



MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA „VALAHIA” DIN TÂRGOVIȘTE
FACULTATEA DE INGINERIE ELECTRICĂ, ELECTRONICĂ ȘI TEHNOLOGIA
INFORMAȚIEI
DEPARTAMENTUL DE AUTOMATICĂ, INFORMATICĂ ȘI INGINERIE
ELECTRICĂ

FIȘA DISCIPLINEI 2026-2027

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Valahia din Târgoviște
1.2 Facultatea	Inginerie Electrică, Electronică și Tehnologia Informației
1.3 Departamentul	Automatică, Informatică și Inginerie Electrică
1.4 Domeniul de studii	Ingineria Sistemelor
1.5 Ciclul de studii	Master
1.6 Programul de studii	Automatică avansată, producție și informatică industrială

2. Date despre disciplină

2.1 Denumirea disciplinei	Tehnici de securitate pentru sisteme informatice (MAI 2 L S 07)						
2.2 Titularul activităților de curs	Conf. dr. ing. Mihai Bîzoi						
2.3 Titularul activităților de seminar	Conf. dr. ing. Mihai Bîzoi						
2.4 Anul de studiu	II	2.5 Semestrul	I	2.6 Tipul de evaluare	C	2.7 Regimul disciplinei	L-S

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 seminar/laborator	1
3.4 Total ore din planul de învățământ	28	din care: 3.5 curs	14	3.6 seminar/laborator	14
Distribuția fondului de timp					ore
Studiul după manual, suport de curs, bibliografie și notițe					8
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					4
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					6
Tutoriat					2
Examinări					2
Alte activități					0
3.7 Total ore studiu individual					22
3.9 Total ore pe semestru					50
3.10 Numărul de credite					2

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	- Sisteme de operare; - Rețele de calculatoare; - Tehnologii web; - Cloud computing.
4.2 de competențe	- Administrarea sistemelor de operare Linux și Windows; - Configurarea serviciilor și a protocoalelor de rețea TCP/IP; - Programarea și depanarea aplicațiilor web.

5. Condiții (acolo unde este cazul)

5.1 de desfășurare a cursului	Sală de curs cu videoproiector și calculator sau tablă interactivă sau calculator și conexiune Internet pentru activitate online. În funcție de situația epidemiologică sau alte situații neprevăzute, cursurile se vor desfășura online, în conformitate cu procedura aplicată, pe platformele Moodle și Teams.
5.2 de desfășurare a seminarului/laboratorului	Sală de laborator cu calculatoare și software specific sau calculatoare cu software specific și conexiuni Internet. În funcție de situația epidemiologică sau alte situații neprevăzute, laboratoarele se vor desfășura online, în conformitate cu procedura aplicată, pe platformele Moodle și Teams.

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

6.1 Obiectivul general al disciplinei	Formarea capacității de a identifica, evalua și trata riscurile de securitate ale sistemelor informatice, inclusiv ale celor care conduc procese industriale, prin aplicarea sistematică a tehnicilor de testare, de protecție și de detecție și a cerințelor de reglementare în vigoare.
6.2 Obiectivele specifice	• Înțelegerea modelelor de amenințare, a metodologiilor de analiză a riscului și a cadrului normativ european și național de securitate cibernetică; • Stăpânirea tehnicilor de dezvoltare și de testare a codului sigur, inclusiv a securității lanțului de aprovizionare software; • Aplicarea mecanismelor de control al accesului, de criptografie aplicată și de securizare a sistemelor și a rețelor; • Organizarea detecției și a răspunsului la incidente, pe baza jurnalelor, a regulilor de detecție și a informațiilor despre amenințări.

7. Rezultatele învățării

7.1 Cunoștințe (<i>Rezultatul asimilării de informații prin învățare. Cunoștințele reprezintă ansamblul de fapte, principii, teorii și practici legate de un anumit domeniu de muncă sau de studiu. Pot fi teoretice și/sau faptice</i>) C1. Descrie modelele de amenințare, proprietățile de securitate și particularitățile sistemelor industriale, în raport cu cadrul european de reglementare (Directiva NIS2, Regulamentul privind reziliența cibernetică). C2. Explică metodologiile de analiză și de tratare a riscului și sistemele de evaluare și prioritizare a vulnerabilităților (CVSS, EPSS, catalogul vulnerabilităților exploatare activ). C3. Prezintă clasele principale de vulnerabilități ale aplicațiilor, principiile codului sigur și tehnicile de testare statică, dinamică și a dependențelor software. C4. Descrie mecanismele de autentificare, de control al accesului, de criptografie aplicată și de detecție a incidentelor, împreună cu principiile arhitecturii de încredere zero.
7.2 Aptitudini (<i>Capacitatea de a aplica cunoștințe și de a utiliza know-how pentru a duce la îndeplinire sarcini și a rezolva probleme. Aptitudinile sunt descrise ca fiind cognitive (implicând utilizarea gândirii logice, intuitive și creative) sau practice (implicând dexteritate manuală și utilizarea de metode, materiale, unelte și instrumente)</i>) A1. Inventariază suprafața de atac a unui sistem și evaluează vulnerabilitățile acestuia cu instrumente de scanare, prioritizând remediarea pe criterii explicite. A2. Identifică, exploatează într-un mediu controlat și remediază vulnerabilități ale aplicațiilor web, verificând efectul corecției. A3. Integrează analiza statică, analiza dependențelor și generarea listei de componente software (SBOM) într-o conductă de integrare continuă. A4. Securizează sistemul de operare, accesul la distanță și comunicațiile criptate și formulează reguli de detecție pe baza jurnalelor și a traficului de rețea.
7.3 Responsabilitate și autonomie (<i>Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale</i>) R1. Respectă cadrul legal și etic al testării de securitate, acționând numai în medii autorizate și în limitele mandatului primit. R2. Argumentează deciziile de tratare a riscului prin evaluări proprii, documentate și reproductibile, distingând între vulnerabilitatea teoretică și riscul efectiv. R3. Își asumă responsabilitatea pentru securitatea sistemelor pe care le proiectează sau le administrează, inclusiv pentru raportarea incidentelor către autoritățile competente. R4. Își actualizează autonom cunoștințele pe baza surselor de informații despre amenințări și a publicațiilor de vulnerabilități.

8. Conținuturi

8.1 Curs	Metode de predare	Observații
----------	-------------------	------------

C1. Securitatea sistemelor informatice astăzi (Confidențialitate, integritate, disponibilitate, peisajul amenințărilor și actorii acestora, modelarea amenințărilor cu STRIDE, particularitățile sistemelor industriale și seria de standarde IEC 62443, cadrul european: Directiva NIS2 și Regulamentul privind reziliența cibernetică).	Expunerea, conversația, demonstrația	2 ore
C2. Analiza și managementul riscului (Terminologie, metodologii calitative și cantitative, pierderea anuală estimată, ISO/IEC 27005 și NIST CSF 2.0, evaluarea vulnerabilităților cu CVSS 4.0, probabilitatea de exploatare EPSS, catalogul KEV, registrul de riscuri și opțiunile de tratare).	Expunerea, conversația, demonstrația	2 ore
C3. Vulnerabilități ale aplicațiilor și cod sigur (OWASP Top 10 și CWE Top 25, injecții și validarea intrărilor, erori de gestiune a memoriei și limbaje cu siguranța memoriei, gestiunea sesiunilor, securitatea interfețelor API, principiul „secure by design”, cerințele OWASP ASVS).	Expunerea, conversația, demonstrația	2 ore
C4. Testarea securității software (Analiză statică, dinamică și interactivă, fuzzing, testarea de penetrare și metodologiile ei — OWASP WSTG, PTES, instrumente de testare, integrarea testelor în conducta de livrare — DevSecOps, raportarea constatărilor).	Expunerea, conversația, demonstrația	2 ore
C5. Securitatea lanțului de aprovizionare software (Dependente directe și tranzitive, lista componentelor software — SBOM, formatele SPDX și CycloneDX, semnarea artefactelor, cadrul SLSA, incidente de referință — SolarWinds, Log4Shell, XZ Utils, obligațiile producătorilor conform Regulamentului privind reziliența cibernetică).	Expunerea, conversația, demonstrația	2 ore
C6. Identitate, acces și criptografie aplicată (Autentificare multifactor și FIDO2, OAuth 2.0 și OpenID Connect, privilegiul minim, gestiunea secretelor, TLS 1.3 și infrastructura de chei publice, arhitectura de încredere zero — NIST SP 800-207, tranziția către criptografia post-cuantică).	Expunerea, conversația, demonstrația	2 ore
C7. Detecția și răspunsul la incidente (Jurnale și sisteme SIEM, cadrul MITRE ATT&CK, indicatori de compromitere, informații despre amenințări și schimbul lor — STIX/TAXII, noțiuni de analiză a programelor malițioase, ciclul de răspuns — NIST SP 800-61r3, raportarea incidentelor, recapitulare).	Expunerea, conversația, demonstrația	2 ore
Bibliografie 1. Bizoi Mihai, Tehnici de securitate pentru sisteme informatice – notițe de curs, https://moodle.valahia.ro 2. Stallings W., Brown L., Computer Security: Principles and Practice, 5th Edition, Pearson, 2023; 3. Anderson R., Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition, Wiley, 2020; 4. Shostack A., Threat Modeling: Designing for Security, Wiley, 2014; 5. Aumasson J.-P., Serious Cryptography: A Practical Introduction to Modern Encryption, 2nd Edition, No Starch Press, 2024; 6. McGraw G., Software Security: Building Security In, Addison-Wesley, 2006; 7. NIST, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, 2024, https://doi.org/10.6028/NIST.CSWP.29 8. Directiva (UE) 2022/2555 (NIS2) și Regulamentul (UE) 2024/2847 privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale, https://eur-lex.europa.eu		
8.2 Seminar/laborator	Metode de predare	Observații
L1. Inventarierea suprafeței de atac: descoperirea sistemelor și a serviciilor, scanarea vulnerabilităților și prioritizarea lor după CVSS și EPSS.	Expunerea, demonstrația, lucrări practice	2 ore
L2. Securizarea sistemului de operare și a accesului la distanță: întărire după ghidurile CIS, autentificare SSH cu chei, filtrare cu nftables.	Expunerea, demonstrația, lucrări practice	2 ore
L3. Vulnerabilități web: identificarea, exploatarea controlată și remedierea injecțiilor și a atacurilor XSS pe o aplicație vulnerabilă intenționat.	Expunerea, demonstrația, lucrări practice	2 ore
L4. Analiza statică și a dependențelor: SAST, generarea SBOM și scanarea componentelor, integrate într-o conductă de integrare continuă.	Expunerea, demonstrația, lucrări practice	2 ore
L5. Criptografie aplicată: configurarea și evaluarea TLS 1.3, certificate digitale și gestiunea secretelor.	Expunerea, demonstrația, lucrări practice	2 ore
L6. Detecție și răspuns: colectarea jurnalelor, inspectarea traficului, reguli de detecție și maparea pe MITRE ATT&CK.	Expunerea, demonstrația, lucrări practice	2 ore
L7. Colocvii de laborator.	Evaluare	2 ore

Bibliografie

1. Bîzoi M., Tehnici de securitate pentru sisteme informatice – lucrări de laborator, <https://moodle.valahia.ro>
2. ***, OWASP Web Security Testing Guide, v4.2, <https://owasp.org/www-project-web-security-testing-guide/>
3. ***, CIS Benchmarks, Center for Internet Security, <https://www.cisecurity.org/cis-benchmarks>
4. ***, MITRE ATT&CK, <https://attack.mitre.org/>
5. ***, NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, NIST, 2025, <https://doi.org/10.6028/NIST.SP.800-61r3>

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

Conținuturile disciplinei au fost stabilite prin raportare la cadrele de referință utilizate de comunitatea profesională de securitate (OWASP, MITRE ATT&CK, NIST CSF 2.0, seria IEC 62443), la cerințele de competențe formulate de întreprinderile de profil și de operatorii de servicii esențiale din zonele limitrofe orașelor Târgoviște și București, precum și la obligațiile care decurg din Directiva NIS2, din legislația națională de transpunere a acesteia și din Regulamentul privind reziliența cibernetică, astfel încât absolventul să poată participa, încă de la angajare, la evaluarea riscurilor, la dezvoltarea sigură a aplicațiilor și la răspunsul la incidente în organizațiile care operează sisteme informatice și industriale.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Înșușirea conceptelor, a metodelor și a reglementărilor de securitate	Colocviu (lucrare scrisă sau test online)	60%
10.5 Seminar/laborator	Realizarea lucrărilor de laborator și rezolvarea unei sarcini practice	Colocviu de laborator	40%
10.6 Standard minim de performanță			
• Cunoștințe (C1–C4): explică corect modelele de amenințare, metodele de evaluare a riscului și a vulnerabilităților, clasele principale de vulnerabilități și mecanismele de protecție, folosind terminologia de specialitate. • Aptitudini (A1–A4): realizează integral cel puțin cinci dintre cele șase lucrări de laborator și rezolvă, la colocviu, o sarcină practică de evaluare, remediere sau securizare a unui sistem. • Responsabilitate și autonomie (R1–R4): justifică prioritizarea unei vulnerabilități printr-o evaluare proprie a riscului și respectă, în toate activitățile practice, limitele legale și etice ale testării de securitate. • Condiții de promovare: obținerea a cel puțin 50% din punctajul fiecărei componente de evaluare, atât la verificarea teoretică, cât și la colocviul de laborator.			

Data completării
08.09.2026

Titularul de curs
Conf. dr. ing. Mihai BÎZOI

Titularul de aplicații
Conf. dr. ing. Mihai BÎZOI

Data avizării în
departament
23.09.2026

Director de departament
Conf. dr. ing. Mihai BÎZOI

Data avizării în
Consiliul Facultății
24.09.2026

Decan
Conf. dr. ing. Nicoleta ANGELESCU