**Politechnika Opolska**
**Wydział Elektrotechniki, Automatyki i Informatyki**

# KARTA OPISU PRZEDMIOTU

| STUDIA PODYPLOMOWE | **INFORMATYKA Z ELEMENTAMI INFORMATYKI ŚLEDCZEJ** |
|---|---|

| NAZWA PRZEDMIOTU | **TECHNICZNE ASPEKTY BEZPIECZEŃSTWA DANYCH** | | |
|---|---|---|---|
| SUBJECT TITLE | **DATA SECURITY** | | |
| SEMESTR STUDIÓW | ECTS (pkt.) | TRYB ZALICZENIA PRZEDMIOTU | KOD PRZEDMIOTU |
| 1 | 6 | ~~EGZAMIN~~ – ZALICZENIE NA OCENĘ *) | |
| Wymagania wstępne w zakresie przedmiotu | Nazwy przedmiotów | - | |
| | Wiedza | 1. Podstawowa wiedza z zakresu technologii informacyjnej | |
| | Umiejętności | 1. Potrafi obsługiwać komputer i system operacyjny | |
| | Kompetencje społeczne | 1. Potrafi współdziałać i pracować w grupie | |

| **PROGRAM PRZEDMIOTU** | | |
|---|---|---|
| FORMA ZAJĘĆ | LICZBA GODZIN ZAJĘĆ W SEMESTRZE | PROWADZĄCY ZAJĘCIA (tytuł/stopień naukowy, imię i nazwisko) |
| WYKŁAD | 10 | MGR INŻ. ARTUR KALINOWSKI |
| ĆWICZENIA | | |
| LABORATORIUM | 15 | MGR INŻ. ARTUR KALINOWSKI |
| PROJEKT | | |
| SEMINARIUM | | |

| **TREŚCI KSZTAŁCENIA (PROGRAM NAUCZANIA)** | | | |
|---|---|---|---|
| **WYKŁAD** | SPOSÓB REALIZACJI: | WYKŁAD Z WYKORZYSTANIEM RZUTNIKA | |
| Lp. | Tematyka zajęć | | Liczba godzin |
| 1. | Pojęcie wycieku danych i typy wycieków danych | | 1 |
| 2. | Zdalne pozyskiwanie informacji o użytkowniku i komputerze | | 1 |
| 3. | Identyfikacja użytkowników w serwisach internetowych, ich zainteresowań i geolokalizacji | | 1 |
| 4. | Analiza metadanych | | 1 |
| 5. | Metody ujawniania wycieków danych | | 1 |
| 6. | Metody zapobiegania wyciekom danych | | 1 |
| 7. | Techniki wykradania danych i ich skuteczność | | 1 |
| 8. | Wykorzystanie rygorystycznej polityki bezpieczeństwa z punktu widzenia intruzów | | 1 |
| 9. | Zabezpieczanie nośników danych przed niepowołanym odczytem | | 1 |
| 10. | Bezpieczne usuwanie danych z nośników<br>Zaliczenie przedmiotu. | | 1 |
| | | RAZEM GODZIN W SEMESTRZE | 10 |
| Sposoby sprawdzenia zamierzonych efektów kształcenia | | Kolokwium pisemne | |

| **LABORATORIUM** | SPOSÓB REALIZACJI: | ZAJĘCIA PRAKTYCZNE Z KOMPUTEREM |
|---|---|---|

| Lp. | Tematyka zajęć | Liczba godzin |
|---|---|---|
| 1. | Wykorzystanie harvesterów do pozyskiwania danych o użytkownikach i komputerach | 1 |
| 2. | Zastosowanie wyrażeń regularnych do wyszukiwania danych określonego typu | 1 |
| 3. | Analiza informacji ujawnianych przez przeglądarki internetowe i pozyskiwanie danych o komputerze użytkownika | 1 |
| 4. | Praktyczne wykorzystanie wycieku danych z aplikacji użytkownika | 1 |
| 5. | Wykorzystywanie błędów w logice działania aplikacji sieciowych do pozyskiwania danych | 1 |
| 6. | Techniki inżynierii społecznej i ich wykorzystanie | 1 |
| 7. | Pozyskiwanie informacji o użytkowniku na podstawie metadanych | 1 |
| 8. | Wykorzystanie serwisu Google do niejawnego pozyskiwania istotnych danych | 1 |
| 9. | Praktyczne wykorzystanie protokołu SNMP w celu przeprowadzenia ataku na urządzenie sieciowe | 1 |
| 10. | Pozyskiwanie danych tekstowych i binarnych z plików pagefile.sys oraz hiberfil.sys w celu odnalezienia poszukiwanych informacji o działaniach użytkownika | 1 |
| 11. | Komunikacja i wykradanie danych z użyciem protokołu ICMP | 1 |
| 12. | Pozyskiwanie informacji o użytkownikach w sieci lokalnej, pozyskiwanie listy loginów oraz komputerów na których pracują użytkownicy z danym loginem | 1 |
| 13. | Tworzenie skanerów użytkowników i haseł | 1 |
| 14. | Odzyskiwanie skasowanych i zmodyfikowanych plików | 1 |
| 15. | Techniki fałszowania i szybkiego zamazywania danych na nośnikach | 1 |
| | RAZEM GODZIN W SEMESTRZE | 15 |

| Sposoby sprawdzenia zamierzonych efektów kształcenia: | Wykonanie zadań wyznaczonych w trakcie zajęć |
|---|---|

| | | |
|---|---|---|
| Efekty kształcenia dla przedmiotu – po zakończonym cyklu kształcenia | Wiedza | 1. Zna podstawowe metody i narzędzia pomagające wykryć wyciek danych.<br>2. Dysponuje wiedzą o wykorzystywaniu błędów w logice działania aplikacji do pozyskiwania danych.<br>3. Zna i rozumie podstawowe pojęcia i zasady z zakresu ochrony danych oraz potrafi ustalić stopień bezpieczeństwo swoich danych. |
| | Umiejętności | 1. Ma umiejętność samokształcenia się<br>2. Potrafi posługiwać się technikami informacyjno-komunikacyjnymi właściwymi do realizacji zadań związanych z analizą bezpieczeństwa i wycieku danych |
| | Kompetencje społeczne | 1. Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role.<br>2. Prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu. |

ZAŁOŻENIA I CELE PRZEDMIOTU:
Celem przedmiotu jest zdobycie podstawowej wiedzy i umiejętności w zakresie analizowania i wykorzystywania wycieków danych do pozyskiwania wymaganych informacji oraz eliminowania potencjalnego zagrożenia związanego z wyciekiem danych.

METODY DYDAKTYCZNE:
Wykład – wykład konwencjonalny, wykład problemowy, dyskusja (środki: rzutnik, komputer, prezentacje, urządzenia sieciowe).
Laboratorium – metoda laboratoryjna problemowa, metoda zajęć praktycznych (środki: komputery, spreparowane pliki opracowane przez prowadzącego).

FORMA I WARUNKI ZALICZENIA PRZEDMIOTU:
Wykład – zaliczenie pisemne na ocenę.
Laboratorium – ocena na podstawie ocen cząstkowych z poszczególnych zadań do wykonania. Ocena odzwierciedlająca wiedzę, kreatywność i zdobyte umiejętności techniczne.

LITERATURA PODSTAWOWA:

[1] Viega J., *Mity bezpieczeństwa IT. Czy na pewno nie masz czego się bać?*, ISBN: 978-83-246-2588-8, Helion, 2012
[2] Erickson J., *Hacking. Sztuka penetracji.*, ISBN: 83-7361-418-4, Helion, 2004

LITERATURA UZUPEŁNIAJĄCA:

[1] Lockhart A., *125 sposobów na bezpieczeństwo sieci.*, ISBN: 978-83-246-0986-4, Helion, 2007
[2] Ross J., *Bezpieczne programowanie. Aplikacje hakeroodporne.*, ISBN: 978-83-246-2405-8, Helion, 2009

*) niewłaściwe przekreślić

| | |
|---|---|
| ..... | ..... |
| /Kierownik studiów podyplomowych/ | /autor – osoba prowadząca wykład/ |
| ..... | ..... |
| /Kierownik jednostki organizacyjnej: pieczęć i podpis/ | /Dziekan Wydziału WEAiI: pieczęć i podpis/ |