

**TEHNOLOGII ALE SECURITĂȚII INFORMAȚIONALE**
**1. Date despre disciplină/modul**

<b>Facultatea</b>	<b>Facultatea Calculatoare, Informatică și Microelectronică</b>				
<b>Departamentul</b>	<b>INGINERIA SOFTWARE ȘI AUTOMATICĂ</b>				
<b>Ciclul de studii</b>	Studii superioare de licență, ciclul I				
<b>Programul de studii</b>	Tehnologia informației				
<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>
Anul II ( <i>învățământ cu frecvență</i> )	IV	E	D	-	4
Anul II ( <i>învățământ cu frecvență redusă</i> )	IV	E	D	-	4

**2. Timpul total estimat**

Total ore în planul de învățământ	Din care				
	Ore auditoriale		Lucrul individual		
	Curs	Laborator	Proiect de an	Studiul materialului teoretic	Pregătire aplicații
Învățământ cu frecvență	30	30	-	30	30
Învățământ cu frecvență redusă	12	12		48	48

**3. Precondiții de acces la disciplină/modul**

<b>Conform planului de învățământ</b>	Programarea calculatoarelor, Algebra liniară, Matematica discretă
<b>Conform competențelor</b>	Cunoștințe și abilități de operare cu sistemele informaționale, dispozitivele terminale

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

<b>Curs</b>	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector, calculator și acces la internet. Nu vor fi tolerate întârzierile studenților, precum și convorbirile telefonice în timpul cursului.
<b>Laborator/ seminar</b>	Studenții vor perfecta rapoarte conform condițiilor impuse de indicațiile 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. Competențe specifice acumulate**

<b>Competențe profesionale</b>	<p><b>CP1. Elaborarea și proiectarea arhitecturii</b></p> <p><b>2P.</b> Cerințele arhitecturii sistemelor: performanță, mentenabilitate, extensibilitate, scalabilitate, disponibilitate, securitate și accesibilitate.</p> <p><b>4P.</b> Arhitectura întreprinderii și standardele interne ale companiei.</p> <p><b>15P.</b> Utilizează cunoștințele sale tehnologice din diferite domenii pentru a elabora și implementa arhitectura întreprinderii.</p> <p><b>CP3. Integrarea componentelor</b></p> <p><b>1P.</b> Componente/module hardware/software, indiferent dacă sunt vechi, existente sau noi.</p> <p><b>18P.</b> Securizează și face backup-ul datelor pentru a asigura integritatea lor în timpul integrării datelor sau a sistemului.</p> <p><b>CP5. Implementarea soluțiilor</b></p> <p><b>5P.</b> Tehnologiile și standardele care se utilizează în timpul implementării/ /desfășurării.</p> <p><b>CP7. Ingineria sistemelor</b></p> <p><b>6P.</b> Bazele securității informației</p> <p><b>16P.</b> Conduce auditurile de gestionare a riscurilor și acționează pentru a reduce impactul acestora.</p> <p><b>17P.</b> Aplică arhitecturi software și/sau hardware adecvate.</p> <p><b>CP8. Managementul problemelor</b></p> <p><b>17P.</b> Alocă resurse adecvate activităților de întreținere, luând în considerare costurile și riscurile.</p>
--------------------------------	--

<b>Competențe transversale</b>	<b>22 T.</b> Demonstrează executarea responsabilă a sarcinilor profesionale în condiții de autonomie. <b>24 T.</b> Conștientizează nevoia de formare continuă cu utilizarea eficientă a resurselor și tehnicilor de învățare pentru dezvoltarea personală și profesională.
--------------------------------	---

## 6. Obiectivele disciplinei/modulului

<b>Obiectivul general</b>	Studierea elementelor de bază ale securității informațiilor, atât sub aspectul de management, cât și cel tehnic. 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. Studiarea elementelor de bază ale aplicării criptografiei în sistemele informaționale și a altor tehnologii de securizare.
<b>Obiectivele specifice</b>	<ul style="list-style-type: none"> <li>• Analiza atacurilor care se bazează pe factorul uman;</li> <li>• Cunoașterea și utilizarea tehnologiilor pentru asigurarea securității informaționale;</li> <li>• Evaluarea modelelor de amenințări și influența acestora asupra unei organizații;</li> <li>• Crearea politicilor de securitate relevante organizației și mediului;</li> <li>• Compararea diferitelor utilizări și abordări ale criptografiei;</li> <li>• Pregătirea și răspunsul la incidentele de securitate, securizarea sistemelor informaționale;</li> <li>• Studiarea atacurilor comune în rețea, controlul accesului.</li> </ul>

## 7. Conținutul disciplinei

Tematica activităților didactice	Numărul de ore	
	învățământ cu frecvență	învățământ cu frecvență redusă
<b>Tematica cursurilor</b>		
1. Prezentare generală a securității informaționale. Termeni de bază și definiții	2	0,5
2. Amenințări de securitate. Vulnerabilitatea sistemelor informaționale Programe malițioase	2	0,5
3. Atacuri asupra rețelelor de calculatoare	2	0,5
4. Atacuri asupra aplicațiilor și serviciilor web	2	0,5
5. Cubul McCumber. Principiile fundamentale ale securității informației	2	1
6. Principiul de confidențialitate. Criptarea simetrică. Algoritmi de criptare simetrică	2	1
7. Criptarea asimetrică. Algoritmi de criptare asimetrică	2	1
8. Controlul accesului. Tipuri și strategii de control al accesului	2	1
9. Principiul de integritate. Funcții criptografice hash	2	1
10. Semnătura digitală și certificate digitale	2	1
11. Principiul de disponibilitate. Tehnici pentru asigurarea disponibilității datelor	2	1
12. Tehnologii de securitate bazate pe software și hardware	2	1
13. Tehnologii de securitate bazate pe rețea și cloud	2	1
14. Politici, proceduri, standarde de securitate a informației	2	1
15. Sisteme de management al securității informației	2	0
<b>Total curs:</b>	<b>30</b>	<b>12</b>
<b>Tematica lucrărilor de laborator</b>		
LL1. Analiza programelor malware. Analiza statică și dinamică	2	0,5
Configurarea programelor antivirus	2	0,5
LL2. Tipuri de atacuri în SI. Analiza tehnicilor de inginerie socială	2	0,5
Capturarea și analiza traficului. Simularea atacurilor DoS	2	0,5
LL3. Configurarea drepturilor de acces în Windows și Linux	2	1
Instalarea și configurarea mașinii virtuale	2	1
LL4. Implementarea algoritmilor de criptare simetrică și asimetrică	2	1
Semnătura digitală	2	1
Algoritmii DES/AES, RSA	2	1
Studiu de caz	2	1
LL 5. Configurare firewall software și VPN	2	1

Tematica activităților didactice	Numărul de ore	
	învățământ cu frecvență	învățământ cu frecvență redusă
Studiul sistemelor bazate pe IDS și IPS	2	1
LL 6. Crearea politicilor de securitate bazate pe SMSI	2	1
Clasificarea activelor organizației. Definirea contextului	2	1
Politicile de Management a Riscurilor. Măsurile de control	2	0
<b>Total lucrări de laborator:</b>	<b>30</b>	<b>12</b>

### 8. Referințe bibliografice

<b>Principale</b>	<ol style="list-style-type: none"> <li>1. Michael E. Whitman and Herbert J. Mattord - Principles of Information Security, ISBN-13: 978-1337102063, 2013;</li> <li>2. Christof Paa and Jan Pelzl - Understanding Cryptography: A Textbook for Students and Practitioners, 2010. Springer;</li> <li>3. www.netacad.com,</li> <li>4. Anderson R. – Security Engineering : A Guide to Building Dependable Distributed Systems, NY,2001;</li> <li>5. Andress, M. – Surviving Security: How to Integrate People, Process and Technology, SAMS, Indianapolis, 2002;</li> <li>6. Davis D. – "The Problems Catch Up With The Solution", in Card Technology, April 2003;</li> <li>7. Ioan-Cosmin MIHAI – Securitatea informațiilor, Editura Sitech, 2012; ISBN 978-606-11-29203-4;</li> <li>8. King, C.M., Dalton, C.E., Osmanaglu, T.E. – Security Architecture: Design, Deployment&amp;Operations,Osborne/McGraw-Hill, New York, 2001;</li> <li>9. Krutz R.L, Vines R.D. – The CISSP Prep Guide – Mastering the Ten Domains of Computer Security, Wiley &amp; Sons, Inc. New York, 2001;</li> <li>10. Schwartan W. – Information Warfare, 2nd Edition , Thunder's Mouth Press, New York, 1996;</li> <li>11. Ioan-Cosmin MIHAI – Securitatea sistemului informatic, Editura Dunărea de Jos, 2007 ISBN 978-973-627-369-8;</li> <li>12. Victor Valeriu PATRICIU, Monica Ene PIETROSANU, Ion BICA, Justin PRIESCU – Semnături electronice și securitate informatică, Editura All, 2006;</li> <li>13. Aurel Serb, Constantin Baron, Narcisa Isaila, Securitatea informatica in societatea informationala, Bucuresti: Pro Universitaria, 2013;</li> <li>14. Smart N. Информационная безопасность, Moscova, Tehnosfera 2006;</li> <li>15. Steven M. Bellovin, Michael Merritt - Limitations of the Kerberos Authentication System, AT&amp;T Bell Labs,2010.</li> </ol>
<b>Suplimentare</b>	<ol style="list-style-type: none"> <li>1. Leitner Achim, "Rețele WLAN sigure, cu un tunel OpenVPN criptat", Linux Magazin, nr. 22, iunie 2005;</li> <li>2. OpenVPN: <a href="http://openvpn.sourceforge.net/">http:// openvpn. sourceforge. Net;</a></li> <li>3. Biblioteca LZO: <a href="http://www.oberhumer.com/opensource/lzo/">http:// www. oberhumer. com/opensource/ lzo/;</a></li> <li>4. Proiect OpenSSL: <a href="http://www.openssl.org/">http:// www. openssl. org/;</a> Driver TUN/ TAP: <a href="http://vtun.sourceforge.net/tun/">http:// vtun. sourceforge. net/ tun/;</a></li> <li>5. Thomas T., Primii pași în securitatea rețelelor, Corint, București, 2005;</li> <li>6. Lachi A., Securitatea Sistemelor Informaționale, Partea I, Îndrumar de laborator, UTM, Chișinău, 2011;</li> <li>7. Lachi A., Securitatea Sistemelor Informaționale, Partea I, Îndrumar de laborator, UTM, Chișinău, 2015;</li> <li>8. <a href="http://www.squid-cache.org">www.squid-cache.org</a></li> <li>9. <a href="http://www.wingate.com/download.php">http://www.wingate.com/download.php</a></li> </ol>

## 9. Evaluare

Periodică		Curentă	Studiu individual	Proiect/teză	Examen
EP 1	EP 2				
<b>Învățământ cu frecvență</b>					
15%	15%	15%	15%		40%
<b>Învățământ cu frecvență redusă</b>					
25%			25%		50%
Standard minim de performanță:					
<ul style="list-style-type: none"> <li>• Prezența și activitatea la cursuri, lucrări de laborator;</li> <li>• Obținerea notei minime de „5” la evaluările periodice, activitatea curentă, lucrul individual;</li> <li>• Obținerea notei minime de „5” la examenul final.</li> </ul>					

## 10. Criterii de evaluare

Activitate	Componente evaluare	Metodă de evaluare, Criterii de evaluare	Pondere în nota finală a activității	Ponderea în evaluarea disciplinei
<b>Învățământ cu frecvență</b>				
<b>Evaluare periodică I</b>	Conținut teoretic, teme 1-7	Test pe platforma Moodle	100%	<b>15%</b>
<b>Evaluare periodică II</b>	Conținut teoretic, teme 8-15	Test pe platforma Moodle	100%	<b>15%</b>
<b>Evaluare curentă</b>	Activitatea practică	Susținerea lucrărilor de laborator	50%	<b>15%</b>
		Implicarea în procesul de învățare activă la cursuri	25%	
		Rezultatele mini-testelor curente realizate la orele de curs	25%	
<b>Studiul individual</b>	Sarcina 1: Crearea mindmap-urilor la temele studiate la curs	Prezentare/discurs public	50%	<b>15%</b>
	Sarcina 2: Realizarea a 2 politici de securitate pentru o organizație	Portofoliu prezentat spre evaluare	50%	
<b>Evaluarea finală</b>	Conținut teoretic și practic	Examen scris, în baza biletului individual	100%	<b>40%</b>
<b>Învățământ cu frecvență redusă</b>				
<b>Evaluare periodică I</b>	Conținut teoretic, teme 1-7	Test pe platforma Moodle	100%	<b>10%</b>
<b>Evaluare periodică II</b>	Conținut teoretic, teme 8-15	Test pe platforma Moodle	100%	<b>10%</b>
<b>Evaluare curentă</b>	Activitatea practică	Susținerea lucrărilor de laborator	50%	<b>5%</b>
		Implicarea în procesul de învățare activă la cursuri	25%	
		Rezultatele mini-testelor curente realizate la orele de curs	25%	
<b>Studiul individual</b>	Sarcina 1: Crearea mindmap-urilor la temele studiate la curs	Prezentare/discurs public	50%	<b>25%</b>
	Sarcina 2: Realizarea a 2 politici de securitate pentru o organizație	Portofoliu prezentat spre evaluare	50%	
<b>Evaluarea finală</b>	Conținut teoretic și practic	Examen scris, în baza biletului individual	100%	<b>50%</b>