**Nazwa przedmiotu:**

Bezpieczeństwo informacyjne ITS

**Koordynator przedmiotu:**

prof. dr hab. inż. Mirosław Siergiejczyk, Wydział Transportu Politechniki Warszawskiej, Zakład Telekomunikacji w Transporcie

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Transport

**Grupa przedmiotów:**

Specjalnościowe

**Kod przedmiotu:**

TR.NMP354

**Semestr nominalny:**

3 / rok ak. 2020/2021

**Liczba punktów ECTS:**

2

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

60 godz., w tym: praca na wykładach 9 godz., praca na ćwiczeniach 9 godz., zapoznanie się ze wskazaną literaturą 12 godz., konsultacje 3 godz., przygotowanie się do zaliczeń 14 godz., przygotowanie się do egzaminu 11 godz., udział w egzaminie 2 godz.

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

1,0 pkt ECTS (23 godz., w tym: praca na wykładach 9 godz., praca na ćwiczeniach 9 godz., konsultacje 3 godz., udział w egzaminie 2 godz.)

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

0

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład:  | 15h |
| Ćwiczenia:  | 15h |
| Laboratorium:  | 0h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

brak

**Limit liczby studentów:**

wykład: brak, ćwiczenia: 30 osób

**Cel przedmiotu:**

Umiejętność identyfikacji podstawowych problemów związanymi z bezpieczeństwem transmisji, przetwarzania i przechowywania informacji w inteligentnych systemach transportowych. Poznanie aktów normatywnych dotyczących regulacji w zakresie transmisji, przetwarzania i przechowywania informacji. Umiejętność wykorzystania metod i mechanizmów zapewnienia bezpieczeństwa w inteligentnych systemach transportowych.

**Treści kształcenia:**

Wykład: Bezpieczeństwo jako własność eksploatacyjna systemów telematyki. Definicje bezpieczeństwa, modele bezpieczeństwa systemów. Istota polityki bezpieczeństwa, założenia polityki bezpieczeństwa systemów ITS. Normy i inne akty prawne określające zasady bezpieczeństwa systemów informatycznych i telekomunikacyjnych. Identyfikacja zagrożeń przesyłania, przetwarzania i przechowywania informacji w systemach inteligentnego transportu. Zagrożenia transmisji w sieciach przewodowych. Zagrożenia transmisji w sieciach bezprzewodowych. Zagrożenia transmisji informacji w rozległych sieciach publicznych i sieci Internet. Analiza i ocena ryzyka zagrożeń w systemach ITS. Metody i mechanizmy zapewnienia bezpieczeństwa w systemach ITS. Problematyka zapewnienia bezpieczeństwa aplikacji w systemach ITS. Metody zapewnienia niezawodności i bezpieczeństwa oprogramowania. Zagadnienia bezpieczeństwa logicznego – protokoły bezpiecznej transmisji, wirtualne sieci prywatne, jako sieci zapewniające bezpieczeństwo transmisji, sposoby autoryzowane dostępu do zasobów sieciowych i transmitowanych informacji. Wybrane zagadnienia zabezpieczeń fizycznych – kontrola dostępu, monitorowanie pomieszczeń, systemy sygnalizacji i ochrony fizycznej. Zasady zapewnienia bezpieczeństwa energetycznego systemów ITS.

Ćwiczenia: Identyfikacja zagrożeń w sieciach i systemach teleinformatycznych. Analiza i ocena zagrożeń w systemach ITS. Opracowanie mechanizmów bezpieczeństwa dla wybranych systemów inteligentnego transportu kolejowego, drogowego i lotniczego. Opracowanie schematów bezpiecznego zasilania w wybranych systemach ITS.

**Metody oceny:**

Zaliczenie wykładu następuje na podstawie sprawdzenia wiedzy teoretycznej podczas zajęć. Ocena formująca: Wykład - dwie kartkówki dotyczące wybranych zagadnień teoretycznych. Ocena podsumowująca: kolokwium pisemne zawierające od 5 do 10 pytań, ponad 50% poprawnych odpowiedzi to ocena pozytywna, dalsze stopniowanie o pół oceny co 10%. Możliwość odpowiedzi ustnych. Podczas sprawdzianu zabronione jest korzystanie z materiałów pomocniczych w jakiejkolwiek formie.
Zaliczenie ćwiczeń następuje na podstawie sprawdzenia wiedzy podczas zajęć. Ocena formułująca: dwie kartkówki po określonej serii ćwiczeń. Ocena podsumowująca: kolokwium pisemne zawierające od 5 do 10 pytań, ponad 50% poprawnych odpowiedzi to ocena pozytywna, dalsze stopniowanie o pół oceny co 10%. Możliwość odpowiedzi ustnych.
Dopuszcza się korzystanie z komputerów, telefonów komórkowych oraz materiałów przesyłanych bądź wydrukowanych przez prowadzących do realizacji wyznaczonych ćwiczeń.
Ocena końcowa z przedmiotu jest średnią arytmetyczną oceny z wykładu i ćwiczeń. Z tym że, ocena końcowa będzie pozytywna tylko gdy obydwie oceny (z wykładu, ćwiczeń) będą pozytywne.

**Egzamin:**

tak

**Literatura:**

1) Balinsky A., Miller D., Sankar K., Sundaralingam S.: Bezpieczeństwo sieci bezprzewodowych. Ochrona sieci 802.11. Porady eksperta. Mikom Warszawa 2005;
2) Cole E., Krutz R. L., Conley J.:Bezpieczeństwo sieci: biblia. Helion Gliwice 2005;
3) Fry Ch., Nystrom M.: Monitoring i bezpieczeństwo sieci. Wydawnictwo Helion Gliwice 2010;
4) Jaźwiński J.,Ważyńska-Fiok K.: Bezpieczeństwo systemów. WNT Warszawa 1993;
5) Kowalewski J., Kowalewski M.: Zagrożenia informacji w cyberprzestrzeni, Cyberterroryzm. Oficyna Wydawnicza Politechniki Warszawskiej 2017;
6) Kowalewski J., Kowalewski M.: Ochrona informacji i systemów teleinformatycznych w cyberprzestrzeni, Oficyna Wydawnicza Politechniki Warszawskiej 2017;
7) Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych. PWN Warszawa 2009;
8) Liderman K.: Bezpieczeństwo informacyjne. Nowe wyzwania. Wydawnictwo Naukowe PWN 2018;
9) Praca zbiorowa Cyberbezpieczeństwo. Zarys wykładu Redakcja naukowa: C. Banasiński. Wyd. Wolters Kluwer Polska 2018;
10) Praca zbiorowa. Cyberbezpieczeństwo. Zarys wykładu. Wyd. Wolters Kluwer 2018;
11) Redakcja: Gryszczyńska A., Szpor G.: Internet. Strategie bezpieczeństwa. CH Beck 2017;
12) Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Tom 2. Wydawnictwo Helion 2019;
13) Sutton R. J.: Bezpieczeństwo telekomunikacji. Wydawnictwo WKŁ Warszawa 2004;
14) Strebe M.: Podstawy bezpieczeństwa sieci. MIKOM Warszawa 2005;
15) Normy w zakresie bezpieczeństwa ISO, EN, PN;
16) Strony internetowe.

**Witryna www przedmiotu:**

www.twt.wt.pw.edu.pl

**Uwagi:**

O ile nie powoduje to zmian w zakresie powiązań danego przedmiotu z kierunkowymi efektami w treściach kształcenia mogą być wprowadzane na bieżąco zmiany związane z uwzględnieniem najnowszych osiągnięć naukowych.

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka W01:**

Posiada rozszerzoną i pogłębioną wiedzę teoretyczną dotyczącą potrzeb i zasad dotyczących bezpieczeństwa transmisji, przetwarzania i przechowywania informacji dla potrzeb wspomagania realizacji zadań transportowych

Weryfikacja:

Na kolokwium pisemnym kilka pytań z danego zagadnienia. Uzyskanie 51% poprawnych
odpowiedzi umożliwia wystawienie oceny pozytywnej. Możliwość ustnych odpowiedzi.

**Powiązane charakterystyki kierunkowe:** Tr2A\_W06

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

**Charakterystyka W02:**

Zna budowę, zasadę działania i własności systemów zapewniających bezpieczeństwo transmisji, przetwarzania i przechowywania informacji w systemach telematyki transportu

Weryfikacja:

Na kolokwium pisemnym kilka pytań z danego zagadnienia. Uzyskanie 51% poprawnych odpowiedzi umożliwia wystawienie oceny pozytywnej. Możliwość ustnych odpowiedzi.

**Powiązane charakterystyki kierunkowe:** Tr2A\_W06

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

**Charakterystyka W03:**

Zna podstawowe metody, techniki, narzędzia i materiały stosowane w budowie rozwiązań zapewniających bezpieczeństwo transmisji, przetwarzania i przechowywania informacji w systemach telematyki transportu

Weryfikacja:

Na kolokwium pisemnym kilka pytań z danego zagadnienia. Uzyskanie 51% poprawnych
odpowiedzi umożliwia wystawienie oceny pozytywnej. Możliwość ustnych odpowiedzi.

**Powiązane charakterystyki kierunkowe:** Tr2A\_W08

**Powiązane charakterystyki obszarowe:** I.P7S\_WG

### Profil ogólnoakademicki - umiejętności

**Charakterystyka U01:**

Potrafi pozyskiwać informacje z literatury, baz danych oraz innych źródeł także w języku angielskim o budowie, zasadzie działania, własnościach użytkowych i wdrażaniu sieci systemów bepieczeńtwa transmisji, przetwarzania i przechowywania informacji w systemach telematyki transportu

Weryfikacja:

Na kolokwium pisemnym kilka pytań. Ponad 50% poprawnych odpowiedzi to ocena pozytywna. Możliwość ustnych odpowiedz.

**Powiązane charakterystyki kierunkowe:** Tr2A\_U01

**Powiązane charakterystyki obszarowe:** I.P7S\_UW

**Charakterystyka U02:**

Potrafi wykorzystać metody analityczne, do formułowania i rozwiązywania zadań inżynierskich i prostych problemów badawczych dotyczących transportu, w tym potrafi dokonać oceny bezpieczeństwa systemów telematyki transportu

Weryfikacja:

Na kolokwium pisemnym kilka pytań. Ponad 50% poprawnych odpowiedzi to ocena pozytywna. Możliwość ustnych odpowiedz.

**Powiązane charakterystyki kierunkowe:** Tr2A\_U17, Tr2A\_U19

**Powiązane charakterystyki obszarowe:** I.P7S\_UW, III.P7S\_UW.2.o, III.P7S\_UW.4.o

**Charakterystyka U03:**

Potrafi wykorzystywać do formułowania i rozwiązywania zadań w zakresie oceny przydatności systemów bepieczeńtwa transmisji, przetwarzania i przechowywania informacji w systemach telematyki transportu odpowiednie metody analityczne

Weryfikacja:

Na kolokwium pisemnym kilka pytań. Ponad 50% poprawnych odpowiedzi to ocena pozytywna. Możliwość ustnych odpowiedz.

**Powiązane charakterystyki kierunkowe:** Tr2A\_U17, Tr2A\_U19

**Powiązane charakterystyki obszarowe:** III.P7S\_UW.2.o, I.P7S\_UW, III.P7S\_UW.4.o