



Buletin informativ

August 2025

Despre programa de Securitate Cibernetică

Apariția tot mai mare a amenințărilor cibernetice și dependența tot mai mare de tehnologiile digitale fac imperativă implementarea unei programe de învățământ robuste în domeniul securității cibernetice. Cooperarea dintre universități este o oportunitate excelentă pentru îmbunătățirea calității educației, crearea de programe de studiu inovatoare și îmbogățirea experienței studenților. Pentru a obține cele mai bune rezultate, este important să se aleagă metodologiile și strategiile potrivite. Vom folosi hMOOC-uri, educație federată și metodologii de învățare bazate pe provocări pentru a implementa programa digitală de securitate cibernetică. Programa propusă de securitate cibernetică își propune să familiarizeze cursanții cu disciplinele cheie: Fundamentele securității cibernetice, Managementul identității și accesului, Atacuri și apărare cibernetică și Managementul securității cibernetice. Scurtă descriere a cursurilor asociate și contextualizarea lor în scenarii de securitate cibernetică:

Fundamentele securității cibernetice

Securitatea cibernetică este un domeniu complex care implică o combinație de concepte tehnice și teoretice. Cursul „Fundamentele securității cibernetice” oferă o imagine de ansamblu cuprinzătoare a problemelor de securitate informatică și a informațiilor, conceptele fundamentale de securitate cibernetică, principiile, modelele formale de securitate, metodele hardware și software de securitate a tehnologiei informației și standardele de abilitate, precum și dezvoltarea abilităților de aplicare a acestora. Acesta acoperă diverse subiecte, inclusiv probleme de securitate IT, modele de securitate a informațiilor, criptografie și metode securizate de codificare a informațiilor, standarde și specificații de securitate a informațiilor și IT, securitatea hardware, gestionarea identității, mecanismele de securitate a sistemului de operare și securitatea sistemului de fișiere. Cursul este conceput pentru a dota studenții cu cunoștințele și abilitățile necesare pentru a aborda provocările în continuă evoluție în materie de securitate cibernetică cu care se confruntă organizațiile din prezent.

Managementul identității și accesului

Cursul „Managementul identității și accesului” este o componentă cheie a curriculumului de securitate cibernetică, abordând nevoia tot mai mare de metode sigure și eficiente de gestionare a identităților digitale în organizațiile contemporane. Acest curs se concentrează pe principiile, tehnologiile și practicile necesare pentru a proteja accesul la activele digitale critice, asigurând confidențialitatea, integritatea și disponibilitatea. Studenții vor explora ciclul de viață al gestionării identității, inclusiv crearea, verificarea și dezafectarea identității, alături de mecanisme moderne de control al accesului. Cursul pune accent atât pe fundamentele teoretice, cât și pe aplicațiile practice.



Atacuri cibernetice și apărări cibernetice: instrumente și metode

„CyberAttacks și CyberDefenses” oferă o înțelegere aprofundată a amenințărilor cibernetice și a măsurilor defensive. Începe cu o introducere în diverse atacuri și amenințări cibernetice, explicând „CyberKillChain” și metodologia MITRE ATT&CK pentru analiza tacticilor de atac. Cursul acoperă tipurile de programe malware și conceptul de Apărare în Adâncime, punând accent pe strategiile de securitate multistratificate. Studenții învață despre standardele de Securitate Cibernetică și tehnicile de hacking etc, inclusiv OWASP TOP-10 și vulnerabilități comune, cum ar fi „SQL injection” și XSS. Cursul aprofundează, de asemenea, testarea de penetrare software, Red Teaming, Phishing as a Service și securitatea WiFi. În plus, acoperă Securitatea Rețelei și Apărarea Perimetrală, concentrându-se pe securitatea de Nivel 2, Firewall-urile de Generație Următoare (NGFW), sistemele IDS/IPS și tehnologiile VPN, cum ar fi IPsec și OpenVPN. Sunt explorate aspecte cheie ale monitorizării sistemului pentru detectarea amenințărilor, alături de strategii pentru gestionarea incidentelor de securitate cibernetică. Cursul se încheie cu o prezentare generală a Operațiunilor Cibernetice și a Centrelor de Operațiuni de Securitate (SOC), împreună cu soluțiile SIEM/SOAR și rolul tot mai mare al inteligenței artificiale în securitatea cibernetică pentru a îmbunătăți detectarea amenințărilor și răspunsurile automate.

Managementul Securității Cibernetică

Acest curs va oferi studenților o prezentare generală a principiilor de management al securității cibernetice. Participanții vor învăța cum să asigure confidențialitatea, integritatea și disponibilitatea activelor securizate, să identifice riscurile de securitate, cerințele și contramăsurile care atenuează aceste riscuri și să implementeze cerințele de securitate. Cursul se bazează pe modelul de domeniu bine stabilit pentru managementul riscurilor de securitate și pe principiile securității bazate pe modele. Managementul securității va fi ilustrat prin aplicarea standardelor și modelelor de management al securității. Folosind abordarea învățării bazate pe provocări, participanții vor explora provocările managementului securității în sistemele conștiente de procesele de afaceri, infrastructura inteligentă, sistemele distribuite, sistemele conștiente de risc și pregătite pentru investigații criminalistice și sistemele securizate de management al identității.

COORDONATOR DE PROIECT



PARTENERI DE PROIECT



<https://www.cyberchallenge-erasmus.eu/>

Universitatea de Tehnologie din Kaunas
Facultatea de Informatică, strada
Studentilor nr. 50, Kaunas, Lituania



Funded by
the European Union



CYBERCHALLENGE
Challenges Solving in
Cybersecurity Study Program

CYBERCHALLENGE - Rezolvarea Provocărilor în Securitatea Cibernetică - Program de Studii Nr. 2024-1-LT01-KA220-HED-000252504

