FACULTATEA CALCULATOARE, INFORMATICĂ ȘI MICROELECTRONICĂ
DEPARTAMENTUL INGINERIA SOFTWARE ȘI AUTOMATICĂ

APROBAT
la şedinţa Departamentului ISA
nr.____din_____
Șef departament
FIODOROV Ion
conf. univ., dr.
_____

APROBAT
la şedinţa Consiliului Facultăţii CIM
nr.____din_____
Președintele Consiliului CIM
CIORBĂ Dumitru,
conf. univ., dr.
_____

Program de master: *Tehnologia informației pentru afaceri*

Cod, Denumirea modulului: F.O.006. Fundamente ale securității cibernetice

Beneficiari: *Masteranzii anului II, învățământ cu frecvență*

Ciclul de învățământ: *Studii superioare de master, ciclul II*

Numărul de credite ECTS: *5*

Titularul disciplinei

_____lect.univ.dr., Arina ALEXEI_____

Nume, prenume, semnătura titularului

I. PRELIMINARII

Scopul cursului 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 educaționale includ:

- 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.

Sarcinile implică evaluarea prin teste formative pe parcursul semestrului, sarcini practice și prezentări orale pe teme relevante.

II. PRECONDIŢII DE ACCES LA DISCIPLINĂ/MODUL

Pentru a atinge obiectivele cursului studenţii trebuie să posede cunoștințe despre sistemele IT, Fundamentele rețelelor de calculatoare IT, Fundamentele tehnologiei informației, componentele sistemelor informaționale.

III. COMPETENŢELE CARE URMEAZĂ A FI DEZVOLTATE

Disciplina/modulul prevede formarea următoarelor competenţe profesionale şi transversale:

Competențe profesionale:

- *CPM1. Sistemul informatic (SI) și alinierea strategiilor de afaceri*
- *CPM4. Monitorizarea tendințelor tehnologice*
- *CPM7. Furnizarea de servicii*
- *CPM10. Managementul schimbărilor în afaceri*

Competenţe transversale:

- *CTM2. Interacțiune socială*
- *CTM3. Dezvoltare profesională și personală.*

IV. ADMINISTRAREA DISCIPLINEI/MODULULUI

Cod	Anul	Semestrul	Numărul de ore				Credite
			Curs	Lucrări practice	Proiectare	Lucrul individual	
F.O.006	Învăţământ cu frecvenţă						
	II	III	20	20		110	5

V. REZULTATELE ÎNVĂŢĂRII, CONŢINUTURI ŞI METODE DIDACTICE APLICATE

Rezultatele învăţării. Studentul trebuie:	**Conţinuturi**		**Metode de predare**	**Realizarea în timp (ore)**	
	Curs	**Seminare/lucrări practice**		**învăţământ cu frecvenţă**	
				curs	**practice**
În rezultatul însușirii temei studentul trebuie: ***să cunoască:*** *- Domeniile cibernetice,* *- Concepte cheie în sistemele cibernetice,* *- Cubul McCumber;* *- Impactul atacurilor cibernetice;* *- Profilul criminalilor în securitate cibernetică.* ***să fie capabil:*** *- Verifice securitatea contului personal Google;* *- Securizeze contul google* *- Să implementeze verificarea în mai mulți pași;* *- Verifice activitatea contului personal.*	1. DOMENIUL SECURITĂȚII CIBERNETICE	AP1. Securitatea contului GOOGLE	-Expunerea materialului, -Prezentare PowerPoint cu utilizarea tablei interactive, -Materiale video demonstrative de pe Youtube, -Demonstrații în timp real.	**2**	**2**
În rezultatul însușirii temei studentul trebuie: ***să cunoască:*** *- Vulnerabilități de securitate,* *- Vectori de atac,* *- Activele informaționale,* *- Tehnicile ingineriei sociale..* ***să fie capabil:*** *- Analizeze termenii politicilor de servicii;* *- Implementeze setări de confidențialitate;* *- Determine ce poate face furnizorul de servicii cu datele;* *- Implementeze acțiuni de protejare ale serviciului.*	2. AMENINȚĂRI DE SECURITATE	AP2.Dreptul de proprietate a datelor	-Expunerea materialului, -Prezentare PowerPoint cu utilizarea tablei interactive, -Materiale video demonstrative de pe Youtube, -Demonstrații în timp real.	**2**	**2**
În rezultatul însușirii temei studentul trebuie: ***să cunoască:*** *- Programele malware,*	3. PROGRAME MALWARE	AP3. Identificarea și analiza atacurilor cibernetice	-Expunerea materialului,	**2**	**4**

Rezultatele învăţării. Studentul trebuie:	Conţinuturi		Metode de predare	Realizarea în timp (ore)	
	Curs	Seminare/lucrări practice		învăţământ cu frecvenţă	
				curs	practice
- *Malware cu funcționalități specifice;* - *Analiza și protecția anti-malware.* ***să fie capabil:*** - *Exploreze atacurile cibernetice;* - *Analizeze amenințările comune de securitate;* - *Exploreze atacurile cibernetice recente;* - *Să identifice amenințările specifice triadei CIA.*			-Prezentare PowerPoint cu utilizarea tablei interactive, -Materiale video demonstrative de pe Youtube, -Demonstrații în timp real.		
În rezultatul însușirii temei studentul trebuie: ***să cunoască:*** - *Atacuri cibernetice: de inundare, interceptare, spoofing,* - *Atacuri asupra drepturilor de acces;* - *Atacuri asupra aplicațiilor;* - *Atacuri pe partea de server al aplicațiilor web;* - *Atacuri pe partea de client al aplicațiilor web;* - *Atacuri imparțiale.*	4. ATACURI CIBERNETICE		-Expunerea materialului, -Prezentare PowerPoint cu utilizarea tablei interactive, -Materiale video demonstrative de pe Youtube, -Demonstrații în timp real.	**2**	
În rezultatul însușirii temei studentul trebuie: ***să cunoască:*** - *Concepte generale;* - *Tipuri de control al accesului;* - *Modele de control al accesului.* ***să fie capabil:*** - *Cripteze o unitate externă de stocare a datelor;* - *Cripteze unitatea care conține sistemul de operare;* - *Decripteze unitățile criptate.*	5. CONTROLUL ACCESULUI	AP4. Bitlocker and Bitlocker To Go	-Expunerea materialului, -Prezentare PowerPoint cu utilizarea tablei interactive, -Materiale video demonstrative de pe Youtube, -Demonstrații în timp real.	**2**	**2**
În rezultatul însușirii temei studentul trebuie: ***să cunoască:*** - *Tipurile și arhitectura firewall-urilor;* - *Filtre de conținut;*	6. TEHNOLOGII ALE SECURITĂȚII CIBERNETICE	AP5. Configurare Windows Local Security Policy	-Expunerea materialului, -Prezentare PowerPoint cu utilizarea tablei interactive,	**4**	**4**

Rezultatele învăţării. Studentul trebuie:	Conţinuturi		Metode de predare	Realizarea în timp (ore)	
	Curs	Seminare/lucrări practice		învăţământ cu frecvenţă	
				curs	practice
- *Rețele virtuale private;* - *Sisteme de detecție și prevenire a intruziunilor.* ***să fie capabil:*** - *Examineze cerințele de securitate;* - *Utilizeze instrumentul Politică de securitate locală Windows;* - *Configureze setările de securitate ale politicii privind parolele;* - *Configureze setările de securitate ale politicii privind blocarea contului;.* - *Configureze setările de securitate ale politicii de audit;* - *Testeze setările de securitate ale politicilor de securitate;* - *Exporte și importe setările politicilor de securitate.*			-Materiale video demonstrative de pe Youtube, -Demonstrații în timp real.		
În rezultatul însușirii temei studentul trebuie: ***să cunoască:*** - *Concepte de bază,* - *Algoritmi hash,* - *Algoritmi simetrici de criptare;* - *Algoritmi asimetrici de criptare;* - *Managementul cheilor criptografice.* ***să fie capabil:*** - *Utilizeze managerul de utilizatori și grupuri locale;;* - *Verifice permisiunile de utilizator și de grup;* - *Creeze noi grupuri și să aloce drepturi de acces;* - *Modifice permisiunile de utilizator și de grup;* - *Utilizeze algoritmii de criptare simetrici clasici.*	7. CRIPTOGRAFIA	AP6. Configurare Utilizatori si Grupuri in Windows	-Expunerea materialului, -Prezentare PowerPoint cu utilizarea tablei interactive, -Materiale video demonstrative de pe Youtube, -Demonstrații în timp real.	**2**	**2**

Rezultatele învăţării. Studentul trebuie:	Conţinuturi		Metode de predare	Realizarea în timp (ore)	
	Curs	Seminare/lucrări practice		învăţământ cu frecvenţă	
				curs	practice
În rezultatul însușirii temei studentul trebuie: ***să cunoască:*** - *Riscul cibernetic;* - *Evaluarea vulnerabilităților de securitate;* - *Managementul riscului cibernetic.* ***să fie capabil:*** - *Creeze și partajeze foldere;* - *Configureze caracteristicile programelor permise în Windows Firewall;* - *Exploreze caracteristicile complexe de securitate în Windows Firewall* - *Verifice starea firewall-ului și cum funcționează setările configurate.*	8. GESTIONAREA RISCULUI CIBERNETIC	AP7. Configurare Windows Firewall	-Expunerea materialului, -Prezentare PowerPoint cu utilizarea tablei interactive, -Materiale video demonstrative de pe Youtube, -Demonstrații în timp real.	**2**	**4**
În rezultatul însușirii temei studentul trebuie: ***să cunoască:*** - *Politici de securitate;* - *Standarde de securitate;* - *Personal de securitate;* - *Programe de îmbunătățire continuă.*	9. PROGRAME DE SECURITATE CIBERNETICĂ		-Expunerea materialului, -Prezentare PowerPoint cu utilizarea tablei interactive, -Materiale video demonstrative de pe Youtube, -Demonstrații în timp real.	**2**	

VI. SUGESTII PENTRU ACTIVITATEA INDIVIDUALĂ A STUDENŢILOR

Nr. crt.	Capitol, temă	Conținut activitate individuală	Durata, ore	Forma de control	Termeni de control (perioada)
1	DOMENIUL SECURITĂȚII CIBERNETICE	Studiu de caz 1	4	Încărcarea pe platforma ELSE	1 săptămână
		Elaborarea raportului și pregătirea pentru susținerea activității practice	4	Încărcarea pe platforma ELSE	1 săptămână
2	AMENINȚĂRI DE SECURITATE	Studiu de caz 2	4	Încărcarea pe platforma ELSE	1 săptămână
		Elaborarea raportului și pregătirea pentru susținerea activității practice	4	Încărcarea pe platforma ELSE	1 săptămână
3	PROGRAME MALWARE	Studiu de caz 3	4	Încărcarea pe platforma ELSE	1 săptămână
		Elaborarea raportului și pregătirea pentru susținerea activității practice	4	Încărcarea pe platforma ELSE	1 săptămână
4	ATACURI CIBERNETICE	Studiu de caz 4	4	Încărcarea pe platforma ELSE	1 săptămână
5	CONTROLUL ACCESULUI	Studiu de caz 5	4	Încărcarea pe platforma ELSE	1 săptămână
		Elaborarea raportului și pregătirea pentru susținerea activității practice	4	Încărcarea pe platforma ELSE	1 săptămână
6	TEHNOLOGII ALE SECURITĂȚII CIBERNETICE	Studiu de caz 6	4	Încărcarea pe platforma ELSE	1 săptămână
		Elaborarea raportului și pregătirea pentru susținerea activității practice	4	Încărcarea pe platforma ELSE	1 săptămână

Nr. crt.	Capitol, temă	Conținut activitate individuală	Durata, ore	Forma de control	Termeni de control (perioada)
7	CRIPTOGRAFIA	Studiu de caz 7	4	Încărcarea pe platforma ELSE	1 săptămână
		Elaborarea raportului și pregătirea pentru susținerea activității practice	4	Încărcarea pe platforma ELSE	1 săptămână
8	GESTIONAREA RISCULUI CIBERNETIC	Studiu de caz 8	4	Încărcarea pe platforma ELSE	1 săptămână
		Elaborarea raportului și pregătirea pentru susținerea activității practice	4	Încărcarea pe platforma ELSE	1 săptămână
9	PROGRAME DE SECURITATE CIBERNETICĂ	Studiu de caz 9	4	Încărcarea pe platforma ELSE	1 săptămână
10	Politici de securitate generale și specifice	Elaborarea politicii de securitate generale și a unei politici de securitate specifică	46	Încărcarea pe platforma ELSE	1 lună
		Total	110		

VII. EVALUAREA DISCIPLINEI

Periodică		Curentă	Studiu individual	Proiect/teză	Examen
EP 1	**EP 2**				
Învăţământ cu frecvenţă					
15%	15%	15%	15%		40%
Standard minim de performanță: - Prezența și activitatea la cursuri, lucrări practice; - Obținerea notei minime de „5” la evaluările periodice, activitatea curentă, lucrul individual; Obținerea notei minime de „5” la examenul final.					

VIII. CRITERII DE EVALUARE

Denumire	Modul de desfăşurare	Pondere pe componente de conţinut
Învăţământ cu frecvenţă		
Evaluare curentă		**15%**
	Prezentarea și susținerea activităților practice	*50%*
	Implicarea în procesul de învățare activă la cursuri	*25%*

Denumire	Modul de desfăşurare	Pondere pe componente de conţinut
	Rezultatele mini-testelor curente realizate la orele de curs	*25%*
Studiu individual		**15%**
Sarcina 1: Studii de caz	***Prezentare la temă***	*50%*
Sarcina 2: Politici de securitate	***Portofoliu prezentat spre evaluare***	*50%*
Evaluare periodică		
EP 1	***Test pe platforma ELSE***	**15%**
EP 2	***Test pe platforma ELSE***	**15%**
Examen semestrial	***Scris, în baza biletului individual***	**40%**

IX. LISTA DE SUBIECTE PENTRU EVALUĂRI PERIODICE ŞI CEA FINALĂ

CHESTIONAR PENTRU EP I

INCLUDE SUBIECTE DIN TEMELE 1-5

1. DOMENIUL SECURITĂȚII CIBERNETICE

1.1. EVOLUȚIE ȘI TENDINȚE MODERNE

1.2. CONCEPTE-CHEIE

1.3. CUBUL MCCUMBER

1.4. IMPACTUL ATACURILOR CIBERNETICE

1.5. PROFILUL ATACATORILOR CIBERNETICI

1.6. IMPLEMENTAREA SECURITĂȚII CIBERNETICE ÎN ORGANIZAȚII

2. AMENINȚĂRI DE SECURITATE

2.1. VULNERABILITĂȚI DE SECURITATE

2.2. VECTORI DE ATAC

2.3. ACTIVE INFORMAȚIONALE

2.4. INGINERIA SOCIALĂ

3. PROGRAME MALWARE

3.1. PROGRAME MALWARE

3.2. MALWARE CU FUNCȚIONALITĂȚI SPECIFICE

3.3. ANALIZĂ ȘI PROTECȚIE ANTI-MALWARE

4. ATACURI CIBERNETICE

4.1. ATACURI ÎN REȚEA

4.1.1. ATACURI DE INUNDARE

4.1.2. ATACURI DE INTERCEPTARE

4.1.3. ATACURI DE SPOOFING/FALSIFICARE

4.1.4. ATACURI ASUPRA DREPTURILOR DE *ACCES*

4.2. ATACURI ASUPRA APLICAȚIILOR

4.2.1. ATACURI PE PARTEA DE SERVER A APLICAȚIILOR WEB

4.2.2. ATACURI PE PARTEA DE CLIENT A APLICAȚIILOR WEB

4.2.3. ATACURI IMPARȚIALE

5. CONTROLUL ACCESULUI

5.1. CONCEPTE GENERALE

5.2. TIPURI DE CONTROL AL ACCESULUI

5.3. MODELE DE CONTROL AL ACCESULUI

CHESTIONAR PENTRU EP A II-A

INCLUDE SUBIECTE DIN TEMELE 6-9

6. TEHNOLOGII ALE SECURITĂȚII CIBERNETICE

6.1. FIREWALL

6.1.1. TIPURI DE FIREWALL

6.1.2. ARHITECTURA FIREWALL-URILOR

6.2. FILTRE DE CONȚINUT

6.3. REȚELE PRIVATE VIRTUALE (VPN)

6.4. SISTEME DE DETECȚIE ȘI PREVENIRE A INTRUZIUNILOR

7. CRIPTOGRAFIA

7.1. CONCEPTE DE BAZĂ

7.2. ALGORITMI HASH

7.3. ALGORITMI SIMETRICI DE CRIPTARE

7.4. ALGORITMI ASIMETRICI DE CRIPTARE

7.5. MANAGEMENTUL CHEILOR DE CRIPTARE

7.6. CRIPTAREA SIMETRICĂ VERSUS ASIMETRICĂ

8. GESTIONAREA RISCULUI CIBERNETIC

8.1. EVALUAREA VULNERABILITĂȚILOR

8.2. MANAGEMENTUL RISCULUI CIBERNETIC

9. PROGRAME DE SECURITATE CIBERNETICĂ

9.1. POLITICI DE SECURITATE

9.2. STANDARDE DE SECURITATE

9.3. PERSONALUL DE SECURITATE

9.4. PROGRAME DE ÎMBUNĂTĂȚIRE CONTINUĂ

CHESTIONAR PENTRU EXAMEN

1. DOMENIUL SECURITĂȚII CIBERNETICE
2. AMENINȚĂRI DE SECURITATE
3. PROGRAME MALWARE
4. ATACURI CIBERNETICE
5. CONTROLUL ACCESULUI
6. TEHNOLOGII ALE SECURITĂȚII CIBERNETICE
7. CRIPTOGRAFIA
8. GESTIONAREA RISCULUI CIBERNETIC
9. PROGRAME DE SECURITATE CIBERNETICĂ

X. REFERINȚE BIBLIOGRAFICE

Obligatorii

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.

11. 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. ALEXEI, A. Cadrul Sistemic de Securitate a Comunicațiilor Electronice pentru Instituțiile de Învățământ Superior din Republica Moldova. UTM, Chișinău, 2023.
7. 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.
8. FRENZEL, L. E. Principles of Electronic Communication Systems. McGrawHill Education, 4th ed., 2016. ISBN: 978-0-07-337385-0.
9. 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.
10. WILLS, Mike. 2020. The Official (ISC)2 SSCP CBK Reference. 5th ed. John Wiley & Sons, Inc. Indianapolis, Indiana. ISBN 1119874866.
11. 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.
12. 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.