

KARTA PRZEDMIOTU (SYLABUS)

Opis przedmiotu

| | | | | |
|---|--------------------|---|--|---------------------|
| Kod przedmiotu | | Nazwa przedmiotu | Bezpieczeństwo aplikacji i sieci komputerowych | |
| AIwB/O/I/ST/B1-37b | | | Security of computer applications and networks | |
| Język wykładowy | | Polski | | |
| Rok akademicki | | 2026/2027 | | |
| Kierunek | | Sztuczna Inteligencja w Biznesie | | |
| w zakresie | | - | | |
| Poziom studiów | | studia pierwszego stopnia | | |
| Profil studiów | | ogólnoakademicki | | |
| Forma studiów | | studia stacjonarne | | |
| Semestr / semestry | | semestr czwarty | | |
| Przynależność do grupy zajęć | | B. Grupa zajęć kierunkowych B1. Grupa zajęć kierunkowych wybieralnych | | |
| Status przedmiotu | | Wybieralny | | |
| Formy realizacji zajęć dydaktycznych, wymiar, punkty ECTS | | Forma zajęć | Liczba godzin zajęć dydaktycznych | Liczba punktów ECTS |
| | | Wykład | 15 [h] | 3,5 ECTS |
| | | Ćwiczenia | [h] | |
| | | Laboratorium | 30 [h] | |
| Powiązanie przedmiotu | z profilem studiów | Związany z prowadzoną działalnością naukową w dyscyplinie informatyka techniczna i telekomunikacja | | 3 ECTS |
| | z uprawnieniami | | | ECTS |
| | z dyscypliną | Informatyka techniczna i telekomunikacja | | 3,5 ECTS |
| Forma nauczania | | Tradycyjna - zajęcia zorganizowane w Uczelni/ zajęcia realizowane z wykorzystaniem metod i technik kształcenia na odległość | | |
| Wymagania wstępne | | Wymagana znajomość z przedmiotu analiza matematyka, bardzo dobra znajomość podstawy programowania. | | |
| Jednostka prowadząca | | Katedra Biznesu i Finansów Międzynarodowych | | |
| Koordynator | | Dr inż. Jacek Wołoszyn | | |
| Adres strony internetowej pjo | | http://weif.uniwersytetradom.pl | | |
| Adres e-mail, telefon koordynatora | | Jacek.woloszyn@urad.edu.pl (48) 361-7410 | | |

**EFEKTY UCZENIA SIĘ, TREŚCI PROGRAMOWE, REALIZACJA ZAJĘĆ DYDAKTYCZNYCH,
WERYFIKACJA EFEKTÓW UCZENIA SIĘ**

| | |
|-----------------------------------|---|
| Cel kształcenia: | Celem kształcenia jest zapoznanie studentów z metodami ochrony aplikacji oraz sieci komputerowych przed zagrożeniami cybernetycznymi, w szczególności z mechanizmami zabezpieczania komunikacji sieciowej, ochrony aplikacji przed podatnościami oraz identyfikacji i przeciwdziałania atakom na systemy informatyczne. |
| Treści programowe: | <p>Treści zajęć są powiązane z prowadzonymi badaniami naukowymi.</p> <p>Treści wykładów:</p> <p>Podstawowe pojęcia związane z bezpieczeństwem aplikacji i sieci komputerowych. Architektura sieci komputerowych oraz podstawowe protokoły komunikacyjne w kontekście bezpieczeństwa. Rodzaje zagrożeń i ataków na aplikacje oraz sieci komputerowe (np. ataki typu DoS/DDoS, phishing, malware, ataki na aplikacje webowe). Podatności aplikacji i systemów informatycznych oraz metody ich identyfikacji. Mechanizmy zabezpieczania aplikacji, w tym uwierzytelnianie, autoryzacja, szyfrowanie oraz zarządzanie sesjami użytkowników. Bezpieczeństwo komunikacji sieciowej – protokoły szyfrowane (np. HTTPS, VPN), zapory sieciowe oraz systemy wykrywania intruzów. Podstawy testowania bezpieczeństwa aplikacji i sieci komputerowych. Przegląd standardów i dobrych praktyk w zakresie bezpieczeństwa systemów informatycznych.</p> <p>Suma: 15 [h]</p> <p>Treść laboratoriów:</p> <p>Konfiguracja podstawowych mechanizmów bezpieczeństwa w sieciach komputerowych. Analiza ruchu sieciowego oraz identyfikacja potencjalnych zagrożeń. Testowanie podatności aplikacji webowych oraz analiza podstawowych typów ataków (np. XSS, SQL Injection). Konfiguracja mechanizmów uwierzytelniania i autoryzacji w aplikacjach. Zastosowanie narzędzi do monitorowania bezpieczeństwa sieci oraz analizy logów systemowych. Podstawy testów penetracyjnych w kontrolowanym środowisku laboratoryjnym. Implementacja prostych mechanizmów zabezpieczających aplikacje oraz komunikację sieciową. Analiza przypadków naruszeń bezpieczeństwa oraz opracowanie podstawowych procedur ochrony systemów.</p> <p>Suma: 30 [h]</p> |
| Metody dydaktyczne (kształcenia): | <ul style="list-style-type: none"> - metody podające (wykład informacyjny), - metody programowane (z wykorzystaniem komputera), - Obserwacja <p>Zajęcia prowadzone w programie Python3. a także wykorzystanie Biblioteki Numpy, Pandas, Matplotlib, Scikit-learn Tensorflow, Pytorch,</p> |
| | <p>Warunkiem zaliczenia przedmiotu jest osiągnięcie wszystkich wymaganych efektów uczenia się określonych dla danego przedmiotu. Uzyskanie pozytywnych ocen ze wszystkich form zajęć wchodzących w skład danego przedmiotu jest równoznaczne z jego zaliczeniem i zdobyciem przez studenta liczby punktów ECTS przyporządkowanej temu przedmiotowi.</p> <p>Sposób obliczenia oceny końcowej z przedmiotu określa regulamin studiów.</p> <p>Sposób obliczania oceny z poszczególnych form zajęć przedstawia się następująco:</p> <p>Na ocenę z laboratorium składa się: punktowa ocena wykonanego projektu</p> <p>Na ocenę z wykładu składa się wynik otwartego testu pisemnego.</p> <p>Ocena z egzaminu – wynik otwartego testu pisemnego.</p> |

| | |
|--|--|
| | <p>Zdobyte w poszczególnych formach zajęć punkty przeliczane zostają na ocenę wg skali:</p> <p>Ocena 2 poniżej 51%</p> <p>Ocena 3 od 51%</p> <p>Ocena 3,5 od 61%</p> <p>Ocena 4 od 71%</p> <p>Ocena 4,5 od 81%</p> <p>Ocena 5 od 91%</p> |
|--|--|

| Efekty uczenia się dla przedmiotu w odniesieniu do efektów kierunkowych i formy zajęć | | | | Metody weryfikacji efektów uczenia się | |
|---|--|------------------------------------|-------------------------|--|---|
| Numer efektu uczenia się | Opis efektów uczenia się dla przedmiotu (PEU) Student, który zaliczył przedmiot (W) zna i rozumie/ (U) potrafi /(K) jest gotów do: | Kierunkowy efekt uczenia się (KEU) | Forma zajęć | Forma weryfikacji (zaliczeń) | Metody sprawdzania i oceny |
| W1 | zna i rozumie podstawowe zagrożenia bezpieczeństwa aplikacji oraz sieci komputerowych, a także metody ich identyfikacji i ograniczania. | K_W03 K_W05 K_W09 | wykład | Zaliczenie na ocenę | pisemny test otwarty |
| W2 | zna i rozumie mechanizmy zabezpieczania aplikacji oraz komunikacji sieciowej, w tym uwierzytelnianie, autoryzację, szyfrowanie i kontrolę dostępu. | K_W03 K_W05 K_W09 | wykład | Zaliczenie na ocenę | pisemny test otwarty |
| U1 | potrafi analizować podatności aplikacji i sieci komputerowych oraz identyfikować potencjalne zagrożenia bezpieczeństwa. | K_U05 K_U09 | laboratorium | Zaliczenie na ocenę | ocena zadań laboratoryjnych |
| U2 | potrafi stosować podstawowe narzędzia i techniki zwiększające bezpieczeństwo aplikacji oraz infrastruktury sieciowej. | K_U05 K_U09 | laboratorium | Zaliczenie na ocenę | ocena zadań laboratoryjnych |
| K1 | jest gotów do przestrzegania zasad bezpieczeństwa informacji podczas projektowania i użytkowania systemów informatycznych. | K_K02 K_K05 | Wykład/ laboratorium | Zaliczenie na ocenę | Obserwacja, aktywność na zajęciach obserwacja |
| K2 | jest gotów do ciągłego rozwijania wiedzy w zakresie nowych zagrożeń oraz metod ochrony aplikacji i sieci komputerowych. | K_K02 K_K05 | Wykład/ laboratorium | Zaliczenie na ocenę | Obserwacja, aktywność na zajęciach obserwacja |

| Literatura i pomoce naukowe |
|--|
| <p>Literatura podstawowa:</p> <ol style="list-style-type: none"> 1. Stuttard D., Pinto M., <i>The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws</i>, 2nd Edition, Wiley, 2011. 2. Kurose J. F., Ross K. W., <i>Computer Networking: A Top-Down Approach</i>, 8th Edition, Pearson, 2021. 3. Stallings W., <i>Network Security Essentials: Applications and Standards</i>, 6th Edition, Pearson, 2020. 4. Anderson R., <i>Security Engineering: A Guide to Building Dependable Distributed Systems</i>, 3rd Edition, Wiley, 2020. 5. Bishop M., <i>Computer Security: Art and Science</i>, 2nd Edition, Addison-Wesley, 2018. <p>Literatura uzupełniająca:</p> <ol style="list-style-type: none"> 1. Kim D., Solomon M., <i>Fundamentals of Information Systems Security</i>, 3rd Edition, Jones & Bartlett Learning, 2021. 2. Easttom C., <i>Network Defense and Countermeasures</i>, 2nd Edition, Pearson, 2018. 3. Vacca J. R., <i>Computer and Information Security Handbook</i>, 3rd Edition, Elsevier, 2017. 4. Scarfone K., Mell P., <i>Guide to Intrusion Detection and Prevention Systems (IDPS)</i>, NIST Special Publication, 2018. 5. Behl A., Behl K., <i>Cybersecurity and Cyberwar: What Everyone Needs to Know</i>, Oxford University Press, 2020. 6. Gruszczak A., <i>Cyberbezpieczeństwo w teorii i praktyce</i>, Difin, Warszawa, 2020. 7. OWASP Foundation, <i>OWASP Top 10 – The Ten Most Critical Web Application Security Risks</i>, OWASP, 2021. |

8. 21st Century Computer Science - Challenges and Dilemmas : Artificial Intelligence - The Future of IT. (2025). W J. W. Wołoszyn & A. M. Molga (Redaktorzy), Monografie - Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego (No. 345; s. 155). Uniwersytet Radomski im. Kazimierza Pułaskiego. <https://katalog.uniwersytetradom.pl/1783601768532/ksiazka/21st-century-computer-science-challenges-and-dilemmas?bibFilter=178>
 9. Molga, A. M., & Wołoszyn, J. W. (2025). AI and Cybersecurity-Will AI Become the Shield of the Network? Dydaktyka Informatyki , Article 20. <https://doi.org/10.15584/di.2025.20.5>
- Szczegółowy wykaz dodatkowych źródeł i pomocy naukowych na pierwszych zajęciach podają prowadzący.

| Nakład pracy studenta potrzebny do osiągnięcia zakładanych efektów uczenia się – bilans punktów ECTS | | |
|--|---|---------------------|
| Udział w zajęciach, aktywność | Obciążenie studenta [h] | |
| | Praca własna studenta - zajęcia bez nauczyciela (ZBN) | Zajęcia dydaktyczne |
| Udział w wykładach i laboratoriach | X | 45 [h] |
| Przygotowanie do <i>zajęć</i> , Przygotowanie do <i>zaliczenia</i> | 43 [h] | X |
| Sumaryczne obciążenie pracą studenta | 43 [h]/ 1,7 ECTS | 45 [h]/ 1,8 ECTS |
| Punkty ECTS za przedmiot | 3,5 ECTS | |

| Informacje dodatkowe, uwagi |
|---|
| <p>W przypadku studentów ze szczególnymi potrzebami, w tym: z niepełnosprawnością, przewlekle chorych, określone powyżej (w karcie) metody i formy weryfikacji efektów uczenia się dostosowuje się odpowiednio do indywidualnych potrzeb tych studentów.</p> <p>Szczegółowe zasady i formy wsparcia studentów ze szczególnymi potrzebami: w tym z niepełnosprawnością, przewlekle chorych podczas zajęć, zaliczeń i egzaminów określono w: Regulaminie Studiów, Zasadach Studiowania, Procedurze dotyczącej zapewnienia dostępności procesu kształcenia studentom ze szczególnymi potrzebami, w tym: z niepełnosprawnością, przewlekle chorych.</p> |