BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH

Kod przedmiotu: BTS

Rodzaj przedmiotu: kierunkowy, obieralny

Specjalność: Technologie internetowe i sieci komputerowe

Wydział: Informatyki

Kierunek: Informatyka

Poziom studiów: pierwszego stopnia – VI poziom PRK

Profil studiów: praktyczny

Forma studiów: stacjonarna/niestacjonarna

Rok: 3

Semestr: 6

Formy zajęć i liczba godzin:

Forma stacjonarna

wykłady – 30

laboratorium – 20

Forma niestacjonarna

wykłady – 20

laboratorium – 15

Zajęcia prowadzone są w języku polskim.

Liczba punktów ECTS: 4

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, ochrony systemów komputerowych i sieci przed cyberatakami i innymi tego typu zastosowaniami opartymi przede wszystkim na technikach kryptograficznych.

2. Określenie przedmiotów wprowadzających wraz z wymaganiami wstępnymi:

Wymogi wstępne dotyczą wiedzy pobranej przez studentów na przedmiotach Systemy Operacyjne oraz Sieciowe Systemy Operacyjne.

3. Opis form zajęć

a) Wykłady

- **Treści programowe:**
  1. Logika działania oraz metody wykorzystania algorytmów haszujących.
  2. Algorytm HMAC, problematyka wykorzysta algorytmów haszujących do haszowania haseł dostęowych, oraz wykorzystanie mechanizmu tzw. soli dla haszowania haseł dostępowych.
  3. Logika działania oraz metody wykorzystania klucza symatrycznego.
  4. Logika działania oraz metody wykorzystania klucza asymetrycznego.
  5. Protokół PGP oraz infrastruktura klucza publicznego (PKI) jako rozwiązania weryfikacji autentyczności klucza publicznego.
  6. Logika działania oraz metody wykorzystania podpisu elektronicznego. Kwalifikowany a niekwalifikowany podpis elektroniczny.
  7. Logika działania protokołu SSL/TLS. Algorytm Diffiego-Hellmana.
  8. Rodzaje certyfikatów SSL, i kryteria ich wyboru.
  9. Budowa certyfikatu x.509, i formaty zapisu certyfikatów x.509
  10. Problematyka bezpieczeństwa przechowywania klucza prywatnego.
  11. Mechanizmy wsparcia procesu uwierzytelniania - 2FA, U2F, FIDO2.

- **Metody dydaktyczne**:

  Wykład prowadzony jest w formie prezentacji multimedialnej, 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 w formie pisemnej, zawierającego trzy pytania otwarte.

- **Wykaz literatury podstawowej**:
  1. Ferguson N., Schneier B.: Kryptografia w praktyce. Wyd. Helion, Gliwice 2004
  2. Adams C., Lloyd S.: PKI. Podstawy i zasady działania. Wyd. Helion, Gliwice 2007
  3. Aumasson Jean-Philippe: Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania, PWN 2018
  4. Marcin Karbowski: Podstawy kryptografii. Wydanie III. Helion 2014
  5. Douglas R. Stinson, Maura Paterson: Kryptografia W teorii i praktyce, PWN 2021

- **Wykaz literatury uzupełniającej**:
  1. Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka. T. 1. Gliwice: Helion, cop. 2019.
  2. B.Schneier: Kryptografia dla praktyków. WNT, Warszawa 2002

b) Ćwiczenia laboratoryjne

- **Treści programowe:**
  1. Przykłady wykorzystania algorytmów haszujących oraz klucza symetrycznego
  2. Wykorzystanie protokołu PGP oraz serwera SKS
  3. Podpis elektroniczny i szyfrowanie e-maili z wykorzystaniem certyfikatów S/MIME oraz OpenPGP
  4. Uwierzytelnianie z wykorzystaniem klucza asymetrycznego na przykładzie SSH
  5. Wykorzystanie certyfikatów SSL samopodpisanych na przykładzie kontenerów Docker oraz aplikacji NGINX Proxy Manager
  6. Wykorzystanie certyfikatów SSL od ZeroSSL na przykładzie kontenerów Docker oraz aplikacji NGINX Proxy Manager – jako przykład problematyki mechanizmów weryfikacji kupnych prawa własności do domeny DNS
  7. Zarządzanie certyfikatami SSL z Let's Encrypt
  8. Instalacja i konfiguracja infrastruktury klucza publicznego w systemie Linux

- **Metody dydaktyczne**:

  W trakcie laboratorium prowadzący omawia zagadnienia związane z realizacją poszczególnych ćwiczeń, a następnie studenci samodzielnie realizują zadania określone przez prowadzącego.

- **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 za sprawozdania z zadań do samodzielnej realizacji. 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. Ferguson N., Schneier B.: Kryptografia w praktyce. Wyd. Helion, Gliwice 2004
  2. Adams C., Lloyd S.: PKI. Podstawy i zasady działania. Wyd. Helion, Gliwice 2007
  3. Aumasson Jean-Philippe: Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania, PWN 2018
  4. Marcin Karbowski: Podstawy kryptografii. Wydanie III. Helion 2014
  5. Douglas R. Stinson, Maura Paterson: Kryptografia W teorii i praktyce, PWN 2021
  6. Jeeva S. Chelladhurai, Vinod Singh, Pethuru Raj: Docker dla praktyków. Wydanie II. Helion 2018

- **Wykaz literatury uzupełniającej**:
  1. Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka. T. 1. Gliwice: Helion, cop. 2019.
  2. B.Schneier: Kryptografia dla praktyków. WNT, Warszawa 2002
  3. Ferguson N., Schneier B.: Kryptografia w praktyce. Wyd. Helion, Gliwice 2004

4. Opis sposobu wyznaczania punktów ECTS

a. forma stacjonarna

Forma zajęć	Formy aktywności studenta	Średnia ilość godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	30
	Czytanie wskazanej literatury	15
	Przygotowanie do zaliczenia	15
Ćwiczenia	Kontakt z nauczycielem	45
	Czytanie wskazanej literatury	10
	Wykonanie zadań do samodzielnej realizacji w domu	10
	Realizacja projektu	25

Całkowita ilość godzin aktywności studenta	150
Liczba punktów ECTS dla modułu	6

b. forma niestacjonarna

Forma zajęć	Formy aktywności studenta	Średnia ilość godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	20
	Czytanie wskazanej literatury	20
	Przygotowanie do zaliczenia	20
Ćwiczenia	Kontakt z nauczycielem	20
	Czytanie wskazanej literatury	15
	Wykonanie zadań do samodzielnej realizacji w domu	20
	Realizacja projektu	35

Całkowita ilość godzin aktywności studenta	150
Liczba punktów ECTS dla modułu	6

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 – 75
   - Liczba punktów ECTS – 3,0

b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
   - Liczba godzin kontaktowych – 45
   - Liczba punktów ECTS – 3,6

b. forma niestacjonarna

a) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
   - Liczba godzin kontaktowych – 40
   - Liczba punktów ECTS – 1,6

b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
   - Liczba godzin kontaktowych – 20
   - Liczba punktów ECTS – 3,6

6. Zakładane efekty uczenia się

Efekt przedmiotowy (Symbol)	Efekty kształcenia dla przedmiotu	Odniesienie do kierunkowych efektów uczenia się
BTS_01	… posiada szczegółową i podbudowaną teoretycznie wiedzę w zakresie działania oraz metod wykorzystania algorytmów haszujących, klucza symetrycznego i klucza asymetrycznego	K_W04, K_W06 K_U01, K_U18 K_K01
BTS_02	… posiada szczegółową i podbudowaną teoretycznie wiedzę w zakresie możliwości praktycznego wykorzystania klucza asymetrycznego, a w szczególności różnic praktycznych pomiędzy protokołem PGP a Infrastrukturą Klucza Publicznego	K_W04, K_W06 K_K01 K_U24
BTS_03	… posiada szczegółową i podbudowaną teoretycznie wiedzę w zakresie zarządzania autonomicznym lokalnym urzędem certyfikującym, oraz logiki wykorzystania certyfikatów SSL, jak i certyfikatów S/MIME	K_W04, K_W06 K_U02, K_U24
BTS_04	… posiada świadomość celów stosowania, i potrafi odpowiednio wykorzystać technologię podpisu elektronicznego w ramach systemów informatycznych	K_W06, K_U24
BTS_05	… posiada świadomość celów oraz metod wykorzystania mechanizmów wsparcia procesu uwierzytelniania takich jak: 2FA, U2F, FIDO2	K_W06, K_U24
BTS_06	… potrafi zrealizować projekt obejmujący zabezpieczenie lokalnej infrastruktury kontenerów Docker z wykorzystaniem mechanizmów kryptografii, certyfikatów SSL, oraz sieci izolowanej VPN	K_W06, K_W12 K_W13, K_W14 K_W15, K_U02 K_U05, K_U11 K_U13, K_U15 K_U18, K_U19 K_K01, K_K03 K_U24

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

Efekt nr	Forma zajęć		Sposób sprawdzenia osiągnięcia efektu
	wykład	ćwiczenia	
BTS_01	*v*	*v*	Egzamin, sprawozdania z laboratorium
BTS_02	*v*	*v*	Egzamin, sprawozdania z laboratorium
BTS_03	*v*	*v*	Egzamin, sprawozdania z laboratorium
BTS_04	*v*	*v*	Egzamin, sprawozdania z laboratorium
BTS_05	*v*		Egzamin
BTS_06		*v*	Projekt, prezentacja osiągniętych wyników w projekcie

8. Kryteria uznania osiągnięcia przez studenta efektów uczenia się.

Efekt	Efekt jest uznawany za osiągnięty gdy:
BTS_01	a) student sporządził sprawozdania z zadań laboratoryjnych oraz sprawozdań do samodzielnej realizacji, zawierające poprawnie wykonane założone ćwiczenia, b) student zaliczy pracę kontrolną w formie egzaminu pisemnego z wykładu, zawierającego 3 pytania otwarte
BTS_02	a) student sporządził sprawozdania z zadań laboratoryjnych oraz sprawozdań do samodzielnej realizacji, zawierające poprawnie wykonane założone ćwiczenia, b) student zaliczy pracę kontrolną w formie egzaminu pisemnego z wykładu, zawierającego 3 pytania otwarte
BTS_03	a) student sporządził sprawozdania z zadań laboratoryjnych oraz sprawozdań do samodzielnej realizacji, zawierające poprawnie wykonane założone ćwiczenia, b) student zaliczy pracę kontrolną w formie egzaminu pisemnego z wykładu, zawierającego 3 pytania otwarte
BTS_04	a) student sporządził sprawozdania z zadań laboratoryjnych oraz sprawozdań do samodzielnej realizacji, zawierające poprawnie wykonane założone ćwiczenia, b) student zaliczy pracę kontrolną w formie egzaminu pisemnego z wykładu, zawierającego 3 pytania otwarte
BTS_05	student zaliczy pracę kontrolną w formie egzaminu pisemnego z wykładu, zawierającego 3 pytania otwarte
BTS_06	student wykonał samodzielny projekt obejmujący zabezpieczenie lokalnej infrastruktury kontenerów Docker z wykorzystaniem mechanizmów kryptografii, certyfikatów SSL, oraz sieci izolowanej VPN, oraz zaprezentował to rozwiązanie wykładowcy