

FIȘA DISCIPLINEI
Introducere în securitate cibernetică

Anul universitar 2026-2027

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Babeș-Bolyai din Cluj Napoca
1.2. Facultatea	Istorie și Filosofie
1.3. Departamentul	Studii Internaționale și Istorie Contemporană
1.4. Domeniul de studii	Studii de Securitate
1.5. Ciclul de studii	Licență
1.6. Programul de studii / Calificarea	Studii de securitate
1.7. Forma de învățământ	Zi

2. Date despre disciplină

2.1. Denumirea disciplinei	Introducere în securitate cibernetică			Codul disciplinei	HLE3318
2.2. Titularul activităților de curs	Iulian-Florentin Popa				
2.3. Titularul activităților de seminar					
2.4. Anul de studiu	2	2.5. Semestrul	3	2.6. Tipul de evaluare	Examen
2.7. Regimul disciplinei	Opțional		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)					25
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					20
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii și eseuri					15
Tutoriat (consiliere profesională)					1
Examinări					4
Alte activități					4
3.7. Total ore studiu individual (SI) și activități de autoinstruire (AI)				69	
3.8. Total ore pe semestru				125	
3.9. Numărul de credite				5	

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	Nu este cazul
4.2. de competențe	Sunt necesare competențe elementare de operare a instrumentelor și echipamentelor TIC

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Nu este cazul
5.2. de desfășurare a seminarului/ laboratorului	Tablă inteligentă sau videoproiector, stații de lucru (ex. PC, laptop)

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

¹ Se 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.

Competențe profesionale	
Codul competenței	Competență
CP1	Analiza mediului de securitate național și internațional
CP3	Evaluarea riscurilor și vulnerabilităților de securitate
CP11	Consiliere strategică și formularea de recomandări în domeniul securității
Competențe transversale	
Codul competenței	Competență
CT4	Etică profesională și responsabilitate socială
CT5	Autonomie decizională și managementul responsabil al sarcinilor

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)
CP1	1. C11: Studentul/Absolventul explică concepte-cheie din studiile strategice și securitatea internațională (amenințări hibride, descurajare, securitate umană) relevante pentru evaluări de securitate.	1. Studentul/Absolventul elaborează evaluări de securitate și scenarii prospective pe baza indicatorilor geopolitici și a analizelor de risc.
CP3	2. C12: Studentul/Absolventul descrie cadre de management al riscului (identificare–analiză–evaluare–tratare–monitorizare) aplicabile securității fizice și organizaționale.	2. A9: Studentul/Absolventul aplică instrumente de evaluare a vulnerabilităților și propune măsuri de reducere a riscului (mitigare) adaptate contextului organizațional.
CP11	Studentul/Absolventul descrie metodele de analiză strategică, evaluare a riscurilor și fundamentare a procesului decizional utilizate în domeniul securității.	A13: Studentul/Absolventul formulează recomandări de securitate și planuri de măsuri pentru clienți/organizații, utilizând date și evaluări analitice.
CT4	Studentul/Absolventul explică principiile eticii profesionale, integrității academice și responsabilității sociale în activitățile profesionale și instituționale.	A3: Studentul/Absolventul aplică principiile etice fundamentale și legislația în domeniul cercetării științifice, inclusiv în ceea ce privește aspectele legate de integritatea cercetării. Efectuează, revizuieste sau raportează cercetări, evitând comportamentele greșite, cum ar fi fabricarea, falsificarea și plagiatul. A5: Studentul/Absolventul dezvoltă și demonstrează cunoașterea aprofundată și înțelegerea complexă a unui anumit domeniu de cercetare, inclusiv a cercetării responsabile, a principiilor etice și de integritate științifică în materie de cercetare, respectul vieții private și a cerințelor RGPD, legate de activitățile de cercetare dintr-o anumită disciplină.
CT5	Studentul/Absolventul descrie metode și instrumente de organizare a activităților, management al timpului și prioritizare a sarcinilor în contexte academice și organizaționale.	Studentul/Absolventul gestionează în mod autonom activitățile academice și sarcinile individuale, respectând termenele, standardele etice și cerințele specifice mediului universitar.

7. Rezultatele învățării specifice disciplinei

Cunoștințe și înțelegere (Knowledge and understanding)
--

² Se 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.

1. Studentul/Absolventul explică principiile fundamentale ale securității cibernetice, tipologiile amenințărilor informatice (malware, phishing, ransomware, atacuri APT) și impactul acestora asupra securității organizaționale și naționale.
2. Studentul/Absolventul descrie mecanismele de protecție a infrastructurilor și terminalelor cibernetice, incluzând controlul accesului, managementul identității, criptarea datelor, securitatea rețelelor și managementul incidentelor de securitate cibernetică.
3. Studentul/Absolventul înțelege rolul tehnologiilor de securitate cibernetică și al instrumentelor pentru detectarea, analiza și prevenirea amenințărilor cibernetice în contexte instituționale și internaționale.
4. Studentul/Absolventul descrie etapele răspunsului la incidente cibernetice și ale managementului crizelor digitale, incluzând identificarea incidentelor, analiza impactului, comunicarea de criză și măsurile de recuperare operațională.
Abilități academice specifice (Specific academic skills)
1. Studentul/Absolventul aplică metodologia de analiză a riscurilor cibernetice, a vulnerabilităților și pentru evaluarea impactului amenințărilor asupra sistemelor informatice și infrastructurilor critice.
2. Studentul/Absolventul descrie și utilizează concepte și teorii specifice securității cibernetice pentru analiza fenomenelor din sfera securității cibernetice.
3. Studentul/Absolventul realizează activități de documentare academică și analiză interdisciplinară utilizând surse științifice, baze de date și resurse digitale relevante pentru domeniul securității cibernetice.

8. Conținuturi

8.1 Curs	Metode de predare - învățare	Observații ³
Fundamentele securității cibernetice. Dimensiunea cibernetică a securității	Prelegerea, dezbateră	
Terminologie de specialitate. Riscuri, amenințări și vulnerabilități de securitate cibernetică	Prelegerea, dezbateră	
Triada CIA și cubul securității cibernetice	Prelegerea, dezbateră, studiul de caz	
Securitatea cibernetică a organizațiilor. Cerințe minime de securitate cibernetică a organizațiilor	Prelegerea, dezbateră	
Securitatea cibernetică a dispozitivelor mobile	Prelegerea, dezbateră	
Securitatea fizică a terminalelor și infrastructurilor cibernetice	Prelegerea, dezbateră	
Securitatea cibernetică a resurselor umane. Cerințe de securitate	Prelegerea, dezbateră	
Răspunsul la incidente de securitate cibernetică	Prelegerea, dezbateră, studiul de caz	
Organizarea răspunsului la incidente de securitate cibernetică	Prelegerea, dezbateră, studiul de caz	
Standarde de securitate cibernetică	Prelegerea, dezbateră, studiul de caz	
Securitatea cibernetică a dispozitivelor mobile	Prelegerea, dezbateră, studiul de caz	
Securitatea cibernetică a dispozitivelor IoT	Prelegerea, dezbateră, studiul de caz	
Inteligența artificială generativă și modelele lingvistice de mari dimensiuni (LLM) în securitatea cibernetică. Securitate cibernetică asistată de AI	Prelegerea, dezbateră, studiul de caz	
Strategia de securitate cibernetică a României	Prelegerea, dezbateră, studiul de caz	
Ozkaya, Erdal, <i>Cybersecurity: The Beginner's Guide. A Comprehensive Guide to Getting Started in Cybersecurity</i> , Birmingham, Packt Publishing, 2019. McDonough, Bart, <i>Cyber Smart: Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals</i> , Indianapolis, Wiley, 2019. Blau, Alex et al., <i>Cybersecurity</i> , Boston, Massachusetts, Harvard Business Review Press, 2019.		

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

Brooks, Charles J., Craig, Philip, Short, Donald, Somerset, Christopher, *Cybersecurity Essentials*, Hoboken, New Jersey, John Wiley & Sons, 2018.

Sanger, David E., *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, New York, Crown Publishing Group, 2018.

Directoratul Național pentru Securitate Cibernetică (DNSC), *Ghid de securitate cibernetică*, București, 2021, disponibil la: Ghid de securitate cibernetică 2021.

Serviciul Român de Informații (SRI), *Ghid de bune practici de securitate cibernetică*, București, 2020, disponibil la: Ghid de bune practici de securitate cibernetică.

Fortinet, *AI In Cybersecurity: Key Benefits, Defense Strategies, & Future Trends*, disponibil la: fortinet.com.

H O T Ă R Ă R E privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027, disponibil la <https://securitatea-cibernetica.ro/documente/Strategia-de-securitate-cibernetica-a-Romaniei.pdf>.

CIS Critical Security Controls v 8.1, disponibil la <https://learn.cisecurity.org/cis-controls-download>

8.2 Seminar / laborator	Metode de predare - învățare	Observații
Fundamentele securității cibernetică.	Prelegerea, dezbateră	
Dimensiunea cibernetică a securității		
Terminologie de specialitate. Riscuri, amenințări și vulnerabilități de securitate cibernetică	Prelegerea, dezbateră	
Triada CIA și cubul securității cibernetică	Prelegerea, dezbateră, studiul de caz	
Securitatea cibernetică a organizațiilor. Cerințe minime de securitate cibernetică a organizațiilor	Prelegerea, dezbateră	
Securitatea cibernetică a dispozitivelor mobile	Prelegerea, dezbateră	
Securitatea fizică a terminalelor și infrastructurilor cibernetică	Prelegerea, dezbateră	
Securitatea cibernetică a resurselor umane. Cerințe de securitate	Prelegerea, dezbateră	
Răspunsul la incidente de securitate cibernetică	Prelegerea, dezbateră, studiul de caz	
Organizarea răspunsului la incidente de securitate cibernetică	Prelegerea, dezbateră, studiul de caz	
Standarde de securitate cibernetică	Prelegerea, dezbateră, studiul de caz	
Securitatea cibernetică a dispozitivelor mobile	Prelegerea, dezbateră, studiul de caz	
Securitatea cibernetică a dispozitivelor IoT	Prelegerea, dezbateră, studiul de caz	
Inteligența artificială generativă și modelele lingvistice de mari dimensiuni (LLM) în securitatea cibernetică	Prelegerea, dezbateră, studiul de caz	
Strategia de securitate cibernetică a României	Prelegerea, dezbateră, studiul de caz	

Ozkaya, Erdal, *Cybersecurity: The Beginner's Guide. A Comprehensive Guide to Getting Started in Cybersecurity*, Birmingham, Packt Publishing, 2019.

McDonough, Bart, *Cyber Smart: Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals*, Indianapolis, Wiley, 2019.

Blau, Alex et al., *Cybersecurity*, Boston, Massachusetts, Harvard Business Review Press, 2019.

Brooks, Charles J., Craig, Philip, Short, Donald, Somerset, Christopher, *Cybersecurity Essentials*, Hoboken, New Jersey, John Wiley & Sons, 2018.

Sanger, David E., *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, New York, Crown Publishing Group, 2018.

Directoratul Național pentru Securitate Cibernetică (DNSC), *Ghid de securitate cibernetică*, București, 2021, disponibil la: Ghid de securitate cibernetică 2021.

Serviciul Român de Informații (SRI), *Ghid de bune practici de securitate cibernetică*, București, 2020, disponibil la: Ghid de bune practici de securitate cibernetică.

Fortinet, *AI In Cybersecurity: Key Benefits, Defense Strategies, & Future Trends*, disponibil la: fortinet.com.

H O T Ă R Ă R E privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027, disponibil la <https://securitatea-cibernetica.ro/documente/Strategia-de-securitate-cibernetica-a-Romaniei.pdf>
 CIS Critical Security Controls v 8.1, disponibil la <https://learn.cisecurity.org/cis-controls-download>

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	Gradul de însușire a conceptelor fundamentale de securitate cibernetică; capacitatea de analiză și interpretare a amenințărilor și vulnerabilităților cibernetică; utilizarea corectă a terminologiei de specialitate	Examen	50%
9.5 Seminar/laborator	Capacitatea de aplicare a noțiunilor teoretice în platformele și exercițiile de securitate cibernetică; înțelegerea mecanismelor de protecție și răspuns la incidente	Testare CISCO	25%
	Capacitatea de analiză critică și rezolvare a unor scenarii de securitate cibernetică; argumentarea soluțiilor propuse și utilizarea surselor academice și tehnice relevante	Exercițiu teoretic-aplicativ	25%
9.6 Standard minim de promovare			
Pentru promovarea disciplinei, studentul trebuie să obțină minimum nota 5 (cinci). Studentul trebuie să demonstreze cunoștințe de bază privind conceptele fundamentale ale securității cibernetică, tipologiile amenințărilor, principiile securității cibernetică și mijloacele de utilizare responsabilă a tehnologiilor digitale.			

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

  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 SANITATE	7 ENERGIE CURATĂ ȘI LA PREȚURI ACCESIBILE	8 MUNCĂ DECENTĂ ȘI CREȘTERE ECONOMICĂ	9 INDUSTRIE, INOVAȚIE ȘI INFRASTRUCTURĂ
								
								Nu se aplică nici o etichetă
								

⁴ Criteriile 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.

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

⁶ Selectați 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 (de ex. prin prezentarea/introducerea cadrului general al dezvoltării durabile etc.) atunci se poate alocă eticheta generală de Dezvoltare Durabilă. Dacă niciuna dintre etichete nu descrie disciplina, selectați ultima opțiune: „Nu se aplică nici o etichetă”.

Data completării:

...

Semnătura titularului de curs

.....

Semnătura titularului de seminar

.....