MD-2068, CHIŞINĂU, STR. STUDENŢILOR, 9/7, TEL: 022 50-99-63, www.utm.md

TEHNOLOGII ALE SECURITĂȚII INFORMAȚIONALE

1. Date despre disciplină

Facultatea	**FACULTATEA CALCULATOARE, INFORMATICĂ ȘI MICROELECTRONICĂ**				
Departamentul	**INGINERIA SOFTWARE ȘI AUTOMATICĂ**				
Ciclul de studii	Studii superioare de licenţă, ciclul I				
Programul de studii	Tehnologia informației, Securitatea informațională				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opţionalitate**	**Credite ECTS**
Anul II *(învăţământ cu frecvenţă)*	IV	E	D	-	4

2. Timpul total estimat

Total ore în planul de învăţământ	**Din care**				
	Ore auditoriale		**Lucrul individual**		
	Curs	**Laborator**	**Proiect de an**	**Studiul materialului teoretic**	**Pregătire aplicaţii**
Învăţământ cu frecvenţă	30	30	-	30	30

3. Precondiţii de acces la disciplină/modul

Conform planului de învăţământ	Programarea calculatoarelor Algebra liniară Matematica discretă
Conform competenţelor	Cunoștințe și abilități de operare cu sistemele informaționale, dispozitivele terminale

4. Condiţii de desfăşurare a procesului educaţional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector, calculator și acces la internet. Nu vor fi tolerate întârzierile studenţilor, precum şi convorbirile telefonice în timpul cursului.
Laborator	Studenţii vor perfecta rapoarte conform condiţiilor impuse de indicaţiile metodice. Termenul de predare a lucrării de laborator – 1 săptămână după finalizarea acesteia. Pentru predarea cu întârziere a lucrării aceasta se depunctează cu 1pct./săptămână de întârziere.

5. Competenţe specifice acumulate

Competenţe profesionale	***CP1. Elaborarea și proiectarea arhitecturii*** **2P.** Cerințele arhitecturii sistemelor: performanță, mentenabilitate, extensibilitate, scalabilitate, disponibilitate, securitate și accesibilitate. **4P.** Arhitectura întreprinderii și standardele interne ale companiei. **15P.** Utilizează cunoștințele sale tehnologice din diferite domenii pentru a elabora şi implementa arhitectura întreprinderii. ***CP3. Integrarea componentelor*** **1P.** Componente/module hardware/software, indiferent dacă sunt vechi, existente sau noi. **18P.** Securizează și face backup-ul datelor pentru a asigura integritatea lor în timpul integrării datelor sau a sistemului.

	CP5. Implementarea soluțiilor **5P.** Tehnologiile și standardele care se utilizează în timpul implementării/ /desfăşurării. ***CP7. Ingineria sistemelor*** **6P.** Bazele securităţii informaţiei **16P.** Conduce auditurile de gestionare a riscurilor și acționează pentru a reduce impactul acestora. **17P.** Aplică arhitecturi software și/sau hardware adecvate. ***CP8. Managementul problemelor*** **17P.** Alocă resurse adecvate activităților de întreținere, luând în considerare costurile și riscurile.
Competenţe transversale	**22 T.** Demonstrează executarea responsabilă a sarcinilor profesionale în condiţii de autonomie. **24 T.** Conştientizează nevoia de formare continuă cu utilizarea eficientă a resurselor şi tehnicilor de învăţare pentru dezvoltarea personală şi profesională.

6. Obiectivele disciplinei/modulului

Obiectivul general	Studierea elementelor de bază ale securității informațiilor, cu accent pe operaționalitatea sistemelor de securitate. De a analiza și înțelege diferite tipuri de incidente și atacuri de securitate, metode de prevenire, detecție și reacție la incidentele și atacurile asupra securității informaționale. Studierea elementelor de bază ale aplicării criptografiei în sistemele informaționale și a altor tehnologii de securizare a dispozitivelor terminale, infrastructurii de rețea și Cloud.
Obiectivele specifice	• *Analiza atacurilor care se bazează pe factorul uman;* • *Cunoaşterea şi utilizarea tehnologiilor pentru asigurarea securităţii informaţionale;* • *Evaluarea modelelor de ameninţări şi influenţa acestora asupra unei organizaţii;* • *Crearea politicilor de securitate relevante organizaţiei şi mediului;* • *Compararea diferitelor utilizări şi abordări ale criptografiei;* • *Pregătirea şi răspunsul la incidentele de securitate, securizarea sistemelor informaţionale;* • *Studierea atacurilor comune în reţea, controlul accesului.*

7. Conţinutul disciplinei

Tematica activităţilor didactice	**Numărul de ore**	
	învăţământ cu frecvenţă	**învăţământ cu frecvenţă redusă**
Tematica cursurilor		
1. Introducere în securitatea informației. Termeni de bază și definiții.	**2**	
2. Vulnerabilitatea sistemelor informaționale. Vectori de atac	**2**	
3. Programe malițioase. Ingineria socială	**2**	
4. Atacuri cibernetice	**2**	
5. Controlul accesului	**2**	
6. Administrarea conturilor și utilizatorilor	**2**	
7. Criptografia simetrică și asimetrică	**2**	
8. Algoritmi de hashing. Utilizare hashing	**2**	
9. Semnătura digitală. Certificate digitale	**2**	
10. Disponibilitatea. Redundanță și reziliență	**2**	
11. Protecția domeniilor cibernetice	**2**	

Tematica activităţilor didactice	Numărul de ore	
	învăţământ cu frecvenţă	învăţământ cu frecvenţă redusă
12. Protecția sistemului și a dispozitivelor terminale	**2**	
13. Protecția infrastructurii de rețea	**2**	
14. Protecția Cloud	**2**	
15. Sisteme de securitate	**2**	
Total curs:	**30**	
Tematica lucrărilor de laborator		
LL1. Analiza programelor malware. Analiza statică și dinamică. Configurarea programelor antivirus	**4**	
LL2. Detectarea amenințărilor și vulnerabilităților de securitate	**4**	
LL3. Controlul accesului	**6**	
LL4. Algoritmi de criptare/decriptare. Semnătura electronică	**4**	
LL 5. Configurare VPN. IDPS. Firewall	**6**	
LL 6. Crearea politicilor de securitate. Configurare tehnologii software de securitate	**4**	
LL7. Prezentarea rezultatelor obținute	**2**	
Total lucrări de laborator:	**30**	

8. Referinţe bibliografice

Principale	**1.** Cybersecurity essentials course. CISCO 2023 version. Disponibil: https://www.netacad.com /courses/ cybersecurity/cybersecurity-essentials **2.** WHITMAN, M. E., MATTORD, H.J. 2021. Principles of Information Security. 7th ed. Cengage Learning, p. 658. ISBN: 9780357710777 **3.** WHITMAN, M. E., MATTORD, H.J. 2016. Management of Information Security, 6th ed. Cengage, p.752. ISBN: 978-1-337-40571-3. **4.** CIAMPA, Mark. 2022. CompTIA Security+. Guide to Network Security Fundamentals. Ed. Cengage Learning, p. 784. ISBN: 9780357424377 **5.** ISO/IEC 27005: Information technology – Security techniques – Information security risk management. International Organization for Standardization. Geneva, Switzerland, 2018. **6.** SEIDL, David. 2021. CompTIA Security+. Practice tests. Sybex; 2nd edition, p. 336. ISBN: 9781119735465. **7.** THAKUR, K., PATHAN, A. Cybersecurity Fundamentals. CRC Press, 2020. DOI: 10.1201/9781003035626. **8.** ALEXEI, Arina. Indicații metodice la lucrările de laborator ”Tehnologii ale securității informaționale”. Editura UTM, Chișinău, 2024. ISBN 978-9975-64-448-8. **9.** ISO/IEC 27001: INFORMATION SECURITY MANAGEMENT. International Organization for Standardization. Geneva, Switzerland, 2023. Disponibil: https: //www.iso.org/isoiec-27001-information-security.html.
Suplimentare	**1.** HAUFE, K., et al. ISMS Core Processes: A Study. In: *Procedia Computer Science*. 2016, vol. 100, pp. 339–346. DOI: 10.1016/J.PROCS.2016.09.167. **2.** ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary, “International Organization for Standardization,” Geneva, Switzerland. Accessed: 05.08.2024. [Online]. Available: https://www.iso.org/standard/73906.html. **3.** ALEXEI, A. Cadrul Sistemic de Securitate a Comunicațiilor Electronice pentru Instituțiile de Învățământ Superior din Republica Moldova. UTM, Chișinău, 2023.

	4. BOLUN, I., CIORBĂ, D., ZGUREANU, A., BULAI, R. Informatics security assessment in the Republic of Moldova. In: Journal of Engineering Science, vol. XXVII, no. 4, pp. 103–119, 2020. DOI:10.5281/zenodo.4288297. ISSN 2587-347. **5.** FRENZEL, L. E. Principles of Electronic Communication Systems. McGrawHill Education, 4th ed., 2016. ISBN: 978-0-07-337385-0.

9. Utilizarea IA generativă

Permisiunea de utilizare	Utilizarea IA generative în cadrul temelor și proiectelor este permisă, cu condiția ca studenții să respecte următoarele reguli: • IA generativă poate fi utilizată pentru generarea de idei, structuri de text sau cod, dar toate materialele generate trebuie să fie revizuite și ajustate de către student pentru a se asigura că acestea corespund cerințelor academice. • Orice utilizare a IA generative trebuie să fie declarată în secțiunea de apendice a fiecărei lucrări, folosind fraza: "În timpul pregătirii acestei lucrări, autorul a utilizat [NUME INSTRUMENT / SERVICIU] în scopul [MOTIV]. După utilizarea acestui instrument/serviciu, autorul a revizuit și editat conținutul după cum a fost necesar și își asumă întreaga responsabilitate pentru conținutul lucrării."
Restricții de utilizare	Studenții nu trebuie să considere IA generativă ca o sursă de încredere pentru informații, deoarece nu oferă referințe clare sau surse documentate. • Nu este permisă citarea directă a conținutului generat de IA în lucrările academice ca și cum ar fi sursă primară. • Activitățile în care este interzis utilizarea IA generativă sunt specificare de profesor și sunt de regulă evaluări intermediare și finale sau care nu presupun activități de dezvoltare a competenților profesionale.

10. Evaluare

Periodică		**Curentă**	**Studiu individual**	**Proiect/teză**	**Examen**
EP 1	**EP 2**				
Învăţământ cu frecvenţă					
15%	15%	15%	15%		40%
Învăţământ cu frecvenţă redusă					
25%			25%		50%
Standard minim de performanţă: • Prezenţa şi activitatea la cursuri, lucrări de laborator; • Obţinerea notei minime de „5” la evaluările periodice, activitatea curentă, lucrul individual; • Obţinerea notei minime de „5” la examenul final.					

11. Criterii de evaluare

Activitate	**Componente evaluare**	**Metodă de evaluare, Criterii de evaluare**	**Pondere în nota finală a activității**	**Ponderea în evaluarea disciplinei**
Învăţământ cu frecvenţă				
Evaluare periodică I	Conținut teoretic, teme 1-7	Test pe platforma Moodle	100%	**15%**
Evaluare periodică II	Conținut teoretic, teme 8-15	Test pe platforma Moodle	100%	**15%**
		Susținerea lucrărilor de laborator	50%	**15%**

Activitate	Componente evaluare	Metodă de evaluare, Criterii de evaluare	Pondere în nota finală a activității	Ponderea în evaluarea disciplinei
Evaluare curentă	Activitatea practică	Implicarea în procesul de învățare activă la cursuri	25%	
		Rezultatele mini-testelor curente realizate la orele de curs	25%	
Studiul individual	Sarcina 1: Crearea mindmap-urilor la temele studiate la curs	Prezentare/discurs public	50%	**15%**
	Sarcina 2: Elaborarea unui sistem de management al securității informaționale	Portofoliu prezentat spre evaluare	50%	
Evaluarea finală	Conținut teoretic și practic	Test pe platforma Moodle/ Examen scris	100%	**40%**