FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea Babeş-Bolyai din Cluj-Napoca**
1.2 Facultatea	**Facultatea de Matematică şi Informatică**
1.3 Departamentul	**Departamentul de Matematică și Informatică al Liniei Maghiare**
1.4 Domeniul de studii	**Informatică**
1.5 Ciclul de studii	**Licență**
1.6 Programul de studiu / Calificarea	**Informatică**

2. Date despre disciplină

2.1 Denumirea disciplinei	**Securitate IT**						
2.2 Titularul activităţilor de curs	**Lect. dr. ing. Kolumbán Sándor**						
2.3 Titularul activităţilor de seminar	**Lect. dr. ing. Kolumbán Sándor**						
2.4 Anul de studiu	**3**	2.5 Semestrul	**6**	2.6. Tipul de evaluare	**Examen**	2.7 Regimul disciplinei	**Opțional**
2.8 Codul disciplinei	**MLM5255**						

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

3.1 Număr de ore pe săptămână	**3**	Din care: 3.2 előadás	**2**	3.3 seminar/laborator	**1**
3.4 Total ore din planul de învățământ	**36**	Din care: 3.5 előadás	**24**	3.6 seminar/laborator	**12**
Distribuţia fondului de timp:					ore
Pregătire pentru ore					**20**
Pregătire pentru examen parțial					**30**
Elaborarea temelor pentru acasă					**20**
Stăpânirea materialului de învățare scris					**14**
Pregătire pentru examen					**30**
Alte activităţ:					**-**
3.7 Total ore studiu individual	**114**				
3.8 Total ore pe semestru	**150**				
3.9 Numărul de credite	**6**				

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	● Nu este cazul
4.2 de competenţe	● Bazele programări ● Limbaje Java și C/C++ ● Sisteme de operare ● Rețele de comunicare

5. Condiţii (acolo unde este cazul)

5.1 De desfăşurare a cursului	● Sală de curs echipat cu tablă şi videoproiector.
5.2 De desfăşurare a seminarului/laboratorului	● Laborator dotat cu calculatoare și o rețea wireless fiabilă ● Sursă de alimentare pentru calculatoare portabile

6. Competenţele specifice acumulate

Competențe profesionale	C1 Programarea în limbaje de nivel înalt C1.3 Elaborarea codurilor sursă adecvate și testarea unitară a unor componente într-un limbaj de programare cunoscut, pe baza unor specificații de proiectare date C1.4 Testarea unor aplicații pe baza unor planuri de test C6 Proiectarea si administrarea rețelelor de calculatoare C6.5 Realizarea unor proiecte de rețele de calculatoare
Competențe transversale	CT3 Utilizarea unor metode și tehnici eficiente de învățare, informare, cercetare și dezvoltare a capacităților de valorificare a cunoștințelor, de adaptare la cerințele unei societăți dinamice și de comunicare în limba română și într-o limbă de circulație internațională

7. Obiectivele disciplinei (reieşind din grila competenţelor acumulate)

7.1 Obiectivul general al disciplinei	Scopul cursului este de a crește gradul de conștientizare a securității de către studenții IT, de a le modela percepția asupra securității, de a-i pregăti pentru provocările practice de securitate IT și de a le oferi o imagine de ansamblu a soluțiilor de securitate IT în practică. În acest scop, cursul oferă o prezentare generală introductivă a diferitelor domenii ale securității IT, descriind provocările și soluțiile din fiecare domeniu. În unele dintre domeniile prioritare (de exemplu, securitatea software, securitatea sistemelor web, criptografia), exercițiile practice vor fi efectuate într-un mediu de laborator, astfel încât, în aceste domenii, cursul urmărește să ofere o înțelegere a metodelor prezentate în prelegeri și a aplicării acestora. De asemenea, cursul este destinat să ofere o bază pentru studenții care doresc să își aprofundeze cunoștințele în domeniul securității IT în cadrul unui program de masterat.
7.2 Obiective specifice	

8. Conţinutul cursului

8.1 Curs	Metode de predare	Observaţii
Concepte de bază ale securității IT, abordarea bazată pe riscuri a securității IT: obiective de securitate de bază (CIA, AAA); prezentare generală a modelelor de atac, a vulnerabilităților, a mecanismelor de securitate; gestionarea riscurilor, ingineria securității și procesele operațiunilor de securitate; aspecte etice în securitatea IT. (2x45 minute)	curs, proiecție, explicație, exemple	

Istoria criptografiei: introducere în conceptele criptografice de bază prin exemple istorice, prezentând în același timp principalele repere din istoria criptografiei. Algoritmi criptografici moderni: criptografie cu cheie simetrică și asimetrică, funcții hash, autentificarea mesajelor, semnătura digitală, generarea de numere aleatorii, protocoale de schimb de chei, PKI. Prezentare generală a aplicațiilor criptografice moderne, probleme practice ale sistemelor criptografice. (6x45 minute)	curs, proiecție, explicație, exemple	
Concepte, metode și aplicații de autentificare: o introducere în metodele de autentificare bazate pe cunoștințe, posesie și atribute utilizate în prezent. Principiile lor de funcționare, avantajele și dezavantajele. Atacuri posibile împotriva fiecărei metode, apărări împotriva atacurilor. Autentificare cu doi și mai mulți factori. Studii de caz. Introducere în conceptele și funcționarea unor standarde, cadre și protocoale legate de autentificare (de exemplu, OpenID, Kerberos, FIDO). Concepte de acordare a licențelor, metode, aplicare: scopul acordării licențelor, abordări. Introducere în conceptele și funcționarea unora dintre principalele standarde, cadre și protocoale (de exemplu, OAuth, SAML) legate de autorizare; exemple din viața noastră de zi cu zi, studii de caz. (4x45 minute)	curs, proiecție, explicație, exemple	
Controlul accesului și concepte conexe. Model general de control al accesului și cele două abordări principale ale acestuia: DAC, MAC. Autorizarea și controlul accesului pe sistemele de operare bazate pe Linux: utilizatori, grupuri, biți de permisiune; POSIX ACLs, SELinux, AppArmor. Autorizarea și controlul accesului pe sistemele de operare Windows: utilizatori, grupuri, permisiuni la nivel de sistem de fișiere și partajare. (2x45 minute)	curs, proiecție, explicație, exemple	

Provocări legate de securitatea software-ului: probleme potențiale și soluții în timpul proiectării, dezvoltării, testării și exploatării. Introducere în provocările de securitate în etapele procesului de dezvoltare a aplicațiilor; provocările de securitate în proiectare; analiza și testarea de securitate a software-ului (revizuirea codului, analiza riscurilor arhitecturale, testarea penetrării software-ului, fuzzing), introducerea unor instrumente care ajută la testare. Provocări de implementare pentru limbajele de programare de nivel scăzut: cauzele și exploatarea erorilor de corupere a memoriei (tipuri de probleme de securitate care rezultă din erorile de programare, modul în care funcționează tehnicile de exploatare, exemple ilustrative, de exemplu, depășirea tamponului, depășirea heap-ului, format string, ROP etc.); prezentarea de soluții de protecție pentru a face atacurile mai dificile. Provocări în sistemele web: prezentarea atacurilor din partea clientului și a serverului (injecție SQL, XSS, CSRF etc.) și a posibilelor soluții de protecție (SOP, CSP etc.) care reprezintă o amenințare pentru aplicații. (8x45 minute)	curs, proiecție, explicație, exemple	
Provocări legate de securitatea rețelelor: fazele unui atac tipic asupra unei rețele (detectare, penetrare, instalare de backdoor, deplasare laterală și escaladarea privilegiilor, intruziune rădăcină), metode și instrumente utilizate în fiecare fază; testarea securității rețelelor (testare prin penetrare, hacking etic). (2x45 minute)	curs, proiecție, explicație, exemple	
Soluții de securitate a rețelelor: protecție perimetrală cu firewall-uri, tipuri de firewall-uri, modul în care acestea funcționează, setări tipice de configurare și defecțiuni tipice; tipuri de sisteme de detectare a intruziunilor și SIEM, modul în care acestea funcționează, rețele private virtuale. (4x45 minute)	curs, proiecție, explicație, exemple	
Conceptul și funcționarea programelor malițioase (malware): Tipuri de software rău intenționat (viruși, viermi, troieni etc.), modul în care funcționează, cum se răspândesc și cum se ascund (rootkit-uri), aplicații (criminalitate informatică, botnet-uri, atacuri țintite). Detectarea programelor malware. (2x45 minute)	curs, proiecție, explicație, exemple	
Aspecte operaționale ale securității sistemelor informatice: Gestionarea vulnerabilităților, actualizare, back-up. Gestionarea incidentelor de securitate: detectarea infecțiilor cu programe malware, gestionarea incidentelor bazate pe programe malware, analiza jurnalelor, noțiuni de bază privind analiza criminalistică a memoriei și a discurilor. (2x45 minute)	curs, proiecție, explicație, exemple	

Protecția datelor cu caracter personal (viața privată): Confidențialitatea și conceptul de date personale, exemple motivaționale. Tehnici de urmărire web (de exemplu, amprentarea browserului, module cookie de la terți). Operarea sistemelor de comunicații anonime, domenii de aplicare. Auditarea interogărilor. Anonimizare, profilare psihologică. (2x45 minute)	curs, proiecție, explicație, exemple	
Provocări de securitate ale învățării automate: Exemple motivaționale. Probleme CIA (confidențialitate, integritate, disponibilitate) în învățarea automată, auditarea modelelor de mașini, fundal juridic. Confidențialitate: Inversare de model, atac de Membership. Integritate: Tipuri de atac (evaziune), poluare a datelor de învățare (poluare vizată). Disponibilitate: Generarea schemelor de tip sponge, poluare nețintă (untargeted pollution). (4x45 minute)	curs, proiecție, explicație, exemple	
Abordarea economică a securității și confidențialității: Rolul stimulentelor economice individuale și organizaționale în securitatea informațiilor. Informații asimetrice: contraselecție, hazard moral, piață tragac (The Market for Lemons). Lipsa de aliniere a stimulentelor: exemple, piață pentru instrumente și servicii de securitate IT. Externalități: securitatea ca externalitate, dependențe încrucișate de securitate. Economia vulnerabilităților. Asigurare cibernetică. Probleme economice de confidențialitate, dependențe încrucișate de confidențialitate, exemple: Facebook, Google, genom, locație, sisteme k-anonim. (4x45 minute)	curs, proiecție, explicație, exemple	

Bibliografie

1. Materiale de lectură online pentru prelegeri (capitole de carte, articole, serii de bloguri)
2. Capitole ale colecției online Cyber Security Body Of Knowledge (CyBOK) (https://www.cybok.org/)

8.2 Laboratoare	**Metode de predare**	**Observaţii**
Laborator 1: Folosirea unei biblioteci de programe criptografice: Crearea de programe folosind mecanisme criptografice (criptare, semnătură digitală) folosind biblioteci de programe criptografice adecvate.	Soluția problemelor	
Laborator 2: Validare input: Stăpânirea verificărilor adecvate ale datelor care vin prin interfața de atac prin crearea unei aplicații care poate gestiona corect intrările specificate, potențial periculoase.	Soluția problemelor	
Laborator 3: Testarea securității software: Cunoașterea și învățarea metodelor de testare care apar în cazul aplicațiilor dezvoltate cu diferite tehnologii, cu accent	Soluția problemelor	

deosebit pe aplicațiile dezvoltate în limbaje de nivel scăzut.		
Laborator 4: Securitatea sistemelor web: Înțelegerea și testarea atacurilor care amenință aplicațiile web; selectarea sau aplicarea potenţialelor de apărare care opresc atacurile.	Soluția problemelor	
Laborator 5: Managementul incidentelor, analiza digitala (forensics): Analiza jurnalelor, analiza traficului de rețea înregistrat (packet capture), analiza digitală a imaginii de memorie și stocarea de rezervă (memory and disk forensics).	Soluția problemelor	
Laborator 6: Protecția datelor cu caracter personal (viața privată): Dezvoltarea unui auditor de interogări folosind o bibliotecă de algebră liniară potrivită.	Soluția problemelor	
Bibliografie 1. Materiale de lectură online pentru prelegeri (capitole de carte, articole, serii de bloguri) 2. Capitole ale colecției online Cyber Security Body Of Knowledge (CyBOK) (https://www.cybok.org/)		

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

- Tematica cursului se suprapune cu cea a unor discipline similare predate în marile universități.
- Materialele didactice au fost elaborate pe baza lucrărilor celor mai recunoscuți autori la nivel internațional, iar lecturile recomandate se bazează, de asemenea, pe cele mai relevante lucrări din domeniu.
- Subiectele predate în acest curs sunt necesare pentru un loc de muncă în industria actuală de dezvoltare de software grafic, iar companiile așteaptă acest tip de cunoștințe.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	1 examen parțial (condiție pentru finalizarea cu succes: atingerea a cel puțin 40% din punctajul care poate fi obținut)		33,(3)%
	Examen scris (condiție pentru finalizarea cu succes: atingerea a cel puțin 40% din punctajul examenului)		66,(6)%
10.5 Seminar / Laborator	În cazul a 6 laboratoare, cel puțin 4 laboratoare trebuie finalizate cu succes (dacă unul dintre laboratoare este ratat pe parcursul semestrului, 3 laboratoare trebuie finalizate cu succes) pentru a obține semnătura (condiție pentru finalizarea cu succes: cel puțin 75% din laboratoare). puncte obținute în timpul practicii de laborator)		0 %

10.6 Standard minim de performanţă
Condiții pentru o notă de trecere: ● Obținerea notei min. 40% la examenul parțial și examenul final. ● Obținerea min. 75% din punctajul totale al laboratoarelor.

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
19. iulie, 2024.	Lect. dr. ing. Kolumbán Sándor	Lect. dr. ing. Kolumbán Sándor

Data avizării în departament	Semnătura directorului de departament
19. iulie, 2024.	Conf. dr. ANDRÁS Szilárd Károly