MD-2045, CHIŞINĂU, str. STUDENŢILOR, 9/7, TEL: 022 50-99-08 | FAX: 022 50-99-05, www.utm.md

L.A.005 PROGRAME MALIȚIOASE ȘI RĂSPUNS LA INCIDENTE

1. Date despre unitatea de curs/modul

Facultatea	Calculatoare, Informatică și Microelectronică				
Catedra/departamentul	Ingineria Software și Automatică				
Ciclul de studii	Studii superioare de licență, ciclul I				
Programul de studiu	0613.3 Inginerie Software				
Anul de studiu	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opționalitate**	**Credite ECTS**
III (învățământ cu frecvență);	5	E	L-Disciplină la liberă alegere	A - unitate de curs opționale	3

2. Timpul total estimat

Total ore în planul de învățământ	Din care				
	Ore auditoriale		Lucrul individual		
	Curs	Laborator/seminar	Proiect de an	Studiul materialului teoretic	Pregătire aplicații
90	30	15	-	30	15

3. Precondiții de acces la unitatea de curs/modul

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

4. Condiții de desfăcurare a procesului educațional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector ei calculator. Nu vor fi tolerate întârzierile studenților, precum ei convorbirile telefonice în timpul cursului.
Laborator/seminar	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 profesionale	***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 ameniță̆rilor 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 prtecție ce reies din necesități 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 unității de curs/modulului

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 malișioase.
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 polimorfizmul și scopul lui. Să înțeleagă arhitectura de protecție a sistemelor antimalware. Să cunoască metode de scanare și curațire a sistemului.

7. Conținutul unității de curs/modulului

Tematica activităților didactice	Numărul de ore	
	învățământ cu frecvență	învățământ cu frecvență redusă
Tematica prelegerilor		
T1. Viruşii, istoricul apariţiei şi răspîndirea lor. Definiții și clasificarea programelor malițioase.	2	
T2. Viermi, Troiani, Rootkituri . Structura, depistarea, ciclul de viață, modul de acțiune.	3	
T3. Viruși DOS și Win9x. Structura, depistarea, ciclul de viață, modul de acțiune.	3	
T4. Viruși Win 32. Structura, depistarea, ciclul de viață, modul de acțiune.	3	
T5. Amenințări și versiuni Ransomware	3	
T6. Structura fișierelor de format Portable Executable. Infectarea fișierelor cu PE. Medode de infectare.	3	
T7. Tehnici de infectare a fișierelor de format PE și mecanizme de corectare a programelor infectate	3	
T8. Anti-Debuging (SEH). Tehnici și metode de Anti-Debuging	3	
T9. Polimorfizm. Metamorfizm.	3	

T10. Arhitectura de securitate a sistemelor antivirus	2	
T11. Metode de scanare și curățire a sistemului, crearea unui antivirus	2	
Total prelegeri:	**30**	

Tematica activităților didactice	Numărul de ore	
	învățământ cu frecvență	învățământ cu frecvență redusă
Tematica lucrărilor de laborator/seminarelor		
LL1. Viruși, Viermi, Troiani, Rootkituri	2	
LL2. Insrtumente de spionare (KeyLoger, Spyware, Backdoors)	2	
LL3. Amenințarile Ransomware	2	
LL4. Formatul fișierelor PE - Portable Executable și metodele de infectare a acestor fișiere	2	
LL5. Metode antidebug (SEH)	2	
LL6. Polimorfizm	2	
LL7. Metode de scanare și curațire a sistemului. Crearea unui antivirus	3	
Total lucrări de laborator/seminare:	**15**	

8. Referințe bibliografice

Principale	1. Dumitru Oprea, *Protecţia şi securitatea informaţiilor*. Ed. II, Polirom, Iaşi, 2007. – 445 p. 2. Popa Sorin Eugen, Securitatea sistemelor informatice, Bacău, 2007. – 136 p. 3. N.Ploteanu, S.Maftea, R.Griniuc, A.Coţofană, *Pasul II în ciberspaţiu: Securitatea Informaţională*, Academia „Ştefan cel Mare”, Chişinău, 2008. – 336 p. 4. Mark Stamp, *Information security. Principles and Practice,* Second Edition, SanJose State University, AJOHN WILEY&SONS, USA, 2011. - 608 p. 5. С. И. Макаренко, *Информационная безопасность,* Ставрополь СФ МГГУ им. М. А. Шолохова, 2009. 6. С. А. Нестеров, *Информационная безопасность и защита информации*, Санкт-Петербург, Издательство Политехнического университета, 2009. 7. А. Петров, *Компьютерная безопасность*, ДМК, Москва, 2000. 8. Юров В., Хорошенко С. "Assembler: учебный курс". 9. Собейкис В. Г. "Азбука хакера-3. Компьютерная вирусология" 10. Олег Зайцев” Rootkits, SpyWare/AdWare, Keyloggers & BackDoors. Обнаружение и защита”. 11. Szor P. The art of computer virus research and defense. 12. Mollin R. A. Introduction to Cryptography. 13. Агафонов А. Эмуляция программного кода, http:// www.uinc.ru/articles/47/
Suplimentare	http://vxheaven.org/lib/static/vdat/tumisc60.htm http://vxheaven.org/lib/ http://www.allasm.ru/vir.php http://webanetlabs.net/publ/11 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**	**Lucru individual**	**Examen**
EP 1	**EP 2**			
Învățământ cu frecvență				
15%	15%	15%	15%	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.				