

FIȘA DISCIPLINEI

Securitatea aplicațiilor pentru dispozitive mobile și IoT

Anul universitar 2026-2027

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Babeș-Bolyai
1.2. Facultatea	Facultatea de Matematică și Informatică
1.3. Departamentul	Departamentul de Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Master
1.6. Programul de studii / Calificarea	Cybersecurity
1.7. Forma de învățământ	Cu frecvență

2. Date despre disciplină

2.1. Denumirea disciplinei	Securitatea aplicațiilor pentru dispozitive mobile și IoT			Codul disciplinei	MME8209
2.2. Titularul activităților de curs	Dan Cojocar, PhD				
2.3. Titularul activităților de seminar	Dan Cojocar, PhD				
2.4. Anul de studiu	2	2.5. Semestrul	3	2.6. Tipul de evaluare	Examen
2.7. Regimul disciplinei	Obligatoriu			2.8. Tipul disciplinei	Disciplină de specializare (DS)

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1. Număr de ore pe săptămână	4	din care: 3.2 curs	2	3.3. seminar/ laborator/ proiect	2
3.4. Total ore din planul de învățământ	56	din care: 3.5 curs	28	3.6. seminar/laborator	28
Distribuția fondului de timp pentru studiul individual (SI) și activități de autoinstruire (AI)					ore
Studiul după manual, suport de curs, bibliografie și notițe (AI)					30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					20
Pregătire seminar/ laboratoare/ proiecte, teme, referate, portofolii și eseuri					24
Tutoriat (consiliere profesională)					10
Examinări					10
Alte activități					0
3.7. Total ore studiu individual (SI) și activități de autoinstruire (AI)					94
3.8. Total ore pe semestru					150
3.9. Numărul de credite					6

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	Programarea aplicațiilor mobile, Fundamentele programării (ex: Java/Kotlin/Swift, Python), Programare orientată pe obiecte, Rețele de calculatoare, Sisteme de operare.
4.2. de competențe	Cunoștințe de bază de programare, înțelegerea arhitecturilor client-server, familiaritate cu sisteme de operare comune (Linux, Windows, Android, iOS).

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Sală de curs cu proiector și acces la internet.
5.2. de desfășurare a seminarului/ laboratorului	<ul style="list-style-type: none">Laborator cu calculatoare (Windows, Linux sau macOS).Acces la internet pentru descărcarea uneltelor și accesarea resurselor.Posibilitatea de a instala software (emulatoare, unelte de securitate, IDE-uri).

6.1. Competențele dobândite în urma absolvirii programului de studii (se preiau din planul de învățământ)¹

Competențe profesionale	
Codul competenței	Competență

¹Se vor prelua din Planul de învățământ al programului de studii acele competențe profesionale și/sau transversale la dezvoltarea cărora contribuie disciplina pentru care se elaborează fișa disciplinei. Pentru fiecare competență se va prelua întregul enunț, inclusiv codul competenței, cu formularea care apare în planul de învățământ, fără modificări. Dacă nu se preia nici o competență din oricare din cele două categorii, se șterge linia din tabel aferentă acelei categorii.

CP3	Utilizarea nuanțată și pertinentă a criteriilor și metodelor de verificare, validare și evaluare a soluțiilor software pentru a asigura securitatea acestora.
CP4	Capacitate avansată de analiză, proiectare și construcție securizată a sistemelor informatice, folosind o gamă variată de platforme hardware și software, limbaje și medii de programare și instrumente de modelare, verificare și validare.
CP7	Înșușirea modului de funcționare a principalelor forme de aplicații malware și a principalelor forme de atacuri în Internet, precum și a metodelor de protecție împotriva acestora.
Competențe transversale	
Codul competenței	Competență
CT1	Abilități de comunicare profesională: descrierea clară, concisă, verbală și în scris a rezultatelor profesionale.
CT2	Comportarea onorabilă, etică, respectarea deontologiei profesionale.
CT3	Aplicarea regulilor de muncă organizată și eficientă, responsabilitate și seriozitate față de munca depusă atât individual cât și în echipă.

6.2. Rezultatele învățării specifice programului de studii (se preiau din planul de învățământ)²

Rezultatele învățării vizate prin disciplină		
Codul competenței	Cunoștințe și înțelegere (Knowledge and understanding)	Abilități academice specifice (Specific academic skills)
CP4	Studentul/absolventul dobândește cunoștințe despre cele mai grave tipuri de vulnerabilități în domeniu, precum și despre măsurile de prevenție a acestor vulnerabilități. Studentul/absolventul cunoaște conceptele de baza ale programării aplicațiilor pentru dispozitive mobile și a modelelor de securitate folosite în cadrul unor asemenea aplicații.	Studentul/absolventul este capabil să înțeleagă tehnicile clasice de analiză statică utilizate pentru analiza și verificarea securității programelor. Studentul/absolventul are capacitatea de a evalua caracteristicile de securitate ale unei aplicații software la nivelul codului sursă.

7. Rezultatele învățării specifice disciplinei (derivate de fiecare titular de disciplină din grila competențelor și a rezultatelor învățării la nivel de program de studii)

Cunoștințe și înțelegere (Knowledge and understanding)
<ul style="list-style-type: none"> • Studentul/absolventul cunoaște conceptele de baza ale programării aplicațiilor pentru dispozitive mobile și a modelelor de securitate folosite în cadrul unor asemenea aplicații. • Studentul/absolventul are cunoștințe despre cele mai populare tipuri de aplicații malware, despre arhitectura și modul de funcționare a acestora. • Studentul/absolventul dobândește cunoștințe despre cele mai grave tipuri de vulnerabilități în domeniu, precum și despre măsurile de prevenție a acestor vulnerabilități.
Abilități academice specifice (Specific academic skills)
<ul style="list-style-type: none"> • Studentul/absolventul este capabil să dezvolte sisteme software securizate. • Studentul/absolventul este capabil să identifice posibilele probleme de securitate în sistemele software. • Studentul/absolventul dobândește abilitățile de a utiliza diverse instrumente în procesul de testare pentru identificarea vulnerabilităților software.

8. Conținuturi

8.1. Curs	Metode de predare - învățare	Observații³
1. Securitate mobilă: amenințări, apărări și realități moderne <ul style="list-style-type: none"> • Principiile securității mobile (CIA) • Taxonomia amenințărilor (malware, phishing, atacuri de rețea) • De ce mobilul e diferit; evaluarea riscului 	Expunere interactivă, Explicație, Conversație, Exemple, Demonstratie didactică	
2. Elementul uman: inginerie socială și securitate centrată pe utilizator <ul style="list-style-type: none"> • Psihologia ingineriei sociale și a înșelăciunii • Comportamentul și conștientizarea utilizatorului 		

²Se menționează rezultatele învățării specifice programului de studiu la dezvoltarea cărora contribuie disciplina pentru care se elaborează fișa. Enunțurile, preluate fără modificări din Planul de învățământ în funcție de tipul disciplinei (DF/DS/DC) se trec în dreptul competenței asociate.

³De exemplu aspecte organizatorice, recomandări pentru studenți, aspecte specifice legate de curs/seminar cum ar fi invitarea unor practicieni în domeniu etc.

<ul style="list-style-type: none"> • Gestionarea permisiunilor și a confidențialității 		
<p>3. Securizarea ecosistemului de aplicații</p> <ul style="list-style-type: none"> • Grădina închisă Apple vs modelul deschis Google Play • Verificarea (vetting) aplicațiilor • Riscurile sideloading-ului 		
<p>4. Securitatea practică a aplicațiilor mobile</p> <ul style="list-style-type: none"> • Strategiile atacatorului • OWASP Mobile Top 10 (2024) • Credențiale și securitatea lanțului de aprovizionare 		
<p>5. Cursa înarmării împotriva malware-ului mobil</p> <ul style="list-style-type: none"> • Malware modern: spyware, ransomware, troieni • Detecție bazată pe semnături vs comportament • ML pentru detecția malware 		
<p>6. Managementul identității și accesului (IAM) în lumea mobilă</p> <ul style="list-style-type: none"> • Mediul mobil ostil și dilema UX • Sesiuni always-on • Ecosisteme diverse 		
<p>7. Confidențialitate mobilă avansată</p> <ul style="list-style-type: none"> • Economia datelor și actorii ei • Trackere în codul aplicațiilor • Limitarea urmăririi 		
<p>8. Dezvoltarea unei strategii corporative de securitate mobilă</p> <ul style="list-style-type: none"> • Imperativul strategic și părțile interesate • Costul lipsei unei strategii • BYOD și MDM 		
<p>9. Criminalistică digitală mobilă: achiziția și analiza probelor</p> <ul style="list-style-type: none"> • Obiectivele criminalisticii mobile • Telefonul ca martor principal • Achiziția și analiza probelor 		
<p>10. Criptografie aplicată pentru dispozitive mobile și IoT</p> <ul style="list-style-type: none"> • Fundamente criptografice • Criptare simetrică și moduri de operare • De ce ECB este periculos 		
<p>11. Nexusul de securitate Mobile-IoT</p> <ul style="list-style-type: none"> • Planul de control mobil pentru IoT • IoT centrat pe aplicație • Modele de arhitectură: direct, releu cloud, hibrid 		
<p>12. Aplicații specializate și viitorul securității mobile</p> <ul style="list-style-type: none"> • Studiu de caz: mobil în aplicarea legii (CJIS) • Credențiale derivate • Model de amenințare: dispozitivul pierdut 		
<p>13. Testare de penetrare mobilă și IoT (practic)</p> <ul style="list-style-type: none"> • Construirea unui laborator de pentest (emulator vs dispozitiv) • Cerința de root • Analiză statică (SAST) și unelte esențiale 		
<p>14. Recapitulare pentru examen și discuții</p> <ul style="list-style-type: none"> • Recapitularea temelor cheie • Structura și logistica examenului • Prezentarea proiectelor finale 	Expunere interactivă, Explicație, Conversație, Discuții evaluare.	
<ul style="list-style-type: none"> • “Dwivedi, H., Clark, C., & Thiel, D. V. (2010). Mobile application security (Vol. 275). New York: McGraw-Hill.” • “Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. International Journal of Information Management, 52, 102063.” 		

<ul style="list-style-type: none"> • “Russell, B., & Van Duren, D. (2016). Practical internet of things security. Packt Publishing Ltd.” • “Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020, May). Mobile application security penetration testing based on OWASP. In IOP Conference Series: Materials Science and Engineering (Vol. 846, No. 1, p. 012036). IOP Publishing” • OWASP Internet of Things Top 10 		
8.2. Seminar / laborator	Metode de predare - învățare	Observații
1. [Introducere și configurarea proiectului] Discuții despre temele cursului, brainstorming idei de proiect. Configurarea uneltelor de dezvoltare și securitate.	Exposure: description, discussion. Evaluation.	Ședințele de seminar/proiect se desfășoară pe parcursul a 2 ore, o dată la două săptămâni.
2. [Propunerea proiectului și modelarea amenințărilor] Studenții își prezintă ideile de proiect, scopul și arhitectura inițială. Realizarea unui exercițiu de modelare a amenințărilor (ex: STRIDE).		
3. [Analiza vulnerabilităților 1] Laborator practic despre analiza statică (SAST) și ingineria inversă a aplicațiilor Android/iOS.		
4. [Analiza vulnerabilităților 2] Laborator practic despre analiza dinamică (DAST) și interceptarea traficului de rețea (ex: Burp Suite, mitmproxy).		
5. [Implementare sigură] Verificarea progresului proiectului. Concentrare pe implementarea controalelor de securitate (ex: stocare sigură, autentificare corectă, validarea intrărilor).		
6. [Pre-prezentări proiecte] Demonstrații ale proiectelor aproape finalizate și revizuirea codului de către colegi/instructor. Sesiune de feedback.		
7. [Prezentări finale și predarea proiectelor] Evaluarea finală a proiectului. Demonstrarea și apărarea măsurilor de securitate implementate.		
<ul style="list-style-type: none"> • “Dwivedi, H., Clark, C., & Thiel, D. V. (2010). Mobile application security (Vol. 275). New York: McGraw-Hill.” • “Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. International Journal of Information Management, 52, 102063.” • “Russell, B., & Van Duren, D. (2016). Practical internet of things security. Packt Publishing Ltd.” • “Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020, May). Mobile application security penetration testing based on OWASP. In IOP Conference Series: Materials Science and Engineering (Vol. 846, No. 1, p. 012036). IOP Publishing” • OWASP Internet of Things Top 10 		

9. Evaluare

Tip activitate	9.1. Criterii de evaluare ⁴	9.2. Metode de evaluare ⁵	9.3. Pondere din nota finală
9.4 Curs	<ul style="list-style-type: none"> • Examen scris final. 	<ul style="list-style-type: none"> • Examen scris care acoperă conceptele teoretice din toate prelegerile. 	<ul style="list-style-type: none"> • 40%
9.5 Seminar/laborator	<ul style="list-style-type: none"> • Proiect de semestru. • Activități practice de laborator și verificări ale etapelor (milestones). 	<ul style="list-style-type: none"> • Evaluarea etapelor proiectului, prezentarea finală și codul/raportul predat. • Evaluarea abilităților practice în timpul sesiunilor de laborator. 	<ul style="list-style-type: none"> • 60%
9.6. Standard minim de promovare			
<ul style="list-style-type: none"> • Participarea la minimum 75% din ședințele de seminar/proiect. • Obținerea unei note de cel puțin 5 (pe o scară de la 1 la 10) la examenul scris final. • Obținerea unei note de cel puțin 5 (pe o scară de la 1 la 10) la activitățile de proiect/seminar pe parcursul semestrului. 			

⁴Criteriile de evaluare trebuie să reflecte direct rezultatele învățării vizate la nivel de program de studii, respectiv la nivel de disciplină. Mai concret, se evaluează achizițiile de învățare menționate în rezultatele anticipate ale învățării.

⁵Se recomandă stabilirea atât a metodelor de evaluare finală, cât și a strategiei de evaluare pe parcurs.

- Nota finală agregată trebuie să fie de cel puțin 5.

10. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)⁶

	<input type="checkbox"/>	Eticheta generală pentru Dezvoltare durabilă						
1 FĂRĂ SĂRĂCIE 	2 FOAMETE „ZERO” 	3 SĂNĂTATE ȘI BUNĂSTĂRE 	4 EDUCATIE DE CALITATE 	5 EGALITATE DE GEN 	6 APĂ CURATĂ ȘI SANITATIE 	7 ENERGIE CURATĂ ȘI LA PREȚURI ACCESIBILE 	8 MUNCĂ DECENTĂ ȘI CREȘTERE ECONOMICĂ 	9 INDUSTRIE, INOVATIE ȘI INFRASTRUCTURĂ 
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10 INEGALITĂȚI REDUSE 	11 ORAȘE ȘI COMUNITĂȚI DURABILE 	12 CONSUM ȘI PRODUCȚIE RESPONSABILE 	13 ACȚIUNE CLIMATICĂ 	14 VIAȚA ACVATICĂ 	15 VIAȚA TERESTRĂ 	16 PACE, JUSTITIE ȘI INSTITUȚII EFICIENTE 	17 PARTENERIATE PENTRU REALIZAREA OBIECTIVELOR 	Nu se aplică nicio etichetă
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Data completării:

Semnătura titularului de curs,
Dan Cojocar, PhD

Semnătura titularului de seminar,
Dan Cojocar, PhD

Data avizării în departament:

Semnătura directorului de departament,
Adrian Sterca, PhD

⁶Selecțai o singură etichetă, cea care, în conformitate cu Procedura de aplicare a etichetelor ODD în procesul academic, se potrivește cel mai bine disciplinei. Dacă disciplina tratează tema dezvoltării durabile la modul general atunci se poate alocă eticheta generală de Dezvoltare durabilă. Dacă niciuna dintre etichete nu descrie disciplina, selecțai ultima opțiune: „Nu se aplică nicio etichetă“.