*Załącznik nr 1 do Uchwały nr \_\_\_\_\_\_\_ - 2018/2019 z dnia 25 marca 2019 r.*

*w sprawie wytycznych dla tworzenia i zmian programów studiów pierwszego stopnia, drugiego stopnia*

*oraz jednolitych studiów magisterskich rozpoczynających się od roku akademickiego 2019/2020.*

Opis **zajęć (sylabus)**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nazwa zajęć: | | Ochrona informacji i bezpieczeństwo systemów komputerowych | | | | | | | **ECTS** | | **5** |
| Nazwa zajęć w j. angielskim: | | Information protection and security of Computer Systems | | | | | | | | | |
| Zajęcia dla kierunku studiów: | | **Informatyka** | | | | | | | | | |
|  | |  | | | | | | | | | |
| Język wykładowy: | | polski | | | | Poziom studiów: | | studia I stopnia | | | |
| Forma studiów: | 🗷 stacjonarne  🞎 niestacjonarne | Status zajęć: | 🞎 podstawowe  🗷 kierunkowe | 🗷 obowiązkowe  🞎 do wyboru | | Numer semestru: ……6. | | 🞎 semestr zimowy 🗷 semestr letni | | | |
|  |  | Rok akademicki, od którego obowiązuje opis (rocznik): | | | | 2019/2020 | Numer katalogowy: | **ZIM-IN-1S-06L-44\_5** | | | |
|  | | | | | | | | | | | |
| Koordynator zajęć: | |  | | | | | | | | | |
| Prowadzący zajęcia: | |  | | | | | | | | | |
| Jednostka realizująca: | |  | | | | | | | | | |
| Jednostka zlecająca: | |  | | | | | | | | | |
| Założenia, cele i opis zajęć: | | Celem przedmiotu jest zapoznanie studentów z podstawowymi zagrożeniami bezpieczeństwa informacji oraz mechanizmami zabezpieczeń przed atakami, kryptograficznymi technikami zabezpieczeń danych, uwierzytelniania podmiotów i danych, mechanizmami kontroli dostępu, bezpieczne przechowywania oraz przesyłania danych. Opis tematów poruszanych podczas zajęć wykładowych:  1. Wprowadzenie do ochrony informacji (właściwości bezpieczeństwa, uwierzytelnienie i autoryzacja, koncepcja zaufania i wiarygodności, zagrożenia i ataki). 2. Zarządzania bezpieczeństwem systemów informatycznych  * Analiza i szacowania ryzyka * Postępowania z ryzykiem * Polityka bezpieczeństwa * Zarządzania ciągłością działania  1. Podstaw kryptografii symetrycznej a asymetrycznej  * Kryptografia symetryczna a asymetryczna * Zaawansowane protokoły kryptograficzne  1. Metody uwierzytelnienie danych (metody oparty na wiedzy, posiadaniu i cechy osobistej, siła protokołów uwierzytelniana, techniki ataków na hasła, techniki przechowywania haseł, kody uwierzytelniania wiadomości) 2. Kontrola dostępu (fizyczne zabezpieczenie danych, logiczna kontrola dostępu do danych, projektowanie bezpiecznej architektury, techniki zapobiegania wyciekowi informacji)  * Uznaniowa kontrola dostępu (MAC) * Nieuznaniowa kontrola dostępu (DAC, RBAK)  1. Protokoły bezpiecznej komunikacji (protokoły SSL/TLS, SSH, HTTPS, ataki na protokół TLS, protokoły IPsec i VPN) 2. Projektowania bezpiecznych aplikacji  * Tworzenia profili i zadania zabezpieczeń * Projektowania, implementacje i testowania TOE  Opis tematów poruszanych podczas zajęć Laboratoryjnych:  1. Badanie działania i właściwości szyfrów kryptograficznych 2. Wstęp do kryptografii 3. Zabezpieczenie poczty elektronicznej 4. Protokoły bezpiecznej komunikacji. 5. Implementacja podstawowych szyfrów symetrycznych i asymetrycznych 6. Metody bezpiecznego przechowywania danych i przesyłania danych 7. Metody kontroli dostępu 8. Wybrane techniki hakerskie i obrona przed nimi. | | | | | | | | | |
| Formy dydaktyczne, liczba godzin: | | 1. Wykład: liczba godzin ...30; 2. ćwiczenia laboratoryjne: liczba godzin ...30; | | | | | | | | | |
| Metody dydaktyczne: | | wykład, dyskusja problemu, rozwiązywanie problemu, konsultacje | | | | | | | | | |
| Wymagania formalne  i założenia wstępne: | | Wymagana jest wiedza z zakresu matematyki dyskretnej, programowanie, algorytmy i systemy operacyjne | | | | | | | | | |
| Efekty uczenia się: | | Wiedza:  1 - Identyfikuje typowe podatności i zagrożenia występujące w systemach informacyjnych, zna podstawowe mechanizmy ochrony informacji, w tym metody kryptograficzne, modele kontroli dostępu, protokoły uwierzytelniania oraz bezpieczne protokoły wymiany informacji. | | | Umiejętności:  1 - Analizuje typowe podatności i zagrożenia występujące w systemach informacyjnych, potrafi sformułować wymagania bezpieczeństwa, dobierać mechanizmy zabezpieczeń, projektuje proste systemy zabezpieczeń na poziomie aplikacji, systemów operacyjnych i sieci. | | | | | Kompetencje:  ……………………..  …………………….. | |
| Sposób weryfikacji efektów uczenia się: | | Kolokwium pisemne | | | | | | | | | |
| Forma dokumentacji osiągniętych efektów uczenia się: | | Kolokwium pisemne z ocenami | | | | | | | | | |
| Elementy i wagi mające wpływ  na ocenę końcową: | | **Kolokwium pisemne – 100%** | | | | | | | | | |
| Miejsce realizacji zajęć: | | Wykład -sala audytoryjna, ćwiczenia laboratoryjne – laboratorium komputerowe | | | | | | | | | |
| Literatura podstawowa i uzupełniająca:  Literatura podstawowa:   * William Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii, Helion, 2011. * Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry, Teoria bezpieczeństwa systemów komputerowych, Helion, Warszawa, 2005.   Literatura uzupełniająca:   * Dieter Gollmann, Computer Security, John Wiley & Sons, Cichester, 2006. * Ross Anderson, Security Engineering – A Guide to Building Dependable Distributed Systems, John Wiley & Sons, 2008. * Mark Stamp, Information Security Principles and Practice, JohnWiley & Sons, New Jersey, 2006. * William Stallings, ryptography and Network Security - Principles and practice, Pearson Education Limited, Boston, 2017. | | | | | | | | | | | |
| UWAGI  Minimalna liczba punktów konieczna do zaliczenia: 50% | | | | | | | | | | | |

Wskaźniki ilościowe charakteryzujące moduł/przedmiot:

|  |  |
| --- | --- |
| Szacunkowa sumaryczna liczba godzin pracy studenta (kontaktowych i pracy własnej) niezbędna dla osiągnięcia zakładanych dla zajęć efektów uczenia się - na tej podstawie należy wypełnić pole ECTS: | **60 h** |
| Łączna liczba punktów ECTS, którą student uzyskuje na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich lub innych osób prowadzących zajęcia: | **3 ECTS** |

Tabela zgodności kierunkowych efektów uczenia się z efektami przedmiotu:

|  |  |  |  |
| --- | --- | --- | --- |
| kategoria efektu | Efekty uczenia się dla zajęć: | Odniesienie do efektów dla programu studiów dla kierunku | Oddziaływanie zajęć na efekt kierunkowy\*) |
| Wiedza | Identyfikuje typowe podatności i zagrożenia występujące w systemach informacyjnych, zna podstawowe mechanizmy ochrony informacji, w tym metody kryptograficzne, modele kontroli dostępu, protokoły uwierzytelniania oraz bezpieczne protokoły wymiany informacji. | K\_W09 / P6S\_WG | 3 |
| Umiejętności | Analizuje typowe podatności i zagrożenia występujące w systemach informacyjnych, potrafi sformułować wymagania bezpieczeństwa, dobierać mechanizmy zabezpieczeń, projektuje proste systemy zabezpieczeń na poziomie aplikacji, systemów operacyjnych i sieci. | K\_U16 / P6S\_UW | 2 |
| Kompetencje - |  |  |  |
| Kompetencje - |  |  |  |

\*)

3 – zaawansowany i szczegółowy,

2 – znaczący,

1 – podstawowy,