KATALOG PRZEDMIOTÓW

Kierunek: Cyberbezpieczeństwo

Forma: niestacjonarne, interaktywne przez Internet
Co to są studia interaktywne?

Rodzaj: podyplomowe

Język: polski

Jednostka organizacyjna: Wyższa Szkoła Biznesu – National Louis University

Czas trwania: 2 semestry

Opłaty:
- 85 zł opłata rekrutacyjna
- 3 950 zł czesne (płatne w 10 ratach po 395 zł/mc)
- 30 zł opłata za dyplom

W przeciągu kilku ostatnich lat w raz z wzrostem cyfryzacji obserwuje się coraz większą liczbę przestępstw komputerowych, które po dogłębnych analizach wskazują coraz to większy poziom złożoności. Studia z zakresu cyberbezpieczeństwa poddadzą dogłębnej analizie sposoby zdobywania chronionych danych stanowiących często majątek firmy mając na celu ich skuteczne zabezpieczenie.

Dlatego też jedną z najważniejszych umiejętności nabytych na studiach będą informację związane z ochroną własności intelektualnych oraz RODO. Studia przygotowane zostały o najnowocześniejsze modele wykorzystywane w walce z przestępczością internetową, zabezpieczaniem danych komercyjnych jak i informacji niejawnych. Kursy zrealizowane w formie projektu kształtują podłoże do pracy zespołowej, podnosząc tym samym skuteczność pracy związanej z bezpieczeństwem sieci, systemów komputerowych czy też całej infrastruktury IT.

Masowy rozwój technologii sprawił iż dotychczasowe metody ochrony Internetu stały się przestarzałe i całkowicie nieskuteczne, dlatego studenci tych studiów w większości odbywać będą zajęcia z praktykami, co przedstawi panujący obraz w firmach oraz

pozwoli zdobyć pewnego rodzaju doświadczenie w tematyce cyberbezpieczeństwa, które bez wątpienia znajdzie swoje odzwierciedlenie w przyszłej pracy.

Studia podyplomowe są również doskonałym przygotowaniem do zawodu Inspektora Ochrony Danych Osobowych jak również dla zawodów odpowiedzialnych za utrzymanie infrastruktury teleinformatycznej, gdzie prócz aspektów prawnych absolwent zdobywa wiedzę z zakresu IT, na podstawie której może w własnym zakresie ocenić ryzyko przetwarzania danych oraz sposoby jego ograniczenia.

Administracja danymi osobowymi

Kod: NET_1_003.100

ECTS: 6

Liczba godzin: 30 (wykład: 30)

Forma zaliczenia przedmiotu: Z/E

Opis przedmiotu:

Kurs obejmuje wszystkie praktyczne aspekty europejskiego prawa i praktyki w zakresie ochrony danych osobowych. Analizie zostanie poddana problematyka danych osobowych, w tym zasady ich przetwarzania. W trakcie kursu szczegółowo przedstawione zostanie ogólne rozporządzenie o ochronie danych (RODO), a także odpowiednie decyzje Trybunału Sprawiedliwości oraz kluczowe wytyczne Europejskiej Rady Ochrony Danych i innych instytucji.

Treści programowe:

1. Terminologia i definicje.
2. Zasady ochrony danych.
3. Odpowiedzialność i przejrzystość.
4. Uzasadnienia przetwarzania danych.
5. Dane osobowe kategorii specjalnej.
6. Prawa osób fizycznych.
7. Bezpieczeństwo danych.
8. Powiadamianie o naruszeniach bezpieczeństwa.
9. Outsourcing.
10. Rola inspektora ochrony danych.
11. Oceny wpływu na ochronę danych.
12. Międzynarodowe przekazywanie danych.
13. Egzekwowanie przez organy nadzorcze.

Audyt bezpieczeństwa danych i analiza zagrożeń

Kod: NET_1_004.100

ECTS: 6

Liczba godzin: 30 (wykład: 15, ćwiczenia: 15)

Forma zaliczenia przedmiotu: Z/E

Opis przedmiotu:

Podstawowym elementem kursu jest pozyskanie przez studenta wiedzy na temat realizacji testów bezpieczeństwa z podziałem na testy manualne oraz automatyczne. Tworzenie raportów oraz oceny ryzyka, po przez wykorzystanie odpowiednich schematów oraz analizy przykładowej infrastruktury. W ramach powiązanej tematyki w trakcie kursu zostaną poruszone również techniczne aspekty odnoszące się do polityki bezpieczeństwa oraz przepisów RODO.

Treści programowe:

1. Audyt bezpieczeństwa w firmie.
2. Analiza ryzyka.
3. Polityka bezpieczeństwa.
4. Zabezpieczenie pracy zdalnej oraz urządzeń mobilnych.
5. Spotkanie z praktykiem - nowoczesne metody monitoringu infrastruktury.

Sieci komputerowe

Kod: ICT_1_012.100

ECTS: 6

Liczba godzin: 30 (wykład: 15, laboratorium: 15)

Forma zaliczenia przedmiotu: E

Opis przedmiotu:

Przedmiot obejmuje podstawy działania sieci komputerowych, w tym najważniejsze protokoły i mechanizmy oraz działanie najważniejszych urządzeń wykorzystywanych w sieciach (przełączników, koncentratorów, punktów dostępowych, routerów). Słuchacze zapoznają się ze stosem protokołów TCP/IP (w wersji IPv4 i IPv6), poznają technologie stosowane w przewodowych i bezprzewodowych lokalnych sieciach komputerowych. W stopniu podstawowym poznają też najważniejsze technologie stosowane w sieciach rozległych. Słuchacze poznają podstawy routowania i najważniejsze zagadnienia związane z bezpieczeństwem sieci komputerowych.

Treści programowe:

1. ABC sieci komputerowych.
2. Podstawowe pojęcia: procesy działające w sieci komputerowej, gdy programy komunikują się między sobą za pośrednictwem sieci (przykład: przeglądarka internetowa i serwer WWW).
3. Protokół ARP.
4. Enkapsulacja PDU.
5. IPv4.
6. ICMP.
7. Reguły adresowania IPv4: adresowanie klasowe i bezklasowe.
8. Routing statyczny.
9. Trasy domyślne i zmienne.
10. Routing dynamiczny - podstawowe pojęcia.
11. Protokoły routingu RIP, IGRP. Protokoły routingu EIGRP, OSPF.
12. TCP i UDP. Protokół drzewa opinającego. Sieci VLAN.
13. Podstawy asymetrycznych i symetrycznych metod szyfrowania.
14. Podpisy cyfrowe.
15. Bezpieczne protokoły (podstawy): SSL / TLS, IPSec.
16. IPv6.
17. Sieci Wi-Fi.
18. WAN.

Wprowadzenie do studiów

Kod: GEN_2_024.100

ECTS: 1

Liczba godzin: 30 (wykład: 9, projekt: 21)

Forma zaliczenia przedmiotu: Z

Opis przedmiotu:

Kurs wprowadzający do studiów i studiowania. Obejmuje swoim zakresem przedstawienie systemu szkolnictwa wyższego, sposobu funkcjonowania Naszej Uczelni (w tym zasad BHP oraz systemu CloudA) oraz problematyki studiów na tle rynku pracy. W drugiej części przedstawione są aspekty funkcjonowania biblioteki oraz standardy bibliograficzne oraz edycyjne obowiązujące na Uczelni.

Treści programowe:

1. System szkolnictwa wyższego
2. Wyższa Szkoła Biznesu - National-Louis University z siedzibą w Nowym Sączu.
3. Podstawowe akty prawa wewnętrznego
4. Organizacja procesu dydaktycznego z systemem CloudA
5. Zasady BHP
6. Rynek pracy. Wyzwania stojące przed studentem
7. Biblioteka w erze informatyzacji
8. Standardy edycyjne

Internet rzeczy

Kod: NET_1_005.100

ECTS: 6

Liczba godzin: 30 (wykład: 15, ćwiczenia: 15)

Forma zaliczenia przedmiotu: Z/E

Opis przedmiotu:

Kurs wprowadza w zagadnienia związane z Internetem rzeczy (IoT). Zakres przedmiotowy obejmuje technologię stosowane do budowy tego rodzaju urządzeń, sposób komunikacji, sposób przechowywania danych oraz rodzaje systemów rozproszonych potrzebnych do ich obsługi. Ważną kwestię będą stanowiły problemy bezpieczeństwa danych.

Treści programowe:

1. Wprowadzenie do internetu rzeczy (IoT).
2. Czujniki stosowane w IoT.
3. Platformy stosowane w IoT.
4. Sposoby komunikacji z urządzeniami IoT.
5. Sieciowe protokoły komunikacyjne IoT.
6. Gromadzenie danych oraz dockery.
7. Przetwarzanie oraz prezentacja wyników.
8. Bezpieczeństwo IoT.

Inżynieria systemowa

Kod: NET_1_001.100

ECTS: 6

Liczba godzin: 30 (wykład: 15, ćwiczenia: 15)

Forma zaliczenia przedmiotu: Z/E

Opis przedmiotu:

Przedmiot jest kontynuacja kursu systemy operacyjne, na zajęciach student zdobywa niezbędną wiedzę z zakresu utwardzania systemów operacyjnych jak również metod bezpiecznego przechowywania, przetwarzania oraz udostępniania danych, potwierdzając zdobyte umiejętności w postaci wygenerowanego raportu.

Treści programowe:

1. Metody bezpiecznych połączeń zdalnych.
2. Infrastruktura klucza publicznego.
3. Zasady oraz sposoby przyznawania uprawnień.
4. Bezpieczny transfer danych.
5. Podstawy utwardzania systemu operacyjnego – hardening.
6. Testy automatyczne systemów operacyjnych i generowanie raportów.

Kryptografia

Kod: NET_1_007.100

ECTS: 6

Liczba godzin: 30 (wykład: 15, ćwiczenia: 15)

Forma zaliczenia przedmiotu: Z/E

Opis przedmiotu:

Kurs stanowi wprowadzenie do współczesnej kryptografii i bezpieczeństwa komunikacji. Prezentowane treści dotyczą działania algorytmów kryptograficznych oraz protokołów. Kurs obejmuje pojęcia szyfrów blokowych i kodów uwierzytelniania wiadomości, szyfrowania klucza publicznego, podpisów cyfrowych, a także obejmuje typowe przykłady i zastosowania schematów, w tym AES, RSA-OAEP i algorytmu podpisu cyfrowego. Na przykładach praktycznych rozwiązań uczestnik uczy się projektowania, wykonania i oceny nowoczesnych rozwiązań z zakresu bezpieczeństwa.

Treści programowe:

1. Klasyczne (symetryczne) kryptosystemy monoalfabetyczne i polialfabetyczne (kryptosystem Cezara, Hilla, afiniczny, Vigenere'a, Beaufort'a, Playfair'a).
2. Częściowe odkrywanie sekretu; Dowody o wiedzy zerowej.
3. Protokół kryptograficzny – wprowadzenie; Rzut monetą przez telefon; poker telefoniczny.
4. Krzywe eliptyczne; kryptografia na krzywych eliptycznych.
5. Logarytm dyskretny i przydzielanie kluczy; ciała Galois cd.; kryptosystem Rabina, ElGamala, McEliece; podpis elektroniczny – wykorzystanie RSA.
6. Problemy faktoryzacji; algorytm oparty na krzywych eliptycznych; podstawy teorii krzywych eliptycznych.
7. Liczby pseudopierwsze – testy pierwszości: Fermata, Solovaya-Strassena, Millera-Rabina.
8. Algorytm Shamira przełamania kryptosystemu plecakowego, elementy teorii krat i algorytm LLL; tw. uzasadniające poprawność.
9. Idea klucza publicznego, funkcje jednokierunkowe; problem plecakowy i kryptosystem plecakowy.
10. AES; elementy ciał Galois.
11. DES, schemat Feistela; kryptoanaliza różnicowa; metody probabilistyczne.

12. Maszyny rotorowe – ENIGMA; podstawy teoretyczne; historia; tw. które rozstrzygnęło II wojnę światową.
13. Twierdzenia i algorytmy z arytmetyki modularnej i podstaw teorii liczb.

Laboratorium Hack the Box

Kod: NET_1_002.100

ECTS: 6

Liczba godzin: 45 (ćwiczenia: 15, projekt: 30)

Forma zaliczenia przedmiotu: Z

Opis przedmiotu:

Laboratorium Hack the Box ma na celu zdobycie umiejętności praktycznych, pracy w grupie oraz zdolności analitycznego myślenia. Kurs polega na zdobywaniu flag po przez wykryte podatności w wyspecjalizowanym laboratorium zdalnym, wykorzystując do tego celu połączenie VPN. W zależności od zdobytych uprawnień w ramach jednego z dziesięciu dostępnych systemów operacyjnych student ma możliwość przejęcia dwóch flag, zwykłego użytkownika lub użytkownika z uprawnieniami administracyjnymi.

Treści programowe:

1. Rekonesans systemów operacyjnych.
2. Podstawy Sniffingu.
3. Klasyfikacja podatności.
4. Rodzaje ataków - Spoofing, DoS/DDoS, SQL injection, XXS.
5. Zastosowanie freamework-ów - Metasploit .