*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: | | Bezpieczeństwo sieci komputerowych | | | | | | | | **ECTS** | **4** |
| Nazwa zajęć w j. angielskim: | | Network Security | | | | | | | | | |
| Zajęcia dla kierunku studiów: | | **Informatyka** | | | | | | | | | |
|  | |  | | | | | | | | | |
| Język wykładowy: | | polski | | | | Poziom studiów: | | | studia II stopnia | | |
| Forma studiów: | 🗷 stacjonarne  🞎 niestacjonarne | Status zajęć: | 🞎 podstawowe  🗷 kierunkowe | 🞎 obowiązkowe  🗷 do wyboru | | Numer semestru: ……2….. | | | 🞎 semestr zimowy 🗷 semestr letni | | |
|  |  | Rok akademicki, od którego obowiązuje opis (rocznik): | | | | 2019/2020 | Numer katalogowy: | | **ZIM-IN-2S-02Z-15\_1** | | |
|  | | | | | | | | | | | |
| Koordynator zajęć: | | **mgr inż. Grzegorz Wieczorek** | | | | | | | | | |
| Prowadzący zajęcia: | |  | | | | | | | | | |
| Jednostka realizująca: | |  | | | | | | | | | |
| Jednostka zlecająca: | |  | | | | | | | | | |
| Założenia, cele i opis zajęć: | | Celem przedmiotu jest zapoznanie studentów z tematyką bezpieczeństwa sieci komputerowej do analizy wystąpienia incydentu po systemy automatycznego reagowania na incydenty takie jak systemy WAF, IDS, IPS. Analiza zdarzeń sieciowych może być użyteczna przy pracy z systemami przetwarzającymi dane poufne, wrażliwe i dane osobowe. Aktywna ochrona sieci komputerowej pozawala na unikanie poważnych incydentów bezpieczeństwa i wycieków danych z sieci i systemów. Opis tematów poruszanych podczas zajęć:  1. Wprowadzenie do bezpieczeństwa sieciowego 2. Typy incydentów sieciowych i ich klasyfikacja 3. Incydenty powstające w trakcie aktywnego rekonesansu sieci, np. skanowanie portów. 4. Omówienie architektury zabezpieczeń sieci komputerowych 5. Wprowadzenie do systemów typu firewall, np. FirewallD 6. Wstęp do systemów korelacji zdarzeń i incydentów sieciowych 7. Zapoznanie z systemami SIEM 8. Szyfrowanie w połączeniach VPN 9. Omówienie działania protokołu SSL z przykładami ataków wykorzystujących znane exploity 10. Wstęp do systemów IPS i IDS 11. Omówienie firewalli aplikacyjnych (WAF) 12. Omówienie systemów UTM | | | | | | | | | |
| Formy dydaktyczne, liczba godzin: | | 1. wykład; liczba godzin ...15...; 2. ćwiczenia laboratoryjne; liczba godzin ...30...; | | | | | | | | | |
| Metody dydaktyczne: | | wykład, dyskusja problemu, rozwiązywanie problemu, konsultacje, projekty | | | | | | | | | |
| Wymagania formalne  i założenia wstępne: | | Wymagana jest wiedza z zakresu sieci komputerowych i usług sieciowych. | | | | | | | | | |
| Efekty uczenia się: | | Wiedza:  Ma zaawansowaną wiedzę na temat struktury, zasady działania oraz komunikacji w systemie informatycznym.  Zna zasady prywatności i ścigania przestępstw, bezpieczeństwa systemów czasu rzeczywistego oraz wpływ technologii komputerowych na zdrowie i na środowisko naturalne.  Ma podstawową wiedzę dotyczącą transferu technologii w odniesieniu do rozwiązań informatycznych. | | | Umiejętności:  Ma praktyczne umiejętności w zakresie technik bezpieczeństwa IT, potrafi stosować różnorodne metody zapobiegania i obrony przed atakami IT. | | | Kompetencje: | | | |
| Sposób weryfikacji efektów uczenia się: | | Kolokwium pisemne / projekt | | | | | | | | | |
| Forma dokumentacji osiągniętych efektów uczenia się: | | Kolokwium pisemne z ocenami, projekt | | | | | | | | | |
| Elementy i wagi mające wpływ  na ocenę końcową: | | **Kolokwium pisemne – 51%**  **Projekt – 49%** | | | | | | | | | |
| Miejsce realizacji zajęć: | | Wykład -sala audytoryjna, ćwiczenia laboratoryjne – laboratorium komputerowe | | | | | | | | | |
| Literatura podstawowa i uzupełniająca:  Literatura podstawowa:   * Liderman K.: Bezpieczeństwo informacyjne * Weidman G.: Bezpieczny system w praktyce. Wyższa szkoła hackingu i testy penetracyjne * Serafin M.: Sieci VPN. Zdalna praca i bezpieczeństwo danych. Wydanie II rozszerzone   Literatura uzupełniająca:   * Materiały firmowe, m. in. Imperva, Fortinet i inne. * Materiały z Internetu wskazane w materiałach do wykładu. | | | | | | | | | | | |
| 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: | **1,5 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 1 | Ma zaawansowaną wiedzę na temat struktury, zasady działania oraz komunikacji w systemie informatycznym. | K\_W08 | 3 |
| Wiedza 2 | Zna zasady prywatności i ścigania przestępstw, bezpieczeństwa systemów czasu rzeczywistego oraz wpływ technologii komputerowych na zdrowie i na środowisko naturalne. | K\_W09 | 3 |
| Wiedza 3 | Ma podstawową wiedzę dotyczącą transferu technologii w odniesieniu do rozwiązań informatycznych. | K\_W12 | 2 |
| Umiejętności 1 | Ma praktyczne umiejętności w zakresie technik bezpieczeństwa IT, potrafi stosować różnorodne metody zapobiegania i obrony przed atakami IT. | K\_U05 | 3 |

\*)

3 – zaawansowany i szczegółowy,

2 – znaczący,

1 – podstawowy,