TEHNOLOGII ALE SECURITĂȚII INFORMAȚIONALE

1. Date despre disciplină/modul

Facultatea	**Facultatea Calculatoare, Informatică și Microelectronică**				
Departamentul	**INGINERIA SOFTWARE ŞI AUTOMATICĂ**				
Ciclul de studii	Studii superioare de licenţă, ciclul I				
Programul de studii	3.5 Informatica aplicată				
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/ seminar	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, 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. Studierea elementelor de bază ale aplicării criptografiei în sistemele informaționale și a altor tehnologii de securizare.
Obiectivele specifice	• *Analiza atacurilor care se bazează pe factorul uman;* • *Cunoașterea și utilizarea tehnologiilor pentru asigurarea securității informaționale;* • *Evaluarea modelelor de amenințări și influența acestora asupra unei organizații;* • *Crearea politicilor de securitate relevante organizației și mediului;* • *Compararea diferitelor utilizări și abordări ale criptografiei;* • *Pregătirea și răspunsul la incidentele de securitate, securizarea sistemelor informaționale;* • *Studierea atacurilor comune în rețea, controlul accesului.*

7. Conţinutul disciplinei

Tematica activităţilor didactice	**Numărul de ore**
	învăţământ cu frecvenţă
1. Prezentare generală a securității informaționale.	**2**
2. Bazele securității informaționale și importanța factorului uman	**2**
3. Securitatea informației în sistemele informaționale	**2**
4. Securitatea informației pentru dispozitivele terminale	**2**
5. Tehnologii ale securității informaționale: Firewall și VPN	**2**
6. Tehnologii ale securității informaționale: Sisteme de detecție a intruziunilor, controlul accesului și alte instrumente	**2**
7. Securitatea informației și criptografia	**2**
8. Criptografia simetrică. Algoritmi și standarde de criptare simetrică	**2**
9. Criptografia asimetrică. Algoritmi și standard de criptare asimetrică	**2**
10. Integritatea datelor și semnătura digitală	**2**
11. Riscul managementului de securitate	**2**
12. Aspecte practice ale managementului riscului	**2**
13. Managementul riscului de Securitate într-o organizație	**2**
14. Politici, proceduri și standarde de securitate	**2**
15. Discuții finale	**2**
Total curs:	**30**
LL1. Analiza incidentelor de securitate cu impact major din ultimii 5 ani.	**2**
LL2. Explorarea tehnicilor de inginerie socială.	**2**
LL3. Configurarea unui mediu cibernetic protejat.	**2**
LL4. Configurarea politicilor locale de securitate în Windows	**2**
LL5. Configurare Windows Firewall. Configurarea modului de transport VPN	**2**
LL6. Instalarea mașinii virtuale Ubuntu pe PC. Configurarea mecanismelor de autentificare, autorizare și contabilizare.	**2**
LL7. Criptarea fișierelor și datelor.	**2**
LL8. Utilizarea criptării simetrice.	**2**
LL9. Utilizarea verificărilor de integritate a datelor și fișierelor	**2**
LL10. Utilizarea semnăturilor digitale	**2**
LL11. Identificarea activelor informaționale. Detectarea amenințărilor și vulnerabilităților de securitate	**2**
LL12. Evaluarea riscului informațional. Completarea planului de tratare a riscului informațional	**2**
LL13. Crearea unui SMSI pentru o organizație	**2**
LL14. Crearea unei politici generice și a unei politici specifice pentru organizație	**2**
LL15. Prezentarea rezultatelor obținute	**2**
Total lucrări de laborator:	**30**

8. Referinţe bibliografice

Principale	**1.** Michael E. Whitman and Herbert J. Mattord - Principles of Information Security, ISBN-13: 978-1337102063, 2013; **2.** Christof Paa and Jan Pelzl - Understanding Cryptography: A Textbook for Students and Practitioners, 2010. Springer; **3.** www.netacad.com, **4.** Anderson R. – Security Engineering : A Guide to Building Dependable Distributed Systems, NY,2001; **5.** Andress, M. – Surviving Security: How to Integrate People, Process and Technology, SAMS, Indianapolis, 2002; **6.** Davis D. – "The Problems Catch Up With The Solution", in Card Technology, April 2003; **7.** Ioan-Cosmin MIHAI – Securitatea informațiilor, Editura Sitech, 2012; ISBN 978-606-11-29203-4; **8.** King, C.M., Dalton, C.E., Osmanaglu, T.E. – Security Arhitecture: Design, Deployment&Operations,Osborne/McGraw-Hill, New York, 2001; **9.** Krutz R.L, Vines R.D. – The CISSP Prep Guide – Mastering the Ten Domains of Computer Security, Wiley & Sons, Inc. New York, 2001; **10.** Schwartan W. – Information Warfare, 2nd Edition , Thunder's Mouth Press, New York, 1996; **11.** Ioan-Cosmin MIHAI – Securitatea sistemului informatic, Editura Dunărea de Jos, 2007 ISBN 978-973-627-369-8; **12.** Victor Valeriu PATRICIU, Monica Ene PIETROSANU, Ion BICA, Justin PRIESCU – Semnături electronice și securitate informatică, Editura All, 2006; **13.** Aurel Serb, Constantin Baron, Narcisa Isaila, Securitatea informatica in societatea informationala, Bucuresti: Pro Universitaria, 2013; **14.** Smart N. Информационная безопасность, Moscova, Tehnosfera 2006; **15.** Steven M. Bellovin, Michael Merritt - Limitations of the Kerberos Authentication System, AT&T Bell Labs,2010.
Suplimentare	1. Leitner Achim, "Reţele WLAN sigure, cu un tunel OpenVPN criptat", Linux Magazin, nr. 22, iunie 2005; 2. OpenVPN: http:// openvpn. sourceforge. Net; 3. Biblioteca LZO: http:// www. oberhumer. com/opensource/ lzo/; 4. Proiect OpenSSL: http:// www. openssl. org/; Driver TUN/ TAP: http:// vtun. sourceforge. net/ tun/; 5. Thomas T., Primii paşi în securitatea reţelelor, Corint, Bucureşti, 2005; 6. Lachi A., Securitatea Sistemelor Informaționale, Partea I, Îndrumar de laborator, UTM, Chișinău, 2011; 7. Lachi A., Securitatea Sistemelor Informaționale, Partea I, Îndrumar de laborator, UTM, Chișinău, 2015; 8. www.squid-cache.org 9. http://www.wingate.com/download.php

9. 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.					

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 1-7	Test pe platforma Moodle	100%	**15%**
Evaluare periodică II	Conținut teoretic, teme 8-15	Test pe platforma Moodle	100%	**15%**
Evaluare curentă	Activitatea practică	Susținerea lucrărilor de laborator	50%	**15%**
		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: Realizarea a 2 politici de securitate pentru o organizație	Portofoliu prezentat spre evaluare	50%	
Evaluarea finală	Conținut teoretic și prcatic	Examen scris, în baza biletului individual	100%	**40%**