Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2021/2022

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma sudiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo przemysłowych systemów transmisji danych
Nazwa przedmiotu w języku angielskim	Securityof industrial transmission systems
Kod przedmiotu	WIiT I oIIS D9 21/22
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	3.00
Semestry	3

2 Rodzaj zajęć, liczba godzin w planie studiów

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

3 Cele przedmiotu

Cel 1 Zapoznanie studentów z głównymi zagrożeniami wobec sieci przemysłowych oraz metodami reagowania przeciwdziałania

Cel 2 Zapoznanie studentów z metodami analizy zagrożeń wobec sieci przemysłowych oraz metodami działania zespołów reagowania i przeciwdziałania

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Zaliczenie przedmiotu Sieci komputerowe

5 Efekty kształcenia

EK1 Wiedza Student objaśnia podstawowe pojęcia dotyczące zagrożeń w systemach przemysłowych

EK2 Wiedza Student objaśnia podstawowe pojęcia dotyczące reagowania i przeciwdziałania zagrożeniom bezpieczeństwa w przemyśle

EK3 Umiejętności Student potrafi zrealizować podstawowe metody z zakresu poprawy bezpieczeństwa systemów przemysłowych, student potrafi zorganizować centrum reagowania kryzysowego

EK4 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.

6 Treści programowe

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Analiza bezpieczeństwa 2 wybranych przedsiembiorstw	8
L2	Analiza wykrytych podatności oraz zagrożeń	8
L3	Organizacja centrum reagowania na incydenty związane z naruszeniem bezpieczeństwa	8
L4	Planowanie centrum monitoringu ciągłego	6

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Wprowadzenia do zagadnienia bezpieczeństwa systemów przemysłowych	2
W2	Typy przemysłowych systemów kontroli: SCADA, DCS, PLC	2
W3	Charakterystyka, zagrożenia i podatności systemów typu ICS	3
W4	Metody zapewniania bezpieczeństwa w systemach ICS	3
W5	Struktura sieciowa systemów przemysłowych	2
W6	Metody podnoszenia bezpieczeństwa w sieciach przemysłowych	2

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W7	Wykrywanie intruzów i ataki na sieci przewodowe	2
W8	Autoryzacja, autentykcaja oraz techniki kryptograficzne w systemach przemysłowych	2
W9	Organizacja centrum reagowania na zagrożenia bezpieczeństwa	2
W10	Krytyczne obszary kontrolne w zakresie bezpieczeństwa systemów przemysłowych SANS TOP 20	2
W12	Narzędzia i metody ciągłego monitoringu w systemach przemysłowych	2
W13	Metody przeciwdziałania atakom na bezpieczeństwo w systemach przemysłowych	3
W14	Podsumowanie	3

7 Narzędzia dydaktyczne

N1 Ćwiczenia laboratoryjne

N2 Konsultacje

N3 Wykłady

N4 Ćwiczenia projektowe

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	60
Konsultacje przedmiotowe	5
Egzaminy i zaliczenia w sesji	1
Zaliczenia	4
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	10
Opracowanie wyników	5
Przygotowanie raportu, projektu, prezentacji, dyskusji	5
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**90**
Sumaryczna liczba punktów ECTS dla przedmiotu	3.00

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 systemów przemysłowych oraz nie potrafi wymienić metod wykorzystywanych w analizie. Student nie potrafi wymienić ani jednego przykładu z ww zagadnień.
Na ocenę 3.0	Student zna wybrane zagrożenia systemów przemysłowych oraz metody ich wykrywania. Student potrafi wymienić po jednym przykładzie z ww zagadnień,
Na ocenę 3.5	Student zna wybrane zagrożenia systemów przemysłowych oraz metody ich wykrywania. Potrafi podać różne przykłady dla każdego wymienionego zagadnienia.
Na ocenę 4.0	Student zna zagrożenia systemów przemysłowych oraz metody ich wykrywania. Potrafi podać różne przykłady dla każdego wymienionego zagadnienia.
Na ocenę 4.5	Student zna szczegółowo zagrożenia systemów przemysłowych. Potrafi podać różne przykłady dla każdego wymienionego zagadnienia. Potrafi podać oraz rozumie matematyczne podstawy wybranych metod zabezpieczania systemów przemysłowych.
Na ocenę 5.0	Student zna szczegółowo zagrożenia systemów przemysłowych. Potrafi podać różne przykłady dla każdego wymienionego zagadnienia. Potrafi podać oraz rozumie matematyczne podstawy wybranych metod. Student potrafi dobrać metody zabezpieczania ww w zależności od konkretnych przykładów zagrożeń.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie zna ogólnych zasad dotyczących budowy centrum reagowania i monitorowania zagrożeń bezpieczeństwa w systemach przemysłowych. Student nie potrafi wymienić ani jednego przykładu z ww zagadnień.
Na ocenę 3.0	Student zna ogólne zasady dotyczące budowy centrum reagowania i monitorowania zagrożeń bezpieczeństwa w systemach przemysłowych. Student potrafi wymienić po jednym przykładzie z ww zagadnień,
Na ocenę 3.5	Student zna ogólne zasady dotyczące budowy centrum reagowania i monitorowania zagrożeń bezpieczeństwa w systemach przemysłowych. Potrafi podać różne przykłady dla każdego wymienionego zagadnienia.
Na ocenę 4.0	Student zna zasady dotyczące budowy centrum reagowania i monitorowania zagrożeń bezpieczeństwa w systemach przemysłowych. Potrafi podać różne przykłady dla każdego wymienionego zagadnienia.
Na ocenę 4.5	Student zna ogólne zasady dotyczące budowy centrum reagowania i monitorowania zagrożeń bezpieczeństwa w systemach przemysłowych w sposób szczegółowy. Potrafi podać różne przykłady dla każdego wymienionego zagadnienia. Potra podać oraz rozumie matematyczne podstawy wybranych metod zabezpieczania ruchu sieciowego
Na ocenę 5.0	Student zna ogólne zasady dotyczące budowy centrum reagowania i monitorowania zagrożeń bezpieczeństwa w systemach przemysłowych w sposób szczegółowy. Potrafi podać różne przykłady dla każdego wymienionego zagadnienia. Potra podać oraz rozumie matematyczne podstawy wybranych metod zabezpieczania ruchu sieciowego. Student potrafi dobrać ww metody w zależności od konkretnych przykładów zagrożeń.

Efekt kształcenia 3	
Na ocenę 2.0	Student nie zna podstawowych protokołów i metod analizy zagrożeń oraz nie potrafi wymienić metod reagowania kryzysowego. Student nie potrafi scharakteryzować ani jednego przykładu omawianych technik.
Na ocenę 3.0	Student zna podstawowe protokoły i metody analizy zagrożeń oraz potrafi wymienić metody reagowania kryzysowego. Student potrafi scharakteryzować jednego przykład omawianych technik.
Na ocenę 3.5	Student zna podstawowe protokoły i metody analizy zagrożeń oraz potrafi wymienić metody reagowania kryzysowego. Student potrafi skonfigurować oraz zaimplementować wybrany przykład z zakresu omawianych technik.
Na ocenę 4.0	Student zna różne protokoły i metody analizy zagrożeń oraz potrafi wymienić metody reagowania kryzysowego. Student potrafi skonfigurować oraz zaimplementować wybrane przykłady omawianych technik.
Na ocenę 4.5	Student zna szczegółowo protokoły i metody analizy zagrożeń oraz potrafi wymienić metody reagowania kryzysowego. Student potrafi skonfigurować oraz zaimplementować wybrane przykłady omawianych technik. Student potrafi podać i rozumie matematyczne podstawy wybranych metod oraz potrafi je zastosować w zależności od spodziewanych zagrożeń.
Na ocenę 5.0	Student zna szczegółowo protokoły i metody analizy zagrożeń oraz potrafi wymienić metody reagowania kryzysowego. Student potrafi skonfigurować oraz zaimplementować wybrane przykłady omawianych technik. Student potrafi podać i rozumie matematyczne podstawy wybranych metod oraz potrafi je zastosować w zależności od spodziewanych zagrożeń. Student potrafi wykonać analizę potencjalnych zagrożeń oraz dobrać metody i środki ochrony .
Efekt kształcenia 4	
Na ocenę 2.0	Student nie potrafi samodzielnie, bądź w grupie wykonać zadań praktycznych. Nie wykonuje poleceń nauczyciela, nie potrafi wykonać poleceń uzgodnionych z grupą.
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 kierować pracą 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 kierować pracą małej grupy, potrafi w sposób zrozumiały przedstawić wyniki jej pracy oraz rozwiązywać w sposób kreatywny powstałe podczas pracy problemy.

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_W02	Cel 1 Cel 2	L1 L2 L3 L4 W1 W2 W3 W4 W5 W6 W7 W8 W9	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK2	I2_W04 I2_W05	Cel 1 Cel 2	W10 W12 W13 W14	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK3	I2_U08 I2_U09	Cel 1 Cel 2	L1 L2 L3 L4 W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W12 W13 W14	N1 N2 N3 N4	F1 F2 F3 P1 P2
EK4	I2_K04	Cel 1 Cel 2	W10 W12 W13 W14	N1 N2 N3 N4	F1 F2 F3 P1 P2

11 Wykaz literatury

Literatura podstawowa

[1] A. Kozak, M. Kościelny, P. Pacyna, D. Gołębiewski, K. Paturej, J. Świątkowska, — *Cybersecurity and Industrial Plants Foundation of the Industry 4.0 Project and a chance for Poland, Cybersec 2016, 26-27 September 2016, Kraków, Poland.*, -, 0, -

[2] P. Chołda, T. Chmielecki, P. Pacyna, P. Potrawka, N. Rapacz, R. Stankiewicz, P. Wydrych, — *Enterprise-oriented Cybersecurity Management,*, -, 0, -

[3] NIST — *Guide to Industrial Control Systems (ICS) Security*, -, 0, -

Literatura uzupełniająca

[1] SANS — *https://www.sans.org/critical-security-controls/*, -, 0, -

[2] Gerard Johansen — *Digital Forensics and Incident Response A practical guide to deploying digital forensic techniques in response to cyber security incidents*, -, 0, -

[3] T. Luttgens, Matthew Pepe, Kevin Mandia — *Incident Response & Computer Forensics*, -, 0, -

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr inż. Andrzej Wilczyński (kontakt: `andrzej.wilczynski@pk.edu.pl`)

13 Zatwierdzenie karty przedmiotu do realizacji

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