

Protokoły kryptograficzne Sylabus zajęć

Informacje podstawowe

Kierunek studiów Informatyka Specjalność - Jednostka organizacyjna Wydział Matematyki i Informatyki Poziom studiów studia drugiego stopnia poinżynierskie Forma studiów studia stacjonarne Profil studiów profil ogólnoakademicki		Cykl dydaktyczny 2024/25 Kod zajęć 06INFS.44S.01040.24 Języki wykładowe polski Obligatoryjność Fakultatywny Blok zajęciowy Przedmioty specjalnościowe
Koordynator zajęć	Maciej Grześkowiak	
Prowadzący zajęcia	Maciej Grześkowiak, Marcin Gogolewski, Tomasz Kowalski	
Okres Semestr 3	Forma zajęć / liczba godzin / forma zaliczenia • Wykład: 15, Zaliczenie z oceną • Laboratorium: 15, Zaliczenie z oceną	Liczba punktów ECTS 3

Cele kształcenia dla zajęć

Kod	Cel
C1	Prezentacja współczesnych protokołów kryptograficznych.
C2	Umiejętność bezpiecznej konfiguracji środowiska kryptograficznego.
C3	Znajomość działania bezpiecznej komunikacji środowiska pracy.

Wymagania wstępne

Umiejętność programowania na poziomie inżyniera informatyki. Znajomość protokołu TCP/IP. Znajomość podstawowych protokołów kryptograficznych.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy - Student/ka:			
W1	zna współczesne protokoły kryptograficzne oraz zasady działania bezpiecznej komunikacji środowiska pracy.	INF_K4_W01, INF_K4_W02, INF_K4_W03, INF_K4_W04, INF_K4_W05	Kolokwium pisemne, Projekt, Zadania wykonywane podczas zajęć
Umiejętności - Student/ka:			
U1	potrafi bezpiecznie skonfigurować środowisko kryptograficzne.	INF_K4_U02, INF_K4_U03, INF_K4_U04, INF_K4_U06, INF_K4_U07	Kolokwium pisemne, Projekt, Zadania wykonywane podczas zajęć

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Infrastruktura Klucza Publicznego PKI.	W1, U1	Wykład, Laboratorium
2.	Certyfikaty X.509.	W1, U1	Wykład, Laboratorium
3.	Protokół TLS 1.3.	W1, U1	Wykład, Laboratorium
4.	Protokół WireGuard.	W1, U1	Wykład, Laboratorium
5.	Nieinteraktywny protokół zk-SNARK.	W1, U1	Wykład, Laboratorium

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień, Wykład konwersatoryjny, Dyskusja, Metoda ćwiczeniowa, Metoda projektu
Laboratorium	Praca z tekstem, Metoda ćwiczeniowa, Metoda laboratoryjna, Praca w grupach

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Warunkiem przystąpienia do zaliczenia wykładu jest uzyskanie zaliczenia z laboratorium. Na końcową ocenę składa się wynik uzyskany na egzaminie pisemnym. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.
Laboratorium	Zaliczenie laboratorium. Końcowa ocena składa się z następujących elementów: 1. projekt – 50%, 2. zadania wykonywane podczas zajęć – 50%. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.

Literatura

Obowiązkowa

1. W. Stallings, Cryptography and Network Security, Pearson 2020.
2. Jason A. Donenfeld, WireGuard: Next Generation Kernel Network Tunnel, Proceedings of the Network and Distributed System Security Symposium, NDSS 2017.

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykład	15
Laboratorium	15
Przygotowanie do zajęć	5
Czytanie wskazanej literatury	15
Przygotowanie projektu	15
Przygotowanie do zaliczenia	10
Łączny nakład pracy studenta	Liczba godzin 75
Liczba punktów ECTS	ECTS 3

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
INF_K4_U02	Absolwent/ka potrafi adaptować istniejące oraz tworzyć nowe metody informatyczne do rozwiązywania nieszablonowych problemów praktycznych i teoretycznych
INF_K4_U03	Absolwent/ka potrafi stosować zaawansowane metody budowy oprogramowania, rozstrzyga o ich przydatności, w tym podejmuje decyzje dotyczące wyboru technik prowadzących do otrzymania oprogramowania wysokiej jakości
INF_K4_U04	Absolwent/ka potrafi projektować i implementować systemy informatyczne o różnej złożoności i różnych architekturach
INF_K4_U06	Absolwent/ka potrafi rozwiązywać złożone problemy z wybranych obszarów informatyki oraz proponować nowe algorytmy, narzędzia i metody wykorzystując odpowiednio dobrane źródła, które poddaje krytycznej analizie, syntezie i twórczej interpretacji
INF_K4_U07	Absolwent/ka potrafi wyrażać krytyczne opinie na temat architektury oraz użyteczności wykorzystywanych systemów informatycznych
INF_K4_W01	Absolwent/ka zna i rozumie w pogłębionym stopniu pojęcia z działów matematyki niezbędne do rozwiązywania zaawansowanych problemów w informatyce
INF_K4_W02	Absolwent/ka zna i rozumie współczesny stan badań i tendencje rozwojowe w wiodących obszarach informatyki
INF_K4_W03	Absolwent/ka zna i rozumie w pogłębionym stopniu współczesne metody, narzędzia i technologie informatyczne właściwe dla wybranych obszarów zastosowań niezbędne przy budowie złożonych systemów informatycznych oraz przy prowadzeniu prac badawczo-rozwojowych
INF_K4_W04	Absolwent/ka zna i rozumie zasady rozwiązywania problemów z wykorzystaniem zaawansowanych algorytmów i metod informatycznych
INF_K4_W05	Absolwent/ka zna i rozumie budowę oraz cykl życia przykładowych systemów informatycznych wykorzystywanych w praktyce oraz zna ograniczenia złożonych systemów informatycznych