

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA OVIDIUS DIN CONSTANȚA

Aleea Universității, nr.1, Campus, Corp A, cod 900470 Constanța, România

Tel./Fax: +4 0241 606.407 / +4 0241 606.467

E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

Facultatea: de MATEMATICA ȘI INFORMATIĂ

Domeniul de masterat: INFORMATICĂ

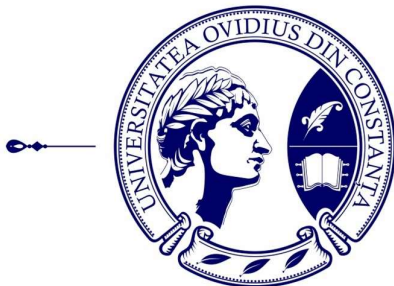
**Programul de studii universitare de masterat: SECURITATE CIBERNETICA SI INVATARE AUTOMATA (ÎN LIMBA ENGLEZĂ)/
CYBER SECURITY AND MACHINE LEARNING**

COMPATIBILITATEA DINTRE OBIECTIVE ȘI REZULTATELE ÎNVĂȚĂRII

Obiectivele programului de studii Cyber Security and Machine Learning (Securitate cibernetică și învățare automată) sunt exprimate în termeni de **competențe profesionale și competențe transversale**

A. COMPATIBILITATEA DINTRE COMPETENȚELE ESCO ALE PROGRAMULUI DE STUDII *CYBER SECURITY AND MACHINE LEARNING (SECURITATE CIBERNETICĂ ȘI ÎNVĂȚARE AUTOMATĂ)* ȘI REZULTATELE ÎNVĂȚĂRII

COMPETENȚE ESCO	REZULTATELE ÎNVĂȚĂRII
C1. Capacitatea de a implementa gestionarea riscurilor in TIC: Dezvolta si implementeaza proceduri pentru identificarea, evaluarea, tratarea si atenuarea riscurilor TIC, Analizeaza si gestioneaza riscurile si incidentele de securitate, Recomanda masuri de imbunatatire a strategiei de securitate digitala.	Absolventul: • Identifică, clasifică și evaluează riscurile asociate infrastructurilor și serviciilor TIC, utilizând metode calitative și cantitative de analiză a riscurilor • Elaborează și implementează proceduri de tratare și atenuare a riscurilor, respectând standarde internaționale de securitate cibernetică (ISO/IEC 27005, NIST SP 800-30) • Analizează incidentele de securitate, determinând cauzele, impactul și posibilele vulnerabilități exploatare • Propune măsuri corective și preventive pentru îmbunătățirea strategiei de securitate digitală a organizației • Contribuie la dezvoltarea unei culturi organizaționale orientate spre managementul proactiv al riscurilor și reziliența cibernetică.
C2. Capacitatea de a dezvolta strategia de securitate a informațiilor,	• Absolventul:



MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA OVIDIUS DIN CONSTANȚA

Aleea Universității, nr.1, Campus, Corp A, cod 900470 Constanța, România

Tel./Fax: +4 0241 606.407 / +4 0241 606.467

E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

pentru a maximiza integritatea informațiilor, disponibilitatea și confidentialitatea datelor.

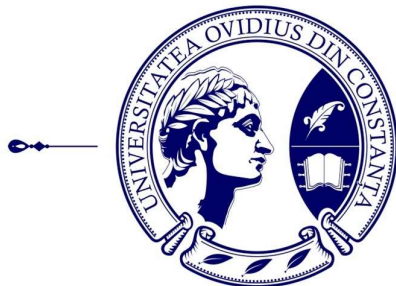
- Analizează infrastructura informațională a unei organizații și identifică activele critice care necesită protecție
- Elaborează politici și proceduri de securitate a informațiilor, aliniate la principiile fundamentale de confidențialitate, integritate și disponibilitate (CIA Triad)
- Definește obiective strategice și planuri de acțiune pentru implementarea unei arhitecturi de securitate coerente și eficiente
- Aplică standarde și bune practici recunoscute la nivel internațional (ISO/IEC 27001, NIST Cybersecurity Framework) în dezvoltarea și auditarea strategiei de securitate
- Evaluează periodic eficiența măsurilor de securitate adoptate și propune îmbunătățiri continue pentru creșterea rezilienței organizaționale la amenințări cibernetice.

○

C3. Capacitatea de a conduce exerciții de recuperare a datelor în urma dezastrelor în funcționarea sau securitatea sistemelor TIC, cum ar fi în ceea ce privește recuperarea datelor, protecția identității și a informațiilor și măsurile care trebuie luate pentru a preveni alte probleme.

Absolventul:

- Proiectează și coordonează planuri de continuitate a activității (Business Continuity Plans) și de recuperare în caz de dezastru (Disaster Recovery Plans) pentru sisteme informatice complexe
- Evaluează impactul incidentelor critice asupra datelor, infrastructurii și serviciilor TIC, propunând soluții rapide și eficiente pentru restabilirea funcționalității
- Aplică proceduri de backup, restaurare și replicare a datelor, asigurând integritatea și disponibilitatea informațiilor după incidente majore
- Gestionează măsuri de protecție a identității digitale și a datelor sensibile în procesele de remediere post-incident
- Coordonează exerciții simulate de recuperare după dezastru și propune îmbunătățiri pentru prevenirea incidentelor similare în viitor.



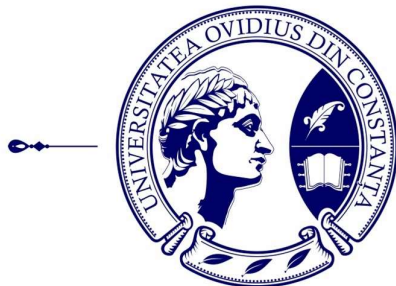
MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA OVIDIUS DIN CONSTANȚA

Aleea Universității, nr.1, Campus, Corp A, cod 900470 Constanța, România

Tel./Fax: +4 0241 606.407 / +4 0241 606.467

E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

C4. Capacitatea de a efectua teste de securitate TIC, cum ar fi testele de penetrare a rețelei, testarea fara fir, evaluarile codurilor, evaluarile de tip wireless si/sau firewall, în conformitate cu metodele si protocoalele acceptate la nivel de industrie pentru a identifica si a analiza eventuale vulnerabilitati.	Absolventul: • Planifică, configurează și execută teste de penetrare (penetration testing) asupra aplicațiilor, rețelilor și infrastructurilor informatice, respectând cadre metodologice recunoscute (OWASP, PTES, NIST SP 800-115) • Utilizează instrumente specializate pentru scanarea și evaluarea vulnerabilităților în medii locale, cloud și mobile • Evaluează securitatea aplicațiilor software prin analiza codului sursă (code review) și testarea componentelor critice • Interpretează rezultatele testelor de securitate și redactează rapoarte tehnice care includ riscurile identificate, impactul potențial și recomandările de remediere • Respectă principiile etice și cadrul legal asociat testării de securitate, asigurând confidențialitatea datelor și evitarea impactului negativ asupra sistemelor testate
C5. Capacitatea de a gestiona planurile de recuperare în urma dezastrelor ce pot cauza pierderi de date din sistemul informational.	Absolventul: • Elaborează, implementează și menține planuri de recuperare a datelor în caz de dezastru (Disaster Recovery Plans), adaptate tipului și dimensiunii infrastructurii informatice • Evaluează riscurile asociate pierderii datelor și stabilește priorități pentru restaurarea sistemelor critice, în funcție de impactul asupra activității organizației • Coordonează procesele de backup, replicare și arhivare a datelor, aplicând soluții moderne de redundanță și stocare sigură • Gestionează procesul de restaurare a sistemelor și verifică integritatea datelor recuperate, asigurând continuitatea operațională minimă



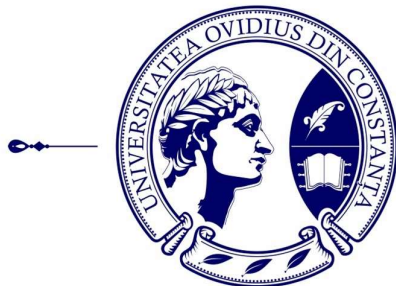
MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA OVIDIUS DIN CONSTANȚA

Aleea Universității, nr.1, Campus, Corp A, cod 900470 Constanța, România

Tel./Fax: +4 0241 606.407 / +4 0241 606.467

E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

	• Revizuieste și actualizează periodic planurile de recuperare, integrând lecțiile învățate din testări și incidente anterioare pentru a îmbunătăți reziliența sistemului informațional.
C6. Capacitatea de a gestiona securitatea sistemelor TIC: Aplica tehnici de detectare pentru securitate. Înțelege tehnicile de atac cibernetic și pune în aplicare contramăsuri eficiente.	Absolventul: • Monitorizează și analizează evenimentele și alertele de securitate din infrastructurile TIC, utilizând sisteme specializate de detecție și prevenire a intruziunilor (IDS/IPS, SIEM) • Identifică tiparele și tehnicile specifice atacurilor cibernetice (phishing, malware, ransomware, DDoS, SQL injection etc.) și evaluează gradul de expunere al sistemelor • Aplică contramăsuri eficiente pentru prevenirea, detectarea și răspunsul la incidente, bazându-se pe bune practici și standarde internaționale (MITRE ATT&CK, NIST, ENISA) • Coordonează activitățile de reacție la incidente și asigură restaurarea rapidă a funcționalității sistemelor compromise • Evaluează eficiența măsurilor de protecție implementate și propune îmbunătățiri continue ale mecanismelor de securitate.
C7. Capacitatea de a realiza analize de date, de a culege date și statistici în vederea testării și evaluării pentru a genera afirmații și previziuni de tipare, cu scopul de a descoperi informații utile în procesul de decizie.	• Absolventul: • Colectează, curăță și prelucrează seturi complexe de date provenite din surse eterogene, asigurând calitatea și integritatea informațiilor • Aplică tehnici de analiză statistică, explorare a datelor (data mining) și vizualizare pentru identificarea tendințelor, corelațiilor și anomaliilor relevante • Utilizează algoritmi de învățare automată pentru generarea de modele predictive și descriptive care sprijină procesul decizional • Interpretează critic rezultatele analizelor, formulând concluzii și recomandări bazate pe date concrete



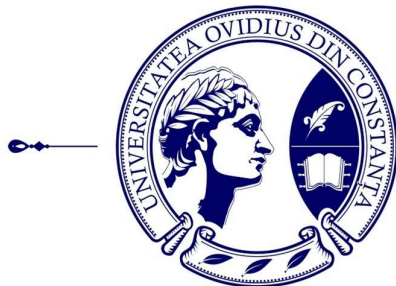
MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA OVIDIUS DIN CONSTANȚA

Aleea Universității, nr.1, Campus, Corp A, cod 900470 Constanța, România

Tel./Fax: +4 0241 606.407 / +4 0241 606.467

E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

	• Documentează și comunică rezultatele analitice într-o formă clară și profesionistă, adaptată contextului organizațional sau de cercetare.
C8. Capacitatea de a mentine securitatea bazelor de date.	Absolventul: • Proiectează și implementează politici de securitate pentru baze de date, asigurând confidențialitatea, integritatea și disponibilitatea informațiilor stocate • Gestionează conturile utilizatorilor, rolurile și privilegiile de acces, aplicând principiul least privilege și controale bazate pe rol (RBAC) • Aplică metode de criptare a datelor la nivel de coloană, rând sau tabel, precum și tehnici de mascare și anonimizare a informațiilor sensibile • Monitorizează activitățile din baza de date pentru detectarea accesărilor neautorizate și a încercărilor de compromitere • Asigură implementarea planurilor de backup și recuperare a datelor, precum și auditarea periodică a configurărilor de securitate ale sistemului de gestiune a bazelor de date.
C9. Capacitatea de a crea modele de date, utilizand tehnici si metodologii specifice.	Absolventul: • Analizează cerințele informaționale ale sistemelor informatice și identifică entitățile, atributele și relațiile dintre acestea • Utilizează metode formale de modelare a datelor (ER, UML, modele relaționale) pentru proiectarea schemelor conceptuale și logice ale bazelor de date • Aplică principii de normalizare și optimizare pentru crearea de modele de date eficiente, coerente și scalabile • Utilizează instrumente software specializate pentru modelarea și documentarea structurilor de date, integrând bune practici de guvernanta a datelor



MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA OVIDIUS DIN CONSTANȚA

Aleea Universității, nr.1, Campus, Corp A, cod 900470 Constanța, România

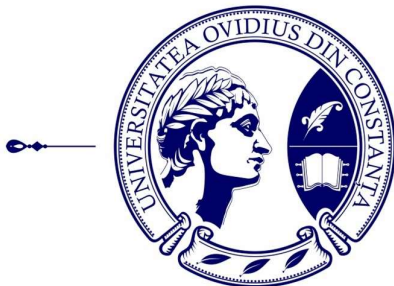
Tel./Fax: +4 0241 606.407 / +4 0241 606.467

E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

	• Evaluează și validează modelele de date în raport cu cerințele sistemului și cu nevoile organizaționale, asigurând compatibilitatea cu politicile de securitate și confidențialitate a datelor.
C10. Capacitatea de a proiecta arhitecturi de tip cloud și de a dezvolta servicii de tip cloud computing.	Absolventul: • Analizează cerințele sistemelor informatice și selectează modele adecvate de implementare a arhitecturilor cloud (IaaS, PaaS, SaaS, FaaS) • Proiectează și implementează soluții cloud scalabile, sigure și eficiente, utilizând platforme consacrate (AWS, Azure, Google Cloud, Oracle Cloud) • Dezvoltă și gestionează servicii de tip cloud computing, integrând tehnologii de containerizare, virtualizare și orchestrare (Docker, Kubernetes) • Aplică politici de securitate, confidențialitate și conformitate în mediile cloud, protejând datele și resursele distribuite • Monitorizează performanța și disponibilitatea serviciilor cloud, implementând mecanisme de optimizare și recuperare în caz de defecțiuni.

B. COMPATIBILITATEA DINTRE COMPETENȚELE TRANSVERSALE ALE PROGRAMULUI DE STUDII *INFORMATICĂ* ȘI REZULTATELE ÎNVĂȚĂRII

COMPETENȚE TRANSVERSALE	REZULTATELE ÎNVĂȚĂRII
CT1. Aplicarea regulilor de organizare a muncii, înțelegerea responsabilităților și respectarea regulilor de etică profesională, precum și a celor de securitate și confidențialitate a datelor	Absolventul demonstrează abilitatea de a: • respecta principiile de etică profesională și deontologie în activitățile de cercetare, dezvoltare software și securitate cibernetică



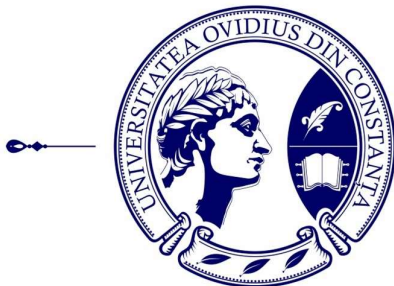
MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA OVIDIUS DIN CONSTANȚA

Aleea Universității, nr.1, Campus, Corp A, cod 900470 Constanța, România

Tel./Fax: +4 0241 606.407 / +4 0241 606.467

E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

	• aplica regulile de organizare a muncii individuale și în echipă, asumându-și responsabilitățile specifice proiectelor de securitate și analiză a datelor • asigura protecția și confidențialitatea informațiilor sensibile, în conformitate cu legislația în vigoare (GDPR, NIS2, ISO/IEC 27001) și politicile interne ale organizațiilor • evalua impactul deciziilor tehnice asupra aspectelor etice, juridice și sociale, adoptând o atitudine responsabilă în utilizarea tehnologiilor digitale și a inteligenței artificiale • promova un comportament profesional integru, bazat pe respectarea drepturilor de proprietate intelectuală, securitatea informațiilor și colaborarea etică în mediul academic și profesional.
CT2. Identificarea rolului unei echipe interdisciplinare și asumarea responsabilităților corespunzătoare profilului profesional și personal	Absolventul demonstrează abilitatea de a: • recunoaște structura, rolurile și dinamica unei echipe interdisciplinare implicate în proiecte de securitate cibernetică și învățare automată • colaborează eficient cu specialiști din domenii complementare — precum rețelistică, dezvoltare software, analiză de date, drept cibernetic sau management IT — pentru atingerea obiectivelor comune • își asuma responsabilitățile și contribuția personală în cadrul echipei, în funcție de competențele profesionale și de obiectivele proiectului • manifesta abilități de comunicare, negociere și leadership în contexte de lucru colaborativ, inclusiv în echipe internaționale sau virtuale • valorifica diversitatea de perspective și expertize din echipă pentru a genera soluții inovatoare și eficiente la probleme complexe de



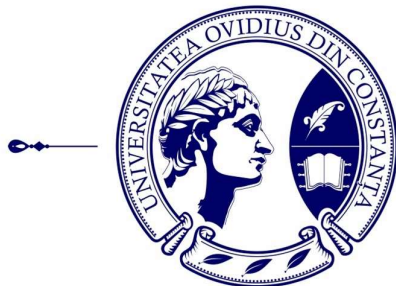
MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA OVIDIUS DIN CONSTANȚA

Aleea Universității, nr.1, Campus, Corp A, cod 900470 Constanța, România

Tel./Fax: +4 0241 606.407 / +4 0241 606.467

E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

CT3. Utilizarea eficientă a surselor de informare și comunicare și a pregătirii profesionale	securitate și analiză inteligentă a datelor. Absolventul demonstrează abilitatea de a: • identifica, evalua critic și utiliza eficient surse de informare științifică, tehnică și profesională din domeniile securității cibernetice, învățării automate și tehnologiilor informaționale • folosi instrumente digitale moderne, baze de date, platforme de cercetare și canale de comunicare profesională pentru documentare, analiză și colaborare • redacta și prezenta rapoarte, studii și documentații tehnice în mod clar, coerent și argumentat, adaptând stilul de comunicare la contextul profesional și la publicul țintă • comunica eficient în limba română și în limba engleză, utilizând terminologia de specialitate specifică securității informațiilor și inteligenței artificiale • aplica principiile etice și legale în procesul de colectare, prelucrare și diseminare a informațiilor, asigurând protejarea datelor și respectarea proprietății intelectuale.
CT4. Gândire analitică, capacitatea de rezolvare a problemelor	Absolventul demonstrează abilitatea de a: • analiza situații complexe din domeniul securității cibernetice și al învățării automate, identificând cauzele, consecințele și relațiile dintre elementele implicate • aplica metode logice, algoritmice și statistice pentru formularea și rezolvarea problemelor tehnice, operaționale sau de cercetare • evalua alternative și selecta soluții optime bazate pe criterii de performanță, securitate și eficiență • integra instrumente informatice, modele predictive și tehnologii emergente pentru soluționarea problemelor reale din mediul organizațional sau de cercetare • manifesta spirit critic, rigoare științifică și creativitate în abordarea



MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA OVIDIUS DIN CONSTANȚA

Aleea Universității, nr.1, Campus, Corp A, cod 900470 Constanța, România

Tel./Fax: +4 0241 606.407 / +4 0241 606.467

E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

	problemelor noi, contribuind la inovare și la îmbunătățirea continuă a proceselor.
CT5. Capacitatea de interpretare, sintetizare și analiză critică a rezultatelor	Absolventul demonstrează abilitatea de a: • interpreta date, rezultate experimentale și analize tehnice, extrăgând concluzii relevante și argumentate științific • evalua validitatea și fiabilitatea rezultatelor obținute în procesele de cercetare, testare și implementare a soluțiilor de securitate cibernetică și învățare automată • sintetiza informațiile din surse multiple, integrându-le într-o viziune coerentă asupra problemelor analizate • formula judecăți critice bazate pe dovezi, identificând limitele, implicațiile și posibilitățile de extindere ale rezultatelor • comunica concluziile și recomandările într-o manieră clară, logică și fundamentată, adaptată contextului profesional, științific sau managerial.

Decan,

Conf. univ. dr. Nicola Aurelian

Coordonator program de studii de masterat,

Conf. univ. dr. Băutu Elena