* + - 1. **KARTA PRZEDMIOTU**

|  |  |
| --- | --- |
| Nazwa przedmiotu | * + - 1. **Informatyczny audyt bezpieczeństwa** |

**1. Usytuowanie przedmiotu w systemie studiów**

|  |  |
| --- | --- |
| 1.1. Kierunek studiów | **Informatyka** |
| 1.2. Forma i ścieżka studiów | **Stacjonarne/Niestacjonarne** |
| 1.3. Poziom kształcenia | **Studia I stopnia** |
| 1.4. Profil studiów | **Praktyczny** |

|  |  |
| --- | --- |
| 1.5. Specjalność | **Cyberbezpieczeństwo i informatyka śledcza** |
| 1.6. Koordynator przedmiotu | **Dr Mateusz Górka; mgr Lech Daniel; mgr Sylwia Jędrzejczyk** |

**2. Ogólna charakterystyka przedmiotu**

|  |  |
| --- | --- |
| 2.1. Przynależność do grupy przedmiotu | **Do wyboru/praktyczny** |
| 2.2. Liczba ECTS | **4** |
| 2.3. Język wykładów | **Polski** |
| 2.4. Semestry, na których realizowany jest przedmiot | **V** |
| 2.5.Kryterium doboru uczestników zajęć | **Dla specjalności: Cyberbezpieczeństwo i informatyka śledcza** |

1. **efekty uczenia się i sposób prowadzenia zajęć**
   1. **Cele przedmiotu**

|  |  |
| --- | --- |
| **Lp.** | **Cele przedmiotu** |
|
| C1 | Zapoznanie się z zagadnieniem bezpieczeństwa systemów komputerowych, obowiązującymi w tym zakresie przepisami i normami ISO oraz problematyką˛ tworzenia Polityk, Zasad i Procedur Bezpieczeństwa systemów komputerowych. |
| C2 | Zapoznanie się z najczęściej spotykanymi zagrożeniami, błędami prowadzącymi do powstania luk w bezpieczeństwie systemów oraz technikami ich unikania. |
| C3 | Nabycie umiejętności korzystania z narzędzi do analizy zabezpieczeń, narzędzi do monitoringu, systemami wykrywania ataków i sposobami ochrony przed atakami - uzupełnieniem jest omówienie zagadnień z zakresu informatyki śledczej. |
| C4 | Zapoznanie z modelami bezpieczeństwa i klasami bezpieczeństwa systemów. Uzyskanie wiedzy o modelach uwierzytelniania, strategiach kontroli dostępu w tym także w kontekście bezpieczeństwa protokołów komunikacyjnych i usług aplikacyjnych. |
| C5 | Studium przypadku - poznanie praktycznych metod wyboru i zastosowania odpowiednich zabezpieczeń na podstawie prawdziwego wydarzenia - studenci zapoznają się z przyczynami wystąpienia incydentów, sposobami ich wykrywania i analizą. |

* 1. **Przedmiotowe efekty uczenia się, z podziałem na wiedzę, umiejętności i kompetencje, wraz z odniesieniem do kierunkowych efektów uczenia się**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Opis przedmiotowych efektów  uczenia się** | **Odniesienie do  kierunkowych efektów**  **uczenia się (symbole)** | **Sposób realizacji (zaznaczyć „X”)** | | | |
| **ST** | | **NST** | |
| **Zajęcia na Uczelni** | **Zajęcia na  platformie** | **Zajęcia na Uczelni** | **Zajęcia na  platformie** |
| Po zaliczeniu przedmiotu student w zakresie **wiedzy** zna i rozumie | | | | | | |
| W1 | Metody rozwiązywania problemów bezpieczeństwa stosowane w systemach komputerowych i wie jak je stosować. | INF\_W05  INF\_W15 |  | X |  | X |
| W2 | Zasady bezpieczeństwa przy używaniu i projektowaniu systemów informatycznych. |  | X |  | X |
| W3 | Zasady zapewnienia zgodności poziomu bezpieczeństwa systemów komputerowych z wymogami prawnymi. |  | X |  | X |
| W4 | Ma wiedzę o narzędziach stosowanych do analizy bezpieczeństwa systemu komputerowego. |  | X |  | X |
| W5 | Rolę bezpieczeństwa danych i systemów informatycznych dla funkcjonowania współczesnego społeczeństwa. |  | X |  | X |
| Po zaliczeniu przedmiotu student w zakresie **umiejętności** potrafi | | | | | | |
| U1 | Identyfikować zagrożenia dotyczące bezpieczeństwa systemów komputerowych. | INF\_U13  INF\_U25 | X |  | X |  |
| U2 | Dobrać metody i narzędzia ochrony systemów komputerowych. | X |  | X |  |
| U3 | Identyfikować zgodność poziomu bezpieczeństwa systemu komputerowego z wymogami prawnymi. | X |  | X |  |
| U4 | Wdrożyć system bezpieczeństwa danych i systemów informatycznych. | X |  | X |  |
| Po zaliczeniu przedmiotu student w zakresie **kompetencji społecznych** jest gotów do | | | | | | |
| K1 | Profesjonalnych działań w zakresie bezpieczeństwa informatycznego wymagających stałego pogłębiania wiedzy i umiejętności. | INF\_K02  INF\_K05 | X |  | X |  |
| K2 | Zrozumienia konsekwencji i skutków zaniechań i podejmowanych działań z zakresu bezpieczeństwa. | X |  | X |  |
| K3 | Dbałości o prywatność oraz ochronę danych. Posiada świadomość etyczną. | X |  | X |  |

**3.3. Formy zajęć dydaktycznych i ich wymiar godzinowy - Studia stacjonarne (ST), Studia niestacjonarne (NST)**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ścieżka** | **Wykład** | **Ćwiczenia** | **Projekt** | **Warsztat** | **Laboratorium** | **Seminarium** | **Lektorat** | **Zajęcia prowadzone z wykorzystaniem metod i technik kształcenia na odległość w formie wykładu** | **Inne** | **Punkty ECTS** |
| **ST** |  |  |  |  | 30 |  |  | 20 |  | 4 |
| **NST** |  |  |  |  | 15 |  |  | 10 |  | 4 |

**3.4. Treści kształcenia** (oddzielnie dla każdej formy zajęć: (W, ĆW, PROJ, WAR, LAB, LEK, INNE). Należy zaznaczyć (X), w jaki sposób będą realizowane dane treści (zajęcia na uczelni lub zajęcia na platformie e-learningowej prowadzone z wykorzystaniem metod i technik kształcenia na odległość)

**RODZAJ ZAJĘĆ: WYKŁAD**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Treść zajęć** | **Odniesienie do przedmiotowych efektów uczenia się** | **Sposób realizacji (zaznaczyć „X”)** | | | |
| **ST** | | **NST** | |
| **Zajęcia na Uczelni** | **Zajęcia na  platformie** | **Zajęcia na Uczelni** | **Zajęcia na  platformie** |
| **1.** | Podstawowe zagadnienia i definicje z zakresu bezpieczeństwa systemów komputerowych. Znaczenie bezpieczeństwa systemów komputerowych. | **W1** |  | **X** |  | **X** |
| **2.** | Polityka Bezpieczeństwa. Przygotowanie do opracowania polityki bezpieczeństwa systemu. Analiza ryzyka czyli analiza zasobów, oraz zagrożeń i podatności zasobów. | **W2, W4** |  | **X** |  | **X** |
| **3.** | Sformułowanie polityki i opracowanie na tej podstawie dokumentu „Polityki bezpieczeństwa systemu”. Podstawowe zasady polityki bezpieczeństwa. Ogólne zasady polityki  bezpieczeństwa | **W3** |  | **X** |  | **X** |
| **4.** | Audyty bezpieczeństwa systemu. | **W5** |  | **X** |  | **X** |
| **5.** | Audyt Bezpieczeństwa Czynnika Ludzkiego. Czynniki zwiększające ryzyko. | **W5** |  | **X** |  | **X** |
| **6.** | Podsumowanie zajęć i omówienie ocen. |  |  | **X** |  | **X** |

**RODZAJ ZAJĘĆ: LABORATORIUM**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Treść zajęć** | **Odniesienie do przedmiotowych efektów uczenia się** | **Sposób realizacji (zaznaczyć „X”)** | | | |
| **ST** | | **NST** | |
| **Zajęcia na Uczelni** | **Zajęcia na  platformie** | **Zajęcia na Uczelni** | **Zajęcia na  platformie** |
| **1.** | Bezpieczeństwo systemów komputerowych z punktu widzenia metod konfiguracji. Znaczenie bezpieczeństwa systemów komputerowych. | **U1, K1** | **X** |  | **X** |  |
| **2.** | Polityka Bezpieczeństwa. Przygotowanie do opracowania polityki bezpieczeństwa systemu - przykłady. Analiza ryzyka czyli analiza zasobów, oraz zagrożeń i podatności zasobów. Metody przeciwdziałania zagrożeniom. | **U2, K1** | **X** |  | **X** |  |
| **3.** | Sformułowanie polityki i opracowanie na tej podstawie dokumentu „Polityki bezpieczeństwa systemu”. Podstawowe zasady polityki bezpieczeństwa. Ogólne zasady polityki  bezpieczeństwa – praktyczne przykłady i metody. | **U3** | **X** |  | **X** |  |
| **4.** | Audyty bezpieczeństwa systemu - przygotowanie i procedury przeprowadzenia informatycznego audytu bezpieczeństwa. | **U4, K1** | **X** |  | **X** |  |
| **5.** | Audyt Bezpieczeństwa Czynnika Ludzkiego. Czynniki zwiększające ryzyko. Podatności na błędy. | **U4, K2, K3** | **X** |  | **X** |  |
| **6.** | Podsumowanie zajęć i omówienie ocen. |  | **X** |  | **X** |  |

**3.5. Metody weryfikacji efektów uczenia się** (wskazanie i opisanie metod prowadzenia zajęć oraz weryfikacji osiągnięcia efektów uczenia się oraz sposobu dokumentacji)

|  |  |  |  |
| --- | --- | --- | --- |
| **Efekty przedmiotowe** | **Metody dydaktyczne** | **Metody weryfikacji efektów uczenia się** | **Sposoby dokumentacji** |
| **WIEDZA** | | | |
| **W1-W5** | wykład informacyjny, konwersatoryjny z wykorzystaniem multimediów | Test – zaliczenie wykładu | Arkusz testu |
| **UMIEJĘTNOŚCI** | | | |
| **U1-U4** | Studium przypadku, dyskusje, wykonywanie zadań | Zaliczenie laboratorium - studenci wykonują profesjonalne analizy SWOT poszczególnych części audytu, czyli audytu legalności oprogramowania, audytu sprzętu oraz jego ewidencji, audytu bezpieczeństwa zastosowanych technologii zabezpieczeń. | Oceniona praca |
| **KOMPETENCJE SPOŁECZNE** | | | |
| **K1-K3** | Studium przypadku, dyskusje, wykonywanie zadań | Zaliczenie laboratorium - studenci wykonują profesjonalne analizy SWOT poszczególnych części audytu, czyli audytu legalności oprogramowania, audytu sprzętu oraz jego ewidencji, audytu bezpieczeństwa zastosowanych technologii zabezpieczeń. | Oceniona praca |

**3.6. Kryteria oceny osiągniętych efektów uczenia się**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Efekt uczenia się** | **Na ocenę 3 lub „zal.”**  **student zna i rozumie/potrafi/jest gotów do** | **Na ocenę 3,5 student zna i rozumie/potrafi/jest gotów do** | **Na ocenę 4 student zna i rozumie/potrafi/jest gotów do** | **Na ocenę 4,5 student zna i rozumie/potrafi/jest gotów do** | **Na ocenę 5 student zna i rozumie/potrafi/jest gotów do** |
| W | 51-60% wiedzy wskazanej w efektach uczenia się | 61-70% wiedzy wskazanej w efektach uczenia się | 71-80% wiedzy wskazanej w efektach uczenia się | 81-90% wiedzy wskazanej w efektach uczenia się | 91-100% wiedzy wskazanej w efektach uczenia się |
| U | 51-60% umiejętności wskazanych w efektach uczenia się | 61-70% umiejętności wskazanych w efektach uczenia się | 71-80% umiejętności wskazanych w efektach uczenia się | 81-90% umiejętności wskazanych w efektach uczenia się | 91-100% umiejętności wskazanych w efektach uczenia się |
| K | 51-60% umiejętności wskazanych w efektach uczenia się | 61-70% umiejętności wskazanych w efektach uczenia się | 71-80% umiejętności wskazanych w efektach uczenia się | 81-90% umiejętności wskazanych w efektach uczenia się | 91-100% umiejętności wskazanych w efektach uczenia się |

**3.7. Zalecana literatura**

**Podstawowa**

1. Stallings William, Brown Lawrie, Bezpieczeństwo systemów informatycznych : zasady i praktyka. T. 1, Helion, Gliwice, 2023
2. Stallings William, Brown Lawrie, Bezpieczeństwo systemów informatycznych : zasady i praktyka. T. 2, Helion, Gliwice,

#### Polaczek Tomasz, Audyt bezpieczeństwa informacji w praktyce, Helion, Gliwice, 2006

1. Diogenes Yuri, Ozkaya Erdal, Cyberbezpieczeństwo : strategie ataku i obrony: jak osiągnąć najwyższy możliwy stan zabezpieczeń systemu informatycznego, Helion, Gliwice, 2023
2. IT Auditing Using Controls to Protect Information Assets – Chris Davis, Mike Schiller, Kevin Wheeler

**Uzupełniająca**

1. Liderman Krzysztof, Bezpieczeństwo informacyjne : nowe wyzwania, PWN, Warszawa, 2017
2. Liderman Krzysztof, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa, 2009
3. Tarapata Jolanta (red.), Odporność organizacji : cyfryzacja, bezpieczeństwo, innowacje, Difin, Warszawa, 2022

**4. Nakład pracy studenta - bilans punktów ECTS**

|  |  |  |
| --- | --- | --- |
| **Rodzaje aktywności studenta** | **Obciążenie studenta** | |
| **ST** | **NST** |
| **Zajęcia wymagające bezpośredniego kontaktu studenta z nauczycielem akademickim w siedzibie uczelni** | **50** | **25** |
| Zajęcia przewidziane planem studiów | 50 | 25 |
| **Praca własna studenta** | **50** | **75** |
| Przygotowanie bieżące do zajęć, przygotowanie prac projektowych/prezentacji/itp. | 25 | 35 |
| Przygotowanie do zaliczenia zajęć | 25 | 40 |
| **SUMARYCZNE OBCIĄŻENIE GODZINOWE STUDENTA** | **100** | **100** |
| **Liczba punktów ECTS** | **4** | **4** |

|  |  |
| --- | --- |
| Data ostatniej zmiany | 30.09.2024 |
| Zmiany wprowadził | Zespół ds. Jakości Kształcenia INF |
| Zmiany zatwierdził | Mgr Arkadiusz Gwarda |