ROMÂNIA
UNIVERSITATEA BABEŞ-BOLYAI CLUJ-NAPOCA
FACULTATEA DE ISTORIE ŞI FILOSOFIE
DEPARTAMENTUL STUDII INTERNAŢIONALE ŞI ISTORIE CONTEMPORANĂ

FIŞA DISCIPLINEI

Managementul securității sistemelor informatice

1. Date despre program

1.1. Instituţia de învăţământ superior	Universitatea Babeş-Bolyai Cluj-Napoca
1.2. Facultatea	Facultatea de Istorie şi Filosofie
1.3. Departamentul	Studii Internaţionale şi Istorie Contemporană
1.4. Domeniul de studii	Științe politice
1.5. Ciclul de studii	Masterat
1.6. Programul de studii / Calificarea	MSSC / SICO

2. Date despre disciplină

2.1. Denumirea disciplinei				Managementul securității sistemelor informatice			
2.2. Titularul activităţilor de curs							
2.3. Titularul activităţilor de seminar							
2.4. Anul de studiu	2	2.5. Semestrul	2	2.6. Tipul de evaluare	Examen sc	2.7. Regimul disciplinei	DS

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1. Număr de ore pe săptămână	3	Din care 3.2. curs	2	Din care 3.3. seminar/ laborator	1
3.4. Total ore din planul de învăţământ	42	Din care 3.5. curs	28	Din care 3.6. seminar/ laborator	14
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					24
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					24
Pregătire seminarii/ laboratoare, teme, referate, portofolii si eseuri					27
Tutoriat					4
Examinări					4
Alte activităţi:……..					
3.7. Total ore studiu individual					83
3.8. Total ore pe semestru					125
3.9. Numărul de credite					5

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	nu este cazul
4.2. de competenţe	nu este cazul

5. **Condiţii** (acolo unde este cazul)

5.1. de desfăşurare a cursului	nu este cazul
5.2. de desfăşurare a seminarului/ laboratorului	nu este cazul

6. **Competenţele specifice acumulate**

Competenţe profesionale	* Culegerea, verificarea şi colectarea datelor privind securitatea sistemelor informatice/cibernetice. * Utilizarea cunoștințelor acumulate pentru interpretarea incidentelor de securitate cibernetică și luarea timpurie a deciziilor. * Cunoașterea metodelor și tehnicilor de avertizare timpurie, asigurarea continuității și răspuns la incidente de securitate cibernetică. * Elaborarea și planificarea activităților circumscrise securității sistemelor informatice/cibernetice.
Competenţe transversale	* Oferirea de expertiză în domeniul elaborării documentațiilor de evaluare, audit și analiză a securității sistemelor informatice/cibernetice. * Stabilirea strategiei, obiectivelor și cadrului de management în domeniul securității informației, armonizate cu strategia organizației.

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Formarea abilităților necesare managementului securității sistemelor, infrastructurilor și terminalelor cibernetice în organizații.
7.2 Obiectivele specifice	Dobândirea deprinderilor necesare gestionării în condiții optime a securității cibernetice în organizații. Dezvoltarea abilităților necesare identificării timpurii a riscurilor, vulnerabilităților și amenințărilor la adresa securității sistemelor informatice/cibernetice. Dezvoltarea abilităților necesare elaborării de politici și strategii de securitate cibernetică Dezvoltarea culturii de securitate cibernetică a cursanților.

8. **Conţinuturi**

8.1 Curs	**Metode de predare**	**Observații**
Noțiuni introductive. Terminologie și concepte	Prelegerea, explicarea	
Dimensiunea informatică și cibernetică a managementului securității în organizații	Prelegerea, explicarea	
Noțiuni introductive privind sistemele informatice din cadrul organizațiilor	Prelegerea, explicarea	
Sisteme de management a securității sistemelor informatice	Prelegerea, explicarea	
Riscuri, amenințări, vulnerabilități și oportunități specifice	Prelegerea, explicarea	

Responsabilitățile personalului desemnat	Prelegerea, explicarea	
Evaluarea și auditul securității sistemelor informatice	Prelegerea, explicarea	
Incidentele de securitate informatică	Prelegerea, explicarea	
Asigurarea continuității post-incident	Prelegerea, explicarea	
Securitatea cibernetică a personalului	Prelegerea, explicarea	
Securitatea cibernetică a facilităților	Prelegerea, explicarea	
Structuri de de securitate informatică / cibernetică: SOC, CERT, CSIRT	Prelegerea, explicarea	
Planificarea și managementul SOC	Prelegerea, explicarea	
Dezvoltarea și managementul politicilor de securitate informatică	Prelegerea, explicarea	

Bibliografie

ISACA, Cybersecurity Fundamentals Glossary, 2014.
ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems.
David Nathans, Designing and Building A Security Operations Center, Waltham, Elsevier, 2015.
Joseph Muniz, Gary McIntyre, Nadhem AlFardan, Security Operations Center, Indianapolis, Cisco Press, 2016.
Melissa Higgins (author);M. G Higgins ; Joshua J. Pauli (contributors), Cybersecurity, Minneapolis, Abdo Publishing, 2016.
John Sammons, Michael Cross, The basics of cyber safety: computer and mobile device safety made easy, Amsterdam, Elsevier, 2017.
Charles J. Brooks, Philip Craig, Donald Short Somerset, Cybersecurity essentials, John Wiley & Sons, 2018.
Bart McDonough, Cyber smart: five habits to protect your family, money, and identity from cyber criminals, Indianapolis, Wiley, 2019.
Erdal Ozkaya, Cybersecurity: the beginner's guide : a comprehensive guide to getting started in cybersecurity, Birmingham, Packt, 2019.

—
Glosar de termeni utilizați în securitatea cibernetică (CERT-RO)
Ghid – Amenințări generice la adresa securității cibernetice (CERT-RO)
Ghid – Cum să te ferești de viruși, viermi și troieni (CERT-RO)
Ghid – Securitatea utilizatorului final (CERT-RO)
Cod de bune practici pentru Securitatea Sistemelor Informatice și de Comunicații (CERT-RO)
Ghid referitor la rolul structurilor de tip CERT şi utilitatea CERT-urilor private (CERT-RO)
Raport de evaluare privind cea de a şaptea rundă de evaluări reciproce „Punerea în aplicare la nivel practic şi funcţionarea politicilor europene de prevenire şi de combatere a criminalităţii informatice” - Raport privind România (DECLASIFICAT)
Ghid – securitatea terminalelor mobile (CERT-RO)
Ghid – Securitatea în rețele sociale şi controlul parental în mediul online (CERT-RO)

8.2 Seminar / laborator	Metode de predare	Observații
Organizarea securității sistemelor informatice - Partea I		
Organizarea securității sistemelor informatice - Partea a II-a		
Culegerea datelor privind securitatea sistemelor informatice		
Cerințe minime de securitate informatică		
Evaluarea și analiza datelor privind securitatea sistemelor informatice		
Mentenanța sistemelor informatice		
Managementul incidentelor de securitate informatică		
Asigurarea continuității sistemelor informatice		
Instrumente automate de audit și diagnoză a securității sistemelor informatice		
Exercițiu practic: detecția timpurie și răspunsul la un incident minor		
Exercițiu practic: detecția timpurie și răspunsul la un incident major		
Exercițiu practic – Elaborarea raportului de audit și diagnoză - Partea I		
Exercițiu practic – Elaborarea raportului de audit și diagnoză - Partea II		
Recapitulare		

Bibliografie

ISACA, Cybersecurity Fundamentals Glossary, 2014.
ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems.
David Nathans, Designing and Building A Security Operations Center, Waltham, Elsevier, 2015.
Joseph Muniz, Gary McIntyre, Nadhem AlFardan, Security Operations Center, Indianapolis, Cisco Press, 2016.
Melissa Higgins (author);M. G Higgins ; Joshua J. Pauli (contributors), Cybersecurity, Minneapolis, Abdo Publishing, 2016.
John Sammons, Michael Cross, The basics of cyber safety: computer and mobile device safety made easy, Amsterdam, Elsevier, 2017.
Charles J. Brooks, Philip Craig, Donald Short Somerset, Cybersecurity essentials, John Wiley & Sons, 2018.
Bart McDonough, Cyber smart: five habits to protect your family, money, and identity from cyber criminals, Indianapolis, Wiley, 2019.
Erdal Ozkaya, Cybersecurity: the beginner's guide : a comprehensive guide to getting started in cybersecurity, Birmingham, Packt, 2019.

—
Glosar de termeni utilizați în securitatea cibernetică (CERT-RO)
Ghid – Amenințări generice la adresa securității cibernetice (CERT-RO)
Ghid – Cum să te ferești de viruși, viermi și troieni (CERT-RO)
Ghid – Securitatea utilizatorului final (CERT-RO)
Cod de bune practici pentru Securitatea Sistemelor Informatice și de Comunicații (CERT-RO)
Ghid referitor la rolul structurilor de tip CERT şi utilitatea CERT-urilor private (CERT-RO)
Raport de evaluare privind cea de a şaptea rundă de evaluări reciproce „Punerea în aplicare la nivel practic şi funcţionarea politicilor europene de prevenire şi de combatere a criminalităţii informatice” - Raport privind România (DECLASIFICAT)
Ghid – securitatea terminalelor mobile (CERT-RO)
Ghid – Securitatea în rețele sociale şi controlul parental în mediul online (CERT-RO)

9. Coroborarea conţinuturilor disciplinei cu aşteptarile reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului

Disciplina a fost elaborată în concordanţă cu lucrările din domeniu, publicate în ţară şi străinatate.

10. Evaluare

Tip de activitate	10.1. Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Examen	Lucrare scrisă descriptivă	50%
10.5. Seminar/ laborator	Elaborarea lucrărilor de seminar	Proiect practice și lucrări scrise descriptive	50%
	Oficiu		0
10.6. Standard minim de performanţă			
Răspunsurile să nu cuprindă erori grave. Activitate minimă în timpul semestrului, însemnând participare la activităţi în cadrul seminarilor și prezenţă 75 % la seminarii. Capacitate de descriere a problematicilor, dar fără surprinderea semnificaţiei acestora.			

Data completării: Semnătura titularului de curs: Semnătura titularului de seminar:

....

Data avizării în departament Semnătura directorului de departament

....