Załącznik nr 9
do Zarządzenia Rektora PŚk Nr 35/19
w brzmieniu ustalonym Zarządzeniem Nr 12/22

# KARTA PRZEDMIOTU

| | | |
|---|---|---|
| Kod przedmiotu | studia stacjonarne: | |
| | studia niestacjonarne: | |
| Nazwa przedmiotu | **Podstawy bezpieczeństwa systemów komputerowych** | |
| Nazwa przedmiotu w języku angielskim | **Essentials of computer systems security** | |
| Obowiązuje od roku akademickiego | **2022/23** | |

## USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

| | |
|---|---|
| Kierunek studiów | **Informatyka** |
| Poziom kształcenia | **I stopień** |
| Profil studiów | **ogólnoakademicki** |
| Forma i tryb prowadzenia studiów | **studia stacjonarne i niestacjonarne** |
| Zakres | **Systemy informacyjne** |
| Jednostka prowadząca przedmiot | **Katedra Informatyki, Elektroniki i Elektrotechniki** |
| Koordynator przedmiotu | **dr hab. inż. Filip Rudziński, prof. PŚk** |
| Zatwierdził | **Dziekan Wydziału Elektrotechniki, Automatyki i Informatyki<br>dr hab. inż. Roman Deniziak, prof. PŚk** |

## OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

| | | |
|---|---|---|
| Przynależność do grupy/bloku przedmiotów | | **przedmiot kierunkowy** |
| Status przedmiotu | | **obowiązkowy** |
| Język prowadzenia zajęć | | **polski** |
| Usytuowanie w planie studiów - semestr | studia stacjonarne | **semestr VII** |
| | studia niestacjonarne | **semestr VII** |
| Wymagania wstępne | | **brak** |
| Egzamin (TAK/NIE) | | **NIE** |
| Liczba punktów ECTS | | **3** |

| **Forma prowadzenia zajęć** | | **wykład** | **ćwiczenia** | **laboratorium** | **projekt** | **inne** |
|---|---|---|---|---|---|---|
| **Liczba godzin w semestrze** | studia stacjonarne: | **15** | | | **30** | |
| | studia niestacjonarne: | **9** | | | **18** | |

## EFEKTY UCZENIA SIĘ

| Kategoria | Symbol efektu | Efekty uczenia się | Odniesienie do efektów kierunkowych |
|---|---|---|---|
| Wiedza | W01 | Student zna i rozumie zagadnienia z obszaru kryptografii symetrycznej i asymetrycznej. | INF1_W32 |
| | W02 | Student zna i rozumie zagrożenia bezpieczeństwa systemów operacyjnych i aplikacji oraz narzędzia do przeciwdziałania im. | INF1_W32 |
| | W03 | Student zna i rozumie zagrożenia bezpieczeństwa infrastruktury sieciowej i usług sieciowych, baz danych oraz narzędzia do przeciwdziałania im. | INF1_W23 |
| Umiejętności | U01 | Student potrafi wykorzystać implementacje algorytmów szyfrowania danych w wybranych problemach kryptograficznych | INF1_U32 |
| | U02 | Student potrafi poprawnie konfigurować system operacyjny w celu osiągnięcia zakładanego poziomu bezpieczeństwa danych lokalnych. | INF1_U32 |
| | U03 | Student potrafi poprawnie konfigurować serwery sieciowe w celu osiągnięcia zakładanego poziomu bezpieczeństwa danych w sieci | INF1_U32 |
| | U04 | Student potrafi dokonać analizy zagrożeń systemu komputerowego i właściwie dobrać narzędzia i zabezpieczenia przeciwdziałające im. | INF1_U32 |
| Kompetencje społeczne | K01 | Student jest gotów do uznania znaczenia wiedzy z obszaru bezpieczeństwa systemów komputerowych oraz potrzeby ciągłego jej poszerzania | INF1_K01 |
| | K02 | Student jest gotów do krytycznej oceny posiadanych umiejętności w zakresie bezpieczeństwa systemów komputerowych i rozumie potencjalne skutki swojej działalności na podstawie niewystarczających umiejętności | INF1_K02 |

## TREŚCI PROGRAMOWE

| Forma zajęć | Treści programowe |
|---|---|
| wykład | 1. **Wprowadzenie do bezpieczeństwa systemów komputerowych** (elementy kryptografii, zagrożenia systemów komputerowych, wybrane strategie i rozwiązania, polityka bezpieczeństwa w zarysie).<br>2. **Kryptosystemy symetryczne** (szyfry afiniczne, monoalfabetyczne, homomorficzne i polialfabetyczne, kaskadowe algorytmy szyfrowania danych, algorytm Lucifer, algorytm DES, tryby funkcjonowania DES, algorytm 3DES, algorytmy FEAL, IDEA, RC6, Rijndael, Serpent, Twofish, MARS).<br>3. **Kryptosystemy asymetryczne** (algorytm RSA i jego złożoność obliczeniowa, algorytmy: Merklego-Hellmana, ElGamal, protokół wymiany kluczy Diffiego-Hellmana, kryptosystemy hybrydowe w zarysie).<br>4. **Funkcje mieszające i generatory liczb pseudolosowych** (wprowadzenie do funkcji mieszających, mieszanie szeregowe i równoległe, algorytmy MD5 i SHA-1, mieszanie bazujące na kryptosystemach – schematy Rabina i Daviesa, schematy z kluczem prywatnym CBC i CFB, generatory liniowe, bitowe, bazujące na odejmowaniu z pożyczką i mnożeniu z przeniesieniem, bezpieczeństwo generatorów, testy generatorów – test Pi, wartości oczekiwanej, wariancji, itp).<br>5. **Wybrane elementy bezpieczeństwa systemów operacyjnych** (złośliwe oprogramowanie: wirusy, konie trojańskie, itp., oprogramowanie zabezpieczające: zapory ogniowe, antywirusowe, itp., konfiguracja kont i uprawnień użytkowników).<br>6. **Wybrane elementy bezpieczeństwa infrastruktury sieciowej** i **usług sieciowych** (sieci VPN typu użytkownik – serwer oraz serwer – serwer, protokoły PPTP, L2TP i SSTP, protokół IPSec, certyfikaty bezpieczeństwa, serwery proxy, bezpieczeństwo usług WWW, poczty elektronicznej, komunikatorów internetowych, itp., protokoły SSH i SSL, tunelowanie portów).<br>7. **Wybrane elementy bezpieczeństwa aplikacji bazodanowych** (projekt relacyjnej bazy danych z wykorzystaniem procedur składowanych, ukrywanie schematu bazy danych, konfigurowanie uprawnień użytkowników, bezpieczne połączenia klient-serwer, zabezpieczanie przed utratą danych). |

| | |
|---|---|
| projekt | 1. **Projekt symetrycznego systemu kryptograficznego** (komputerowa implementacja systemu do szyfrowania/deszyfrowania danych z wykorzystaniem wybranego kryptosystemu symetrycznego i języka programowania).<br>2. **Projekt asymetrycznego systemu kryptograficznego** (komputerowa implementacja systemu do szyfrowania/deszyfrowania danych z wykorzystaniem wybranego kryptosystemu asymetrycznego i języka programowania).<br>3. **Badanie funkcji skrótu i generatorów liczb pseudolosowych** (komputerowa implementacja systemu do wyznaczania wartości funkcji skrótu z wiadomości oraz przeprowadzenie symulacji dotyczących odporności funkcji na tzw. atak urodzinowy, przeprowadzenie testów wybranych generatorów liczb pseudolosowych (test wartości oczekiwanej, wariancji, Pi).<br>4. **Projekt bezpiecznego serwera usług sieciowych** (projekt serwera usług sieciowych FTP, HTTP, POP3, IMAP, SMTP, i inne z wykorzystaniem systemu operacyjnego MS Windows Server, w tym konfiguracja zapory ogniowej, konfiguracja kont użytkowników i zabezpieczenia ich przed nieuprawnionym dostępem do danych).<br>5. **Projekt bezpiecznego połączenia VPN** (projekt konfiguracji bezpiecznego połączenia pomiędzy komputerami w ramach sieci VPN (połączenie serwera i stacji roboczej) z wykorzystaniem systemu operacyjnego MS Windows Server i protokołu SSTP).<br>6. **Projekt bezpiecznej bazy danych** (projekt relacyjnej bazy danych z wykorzystaniem procedur składowanych, konfiguracja kont i uprawnień użytkowników, implementacja aplikacji klient-serwer). |

## METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

| Symbol efektu | Metody sprawdzania efektów uczenia się | | | | | |
|---|---|---|---|---|---|---|
| | Egzamin ustny | Egzamin pisemny | Kolokwium | Projekt | Sprawozdanie | Inne |
| W01 | | | | X | | |
| W02 | | | | X | | |
| W03 | | | | X | | |
| U01 | | | | X | | |
| U02 | | | | X | | |
| U03 | | | | X | | |
| U04 | | | | X | | |
| K01 | | | | X | | |
| K02 | | | | X | | |

## FORMA I WARUNKI ZALICZENIA

| Forma zajęć | Forma zaliczenia | Warunki zaliczenia |
|---|---|---|
| wykład | zaliczenie z oceną | Uzyskanie co najmniej 50% punktów z projektów. |
| projekt | zaliczenie z oceną | Uzyskanie co najmniej 50% punktów z projektów. |

## NAKŁAD PRACY STUDENTA

<table>
<tr><th colspan="13">Bilans punktów ECTS</th></tr>
<tr><th rowspan="3">Lp.</th><th rowspan="3">Rodzaj aktywności</th><th colspan="10">Obciążenie studenta</th><th>Jed-nostka</th></tr>
<tr><th colspan="5">studia stacjonarne</th><th colspan="5">studia niestacjonarne</th><th></th></tr>
<tr><td rowspan="2">1.</td><td rowspan="2">Udział w zajęciach zgodnie z planem studiów</td><td>W</td><td>C</td><td>L</td><td>P</td><td>S</td><td>W</td><td>C</td><td>L</td><td>P</td><td>S</td><td rowspan="2">h</td></tr>
<tr><td>15</td><td></td><td></td><td>30</td><td></td><td>9</td><td></td><td></td><td>18</td><td></td></tr>
<tr><td>2.</td><td>Inne (konsultacje, egzamin)</td><td>1</td><td></td><td></td><td>2</td><td></td><td>1</td><td></td><td></td><td>2</td><td></td><td>h</td></tr>
<tr><td>3.</td><td>Razem przy bezpośrednim udziale nauczyciela akademickiego</td><td colspan="5">48</td><td colspan="5">30</td><td>h</td></tr>
<tr><td>4.</td><td>Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego</td><td colspan="5">1,92</td><td colspan="5">1,2</td><td>ECTS</td></tr>
<tr><td>5.</td><td>Liczba godzin samodzielnej pracy studenta</td><td colspan="5">27</td><td colspan="5">45</td><td>h</td></tr>
<tr><td>6.</td><td>Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy</td><td colspan="5">1,08</td><td colspan="5">1,8</td><td>ECTS</td></tr>
<tr><td>7.</td><td>Nakład pracy związany z zajęciami o charakterze praktycznym</td><td colspan="5">30</td><td colspan="5">18</td><td>h</td></tr>
<tr><td>8.</td><td>Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym</td><td colspan="5">1,2</td><td colspan="5">0,72</td><td>ECTS</td></tr>
<tr><td>9.</td><td>Sumaryczne obciążenie pracą studenta</td><td colspan="5">75</td><td colspan="5">75</td><td>h</td></tr>
<tr><td>10.</td><td>Punkty ECTS za moduł<br>1 punkt ECTS=25 godzin obciążenia studenta</td><td colspan="10">3</td><td>ECTS</td></tr>
</table>

## LITERATURA


1. Pieprzyk J., Hardjono T., Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion, 2005.
2. Stallings W., Network Security Essentials. Prentice Hall, 2003.
3. Stokłosa J., Bliski T., Pankowski T., Bezpieczeństwo danych w systemach informatycznych. PWN, 2001.
4. Ferguson N., Schneier B., Kryptografia w praktyce., Helion, 2004.
5. Cheswick W. R. Firewalle i bezpieczeństwo w sieci. Helion, 2003.