#### karta przedmiotu

|  |  |
| --- | --- |
| Nazwa przedmiotu | Bezpieczeństwo systemów informatycznych |

1. Usytuowanie przedmiotu w systemie studiów

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

|  |  |
| --- | --- |
| 1.5. Wydział | Wydział nauk technicznych |
| 1.6. Specjalność | Dla wszystkich specjalności |
| 1.7. Koordynator przedmiotu | dr Michał Kalisz |

2. Ogólna charakterystyka przedmiotu

|  |  |
| --- | --- |
| 2.1. Przynależność do grupy przedmiotu | kierunkowy |
| 2.2. Liczba ECTS | 2 |
| 2.3. Język wykładów | polski |
| 2.4. Semestry, na których realizowany jest przedmiot | 5 |
| 2.5.Kryterium doboru uczestników zajęć | - |

1. Efekty kształcenia i sposób prowadzenia zajęć
   1. Cele przedmiotu

|  |  |
| --- | --- |
| Lp. | Cele przedmiotu |
|
| C1 | Zapoznanie z głównymi problemami bezpieczeństwa systemów informatycznych |
| C2 | Zapoznanie z metodami wykrywania i zapobiegania naruszeniem bezpieczeństwa systemów informatycznych |
| C3 | Opanowanie podstawowych zasad tworzenia bezpiecznej infrastruktury informatycznej. |

3.2. Przedmiotowe efekty kształcenia, z podziałem na wiedzę, umiejętności i kompetencje, wraz z odniesieniem do kierunkowych efektów kształcenia

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Lp. | Opis przedmiotowych efektów kształcenia | Odniesienie do kierunkowych efektów  kształcenia | |  | | |
| Po zaliczeniu przedmiotu student w zakresie **wiedzy** potrafi | | | |
| W1 | Ma szczegółową wiedzę związaną z głównymi problemami bezpieczeństwa systemów informatycznych | INF\_W04 | |
| W2 | Ma podstawową wiedzę o cyklu życia i utrzymania systemów informatycznych w celu zapewniania pożądanego poziomu bezpieczeństwa. | INF\_W05 | |
| W3 | Zna protokoły i standardy dotyczące bezpieczeństwa systemów informatycznych | INF\_W07 | |  | | |
| Po zaliczeniu przedmiotu student w zakresie **umiejętności** potrafi | | | |
| U1 | Potrafi identyfikować zagrożenia bezpieczeństwa systemów informatycznych i odpowiednio na nie reagować. | INF\_U11 | |
| U2 | Potrafi dokonać krytycznej analizy systemu informatycznego, pod względem bezpieczeństwa. | INF\_U13 | |
| U3 | Potrafi implementować standardowe mechanizmy bezpieczeństwa systemów informatycznych | INF\_U19 | |
| Po zaliczeniu przedmiotu student w zakresie **kompetencji społecznych** potrafi | | |  | |  | InzA\_W02, InzA\_W01 |
| K1 | Rozumie potrzebę stałego pogłębiania wiedzy w dziedzinie bezpieczeństwa systemów informatycznych. | INF\_K01 | |  | | |
| K2 | Ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżynierskiej, w tym jej wpływu na środowisko, i związanej z tym odpowiedzialności za podejmowane decyzje | INF\_K02 | |

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ścieżka | Wykład | Ćwiczenia | Projekt | Warsztat | Laboratorium | Seminarium | Lektorat | Dodatkowe zajęcia prowadzone z wykorzystaniem metod i technik kształcenia na odległość w formie  wykładu | Inne | **Punkty ECTS** |
| NST | 10 |  |  |  |  |  |  | 10 |  | 2 |

3.4. Treści kształcenia

RODZAJ ZAJĘĆ: wykład

|  |  |
| --- | --- |
| Lp. | Treść zajęć |
| NST | |
| ZAJĘCIA NA UCZELNI | DODATKOWE ZAJĘCIA NA PLATFORMIE |
| 1. | Przykładowe problemy z dziedziny bezpieczeństwa IT. | W | W |
| 2. | Podatności i zagrożenia, ich klasyfikacja i źródła aktualnych informacji. | W | W |
| 3. | Podstawy bezpieczeństwa: poufność, integralność, dostępność; ochrona danych w spoczynku, podczas transmisji i podczas przetwarzania; mechanizmy bezpieczeństwa: technologie, polityki i procedury, czynnik ludzki. | W | W |
| 4. | Czynniki zagrożeń. Wykrywanie zagrożeń. | W | W |
| 5. | Kontrola dostępu. Ochrona systemu. | W | W |
| 6. | Bezpieczeństwo infrastruktury. | W | W |
| 7. | Kryptograficzne mechanizmy bezpieczeństwa. | W | W |
| 8. | Rozwiązania specjalistyczne. | W | W |

3.5. Metody weryfikacji efektów kształcenia (zaznaczyć „X” w odniesieniu do poszczególnych efektów)

Studia niestacjonarne:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Efekt kształcenia | Forma weryfikacji | | | | | | | |
| Egzamin ustny | Egzamin pisemny | Projekt | Kolokwium | Zadania domowe | Referat/  Prezentacja | Dyskusje | Inne (jakie?) |
| W1 | X |  |  |  |  |  | X |  |
| W2 | X |  |  |  |  |  | X |  |
| W3 | X |  |  |  |  |  | X |  |
| U1 | X |  |  |  |  |  | X |  |
| U2 | X |  |  |  |  |  | X |  |
| U3 | X |  |  |  |  |  | X |  |
| K1 | X |  |  |  |  |  | X |  |
| K2 | X |  |  |  |  |  | X |  |

3.6. Kryteria oceny osiągniętych efektów kształcenia

|  |  |  |  |
| --- | --- | --- | --- |
| Efekt kształcenia | Na ocenę 3 lub „zal.”  student potrafi | Na ocenę 4 student potrafi | Na ocenę 5 student potrafi |
| W1 | zna podstawowe problemy bezpieczeństwa systemów informatycznych | zna podstawowe problemy bezpieczeństwa systemów informatycznych i potrafi je sklasyfikować | zna podstawowe problemy bezpieczeństwa systemów informatycznych i potrafi je sklasyfikować i ocenić poziom ryzyka |
| W2 | zna podstawowe zasady zapewniania bezpieczeństwa systemów informatycznych | zna podstawowe zasady zapewniania bezpieczeństwa systemów informatycznych i wie w jakich sytuacjach należy je stosować | zna podstawowe zasady zapewniania bezpieczeństwa systemów informatycznych i wie w jakich sytuacjach należy je stosować w sposób możliwie optymalny |
| W3 | Potrafi wymienić protokoły i standardy dotyczące bezpieczeństwa systemów informatycznych | Potrafi wymienić i scharakteryzować protokoły i standardy dotyczące bezpieczeństwa systemów informatycznych | Potrafi wymienić, scharakteryzować i ocenić przydatność protokołów i standardy dotyczących bezpieczeństwa systemów informatycznych |
| U1 | Potrafi identyfikować zagrożenia bezpieczeństwa systemów informatycznych. | Potrafi identyfikować zagrożenia bezpieczeństwa systemów informatycznych i odpowiednio na nie reagować. | Potrafi identyfikować zagrożenia bezpieczeństwa systemów informatycznych, skutecznie przeciwdziałać im i odpowiednio na nie reagować. |
| U2 | Potrafi wskazać potencjalnie zagrożone elementy systemu informatycznego. | Potrafi wskazać potencjalnie zagrożone elementy systemu informatycznego i ocenić ryzyko. | Potrafi wskazać potencjalnie zagrożone elementy systemu informatycznego, ocenić ryzyko i zaproponować skuteczne rozwiązania. |
| U3 | Potrafi implementować podstawowe mechanizmy bezpieczeństwa systemów informatycznych. | Potrafi implementować podstawowe mechanizmy bezpieczeństwa systemów informatycznych, w sposób skutecznie zabezpieczający przed aktualnymi zagrożeniami. | Potrafi optymalnie wybrać i za implementować podstawowe mechanizmy bezpieczeństwa systemów informatycznych, w sposób skutecznie zabezpieczający przed aktualnymi zagrożeniami. |
| K1 | Potrafi wskazać kilka certyfikatów zawodowych, szkoleń, źródeł pisanych lub elektronicznych, rozwijających wiedzę z zakresu bezpieczeństwa systemów informatycznych. | Potrafi uzasadnić konieczność zdobywania certyfikatów zawodowych, szkoleń oraz materiałów firmowych i technicznych standardów rozwijających wiedzę z zakresu bezpieczeństwa systemów informatycznych. | Dostrzega potrzebę zdobywania certyfikatów zawodowych, szkoleń dotyczących rozwoju zawodowego inżyniera bezpieczeństwa systemów informatycznych. |
| K2 | rozumie potrzebę ochrony danych | rozumie potrzebę ochrony danych oraz i jest świadomy odpowiedzialności | rozumie potrzebę ochrony danych oraz i jest świadomy odpowiedzialności, zna przepisy dotyczące ochrony danych osobowych |

3.7. Zalecana literatura

**Podstawowa**

W. Stallings, L. Brown, *Computer Security: Principles and Practice*, Pearson Education, 2018.

M. Stamp, *Information Security: Principles and Practice*, Wiley, 2011.

W. Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education, 2017.

David Salomon, Elements of Computer Security, Springer-Verlag, 2010.

**Uzupełniająca**

* materiały do kursu Cybersecurity Essentials (Cisco Netacad), dostępne po zalogowaniu się na platformę CISCO
* materiały do kursu CCNA Security (Cisco Netacad), dostępne po zalogowaniu się na platformę CISCO
* publikacje dotyczące problemu bezpieczeństwa systemów informatycznych

4. Nakład pracy studenta - bilans punktów ECTS

|  |  |  |
| --- | --- | --- |
| **Rodzaje aktywności studenta** | **Obciążenie studenta** | |
| **studia ST** | **studia NST** |
| **Zajęcia wymagające bezpośredniego kontaktu studenta z nauczycielem akademickim w siedzibie uczelni** |  | **10** |
| Zajęcia przewidziane planem studiów |  | 10 |
| Konsultacje dydaktyczne (mini. 10% godz. przewidzianych na każdą formę zajęć) |  | 2 |
| **Praca własna studenta** |  | **40** |
| Przygotowanie bieżące do zajęć |  | 10 |
| Przygotowanie prac projektowych/prezentacji/itp. |  | 10 |
| Przygotowanie do zaliczenia zajęć |  | 10 |
| Przygotowanie do zaliczenia całego przedmiotu |  | 10 |
| **SUMARYCZNE OBCIĄŻENIE GODZINOWE STUDENTA** |  | **50** |
| **Liczba punktów ECTS** |  | **2** |

|  |  |
| --- | --- |
| Data ostatniej zmiany | 29.10.2021 r. |
| Zmiany wprowadził | dr Michał Kalisz |
| Zmiany zatwierdził | dr inż. Michalina Gryniewicz-Jaworska |