

Prawne aspekty cyberprzestrzeni

Głównym celem zajęć powinno być zapoznanie studenta z zagrożeniami i wyzwaniem w cyberprzestrzeni oraz z regulacjami prawnymi pozwalającymi na zapobieganie, zwalczanie i przeciwdziałanie możliwym incydentom w zgodzie z literą prawa polskiego, europejskiego oraz międzynarodowego.

W tym celu student powinien zostać zapoznany z:

- podstawowymi pojęciami cyberprzestrzeni, cyberataków, cyberprzestępstwa, cyberterrorizmu oraz cyberwojny,
- pojęciami związanymi z hackingiem, w szczególności z etycznym hackingiem,
- przykładami cyberataków w Polsce i na świecie,
- rolą i zadaniami kluczowych podmiotów krajowych w sektorze cyberbezpieczeństwa:
 - o Ministra ds. Cyfryzacji oraz Ministerstwa Cyfryzacji,
 - o Ministra ds. Obrony,
 - o Pełnomocnik Rządu ds. Cyberbezpieczeństwa,
 - o Kolegium ds. Cyberbezpieczeństwa,
 - o zespołów CERT.
- regulacjami prawne obowiązujące w Polsce w zakresie ochrony w cyberprzestrzeni
 - o Strategią Cyberbezpieczeństwa RP na lata 2019-2024,
 - o ustawą o krajowym systemie cyberbezpieczeństwa, która wdraża dyrektywę NIS oraz Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024,
 - o aktami dotyczące ochrony danych osobowych w tym ogólne rozporządzenie o ochronie danych (RODO),
 - o Narodowymi Standardami Cyberbezpieczeństwa (NSC)
- rolą i zadaniami Unii Europejskiej oraz Agencji Unii Europejskiej ds. Cyberbezpieczeństwa w sektorze cyberbezpieczeństwa,
- europejskimi dokumentami prawnymi pozwalającymi na reagowanie na incydenty w przestrzeni cybernetycznej
 - o Europejską Strategią Cyberbezpieczeństwa,
 - o dyrektywami NIS i NIS2,
 - o Aktem o cyberbezpieczeństwie,
 - o Aktem o cyberodporności,
 - o Aktem o cybersolidarności.
- międzynarodowymi regulacje prawne pozwalające na działanie państw w cyberprzestrzeni,
- instytucjami oraz procedurami związanymi z raportowaniem incydentów.

Pomocna literatura:

1. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
<https://www.dziennikustaw.gov.pl/DU/rok/2018/pozycja/1560>
2. Strategia Cyberbezpieczeństwa RP na lata 2019-2024
<https://www.dziennikustaw.gov.pl/MP/rok/2019/pozycja/1037>

3. Cyberbezpieczeństwo; red: Cezary Banasiński, Marcin Rojszczak; Wolters Kluwer, 2020
4. Dyrektywa Parlamentu Europejskiego i Rady UE 2013/40/UE z dn. 12.08.2013 r. dotycząca ataków na systemy informatyczne (zastąpiła Decyzję 2005/222/WSiSW Rady UE z 2005 r.).
5. Dyrektywa NIS Parlamentu Europejskiego i Rady UE 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej.