Sadalage P.J., Fowler M.: NoSQL. Kompendium wiedzy. Wyd. Helion, Gliwice, 2015. 3. Stallings W.: Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji, Wyd. Helion, Gliwice, 2012.	
Literatura dodatkowa:	
1. Prasad P.: Testy penetracyjne nowoczesnych serwisów. Kompendium inżynierów bezpieczeństwa, Wyd. Helion, Gliwice, 2017. 2. Harrison G.: NoSQL, NewSQL i BigData. Bazy danych następnej generacji, Wyd. Helion, Gliwice, 2019.	
Planowane formy/działania/metody dydaktyczne:	
Ćwiczenia laboratoryjne – zajęcia praktyczne z wykorzystaniem wybranych narzędzi programowych. Na stronie internetowej prowadzącego zamieszczane są materiały z problemami i zadaniami laboratoryjnymi.	
Sposoby weryfikacji efektów uczenia się osiąganym przez studenta:	
Weryfikacja efektów w zakresie wiedzy będzie prowadzona w toku weryfikacji przygotowania do kolejnych zajęć laboratoryjnych. Student będzie oceniany w zakresie przygotowania do zajęć w postaci krótkich testów sprawdzających. Weryfikacja efektów w zakresie umiejętności będzie realizowana systematycznie na zajęciach laboratoryjnych. Student otrzyma zadania do wykonania w postaci problemów do rozwiązania lub zadań o charakterze projektowym. Student będzie musiał wykazać poprawność przygotowanego rozwiązania.	
Forma i warunki zaliczenia:	
Na ocenę z zajęć składają się oceny cząstkowe uzyskane na regularnych zajęciach z nauczycielem akademickim, za które można uzyskać sumarycznie 100 pkt. Zaliczenie zajęć laboratoryjnych możliwe po uzyskaniu co najmniej 51% liczby punktów z tej formy zaliczenia. Ocena końcowa z przedmiotu, w zależności od sumy uzyskanych punktów (maksymalnie 100 pkt) jest następująca (w nawiasach ocena wg skali ECTS): • 0 – 50 pkt: niedostateczna (F), • 51 – 60 pkt: dostateczna (E), • 61 – 70 pkt: dostateczna plus (D), • 71 – 80 pkt: dobra (C), • 81 – 90 pkt: dobra plus (B), • 91 – 100 pkt: bardzo dobra (A).	
Bilans punktów ECTS:	
Studia stacjonarne	
Aktywność	Obciążenie studenta
Ćwiczenia	30 godz.
Konsultacje	5 godz.

Studiowanie literatury	5 godz.
Przygotowanie do ćwiczeń laboratoryjnych	10 godz.
Sumaryczne obciążenie pracą studenta	50 godz.
Punkty ECTS za przedmiot	2 ECTS
Studia niestacjonarne	
Aktywność	Obciążenie studenta
Ćwiczenia	18 godz.
Konsultacje	7 godz.
Studiowanie literatury	5 godz.
Przygotowanie do ćwiczeń laboratoryjnych	20 godz.
Sumaryczne obciążenie pracą studenta	50 godz.
Punkty ECTS za przedmiot	2 ECTS