Cyberbezpieczeństwo - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Cyberbezpieczeństwo
Kod przedmiotu	TI11.3-WE-PD-Cbzp
Wydział	Wydział Informatyki, Elektrotechniki i Automatyki
Kierunek	Technologie informatyczne
Profil	ogólnoakademicki
Rodzaj studiów	podyplomowe
Semestr rozpoczęcia	semestr zimowy 2018/2019

Informacje o przedmiocie

Semestr	1
Liczba punktów ECTS do zdobycia	4
Typ przedmiotu	obowiązkowy
Język nauczania	polski
Sylabus opracował	• dr hab. inż. Bartłomiej Sulikowski, prof. UZ

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	-	-	7 (w tym jako e-learning)	0,47 (w tym jako e-learning)	Egzamin
Laboratorium	-	-	14 (w tym jako e-learning)	0,93 (w tym jako e-learning)	Zaliczenie na ocenę

Cel przedmiotu

Zapoznanie słuchaczy z zagadnieniami związanymi z bezpieczeństwem danych cyfrowych oraz bezpiecznego korzystania z Internetu. Prezentacja mechanizmów zabezpieczeń oraz zagrożeń w sieci Internet. Nauczenie i wykształcenie wymogu korzystania z tzw. dobrych praktyk bezpieczeństwa. Wykształcenie umiejętności rozpoznawania zagrożeń występujących w Internecie. Prezentacja przykładów mechanizmów zabezpieczających transakcje zawierane za pośrednictwem sieci Internet oraz mechanizmów zdalnej autoryzacji i autentykacji stron transakcji internetowych.

Wymagania wstępne

Brak

Zakres tematyczny

Bezpieczeństwo komputerów osobistych. Typy złośliwego oprogramowania (malware), mechanizmy jego dystrybucji i sposoby ochrony przed nim. Bezpieczeństwo systemów z rodziny MS Windows i Linux. Uaktualnienia systemowe. Oprogramowanie antywirusowe. Firewalle programowe. Kopie bezpieczeństwa.

Kradzieże danych osobistych. *Phishing* i ochrona przed nim.

Podstawy kryptograficznej ochrony danych. Algorytmy symetryczne i asymetryczne. Funkcje skrótu. Zastosowania algorytmów kryptograficznych w praktyce biznesowej. Metody kryptoanalizy.

Kontrolowanie dostępu do danych chronionych. Metody autentykacji i autoryzacji użytkowników oraz stron transakcji. Mechanizmy ochrony przechowywania danych wrażliwych. Szacowanie siły haseł i mocy mechanizmów zabezpieczających dostęp do danych. Włamania do systemów – rozpoznawanie i zapobieganie. Potencjalne konsekwencje kradzieży danych cyfrowych.

Zagrożenia systemów teleinformatycznych. Ataki DoS i DDoS. Ochrona przesyłu danych. Sieci VPN. Ataki typu *„Man in the Middle”* i *„spoofing”* – rozpoznawanie i reagowanie. Inne typy ataków (SQL injection, XSS scripting). Zapewnianie bezpieczeństwa elektronicznego środkami sprzętowymi (role firewalli sprzętowych, mechanizmy IDS/IPS, koncentratory VPN, routery z zintegrowanymi usługami).

Bezpieczeństwo urządzeń mobilnych. Zasady bezpiecznego korzystania ze smartphone’ów, tabletów, notebooków. Bezpieczeństwo transakcji z wykorzystaniem kart bankowych. Bezpieczeństwo kart bezprzewodowych (MasterCard PayPass i Visa PayWave). Mechanizmy zabezpieczeń popularnych systemów operacyjnych urządzeń mobilnych (Android, IOS, Windows).

Podpis cyfrowy. Mechanizm składania i weryfikacji podpisu. Ustawa o podpisie elektronicznym. Usługi dodatkowe (znakowanie czasem, podpis wielokrotny itp). Podpis kwalifikowany. Posługiwanie się certyfikatami.

Bezpieczne zawieranie transakcji. Protokół SSL. Autoryzacja kontrahenta na podstawie certyfikatów. Zagrożenia związane z korzystaniem z certyfikatów.

Mechanizmy zabezpieczania transakcji internetowych na wybranych przykładach: bankowość elektroniczna - dostęp do rachunków bankowych, wykonywanie operacji bankowych; funkcjonowanie sklepów elektronicznych; elektroniczne systemy funkcjonowania państwa: urzędy skarbowe, e-sąd, elektroniczne biura podawcze itp.

Metody kształcenia

Wykład - wykład konwencjonalny z wykorzystaniem wideoprojektora.

Laboratorium - zajęcia praktyczne w laboratorium komputerowym.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Zna mechanizmy bezpiecznego przechowywania i przesyłu danych cyfrowych; rozumie zagrożenia wynikające z braku lub stosowanie zbyt słabych zabezpieczeń	• K_W05	• egzamin - ustny, opisowy, testowy i inne	• Wykład
Ma świadomość zagrożeń, jakie niesie ze sobą powszechne używanie środków komunikacji sieciowej	• K_U02 • K_U07 • K_K03	• Przeprowadzenie eksperymentów Analiza wyników przeprowadzonych testów Udział w dyskusji	• Wykład • Laboratorium
Ma świadomość roli społecznej absolwenta uczelni technicznej, a zwłaszcza rozumie potrzebę formułowania i przekazywania społeczeństwu informacji na temat aspektów działalności inżynierskiej i biznesowej w sposób powszechnie zrozumiały	• K_K03	• Udział w dyskusji	• Wykład • Laboratorium
Rozumie konieczność ciągłego uaktualniania wiedzy odnośnie bezpieczeństwa systemu związanego z rozwojem wiedzy i technologii	• K_K01	• udział w dyskusji	• Wykład • Laboratorium
Rozumie konieczność stosowania algorytmów i protokołów kryptograficznych w celu ochrony danych	• K_W05	• egzamin - ustny, opisowy, testowy i inne	• Wykład
Potrafi w sposób bezpieczny przeprowadzić transakcje elektroniczne	• K_U02 • K_U07	• Przeprowadzenie eksperymentów, Analiza wyników przeprowadzonych testów	• Laboratorium

Warunki zaliczenia

Weryfikacja efektów kształcenia będzie odbywała się dwutorowo tzn. zdobycie wiedzy i umiejętności merytorycznych będzie sprawdzane poprzez sprawdzian(y) wiadomości, a kompetencje społeczne poprzez moderowaną przez prowadzącego zajęcia dyskusję.

Wykład - sprawdzian w formie pisemnej realizowany na koniec semestru.

Laboratorium – ocena końcowa stanowi sumę ważoną ocen uzyskanych za realizację poszczególnych ćwiczeń laboratoryjnych.

Ocena końcowa = 50 % oceny zaliczenia z formy zajęć wykład + 50 % oceny zaliczenia z formy zajęć laboratorium.

Literatura podstawowa

1. Kępa, L., Tomasik, P., Dobrzyński, S., Bezpieczeństwo systemu e-commerce, czyli jak bez ryzyka prowadzić biznes w internecie, Gliwice, Helion, 2013.
2. Liderman, K., Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, 2009.
3. Cichoń, M., Biblia e-biznesu, Gliwice, Helion, 2013.

Literatura uzupełniająca

1. Lukatsky, A., Wykrywanie włamań i aktywna ochrona danych, Helion, 2004.
2. Stallings, W., Kryptografia i bezpieczeństwo sieci komputerowych, Tomy 1-2, Helion, 2012.
3. Lehtinen, R., i in., Podstawy ochrony komputerów, Helion (O'Reilly), 2007.
4. Russell, R., i in., Hakerzy atakują. Jak przejąć kontrolę nad siecią, Helion, 2004.

Uwagi

Zmodyfikowane przez dr inż. Anna Pławiak-Mowna, prof. UZ (ostatnia modyfikacja: 27-05-2018 09:00)