**Nazwa przedmiotu:**

Cyberprzestępczość i cyberbezpieczeństwo - perspektywa prawna

**Koordynator przedmiotu:**

dr M. Rojszczak

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Administracja

**Grupa przedmiotów:**

Obieralne

**Kod przedmiotu:**

A21\_CCPP

**Semestr nominalny:**

2 / rok ak. 2021/2022

**Liczba punktów ECTS:**

3

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

Ogółem 75h, w tym 30 ćwiczenia, 45 praca własna studenta (czytanie literatury 25h, przygotowanie do zaliczenia 20h)

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

1,2

**Język prowadzenia zajęć:**

polski

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

1,2

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

|  |  |
| --- | --- |
| Wykład: | 0h |
| Ćwiczenia: | 30h |
| Laboratorium: | 0h |
| Projekt: | 0h |
| Lekcje komputerowe: | 0h |

**Wymagania wstępne:**

Brak wymagań

**Limit liczby studentów:**

grupa obieralna

**Cel przedmiotu:**

Celem przedmiotu będzie omówienie aktualnych trendów w obszarze prawnej regulacji obszaru cyberbezpieczeństwa w prawie krajowym oraz międzynarodowym, ze szczególnym zwróceniem uwagi na problematykę walkę z cyberprzestępczością.

**Treści kształcenia:**

1. Cyberprzestępczość - wprowadzenie
1.1. Cyberprzestępczość w liczbach – aktualne trendy
1.2. Podstawowe kategorie cyberprzestępstw
1.3. Czyny karalne według kodeksu karnego
1.4. Prawo międzynarodowe oraz unijne
1.5. Wprowadzenie do problematyki śledczej
1.6. Darknet a cyberprzestępczość
1.7. Jak nie zostać ofiarą cyberprzestępstwa?
2. Ramy regulacyjne cyberbezpieczeństwa – wprowadzenie
2.1. Cyberbezpieczeństwo - definicje
2.2. Unijny model cyberbezpieczeństwa
2.3. Krajowy System Cyberbezpieczeństwa
2.4. Rola standaryzacji w obszarze cyberbezpieczeństwa

**Metody oceny:**

Podstawą zaliczenia przedmiotu będzie obecność na zajęciach oraz przygotowanie pracy zaliczeniowej.
Tematy prac zostaną przedstawione w kwietniu 2021.
Osoby zainteresowane poprawieniem oceny będą mogły przystąpić do pisemnego sprawdzianu zaliczeniowego w czerwcu 2021 (ostatnie zajęcia w sem. letnim).
Kolokwium zaliczeniowe będzie miało formę pisemnego sprawdzianu składającego się z części testowej (10 pytań w postaci testu jednokrotnego wyboru) oraz części opisowej (5 pytań wymagających krótkiej wypowiedzi). Za poprawną odpowiedź na pytanie z testu jednokrotnego wyboru można uzyskać 1 pkt, zaś za poprawną odpowiedź na pytanie wymagające krótkiej pisemnej wypowiedzi: 0—2 pkt. Ogólna punktacja: 0—12 pkt — ocena niedostateczna, 13—14 pkt — ocena dostateczna, 15 pkt — ocena dostateczna plus, 16—17 pkt — ocena dobra, 18 pkt — ocena dobra plus, 19—20 pkt — ocena bardzo dobra.
Podczas sprawdzianu nie można korzystać z pomocy dydaktycznych i elektronicznych nośników informacji, za wyjątkiem aktów normatywnych w wersji papierowej.
„Jeżeli podczas weryfikacji osiągnięcia efektów uczenia się zostanie stwierdzona niesamodzielność pracy studenta lub korzystanie przez niego z materiałów lub urządzeń innych niż dozwolone w regulaminie przedmiotu, student uzyskuje ocenę niedostateczną i traci prawo do zaliczenia przedmiotu w jego bieżącej realizacji” (§ 19 ust. 4 Regulaminu studiów PW).

**Egzamin:**

nie

**Literatura:**

1. Monografie/komentarze:
1.1. D. Jagiełło, Cyberprzestępczość, [w:] Cyberbezpieczeństwo. Zarys wykładu pod red. C. Banasińskiego, Wolters Kluwer 2018
1.2. M. Siwicki, Cyberprzestępczość, CH Beck 2013
1.3. C. Banasiński, M. Rojszczak (red.), Cyberbezpieczeństwo, Wolters Kluwer 2020
1.4. Dowolny komentarz do KK – np. A. Stefańskiego, CH Beck 2018.
1.5. Komentarz do ustawy o KSC
2. Akty prawne:
2.1. Kodeks karny - w szczególności r. XXXIII: przestępstwa przeciwko ochronie informacji (Dz. U. 2018 poz. 1600)
2.2. Ustawa o krajowym systemie cyberbezpieczeństwa
2.3. Konwencja RE nr 185 o cyberprzestępczości (Dz. U. 2015 poz. 728)
2.4. Dyrektywa 2016/1148 (NIS)
2.5. Rozporządzenie 2019/881 (Cybersecurity Act)

**Witryna www przedmiotu:**

---

**Uwagi:**

W przypadku niezaliczenia przedmiotu student powtarza przedmiot w całości.

## Charakterystyki przedmiotowe