

## **PROGRAMUL DE MASTER**

### **SISTEME AVANSATE DE SECURITATE**

### **(ADVANCED CYBER SECURITY)**

#### **Descrierea disciplinelor din planul de învățământ**

##### **Criptografie aplicată**

Cursul are ca obiective cunoașterea elementelor fundamentale ale criptografiei și înțelegerea aplicării acestor concepte în aplicații punctuale, incluzând cele de securitate națională

Pentru studenți cursul va însemna cunoașterea elementelor fundamentale criptografice, cunoașterea punctelor slabe în implementări și algoritmi criptografici din trecut și prezent, înțelegerea securității unui sistem criptografic, capacitatea de a realiza o evaluare a securității unui sistem criptografic, cunoașterea celor mai răspândiți algoritmi criptografici, atât cu chei simetrice cât și cu chei asimetrice, înțelegerea funcționării și securității celor mai răspândite sisteme criptografice, precum TLS și EMV.

**Titular(i) curs/seminar/laborator:** șl.dr.ing. Marios CHOUDARY

##### **Protocoale de securitate**

Cursul urmărește înțelegerea conceptelor și utilizarea mecanismelor pentru protecția rețelelor de calculatoare și cele pentru realizarea unei conexiuni securizate.

Obiectivele specifice ale cursului sunt:

- Cunoașterea fundamentelor legate de controlul accesului în internet
- Cunoașterea sistemelor de schimb de chei
- Înțelegerea mecanismelor de stabilire a unei conexiuni securizate
- Analiza securității unui protocol de comunicare
- Cunoașterea atacurilor uzuale din Internet și a metodelor de protecție împotriva lor

**Titular(i) curs/seminar/laborator:** șl.dr.ing. Cătălin LEORDEANU, șl.dr.ing. Elena APOSTOL

##### **Securitatea cibernetică a infrastructurilor critice**

Cursul acoperă problematica protecție infrastructurilor critice, ca parte integrantă a securității cibernetice, a modului de realizare a interdependenței și rezilienței acestora.

Cursul își propune instruirea studenților în vederea asigurării securității cibernetice a

infrastructurilor critice și a protecției infrastructurilor critice cibernetice. Obiectivele specifice ale cursului sunt:

- Cunoașterea fundamentelor legate de securitatea cibernetică și integrarea acestora în securitatea națională.
- Cunoașterea mecanismelor de realizare a protecției infrastructurilor critice și a securității cibernetice a acestora
- Implementarea planului de securitate cibernetică a infrastructurilor critice
- Asigurarea palurilor de reziliență a infrastructurilor critice

**Titular(i) curs/seminar/laborator:** lect.univ.dr. Victor VEVERA

## Securitatea sistemelor informaționale

Cursul “Securitatea sistemelor informaționale” pornește de la perspectiva funcționării sistemelor de calcul și aspecte ce țin de securitatea componentelor acestora. Pornind de la structura sistemelor de calcul moderne, vom prezenta obiectivele de securitate (confidențialitate, integritate, disponibilitate, siguranță), modele adversariale, taxonomii de atacuri.

La sfârșitul cursului studenții vor putea să:

- Evalueze nivelul de securitate al unui sistem informațional
- Recunoască amenințări și vulnerabilități la nivelul sistemelor
- Propună soluții, biblioteci, aplicații, arhitecturi care să maximizeze securitatea unui sistem
- Proiecteze și să dezvolte sigur componente în sistemele informaționale
- Folosească bune practici în integrarea fiabilă și securizată a componentelor și gestiunea unui sistem informatic

Partea practică a cursului va presupune:

- Analiza specificațiilor de securitate a sistemelor de operare, aplicațiilor și serviciilor
- Descoperirea vulnerabilităților de securitate, prin auditarea sistemului, codului și tehnici de inginerie inversă (reverse engineering)
- Folosirea tehnicilor de securizare pentru protejarea sistemului și aplicațiilor

**Titular(i) curs/seminar/laborator:** conf.dr.ing. Costin RAICIU, șl.dr.ing. Răzvan DEACONESCU

## Securitatea în sistemele grid și cloud

Cursul urmărește înțelegerea metodelor de a asigura securitatea informațiilor stocate sau în tranzit în cazul folosirii de resurse fizice comune (stocare și networking).

Obiectivele specifice ale cursului sunt:

- cunoașterea sistemelor ce asigură identitatea entităților precum și legăturile de încredere dintre acestea;
- cunoașterea unor reguli de securitate minimale pentru a preveni și contracara atacuri în mediul virtual.

**Titular(i) curs/seminar/laborator:** prof.dr.ing. Nicolae Țăpuș, șl.dr.ing. Mihai CARABAȘ

## Cyberdefense și cyberintelligence. Tehnici de securitate cibernetică

Cursul își propune prezentarea și asimilarea metodologiilor, utilităților și tehnicilor de investigare și securizare a sistemelor de calcul existente. Perspectiva prin care vor fi abordate tematicile este aceea a unui investigator sau analist de securitate, care, având la dispoziție utilitare dedicate și competențele necesare, poate descoperi vulnerabilități și defecte în infrastructura sau aplicațiile folosite.

Obiectivele specifice sunt:

- Descrierea și utilizarea principalelor tehnici de investigare
- Identificarea și remedierea principalelor vulnerabilități ale sistemelor de calcul
- Evaluarea și îmbunătățirea securității pentru sistemele de calcul
- Identificarea principalelor surse de informații pentru securitate
- Implementarea mecanismelor specifice de îmbunătățire a securității sistemelor de calcul
- Folosirea utilităților specifice pentru determinarea securității unei aplicații
- Inspectarea traficului de rețea pentru a determina probleme de securitate

**Titular(i) curs/seminar/laborator:** prof.dr.ing. Nirvana POPESCU, șl.dr.ing. Mihai CHIROIU

## Securitatea dispozitivelor mobile

În cadrul acestui curs vor fi prezentate modele și mecanisme de securitate pentru dispozitive mobile. Vor fi abordate subiectele securității sistemului de operare, rețelei și aplicațiilor.

Obiectivele specifice cursului sunt:

- Cunoașterea arhitecturii sistemelor de operare pentru dispozitive mobile
- Cunoașterea modelelor și mecanismelor de securitate pentru dispozitive mobile
- Înțelegerea mecanismelor de securizare și depanare a aplicațiilor și comunicațiilor prin rețea

- Înțelegerea atacurilor și aplicațiilor malițioase pentru dispozitive mobile
- Înțelegerea modului de identificare și exploatare a vulnerabilităților pe dispozitive mobile

**Titular(i) curs/seminar/laborator:** conf.dr.ing. Dragoș NICULESCU, șl.dr.ing. Laura RUSE

## **Tehnologii de protecție a vieții private**

Acest curs urmărește dezvoltarea competențelor studenților de a asigura confidențialitatea datelor în scenarii și tehnologii diverse (data privacy), respectând standardele, drepturile utilizatorilor și cerințele legale, inclusiv exigențele General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). În cadrul cursului vor fi prezentate principalele concepte și mecanisme pentru protecția datelor, tipurile de scenarii și de tehnologii necesare pentru a asigura confidențialitatea precum și posibilitățile de atac și prevenirea acestora.

Obiectivele specifice sunt:

- Cunoașterea fundamentelor legate de confidențialitatea datelor (data privacy)
- Înțelegerea mecanismelor de asigurare a confidențialității datelor conform exigențelor GDPR
- Analiza confidențialității într-un scenariu de culegere, transmitere, analiză și utilizare a datelor
- Cunoașterea atacurilor privind confidențialitatea datelor și a metodelor de protecție împotriva lor
- Diagnoza platformelor și soluțiilor de comunicare în ceea ce privește asigurarea confidențialității datelor
- Identificarea atacurilor privind datele și prevenirea lor
- Implementarea mecanismelor de asigurare a confidențialității datelor în diferite scenarii de utilizare
- Aplicarea cunoștințelor în cadrul unor proiecte dezvoltate pe parcursul laboratorului

**Titular(i) curs/seminar/laborator:** prof.dr.ing. Răzvan RUGHINIȘ, șl.dr.ing. Mihai CHIROIU

## Proiectarea dispozitivelor criptografice folosind FPGA

Cursul urmărește aprofundarea cunoștințelor cu privire la metodele de proiectare, implementare și testarea de dispozitive criptografice în tehnologia FPGA.

Obiectivele specifice sunt:

- Înțelegerea tuturor fazelor necesare proiectării, implementării și testării unui circuit hardware
- Proiectarea, implementarea și testarea celor mai importante circuit criptografice folosind FPGA
- Înțelegerea vulnerabilităților circuitelor hardware la injectarea de cod malițios și identificarea metodelor de prevenire
- Protecția memoriei în FPGA

**Titular(i) curs/seminar/laborator:** prof.dr.ing. Decebel POPESCU, șl.dr.ing. Vlad CIOBANU

## Managementul incidentelor de securitate cibernetică

Cursul urmărește utilizarea corectă și securizată a aplicațiilor aflate în mediul virtual.

Obiectivele specifice sunt:

- Înțelegerea principalelor pericole privind accesul nesecurizat la Internet
- Cunoașterea elementelor minimale de acces securizat la Internet
- Cunoașterea unor reguli de securitate minimale pentru a preveni și contracara atacuri în mediul virtual.

**Titular(i) curs/seminar/laborator:** CS III Alin ZAMFIROIU

## Managementul securității informației

Cursul acoperă problematica securității informației la nivelul organizației, modului de implementareaa unui sistem de management al securității informației și element legate de auditul de securitate

Cursul își propune instruirea studenților in vederea proiectarii și implementării corecte a unui sistem de securitate a informației (SMSI) folosind standardele recunoscute la nivel internațional și național. Obiectivele specifice ale cursului sunt:

- Cunoașterea elementelor necesare proiectării și implementării unui sistem de management al securității informației
- Cunoașterea standardelor aplicabile la nivel internațional/national privind securitatea informației (ISO27k, COBIT, directiva NIS etc.)
- Implementarea unui sistem de management al securității informației (SMSI)
- Auditarea unui SMSI

**Titular(i) curs/seminar/laborator:** Conf.univ.dr. Meda UDROIU

## Cercetare științifică

Activitatea de cercetare în cadrul acestui program va fi o experiență unică și esențială pentru formarea ta profesională. Va realiza fixarea și aprofundarea cunoștințelor de la cursuri, prin proiecte concrete, și în același timp îți va deschide un orizont de cercetare, inovare, creativitate, ajutându-te să devii un inginer de concepție și nu doar de execuție. Îți vei dezvolta expertiza tehnică avansată, creativitatea, capacitatea de studiu individual avansat, autonomia și responsabilitatea dar și cea de colaborare cu colegi sau specialiști de top, din facultate și industria de profil, în cadrul unor teme complexe și provocatoare.

Fiecare student va primi o temă de cercetare la care va lucra pe parcursul celor 4 semestre, finalizându-se prin proiectul de disertație.

Recomandăm păstrarea aceleiași teme de cercetare pe parcursul celor 4 semestre, pentru a se putea finaliza (în disertație) cu un rezultat avansat, complex.

Exemple de teme:

- Verificarea automată a mecanismelor de securitate în sisteme de operare mobile
- Metode de protecție automată pentru programe C/C++
- Metode criptografice inovative în SoC
- Metode hardware pentru implementarea memoriilor „doar de execuție”.
- Metode de criptare a datelor și instrucțiunilor în memorie
- Analiza / proiectarea și dezvoltarea unui SMSI
- Auditul unui SMSI