

FIȘA DISCIPLINEI

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea de Vest din Timișoara
1.2. Facultatea	Științe Politice, Filosofie și Științe ale Comunicării
1.3. Departamentul	Științe Politice
1.4. Domeniul de studii	Studii de Securitate Globală
1.5. Ciclul de studii	Master
1.6. Programul de studii / calificarea*	Studii de Securitate Globală / Consultant

2. Date despre disciplină

2.1. Denumirea disciplinei	Securitatea Cibernetică						
2.2. Titularul activităților de curs	Lector Dr. Stelian Mihaș						
2.3. Titularul activităților de seminar	Lector Dr. Stelian Mihaș						
2.4. Anul de studii	2	2.5. Semestrul	2	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	DA

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

3.1. Număr de ore pe săptămână	3	din care: 3.2 curs	2	3.3. seminar/laborator	1
3.4. Total ore din planul de învățământ	42	din care: 3.5 curs	28	3.6. seminar/laborator	14
Distribuția fondului de timp*					ore
Studiu după manual, suport de curs, bibliografie și notițe					14
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate					28
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					14
Examinări					7
Tutorat					14
3.7. Total ore studiu individual	77				
3.8. Total ore pe semestru	119				
3.9. Număr de credite	6				

4. Precondiții (acolo unde e cazul)

4.1. de curriculum	
4.2. de competențe	

5. Condiții (acolo unde e cazul)

5.1. de desfășurare a cursului	Conexiune internet, cod Google Classroom: dmw6sig, link: https://classroom.google.com/u/1/c/NjA0Mzg0MjU2MTda Link Meet: https://meet.google.com/lookup/b23h5heneb
--------------------------------	--

5.2. de desfășurare a seminarului / laboratorului	Conexiune internet, cod Google Classroom: whc3dco, link: https://classroom.google.com/u/1/c/Mjc4MTQ3MTY1OTAw Link Meet: https://meet.google.com/lookup/drfljjsky
---	--

6. Competențe specifice acumulate

Competențe profesionale	<ul style="list-style-type: none"> • Cunoașterea principalelor probleme de actualitate și a tendințelor în domeniul securității cibernetice • Cunoașterea și capacitatea de a aplica metodele de încriptare și decriptare • Abilitatea de a aplica funcțiile de hash pentru verificarea integrității unui mesaj sau a unui fișier • Abilitatea de a utiliza certificatele digitale în procesul de autentificare și de comunicare securizată • Recunoașterea importanței stocării distribuite a datelor precum și a procedurilor de backup și restaurare • Cunoașterea metodelor biometrice de identificare • Cunoașterea și utilizarea metodelor electronice de autentificare și de confirmare a identității • Abilitatea de a identifica, preveni și bloca amenințările specifice ale internetului – viruși, troieni, phishing, spoofing, pharming, ransomware, software exploits
Competențe transversale	<ul style="list-style-type: none"> • Conștientizarea importanței protecției datelor, în general • Înțelegerea necesității de a fi la curent cu ultimele noutăți și tehnologii de transmitere, stocare și protecție a datelor • Înțelegerea necesității comunicării securizate viața de zi cu zi • Recunoașterea amenințărilor de securitate și a necesității de a implementa măsuri de prevenire și contracarare a acestora

7. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

7.1 Obiectivul general al disciplinei	<ul style="list-style-type: none"> • Cunoașterea și dobândirea abilităților de utilizare a principalelor concepte de securitate – funcții de hash, protocoale de partajare a cheilor, algoritmi de încriptare/decriptare a datelor, semnăturile și certificatele digitale, infrastructura cheilor publice, principiile protecției datelor precum și comunicarea securizată
7.2 Obiectivele specifice	<ul style="list-style-type: none"> • Cunoașterea și aplicarea principalelor metode de încriptare și decriptare a mesajelor precum și metode de partajare a cheilor • Înțelegerea naturii amenințărilor de securitate • Abilitatea de a recunoaște și a preveni amenințările de securitate • Abilitatea de a implementa modalități de comunicare securizată • Implementarea măsurilor elementare de protecție a sistemelor

	<p>de calcul, de backup și restaurare a datelor</p> <ul style="list-style-type: none"> • Cunoașterea principalelor metode de plăți electronice și a nivelului de securitate pe care îl oferă
--	---

8. Conținuturi*

8.1. Curs	Metode de predare	Observații
01 – Probleme de actualitate și tendințe în domeniul securității cibernetice	Prelegere, conversație, exemplificare	
02 – Puncte de reper istorice în evoluția comunicării securizate	Prelegere, conversație, exemplificare	
03 – Elemente de criptografie, funcții hash – MD5, SHA-1	Prelegere, conversație, exemplificare	
04 – Sisteme de criptare cu cheie simetrică – DES, AES	Prelegere, conversație, exemplificare	
05 – Algoritmul Diffie-Hellman, sisteme de criptare cu cheie asimetrică – RSA	Prelegere, conversație, exemplificare	
06 – Infrastructura cheilor publice, autorități de certificare	Prelegere, conversație, exemplificare	
07 – Standardul de semnătură digitală	Prelegere, conversație, exemplificare	
08 – Comunicarea securizată – VPN, SSL/TLS, SSH	Prelegere, conversație, exemplificare	
09 – Sisteme securizate de stocare – protecția datelor	Prelegere, conversație, exemplificare	
10 – Viruși, troieni, ransomware, exemple, protecție	Prelegere, conversație, exemplificare	
11 – Phishing, pharming, software exploits	Prelegere, conversație, exemplificare	
12 – Reguli practice de protecție	Prelegere, conversație, exemplificare	
13 – Sisteme de autentificare, carduri inteligente, identificare biometrică	Prelegere, conversație, exemplificare	
14 – Atacuri cibernetice sponsorizate guvernamental	Prelegere, conversație, exemplificare	
<p>Bibliografie</p> <ol style="list-style-type: none"> 1. L. Batten, Public Key Cryptography Applications and Attacks, John Wiley and Sons, New Jersey, 2013. 2. Specificația SHA-1 – FIPS 180-2 - http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-2.pdf 3. Specificația AES – FIPS 197 - https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf 		

4. On the security of cloud storage services – Fraunhofer SIT Technical Report, 2012
5. Building and implementing a successful information security policy – Dancho Dancev, Internet Software Marketing, Ltd., 2003
6. ICT Security Standards – Herbert Rwamibazi, EAST AFRITAC IFMIS Rwanda Workshop, 2012
7. Introducing Traffic Analysis, Attacks, Defenses and Public Policy Issues - <http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/TAIntro.pdf>
8. Digital Signature Standard (DSS), <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>
9. Introduction to public key infrastructure - <http://www.tomsitpro.com/articles/public-key-infrastructure-introduction,2-884.html>
10. Introduction to Computer Information Systems/E-Commerce - https://en.wikibooks.org/wiki/Introduction_to_Computer_Information_Systems/E-Commerce

8.2. Seminar/laborator	Metode de predare/ învățare	Observații
1 – Codul naval al SUA în cel de-al doilea război mondial	Proiectele vor fi implementate / prezentate de către echipe de 1-3 studenți. Fiecare echipă va utiliza atât resursele sugerate cât și resursele pe care le vor descoperi și le vor considera necesare pentru implementarea proiectului.	
2 – Wehrmacht Enigma		
3 – Generarea certificatelor digitale		
4 – Detalierea procesului de configurare a stațiilor de lucru pentru comunicare securizată		
5 – Definierea profilului personal și a mecanismelor de confirmare și verificare a conținutului său		
6 – Atacuri cibernetice. Studiu de caz (Coreea de Nord sau Rusia)		
7 – Implementarea standardului de semnătură digitală		

Bibliografie

1. Glossary of US Naval Code Words - <https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/g/glossary-of-us-naval-code-words-navexos-p-4740.html>
2. Mașina Enigma - https://ro.wikipedia.org/wiki/Ma%C8%99ina_Enigma
3. Digital Signature Standard (DSS) - <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>
4. Digital Certificates explained - <http://www.steves-internet-guide.com/ssl-certificates-explained/>

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului

Acest curs, prin competențele pe care le edifică și prin lărgirea orizontului de cunoaștere pe care îl implică reprezintă un prim pas consistent pentru un viitor analist sau consultant de securitate în definirea și implementarea politicilor de securitate a datelor în diferite domenii și la diferite nivele de securitate. Conținutul este în mare măsură în concordanță cu structura cursurilor similare de la alte universități și acoperă o arie tematică fundamentală pentru înțelegerea domeniilor de aplicabilitate, pentru proiectarea și implementarea soluțiilor de securitate și integritate a datelor precum și de comunicare securizată într-un context dinamic. O astfel de calificare oferă un avantaj important celor ce pătrund pe piața muncii.

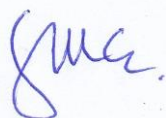
10. Evaluare*

Tip de activitate	10.1. Criterii de evaluare**	10.2. Metode de evaluare***	10.3. Pondere din nota finală
10.4 Curs	Nivelul de cunoaștere în toate domeniile acoperite de curs sau calitatea prezentării unui topic din curs	Examen scris sau o prezentare la curs	50%
10.5. Seminar/laborator	Implementare proiect	Execuția / prezentarea proiectului	20%
	Cunoașterea detaliilor proiectului	Interogare	15%
	Documentarea proiectului	Prezentare, interogare	15%
10.6. Standard minim de performanță <ul style="list-style-type: none"> • Implementarea / prezentarea elementelor de baza ale proiectului • Redactarea și prezentarea unui topic de curs sau • Obținerea notei 5 la examenul scris 			
Nota finală se calculează prin adunarea punctajelor obținute la examenul scris/prezentare topic și la proiectul realizat. La punctajul cumulat se aplică funcția ceil() (cel mai mic întreg mai mare sau egal cu suma punctajelor). Nota de promovare a disciplinei este 5. La fiecare dintre sesiunile de examen (inclusiv cele de restanță și măriri) nota se calculează după aceeași regulă.			

Data completării

Semnătura titularului de curs

Semnătura titularului de seminar




Semnătura directorului de departament