Autor*: dr Piotr Sapiecha*

Bezpieczeństwo społeczne, organizacyjne
i zarządzanie cyberbezpieczeństwem
Cybersecurity - Social and Organizational Security

Poziom kształcenia: I stopień
Forma i tryb prowadzenia przedmiotu: stacjonarna
Kierunek studiów: Cyberbezpieczeństwo
Specjalność:
Grupa przedmiotów:
Poziom przedmiotu: podstawowy
Status przedmiotu: obowiązkowy
Język przedmiotu: polski
Semestr nominalny (tylko dla przedmiotów obowiązkowych): 6
Minimalny numer semestru: 6
Wymagania wstępne, zalecane przedmioty poprzedzające: n/d
Limit liczby studentów: 60

Powód zgłoszenia przedmiotu: program studiów na nowym kierunku Cyberbezpieczeństwo

Cel przedmiotu:

Głównym celem twórców przedmiotu jest przedstawienie studentom spektrum zagadnień, z którymi musi zmierzyć się inżynier (projektant lub użytkownik) w szeroko rozumianym obszarze bezpieczeństwa podczas budowy oraz utrzymania urządzeń lub systemów teleinformatycznych. Dotyczy to kwestii: prawnych, organizacyjnych, społecznych oraz dotyka zagadnień bezpieczeństwa w kontekście: elementów lub całego systemu, osób, przedsięwzięć oraz całych firm. Podczas wykładu zostaną omówione możliwe zagrożenia, oraz ich ewentualne konsekwencje. Przedstawione zostanie jak można zdefiniować funkcje i jak je zaimplementować z wykorzystaniem różnych mechanizmów, tak aby w efekcie uzyskać zamierzone cele, skutkujące bezpieczeństwem systemu. Równocześnie zostaną rozważone różnorodne efekty wprowadzenia danych zabezpieczenia do systemu lub też ich złamania. Zostanie również przedstawiona metodologia analizy ryzyka.

Treść kształcenia:

WYKŁADY:

1. Wprowadzenie do zagadnień ochrony informacji
Prywatność, anonimowość, poufność, zagrożenia, podatności, zabezpieczenia, incydenty, zarządzanie incydentami, obsługa incydentów, współczesne zagrożenia cyberbezpieczeństwa, aktualne przykłady. Organizacje zajmujące się cyberbezpieczeństwem, kontekst prawny.

2. Współczesne obszary związane z bezpieczeństwem teleinformatycznym
Przykłady uzasadniające potrzebę zarządzania bezpieczeństwem: e-płatności-kredyt-czeki i technologia blockchain, podpis EIDAS, e-dowódy, bezpieczeństwo w chmurze obliczeniowej, aktualne możliwe zagrożenia.

3. Projektowanie systemów bezpieczeństwa informacyjnego
Zarządzanie przedsięwzięciem projektowania i budowy systemu bezpieczeństwa informacyjnego, cykl życia systemu, etap analizy w cyklu rozwojowym systemu bezpieczeństwa informacyjnego, dokumentowanie prac projektowych, dobre praktyki w projektowaniu wiarygodnych systemów, testowanie: funkcjonalne, wydajnościowe, pokryciowe, produkcja, serwis i rozwój.

4. Modele ochrony informacji
Organizacja dostępu do informacji, sterowanie dostępem do informacji:
Model Grahama-Denninga, Bella-LaPaduli, Model Biby, Brewera-Nasha, Clarka-Wilsona, Harrisona-Ruzzo-Ullmana, Normy: ISO/IEC 27001.

5. Polityki bezpieczeństwa i dokumentowanie systemu ochrony informacji
Plan, instrukcje i procedury bezpieczeństwa informacyjnego, dokumentowanie przedsięwzięć zapewniania ciągłości działania organizacji, plan zapewniania ciągłości działania, plany kryzysowe, wytyczne z norm i standardów, kopie bezpieczeństwa - infrastruktura i organizacja, ochrona fizyczna, normy, ISO/IEC.

6. Zarządzanie ryzykiem
Charakterystyka procesu zarządzania ryzykiem, norma PN-ISO/IEC 27005:2010, standardy FIPS/NIST, ISO 31000-rodzina norm dotyczących zarządzania ryzykiem, analiza ryzyka - identyfikacja zakresu, środowiska, zagrożeń i podatności, oszacowanie ryzyka – metoda ilościowa, metoda jakościowa, ryzyko akceptowalne i koszty postępowania z ryzykiem.

7. Bezpieczeństwo społeczne
Sieci społecznościowe: zagrożenia i metody przeciwdziałania zagrożeniom. Metody analizy sieci społecznościowych (podać przykłady). Metody zapewnienia prywatności w sieci, ew. inne zagadnienia bezpieczeństwa społecznego.

8. Wojna informacyjna i manipulacja świadomością społeczną
Charakterystyka wojny informacyjnej, jej uczestnicy i jej poziomy, Rola mediów. Techniki manipulacji. Analiza przypadków. Przeciwdziałanie dezinformacji.

9. Tajemnice chronione prawem
Ochrona danych osobowych, tajemnica: lekarska, adwokacka, bankowa, skarbowa, danych telekomunikacyjnych, statystycznych, dane publiczne, prywatność w sieci, aspekty prawne, zatarcie śladów w Internecie, konsekwencje.

10. Ochrona informacji niejawnych
Podstawy prawne, organizacja ochrony informacji niejawnych, rola służb ochrony państwa, klauzule tajności, bezpieczeństwo osobowe i przemysłowe, KT, pełnomocnicy, inspektorzy, administratorzy, certyfikacja urządzeń lub narzędzi, standardy, ocena zgodności: ITSEC, CC. Obrót towarami podwójnego zastosowania, audyt.

11. Infrastruktura krytyczna
Środki i zasoby infrastruktury, podstawy prawne narodowego programu ochrony infrastruktury krytycznej, zapewnienie funkcjonalności, ciągłości działań i integralności, bezpieczeństwo fizyczne, techniczne i osobowe IK.

12. Przyszłość - sztuczna inteligencja i cyberbezpieczeństwo
Analiza bigdata z różnych źródeł: IoT i procesory SGX, chmury, 5G, techniki: maszynowego uczenia i deep learningu, wykrywanie ataków typu DDos, zyski i możliwe straty.

ĆWICZENIA:
–
LABORATORIA:
--
PROJEKT:

W ramach projektu stworzone zostaną zespoły 6-osobowe (2 projektantów + 2 osoby weryfikujące i dokumentujące + 2 atakujących) będą one miały do wykonania zadanie w postaci:
- analizy i zdefiniowania zagrożeń,
- specyfikacji celów i funkcji bezpieczeństwa,
- implementacji mechanizmów bezpieczeństwa,
- wykonanie dokumentacji,
- analiza bezpieczeństwa,
- przeprowadzenia weryfikacji projektu, oraz ataków i ustalenie możliwych słabych ogniw wraz z oceną końcową bezpieczeństwa.

ZAJĘCIA ZINTEGROWANE:

Treść kształcenia - streszczenie w jęz. angielskim:
The main aim of the course is to provide students with issues in the area of security during construction and maintenance of equipment or IT systems. This applies to the following issues: legal, organizational and social aspects, and touches on security issues in the context of: elements or the entire system, people, enterprises and entire companies. During the lecture, possible threats and their possible consequences will be discussed. It will be presented how to define security functions and how to implement them using various mechanisms, so as to obtain a secure system. The risk analysis methodology will also be presented.

Egzamin:
Egzamin będzie formą dyskusji merytorycznej o zrealizowanym projekcie, a w tym: specyfikacji wymagań, architekturze, implementacji, weryfikacji, dokumentacji i analizie bezpieczeństawa.

Literatura i oprogramowanie:

[1] Strategia cyberbezpieczeństwa RP, na lata 2017-2022, Ministerstwo Cyfryzacji, 2017

[2] Pod redakcją: S. Gwoździewicz, K. Tomaszyckiego, Prawne i społeczne aspekty cyberbezpieczeństwa, MII, 2017
[3] Pod redakcją: J. Trubalska, L. Wojciechowski, Bezpieczeństwo państwa w cyberprzestrzeni, WSEI, 2017
[4] Bezpieczeństwo infrastruktury krytycznej, Instytut Kościuszki, 2014
[5] System bezpieczeństwa cyberprzestrzeni RP, NASK, 2015
[6] M. Kubiak, S. Topolewski, Bezpieczeństwo informacyjne w XXI wieku, Imprint, 2016
[7] Wojna informacyjna w Internecie, CSM, 2017

Wymiar godzinowy zajęć:	W	C	L	P
	30	–	-	30

Wymiar w jednostkach ECTS: 5 pkt.

Przewidywane formy kształcenia i organizacja przedmiotu

Realizacja przedmiotu obejmuje następujące formy zajęć:

- wykład prowadzony w wymiarze 2 godz. tygodniowo,
- zajęcia projektowe, w ramach których student będzie wykonywał zadanie typu *case study* związane projektowaniem systemów i ich analizą bezpieczeństwa. Wyniki projektu wraz z wnioskami będą przedstawiane w postaci dokumentacji bezpieczeństwa.

Sprawdzanie założonych efektów kształcenia realizowane jest przez:

- ocenę wiedzy i umiejętności związanych z realizacją zadań projektowych – ocena prezentacji i raportu z przeglądu literatury;
- ocenę wiedzy i umiejętności wykazanych na egzaminie ustnym.

Liczba godzin pracy studenta związanych z osiągnięciem efektów kształcenia (opis):

1. *liczba godzin kontaktowych – **55 godz.**, w tym*
   - *udział w wykładach: **30 godz.**,*
   - *udział w zajęciach projektowych: **15 godz.**,*
   - *udział w konsultacjach związanych z realizacją przedmiotu: **8 godz.***
   - *udział w egzaminie: **2 godz.***

2. *praca własna studenta – **72 godz.**, w tym*
   - *analiza literatury i materiałów wykładowych związana z przygotowaniem do realizacji projektu: **30 godz.***
   - *realizacja projektu: **32 godz.**.*
   - *przygotowanie do egzaminu: **10 godz.***

Łączny nakład pracy studenta wynosi 127 godz., **co odpowiada** 5 pkt. **ECTS.**

Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich: 2 pkt. ECTS (55 godz. kontaktowych).

Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym: 3 pkt. ECTS (co odpowiada 81 godz. realizacji projektu)

Efekty kształcenia/uczenia się

efekty kształcenia/uczenia się student, który zaliczył przedmiot:	forma zajęć/ technika kształcenia	sposób weryfikacji (oceny)*
WIEDZA		
W1: ma wiedzę dotyczącą fundamentalnych pojęć z zakresu bezpieczeństwa teleinformatycznego	wykład + projekt	projekt, egzamin
W2: ma wiedzę na temat zagrożeń teleinformatycznych, ich źródeł i skali skutków	wykład + projekt	project, egzamin
W3: ma podstawową wiedzę z zakresu specyfikacji celów i funkcji zapewniających bezpieczeństwo teleinformatyczne	wykład	projekt egzamin
W4: ma podstawową wiedzę w zakresie: aktów prawnych, norm, standardów, rekomendacji	wykład	projekt egzamin
W5: ma wiedzę z zakresu analizowania ryzyka systemów teleinformatycznych	wykład	egzamin
W6: ma podstawową wiedzę na temat mechanizmów bezpieczeństwa, w tym: teleinformatycznych, oraz kryptograficznych	wykład + projekt	projekt, egzamin
W7: ma podstawową wiedzę na temat tworzenia polityk bezpieczeństwa, ich wdrażania, tworzenia dokumentacji, metod formalnych i półformalnych dowodzenia poprawności systemów	wykład + projekt	projekt, egzamin
W8: rozumie aspekty dotyczące ochrony infrastruktury krytycznej państwa	wykład + projekt	projekt, egzamin
UMIEJĘTNOŚCI		
U1: potrafi wykonać analizę możliwych zagrożeń i ich skalę	wykład + projekt	projekt
U2: potrafi wyspecyfikować cele i funkcje bezpieczeństwa dla systemu teleinformatycznego	wykład + projekt	projekt
U3: potrafi stworzyć plany bezpieczeństwa i je skutecznie wdrożyć	wykład + projekt	projekt
U4: potrafi stosować środki techniczne zapewniające bezpieczeństwo teleinformatyczne, kryptograficzne	wykład + projekt	projekt
U7: potrafi stworzy plany monitoringu, oraz procesy obsługi i zarządzania incydentami	wykład + projekt	projekt
U8: potrafi przeprowadzić analizę ryzyka	projekt	projekt
U9: potrafi krytycznie analizować dostępną literaturę z zakresu domeny wiedzy	projekt	projekt
KOMPETENCJE SPOŁECZNE		
KS1: ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy	wykład + projekt	project
KS2: ma orientację zawodową w obszarze bezpieczeństwa teleinformatycznego i jest świadomy procesu uczenia się w kierunku zwiększania kompetencji w tym obszarze	wykład + projekt	n/d

Uwagi:

Data i podpis autora (kierownika zespołu autorskiego):