

**G.O.001 TEHNOLOGII INFORMAȚIONALE ȘI SECURITATEA CIBERNETICĂ**
**1. Date despre disciplină**

<b>Facultatea</b>	Electronică și Telecomunicații				
<b>Departamentul</b>	Telecomunicații și Sisteme Electronice				
<b>Ciclul de studii</b>	Studii superioare de licență, ciclul I				
<b>Programul de studii</b>	0714.1 TEHNOLOGII ȘI SOFTWARE ÎN REȚELE DE COMUNICAȚII 0714.6 SECURITATEA COMUNICAȚIILOR ELECTRONICE 0710.1 INGINERIE ȘI MANAGEMENT ÎN COMUNICAȚII ELECTRONICE				
<b>Anul de studii</b>	<b>Semestrul</b>	<b>Tip de evaluare</b>	<b>Categoria formativă</b>	<b>Categoria de opționalitate</b>	<b>Credite ECTS</b>
I -învățământ cu frecvență II -învățământ cu frecvență redusă	I I	E	G – unități de curs/module de creare a abilităților și competențelor generale	O – unitate de curs obligatorie	3

**2. Timpul total estimat**

Total ore în planul de învățământ	Din care				
	Ore auditoriale		Lucrul individual		
	Curs	Lucrări practice	Proiect de an	Studiul materialului teoretic	Pregătire aplicații
90	30	15	-	30	15
90	10	8	-	36	36

**3. Precondiții de acces la disciplină**

Conform planului de învățământ	Informatica, Matematica, Fizica
Conform competențelor	Cunoștințe generale privind structura sistemelor informaționale, componente hardware, sisteme de operare.

**4. Condiții de desfășurare a procesului educațional pentru**

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de tablă, proiector și calculator. Nu vor fi tolerate întârzierile studenților, precum și convorbirile telefonice în timpul cursului. În cazul orelor online, acestea se vor realiza în Microsoft Teams
Laborator/seminar	Studenții vor executa lucrările de laborator, conform indicațiilor metodice. Vor perfecta rapoarte în format electronic, pe care le vor încărca pe platforma Moodle, nu mai târziu de o săptămână după efectuarea lucrării.

**5. Competențe specifice acumulate**

Competențe generale	<p><b>Pentru programul de studii IMCE</b></p> <p><b>CG1. Utilizarea în activitatea profesională a legislațiilor de bază definite în științele fundamentale.</b></p> <p><b>CG 1.1.</b> Aplica principiile de bază și prevederile legale relevante pentru utilizarea informațiilor și securitatea cibernetică.</p> <p><b>CG 1.2.</b> Respecta normele etice și juridice privind protecția datelor și proprietatea intelectuală în mediul digital.</p> <p><b>CG2. Aplicarea rezultatelor studiilor de marketing la dezvoltarea produselor/serviciilor competitive.</b></p> <p><b>CG 2.1.</b> Analiza nevoile pieței pentru produse IT și servicii de securitate cibernetică.</p> <p><b>CG 2.2.</b> Propune soluții și servicii IT inovatoare pe baza analizei de piață și a studiilor de marketing.</p> <p><b>Pentru programul de studii TSRC și SCE</b></p> <p><b>CG2. Aplicarea rezultatelor studiilor de marketing la dezvoltarea produselor/serviciilor competitive.</b></p> <p><b>CG 2.1.</b> Analiza nevoile pieței pentru produse IT și servicii de securitate cibernetică.</p> <p><b>CG 2.2.</b> Propune soluții și servicii IT inovatoare pe baza analizei de piață și a studiilor de marketing.</p> <p><b>CG4. Asigurarea respectării cadrului normativ în domeniul SSM și protecției mediului.</b></p> <p><b>CG4.1</b> Aplica regulile de securitate tehnică de igienă a muncii evaluând factorii de risc profesional la</p>
---------------------	--

	locul de muncă.
Competențe profesionale	<p><b>Pentru programul de studii IMCE</b></p> <p><b>CP4. Utilizarea limbajelor de programare specializate.</b></p> <p><b>CP 4.1.</b> Scrie, testa și depana cod folosind limbaje de programare specializate pentru dezvoltarea de aplicații sigure.</p> <p><b>CP 4.2.</b> Implementa algoritmi și structuri de date pentru a rezolva probleme specifice de securitate a informațiilor.</p> <p><b>CP 4.3.</b> Utiliza medii de dezvoltare și instrumente specifice pentru crearea de software.</p> <p><b>Pentru programul de studii TSRC și SCE</b></p> <p><b>CP1. Identificarea tehnologiilor utilizate în domeniul comunicațiilor electronice.</b></p> <p>CP1.1 Identifica caracteristicile tehnologiilor utilizate în domeniul comunicațiilor electronice la proiectarea și exploatarea rețelelor de comunicații.</p>

## 6. Obiectivele disciplinei

Obiectivul general	Cunoașterea componentelor hardware, sistemelor de operare. Implementarea procesului de instalare, configurare și depanare a sistemelor informaționale.
Obiectivele specifice	<p>Cunoașterea noțiunilor specifice tehnologiilor informaționale.</p> <p>Instalarea și utilizarea diferitelor componente hardware și software.</p> <p>Configurarea optimă a produselor software.</p> <p>Depanarea problemelor hardware, sistemelor de operare. Cunoașterea problemelor comune și a soluțiilor aferente componentelor hardware și sistemelor de operare.</p>

## 7. Conținutul disciplinei

Tematica activităților didactice	învățământ cu frecvență	învățământ cu frecvență redusă
T1. Introducere în rețele de calculatoare.	2	0,5
T2. Modele și protocoale de rețea.	2	0,5
T3. Nivelul Fizic.	2	1
T4. Sisteme de numerație.	2	1
T5. Rețeaua Ethernet.	2	1
T6. Nivelul Rețea.	2	1
T7. Nivelul Transport și Nivelul Aplicație.	2	0,5
T8. Conceptele de bază în domeniul securității cibernetice.	2	0,5
T9. Tehnici și tipuri de atac cibernetic.	2	0,5
T10. Protejarea datelor online și a confidențialității.	2	0,5
T11. Strategii de securizare a rețelelor, echipamentelor și datelor.	2	1
T12. Programarea modernă cu Web 2.0 și Web 3.0	2	1
T13. Tehnologia de Cloud.	2	0,5
T14. Inteligența Artificială și Învățarea Automată (Machine Learning).	2	0,5
T15. Automatizarea și rolul acesteia în domeniul securității cibernetice.	2	
<b>Total prelegeri:</b>	<b>30</b>	<b>10</b>

LL1. Packet Tracer. Simularea rețelelor.	1	0,5
LL2. Explorarea nivelului fizic.	2	1
LL3. Adresarea IP.	2	0,5
LL4. Schimbul de date prin intermediul protocoalelor TCP și UDP.	2	0,5
LL5. Identificarea unui loc de muncă în domeniul securității cibernetice.	1	1
LL6. Explorarea criptării fișierelor și datelor. Verificarea integrității fișierelor și datelor.	1	1
LL7. Detectarea vulnerabilităților și amenințărilor.	1	1
LL8. Utilizarea stenografiei.	1	0,5
LL9. Configurarea Modulului de Transport VPN.	2	1
LL10. Configurarea Modulului Tunel VPN.	2	1
<b>Total lucrări de laborator:</b>	<b>15</b>	<b>8</b>

## 8. Referințe bibliografice

Principale	<ol style="list-style-type: none"> <li>Hotărârea Parlamentului Nr. HP391/2023 din 15.12.2023 privind aprobarea Strategiei securității naționale a Republicii Moldova, publicat: 17.01.2024 în MONITORUL OFICIAL Nr. 17-19, <a href="https://presedinte.md/app/webroot/uploaded/Proiect%20SSN_2023.pdf">https://presedinte.md/app/webroot/uploaded/Proiect%20SSN_2023.pdf</a></li> <li>Ludmila PECA, Dinu ȚURCANU. Network security: Practical examples solved to be introduced in network security. SBN 978-9975-45-941-9. Chișinău, Publisher „Tehnica-UTM”, 2023. Disponibil: <a href="http://repository.utm.md/bitstream/handle/5014/22819/Network-security-Practical-">http://repository.utm.md/bitstream/handle/5014/22819/Network-security-Practical-</a></li> </ol>
------------	--

	<p><a href="#">examples-Guide.pdf?sequence=1&amp;isAllowed=y</a></p> <p>3. Cisco Networking Academy. Introducere în Securitatea Cibernetică - este un curs care oferă informații despre securitatea online, diferitele tipuri de malware și atacuri cibernetice, măsurile luate de companii pentru a le elimina / Cisco Systems, 2022, <a href="https://www.netacad.com/portal/web/self-enroll/m/course-1226327">https://www.netacad.com/portal/web/self-enroll/m/course-1226327</a></p> <p>4. Cisco Networking Academy. Curs CCNA Routing &amp; Switching / Cisco Systems, 2023, <a href="https://www.netacad.com/">https://www.netacad.com/</a></p> <p>5. <a href="https://paloaltonetworksacademy.net/course/view.php?id=2351">https://paloaltonetworksacademy.net/course/view.php?id=2351</a></p> <p>6. <a href="https://paloaltonetworksacademy.net/course/view.php?id=2355">https://paloaltonetworksacademy.net/course/view.php?id=2355</a></p>
Suplimentare	<p>1. Hotărârea Guvernului Nr. 811 din 29-11-2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020. Ministerul Justiției, <a href="https://www.legis.md/cautare/getResults?doc_id=110324&amp;lang=ro">https://www.legis.md/cautare/getResults?doc_id=110324&amp;lang=ro</a></p> <p>2. Ludmila PECA, Dinu ȚURCANU. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher „Tehnica-UTM”, 2022. <a href="http://repository.utm.md/bitstream/handle/5014/20549/Computer-networks-Practical-examples-DS.pdf?sequence=1&amp;isAllowed=y">http://repository.utm.md/bitstream/handle/5014/20549/Computer-networks-Practical-examples-DS.pdf?sequence=1&amp;isAllowed=y</a></p> <p>3. Ghid de bune practici privind asigurarea securității pe rețelele sociale, I.P. Serviciul Tehnologia Informației și Securitate Cibernetică, <a href="https://stisc.gov.md/sites/default/files/ghiduri/Ghid%20de%20bune%20practici.pdf">https://stisc.gov.md/sites/default/files/ghiduri/Ghid%20de%20bune%20practici.pdf</a></p> <p>4. Ghid de bune practici pentru securitate cibernetică, Serviciul Român de Informații, <a href="https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf">https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf</a></p> <p>5. Iulian ALECU, Costel CIUCHI, Toma CÎMPEANU, Iulian COMAN, Larisa GĂBUDEANU, Ioan-Cosmin MIHAL, Cosmina MOGHIOR, Nelu MUNTEANU, Gabriel PETRICĂ, Ionuț STOICA, Cătălin ZETU. Ghid de securitate cibernetică, 2021, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO, <a href="https://dnsc.ro/vezi/document/ghid-securitate-cibernetica-2021">https://dnsc.ro/vezi/document/ghid-securitate-cibernetica-2021</a></p>

## 9. Evaluare

Periodică		Curentă	Lucrul individual	Examen final
Atestarea 1	Atestarea 2			
15%	15%	15%	15%	40%
Standard minim de performanță				
Prezența și activitatea la prelegeri, lucrări de laborator;				
Obținerea notei minime de „5” la ambele atestări, activitatea curentă, lucrul individual;				
Obținerea notei minime de „5” la examenul final.				