

| AKADEMIA WSB   |  |  |     |   |   |                           |     |
|--|--|--|-----|---|---|---------------------------|-----|
| Kierunek studiów: Zarządzanie i inżynieria produkcji   |  |  |     |   |   |                           |     |
| Przedmiot: Bezpieczeństwo w sieci i wybrane narzędzia informatyczne  |  |  |     |   |   |                           |     |
| Profil kształcenia: praktyczny   |  |  |     |   |   |                           |     |
| Poziom kształcenia: studia I stopnia   |  |  |     |   |   |                           |     |
| Liczba godzin w semestrze  | 1  |  | 2   |   | 3 |                           | 4   |
|  | I  | II   | III | IV  | V | VI                        | VII |
| Studia stacjonarne (w/ćw/lab/pr/e)*  |  |  | 12w |   |   |                           |     |
| Studia niestacjonarne (w/ćw/lab/pr/e)  |  |  | 12w |   |   |                           |     |
| <b>WYKŁADOWCA</b>  |  |  |     |   |   |                           |     |
| <b>FORMA ZAJĘĆ</b>   | Wykład   |  |     |   |   |                           |     |
| <b>CELE PRZEDMIOTU</b>   | Celem przedmiotu jest poznanie przez studenta potencjalnych zagrożeń płynących z sieci oraz narzędzi informatycznych wpływających na zwiększenie poziomu bezpieczeństwa. |  |     |   |   |                           |     |
| Efekt KIERUNKOWY   | Odniesienie do efektów uczenia się zgodnie z PRK   | Opis efektów uczenia się   |     |   |   | Sposób weryfikacji efektu |     |
|  |  | Wiedza   |     |   |   |                           |     |
| ZIP_W03  | P6S_WG   | W zaawansowanym stopniu wie jak zwiększać swój poziom bezpieczeństwa korzystając z sieci komputerowych. Wie z jakich narzędzi korzystać aby praca w sieci była bezpieczna.                 |     |   |   | Test                      |     |
|  |  | Umiejętności   |     |   |   |                           |     |
| ZIP_U05  | P6S_UW, inż.   | Student potrafi korzystać z różnych narzędzi informatycznych zwiększających poziom bezpieczeństwa.   |     |   |   | Test                      |     |
|  |  | Kompetencje społeczne  |     |   |   |                           |     |
| ZIP_K01<br>ZIP_K02   | P6S_KK   | Student jest gotów do krytycznego spojrzenia na informacje pozyskiwane z sieci Internet, dąży do ich weryfikacji korzystając również z opinii ekspertów                                    |     |   |   | Test, dyskusja            |     |
| ZIP_K06  | P6S_KR   | Student jest gotów do odpowiedzialnego wykonywania czynności zawodowych i podejmowania skutecznych działań w zakresie zwiększania własnego poziomu bezpieczeństwa w sieci oraz innych osób |     |   |   |                           |     |
| <b>Nakład pracy studenta (w godzinach dydaktycznych 1h dyd.=45 minut)**</b>  |  |  |     |   |   |                           |     |
| <b>Stacjonarne</b><br>udział w wykładach = 12<br>udział w ćwiczeniach =<br>przygotowanie do ćwiczeń =<br>przygotowanie do wykładu = 12<br>przygotowanie do egzaminu = 12<br>realizacja zadań projektowych =<br>e-learning =<br>zaliczenie/egzamin = 2<br>inne (określ jakie) =<br><b>RAZEM: 38</b><br><b>Liczba punktów ECTS: 1.5</b><br><b>w tym w ramach zajęć praktycznych:</b> |  |  |     | <b>Niestacjonarne</b><br>udział w wykładach = 12<br>udział w ćwiczeniach =<br>przygotowanie do ćwiczeń =<br>przygotowanie do wykładu = 12<br>przygotowanie do egzaminu = 10<br>realizacja zadań projektowych =<br>e-learning =<br>zaliczenie/egzamin = 2<br>inne (określ jakie) = 2 konsultacje<br><b>RAZEM: 38</b><br><b>Liczba punktów ECTS: 1.5</b><br><b>w tym w ramach zajęć praktycznych:</b> |   |                           |     |

|   |   |
|---|---|
| <b>WARUNKI WSTĘPNE</b>  | Wiedza z zakresu technologii informacyjnej oraz podstaw informatyki   |
| <b>TREŚCI PRZEDMIOTU</b>                                      | <p>Treści realizowane w formie bezpośredniej:</p> <ul style="list-style-type: none"> <li>• Fundamentalne procesy związane z bezpieczeństwem: uwierzytelnienie i autoryzacja, poufność, integralność, dostępność, autentyczność, rozliczalność.</li> <li>• Metody procesu uwierzytelniania: jednokierunkowe, dwukierunkowe</li> <li>• Podział zagrożeń związanych z funkcjonowaniem systemów informatycznych w tym zagrożenia: fizyczne, personalne, organizacyjne, programowe, sprzętowe, administracyjne, z sieci internet.</li> <li>• Zagrożenia płynące z sieci internet: wirusy, makro wirusy, robaki, trojany, spayware, phishing, stealware, exploit, rootkit, backdoor, keylogger, dialer, wabbit, ransomware, SQL injection, DoS.</li> <li>• Praktyczne aspekty prób wyludzeń informacji oraz ataków z sieci internet.</li> <li>• Narzędzia do szyfrowania dysków, katalogów, plików w tym: BitLocker, VeraCrypt, 7zip, WinRar, WinZip,</li> <li>• Zabezpieczanie dokumentów elektronicznych za pomocą podpisu kwalifikowanego podpisu zaufanego (obywatel.gov.pl)</li> <li>• Zabezpieczanie dokumentów pakietu Microsoft Office.</li> <li>• Zabezpieczanie plików *.pdf.</li> </ul> <p>Treści realizowane w formie e-learning:</p> <p>Atak Ransomware – jak się bronić<br/>Zagrożenia płynące z internetu<br/>Zabezpieczanie dokumentów w postaci elektronicznej</p> |
| <b>LITERATURA OBOWIĄZKOWA</b>                                 | - Pieleszek M., Bądź bezpieczny w cyfrowym świecie. Poradnik bezpieczeństwa IT dla każdego, Helion, 2018, ISBN 9788328345898  |
| <b>LITERATURA UZUPEŁNIAJĄCA</b>                               | - Sachin S. Shetty, Charles A. Kamhoua, Laurent L. Njilla, Bezpieczeństwo w sieci - Jak skutecznie chronić się przed atakami (ebook), Wydawnictwo Naukowe PWN, 2020, ISBN 9788301211431<br>- Lidermann K., Bezpieczeństwo informacyjne. Nowe wyzwania (ebook), Wydawnictwo Naukowe PWN, 2018, ISBN 9788301201449<br>- Maurizio Martellini, Cyber Security, Springer International Publishing, 2013, ISBN 978-3-319-02278-9  |
| <b>METODY NAUCZANIA</b>                                       | <p>W formie bezpośredniej na platformie Teams:<br/>Zajęcia prowadzone są w formie wykładu informacyjno-konwersatoryjnego z wykorzystaniem środków audiowizualnych.</p> <p>W formie e-learning, na platformie Moodle:<br/>Prezentacja PowerPoint, dodatkowe materiały informacyjne.</p>  |
| <b>POMOCE NAUKOWE</b>   | Brak  |
| <b>PROJEKT (o ile jest realizowany w ramach modułu zajęć)</b> | Brak  |
| <b>FORMA I WARUNKI ZALICZENIA</b>                             | Zaliczenie z oceną<br>Podstawą zaliczenia przedmiotu jest uzyskanie pozytywnej oceny (min. 50% punktów) z testu końcowego - jednokrotnego wyboru umieszczonego na platformie Moodle.  |

\* W-wykład, ćw- ćwiczenia, lab- laboratorium, pro- projekt, e- e-learning