MD-2068, CHIŞINĂU, STR. STUDENŢILOR, 9/7, TEL: 022 50-99-63, www.utm.md

PROGRAME MALIȚIOASE ȘI RĂSPUNS LA INCIDENTE

1. Date despre disciplină

Facultatea	Calculatoare, Informatică și Microelectronică				
Departamentul	Ingineria Software și Automatică				
Ciclul de studii	Studii superioare de licență, ciclul I				
Programul de studii	0714.4 Automatică și Informatică				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opționalitate**	**Credite ECTS**
Anul III*(învățământ cu frecvență)*	5	E	L– unitate de curs la liberă alegere	L– unitate de curs la liberă alegere	3

2. Timpul total estimat

Total ore în planul de învățământ		**Din care**				
		Ore auditoriale			**Lucrul individual**	
		Curs	**Lucrări practice**	**Seminar**	**Studiul materialului teoretic**	**Proiectare**
Învățământ cu frecvență		30	15		30	15

3. Precondiții de acces la disciplină

Conform planului de învățământ	Arhitectura calculatoarelor; Sisteme de operare: mecanisme interne și principii de proiectare.
Conform competențelor	Limbajul de asamblare.

4. Condiții de desfășurare a procesului educațional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector și calculator. Nu vor fi tolerate întârzierile studenților, precum și convorbirile telefonice în timpul cursului.
Lucrări practice/ seminare	Studenții vor perfecta rapoarte conform condițiilor impuse de indicațiile metodice. Termenul de predare a lucrării de laborator – o săptămână după finalizarea acesteia.

5. Competențe specifice acumulate

Competențe profesionale	***C1 Privind fundamentele științifice și inginerești ale securității informaționale*** • Explicarea soluțiilor inginerești prin utilizarea tehnicilor, conceptelor și principiilor din științele exacte și aplicative. • Rezolvarea prob-lor din domenii de activitate umană prin aplicarea în special al tehnicilor și metodelor antimalware. • Alegerea criteriilor și metodelor pentru analiza avantajelor și dezavantajelor metodelor și procedeelor aplicate la soluționarea problemelor de securitate, în special sistemele antimalware.
Competențe transversale	***C2 Privind aspectele organizaționale și informaționale ale securității*** • Aplicarea conceptelor, teoriilor și metodelor de bază pentru pregătirea algoritmilor necesari elaborării de sisteme antimalware. • Alegerea criteriilor și metodelor de evaluare a eficacității algoritmilor de scanare și prevenire a amenințărilor malițioase. ***C3 Privind măsurile de securitate și control*** • Identificarea și definirea conceptelor, procedeelor și metodelor de verificare, scanare și monitorizare a programelor malware și realizarea măsurilor de prevenire și protecție ce reies din necesitați ale activității umane. • Explicarea tehnologiilor potrivite pentru realizarea sistemelor malware necesare în activitățile organizațiilor.

	• Utilizarea tehnologiilor moderne în definirea soluțiilor antimalware. ***C4 Privind metodele și tehnologiile de dezvoltare a soluțiilor de Securitate*** • Identificarea și definirea conceptelor și metodelor focusate pe procesul de dezvoltare, implementare și utilizare a soluțiilor de antivirus. • Explicarea conceptelor și metodelor folosite pentru dezvoltarea, implementarea și utilizarea măsurilor de prevenire și de protecție. • Aplicarea limbajelor de programare, a mediilor de modelare și dezvoltare, a metodologiilor pentru crearea sistemelor antimalware. • Dezvoltarea și implementarea de software antimalware pentru tipuri de amenințări concrete din mediul digital.

6. Obiectivele disciplinei

Obiectivul general	Să cunoască diversitatea programelor malițioase și antivirus. Clasificarea acestor programe, modul de funcționare, metode de infectare și de răspândire, mijloace de identificare și de înlăturare a consecințelor programelor malițioase.
Obiectivele specifice	Să cunoască clasificarea programelor malițioase. Să studieze codul programelor malițioase și tehnicile de infectare. Să înțeleagă un PE HEADER a unui fișier executabil. Să însușească metode de DEBUG a unei aplicații. Să studieze polimorfismul și scopul lui. Să înțeleagă arhitectura de protecție a sistemelor anti malware. Să cunoască metode de scanare și curățire a sistemului.

7. Conținutul disciplinei

Tematica activităților didactice	**Numărul de ore**	
	învățământ cu frecvență	**învățământ cu frecvență redusă**
Tematica prelegerilor		
T1. Introducere. Definiții soft malițios.	1	
T2. Considerații generale privind programele malițioase.	1	
T3. Considerațiuni generale privind defectele software. Studiu de caz, exemplu evenimentului Buffer Overflow.	2	
T4. Soluții antivirus. Istoricul dezvoltării soluțiilor antivirus. Clasificarea soluțiilor antivirus. Componentele unui sistem antivirus.	2	
T5. Considerațiuni generale privind defectele software. Studiu de caz, exemplu evenimentului Incomplete Mediation.	2	
T6. Considerațiuni generale privind programele malițioase.	2	
T7. Viruşii şi ameninţările lor. Tehnici de penetrare și infectare. Studiu de caz .	2	
T8. Viermii şi bacteriile. Tehnici de penetrare și infectare. Clasificare. Studiu de caz.	1	
T9. Ameninţările de tip Trojan. Tehnici de penetrare și infectare. Studiu de caz.	1	
T10. Backdoor/Rat. Bootkin. Rootkit. Bot. Tehnici de penetrare și infectare. Studiu de caz.	1	
T11. Botnet. Tehnici de penetrare și infectare. Studiu de caz.	1	
T12. PhishingAttacks. Tehnici de penetrare și infectare. Studiu de caz.	1	
T13. Exploitează truse. Tehnici de penetrare și infectare. Studiu de caz.	1	
T14. DistribuitDenial -of-Service Tehnici de penetrare și infectare. Studiu de caz4	1	
T15. Tehnici de penetrare și infectare. Studiu de caz.	1	
T16. Programe de spionaj. Adware. Tehnici de penetrare și infectare. Studiu de caz.	1	
T17. Programe de spionaj. Spyware. Tehnici de penetrare și infectare. Studiu de caz.	1	
T18. Oligomorfizm. Polimorfizm. Metamorfizm. Tehnici de penetrare și infectare. Studiu de caz	1	
T19. Considerațiuni generale privind aplicațiile malițioase de tip Ransomware. Apariția și dezvoltarea aplicațiilor malițioase de tip Ransomware. Studiu de caz.	1	

Tematica activităților didactice	Numărul de ore	
	învățământ cu frecvență	învățământ cu frecvență redusă
T20. Folosirea monedei virtuale Bitcoin în schemele Ransomware. Considerațiuni generale despre Bitcoin. Folosirea criptomonedei Bitcoin. Implicarea monedei virtuale Bitcoin în acte de tip Ransomware.	1	
T21. Ciclul atacului de tip Ransomware. Analiza comportamentului Ransomware.	1	
T22. Prevenirea schemelor frauduloase de tip Ransomware. Studiu de caz.	1	
T23. Analiza, depanarea și dezasamblarea programelor malițioase. Concepte generale de analiză, depanare și dezasamblare. Instrumente de analiză malware (IDA Pro, OllyDbg, WinDbg etc.). Tehnici și metode de obfuscation, anti-dezasamblare, anti-depanare.	1	
T24. Soluții antivirus. Istoricul dezvoltării soluțiilor antivirus. Clasificarea soluțiilor antivirus. Componentele unui sistem antivirus	1	
T25. Tehnici de scanare. Prima generație. Scanare după semnături. A doua generație. Scanare euristică. Virus-specific Detection. Code Emulation.	1	
Total curs:	**30**	
Tematica practici		
P1. Viermi, Troiani, Rootkituri	4	
P2. PE și infectarea fișierelor cu PE	3	
P3. Metode antidebug (SEH)	2	
P4. Polimorfizm	2	
P5. Metode de scanare și curațire a sistemului, crearea unui antivirus	2	
Total practice:	**15**	

8. Referințe bibliografice

Principale	1. Юров В., Хорошенко С., *Assembler: учебный курс.* 2. Собейкис В. Г., *Азбука хакера-3. Компьютерная вирусология*. 3. Олег Зайцев, *Rootkits, SpyWare/AdWare, Keyloggers & BackDoors. Обнаружение и защита*.
Suplimentare	1. http://vxheaven.org/lib/static/vdat/tumisc60.htm 2. http://vxheaven.org/lib/ 3. http://www.allasm.ru/vir.php 4. http://webanetlabs.net/publ/11 5. http://gtorrent.3dn.ru/publ/programmirovanie/virusologija/5

9. Utilizarea IA generativă

Permisiunea de utilizare	Utilizarea IA generative în cadrul temelor și proiectelor este permisă, cu condiția ca studenții să respecte următoarele reguli: • IA generativă poate fi utilizată pentru generarea de idei, structuri de text sau cod, dar toate materialele generate trebuie să fie revizuite și ajustate de către student pentru a se asigura că acestea corespund cerințelor academice. • Orice utilizare a IA generative trebuie să fie declarată în secțiunea de apendice a fiecărei lucrări, folosind fraza: "În timpul pregătirii acestei lucrări, autorul a utilizat [NUME INSTRUMENT / SERVICIU] în scopul [MOTIV]. După utilizarea acestui instrument/serviciu, autorul a revizuit și editat conținutul după cum a fost necesar și își asumă întreaga responsabilitate pentru conținutul lucrării."
Restricții de utilizare	Studenții nu trebuie să considere IA generativă ca o sursă de încredere pentru informații, deoarece nu oferă referințe clare sau surse documentate. • Nu este permisă citarea directă a conținutului generat de IA în lucrările academice ca și cum ar fi sursă primară. • Activitățile în care este interzis utilizarea IA generativă sunt specificare de profesor și sunt de regulă evaluări intermediare și finale sau care nu presupun activități de dezvoltare a competenților profesionale.

10. Evaluare

Periodică		Curentă	Proiect	Examen
EP 1	EP 2			
Învățământ cu frecvență				
10%	10%	10%	30%	40%
Standard minim de performanță. Prezența și activitatea la prelegeri și lucrări practice. Prezentarea proiectului de an. Obținerea notei minime de „5” la fiecare lucrări practice și proiectul de an.				

11. Criterii de evaluare

Activitate	Componente evaluare	Metodă de evaluare, Criterii de evaluare	Pondere în nota finală a activității	Ponderea în evaluarea disciplinei
Învățământ cu frecvență				
Evaluare periodică I	Conținut teoretic, teme 1-5	Test pe MOODLE	100%	**10%**
Evaluare periodică II	Conținut teoretic, teme 6-10	Test pe MOODLE	100%	**10%**
Evaluare curentă	Activitatea practică	Discuții în cadrul orelor de practică	50%	**10%**
		Raport pentru fiecare lucrare de practică încărcat pe MOODLE	50%	
Lucrul individual/Proiect de an	Cercetare la temă	Referat/Prezentare/discurs public. Raportul încărcat pe MOODLE	100%	**30%**
Evaluarea finală	Conținut teoretic și practic	Test pe MOODLE	100%	**40%**