POLITECHNIKA GDAŃSKA

Karta przedmiotu

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Nazwa i kod przedmiotu | Information Systems Security, PG_00055353 | | | | | | |
| Kierunek studiów | Elektronika i telekomunikacja (studia w jęz. angielskim) | | | | | | |
| Data rozpoczęcia studiów | październik 2023 r. | | Rok akademicki realizacji przedmiotu | 2024/2025 | | | |
| Poziom kształcenia | II stopnia | | Grupa zajęć | Grupa zajęć obowiązkowych z zakresu kierunku studiów<br>Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki | | | |
| Forma studiów | stacjonarne | | Sposób realizacji | na uczelni | | | |
| Rok studiów | 2 | | Język wykładowy | polski | | | |
| Semestr studiów | 4 | | Liczba punktów ECTS | 3.0 | | | |
| Profil kształcenia | ogólnoakademicki | | Forma zaliczenia | zaliczenie | | | |
| Jednostka prowadząca | Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Sieci Teleinformacyjnych | | | | | | |
| Imię i nazwisko wykładowcy (wykładowców) | Odpowiedzialny za przedmiot | dr inż. Bartosz Czaplewski | | | | | |
| | Prowadzący zajęcia z przedmiotu | dr inż. Bartosz Czaplewski | | | | | |

| Formy zajęć i metody nauczania | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Forma zajęć | Wykład | Ćwiczenia | Laboratorium | Projekt | Seminarium | RAZEM |
| | Liczba godzin zajęć | 30.0 | 0.0 | 15.0 | 0.0 | 0.0 | 45 |
| | W tym liczba godzin zajęć na odległość: 0.0 | | | | | | |

| Aktywność studenta i liczba godzin pracy | | | | | |
|---|---|---|---|---|---|
| | Aktywność studenta | Udział w zajęciach dydaktycznych, objętych planem studiów | Udział w konsultacjach | Praca własna studenta | RAZEM |
| | Liczba godzin pracy studenta | 45 | 3.0 | 27.0 | 75 |

| | |
|---|---|
| Cel przedmiotu | Poznanie zagrożeń bezpieczeństwa informacji i metod przeciwdziałania tym zagrożeniom. |

| | | | |
|---|---|---|---|
| Efekty uczenia się przedmiotu | Efekt kierunkowy | Efekt z przedmiotu | Sposób weryfikacji i oceny efektu |
| | [K7_U07] potrafi wykorzystać zaawansowane metody wspomagania procesów i funkcji, specyficzne dla kierunków studiów | Student rozumie, identyfikuje oraz klasyfikuje metody kryptografii symetrycznej, kryptografii asymetrycznej, steganografii, cyfrowego odcisku palca. | [SU4] Ocena umiejętności korzystania z metod i narzędzi<br>[SU2] Ocena umiejętności analizy informacji |
| | [K7_W03] zna i rozumie w pogłębionym stopniu budowę i zasady działania komponentów i systemów związanych z kierunkiem studiów, w tym teorie, metody i złożone zależności między nimi oraz wybrane zagadnienia szczegółowe – właściwe dla programu kształcenia | Student identyfikuje, klasyfikuje i rozpoznaje zagrożenia bezpieczeństwa informacji podczas transmisji oraz podstawowe systemy kryptograficzne. Student identyfikuje i klasyfikuje usługi oraz mechanizmy bezpieczeństwa. | [SW1] Ocena wiedzy faktograficznej |
| | [K7_W08] zna i rozumie w pogłębionym stopniu fundamentalne dylematy współczesnej cywilizacji, główne trendy rozwojowe dyscyplin naukowych istotnych dla kierunku kształcenia | Student rozumie i identyfikuje wyzwania związane z dystrybucją kluczy, utworzeniem kanału bezpiecznego, odpornością kryptografii asymetrycznej na działania komputerów kwantowych. Student zna i rozumie jak krytyczne dla współczesnej cywilizacji jest zachowanie właściwego poziomu bezpieczeństwa informacji. | [SW1] Ocena wiedzy faktograficznej |
| | [K7_U06] potrafi analizować działanie elementów, układów i systemów związanych z kierunkiem studiów oraz mierzyć ich parametry i badać charakterystyki techniczne, interpretować uzyskane wyniki i wyciągać wnioski | Student jest w stanie uruchomić, zmierzyć i analizować najważniejsze algorytmy szyfrowania symetrycznego oraz asymetrycznego. | [SU4] Ocena umiejętności korzystania z metod i narzędzi<br>[SU2] Ocena umiejętności analizy informacji |
| | [K7_W06] zna i rozumie w pogłębionym stopniu podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych | Student analizuje procesy szyfrowania i deszyfracji oraz ocenia odporność systemów kryptograficznych na ataki. | [SW1] Ocena wiedzy faktograficznej |
| Treści przedmiotu | 1.Bezpieczeństwo systemu informacyjnego<br>2.Podstawowe aspekty bezpieczeństwa informacji<br>3.Model bezpieczeństwa sieciowego<br>4.Podstawowe aspekty systemów kryptograficznych<br>5.Metody kryptoanalizy<br>6.Szyfry klasyczne<br>7.Wprowadzenie do szyfrów blokowych<br>8.Data Encryption Standard (DES)<br>9.Zasady projektowania szyfrów blokowych<br>10.Tryby pracy szyfrów blokowych<br>11.Szyfrowanie podwójne i potrójne (3DES)<br>12.International Data Encryption Algorithm (IDEA)<br>13.Advanced Encryption Standard (AES)<br>14.Szyfrowanie w łączu i szyfrowanie end-to-end<br>15.Metody dystrybucji kluczy<br>16.Generowanie liczb pseudolosowych<br>17.Szyfr potokowy RC4<br>18.Asymetryczne systemy kryptograficzne<br>19.System RSA<br>20.Dystrybucja kluczy publicznych<br>21.Algorytm Diffiego-Hellmana<br>22.Algorytm ElGamal<br>23.Kryptografia krzywych eliptycznych<br>24.Przyszłość kryptografii asymetrycznej<br>25.Kryptografia asymetryczna odporna na ataki komputerów kwantowych<br>26.Uwierzytelnianie wiadomości<br>27.Jednokierunkowe funkcje skrótu<br>28.Tęczowe tablice<br>29.Właściwości podpisu cyfrowego<br>30.Digital Signature Algorithm (DSA)<br>31.Podstawy steganografii<br>32.Cyfrowy odcisk palca<br>33.Reversible Data Hiding | | |
| Wymagania wstępne i dodatkowe | | | |

<table>
<tr><td>Sposoby i kryteria oceniania osiąganych efektów uczenia się</td><td colspan="2"><table>
<tr><th>Sposób oceniania (składowe)</th><th>Próg zaliczeniowy</th><th>Składowa oceny końcowej</th></tr>
<tr><td>sprawozdania pomiarowe</td><td>50.0%</td><td>40.0%</td></tr>
<tr><td>kolokwium zaliczeniowe</td><td>50.0%</td><td>60.0%</td></tr>
</table></td></tr>
<tr><td rowspan="3">Zalecana lista lektur</td><td>Podstawowa lista lektur</td><td>B. Schneier, Kryptografia dla praktyków, WN-T, Warszawa 2004J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, 2010N. Ferguson,B. Schneier, Kryptografia w praktyce, Helion, 2004W. Stallings, Cryptography and Network Security, Principles and Practice, Fourth Edition, Prentice Hall, 2005M. Stamp, Information Security: Principles and Practice, J. Wiley, 2011</td></tr>
<tr><td>Uzupełniająca lista lektur</td><td>B. Czaplewski, Nowe metody łącznego fingerprintingu i deszyfracji do zabezpieczania obrazów kolorowych, rozprawa doktorska, WETI PG, 2015Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, B. Ma, Reversible Data Hiding: Advances in the Past Two Decades, IEEE Access, 2016</td></tr>
<tr><td>Adresy eZasobów</td><td>Adresy na platformie eNauczanie:</td></tr>
<tr><td>Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania</td><td colspan="2">brak</td></tr>
<tr><td>Praktyki zawodowe w ramach przedmiotu</td><td colspan="2">Nie dotyczy</td></tr>
</table>