KRYPTOGRAFICZNE METODY OCHRONY INFORMACJI

Kod przedmiotu: KMOI2

Rodzaj przedmiotu: kierunkowy, obowiązkowy

Specjalność: ————

Wydział: Informatyki

Kierunek: Informatyka

Poziom studiów: drugiego stopnia – VII poziom PRK

Profil studiów: praktyczny

Forma studiów: stacjonarna/niestacjonarna

Rok: 1

Semestr: 1

Formy zajęć i liczba godzin:

Forma stacjonarna

wykłady – 15

laboratorium – 20

Forma niestacjonarna

wykłady – 10

laboratorium - 14

Zajęcia prowadzone są w języku polskim.

Liczba punktów ECTS: 3

Osoby prowadzące:

wykład:
laboratorium:

1. Założenia i cele przedmiotu:

Celem przedmiotu jest przekazanie studentom wiedzy na temat funkcjonowania nowoczesnych metod służących do ochrony prywatności danych, autentyfikacji użytkowników systemów komputerowych, zabezpieczania przed nieuprawnionymi modyfikacjami danych i innymi tego typu zastosowaniami opartymi na technikach kryptograficznych.

2. Określenie przedmiotów wprowadzających wraz z wymaganiami wstępnymi:

Wymogi wstępne dotyczą wiedzy związanej z podstawami zarządzania systemami operacyjnymi MS Windows oraz GNU/Linux.
Przedmioty wprowadzające: brak

3. Opis form zajęć

a) *Wykłady*

- **Treści programowe:**
  - Zagrożenia dla bezpieczeństwa informacji i sposoby przeciwdziałania tym zagrożeniom.
  - Jednokierunkowe funkcje skrótu. Typy ataków na funkcje jednokierunkowe.
  - Szyfry symetryczne.
  - Szyfry asymetryczne.
  - Zagadnienia dotyczące infrastruktury klucza publicznego oraz podpisu elektronicznego.
  - Zasady działania protokołu SSL/TLS.
  - Zarządzanie urzędem certyfikującym. Lista CRL oraz protokół OCSP.
  - Metody uwierzytelniania użytkowników stosowane w systemach teleinformatycznych (PAP, CHAP, MS-CHAP, LM, NTLM, Kerberos).
  - Szyfrowanie systemów plików.
  - Wykorzystanie protokołu IPsec.

- **Metody dydaktyczne:**
  - Wykład prowadzony jest w formie prezentacji, uzupełnionej przykładami rozwiązywanymi w trakcie wykładu na tablicy oraz na rzutniku multimedialnym. W ramach wykładu, prowadzący wspólnie ze studentami omawiają praktyczne zastosowania prezentowanych treści.

- **Forma i warunki zaliczenia:**
  - Warunkiem zaliczenia wykładu jest zdanie egzaminu końcowego z przedmiotu w formie pisemnej

- **Wykaz literatury podstawowej:**
  1. Materiały multimedialne dostępne online – http://www.moodle.wsti.pl
  2. Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka. T. 1. Gliwice: Helion, cop. 2019.
  3. N. Ferguson, B. Schneier: Kryptografia w praktyce. Helion 2004
  4. AumassonJ.-P.: Nowoczesna kryptografia : praktyczne wprowadzenie do szyfrowania. Warszawa: PWN, 2018.
  5. W. Stallings: Ochrona danych w sieci i intersieci w teorii i praktyce. WNT, Warszawa 1997
- **Wykaz literatury uzupełniającej:**
  1. K. Mitnick: Sztuka podstępu. Łamanie ludzi, nie haseł. Helion 2003
  2. J. Stokłosa, T. Bliski, T. Pankowski: Bezpieczeństwo danych w systemach informatycznych. PWN 2001
  3. M. Kutyłowski, W. Strothmann: Kryptografia, Lupus, 1998
  4. Forshaw J.: Atak na sieć okiem hakera. Wykrywanie i eksploatacja luk w zabezpieczeniach sieci. Gliwice: Helion, cop. 2019.

b) *Laboratorium*

- **Treści programowe:**

- Instalacja i konfiguracja roli Active Directory Certificate Services w systemie Windows Server,
- Zarządzanie certyfikatami w ramach urzędu certyfikacyjnego zintegrowanego z usługą Active Directory w systemie Windows Server, obsługa listy CRL oraz wykorzystanie protokołu OCSP,
- Wdrażanie usługi szyfrowania danych EFS z wykorzystaniem infrastruktury klucza publicznego,
- Wykorzystanie mechanizmu Bitlocker/Bitlocker To Go,
- Instalacja i konfiguracja infrastruktury klucza publicznego w systemie Linux (OpenSSL),
- Szyfrowanie danych na dysku w systemie GNU/Linux (GnuPG, dm-crypt, EncFS)
- Wdrożenie usługi IPsec,
- Konfiguracja uwierzytelnienia przy użyciu mechanizmu Kerberos w systemie GNU/Linux.

- **Metody dydaktyczne:**
  - W trakcie laboratorium prowadzący omawia zagadnienia związane z realizacją poszczególnych ćwiczeń z wykorzystaniem rzutnika multimedialnego, a następnie studenci samodzielnie realizują zadania określone przez prowadzącego opisane w platformie e-learningowej Moodle.

- **Forma i warunki zaliczenia**
  - Warunkiem zaliczenia przedmiotu jest uczestnictwo studenta na zajęciach laboratoryjnych oraz wykazanie się wiedzą z zakresu programu przedmiotu. Studenci uzyskują zaliczenie poprzez zdobycie określonej ilości punktów, przyznawanych za sprawozdania realizowane w trakcie zajęć, oraz sprawozdania zrealizowane z zadań do samodzielnego wykonania w domu po każdym laboratorium, oraz zaliczenia końcowego na ostatnich zajęciach. Zaliczenie otrzymuje student, który uzyskał określoną liczbę punktów, a o której informacja jest opublikowana na stronach WSTI. Ocenę z zaliczenia student uzyskuje w skali wskazanej w regulaminie studiów.

- **Wykaz literatury podstawowej:**
  1. Materiały multimedialne dostępne online – http://www.moodle.wsti.pl
  2. Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka. T. 1. Gliwice: Helion, cop. 2019.
  3. N. Ferguson, B. Schneier: Kryptografia w praktyce. Helion 2004
  4. AumassonJ.-P.: Nowoczesna kryptografia : praktyczne wprowadzenie do szyfrowania. Warszawa: PWN, 2018.
  5. W. Stallings: Ochrona danych w sieci i intersieci w teorii i praktyce. WNT, Warszawa 1997
- **Wykaz literatury uzupełniającej:**
  1. K. Mitnick: Sztuka podstępu. Łamanie ludzi, nie haseł. Helion 2003
  2. J. Stokłosa, T. Bliski, T. Pankowski: Bezpieczeństwo danych w systemach informatycznych. PWN 2001

3. M. Kutyłowski, W. Strothmann: Kryptografia, Lupus, 1998
4. Forshaw J.: Atak na sieć okiem hakera. Wykrywanie i eksploatacja luk w zabezpieczeniach sieci. Gliwice: Helion, cop. 2019

4. Opis sposobu wyznaczania punktów ECTS

a. forma stacjonarna

Forma zajęć	Formy aktywności studenta	Średnia liczba godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	15
	Czytanie wskazanej literatury	5
	Przygotowanie do egzaminu	15
Laboratorium	Kontakt z nauczycielem	20
	Czytanie wskazanej literatury	5
	Przygotowanie do pracy kontrolnej	5
	Samodzielne rozwiązywanie zadań	10

Całkowita ilość godzin aktywności studenta	**75**
Liczba punktów ECTS dla modułu/przedmiotu	**3**

b. forma niestacjonarna

Forma zajęć	Formy aktywności studenta	Średnia liczba godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	10
	Czytanie wskazanej literatury	10
	Przygotowanie do egzaminu	15
Laboratorium	Kontakt z nauczycielem	14
	Czytanie wskazanej literatury	10
	Przygotowanie do pracy kontrolnej	6
	Samodzielne rozwiązywanie zadań	10

Całkowita ilość godzin aktywności studenta	**75**
Liczba punktów ECTS dla modułu/przedmiotu	**3**

5. Wskaźniki sumaryczne

a. forma stacjonarna

a) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
   - Liczba godzin kontaktowych – 35
   - Liczba punktów ECTS – 1,4

b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
   - Liczba godzin kontaktowych – 20
   - Liczba punktów ECTS – 1,6

b. forma niestacjonarna

a) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
   - Liczba godzin kontaktowych – 24
   - Liczba punktów ECTS – 1,0

b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
   - Liczba godzin kontaktowych – 14
   - Liczba punktów ECTS – 1,6

6. Zakładane efekty uczenia się.

Efekt przedmiotowy (Symbol)	Efekty uczenia się dla przedmiotu	Odniesienie do kierunkowych efektów uczenia się
KMOI2_01	… ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie metod szyfrowania danych stosowanych w sieciach komputerowych, ze szczególnym uwzględnieniem Infrastruktury Klucza Publicznego	IIK_W01, IIK_W02, IIK_W03, IIK_W04, IIK_W05, IIK_W08, IIK_U05, IIK_U14, IIK_K04
KMOI2_02	… ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie metod uwierzytelniania użytkowników stosowane w systemach teleinformatycznych	IIK_W01, IIK_W02, IIK_W03, IIK_W04, IIK_W05, IIK_W08, IIK_U05, IIK_U14, IIK_K04
KMOI2_03	… ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie metod i mechanizmów szyfrowania danych na nośnikach danych	IIK_W01, IIK_W02, IIK_W03, IIK_W04, IIK_W05, IIK_W08, IIK_U05, IIK_U14, IIK_K04
KMOI2_04	**…** ma szczegółową i podbudowaną teoretycznie wiedzę w zakresie zarządzania urzędem certyfikującym	IIK_W01, IIK_W02, IIK_W03, IIK_W04, IIK_W05, IIK_W08, IIK_U05, IIK_U14, IIK_K04
KMOI2_05	… rozumie cele stosowania oraz zasady działania, i potrafi wdrożyć usługę IPsec na potrzeby zabezpieczenia transmisji danych w obrębie lokalnej sieci komputerowej	IIK_W01, IIK_W02, IIK_W03, IIK_W04, IIK_W05, IIK_W08, IIK_U05, IIK_U14, IIK_K04

7. Odniesienie efektów uczenia się do form zajęć i sposób oceny osiągnięcia przez studenta efektów uczenia się.

Efekt przedmiotowy (Symbol)	Forma zajęć		Sposób sprawdzenia osiągnięcia efektu
	Wykład	Laboratorium	

KMOI2_01	***v***	***v***	Egzamin, Sprawdzian praktyczny, sprawozdanie z laboratorium, sprawozdanie z zadania domowego
KMOI2_02	***v***	***v***	Egzamin, Sprawdzian praktyczny, sprawozdanie z laboratorium, sprawozdanie z zadania domowego
KMOI2_03	***v***	***v***	Egzamin, Sprawdzian praktyczny, sprawozdanie z laboratorium, sprawozdanie z zadania domowego
KMOI2_04	***v***	***v***	Egzamin, Sprawdzian praktyczny, sprawozdanie z laboratorium, sprawozdanie z zadania domowego
KMOI2_05	***v***	***v***	Egzamin, Sprawdzian praktyczny, sprawozdanie z laboratorium, sprawozdanie z zadania domowego

8. Kryteria uznania osiągnięcia przez studenta efektów uczenia się.

Efekt przedmiotowy (Symbol)	Efekt jest uznawany za osiągnięty, gdy student:
KMOI2_01	Poprawnie rozwiązuje zadania w czasie zajęć. Zalicza ponad 50% zadań do samodzielnej realizacji w domu. Zalicza ponad 50% pytań/zadań w sprawdzianie praktycznym.
KMOI2_02	Poprawnie rozwiązuje zadania w czasie zajęć. Zalicza ponad 50% zadań do samodzielnej realizacji w domu. Zalicza ponad 50% pytań/zadań w sprawdzianie praktycznym.
KMOI2_03	Poprawnie rozwiązuje zadania w czasie zajęć. Zalicza ponad 50% zadań do samodzielnej realizacji w domu. Zalicza ponad 50% pytań/zadań w sprawdzianie praktycznym.
KMOI2_04	Poprawnie rozwiązuje zadania w czasie zajęć. Zalicza ponad 50% zadań do samodzielnej realizacji w domu. Zalicza ponad 50% pytań/zadań w sprawdzianie praktycznym.
KMOI2_05	Poprawnie rozwiązuje zadania w czasie zajęć. Zalicza ponad 50% zadań do samodzielnej realizacji w domu. Zalicza ponad 50% pytań/zadań w sprawdzianie praktycznym.