Program szkolenia "Bezpieczeństwo w cyberprzestrzeni"

Wymagania wstępne (w zakresie wiedzy, umiejętności, kompetencji społecznych)

Brak wymagań.

Założenia i cel kształcenia

Przedmiot ukierunkowany na zapoznanie z ochroną informacji jawnych, niejawnych oraz stanowiących bezpieczeństwo ekonomiczne firmy w systemach teleinformatycznych z punktu widzenia interesów państwa w dziedzinie bezpieczeństwa. Celem jest wyposażenie studentów w wiedzę o założeniach, podstawach prawnych i zasadach ochrony teleinformatycznej i teleinformacyjnej, wybranych procedurach, a także odpowiedzialności personalnej i instytucjonalnej (również w wymiarze karnym).

Efekty uczenia się w zakresie wiedzy, umiejętności, kompetencji społecznych

Uczestnik identyfikuje system ochrony informacji i bezpieczeństwo teleinformatyczne - poszczególne podmioty, rolę osób uczestniczących w organizacji bezpieczeństwa teleinformatycznego oraz wybrane metodyki ochrony teleinformatycznej i teleinformacyjnej. Identyfikuje system bezpieczeństwa teleinformatycznego i teleinformacyjnego na szczeblu instytucjonalnym i osobowym. Uczestnik ustala znaczenie przesłanek ataku w sieciach teleinformatycznych (cyberataków) państwowych i niepaństwowych. Wartościuje bezpieczeństwo teleinformatyczne w kontekście interesów firmy i państwa dziedzinie bezpieczeństwa odróżniając żywotne, ważne od innych istotnych.

Treści programowe	Liczba godzin szkoleniowych	Liczba godzin na pracę własną	Metody prowadzenia szkolenia	Liczba punktów ECTS
19 zasad bezpiecznego urządzenia teleinformatycznego.	4	4	Wykład, prezentacja (multimedialna), opowiadanie.	0,32
Bezpieczeństwo sieci teleinformatycznych. Podatności w systemach teleinformatycznych.	4	2	Wykład, prezentacja	0,24
IoT i IIoT- Internet Rzeczy i Przemysłowy Internet Rzeczy. Wybrane aspekty IoE.	6	0	Wykład, prezentacja (multimedialna), opowiadanie.	0,24
OSINT w cyberprzestrzeni – metody pozyskiwania informacji, analiza cyfrowych śladów.	4	2	Metoda przypadku.	0,24
Zabezpieczenie i szyfrowanie informacji przesyłanych w sieciach teleinformatycznych.	4	0	Wykład.	0,16
Zasady ochrony informacji. Wybrane problemy.	4	0	Wykład problemowy.	0,16
Ochrona informacji niejawnych. Wybrane zagadnienia bezpieczeństwa osobowego, Struktura ochrony informacji niejawnych.	4	0	Wykład problemowy.	0,16
			SUMA	2

Rodzaj (forma) oceny, rozumiane jako metoda weryfikacji efektów uczenia się

Zadania praktyczne, aktywny udział w zajęciach - wykonywanie poleceń prowadzącego.

Posiedzenie Komisji w dniu 29.10.2025
Komisja w składzie:

1. Ernest Lichocki
2. Andrzej Piotrowski
3. Dawid Jóźwiak