

FUNDAMENTE ALE SECURITĂȚII CIBERNETICE

1. Date despre unitatea de curs

Facultatea	Calculatoare, Informatică și Microelectronică				
Catedra/Departamentul	Ingineria Software și Automatică				
Ciclul de studii	Studii superioare de master, ciclul II				
Programul de studii	Tehnologia informației pentru afaceri				
Anul de studii	Semestrul	Tip de evaluare	Categoria formativă	Categoria de opționalitate	Credite ECTS
II (învățământ cu frecvență);	3	E-examen	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 aplicații
150	20	20	-	110	-

3. Precondiții de acces la unitatea de curs

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. Condiții de desfășurare a procesului educațional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector și calculator
Laborator/Seminar	Vor fi perfectate rapoarte ale rezultatelor primite conform condițiilor impuse de indicațiile metodice

5. Competențe specifice acumulate

Competențe profesionale	C1 Operarea cu concepte și metode ale domeniului Tehnologiei Informației C2 Aspecte organizaționale și informaționale ale sistemelor
Competențe transversale	CT1. Aplicarea principiilor, normelor și valorilor eticii profesionale CT2. Identificarea, descrierea și derularea activităților organizate într-o echipă cu dezvoltarea capacităților de comunicare și colaborare, dar și cu asumarea diferitelor roluri (de execuție și conducere) CT3. Demonstrarea spiritului de inițiativă și acțiune pentru actualizarea propriilor cunoștințe profesionale, economice și de cultura organizațională

6. Obiectivele unității de curs

Obiectivul general	Însușirea conceptelor, metodelor și tehnologiilor fundamentale de securitate cibernetică
Obiectivele specifice	Să înțeleagă și să descrie conceptele de bază ale Securității cibernetice Să cunoască tipurile de amenințări asupra infrastructurii informaționale Să însușească și să selecteze tehnologii adecvate protecției informaționale Să aplice corect metodele de protecție în baza legislației din domeniul Securității cibernetice

7. Conținutul unității de curs

Tematica cursului	Numărul de ore
	învățământ cu frecvență
T1. Concepte generale privind Securitatea cibernetică. Obiectul de studiu al securității cibernetică. Atribute ale securității informațiilor. Nivelele de structurare a conceptului de Securitate cibernetică. Aspecte juridice privind securitatea cibernetică. Reglementări legislative pe plan național și internațional privind protecția datelor cu caracter personal și accesul la informații. Legislația internațională privind securitatea și protecția în spațiul cibernetic. Protecția drepturilor de autor (Copyright).	4
T2. Aspectul organizatoric de asigurare a securității informaționale. Introducere în standardizare. Evoluția standardelor de securitate. Aspecte ale familiei de standarde ISO/IEC 27000. Măsurile administrative de protecție a informației. Politici de securitate informațională. Măsurile procedurale de protecție a informației.	4
T3. Vulnerabilități și amenințări la adresa securității informației. Noțiuni de amenințare la adresa securității informației. Identificarea amenințărilor. Software-ul rău intenționat. Alte tipuri de amenințări (atacuri la adresa securității informației). Vulnerabilități de securitate a informației. Risc de securitate a informației. Managementul vulnerabilităților și evaluarea riscurilor în domeniul securității informatice.	4
T4. Metode criptografice de protecție a informației. Obiective și noțiuni de bază ale criptografiei. Evoluția și clasificarea metodelor criptografice. Criptografia modernă. Cifruri cu cheie privată. Cifruri cu cheie publică. Domenii de aplicabilitate. Exemple. Semnături digitale. Infrastructura cheilor publice (PKI). Componentele și funcțiile PKI. Politica de utilizare a certificatelor digitale. Steganografia. Filigranarea.	4
T5. Măsurile generale pentru asigurarea securității cibernetică. Securitatea fizică. Controlul logic al accesului în sistemele informaționale. Identificarea, autentificarea și autorizarea. Managementul parolelor. Modele comune de control al accesului. Jurnalizarea. Securitatea personalului. Asigurarea continuității afacerii. Planificarea pentru backup-uri și restabilirea informațiilor în caz de dezastru.	4
Total ore curs:	20
Tematica lucrărilor de laborator/seminarelor	
LP1. Analiza riscurilor de securitate. Riscuri ce pot afecta confidențialitatea, integritatea, disponibilitatea, non-repudierea.	4
LP2. Analiza controalelor de securitate ale standardului ISO/IEC 27001 (Anexa A). Studiu de caz referitor la corespunderea stării lucrurilor cu controalele de securitate la o întreprindere concretă	4
LP3.. Elaborarea proiectului unei politici de utilizare acceptabile a întreprinderii. Motivarea punctelor cheie prin exemplificarea unor incidente de securitate conexe.	4
LP4. Tehnologii de criptare. Criptare simetrică. Criptare asimetrică. Semnătura digitală. Certificate SSL/TLS. Instrumente stenografice.	4
LP5. Planul de backup și recuperare în caz de dezastru. Elaborarea proiectului unui plan de backup și recuperare în caz de dezastru. Lucrul cu copiile de siguranță și restabilirea informațiilor. Analiza sistemelor de backup și recuperare. Instrumente native de backup în sistemele de operare.	4
Total ore practice:	20

8. Referințe bibliografice

Principale	1. Aurel Șerb, Constantin Baron, Narcisa Isăilă, <i>Securitatea informatică în societatea informațională</i>, București : Pro Universitaria, 2013. – 546 p. 2. Aureliu Zgureanu, <i>Bazele securității informației</i>. Manual. Ch.: ASEM, 2018, 242 p. 3. Constantinescu Zoran, Gabriela Moise, <i>Criptarea informației : ghid practice</i>, Ploiești : Ed. Univ. 2. Petrol-Gaze din Ploiești, 2013. – 120 p. 4. Stelian Flonta, Victor Valeriu Patriciu, Liviu Cristian Miclea, <i>Metode criptografice pentru sisteme structurate</i>, Cluj-Napoca : U.T.Press, 2011. – 260 p. 5. Dumitru Oprea, <i>Protecția și securitatea informațiilor</i>. Ed. II, Polirom, Iași, 2007. – 445 p. 6. Popa Sorin Eugen, <i>Securitatea sistemelor informatice</i>, Bacău, 2007. – 136 p. 7. N.Ploteanu, S.Maftea, R.Griniuc, A.Coțofană, <i>Pasul II în ciberspațiu: Securitatea Informațională</i>, Academia „Ștefan cel Mare”, Chișinău, 2008. – 336 p. 8. Mark Stamp, <i>Information security. Principles and Practice</i>, Second Edition, SanJose State University, AJOHN WILEY&SONS, USA, 2011. - 608 p. 9. Luminița Scripcariu, Ion Bogdan etc., <i>Securitatea rețelelor de comunicații</i>, Casa de editură Venus, Iași, 2008. - 193 p.
Suplimentare	1. Ion Bica, Victor Valeriu Patriciu, <i>Securitatea Comertului Electronic</i>, Editura All, București, 2001. 2. Valentin Matyger, <i>Securitatea Informației în rețelele de calculatoare</i>, Endava, 2010. 3. <i>Protecția datelor cu caracter personal</i>, Documente ale Consiliului Europei, Chișinău, Biroul de Informații al Consiliului Europei în Moldova, 2001. 4. Constantin Popescu, <i>Introducere în Criptografie</i>, http://webhost.uoradea.ro/cpopescu/

9. Evaluare

Periodică		Curentă	Studiu individual	Proiect/teză	Examen
EP 1	EP 2				
10%	10%	10%	30%	-	40%

Standard minim de performanță
Prezența și activitățile la prelegeri și lucrări practice. Obținerea notei minime de „5” la fiecare dintre lucrări și examen

10. Criterii de evaluare

Activitate	Componente evaluare	Metodă de evaluare, Criterii de evaluare	Pondere în nota finală a activității	Ponderea în evaluarea disciplinei
Evaluare periodică I	Conținut teoretic, teme 1-2	Test pe MOODLE	100%	10%
Evaluare periodică II	Conținut teoretic, teme 3-5	Test pe MOODLE	100%	10%
Evaluare curentă	Lucrări practice	Discuții în cadrul lecțiilor practice	50%	10%
		Dosar completat cu Rapoarte pentru fiecare Studiu de caz în discuție	50%	
Studiul individual	Teme individuale	Prezentare/discurs public	100%	30%
Evaluarea finală	Conținut teoretic și practic	Test pe MOODLE. Notare conform baremului	100%	40%