Cyberbezpieczeństwo - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Cyberbezpieczeństwo
Kod przedmiotu	14.1-WH-PolitD-Cyb-S18
Wydział	Wydział Nauk Społecznych
Kierunek	Politologia
Profil	ogólnoakademicki
Rodzaj studiów	drugiego stopnia z tyt. magistra
Semestr rozpoczęcia	semestr zimowy 2022/2023

Informacje o przedmiocie

Semestr	4
Liczba punktów ECTS do zdobycia	3
Typ przedmiotu	obowiązkowy
Język nauczania	polski
Sylabus opracował	• dr Jacek Jędryczkowski

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Wykład	30	2	-	-	Egzamin

Cel przedmiotu

- nabycie wieloaspektowej wiedzy na temat cyberbezpieczeństwa.
- nabycie umiejętności i diagnozowania i rozpoznawania zagrożeń.
- ukształtowanie postaw dbałości o infrastrukturę techniczną oraz dane.

Wymagania wstępne

Podstawowe wiadomości o komputerze i systemie operacyjnym (zakres szkoły średniej).

Zakres tematyczny

- Zagrożenia medialne w sieci (niejawne formy manipulacji). Człowiek jako najsłabsze ogniwo w systemie zabezpieczeń.
- Ochrona danych osobowych oraz danych wrażliwych (metadane a dane wrażliwe). Ochrona tożsamości w sieci.
- Zabezpieczenie systemu operacyjnego (kopia bezpieczeństwa, przenoszenie systemu na nowy dysk, uprawnienia do dostępu, przykłady łamania zabezpieczeń).
- Ochrona danych komputerowych (archiwizacja, dyski sieciowe, dyski NAS, szyfrowanie danych, kasowanie a niszczenie danych, niszczenie nośników).
- Keylogery (sprzętowe i softwerowe); aplikacje do rejestrowania i transmitowania pulpitu; wirusy; poczta elektroniczna i załączniki; makra. System operacyjny na dysku wirtualnym.
- Urządzenia mobilne a utrata prywatności (podsłuchiwanie, różne systemy lokalizacji, łamanie tajemnicy korespondencji); Technologia RFID (wady i zastosowania). Bańka informacyjna.
- Technologia Big Data a gromadzenie i przetwarzanie danych osobowych (Google Analytics, YouTube Analytics). Przykłady największych manipulacji sieciowych.
- Smarthome jako platforma do inwigilacji użytkowników.
- Konfiguracja routera jako techniczne zabezpieczenie sieci. VPN - bezpieczne połączenie z serwerem. Sieć Tor. Charakterystyka i przykłady ataków sieciowych.

Metody kształcenia

- wykład konwersatoryjny i problemowy z zastosowaniem prezentacji multimedialnych i symulacji,
- pokaz, demonstracja (np. z zastosowaniem narzędzi do prezentacji pulpitu nauczyciela lub studenta pozostałym odbiorcom w pracowni komputerowej),
- praca z książką oraz kursem multimedialnym (na platformie i stronie internetowej przedmiotu),
- zajęcia zdalnie (e-learning oraz blended learning) - korzystanie z platformy oraz multimedialnych kursów online prowadzącego.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
zna podstawowe zasady ochrona danych i systemów informatycznych.	• KP2_W02	• test egzaminacyjny z progami punktowymi	• Wykład
zna sposoby ochrony systemów i danych oraz formy ataków (na systemy informatyczne) oraz oddziaływań na użytkowników tych systemów.	• KP2_W05	• test egzaminacyjny z progami punktowymi	• Wykład
potrafi ocenić poziom bezpieczeństwa systemu lub sieci w aspektach prawnych, etycznych i organizacyjnych w świetle obowiązującego prawa;	• KP2_U04	• test egzaminacyjny z progami punktowymi	• Wykład

Warunki zaliczenia

Próg zaliczenia nie mniej niż 55-60% punktów. Ocenę z wykładu wylicza się na podstawie punktów uzyskanych z testu egzaminacyjnego, które są przeliczane na stopnie wg. skali: 95%; 100% =5,0; 85%; 95%)=4,5; 75%; 85%)=4,0; 65%; 75%)=3,5; 55%; 65%)=3,0; 0%; 55%)=2,0;

Literatura podstawowa

1. Brooks Ch.J., Grow Ch., Craig P., Short D., *Cybersecurity Essentials*, Wyd. John Wiley & Sons, Nowy York 2018.
2. *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Warszawa 2014.
3. Jędryczkowski J., Strona przedmiotu "Cybezpieczeństwo": https://staff.uz.zgora.pl/jjedrycz/przedmioty.html (we właściwym semestrze po wybraniu nazwy przedmiotu oraz grupy).
4. Jędryczkowski J., *Ochrona danych i bezpieczeństwo systemu operacyjnego*: https://staff.uz.zgora.pl/jjedrycz/elearning/bezpieczenstwo/pliki/index.html

Literatura uzupełniająca

1. Jędryczkowski J.**,** *Bezpieczeństwo systemu operacyjnego i ochrona danych*, W: red. M. Furmanek, *Technologie informacyjne w warsztacie pracy nauczyciela*, Oficyna Wyd. Uniwersytetu Zielonogórskiego, Zielona Góra 2008.
2. Jędryczkowski J., *JJ Kursy - edukacyjny kanał YouTube*: www.youtube.com/c/JJKursy
3. Jędryczkowski J., *Publikacje*: https://staff.uz.zgora.pl/jjedrycz/publikacje.html
4. *Orędzie o stanie Unii w 2017 r. – Komisja zwiększa zdolności reagowania UE na ataki cybernetyczne.*
5. Szmit M., Lisiak-Felicka D., *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016.

Uwagi

Kurs z materiałami dydaktycznymi, listami zadań oraz wymaganiami jest dostępny stronie prowadzącego: https://staff.uz.zgora.pl/jjedrycz/przedmioty.html po wybraniu nazwy przedmiotu wraz z numerem grupy lub w planie zajęć po wybraniu odpowiedniego Classroomu.

Zmodyfikowane przez dr Jacek Jędryczkowski (ostatnia modyfikacja: 29-04-2022 22:35)