FUNDAMENTE ALE SECURITĂȚII CIBERNETICE

1. Date despre disciplină

Facultatea	Calculatoare, Informatică şi Microelectronică				
Departamentul	Inginerie Software şi Automatica				
Ciclul de studii	Ciclul II, Studii superioare de master				
Programul de studii	Tehnologia informației pentru afaceri				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opţionalitate**	**Credite ECTS**
Anul I *(învățământ cu frecvenţă)*	III	E	S – unitate de curs de specialitate	A - unitate de curs opțională	5

2. Timpul total estimat

Total ore în planul de învățământ	**Din care**				
	Ore auditoriale		**Lucrul individual**		
	Curs	**Practice**	**Proiect de an**	**Studiul materialului teoretic**	**Pregătire aplicaţii**
150	20	20	-	110	-

3. Precondiții de acces la disciplină/modul

Conform planului de învățământ	Tehnologii informaționale și de comunicații
Conform competențelor	Explicarea soluțiilor prin utilizarea tehnicilor, conceptelor și principiilor din științele exacte și aplicative

4. Condiţii de desfăşurare a procesului educaţional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector și calculator
Practice	Vor fi perfectate rapoarte ale activităților practice realizate

5. Competențe specifice acumulate

Competențe profesionale	• CPM1. Sistemul informatic (SI) și alinierea strategiilor de afaceri • CPM4. Monitorizarea tendințelor tehnologice • CPM7. Furnizarea de servicii • CPM10. Managementul schimbărilor în afaceri
Competențe transversale	• CTM2. Interacțiune socială • CTM3. Dezvoltare profesională și personală.

6. Obiectivele disciplinei/modulului

Obiectivul general	Este de a oferi masteranzilor o înțelegere profundă a conceptelor și terminologiei specifice domeniului securității cibernetice. Acesta acoperă identificarea principalelor amenințări și definirea strategiilor de remediere a vulnerabilităților din infrastructura informațională.
Obiectivele specifice	• Însușirea conceptelor-cheie și a terminologiei specifice securității cibernetice; • Identificarea amenințărilor cibernetice; • Definirea strategiilor de identificare și remediere a vulnerabilităților din activele informaționale; • Determinarea componentelor sistemice necesare pentru un program eficient de securitate cibernetică, inclusiv personalul.

7. Conţinutul disciplinei/modulului

Tematica activităților didactice	Numărul de ore învățământ cu frecvență
1. Domeniul Securității Cibernetice	2
2. Amenințări de Securitate	2
3. Programe Malware	2
4. Atacuri Cibernetice	2
5. Controlul Accesului	2
6. Tehnologii ale Securității Cibernetice	4
7. Criptografia	2
8. Gestionarea Riscului Cibernetic	2
9. Programe de Securitate Cibernetică	2
Total curs:	**20**
AP1. Securitatea contului GOOGLE	2
AP2.Dreptul de proprietate a datelor	2
AP3. Identificarea și analiza atacurilor cibernetice	4
AP4. Bitlocker and Bitlocker To Go	2
AP5. Configurare Windows Local Security Policy	4
AP6. Configurare Utilizatori si Grupuri in Windows	2
AP7. Configurare Windows Firewall	4
Total lucrări practice:	**20**

8. Referinţe bibliografice

Principale	1. ALEXEI, Arina. Suport de curs ”Fundamente ale securității cibernetice”. Editura UTM, Chișinău, 2024. ISBN . 2. Cybersecurity essentials course. CISCO 2023 version. Disponibil: https://www.netacad.com /courses/ cybersecurity/cybersecurity-essentials 3. WHITMAN, M. E., MATTORD, H.J. 2021. Principles of Information Security. 7th ed. Cengage Learning, p. 658. ISBN: 9780357710777 4. WHITMAN, M. E., MATTORD, H.J. 2016. Management of Information Security, 6th ed. Cengage, p.752. ISBN: 978-1-337-40571-3. 5. CIAMPA, Mark. 2022. CompTIA Security+. Guide to Network Security Fundamentals. Ed. Cengage Learning, p. 784. ISBN: 9780357424377 6. ISO/IEC 27005: Information technology – Security techniques – Information security risk management. International Organization for Standardization. Geneva, Switzerland, 2018. 7. SEIDL, David. 2021. CompTIA Security+. Practice tests. Sybex; 2nd edition, p. 336. ISBN: 9781119735465. 8. THAKUR, K., PATHAN, A. Cybersecurity Fundamentals. CRC Press, 2020. DOI: 10.1201/9781003035626. 9. ALEXEI, Arina. Indicații metodice la lucrările de laborator ”Tehnologii ale securității informaționale”. Editura UTM, Chișinău, 2024. ISBN 978-9975-64-448-8. 10. 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. ALSHAIKH, M., et al. Information Security Policy: A Management Practice Perspective. In: *Australasian Conference on Information Systems*, 2015. 2. ISMAIL, W. B., et al. A generic framework for information security policy development. In: 2017 4th International Conference on Electrical Engineering,

Computer Science and Informatics (EECSI). 2017, pp. 1-6. DOI: 10.1109/EECSI. 2017.8239132.
3. ALEXEI, Arina. Ensuring Information Security in Public Organizations in the Republic of Moldova through the ISO 27001 Standard. In: *Journal of Social Sciences*, B+, Vol. IV, No 1, 2021, pp. 84-94. ISSN 2587-3490. DOI: https://doi.org/10.52326/jss. utm. 2021. 4(1).11.
4. 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.
5. 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.
6. 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.
7. FRENZEL, L. E. Principles of Electronic Communication Systems. McGrawHill Education, 4th ed., 2016. ISBN: 978-0-07-337385-0.
8. ALEXEI, An., ALEXEI, Ar. The problem of information systems security in SME. In: CEEeGov: Central and Eastern European eDem and eGov Days, Budapest, Hungary, September 2023. ACM, New York, NY, USA, 6 Pages. DOI: https://doi.org/10.1145/3603304. 3603346.
9. WILLS, Mike. 2020. The Official (ISC)2 SSCP CBK Reference. 5th ed. John Wiley & Sons, Inc. Indianapolis, Indiana. ISBN 1119874866.
10. SIKORSKI, Michael, HONIG, Andrew. 2012. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press, 1st edition, p. 800. ISBN: 9781593272906.
11. ALEXEI, Ar., ALEXEI, An. The difference between cyber security vs information security. In: Journal of Engineering Science, Vol. XXIX, no. 4 (2022), pp. 72 – 83. DOI: https://doi.org/10.52326/jes.utm.2022.29(4).08.

9. Evaluare

Periodică		Curentă	Studiu individual	Proiect/teză	Examen
EP 1	**EP 2**				
Învăţământ cu frecvenţă					
15%	15%	15%	15%	-	40%

10. 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 1-5	Test pe MOODLE	100%	**15%**
Evaluare periodică II	Conținut teoretic, teme 6-9	Test pe MOODLE	100%	**15%**
Evaluare curentă	Activitatea practică	Discuții în cadrul seminarelor	50%	**15%**
		Rapoarte pentru fiecare Studiu de caz în discuție și activitate practică	50%	
Studiul individual	Cercetare la temă	Prezentare/discurs public	100%	**15%**
Evaluarea finală	Conținut teoretic și practic	Examen scris. Notare conform baremului	100%	**40%**