AGH UNIVERSITY OF SCIENCE AND TECHNOLOGY

Nazwa modułu: Bezpieczeństwo systemów teleinformatycznych

Rok akademicki: 2014/2015 Kod: ITE-1-603-s Punkty ECTS: 3

Wydział: Informatyki, Elektroniki i Telekomunikacji

Kierunek: Teleinformatyka Specjalność: —

Poziom studiów: Studia I stopnia Forma i tryb studiów: Stacjonarne

Język wykładowy: Polski Profil kształcenia: Ogólnoakademicki (A) Semestr: 6

Strona www: http://www.kt.agh.edu.pl/~niemiec

Osoba odpowiedzialna: dr inż. Niemiec Marcin (niemiec@kt.agh.edu.pl)

Osoby prowadzące: dr inż. Niemiec Marcin (niemiec@kt.agh.edu.pl)

Krótka charakterystyka modułu

Moduł “Bezpieczeństwo systemów teleinformatycznych” jest wprowadzeniem do problematyki bezpieczeństwa i ochrony danych we współczesnych systemach teleinformatycznych.

Opis efektów kształcenia dla modułu zajęć

Kod EKM	Student, który zaliczył moduł zajęć wie/umie/potrafi	Powiązania z EKK	Sposób weryfikacji efektów kształcenia (forma zaliczeń)
Wiedza			
M_W001	Zna i rozumie podstawowe metody i usługi ochrony danych	TE1A_W04, TE1A_W19	Egzamin
M_W002	Dysponuje podstawową wiedzą z zakresu kryptografii	TE1A_W01, TE1A_W04, TE1A_W19	Egzamin
M_W003	Zna, potrafi rozpoznawać i sklasyfikować podstawowe zagrożenia bezpieczeństwa danych	TE1A_W14, TE1A_W19	Egzamin
M_W004	Zna i rozumie zasady działania zapór sieciowych oraz systemów wykrywania zagrożeń	TE1A_W15, TE1A_W14, TE1A_W07, TE1A_W19	Egzamin
M_W005	Potrafi podać przykładowe współczesne algorytmy kryptograficzne oraz zna różnice między szyframi symetrycznymi, szyframi asymetrycznymi i funkcjami skrótu	TE1A_W01, TE1A_W14, TE1A_W19	Egzamin
Umiejętności			

M_U001	Potrafi dobrać odpowiednią metodę ochrony w celu zapewnienia bezpieczeństwa systemu	TE1A_U11, TE1A_U12	Wykonanie ćwiczeń laboratoryjnych, Egzamin
M_U002	Potrafi wybrać algorytm kryptograficzny adekwatny do żądanego poziomu bezpieczeństwa, zasobów i wydajności	TE1A_U14, TE1A_U12	Wykonanie ćwiczeń laboratoryjnych, Egzamin
M_U003	Potrafi opracować politykę bezpieczeństwa dla typowego systemu teleinformatycznego	TE1A_U22, TE1A_U01, TE1A_U12	Wykonanie ćwiczeń laboratoryjnych, Egzamin
M_U004	Potrafi wykonać i zweryfikować podpis elektroniczny dokumentu/pliku	TE1A_U12, TE1A_U07	Wykonanie ćwiczeń laboratoryjnych, Egzamin
M_U005	Potrafi zbudować wirtualną sieć prywatną (VPN) w celu ochrony danych cyfrowych	TE1A_U11, TE1A_U12	Wykonanie ćwiczeń laboratoryjnych, Egzamin
Kompetencje społeczne			
M_K001	Orientuje się we współczesnych rozwiązaniach ochrony danych i może ocenić ich przydatność oraz wybrać rozwiązanie adekwatne do konkretnego systemu	TE1A_K06	Egzamin

Matryca efektów kształcenia w odniesieniu do form zajęć

Kod EKM	Student, który zaliczył moduł zajęć wie/umie/potrafi	Forma zajęć										
		Wykład	Ćwiczenia audytoryjne	Ćwiczenia laboratoryjne	Ćwiczenia projektowe	Konwersatorium	Zajęcia seminaryjne	Zajęcia praktyczne	Zajęcia terenowe	Zajęcia warsztatowe	Inne	E-learning
Wiedza												
M_W001	Zna i rozumie podstawowe metody i usługi ochrony danych	+	-	+	-	-	-	-	-	-	-	-
M_W002	Dysponuje podstawową wiedzą z zakresu kryptografii	+	-	+	-	-	-	-	-	-	-	-
M_W003	Zna, potrafi rozpoznawać i sklasyfikować podstawowe zagrożenia bezpieczeństwa danych	+	-	-	-	-	-	-	-	-	-	-
M_W004	Zna i rozumie zasady działania zapór sieciowych oraz systemów wykrywania zagrożeń	+	-	+	-	-	-	-	-	-	-	-
M_W005	Potrafi podać przykładowe współczesne algorytmy kryptograficzne oraz zna różnice między szyframi symetrycznymi, szyframi asymetrycznymi i funkcjami skrótu	+	-	+	-	-	-	-	-	-	-	-

Umiejętności												
M_U001	Potrafi dobrać odpowiednią metodę ochrony w celu zapewnienia bezpieczeństwa systemu	+	-	+	-	-	-	-	-	-	-	-
M_U002	Potrafi wybrać algorytm kryptograficzny adekwatny do żądanego poziomu bezpieczeństwa, zasobów i wydajności	+	-	+	-	-	-	-	-	-	-	-
M_U003	Potrafi opracować politykę bezpieczeństwa dla typowego systemu teleinformatycznego	+	-	-	-	-	-	-	-	-	-	-
M_U004	Potrafi wykonać i zweryfikować podpis elektroniczny dokumentu/pliku	+	-	+	-	-	-	-	-	-	-	-
M_U005	Potrafi zbudować wirtualną sieć prywatną (VPN) w celu ochrony danych cyfrowych	+	-	+	-	-	-	-	-	-	-	-
Kompetencje społeczne												
M_K001	Orientuje się we współczesnych rozwiązaniach ochrony danych i może ocenić ich przydatność oraz wybrać rozwiązanie adekwatne do konkretnego systemu	+	-	-	-	-	-	-	-	-	-	-

Treść modułu zajęć (program wykładów i pozostałych zajęć)

Wykład

1.Wprowadzenie do problematyki bezpieczeństwa (2 godz.)
Podstawowe pojęcia związane z bezpieczeństwem. Modele bezpieczeństwa w sieciach komputerowych i systemach informatycznych. Przykłady standardów związanych z bezpieczeństwem. Polityka bezpieczeństwa.
2.Podstawy kryptografii (2 godz.)
Podstawowe przekształcenia: podstawienie, permutacja. Kryptografia klasyczna. Schematy kryptograficzne. Steganografia.
3.Algorytmy kryptograficzne (4 godz.)
Współczesne szyfry symetryczne i asymetryczne. Szyfry blokowe i strumieniowe. Przykładowe algorytmy kryptograficzne.
4.Klucze kryptograficzne (2 godz.)
Dystrybucja i uzgadnianie kluczy kryptograficznych. Kryptografia kwantowa.
5.Usługi bezpieczeństwa (4 godz.)
Uwierzytelnianie. Autoryzacja. Poufność i prywatność. Integralność. Niezaprzeczalność.
6.Podpis cyfrowy i certyfikaty (4 godz.)
Klucze prywatne i publiczne. Podpis cyfrowy. Certyfikaty: tworzenie, odwoływanie. Infrastruktura klucza publicznego
7.Zastosowania i aplikacje (2 godz.)
Wirtualne sieci prywatne. Stosowane protokoły bezpieczeństwa.

8.Zagrożenia komputerowe, programy złośliwe i ataki sieciowe (4 godz.)
Wrażliwość systemu. Klasyfikacja zagrożeń. Ataki sieciowe (pasywne i aktywne). Programy złośliwe: klasyfikacja i przykłady. Zagrożenia. Pisanie bezpiecznego oprogramowania.
9.Zapory sieciowe i programy antywirusowe (2 godz.)
Zapory sieciowe. Rodzaje zapór. Metody wykrywania i blokowania ataków sieciowych. Programy antywirusowe.
10.Systemy wykrywania zagrożeń (2 godz.)
Sygnatury zagrożeń. Wykrywanie anomalii. Systemy wykrywania zagrożeń (Intrusion Detection and Prevention Systems).

Ćwiczenia laboratoryjne

1.Podstawy kryptografii, szyfrowanie i kontrola integralności (6 godz.)
2.Uwierzytelnianie i kontrola dostępu (2 godz.)
3.Podpis cyfrowy i certyfikaty (2 godz.)
4.Wirtualne sieci prywatne (4 godz.)
5.Aplikacje i protokoły bezpieczeństwa (4 godz.)
6.Ataki pasywne i aktywne (4 godz.)
7.Ochrona przed zagrożeniami (6 godz.)

Sposób obliczania oceny końcowej

1. Aby uzyskać pozytywną ocenę końcową (OK) niezbędne jest uzyskanie pozytywnej oceny z egzaminu oraz laboratorium (osiągnięte wyniki, sprawozdania, odpowiedzi ustne). Student ma prawo do jednokrotnego zaliczenia poprawkowego pod warunkiem praktycznego wykonania w ramach modułu nie mniej niż 80% wszystkich ćwiczeń laboratoryjnych.
2. Obliczamy średnią ważoną z ocen z laboratorium (30%) i egzaminu (70%).
3. Wyznaczmy ocenę końcową (OK):
- jeśli średnia jest większa niż 4,75, ocena końcowa to 5,0
- jeśli średnia jest większa niż 4,25 i nie większa niż 4,75, ocena końcowa to 4,5
- jeśli średnia jest większa niż 3,75 i nie większa niż 4,25, ocena końcowa to 4,0
- jeśli średnia jest większa niż 3,25 i nie większa niż 3,75, ocena końcowa to 3,5
- jeśli średnia nie jest większa niż 3,25, ocena końcowa to 3,0

Wymagania wstępne i dodatkowe

Znajomość podstaw matematyki, podstawowa znajomość systemów operacyjnych Linux i Windows, podstawy sieci komputerowych

Zalecana literatura i pomoce naukowe

1. Książki o tematyce bezpieczeństwa: np. Marek Ogiela “Systemy utajniania informacji”, William Stallings „Kryptografia i bezpieczeństwo sieci komputerowych”.
2. Artykuły z czasopism poruszających kwestie bezpieczeństwa, np. IEEE Security&Privacy.
3. Materiały z sieci Internet: strony producentów sprzętu i oprogramowania.
4. Zalecenia ITU-T i innych organizacji standaryzacyjnych (np. rekomendacja ITU-T X.805).

Publikacje naukowe osób prowadzących zajęcia związane z tematyką modułu

1. M. Niemiec, A. Pach, „Management of security in quantum cryptography”, IEEE Communications Magazine, vol. 51, no. 8, 2013
2. N. Stoianov , M. Uruena, M. Niemiec, P. Machnik, G. Maestro “Integrated security infrastructures for law enforcement agencies”, Multimedia Tools and Applications, vol. 74, no. 12, 2015
3. Tytus Kurek, Artur Lason, Marcin Niemiec, “First step towards preserving the privacy of cloud-based IDS security policies”, Security and Communication Networks, vol. 8 iss. 18, s. 3481–3491, 2015
4. Miralem Mehic, Marcin Niemiec, Miroslav Voznak, “Calculation of the key length for quantum key distribution”, Elektronika ir Elektrotechnika, vol. 21 no. 6, s. 81–85, 2015
5. Marcin Niemiec, Petr Machnik, “Authentication in virtual private networks based on quantum key

distribution methods”, Multimedia Tools and Applications, Springer US, 2016 vol. 75 iss. 17
6. Manuel Urueña, Petr Machník, Marcin Niemiec, Nikolai Stoianov, “Security architecture for law enforcement agencies”, Multimedia Tools and Applications, Springer US, 2016 vol. 75 iss. 17

Informacje dodatkowe
brak

Nakład pracy studenta (bilans punktów ECTS)

Forma aktywności studenta	Obciążenie studenta
Udział w wykładach	28 godz
Samodzielne studiowanie tematyki zajęć	14 godz
Udział w ćwiczeniach laboratoryjnych	28 godz
Przygotowanie sprawozdania, pracy pisemnej, prezentacji, itp.	14 godz
Sumaryczne obciążenie pracą studenta	84 godz
Punkty ECTS za moduł	3 ECTS