



### KARTA PRZEDMIOTU

|                                      |                            |                            |
|--------------------------------------|----------------------------|----------------------------|
| Kod przedmiotu                       | studia stacjonarne:        | E-ID2C-11-s2, E-ID2C-11-s3 |
|                                      | studia niestacjonarne:     | E-2IZ2C-1015-s3            |
| Nazwa przedmiotu                     | <b>Inżynieria wsteczna</b> |                            |
| Nazwa przedmiotu w języku angielskim | <b>Reverse engineering</b> |                            |
| Obowiązuje od roku akademickiego     | <b>2022/23</b>             |                            |

### USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

|                                  |                                                                                                              |
|----------------------------------|--------------------------------------------------------------------------------------------------------------|
| Kierunek studiów                 | <b>Informatyka</b>                                                                                           |
| Poziom kształcenia               | <b>II stopień</b>                                                                                            |
| Profil studiów                   | <b>Ogólnoakademicki</b>                                                                                      |
| Forma i tryb prowadzenia studiów | <b>Studia stacjonarne i niestacjonarne</b>                                                                   |
| Zakres                           | <b>Cyberbezpieczeństwo</b>                                                                                   |
| Jednostka prowadząca przedmiot   | <b>Katedra Systemów Informatycznych</b>                                                                      |
| Koordinator przedmiotu           | <b>Dr inż. Józef Ciosmak</b>                                                                                 |
| Zatwierdził                      | <b>Dziekan Wydziału Elektrotechniki, Automatyki i Informatyki<br/>dr hab. inż. Roman Deniziak, prof. PŚk</b> |

### OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

|                                          |                       |                                                                                                                         |
|------------------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------|
| Przynależność do grupy/bloku przedmiotów |                       | <b>Przedmiot specjalnościowy</b>                                                                                        |
| Status przedmiotu                        |                       | <b>Wybieralny</b>                                                                                                       |
| Język prowadzenia zajęć                  |                       | <b>Polski</b>                                                                                                           |
| Usytuowanie w planie studiów - semestr   | studia stacjonarne    | <b>Semestr II lub Semestr III</b>                                                                                       |
|                                          | studia niestacjonarne | <b>Semestr II lub Semestr III</b>                                                                                       |
| Wymagania wstępne                        |                       | <b>Architektura systemów komputerowych, Wprowadzenie do cyberbezpieczeństwa, Społeczne aspekty cyberbezpieczeństwa.</b> |
| Egzamin (TAK/NIE)                        |                       | <b>NIE</b>                                                                                                              |
| Liczba punktów ECTS                      |                       | <b>3</b>                                                                                                                |

| Forma prowadzenia zajęć   |                        | wykład    | ćwiczenia | laboratorium | projekt   | inne |
|---------------------------|------------------------|-----------|-----------|--------------|-----------|------|
| Liczba godzin w semestrze | studia stacjonarne:    | <b>30</b> |           |              | <b>30</b> |      |
|                           | studia niestacjonarne: | <b>18</b> |           |              | <b>18</b> |      |

## EFEKTY UCZENIA SIĘ

| Kategoria             | Symbol efektu | Efekty kształcenia                                                                                                                                                                                                                                                             | Odniesienie do efektów kierunkowych              |
|-----------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Wiedza                | W01           | Student zna i rozumie współczesne problemy cyberbezpieczeństwa.                                                                                                                                                                                                                | INF2_W02                                         |
|                       | W02           | Student dysponuje wiedzą pozwalającą na weryfikację zabezpieczeń systemów informatycznych.                                                                                                                                                                                     | INF2_W02, INF2_W08                               |
|                       | W03           | Student ma uporządkowaną wiedzę z zakresu architektury, organizacji i bezpieczeństwa systemów różnych systemów operacyjnych.                                                                                                                                                   | INF2_W02                                         |
| Umiejętności          | U01           | Student potrafi przeprowadzić czynności audytowe pozwalające ocenić stan zabezpieczenia systemu informatycznego i wskazać ewentualne braki                                                                                                                                     | INF2_U01, INF2_U02, INF2_U05, INF2_U06, INF2_U07 |
|                       | U02           | Student potrafi dobrać odpowiedni poziom bezpieczeństwa w celu zapewnienia ochrony przed zagrożeniami.                                                                                                                                                                         | INF2_U01, INF2_U02, INF2_U05, INF2_U06, INF2_U07 |
|                       | U03           | Student potrafi planować i przeprowadzać eksperymenty z zakresu ochrony informatycznej. Ponadto potrafi, przy użyciu odpowiednich metod i narzędzi, monitorować, wykrywać, usuwać i zapobiegać zagrożeniom,                                                                    | INF2_U01, INF2_U02, INF2_U05, INF2_U06, INF2_U07 |
| Kompetencje społeczne | K01           | Student ma świadomość znaczenia cyberbezpieczeństwa we współczesnym świecie. Potrafi określić politykę bezpieczeństwa i zastosować rozwiązania informatyczne pozwalające ją zaimplementować. Rozumie potrzebę ciągłego podnoszenia kompetencji w zakresie cyberbezpieczeństwa. | INF2_K03, INF2_K04                               |

## TREŚCI PROGRAMOWE

| Forma zajęć | Treści programowe                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wykład      | <ol style="list-style-type: none"> <li><b>Wprowadzenie do inżynierii wstecznej</b> (narodziny oprogramowania wstecznego. Cele, wymagania oraz metody wykorzystywane w inżynierii oprogramowania wstecznego).</li> <li><b>Narzędzia programistyczne w inżynierii wstecznej</b> (specjalistyczne oprogramowania do analizy kodu niskopoziomowego, analizy formatów plików wykonywalnych, śledzenia wykonywania kodu)</li> <li><b>Analiza kodu maszynowego</b> (dla wybranych elementów języków programowania i dedykowanych architektur procesorów).</li> <li><b>Omówienie mechanizmów ochrony aplikacji</b> (przed przepełnieniem bufora danych, przepełnieniem stosu, obsługą wyjątków, wykonaniem złośliwego kodu).</li> <li><b>Analiza kodu</b> (analiza statyczna, dekompilacja, rekompilacja, modyfikacja kodu). Utrudnienia w wykonaniu dekompilacji. Mechanizmy i cele ukrywania kodu programu).</li> <li><b>Techniki wstrzykiwania kodu</b> (przegląd dostępnych technik, wybór optymalnej metody do uzyskania dedykowanego celu, implementacja).</li> <li><b>Mechanizmy zabezpieczenia wykonywalnego kodu</b> (kodu z pamięci procesu, rozpoznania punktów rozpoczęcia programów. Packery, szyfratory, protektory, nanomity).</li> <li><b>Techniki przekierowania</b> (przekierowanie/przekserowanie API, techniki śledzenia wykonania procesu, implementacja przekierowania).</li> </ol> |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| projekt | <ol style="list-style-type: none"> <li>1. Studium wybranych narzędzi programistycznych wykorzystywanych w inżynierii wstecznej.</li> <li>2. Wykonanie zadania projektowego z zakresu inżynierii wstecznej – analiza statyczna, dekompilacja, rekompilacja, modyfikacja kodu, próba wstrzykiwania kodu, zabezpieczenia kodu, zamazywanie kodu, śledzenie wykonania procesów w wybranych systemach operacyjnych i dedykowanych architektur.</li> </ol> |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

| Symbol efektu | Metody sprawdzania efektów kształcenia |                 |           |         |              |      |
|---------------|----------------------------------------|-----------------|-----------|---------|--------------|------|
|               | Egzamin ustny                          | Egzamin pisemny | Kolokwium | Projekt | Sprawozdanie | Inne |
| W01           |                                        |                 | X         |         |              |      |
| W02           |                                        |                 | X         |         |              |      |
| W03           |                                        |                 | X         |         |              |      |
| U01           |                                        |                 |           | X       |              |      |
| U02           |                                        |                 |           | X       |              |      |
| U03           |                                        |                 |           | X       |              |      |
| K01           |                                        |                 |           | X       |              |      |

## FORMA I WARUNKI ZALICZENIA

| Forma zajęć | Forma zaliczenia   | Warunki zaliczenia                                            |
|-------------|--------------------|---------------------------------------------------------------|
| wykład      | zaliczenie z oceną | Uzyskanie co najmniej 50% punktów z kolokwium zaliczeniowego. |
| projekt     | zaliczenie z oceną | Uzyskanie co najmniej 50% punktów z zadań projektowych.       |

## NAKŁAD PRACY STUDENTA

| Bilans punktów ECTS |                                                                                                 |                       |   |   |    |   |                          |   |   |    |   |               |
|---------------------|-------------------------------------------------------------------------------------------------|-----------------------|---|---|----|---|--------------------------|---|---|----|---|---------------|
| Lp.                 | Rodzaj aktywności                                                                               | Obciążenie studenta   |   |   |    |   |                          |   |   |    |   | Jednos<br>tka |
|                     |                                                                                                 | studia<br>stacjonarne |   |   |    |   | studia<br>niestacjonarne |   |   |    |   |               |
| 1.                  | Udział w zajęciach zgodnie z planem studiów                                                     | W                     | C | L | P  | S | W                        | C | L | P  | S | h             |
|                     |                                                                                                 | 30                    |   |   | 30 |   | 18                       |   |   | 18 |   |               |
| 2.                  | Inne (konsultacje, egzamin)                                                                     | 2                     |   |   | 2  |   | 2                        |   |   | 2  |   | h             |
| 3.                  | Razem przy bezpośrednim udziale nauczyciela akademickiego                                       | 64                    |   |   |    |   | 40                       |   |   |    |   | h             |
| 4.                  | Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego | 2,56                  |   |   |    |   | 1,6                      |   |   |    |   | ECTS          |
| 5.                  | Liczba godzin samodzielnej pracy studenta                                                       | 11                    |   |   |    |   | 35                       |   |   |    |   | h             |
| 6.                  | Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy                         | 0,44                  |   |   |    |   | 1,4                      |   |   |    |   | ECTS          |
| 7.                  | Nakład pracy związany z zajęciami o charakterze praktycznym                                     | 30                    |   |   |    |   | 18                       |   |   |    |   | h             |

|     |                                                                                             |            |             |      |
|-----|---------------------------------------------------------------------------------------------|------------|-------------|------|
| 8.  | <b>Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym</b> | <b>1,2</b> | <b>0,72</b> | ECTS |
| 9.  | <b>Sumaryczne obciążenie pracą studenta</b>                                                 | <b>75</b>  | <b>75</b>   | h    |
| 10. | <b>Punkty ECTS za moduł</b><br><i>1 punkt ECTS=25 godzin obciążenia studenta</i>            | <b>3</b>   |             | ECTS |

## LITERATURA

1. Eldad Eilam, "Reversing: Secrets of Reverse Engineering", 2005, Wiley, ISBN-10 0764574817.
2. Bruce Dang, Alexandre Gazet, Elias Bachaalany, Sébastien Josse, "Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation", 2014, Wiley, ISBN-10 1118787315.
3. Mateusz Jurczyk, Gynael Colwind, „Praktyczna inżynieria wsteczna. Metody, techniki, narzędzia”, PWN, 2016, ISBN 978-83-01-18951-8.
4. Dmitry Vostokov, „Pattern-Oriented-Diagnostics-Debugging-Malware-Analysis-Reversing-Log-Analysis-Memory-Forensics”, 2018, <https://www.amazon.com/Pattern-Oriented-Diagnostics-Debugging-Reversing-Forensics-ebook/dp/B07L8D86FQ>.
5. Chris Eagle, Kara Nance, "The Ghidra Book The Definitive Guide", 2022, ISBN 101718501021, ISBN-13. 978-1718501027.