|  |  |  |
| --- | --- | --- |
|  | **UNIWERSYTET MORSKI W GDYNI**  **Wydział Zarządzania i Nauk o Jakości** | https://umg.edu.pl/sites/default/files/zalaczniki/wznj-02_0.png |

**KARTA PRZEDMIOTU**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kod przedmiotu |  | Nazwa przedmiotu | w jęz. polskim | **BEZPIECZEŃSTWO SYSTEMÓW INFORMACYJNYCH** |
| w jęz. angielskim | **INFORMATION SYSTEM SECURITY** |

|  |  |
| --- | --- |
| Kierunek | **Zarządzanie** |
| Specjalność | **Informatyka Gospodarcza** |
| Poziom kształcenia | **studia pierwszego stopnia** |
| Forma studiów | **niestacjonarne** |
| Profil kształcenia | **ogólnoakademicki** |
| Status przedmiotu | **obowiązkowy** |
| Rygor | **egzamin** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Semestr studiów** | **Liczba punktów ECTS** | **Liczba godzin w tygodniu** | | | | **Liczba godzin w semestrze** | | | |
| **W** | **C** | **L** | **P** | **W** | **C** | **L** | **P** |
| V | 4 |  |  |  |  | 18 |  | 9 |  |
| **Razem w czasie studiów** | | | | | | **27** | | | |

|  |
| --- |
| **Wymagania w zakresie wiedzy, umiejętności i innych kompetencji** |
| Brak wymagań wstępnych. |

|  |
| --- |
| **Cele przedmiotu** |
| Zapoznanie studenta z istotą bezpieczeństwa, bezpieczeństwa informacyjnego, problematyką bezpieczeństwa systemu informacyjnego (SI) oraz technologii towarzyszących jak: kontrola wewnętrzna, audyt, CAAT’s.  Ukształtowanie podstawowych umiejętności z zakresu obsługi systemów bezpieczeństwa SI. |

|  |  |  |
| --- | --- | --- |
| **Osiągane efekty kształcenia dla przedmiotu (EKP)** | | |
| **Symbol** | **Po zakończeniu przedmiotu student:** | **Odniesienie do kierunkowych efektów kształcenia** |
| EKP\_01 | wymienia, objaśnia i klasyfikuje pojęcia zakresu bezpieczeństwa i polityki bezpieczeństwa SI. | NK\_W06, NK\_U01, NK\_U3 |
| EKP\_02 | ma wiedzę o standardach polityki bezpieczeństwa w odniesieniu do SI. | NK\_W06, NK\_U01 |
| EKP\_03 | potrafi wykorzystać standardy oceny polityki bezpieczeństwa SI (technologie i standardy audytu bezpieczeństwa). | NK\_W06 NK\_U01 |
| EKP\_04 | ma świadomość celów i zasad organizowania pracy zespołu projektującego, wdrażającego i eksploatującego system bezpieczeństwa SI. | NK\_U07, NK\_K02 |
| EKP\_05 | ma podstawowe umiejętności, z zakresu ochrony SI w odniesieniu do współczesnych technologii informatycznych (ochrona dostępu, uwierzytelnianie, analiza antywirusowa, zapory, itd.). | NK\_U01, NK\_U07, NK\_U08 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Treści programowe** | **Liczba godzin** | | | | **Odniesienie do EKP** |
| **W** | **C** | **L** | **P** |
| Kształtowania polityki bezpieczeństwa systemu informacyjnego (SI) (wartość systemu informacyjnego; wartość informacji, sprzętu, oprogramowania, rodzaj i zakres potencjalnych zagrożeń oraz koszt strat wynikających z tych zagrożeń, koszt szkolenia personelu obsługującego system, zakres ochrony fizycznej (zewnętrznej) i programowo-sprzętowej (wewnętrznej), itd. Kontrola wewnętrzna i audyt bezpieczeństwa. | 2 |  |  |  | EKP\_01, EKP\_02, EKP\_03, EKP\_04 |
| Standardy bezpieczeństwa: TCSEC (Trusted Computer Security Evaluation Criteria – Orange Book), ITSEC (Information Technology Security Evaluation Criteria ). Polska Norma PN-I-13335-1 - „Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych.” Norma ISO/IEC TR 13335-3 – „Techniki zarządzania bezpieczeństwem systemów informatycznych”. | 2 |  |  |  | EKP\_01, EKP\_02, EKP\_03, EKP\_04 |
| Bezpieczeństwo systemu informacyjnego (SI). Podmioty bezpieczeństwa informacyjnego w SI: dane, oprogramowanie, sprzęt informatyczny, dokumentacje (archiwa, kopie), użytkownicy. | 3 |  |  |  | EKP\_01, EKP\_02, EKP\_03, EKP\_04 |
| Bezpieczeństwo baz danych i SZBD. Poufność, integralność, nadmiarowość i współbieżność. Technologie identyfikacji, uwierzytelniana, autoryzacji. Upoważnienia. | 3 |  |  |  | EKP\_01, EKP\_02, EKP\_04 |
| Technologie szyfrowania i steganografia. | 2 |  |  |  | EKP\_01, EKP\_02, EKP\_04 |
| Zagrożenia sieciowe. Klasyfikacje zagrożeń sieciowych (wg CERT). Instytucje NASK, CERT, CERN. Istota hakingu. Programy niszczące i szpiegujące. Spam. Technologie ochrony sieciowej-zapory sieciowe. Zagrożenia w sieciach bezprzewodowych (standardy 802.11 i inne). | 2 |  |  |  | EKP\_01, EKP\_02, EKP\_04 |
| Audyt informatyczny, technologie audytu informatycznego. ISACA i jej produkty. COBIT. | 3 |  |  |  | EKP\_01, EKP\_02, EKP\_03, EKP\_04 |
| Technologie CAAT’s. Rynek aplikacji CAAT’s. | 1 |  |  |  | EKP\_01, EKP\_02, EKP\_03, EKP\_04 |
| Identyfikacja stanu komputera – audyt zasobów, identyfikacja systemu. |  |  | 1 |  | EKP\_01, EKP\_02, EKP\_05 |
| Identyfikacja i klasyfikacja zagrożeń dla systemu komputera, przykłady ataków. |  |  | 1 |  | EKP\_01, EKP\_02, EKP\_05 |
| Podstawy bezpieczeństwa w systemie – ochrona dostępu na poziomie użytkownika. |  |  | 1 |  | EKP\_01, EKP\_02, EKP\_05 |
| Udostępnianie zasobów systemu. Ochrona systemu metodami kryptografii. Ochrona obiegu dokumentów - kryptografia, certyfikaty. |  |  | 1 |  | EKP\_01, EKP\_02, EKP\_05 |
| Bezpieczeństwo usług sieciowych na przykładzie serwera WWW.  Ochrona systemów – zapory, detekcja zagrożeń, prewencja. |  |  | 1 |  | EKP\_01, EKP\_02, EKP\_05 |
| Instytucje zajmujące się bezpieczeństwem – przegląd wybranych serwisów. |  |  | 1 |  | EKP\_01, EKP\_02, EKP\_05 |
| Polityka bezpieczeństwa informacji – przykłady. |  |  | 1 |  | EKP\_01, EKP\_02, EKP\_05 |
| Zadanie podsumowujące – implementacja przykładowej polityki bezpieczeństwa w wybranym systemie. |  |  | 2 |  | EKP\_01, EKP\_02, EKP\_05 |
| **Łącznie godzin** | **18** |  | **9** |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Metody weryfikacji efektów kształcenia dla przedmiotu** | | | | | | | | | |
| **Symbol EKP** | **Test** | **Egzamin ustny** | **Egzamin pisemny** | **Kolokwium** | **Sprawozdanie** | **Projekt** | **Prezentacja** | **Zaliczenie praktyczne** | **Inne** |
| EKP\_01 |  |  | X |  |  |  |  |  |  |
| EKP\_02 |  |  | X |  |  |  |  |  |  |
| EKP\_03 |  |  | X |  |  |  |  |  |  |
| EKP\_04 |  |  | X |  |  |  |  |  |  |
| EKP\_05 |  |  |  |  |  |  |  | X |  |

|  |
| --- |
| **Kryteria zaliczenia przedmiotu** |
| Egzamin pisemny (test=5 pytań testowych). Próg zaliczenia 60%.  Zaliczenie laboratorium, zadanie zliczające. Próg zaliczający 75%.  Zaliczenie przedmiotu: pozytywna ocena z laboratorium i pozytywna ocena z egzaminu. |

Uwaga: student otrzymuje ocenę powyżej dostatecznej, jeżeli uzyskane efekty kształcenia przekraczają wymagane minimum.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nakład pracy studenta** | | | | | |
| **Forma aktywności** | **Szacunkowa liczba godzin przeznaczona na zrealizowanie aktywności** | | | | |
| **W** | **C** | **L** | | **P** |
| Godziny kontaktowe | 18 |  | 9 | |  |
| Czytanie literatury | 25 |  | 20 | |  |
| Przygotowanie do zajęć ćwiczeniowych, laboratoryjnych, projektowych |  |  | 10 | |  |
| Przygotowanie do egzaminu, zaliczenia | 15 |  |  | |  |
| Opracowanie dokumentacji projektu/sprawozdania |  |  |  | |  |
| Uczestnictwo w zaliczeniach i egzaminach | 2 |  |  | |  |
| Udział w konsultacjach | 2 |  | 2 | |  |
| **Łącznie godzin** | **62** |  | **41** | |  |
| **Sumaryczna liczba godzin dla przedmiotu** | **103** | | | | |
| **Sumaryczna liczba punktów ECTS dla przedmiotu** | **4** | | | | |
|  | **Liczba godzin** | | | **ECTS** | |
| Obciążenie studenta związane z zajęciami praktycznymi | 41 | | | 2 | |
| Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich | 33 | | | 1 | |

|  |
| --- |
| **Literatura podstawowa** |
| Pipkin D. L.. Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa. WNT. Warszawa 2002.  Żółkiewicz J. Materiały do wykładu „Bezpieczeństwo systemów informacyjnych”. AMG. ILIAS. Gdynia 2016, 2017. |
| **Literatura uzupełniająca** |
| Fisher B. Przestępstwa komputerowe i ochrona informacji. Kantor Wydawniczy Zakamycze 2000. Kraków.  Harley d., R. Slade, U. E. Gattiker. Wirusy cała prawda. Wydawnictwo Translator. Warszawa 2003.  Liderman K. Analiza ryzyka i ochrona informacji. MIKOM-PWN. Warszawa 2008.  Polaczek T. Audyt Bezpieczeństwa Informacji W Praktyce. Helion. Gliwice 2006.  Scambray J., S. McClure, G. Kurtz. Hakerzy - cała prawda. Wydawnictwo Translator. Warszawa 2001.  Schetina E., K. Green, J. Carlson. Bezpieczeństwo w sieci. Helion. Gliwice 2002.  Strebe M. Bezpieczeństwo sieci. Mikom 2005.  PN ISO/IEC 17799:2003.  Norma ISO/IEC TR 13335. |

|  |  |
| --- | --- |
| **Osoba odpowiedzialna za przedmiot** | |
| dr inż. Janusz Żółkiewicz | KSI |
| **Pozostałe osoby prowadzące przedmiot** | |
| mgr Ireneusz Meyer | KSI |
| mgr inż. Henryk Szreder | KSI |