Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2019/2020

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma sudiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo dla licencjatów

1 Informacje o przedmiocie

Nazwa przedmiotu	Przetwarzanie i ochrona danych typu Big Data
Nazwa przedmiotu w języku angielskim	Processing and protection of the Biga Data systems
Kod przedmiotu	WIiT I oIIS D13 19/20
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	5.00
Semestry	3

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
3	30	0	15	0	0	0

3 Cele przedmiotu

Cel 1 Zapoznanie studentów z podstawowymi pojęciami i metodami bezpieczeństwa systemów typu Big Data

Cel 2 Zapoznanie studentów z podstawowymi algorytmami zabezpieczania danych Big Data

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 zaliczenie przedmiotów: algebra, matematyka dyskretna

5 Efekty kształcenia

EK1 Wiedza Student zna podstawowe pojęcia z zakresu bezpieczeństwa danych w systemach Big Data

EK2 Umiejętności Student potra zrealizować podstawowe metody z zakresu zabezpieczania systemów Big Data

EK3 Kompetencje społeczne Student posiada umiejętności pracy w grupie, umiejętności komunikacji z nauczycielem, oraz organizacji pracy w grupie. Student posiada umiejętności komunikacji ze środowiskiem poza uczelnianym w celu popularyzacji wiedzy uzyskanej w ramach nauki oraz prezentacji wyników swoich badań w sposób zrozumiały i czytelny.

EK4 Wiedza Student zna podstawowe pojęcia z zakresu bezpieczeństwa systemów Big Data

6 Treści programowe

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Wstęp do systemów Big Data , charakterystyka i własności	2
W2	Łańcuch odpowiedzialności za bezpieczeństwo w systemach Big Data	2
W3	Bezpieczeństwo danych w odniesieniu do: volume - ilość danych, variety - różnorodność danych, velocity - szybkość napływania nowych danych i ich analizy,value - wartość informacji.	2
W4	Bezpieczeństwo rozproszonych systemów plików oraz baz danych typu NOSQL	2
W5	Anonimizacja, z zarządzania dostępem w systemach Biga Data	2
W6	Bezpieczne przechowywania bloków danych	2
W7	Bezpieczne przeszukiwanie	2
W8	Bezpieczne przetwarzanie danych typu Big Dat	2
W9	Obliczenia współdzielone	2
W10	Szyfrowanie funkcjonalne	2
W11	Automatyzacja strategii obronnych w systemach typu Big Data	2
W12	Prezentacja praktycznych przykładów zabezpieczania poufności danych poprzez anonimizację oraz wybranych algorytmów kryptografii grupowe	2
W13	Prezentacja praktycznych przykładów szyfrowania danych typu Big Data umożliwiających przeszukiwanie oraz wybranych algorytmów kryptografii ślepej	2

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W14	Międzynarodowe standardy i normy dotyczące zapewniania bezpieczeństwa systemów Big Data, organy certyfikujące systemy Big Data	2
W15	Podsumowanie	2

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Wprowadzenie do środowiska Apache Spark. Instrukcja użycia, podstawowe operacje i definicje	2
L2	Podatności dotyczące bezpieczeństwa w Apache Spark. Lista oraz praktyczne przykłady najważniejszych luk bezpieczeństwa Apache Spark.	2
L3	Spark RPC. Bezpieczna komunikacja pomiędzy procesami w Apache Spark. Szyfrowanie i autentykacja. Szyfrowanie lokalnych danych	2
L4	Apache Spark ACL do celów autentykacji. Konfiguracja SSL do bezpieczeń komunikacji w sieci. Domyślne i specyficzne dla protokołu ustawienia SSL	2
L5	Port Security, Key Storing, aplikacja keytool. Narzędzia HTTP X-XSS-Protection i HTTP Strict Transport Security (HSTS).	2
L6	Apache Kerberos. Założenie serwisu Kerberos i jego użycie w Apache Spark do autentykacji	2
L7	Wykrywanie ataku DDoS z użyciem Apache Spark i metod uczenia maszynowego.	2
L8	Podsumowanie	1

7 Narzędzia dydaktyczne

N1 Ćwiczenia laboratoryjne

N2 Dyskusja

N3 Wykłady

N4 Konsultacje

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	45
Konsultacje przedmiotowe	5
Egzaminy i zaliczenia w sesji	5
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	5
Opracowanie wyników	5
Przygotowanie raportu, projektu, prezentacji, dyskusji	5
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**70**
Sumaryczna liczba punktów ECTS dla przedmiotu	5.00

9 Sposoby oceny

Ocena formująca

F1 Ćwiczenie praktyczne

F2 Odpowiedź ustna

F3 Sprawozdanie z ćwiczenia laboratoryjnego

Ocena podsumowująca

P1 Średnia ważona ocen formujących

P2 Test

Warunki zaliczenia przedmiotu

W1 Zaliczenie ćwiczeń mogą uzyskać studenci, którzy regularnie uczęszczali na ćwiczenia

W2 Ocena końcowa jest średnią z ocen P1-P2.

Ocena aktywności bez udziału nauczyciela

B1 Podstawą oceny aktywności bez udziału nauczyciela jest ocena przygotowanego przez studenta sprawozdania z laboratorium

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie zna ogólnych zasad dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania oraz nie potrafi scharakteryzować środowisk Big Data w kontekście bezpieczeństwa danych. Student nie potrafi wymienić ani jednego przykładu z ww zagadnień,
Na ocenę 3.0	Student zna ogólne zasady dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania oraz potrafi scharakteryzować środowiska Big Data w kontekście bezpieczeństwa danych. Student potrafi wymienić po jednym przykładzie z ww zagadnień,
Na ocenę 3.5	Student zna ogólne zasady dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania oraz potrafi scharakteryzować środowiska Big Data w kontekście bezpieczeństwa danych, zarządzania użytkownikami oraz obsługi baz typu NoSQL Student potra podać różne przykłady dla każdego wymienionego zagadnienia.
Na ocenę 4.0	Student zna szczegółowo zasady dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania oraz potrafi scharakteryzować środowiska Big Data w kontekście bezpieczeństwa danych, zarządzania użytkownikami oraz obsługi baz typu NoSQL Student potra podać różne przykłady dla każdego wymienionego zagadnienia.
Na ocenę 4.5	Student zna ogólne zasady dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania oraz potrafi scharakteryzować środowiska Big Data w kontekście bezpieczeństwa danych, zarządzania użytkownikami oraz obsługi baz typu NoSQL Student potra podać różne przykłady dla każdego wymienionego zagadnienia. Potra podać oraz rozumie matematyczne podstawy wybranych metod zabezpieczania danych typu Big Data.
Na ocenę 5.0	Student zna ogólne zasady dotyczących zagrożeń bezpieczeństwa oraz zabezpieczania oraz potrafi scharakteryzować środowiska Big Data w kontekście bezpieczeństwa danych, zarządzania użytkownikami oraz obsługi baz typu NoSQL Student potra podać różne przykłady dla każdego wymienionego zagadnienia. Potra podać oraz rozumie matematyczne podstawy wybranych metod zabezpieczania danych typu Big Data. Student potrafi dobrać metody zabezpieczania ww środowisk do konkretnych przykładów przetwarzania danych typu Big Data.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie jest w stanie pracować na danych typu Big Data w środowisku Apache Spark. Student nie zna podstaw dotyczących bezpieczeństwa oraz podatności w środowisku Apache Spark.
Na ocenę 3.0	Student jest w stanie pracować na danych typu Big Data w środowisku Apache Spark. Student zna podstawy dotyczące bezpieczeństwa oraz podatności w środowisku Apache Spark. Student nie potrafi użyć narzędzi praktycznych służących do zapewnienia bezpieczeństwa.
Na ocenę 3.5	Student jest w stanie pracować na danych typu Big Data w środowisku Apache Spark. Student zna podstawy dotyczące bezpieczeństwa oraz podatności w środowisku Apache Spark. Student potrafi zapewnić bezpieczną komunikację między procesami z użyciem RPC w środowisku Apache Spark. Student jest w stanie zapewnić autentykację z użyciem ACL.

Na ocenę 4.0	Student jest w stanie pracować na danych typu Big Data w środowisku Apache Spark. Student zna podstawy dotyczące bezpieczeństwa oraz podatności w środowisku Apache Spark. Student potrafi zapewnić bezpieczną komunikację między procesami z użyciem RPC w środowisku Apache Spark. Student jest w stanie zapewnić autentykację z użyciem ACL. Student potrafi skonfigurować protokół SSL do bezpiecznej komunikacji w sieci oraz potrafi rozróżnić ustawienia domyślne SSL od specyficznych dla protokołu.
Na ocenę 4.5	Student jest w stanie pracować na danych typu Big Data w środowisku Apache Spark. Student zna podstawy dotyczące bezpieczeństwa oraz podatności w środowisku Apache Spark. Student potrafi zapewnić bezpieczną komunikację między procesami z użyciem RPC w środowisku Apache Spark. Student jest w stanie zapewnić autentykację z użyciem ACL. Student potrafi skonfigurować protokół SSL do bezpiecznej komunikacji w sieci oraz potrafi rozróżnić ustawienia domyślne SSL od specyficznych dla protokołu. Student potrafi użyć narzędzia Port Security oraz potrafi prawidłowo generować i przechowywać klucze kryptograficzne. Student potrafi użyć HTTP X-XSS-Protection oraz HTTP Strict Transport Security.
Na ocenę 5.0	Student jest w stanie pracować na danych typu Big Data w środowisku Apache Spark. Student zna podstawy dotyczące bezpieczeństwa oraz podatności w środowisku Apache Spark. Student potrafi zapewnić bezpieczną komunikację między procesami z użyciem RPC w środowisku Apache Spark. Student jest w stanie zapewnić autentykację z użyciem ACL. Student potrafi skonfigurować protokół SSL do bezpiecznej komunikacji w sieci oraz potrafi rozróżnić ustawienia domyślne SSL od specyficznych dla protokołu. Student potrafi użyć narzędzia Port Security oraz potrafi prawidłowo generować i przechowywać klucze kryptograficzne. Student potrafi użyć HTTP X-XSS-Protection oraz HTTP Strict Transport Security. Student potrafi założyć serwer Kerberos w celach autentykacji użytkowników. Student potrafi symulować atak DDoS oraz pokazać jak się przed nim zabezpieczyć w środowisku Apache Spark z użyciem metod uczenia maszynowego opisanych i pokazanych na laboratoriach.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie potrafi samodzielnie, bądź w grupie wykonać zadań praktycznych. Nie wykonuje poleceń nauczyciela, nie potrafi wykonać poleceń uzgodnionych z grupa
Na ocenę 3.0	Student potrafi samodzielnie wykonać zadania praktyczne. Student wykonuje polecenia nauczyciela, uczęszcza na zajęcia, potrafi wykonać polecenia uzgodnione z grupą.
Na ocenę 3.5	Student potrafi samodzielnie wykonać zadania praktyczne. Student wykonuje polecenia nauczyciela, uczęszcza na zajęcia, potrafi wykonać polecenia uzgodnione z grupą. Student jest aktywny na zajęciach, bierze udział w dyskusjach grupowych.
Na ocenę 4.0	Student potrafi samodzielnie wykonać zadania praktyczne. Student wykonuje polecenia nauczyciela, uczęszcza na zajęcia, potrafi wykonać polecenia uzgodnione z grupą. Student jest aktywny na zajęciach, bierze udział w dyskusjach grupowych. Student potrafi pracować w małej grupie.

Na ocenę 4.5	Student potrafi samodzielnie wykonać zadania praktyczne. Student wykonuje polecenia nauczyciela, uczęszcza na zajęcia, potrafi wykonać polecenia uzgodnione z grupą. Student jest aktywny na zajęciach, bierze udział w dyskusjach grupowych. Student potrafi kierowac praca małej grupy.
Na ocenę 5.0	Student potrafi samodzielnie wykonać zadania praktyczne. Student wykonuje polecenia nauczyciela, uczęszcza na zajęcia, potrafi wykonać polecenia uzgodnione z grupą. Student jest aktywny na zajęciach, bierze udział w dyskusjach grupowych. Student potrafi kierowac praca małej grupy, potrafi w sposób zrozumiały przedstawiać wyniki jej pracy oraz rozwiązywać w sposób kreatywny powstałe podczas pracy problemy.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie potrafi wymienić ani jednego przykładu prezentowanych zagadnień,
Na ocenę 3.0	Student zna ogólne zasady dotyczących zagrożeń bezpieczeństwa systemów Big Data. Student potrafi wymienić po jednym przykładzie z ww zagadnień,
Na ocenę 3.5	Student zna ogólne zasady dotyczących zagrożeń bezpieczeństwa systemów Big Data. Student potrafi wymienić kilka przykładów z ww zagadnień,
Na ocenę 4.0	Student zna szczegółowo zasady dotyczących zagrożeń bezpieczeństwa środowiska Big Data potra podać różne przykłady dla każdego wymienionego zagadnienia.
Na ocenę 4.5	Student zna szczegółowo zasady dotyczących zagrożeń bezpieczeństwa środowiska Big Data potra podać różne przykłady dla każdego wymienionego zagadnienia nz przykładzie konkretnych środowisk, omawianych na wykładzie.
Na ocenę 5.0	Student zna szczegółowo zasady dotyczących zagrożeń bezpieczeństwa środowiska Big Data potra podać różne przykłady dla każdego wymienionego zagadnienia nz przykładzie konkretnych środowisk, omawianych na wykładzie oraz najpopularniejszych rozwiązań komercyjnych,

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I2_W01 I2_W08	Cel 1 Cel 2	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11 W12 W13 W14 W15 L1 L2 L3 L4 L5 L6 L7 L8	N1 N2 N3 N4	F1 F2 F3 P1 P2

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK2	I2_U12	Cel 1 Cel 2	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11 W12 W13 W14 W15 L1 L2 L3 L4 L5 L6 L7 L8	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK3	I2_K01	Cel 1 Cel 2	L1 L2 L3 L4 L5 L6 L7 L8	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK4	I2_W05	Cel 1 Cel 2	W10 W11 W12 W13 W14 W15 L7 L8	N1 N2 N3 N4	F1 F2 F3 P1 P2

11 Wykaz literatury

Literatura podstawowa

[1] ThomasErl, WajidKhattak, andPaulBuhler — *BigDataFundamentals Concepts,Drivers&Techniques*, -, 0, -

[2] Dehghantanha, Ali, Choo, Kim-Kwang Raymond — *Handbook of Big Data and IoT Security*, -, 0, -

[3] Hrushikesha Mohanty Prachet Bhuyan Deepak Chenthati — *Big Data A Primer*, -, 0, -

[4] Arnab Roy — *SECURITY AND PRIVACY OF BIG DATA: A NIST WORKING GROUP PERSPECTIVE*, -, 0, -

Literatura uzupełniająca

[1] Hang-Jung Hsieh, Ting-Yuan Chan — *DETECTION DDOS ATTACKS BASED ON NEURAL-NETWORK USING APACHE SPARK*, -, 0, -

[2] https://www.cvedetails.com — *CVE DETAILS, THE ULTIMATE SECURITY AND VULNERABILITY DATASOURCE*, -, 0, -

[3] https://spark.apache.org/ — *APACHE SPARK Lightning-fast unified analytics engine, documentation and libraries.*, -, 0, -

[4] https://www.oracle.com — *ORACLE JAVA SE DOCUMENTATION*, -, 0, -

[5] https://docs.microsoft.com/pl-pl/system-center/scom/manage-linux-kerberos-auth — *OBSŁUGA UWIERZYTELNIANIA KERBEROS DLA KOMPUTERÓW Z SYSTEMAMI UNIX I LINUX,*, Miejscowość, 0, -

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr Agnieszka Jakóbik (kontakt: akrok@pk.edu.pl)

Osoby prowadzące przedmiot

1 Dr Agnieszka Jakóbik (kontakt: ajakobik@pk.edu.pl)

2 Mgr Jacek Tchórzewski (kontakt: jacek.tchorzewski@pk.edu.pl)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)

Przyjmuję do realizacji (data i podpisy osób prowadzących przedmiot)

. . . . . .

. . . . . .