



## KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Zaawansowane bezpieczeństwo systemów komputerowych

### Przedmiot

Kierunek studiów

Rok/semestr

Informatyka

1/1

Studia w zakresie (specjalność)

Profil studiów

Cyberbezpieczeństwo

ogólnoakademicki

Poziom studiów

Język oferowanego przedmiotu

drugiego stopnia

angielski

Forma studiów

Wymagalność

stacjonarne

obieralny

### Liczba godzin

Wykład

Laboratoria

Inne (np. online)

15

45

Ćwiczenia

Projekty/seminaria

### Liczba punktów ECTS

5

### Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

Odpowiedzialny za przedmiot/wykładowca:

dr inż. Michał Szychowiak

email: [Michal.Szychowiak@cs.put.poznan.pl](mailto:Michal.Szychowiak@cs.put.poznan.pl)

tel. 61 665 2964

Wydział Informatyki i Telekomunikacji

ul. Piotrowo 3 60-965 Poznań

### Wymagania wstępne

Efekty kształcenia ze studiów I stopnia zdefiniowane w Uchwale Senatu PP, a szczególnie efekty K1st\_W1, K1st\_W3, K1st\_W4, K1st\_W6, K1st\_W7, K1st\_U1, K1st\_U2, K1st\_U15, K1st\_U18, K1st\_K1 i K1st\_K2, weryfikowane w procesie rekrutacji na studia 2 stopnia. Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z systemów operacyjnych, sieci komputerowych oraz bezpieczeństwa systemów informatycznych. Ponadto w zakresie kompetencji społecznych student musi prezentować takie postawy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.



### Cel przedmiotu

1. Przekazanie studentom szczegółowej wiedzy z dziedziny bezpieczeństwa systemów komputerowych w zakresie sieci komputerowych i systemów przetwarzania rozproszonego.
2. Rozwijanie u studentów umiejętności rozwiązywania problemów bezpieczeństwa przetwarzania oraz ochrony danych środowisku rozproszonym.

### Przedmiotowe efekty uczenia się

#### Wiedza

1. student ma zaawansowaną i pogłębioną wiedzę z zakresu architektury systemów komputerowych, systemów operacyjnych oraz technologii sieciowych – [K2st\_W1]
2. student ma zaawansowaną wiedzę szczegółową związaną z takimi zagadnieniami jak: analiza stanu bezpieczeństwa systemu, testy penetracyjne, zabezpieczanie systemu operacyjnego, aplikacji i infrastruktury sieciowej – [K2st\_W3]
3. student ma wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w informatyce w dziedzinie bezpieczeństwa systemów informatycznych – [K2st\_W4]
4. student ma zaawansowaną i szczegółową wiedzę o cyklu życia systemów informatycznych sprzętowych lub programowych, w kontekście zagrożeń bezpieczeństwa – [K2st\_W5]
5. student zna podstawowe metody, techniki i narzędzia stosowane przy rozwiązywaniu złożonych zadań inżynierskich z obszaru bezpieczeństwa systemów informatycznych – [K2st\_W6]

#### Umiejętności

1. student potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych – [K2st\_U6]
2. student potrafi - przy formułowaniu i rozwiązywaniu zadań inżynierskich – integrować wiedzę z różnych obszarów informatyki (a w razie potrzeby także wiedzę z innych dyscyplin naukowych) oraz zastosować podejście systemowe, uwzględniające także aspekty pozatechniczne – [K2st\_U5]
3. student potrafi zaproponować ulepszenia (usprawnienia) istniejących rozwiązań technicznych – [K2st\_U8]
4. student potrafi ocenić przydatność metod i narzędzi służących do rozwiązania zadania inżynierskiego, polegającego na budowie lub ocenie systemu informatycznego lub jego składowych pod kątem bezpieczeństwa, w tym dostrzec ograniczenia tych metod i narzędzi – [K2st\_U9]

#### Kompetencje społeczne

1. student rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe – [K2st\_K1]
2. student rozumie znaczenie wykorzystywania najnowszej wiedzy z zakresu informatyki w rozwiązywaniu problemów badawczych i praktycznych z dziedziny bezpieczeństwa informatycznego – [K2st\_K2]



### Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Ocena formująca:

a) w zakresie wykładów na podstawie:

- odpowiedzi na pytania dotyczące materiału omówionego na poprzednich wykładach,

b) w zakresie laboratoriów na podstawie:

- oceny bieżącego postępu realizacji zadań,

Ocena podsumowująca:

a) w zakresie wykładów na podstawie:

- oceny wiedzy i umiejętności wykazanych na zaliczeniu w formie testu wielokrotnego wyboru (20-25 pytań; próg zaliczeniowy: 50% punktów );

b) w zakresie laboratoriów na podstawie:

- oceny przygotowania studenta do poszczególnych sesji zajęć laboratoryjnych (sprawdzian "wejściowy") oraz ocenę umiejętności związanych z realizacją ćwiczeń laboratoryjnych,
- oceny wiedzy i umiejętności związanych z realizacją zadań laboratoryjnych poprzez 1 kolokwium w semestrze.

Dodatkowe punkty za aktywność podczas zajęć, a szczególnie za:

- omówienia dodatkowych aspektów zagadnienia,
- efektywność zastosowania zdobytej wiedzy podczas rozwiązywania zadanego problemu,
- umiejętność współpracy w ramach zespołu praktycznie realizującego zadanie szczegółowe w laboratorium,
- uwagi związane z udoskonaleniem materiałów dydaktycznych.

### Treści programowe

Program przedmiotu obejmuje następujące zagadnienia:

Formalne modele bezpieczeństwa, ze szczególnym uwzględnieniem modeli DAC, CAP, MAC, RBAC i ABAC. Bezpieczeństwo aplikacji w architekturze SOA (Service Oriented Architecture) i usług Web Services. Piaskownice systemowe (chroot) i kontenery (docker). Środowiska systemowe o podwyższonym bezpieczeństwie (RSBAC, AppArmor i SELinux). Rozproszone systemy uwierzytelniania i kontroli dostępu (Kerberos, Active Directory, Radius). Bezpieczna infrastruktura sieciowa, wieloplatformowe sieci VPN (IPsec i OpenVPN, Linux, Windows, Cisco IOS), konfiguracja i wykorzystanie usługi DNSsec. Zaawansowane zapory sieciowe i systemy IDS/IPS (NextGeneration Firewalls,



Snort/Suricata, ModSecurity). Testy penetracyjne systemu operacyjnego i usług aplikacyjnych (Kali Linux, DVWA, BurpSuite). Monitoring i analiza zabezpieczeń.

### Metody dydaktyczne

1. wykład: prezentacja multimedialna, pokaz multimedialny, demonstracja.
2. ćwiczenia laboratoryjne: demonstracja, dyskusja, warsztaty, ćwiczenia praktyczne, praca w zespole.

### Literatura

#### Podstawowa

1. William Stallings, Lawrie Brown, "Computer Security: Principles and Practice", IV ed., Pearson Education, 2018
2. Krzysztof Liderman, "Bezpieczeństwo informacyjne. Nowe wyzwania", PWN, 2017
3. Jie Wang, "Computer Network Security Theory and Practice, Higher Education Press, 2009

#### Uzupełniająca

1. Hakima Chaouchi, Maryline Laurent-Maknavicius, "Wireless and Mobile Networks Security", Wiley, 2009
2. Song Y.Yan, "Cybercryptography: Applicable Cryptography for Cyberspace Security", Springer, 2019
3. Chris Fry, Martin Nystrom, "Security Monitoring", O'Reilly, 2009
4. Bartosz Brodecki, Jerzy Brzeziński, Piotr Sasak, Michał Szychowiak, "Problemy bezpieczeństwa w architekturze SOA", w Damian Niemir, Maciej Stroiński, Jan Węglarz (Eds.): "Nauka w obliczu społeczeństwa cyfrowego", Ośrodek Wydawnictw Naukowych, 2010

### Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	125	5,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	60	2,5
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych, przygotowanie do kolokwium) <sup>1</sup>	65	2,5

<sup>1</sup> niepotrzebne skreślić lub dopisać inne czynności