# Karta zajęć

| Informacje ogólne | | |
|---|---|---|
| Nazwa zajęć: **Cyberbezpieczeństwo** | | |
| Nazwa uczelni: **Wyższa Szkoła Zarządzania i Bankowości w Krakowie** | | |
| Wydział: **Wydział Nauk Stosowanych** | | |
| Kierunek studiów: **Informatyka** | | |
| Poziom studiów: pierwszego stopnia | | |
| Forma studiów:<br>niestacjonarne, stacjonarne | Profil kształcenia:<br>praktyczny | Zakres kształcenia: |
| Rok/Semestr:<br>3/6 | Status zajęć:<br>obowiązkowy | Języki wykładowe:<br>polski |
| Studia niestacjonarne | Forma zajęć | ćwiczenia laboratoryjne |
| | Wymiar zajęć (w godz.) | 16 |
| Studia stacjonarne | Forma zajęć | ćwiczenia laboratoryjne |
| | Wymiar zajęć (w godz.) | 30 |

| | |
|---|---|
| Koordynator zajęć | mgr inż. Marcin Henclik |
| Prowadzący | mgr inż. Marcin Henclik<br>inż. Kajetan Miłosz Miś |
| Cele kształcenia | C1. Poszerzenie zdobytej wiedzy z zakresu bezpieczeństwa systemów i sieci komputerowych.<br>C2. Pokazanie struktury ataków, mechanizmów i narzędzi mających wpływ na bezpieczeństwo systemów.<br>C3. Wskazanie właściwych procedur i modeli konfiguracji poprawiających bezpieczeństwo systemów informatycznych. |
| Wymagania wstępne | Znajomość konfiguracji systemów operacyjnych. Znajomość komponentów oraz zagadnień konfiguracji sieci komputerowych. |

| Efekty uczenia się | | | Odniesienie do efektów uczenia się dla kierunku | Odniesienie do charakterystyk PRK poziomu 6 |
|---|---|---|---|---|
| Wiedza | EU1 | Student wie, na jakie komponenty systemów i sieci należy zwrócić szczególną uwagę w kontekście bezpieczeństwa. | K_W04 | P6U_W<br>P6S_WG |
| | EU2 | Student rozumie jak bezpieczeństwo systemów teleinformatycznych wpływa na tworzone oprogramowanie, standardy i technologie. | K_W15 | P6U_W<br>P6S_WK |
| | EU3 | Student wie jakie etapy, metody i techniki sa wykorzystywane w celu naruszenia bezpieczeństwa organizacji. | K_W08 | P6U_W<br>P6S_WG |
| Umiejętności | EU4 | Student potrafi zaprojektować oraz skonfigurować bezpieczny system teleinformatyczny. | K_U10<br>K_U14 | P6U_U<br>P6S_UW<br>P6S_UO<br>P6S_UK |

| | | | | |
|---|---|---|---|---|
| | EU5 | Student potrafi zastosować zdobytą wiedzę z zakresu bezpieczeństwa w tworzeniu bezpiecznego oprogramowania. | K_U09 | P6U_U<br>P6S_UW |
| | EU6 | Student potrafi odpowiednio ocenić oraz dokonac wyboru oprogramowania i urządzeń podnoszących poziom bezpieczeństwa systemów teleinformatycznych. | K_U12<br>K_U15 | P6U_U<br>P6S_UW<br>P6S_UO<br>P6S_UK |
| Kompetencje społeczne | EU7 | Student jest zorientowany na dobro społeczne i gospodarcze wynikające z przestrzegania zasad bezpieczeństwa systemów teleinformatycznych. | K_K02<br>K_K05 | P6U_U<br>P6S_KR<br>P6S_KO |
| | EU8 | Student wykazuje otwartość na prace w grupie w tym na współpracę między specjalistami IT w organizacji w celu podnoszenia poziomu bezpieczeństwa. | K_K03 | P6U_U<br>P6S_KO |

| **Treści programowe** | |
|---|---|
| Laboratorium | |
| L1 | Wprowadzenie do tematyki cyberbezpieczeństwa z elementami białego wywiadu. |
| L2 | Poszerzenie zdobytej wiedzy o systemach operacyjnych i sieciach komputerowych o elementy bezpieczeństwa. |
| L3 | Systemy szyfrowania, uwierzytelniania i infrastruktura klucza publicznego (PKI). |
| L4 | Rodzaje ataków na infrastrukturę i usługi sieciowe oraz sposoby reagowania na nie. |
| L5 | Polityki bezpieczeństwa oraz sposoby reakcji na incydenty. |
| L6 | Urządzenia i oprogramowanie podnoszące bezpieczeństwo systemów teleinformatycznych. |
| L7 | Podsumowania zdobytej wiedzy przy projektowaniu i konfigurowaniu systemów teleinformatycznych. |

| **Ocena studenta** | | | |
|---|---|---|---|
| Metody/Narzędzia dydaktyczne | N1 | ćwiczenia laboratoryjne | laboratorium |
| | N2 | dyskusje problemowe | laboratorium |
| | N3 | praca w grupach | laboratorium |
| Sposoby oceny/metody weryfikacji uczenia się | Ocena formująca | | |
| | F1 | Ocena ćwiczeń laboratoryjnych | laboratorium |
| | F2 | Ocena z zaliczenia | laboratorium |
| | Ocena podsumowująca | | |
| | P1 | Ocena z egzaminu/zaliczenia | laboratorium |
| | | Na ocenę podsumowującą składa największy wpływ ocena z zaliczenia. Ocena końcowa może zostać podniesiona o wyniki z ćwiczeń laboratoryjnych i zadań domowych. | |

| **Kryteria oceny** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | EU1 | EU2 | EU3 | EU4 | EU5 | EU6 | EU7 | EU8 |
| Na ocenę 3 | 51% | 51% | 51% | 51% | 51% | 51% | 51% | 51% |
| Na ocenę 3,5 | 62% | 62% | 62% | 62% | 62% | 62% | 62% | 62% |
| Na ocenę 4 | 74% | 74% | 74% | 74% | 74% | 74% | 74% | 74% |
| Na ocenę 4,5 | 86% | 86% | 86% | 86% | 86% | 86% | 86% | 86% |
| Na ocenę 5 | 95% | 95% | 95% | 95% | 95% | 95% | 95% | 95% |

| Literatura | |
|---|---|
| Literatura podstawowa | 1. Stallings William, Brown Lawrie: Bezpieczeństwo systemów informatycznych. Tom 1. Wydawnictwo Helion, Gliwice 2019<br>2. Bezpieczeństwo i Niezawodnośc Systemów Informatycznych. Bin GigaCon, Kraków 2017<br>3. Forshaw James: Atak na sieć okiem hakera. Wydawnictwo Helion, Gliwice 2019 |
| Literatura uzupełniająca | 1. Sajdak Michał: Bezpieczeństwo aplikacji webowych. Securitum Szkolenia, Kraków 2019<br>2. Sankar Kirshna, Sundaralingam Sri, Balinski Andrew, Miller Darrin: Bezpieczeństwo bezprzewodowych sieci LAN. Zakład Nauczania Informatyki "Mikom", Warszawa 2005<br>3. Najera-Gutierrez Gilberto, Ansari Juned Ahmed: Kali Linux. Wydawnictwo Helion, Gliwice 2019<br>4. Mitnick Kevin, Wozniak Steve, Simon William L.: Duch w sieci. Wydawnictwo Helion, Gliwice 2019<br>5. Payne Bryson: Podstawy systemu Linux dla hakerów. Wydawnictwo Naukowe PWN, Warszawa 2020 |

| Nakład pracy studenta | | |
|---|---|---|
| | Studia niestacjonarne | Studia stacjonarne |
| Godziny kontaktowe z nauczycielem akademickim lub inną osobą prowadzącą zajęcia (wykłady, ćwiczenia, laboratoria, konwersatoria) | 16 | 30 |
| Przygotowanie do zajęć, w tym studiowanie zalecanej literatury podstawowej i uzupełniającej | 10 | 5 |
| Przygotowanie projektu | 0 | 0 |
| Przygotowanie się do egzaminu / zaliczenia | 10 | 10 |
| Inne (np. esej, prezentacja, referat, koreferat, sprawozdanie z wykonanych zadań) | 14 | 5 |
| **Łączny nakład pracy studenta w godz.** | 50 | 50 |
| **Liczba punktów ECTS** | 2 | 2 |

| Macierz realizacji zajęć | | | | | |
|---|---|---|---|---|---|
| Efekty uczenia się | Odniesienie danego efektu do kierunkowych efektów uczenia się | Cele kształcenia | Treści programowe | Metody/Narzędzia dydaktyczne | Sposoby oceny |
| EU1 | K_W04 | C1, C2, C3 | L2, L4, L6 | N1, N2, N3 | F1, F2, P1 |
| EU2 | K_W15 | C1 | L1 | N1, N2, N3 | F2, P1 |
| EU3 | K_W08 | C3 | L5 | N1, N2, N3 | F2, P1 |
| EU4 | K_U10, K_U14 | C3 | L3, L6, L7 | N1, N2, N3 | F1, F2, P1 |
| EU5 | K_U09 | C3 | L3, L7 | N1, N2, N3 | F2, P1 |
| EU6 | K_U12, K_U15 | C2, C3 | L4, L6, L7 | N1, N2, N3 | F1, F2, P1 |
| EU7 | K_K02, K_K05 | C1 | L1 | N1, N2, N3 | F2, P1 |
| EU8 | K_K03 | C3 | L5 | N1, N2, N3 | F1, F2, P1 |