FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	**Academia Tehnică Militară „Ferdinand I", București**
1.2 Facultatea	**Facultatea de Sisteme Integrate de Armament, Geniu și Mecatronică**
1.3 Departamentul	**Inginerie a Sistemelor de Armament și Mecatronică**
1.4 Domeniul de studii	**Inginerie de armament, rachete și muniții**
1.5 Ciclul de studii	**Licență**
1.6 Programe de studii / Calificări	***Armament, aparatură artileristică și sisteme de conducere a focului*** / *Ofițer inginer*
1.7 Forma de învățământ	**IF** - Învățământ de zi, cu frecvență
1.8 Codul disciplinei	**ARM.II.PM.01**

2. Date despre disciplină

2.1 Denumirea disciplinei				**Elemente de securitate cibernetică**			
2.2 Responsabil de curs				Lt.asist.univ.dr.ing Ioana CIȘMAȘ			
2.3 Titularul activităților de seminar / laborator / proiect				Ing. Alexandra-Victoria CIUVĂȚ			
2.4 Anul de studiu	**II**	2.5 Semestrul	**3**	2.6 Tipul de evaluare	**Cv**	2.7 Regimul disciplinei	**Obligatorie PM**

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

3.1 Număr de ore pe săptămână	**2**	din care: 3.2 curs	**1**	3.3 laborator	**1**	3.4 proiect	**-**
3.5 Total ore din planul de învățământ	**28**	din care: 3.6 curs	**14**	3.7 laborator	**14**	3.8 proiect	**-**

Distribuția fondului de timp pentru studiul individual	28 Ore
Studiul după manual, suport de curs, bibliografie și notițe	**8**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren	**8**
Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri	**8**
Tutorat	**-**
Examinări	**4**
Alte activități	**-**

3.9 Total ore studiu individual	**28**
3.10 Total ore pe semestru	**56**
3.11 Numărul de credite	**2**

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	N/A
4.2 de competențe	N/A

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Prelegerile se desfășoară ca flux de predare cu grupele de studenți, cu durata unui modul de 2 ore. Nu va fi tolerată întârzierea studenților la orele de curs, laborator întrucât aceasta se dovedește disruptivă la adresa procesului educațional. Nu vor fi tolerate convorbirile telefonice sau manevrarea telefoanelor mobile în timpul activităților didactice, nici părăsirea de către studenți a sălii de curs sau de laborator în vederea preluării apelurilor telefonice personale. Orele de curs si laborator aferente disciplinei se desfășoară in semestrul 3.
5.2. de desfășurare a seminarului / laboratorului / proiectului	Lucrările de laborator se desfășoară cu durata unui modul de 2 ore, în unul din laboratoarele existente la nivelul departamentului.

6. Competențele specifice acumulate

Competențe profesionale	• Recunoaşterea şi descrierea conceptelor proprii calculabilităţii, complexităţii, paradigmelor de securizare a sistemelor informatice şi de comunicaţii. • Descrierea structurii şi funcţionării componentelor de comunicaţii necesare pentru asigurarea securităţii informatice a sistemelor informatice şi de comunicaţii • Identificarea şi descrierea cerinţelor şi principiilor folosite pentru asigurarea disponibilităţii si securităţii sistemelor informatice și de comunicații
Competențe transversale	**Executarea responsabilă a sarcinilor profesionale** • Analiza metodică a problemelor întâlnite în activitate, identificând elementele pentru care exista soluții consacrate, asigurând astfel îndeplinirea sarcinilor profesionale. **Familiarizarea cu activitățile de etapizare și organizare specifice implementării aplicațiilor software** • Definirea activităților pe etape, înțelegerea completă a sarcinilor identificate în cadrul etapelor, stabilirea unor fluxuri corecte de implementare. **Conștientizarea nevoii de formare continuă** • Adaptarea la noile tehnologii, dezvoltarea profesională și personală, prin formare continuă folosind surse de documentare diverse (în limba româna și cel puțin, într-o limbă de circulație internațională) și software specializat pentru documentare.
Rezultatele învățării	**Cunoștințe** • Studentul identifică și sumarizează concepte de securitate cibernetică și modul lor de aplicare în probleme concrete. **Aptitudini** • Studentul alege, realizează și explică construcții proprii specifice securității cibernetice. • Studentul analizează cerințe, elaborează, dezvoltă și testează impactul atacurilor cibernetice asupra organizațiilor și persoanelor. • Studentul configurează aplicații și module pentru asigurarea securitățatii sistemelor de operare, inclusiv a proceselor de autentificare, autorizare. **Responsabilitate și autonomie** • Studentul derulează procese specifice construcției modalităților de securizare a sistemelor informatice și de comunicații utilizate, cu descrierea clară și concisă, verbal și în scris, a etapelor parcurse și a rezultatelor obținute. • Studentul arată spirit de inițiativă și acțiune pentru actualizarea și formarea continuă a cunoștințelor sale profesionale în domeniul securității cibernetice și demonstrează un comportament responsabil și etic.

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

7.1 Obiectivul general al disciplinei	• Însușirea de către studenți a noţiunilor de bază utilizate pentru securizarea sistemelor informatice și de comunicații.
7.2 Obiectivele specifice	• Cunoașterea mecanismelor specifice de asigurare a securității cibernetice. • Cunoașterea vulnerabilităților, riscurilor și amenințări cibernetice, precum și a atacurilor cibernetice potențiale și a metodelor de prevenție.

8. Conținuturi

8.1 Curs	Metode de predare	Observații
C.1. Introducere în securitate cibernetică • vulnerabilități, riscuri, amenințări • tipuri de atacuri/atacatori impactul atacurilor cibernetice asupra organizațiilor și persoanelor	*Prelegeri, discuții, cu ilustrări utilizând, laptop, videoproiector, tablă.*	**2 ore**
C.2. Principiile securității cibernetice • integritate, confidențialitate, disponibilitate • protecția datelor personale • backup și criptare Securitate în cloud și protecția datelor online		**2 ore**
C.3. Protecția datelor și infrastructurilor • modelul OSI. IP-uri, DNS; cum funcționează rețelele • sisteme de monitorizare, filtrarea traficului • instrumente hardware și software pentru protecția rețelelor		**2 ore**

securitatea computerelor.		
C.4. Securitatea sistemelor de operare și a dispozitivelor mobile • securitatea sistemelor de operare, autentificare, autorizare, permisiuni, procese, update dispozitive mobile și riscuri de securitate		**2 ore**
C.5. Mecanisme și tehnologii de autentificare • parole, stocarea credențialelor, OTP, 2FA • sms/mail, aplicații dedicate, token, biometrică inginerie socială		**2 ore**
C.6. Standardizare și cadru legislativ • standarde, reglementări, roluri strategia națională pentru securitate cibernetică		**2 ore**
C.7. Atacuri și metode de prevenție • metode de infectare/atac • metode de protecție și prevenție gestionarea incidentelor și răspunsul la atacuri cibernetice		**2 ore**
Bibliografie 1. Lester Evans, „Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social Engineering, Attack and Defense Strategies, and Cyberwarfare 2. Strategia de Securitate cibernetica a Romaniei 3. Resurse electronice, tutoriale		

8.2 Seminar / laborator / proiect	Metode de desfășurare	Observații
L1. Vulnerabilități, riscuri, amenințări la adresa infrastructurilor cibernetice. Tipuri de soluții și acțiuni de răspuns. Impactul atacurilor cibernetice asupra organizațiilor și persoanelor.	*Laboratoarele se desfășoară în laboratoarele de programare ale universității, pe stațiile de calcul din cadrul acestora, urmând indicațiile profesorului si exemplele inițiale de programe furnizate de către profesor pe tablă și/sau videoproiector.*	**2 ore**
L2. Aplicații pentru realizarea de backup și criptare. Modalități de protecție a datelor personale. Soluții de securitate în cloud și protecția datelor online.		**2 ore**
L3. Metode de protecție a infrastructurilor cibernetice. Cum funcționează rețelele de calculatoare și de sisteme de monitorizare sunt necesare pentru pentru protecția acestora.		**2 ore**
L4. Metode de securitate a sistemelor de operare și a dispozitivelor mobile. Securizarea datelor de autentificare, autorizare, permisiuni, procese, actualizări.		**2 ore**
L5. Mecanisme și tehnologii de autentificare prin parole, stocarea credențialelor, OTP, 2FA.		**2 ore**
L6. Standardizare și cadru legislativ. Roluri existente pentru asigurarea securității cibernetice. Strategia națională de securitate cibernetică.		**2 ore**
L7. Atacuri și metode de prevenție. Metode de infectare/atac și modalități de gestionare a incidentelor, precum și răspunsul la atacuri cibernetice.		**2 ore**
Bibliografie 1. Lester Evans, „Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social Engineering, Attack and Defense Strategies, and Cyberwarfare 2. CompTIA Security+ All-in-One Exam Guide, Sixth Edition (Exam SY0-601)) 3. Resurse electronice, tutoriale		

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

Disciplina a fost introdusă conform standardelor militare naționale pentru domeniul „Ştiinţe inginereşti”, domeniul de studii „Inginerie de armament, rachete și muniții”.
Conținutul programului de studii a fost aprobat de factorii responsabili ai beneficiarilor din cadrul structurilor de apărare, ordine publică și securitate națională.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.5 Evaluare sumativă Curs/Laborator	• Cunoașterea terminologiei și a conceptelor specifice securității cibernetice. • Cunoașterea metodelor de protecție a datelor și infrastructurilor. • Cunoaștere metodelor de securizare a sistemelor de operare și a dispozitivelor mobile. • Cunoașterea mecanismelor și tehnologii de autentificare	**Evaluarea sumativă** se face prin **examen scris** la final de semestru. Subiectul de examen va conține 10-15 cerințe de verificare a cunoștințelor, deprinderilor și abilităților practice din domeniul securității cibernetice. Punctajul acordat la evaluarea sumativă (*ES*) este cuprins in intervalul 0 – 10 puncte si se obține pe baza unui barem de corectare stabilit pentru fiecare cerință a subiectului în funcție de dificultatea și complexitatea sa.	(*ES*) 60%
10.4 Evaluare continuă Curs/Laborator	• Cunoașterea terminologiei și a conceptelor specifice securității cibernetice. • Cunoașterea metodelor de protecție a datelor și infrastructurilor. Cunoaștere metodelor de securizare a sistemelor de operare și a dispozitivelor mobile.	**Evaluarea continuă** se realizează pe parcursul semestrului și include rezultatele obținute la **1 test intermediar** dat în timpul semestrului, în cadrul laboratoarelor sau separat de laborator și **nota** obținută **pentru o temă de laborator**. Testul intermediar este propus și evaluat în timpul semestrului, pe baza unui barem de corectare stabilit pentru fiecare cerință în funcție de dificultatea și complexitatea sa. Punctajul testului intermediar va fi cuprins în intervalul 0 - 10 puncte. Tema de laborator se atribuie în timpul semestrului și are un termen clar de predare; evaluarea acesteia se face în baza unor criterii de corectitudine și funcționalitate, punctajul acordat la temă fiind cuprins în intervalul 0 - 10 puncte. *Punctajul acordat la evaluarea continuă (EC) este cuprins în intervalul 0 - 10 puncte, fiind calculat ca o medie aritmetică* a punctajelor obținute la testul intermediar și la tema de laborator.	*(EC)* 40%

Nota finală a disciplinei se calculează folosind relația: *NFD* = 0.6 * *ES* + 0.4 * *EC*

Observații:

- În caz de neprezentare la evaluarea sumativă, nota finală a disciplinei va fi nota 0 (NFD = 0).
- În caz de fraudă (inclusiv tentativa), nota finală a disciplinei va fi nota 1 (NFD = 1).
- În caz de predare a subiectului de examen, nota finală a disciplinei va fi nota 2 (NFD = 2).
- În cazul în care pentru NFD calculat rezultă o valoare mai mică sau egală cu 2, nota finală a disciplinei va fi nota 3 (NFD = 3).

***În caz de re-examinare*:**

- În caz de re-examinare pe motiv de disciplină nepromovată, se poate re-evalua doar componenta sumativă (**ESR**). Testele intermediare din timpul semestrului NU pot fi repetate, rezultatele obținute in timpul semestrului (**EC**) fiind menținute.
Nota finală a disciplinei la re-evaluare în acest caz se calculează folosind relația: NFD = 0.6 * ESR + 0.4 * EC
- În caz de re-examinare în vederea măririi notei, re-examinarea se face printr-o singură evaluare sumativă (**ESR**) care va avea pondere 100%: NFD = ESR
- În caz de examinare ca urmare a participării studentului într-o mobilitate Erasmus+ (sau ca urmare a faptului că studentul s-a aflat într-o situație specială perfect justificată) ce nu a permis evaluarea studentului pe parcursul semestrului, examinarea se face printr-o singură evaluare sumativă (**ES**) care va avea pondere 100%: NFD = ES

10.6 Standard minim de performanță

***Cerințe minime de promovare (cumulativ)*:**

- Studentul identifică și sumarizează **cel puțin trei metode de securizare a utilizatorilor și echipamentelor din cadrul unui sistem informatic și de comunicații**.
- Studentul realizează și explică **cel puțin o implementare de tehnologie de autentificare**
- Studentul **obține minim nota 5.00** conform barem, atât ca notă la evaluarea sumativă (*ES* $\geq$ *5.00*) cât și ca notă finală a disciplinei (*NFD* $\geq$ *5.00*)

Cele 6 unități de credit se acordă pentru promovarea disciplinei cu cel puțin nota cinci (*NFD ≥ 5.00*).

Data completării

____.____.

Titular de curs

Lt.asist.univ.dr.ing.

. Ioana CIȘMAȘ

.....

Titular de seminar/laborator

Ing.

Alexandra-Victoria CIUVĂȚ

.....

Data avizării în Departament

____.____.

Director Departament A1

Col. prof. univ. dr. ing.

Marius-Valeriu CÎRMACI-MATEI

Data avizării în Consiliul Facultății

.....

PAGINĂ ALBĂ