

 UNIVERSITATEA TEHNICĂ A MOLDOVEI	CURRICULUM AL DISCIPLINEI	Cod:	CD/M – 8.1
	SECURITATEA PRODUSELOR PROGRAM	Pagina	1/14

FACULTATEA CALCULATOARE, INFORMATICĂ și MICROELECTRONICĂ
DEPARTAMENTUL INFORMATICĂ ȘI INGINERIA SISTEMELOR

APROBAT

la ședința Departamentului IIS

nr. ___ din _____

Șefă departament

conf. univ., dr. Viorica SUDACEVSCHI

APROBAT

la ședința Consiliului Facultății CIM

nr. ___ din _____

Președintele Consiliului FCIM

conf. univ., dr. Dumitru CIORBĂ

Domeniul general de studiu: 061 Tehnologii ale informației și comunicațiilor

Domeniul de formare profesională: 0612 Proiectarea și administrarea sistemelor informaționale

Program de studiu de master : Știința datelor

Cod, Denumirea disciplinei: S.O.003, SECURITATEA PRODUSELOR PROGRAM

Beneficiari: Studenții anului I, învățământ cu frecvență

Ciclul de învățământ: Studii superioare de Master, ciclul II

Numărul de credite ECTS: 5 (40 ore în auditoriu și 110 ore de activități individuale ale studentului, 1 credit = 8 ore de activități în auditoriu și 22 ore de activități individuale ale studentului)

Titularul disciplinei: conf. univ., dr. Mihail KULEV

semnătura titularului

 UNIVERSITATEA TEHNICĂ A MOLDOVEI	CURRICULUM AL DISCIPLINEI	Cod:	CD/M – 8.1
	SECURITATEA PRODUSELOR PROGRAM	Pagina	2/14

I. PRELIMINARII

Actualmente, domeniul tehnologiilor informaționale resimte necesitate în specialiști de o calificare superioară în securitatea produselor program, capabili în termeni scurți să proiecteze și să implimenteze produse soft oportune pentru economia națională și care satisfac cerințelor mereu crescânde de securitate.

Securitatea software-ului se referă la procesele și practicile implicate în dezvoltarea sistemelor software sigure, care sunt rezistente la atacuri rău intenționate și vulnerabilități neintenționate. Aceasta include toți pașii întreprinși pentru a asigura confidențialitatea, integritatea și disponibilitatea sistemelor software pe parcursul ciclului de viață al dezvoltării software. Securitatea software este critică deoarece vulnerabilitățile software pot duce la atacuri cibernetice, încălcări ale datelor și perturbări majore ale sistemelor informatice. Pe măsură ce sistemele mai critice se bazează pe software, impactul software-ului nesigur devine tot mai sever. Implementarea măsurilor de securitate software a devenit esențială pentru organizații cu scopul de a-și proteja activele și clienții într-o lume digitală tot mai interconectată.

Scopul principal al cursului „**SECURITATEA PRODUSELOR PROGRAM**” ca disciplină didactică, reprezintă oglindirea procedurilor de securitate progresiste existente și de perspectivă, proiectare și implimentare a produselor soft securizate. Cursul și laboratorul vor furniza studenților pregătirea necesară pentru a face față cerințelor angajatorilor din domeniul IT și anume:


- reducerea riscurilor de securitate a softului prin identificarea amenințărilor din timp, proiectarea unei arhitecturi sigure;
- urmărirea celor mai bune practici de elaborare de coduri sursă sigure pe baza unor specificații de securitate
- testarea riguroasă analiza manuală și automatizată de securitate a aplicațiilor folosind metodele, tehnicile și instrumentele soft existente.

Disciplina „**Securitatea produselor program**” este inclusă în categoria disciplinelor de specialitate pentru studenții programului de studiu de master științific **Știința datelor**. Consolidarea materialului teoretic și obținerea abilităților practice se realizează în procesul de desfășurare a lucrărilor de laborator/lucrărilor practice și a proiectelor de master.

Obiectivele principale ale cursului "**Securitatea produselor program**" vizează dezvoltarea competențelor esențiale necesare pentru proiectarea, implementarea și gestionarea unor aplicații software securizate. După finalizarea cursului, studenții vor fi capabili să:

- diferențieze între securitatea produselor program (software) și securitatea informațională;
- explice și aplice modelul CIA (Confidențialitate, Integritate, Disponibilitate) în Securitatea software;
- înțeleagă și să utilizeze OWASP Top 10 pentru a recunoaște cele mai comune vulnerabilități ale aplicațiilor web;
- aplice metode de testare a securității aplicațiilor (testare statică și dinamică);
- aplice principiile de securitate în dezvoltarea software;
- aplice măsuri de protecție aplicațiilor și datelor împotriva atacurilor;
- utilizeze framework-uri și biblioteci de securitate pentru dezvoltarea aplicațiilor;
- evalueze conformitatea softului cu standardele de securitate;
- aplice politici și proceduri de răspuns la incidente și planificare pentru recuperarea după atacuri.

Aceste obiective vor fi atinse printr-o combinație de prelegeri teoretice, studii de caz, exerciții practice și activități de laborator, oferind studenților o viziune practică și aplicată asupra securității software (produselor program).

 UNIVERSITATEA TEHNICĂ A MOLDOVEI	CURRICULUM AL DISCIPLINEI	Cod:	CD/M – 8.1
	SECURITATEA PRODUSELOR PROGRAM	Pagina	3/14

II. PRECONDIȚII DE ACCES LA DISCIPLINĂ

Pentru a atinge obiectivele cursului studenții trebuie să posede abilități în matematica superioară, să cunoască limbajele de programare de nivel înalt, să poată utiliza instrumentele soft și sistemele de operare uzuale. Aceste competențe sunt formate de următoarele unități de curs, prevăzute de planul de învățământ superior: matematica superioară și aplicată, programarea calculatoarelor, structuri de date și algoritmi, tehnici avansate de programare etc.

III. COMPETENȚELE CARE URMEAZĂ A FI DEZVOLTATE

Disciplina/modulul prevede formarea următoarelor competențe profesionale și transversale:

Competențe profesionale

CPM1 Elaborarea și proiectarea arhitecturii sistemului.

Își asumă un nivel ridicat de responsabilitate în definirea strategiei de implementare a noilor tehnologii în conformitate cu nevoile companiei. Ia în considerare infrastructura în vigoare, uzura echipamentelor și noile inovații tehnologice.

K1 Modele de arhitectura, metodologii și instrumente de proiectare a sistemelor

K2 Cerințele arhitecturii sistemelor : performanță, mentenabilitate, extensibilitate, scalabilitate, disponibilitate, securitate și accesibilitate

K3 Costurile, beneficiile și riscurile unei arhitecturi a sistemului

K4 Arhitectura întreprinderii și standardele interne ale companiei

K5 Noi tehnologii emergente (de exemplu, sisteme distribuite, modele de virtualizare, seturi de date, sisteme mobile).

S1 Oferă expertiză pentru a ajuta la rezolvarea problemelor tehnice complexe și pentru a asigura implementarea celor mai bune soluții de arhitectură

S2 Utilizează cunoștințele sale tehnologice din diferite domenii pentru a elabora și implementa arhitectura întreprinderii

S3 Înțelege obiectivele companiei care au impact asupra componentelor arhitecturii (date, aplicații, securitate, dezvoltare etc.)

S4 Ajută la comunicarea arhitecturii întreprinderii și a standardelor, principiilor și obiectivelor către diferite echipe implicate

S5 Dezvoltă modele de design și modele arhitecturale pentru a ajuta analiștii sistemului în proiectarea unor aplicații coerente.

CPM2 Monitorizarea tendințelor tehnologice. Inovație. Dezvoltarea durabilă.

Valorifică o gamă largă de cunoștințe de specialitate privind tehnologiile noi și emergente pentru a formula soluții de viitor pentru întreprindere. Oferă consiliere de specialitate echipei de conducere la luarea deciziilor strategice. Aplică gândirea independentă și cunoașterea tehnologică pentru a integra concepte disparate în soluții originale. Definește obiectivele și strategia de dezvoltare durabilă a SI în conformitate cu politica de sustenabilitate a organizației.


K1 Tehnologiile existente și emergente și aplicațiile lor relevante pe piață

K2 Obiectivele, tendințele și nevoile business-ului, societății și cercetării

K3 Sursele relevante de informații (de exemplu, reviste, conferințe și evenimente, lideri de opinie, forumuri on-line etc.)

K4 Abordările concrete ale programelor de cercetare aplicate

K5 Tehnicile procesului de inovare

 UNIVERSITATEA TEHNICĂ A MOLDOVEI	CURRICULUM AL DISCIPLINEI	Cod:	CD/M – 8.1
	SECURITATEA PRODUSELOR PROGRAM	Pagina	4/14

K6 Criteriile și indicatorii dezvoltării durabile

K7 Responsabilitatea societală corporativă (CSR) a părților interesate din cadrul infrastructurii sistemului informatic

S1 Monitorizează sursele de informații și urmărește continuu pe cele mai promițătoare

S2 Identifică vânzătorii și furnizorii de cele mai promițătoare soluții; evaluează, justifică și le propune pe cele mai potrivite

S3 Identifică avantajele și îmbunătățirile care le aduce adoptarea tehnologiilor emergente

S4 Gândește fără idei preconcepute

S5 Aplică recomandări în cadrul proiectelor care să sprijine cele mai recente strategii de dezvoltare durabilă

CPM3 Dezvoltarea aplicațiilor. Integrarea componentelor. Ingineria sistemelor.

Utilizează cunoștințele de specialitate la scară largă pentru a crea un proces, inclusiv stabilește standardele și practicile interne. Mobilizează echipele și alocă resurse pentru programele de integrare. Gestionează complexitatea prin dezvoltarea procedurilor și arhitecturilor standard în sprijinul dezvoltării produselor consistente. Stabilește și identifică un set de cerințe de sistem care trebuie atribuite elementelor sistemului. Acționează creativ pentru a dezvolta aplicații și a selecta opțiunile tehnice adecvate. Participă la alte activități de dezvoltare. Optimizează dezvoltarea, întreținerea și performanța aplicațiilor.

K1 Programe / module adecvate, SGBD și limbaje de programare adecvate. Tehnologii de ultimă oră.

K3 Impactul integrării unui sistem asupra organizației sau a sistemului existent

K4 Tehnici de interfațare între module, sisteme și componente

K5 Tehnici de testare a integrării

K7 Componente hardware, instrumente și arhitecturi hardware

K8 Proiectarea funcțională și tehnică

K9 Bazele securității informației

K10 Prototipare

S1 Aplică arhitecturi software și / sau hardware adecvate

S2 Măsoară performanța sistemului înainte, în timpul și după integrarea sistemului

S3 Identifică și înregistrează activitățile, problemele și măsurile corective legate de întreținere

S4 Adaptează nevoile clienților la produsele existente

S5 Securizează și face backup-ul datelor pentru a asigura integritatea lor în timpul integrării datelor sau a sistemului

S6 Explică și comunică clientului privind proiectarea / dezvoltarea

S7 Lansează și evaluează rezultatele testelor în funcție de specificațiile produsului

S8 Aplică modele de date, procese, pentru a se dezvolta eficient și productiv.

CPM5 Îmbunătățirea proceselor.

Realizează și autorizează implementarea inovațiilor și îmbunătățirilor care vor spori competitivitatea și/sau eficiența. Demonstrează conducerii avantajele schimbărilor posibile pentru întreprindere.

K1. Metode de cercetare, comparare și metode de măsurare

K2 Metode de evaluare, proiectare și implementare

K3 Procesele interne existente

K4 Dezvoltările/Evoluțiile relevante în domeniul TIC (de exemplu, virtualizarea, datele deschise etc.) și impactul lor potențial asupra proceselor

K5 Specificitatea tehnologiilor web, cloud și mobile

S1 Redactează, documentează și cataloghează procesele și procedurile esențiale

S2 Propune modificări ale procesului pentru a facilita și raționaliza îmbunătățirile

 UNIVERSITATEA TEHNICĂ A MOLDOVEI	CURRICULUM AL DISCIPLINEI		Cod:	CD/M – 8.1
	SECURITATEA PRODUSELOR PROGRAM		Pagina	5/14

Competențe transversale

CTM1 Autonomie și responsabilitate. *Execută unele sarcini profesionale complexe, în condiții de autonomie și de independență profesională.*

CTM2 Interacțiune socială *Își asumă funcții de conducere în activitățile profesionale sau în structurile organizatorice.*

CTM3 Dezvoltare profesională și personală. *Exercită autocontrolul procesului de învățare, previziunea nevoilor de formare, analiza critică a propriei activități profesionale.*

IV. ADMINISTRAREA DISCIPLINEI

Cod	Anul	Semestrul	Numărul de ore						Credite
			Curs	Seminar	Lucrări de laborator	Lucrări practice/de laborator	Proiectare	Lucrul individual	
S.O.003	Învățământ cu frecvență								
	I	II	20			20		110	5


V. REZULTATELE ÎNVĂȚĂRII, CONȚINUTURI ȘI METODE DIDACTICE APLICATE

Rezultatele învățării. Studentul trebuie:	Conținuturi		Metode de predare	Realizarea în timp (ore)*			
	Prelegeri	Lucrări de laborator, Seminare/Lecții practice		învățământ cu frecvență		învățământ cu frecvență redușă	
				prele geri	Pr/ La b	prele geri	Pr/ Lab
1	2	3	4	5	6	7	8
<p>să cunoască: Cunoașterea și utilizarea corectă a noțiunilor și rezultatelor fundamentale</p> <p>să fie capabil: Implementarea corectă a rezultatelor teoretice</p>	<p>Tema 1. Introducere în securitatea produselor program. Importanța securității în dezvoltarea software-ului Tipuri de amenințări și vulnerabilități</p>		<p>Pentru prelegeri: expunerea, învățare prin colaborare, conversația, problematizarea</p>	2			
<p>să cunoască: Cunoașterea și utilizarea corectă a noțiunilor și rezultatelor fundamentale</p> <p>să fie capabil: Implementarea corectă a rezultatelor teoretice</p>	<p>Tema 2. Principiile de bază ale securității produselor program. Confidențialitate, integritate, disponibilitate. Ciclul de viață al dezvoltării software-ului securizat</p>	<p>Lucrare practică/lucrare de laborator nr. 1. Utilizarea instrumentelor de analiză statică pentru evaluarea vulnerabilităților produselor program</p>	<p>Pentru prelegeri: expunerea, învățare prin colaborare, conversația, problematizarea</p> <p>Pentru lucrări practice/de laborator: Implementare/testare cod sursă, tehnici de învățare interactiv-creativă</p>	2	2/2		

<p>să cunoască: Cunoașterea și utilizarea corectă a noțiunilor și rezultatelor fundamentale să fie capabil: Implementarea corectă a rezultatelor teoretice</p>	<p>Tema 3. Securizarea cerințelor și designului. Analiza și validarea cerințelor de securitate. Design securizat și modele arhitecturale</p>		<p>Pentru prelegeri: expunerea, învățare prin colaborare, conversația, problematizarea</p>	2			
<p>să cunoască: Cunoașterea și utilizarea corectă a noțiunilor și rezultatelor fundamentale să fie capabil: Implementarea corectă a rezultatelor teoretice</p>	<p>Tema 4. Tehnici de programare securizată. Practici de programare pentru prevenirea vulnerabilităților comune. Exemple concrete ale unor limbaje de programare</p>		<p>Pentru prelegeri: expunerea, învățare prin colaborare, conversația, problematizarea</p>	2			
<p>să cunoască: Cunoașterea și utilizarea corectă a noțiunilor și rezultatelor fundamentale să fie capabil: Implementarea corectă a rezultatelor teoretice</p>	<p>Tema 5. Auditing și testarea securității. Metode de evaluare a securității software-ului. . Testarea statică, testarea dinamică, testarea penetrantă (penetration testing) și evaluarea codului</p>	<p>Lucrare practică/lucrare de laborator nr. 2. Utilizarea instrumentelor de analiză dinamică pentru evaluarea vulnerabilităților produselor program</p>	<p>Pentru prelegeri: expunerea, învățare prin colaborare, conversația, problematizarea</p> <p>Pentru lucrari practice/de laborator: Implementare/testare cod sursă, tehnici de învățare interactiv-creativă</p>	2	2/2		

<p>să cunoască: Cunoașterea și utilizarea corectă a noțiunilor și rezultatelor fundamentale</p> <p>să fie capabil: Implementarea corectă a rezultatelor teoretice</p>	<p>Tema 6. Managementul vulnerabilităților. Identificarea, clasificarea și tratamentul vulnerabilităților. Instrumente și tehnici de management al patch-urilor</p>	<p>Lucrare practică/lucrare de laborator nr. 3. Securitatea produselor program prin criptarea datelor - implementări în C/C++, Java, C# și Python</p>	<p>Pentru prelegeri: expunerea, învățare prin colaborare, conversația, problematizarea</p> <p>Pentru lucrari practice/de laborator: Implementare/testare cod sursă, tehnici de învățare interactiv-creativă</p>	2	2/2		
<p>să cunoască: Cunoașterea și utilizarea corectă a noțiunilor și rezultatelor fundamentale</p> <p>să fie capabil: Implementarea corectă a rezultatelor teoretice</p>	<p>Tema 7. Securitatea în mediile cloud și mobile. Provocări specifice pentru aplicațiile cloud</p>		<p>Pentru prelegeri: expunerea, învățare prin colaborare, conversația, problematizarea</p>	2			

<p>să cunoască: Cunoașterea și utilizarea corectă a noțiunilor și rezultatelor fundamentale</p> <p>să fie capabil: Implementarea corectă a rezultatelor teoretice</p>	<p>Tema 8. Securitatea în mediile cloud și mobile. Securitatea aplicațiilor mobile</p>	<p>Lucrare practică/lucrare de laborator nr. 4. Securitatea Aplicațiilor Web</p>	<p>Pentru prelegeri: expunerea, învățare prin colaborare, conversația, problematizarea</p> <p>Pentru lucrari practice/de laborator: Implementare/testare cod sursă, tehnici de învățare interactiv-creativă</p>	<p>2</p>	<p>2/2</p>		
<p>să cunoască: Cunoașterea și utilizarea corectă a noțiunilor și rezultatelor fundamentale</p> <p>să fie capabil: Implementarea corectă a rezultatelor teoretice</p> <p>să cunoască: Cunoașterea și utilizarea corectă a noțiunilor și rezultatelor fundamentale</p> <p>să fie capabil: Implementarea corectă a rezultatelor teoretice</p>	<p>Tema 9. Securitatea ciclului de viață al software-ului (DevSecOps). Integrarea securității în procesele DevOps. Automatizarea testării și Implementării securizate</p> <p>Tema 10. Aspecte legale și etice în securitatea software-ului. Reglementări legale relevante. Etica în dezvoltarea software-ului</p>	<p>Lucrare practică/lucrare de laborator nr. 5. Securitatea Aplicațiilor Mobile</p>	<p>Pentru prelegeri: expunerea, învățare prin colaborare, conversația, problematizarea</p> <p>Pentru lucrari practice/de laborator: Implementare/testare cod sursă, tehnici de învățare interactiv-creativă</p> <p>Pentru prelegeri: expunerea, învățare prin colaborare, conversația, problematizarea</p>	<p>2</p> <p>2</p>	<p>2/2</p>		

	CURRICULUM AL DISCIPLINEI	Cod:	CD/M – 8.1
	SECURITATEA PRODUSELOR PROGRAM	Pagina	10/14


VI. SUGESTII PENTRU ACTIVITATEA INDIVIDUALĂ A STUDENȚILOR

Pe parcursul semestrului, studenții realizează activități individuale, care includ:

- studiul literaturii obligatorii conform listei surselor bibliografice prezentate în curriculum;
- elaborarea lucrărilor de laborator în conformitate cu sarcina și structura aprobată.

Pe parcursul semestrului studenților li se propune tematica pentru elaborarea referatelor în scopul aprofundării cunoștințelor teoretice.

Nr. crt.	Capitol, temă	Conținut activitate individuală	Durata, ore	Forma de control	Termeni de control (perioada)
1	T1, T2 LP1/LL1	Înșușire material teoretic	5	Verificare la examen	Examen
		Pregătire lucrare de laborator	6		
		Studiu individual. Subiectul: <i>Utilizarea instrumentelor de analiză statică pentru evaluarea vulnerabilităților produselor program.</i>	6	Verificare îndeplinire sarcină	2 săptămâni de la data stabilirii sarcinii
		Analiză și concluzii la studiul individual	2	Verificare îndeplinire sarcină	Următoarea săptămână
2	T3, T4, T5 LP2/LL2	Înșușire material teoretic	5	Verificare la examen	Examen
		Pregătire lucrare de laborator	6		
		Studiu individual. Subiectul: <i>Utilizarea instrumentelor de analiză dinamică pentru evaluarea vulnerabilităților produselor program.</i>	6	Verificare îndeplinire sarcină	2 săptămâni de la data stabilirii sarcinii
		Analiză și concluzii la studiul individual	2	Verificare îndeplinire sarcină	Următoarea săptămână
3	T6, T7 LP3/LL3	Înșușire material teoretic	5	Verificare la examen	Examen
		Pregătire lucrare de laborator	6		
		Studiu individual. Subiectul: <i>Securitatea produselor program prin criptarea datelor - implementări în C/C++, Java, C# și Python.</i>	6	Verificare îndeplinire sarcină	2 săptămâni de la data stabilirii sarcinii
		Analiză și concluzii la studiul individual	2	Verificare îndeplinire sarcină	Următoarea săptămână
4	T8 LP4/LL4	Înșușire material teoretic	5	Verificare la examen	
		Pregătire lucrare de laborator	6		

 UNIVERSITATEA TEHNICĂ A MOLDOVEI	CURRICULUM AL DISCIPLINEI		Cod:	CD/M – 8.1
	SECURITATEA PRODUSELOR PROGRAM		Pagina	11/14


		Studiu individual. Subiectul: <i>Securitatea aplicațiilor Web.</i>	6	Verificare îndeplinire sarcină	2 săptămâni de la data stabilirii sarcinii
		Analiză și concluzii la studiul individual	2	Verificare îndeplinire sarcină	Următoarea săptămână
5	T9, T10 LP5/LL5	Însușire material teoretic	5	Verificare la examen	Examen
		Pregătire lucrare de laborator	6		
		Studiu individual. Subiectul: <i>Securitatea aplicațiilor mobile.</i>	6	Verificare îndeplinire sarcină	2 săptămâni de la data stabilirii sarcinii
		Analiză și concluzii la studiul individual	2	Verificare îndeplinire sarcină	Următoarea săptămână
6		Pregătirea pentru testele din cadrul evaluărilor curente	6	Testarea	Săptămâna 3, 6
7		Pregătire de examen	9	Verificare la examen	Examen
		Total:	110		

VII. EVALUAREA DISCIPLINEI

Periodică		Curentă	Studiu (Lucru) individual	Proiect/teză	Examen
EP 1	EP 2				
15%	15%	15%	15%	-	40%
<p>Standard minim de performanță</p> <p>Prezența și activitatea la prelegeri, lucrări practice și lucrări de laborator.</p> <p>Obținerea notei minime de „5” la fiecare dintre evaluări și lucrări de laborator.</p> <p>Obținerea notei minime de „5” la examen.</p>					

VIII. CRITERII DE EVALUARE

Denumire	Modul de desfășurare	Pondere pe componente de conținut
Evaluare periodică:		30%
EP 1	- <i>susținerea lucrărilor de laborator LL1 și LL2</i> – 15%	
EP 2	- <i>susținerea lucrărilor de laborator LL3 și LL4</i> – 15%	
Evaluare curentă	- <i>activități la lucrări de laborator</i> – 70% - <i>prezența la lecții</i> – 30%	15%
Studiu (Lucru) individual:		15%

 UNIVERSITATEA TEHNICĂ A MOLDOVEI	CURRICULUM AL DISCIPLINEI	Cod:	CD/M – 8.1
	SECURITATEA PRODUSELOR PROGRAM	Pagina	12/14

Sarcina: <i>Securitatea aplicațiilor mobile</i>	<i>Prezentare / discurs la temă LP5/LL5 – 15%</i>	
Proiect/teză	-	-
Examen semestrial	în formă scrisă / testare	40%


IX. LISTA DE SUBIECTE PENTRU EVALUĂRI PERIODICE ȘI CEA FINALĂ

CHESTIONAR PENTRU EVALUAREA PERIODICĂ 1

1. Securitatea Produselor Program. Scopul și obiectivele disciplinei.
2. Importanța securității în dezvoltarea software-ului.
3. Tipuri de amenințări și vulnerabilități ale produsului program.
4. Principiile de bază ale securității produselor program.
5. Confidențialitate, integritate, disponibilitate a soft-ului
6. Ciclul de viață al dezvoltării software-ului securizat.
7. Securizarea cerințelor și designului softului.
8. Analiza și validarea cerințelor de securitate.
9. Design securizat și modele arhitecturale.
10. Tehnici de programare securizată.
11. Pratici de programare pentru prevenirea vulnerabilităților comune. Exemple concrete ale unor limbaje de programare.
12. Auditing și testarea securității produsului soft.
13. Metode de evaluare a securității software-ului.

CHESTIONAR PENTRU EVALUAREA PERIODICĂ 2

1. Testarea statică de securitate a produsului program și evaluarea codului.
2. Testarea dinamică și testarea penetrantă (penetration testing) a produsului soft.
3. Managementul vulnerabilităților produsului program.
4. Identificarea, clasificarea și tratamentul vulnerabilităților.
5. Instrumente și tehnici de management al patch-urilor.
6. Securitatea în mediile cloud și mobile.
7. Securitatea aplicațiilor Web.
8. Securitatea aplicațiilor mobile.
9. Securitatea ciclului de viață al software-ului (DevSecOps).
10. Integrarea securității în procesele DevOps.
11. Automatizarea testării și implementării securizate a produselor program.
12. Aspecte legale și etice în securitatea software-ului. Reglementări legale relevante.
13. Etica în dezvoltarea software-ului securizat.

 UNIVERSITATEA TEHNICĂ A MOLDOVEI	CURRICULUM AL DISCIPLINEI	Cod:	CD/M – 8.1
	SECURITATEA PRODUSELOR PROGRAM	Pagina	13/14

CHESTIONAR PENTRU EXAMEN

1. Securitatea Produselor Program. Scopul și obiectivele disciplinei.
2. Importanța securității în dezvoltarea software-ului.
3. Tipuri de amenințări și vulnerabilități ale produsului program.
4. Principiile de bază ale securității produselor program.
5. Confidențialitate, integritate, disponibilitate a soft-ului
6. Ciclul de viață al dezvoltării software-ului securizat.
7. Securizarea cerințelor și designului softului.
8. Analiza și validarea cerințelor de securitate.
9. Design securizat și modele arhitecturale.
10. Tehnici de programare securizată.
11. Pratici de programare pentru prevenirea vulnerabilităților comune. Exemple concrete ale unor limbaje de programare.
12. Auditing și testarea securității produsului soft.
13. Metode de evaluare a securității software-ului.
14. Testarea statică de securitate a produsului program și evaluarea codului.
15. Testarea dinamică și testarea penetrantă (penetration testing) a produsului soft.
16. Managementul vulnerabilităților produsului program.
17. Identificarea, clasificarea și tratamentul vulnerabilităților.
18. Instrumente și tehnici de management al patch-urilor.
19. Securitatea în mediile cloud și mobile.
20. Securitatea aplicațiilor Web.
21. Securitatea aplicațiilor mobile.
22. Securitatea ciclului de viață al software-ului (DevSecOps).
23. Integrarea securității în procesele DevOps.
24. Automatizarea testării și implementării securizate a produselor program.
25. Aspecte legale și etice în securitatea software-ului. Reglementări legale relevante.
26. Etica în dezvoltarea software-ului securizat.

X. REFERINȚE BIBLIOGRAFICE

Obligatorii

1. *Securitatea in ciclul de dezvoltare al unui produs software*. Centrul național de răspuns la incidente de securitate cibernetică CERT-RO, 2012. <https://dnsc.ro/vezi/document/securitatea-in-ciclul-de-dezvoltare-software>
2. *Ghid pentru securizarea aplicațiilor și serviciilor web*. Centrul național de răspuns la incidente de securitate cibernetică CERT-RO, 2012. <https://dnsc.ro/vezi/document/ghid-securizare-aplicatii-web>
3. *Security-Driven Software Development: Learn to analyze and mitigate risks in your software projects*, by Aspen Olmsted (Author), Publisher: Packt Publishing - ebooks Account (March 15, 2024), ISBN-13 978-1835462836
4. *Secure Coding in C and C++ (SEI Series in Software Engineering) 2nd Edition*, by Robert Seacord (Author), Addison-Wesley Professional (April 12, 2013), ISBN-13 978-0321822130 IS

 UNIVERSITATEA TEHNICĂ A MOLDOVEI	CURRICULUM AL DISCIPLINEI	Cod:	CD/M – 8.1
	SECURITATEA PRODUSELOR PROGRAM	Pagina	14/14

5. *Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Input Validation & More*, by John Viega, Matt Messier (Authors), Publisher: O'Reilly Media (July 24, 2003, ISBN-13 978-0596003944)
6. *Application Security Program Guide: Building a Comprehensive Application and Product Security Program*, by Ahmed Abdul-Rahman (Author), (December 21, 2023), ISBN-13 979-8988840909

Suplimentare

1. *Software building security in*, Gary McGraw (Author), Addison-Wesley, Boston, 2011, ISBN: 9780321356703, 0321356705
2. *Secure Programming with Static Analysis*, by Brian Chess and Jacob West (2007), ISBN: 0-321-42477-8 Stroustrup, Bjarne (2014). *Programming: Principles and Practice Using C++* (Second ed.). Addison-Wesley. ISBN 978-0-321-99278-9
3. *Microsoft Developer Network (MSDN)*. <https://visualstudio.microsoft.com/msdn-platforms/>