UNIVERSITATEA MARITIMA DIN CONSTANTA

FACULTATEA ELECTROMECANICA NAVALA

RAPORT

In vederea incadrarii unui program nou de studii universitare de master intr-un domeniu de studii universitare de master acreditat

Program de studii

SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

Domeniul

INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE

Invatamant cu frecventa

Constanta

Iulie 2019

Date de contact:

UNIVERSITATEA MARITIMA din CONSTANTA
Constanța, 900663, Str. Mircea cel Bătrîn, Nr. 104
Tel: +40 241 664 740; Fax: +40 241 617 260
E-mail: info[at]cmu-edu.eu web: www.cmu-edu.eu
Webmaster: support[at]cmu-edu.eu

Persoane de contact:

Director department,
Conf.univ.dr.ing. Alexandra RAICU alexandra.raicu@cmu-edu.eu tel 0722 605 508

Nr.inregistrare UMC

RAPORT DE AUTOEVALUARE

Forma de invatamant: IF

Program de studii

SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

Domeniul

INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE

Datele cuprinse în prezentul Raport sunt complete, corecte şi conforme cu principiile eticii profesionale.

Rector,

Prof.univ.dr.ing. Panait Cornel

Director departament

Conf.univ.dr.ing. Raicu Alexandra

Nr. înregistrare Universitate 4960 **/ Data** 18.07.2019

Către

CONSILIUL ARACIS Bucureşti

Instituţia de învăţământ superior
UNIVERSITATEA MARITIMĂ DIN CONSTANŢA
Tel: 0241664740 Fax: 0241617260 E-mail: info@cmu-edu.eu

Consiliul de Administrație al

Universităţii Maritime din Constanța a hotărât ca, în conformitate cu prevederile art. 13, 17, 18, 29-32 din O.U.G. nr. 75 / 2005 privind asigurarea calităţii educaţiei, aşa cum a fost aprobată de Legea 87/2006, să solicite îndeplinirea procedurilor de evaluare pentru:

- **ÎNCADRAREA ÎN DOMENIU** următorului program de studii universitare de **MASTERAT**:
- Facultatea **Electromecanică Navală**
- Domeniul: **Inginerie electronică, telecomunicații și tehnologii informaționale**
- Program de studii: **Securitate Cibernetică și Managementul Riscurilor**
- Tipul de masterat: **profesional**
- Locația /Forma de învățământ **IF**
- Limba de desfăşurare a activităţilor din programul respectiv **română**
- Număr de credite (ECTS) **120**

Vă rugăm să ne transmiteţi contractul de prestări servicii corespunzător tipului de evaluare solicitat, pe care urmează să-l încheiem cu agenţia dumneavoastră.

Menţionăm că am luat la cunoştinţă de valoarea tarifelor stabilite prin H.G nr. 1731/2006 pentru activităţile întreprinse de ARACIS.

RECTOR,
Prof.univ.dr.ing. Cornel PANAIT
LS

MINISTERUL EDUCAȚIEI NAȚIONALE * UNIVERSITATEA MARITIMĂ DIN CONSTANȚA *

Notă: Persoana de contact este Prof.univ.dr.ing. Remus Zăgan, tel: 0727334377 fax 0241664740,
E-mail: zagan.remus@ cmu-edu.eu

SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

FORMA DE ÎNVĂŢĂMÂNT: **IF**

DIN CADRUL FACULTĂŢII ELECTROMECANICA NAVALA

UNIVERSITATEA MARITIMA DIN CONSTANTA

a) Răspuns privind validarea și înscrierea calificării în RNCIS
b) Aprobarea Senatul Universității, de înființare a programului de studii universitare de master ***Securitate cibernetică şi managementul riscurilor*** în domeniu de studii universitare de master acreditat ***Inginerie electronică, telecomunicaţii şi tehnologii informaţionale***;
c) Memoriu de analiza a programului de master ***Securitate cibernetică şi managementul riscurilor;***
d) Adrese firme-institutii pentru sustinerea infiinţării programului de studii master ***Securitate cibernetică şi managementul riscurilor;***
e) Analiza privind oportunitatea înființării unui nou program de studii universitare de master, ***Securitate cibernetică şi managementul riscurilor***, din punct de vedere al corelației cu cerințele pieței muncii;
f) Suplimentul la diplomă pentru programul de studii universitare de master ***Securitate cibernetică şi managementul riscurilor***, limba de predare este limba romana;
g) Planul de învățământ al programului de studii universitare de master ***Securitate cibernetică şi managementul riscurilor***, in limba romana;
h) Fișele disciplinelor din planul de învățământ în limba română;
i) Lista cadrelor didactice care vor acoperi activitățile didactice şi de cercetare. Conform Anexei ARACIS – Tabel privind îndeplinirea indicatorului „cadrele didactice titulare cu pregătirea inițială, sunt doctori şi cercetează în domeniul în care se include disciplinele din postul ocupat"

Adeverință privind validarea calificării
Nr. 3690 / 02.04.2019

Se adevereşte prin prezenta că Facultatea de Electromecanică Navală, din cadrul Universității Maritime din Constanța, reprezentată legal de către domnul prof. univ. dr. ing. Cornel PANAIT, rector, obține validarea calificării *Securitate cibernetică și managementul riscurilor*, aferentă programului de studii universitare de masterat *Securitate cibernetică și managementul riscurilor*.

Se eliberează prezenta adeverință pentru a folosi drept dovadă în vederea acreditării/autorizării provizorii a programului de studii aferent.

Cu deosebită considerație,

PREȘEDINTE
Tiberiu Gabriel DOBRESCU

ROMÂNIA AUTORITATEA NAȚIONALĂ PENTRU CALIFICĂRI MINISTERUL EDUCAȚIEI NAȚIONALE

Având în vedere prevederile Legii Educației Naționale nr. 1/2011
și
prevederile Chartei Universității Maritime din Constanța,

Senatul Universității Maritime din Constanța
emite

HOTĂRÂREA O.11 din 28 noiembrie 2018

Art.1. În unanimitate de voturi s-a aprobat înființarea unui nou program de studii universitare de master, cu durata de 2 ani, denumit: "*Securitate cibernetică și managementul riscurilor*", în domeniul de studii " *Inginerie Electronică Telecomunicații și Tehnologii Informaționale*", cu predare în limba română.

Art.2. Prezenta Hotărâre de difuzează la toate compartimentele universității prin https://owncloud.cmu-edu.eu/s/pTwNIJWLjDpE2Rv și https://cmu-edu.eu/senat-umc/hotarari-senat/.

Conf. univ. dr. ing. Emil OANȚĂ
Președinte al Senatului Universității Maritime din Constanța

UNIVERSITATEA MARITIMĂ DIN CONSTANȚA • SENATUL UNIVERSITAR •

Memoriu de analiza a programului de master *Securitate cibernetică şi managementul riscurilor*

Programul de master *profesional* propus "*Securitate cibernetică şi managementul riscurilor*" este rezultatul organizarii Departamentului Stiinte Generale Ingineresti care vizează adaptarea la cerinţele pieţei de forţă de muncă din domeniul *Inginerie electronică, telecomunicaţii şi tehnologii informaţionale*;

Reprezintă o necesitate cerută de piaţa muncii, în urma numeroaselor discuţii purtate de Universitatea Maritimă Constanţa cu mediul socio-economic, cu specialişti din industrie şi din cadrul structurilor ce asigură Securitate cibernetică a României, la diverse reuniuni, workshop-uri, sau la cele 2 ediţii ale conferinţelor internaţionale de securitate cibernetică la Marea Neagră organizate de universitate.

Motivatie

Atacurile împotriva atacurilor cibernetice cresc în frecvență și complexitate, iar cererea de ingineri de securitate calificați crește, precum și numărul de locuri de muncă deschise în domeniul securității informatice.

Pentru statul român, securitatea cibernetică este „starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic".

Securitatea cibernetică este un subiect discutat frecvent în ultimii ani, fiind un mediu dinamic. Tehnologiile folosite sunt înlocuite, actualizate și modificate constant, apărând astfel noi și noi provocări în contextul în care nivelul de conștientizare al utilizatorilor de Internet este încă unul foarte scăzut.

Interesul companiilor şi organizaţiilor în experţi din aria securitatii cibernetice este în continuă creştere, iar prin infiintarea unui program de studii *Securitate cibernetică şi managementul riscurilor* vor fi pregatiti specialist care vor putea gestiona adecvat riscurile din spatial cybernetic.

Se conştientizeaza de catre cele mai multe companii de faptul ca spatial cibernetic este utilizat de grupari de hackeri, sunt din ce in ce mai multe cazuri de spionaj cibernetic, a crescut criminalitatea cibernetica si creste astfel necesitatea gestionarii corecte a spatiului cibernetic.

Scopul programului "*Securitate cibernetică şi managementul riscurilor*" şi competenţe oferite

Scopul programului propus este de a pregăti specialişti în domeniu si care sa poată contribui la asigurarea unui nivel adecvat de securitate cibernetică, prevenirea şi combaterea criminalităţii informatice, îmbunătăţirea sistemului de management al securităţii informaţiilor.
Prin disciplinele obligatorii incluse în planul de învăţământ se asigură dobândirea de competenţe atât pe componenta analitică cât şi pe cea tehnologică.

Competenţe profesionale

1.Cunoştinţe specifice de telecomunicaţii şi tehnologia informaţiilor

- Folosirea creativă a conceptelor fundamentale din telecomunicaţii şi tehnologia informaţiilor, a metodelor de modelare şi simulare, pentru realizarea modelelor unor sisteme electronice de comunicaţii
- Aplicarea creativă a cunoştinţelor şi metodelor specifice domeniului telecomunicaţii şi tehnologiei informaţiei;

2.Comprehensiunea şi interpretarea actelor normative care reglementează domeniul de referință

- Utilizarea unor strategii diverse de analiză legislativă în vederea înţelegerii şi interpretării prevederilor legislative;
- Însușirea și interpretarea conceptelor și termenilor folosiți în domeniul securității cibernetice;
- Capacitatea de corelare şi realizare de conexiuni logice între două sau mai multe prevederi legislative din diferite state europene;
- Identificarea compatibilităților, a diferențelor și a elementelor contradictorii dintre prevederile legislației naționale și ale celei europene în vederea analizării şi identificării metodelor şi mecanismelor de cooperare transnațională;
- Cunoaşterea modului de organizare şi desfăşurare a proceselor de management al riscurilor de securitate asociate infrastructurilor cibernetice;

3.Elaborarea a noi inițiative în domeniul prevenirii și combaterii criminalității cibernetice

- Aplicarea metodologiilor și utilizarea în mod corespunzător a instrumentelor tehnice specializate de evaluare a securității sistemelor informatice
- Implementarea unor soluţii noi de securitate, eficiente, care să asigure un nivel adecvat de protecție în cazul unor atacuri cibernetice complexe

4.Răspunsul la incidentele de securitate cibernetică

- Cunoșterea și aplicarea prevederilor și procedurilor legale pentru investigarea incidentelor de securitate cibernetică

Competenţe transversale

- Abilitatea de a comunica în diferite medii manifestînd toleranţa; exprimarea şi înţelegerea diferitelor puncte de vedere; negocierea şi abilitatea de a crea încredere şi de a manifesta empatie; abilitatea de a face faţă stresului şi frustrării precum şi abilitatea de a le exprima în mod constructiv.
- Dezvoltarea competenţelor civice şi a deprinderilor civice prin implicarea alături de ceilalţi în domeniul public, solidaritate şi interes în rezolvarea problemelor care afectează comunitatea; reflectarea critică şi creativă şi participarea constructivă în activităţile comunităţii, precum şi în luarea deciziilor cu privire la securitatea organizaţională şi a sistemelor de infractructuri critice.
- Aplicarea, în mod responsabil, a principiilor, normelor şi valorilor eticii profesionale în realizarea sarcinilor profesionale şi identificarea obiectivelor de realizat, a resurselor disponibile, a etapelor de a duratelor de execuţie, a termenelor de realizare aferente şi a riscurilor aferente.
- Identificarea rolurilor şi responsabilităţilor într-o echipă pluridisciplinară şi aplicarea de tehnici de relaţionare şi muncă eficientă în cadrul echipei

- Autoevaluarea obiectivă a nevoii de formare profesională continuă în domeniul telecomunicaţiilor şi tehnologiei informaţionale, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia.

- Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale.
- Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

Grupuri ţintă

Programul de studii de master "*Securitate cibernetică şi managementul riscurilor*" are caracter *profesional* şi vizează în principal absolvenţi ai unui program de studii din domeniul ştiinţelor exacte şi a celor inginereşti cum ar fi domeniile Inginerie electronică, Telecomunicaţii, Calculatoare și Tehnologia Informației, Automatică si Informatică aplicata, dar pot fi, de asemenea, urmate de absolvenți de programe de studii conexe.

Planul de învăţământ este astfel conceput încât să permită, prin alegerea adecvată a disciplinelor opţionale, urmarea unei carieră profesională / de cercetare în proiectarea și implementarea soluțiilor de securitate cibernetică la nivel organizațional, local, național și regional;

Programul de master va asigura dezvoltarea de competențe in implementarea unor infrastructuri de securitate robuste cu metodologii software și hardware, protecția infrastructurilor critice și gestionarea rapidă și eficientă a incidentelor de Securitate;

Instruirea masteranzilor în securitatea cibernetică se va baza pe prezentarea conceptelor de securitate cibernetică, a metodelor de securitate a informațiilor și a evaluării vulnerabilităților organizaționale și dobândirea de abilități practice în determinarea amenințărilor, riscurilor și încălcărilor de securitate,

"*Securitate cibernetică şi managementul riscurilor*" este un program de masterat cu conținut care răspunde cerințelor societății moderne moderne de astăzi.

Oportunităţi de carieră

Absolvenţii programului de studii "*Securitate cibernetică şi managementul riscurilor*" vor putea
activa în companii pentru proiectarea și implementarea securității cibernetice;

Vor putea devein specialiști în domeniul științei și ingineriei, specialiști in tehnologia informației și comunicațiilor.

Deocamdată, în codul ocupaţiilor din România (COR 2018) cele mai apropiate calificări existente sunt:

215222 - Inginer sisteme de Securitate
215220 - Specialist mentenanţă electromecanică-automatică echipamente industriale
215227 - Inginer de cercetare în comunicaţii
251402 - Specialist în proceduri şi instrumente de securitate a sistemelor informatice

Ocupația Inginer de securitate cibernetică nu este încă definită în COR;

Evoluția societății umane este către o societate informațională în care internetul și tehnologiile aferente, conectivitatea și impunerea Industry 4.0, atrage după sine nevoia de specialiști în acest domeniu.

Analiza SWOT

Puncte tari:

1. La Facultatea Electromecanica Navala există expertiza necesară organizării programului "*Securitate cibernetică şi managementul riscurilor*" expertiză dobândită prin derularea unor programe de master acreditate in domeniul *Inginerie electronică, telecomunicaţii şi tehnologii informaţionale* cu care există intersecţie. Astfel amintim aici investiţiile făcute de Universitatea Maritimă din Constanţa în dotarea cu echipamente specifice în domeniul securităţii cybernetic dar si existent resursei umane înalt calificate existente, precum şi a acordurilor de colaborare cu firme specializate în acest domeniu de nişă;

2. Industria IT&C resimte problema creşterii insuficiente a numărului de absolvenţi şi trage semnale legate de cererea mare de specialişti de mulţi ani", spun reprezentanţii Bitdefender. Iar lipsa resimţită în industria IT se poate observa şi în datele statistice, spre exemplu, facultăţile din România aduc în piaţa muncii circa 8.000 de absolvenţi de IT pe an, potrivit datelor de la INS, însă necesarul din piaţă este cel puţin dublu, iar a numărului de specialişti în securitate cibernetică de asemenea.
3. În urma analizării statisticilor şi studiilor efectuate de către firme de prestigiu de pe piaţa internaţională cum ar fi Deloitte (https://www2.deloitte.com/insights/us/en/topics/leadership/global-cio-survey.html), KPMG, KPMG CIO Survey is the world's largest IT leadership survey (https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/06/harvey-nash-kpmg-cio-survey-2018.pdf), s-a putut identifica (în mai toate statele unde s-a realizat colectarea datelor) faptul că cererea de specialişti în securitate cibernetică este tot mai mare, însoţită de cererea de specialişti în analiza datelor, potrivit ediţiei din acest an a CIO Survey realizat de Deloitte la nivel global.
4. Prin structura şi obiectivele propuse, programul "*Securitate cibernetică şi managementul riscurilor*" acoperă o nişă în cadrul programelor de pregătire profesională şi răspunde cererii curente de specialişti în domeniu.

Puncte slabe:

1. Structura programului "*Securitate cibernetică şi managementul riscurilor*" a fost însă concepută astfel încât să asigure competenţele corespunzătoare profilurilor solicitate de mediul economic.

Oportunităţi:

1. Programul "*Securitate cibernetică şi managementul riscurilor*" adreseaza o direcţie de formare profesională considerată atractivă pe plan national si are oportunitatea de a atrage studenţi;
2. Programul "*Securitate cibernetică şi managementul riscurilor*" oferă oportunitatea încheierii unor noi parteneriate academice în beneficiul studenţilor;

Amenintari:

1. Unii specialist pot declara ca s-a atins deja maximul de popularitate şi s-a trecut în porţiunea uşor descendentă a popularităţii.

Scrisori de suport:

1. CAMERA DE COMERT, INDUSTRIE, NAVIGATIE SI AGRICULTURA Constanta
2. INOMAR Cluster
3. CONSTANTA PORT BUSINESS ASSOCIATION
4. GEMENI SOLUTION SRL
5. CERT SIGN SA Bucuresti
6. EASYDO DIGITAL TECHNOLOGIES SRL Bucuresti
7. ARECS- Asociatia Romana pentru Educatie si Cultura de Securitate Bucuresti

150 22.01.2019

CAMERA DE COMERŢ, INDUSTRIE, NAVIGAŢIE ŞI AGRICULTURĂ CONSTANŢA

Împreună pentru afacerea ta

Către,

UNIVERSITATEA MARITIMĂ DIN CONSTANŢA
În atenţia dlui Rector prof.univ.dr.ing. Cornel PANAIT

Având în vedere adresa prin care Universitatea Maritimă din Constanţa solicită opinia Camerei de Comerţ, Industrie, Navigaţie şi Agricultură (CCINA) Constanţa, cu sediul în Constanţa, Bd. Alexandru Lăpuşneanu 185A, telefon: +40 241 619.854 , fax: +40 241 619.454, e-mail: office@ccina.ro, cu privire la înfiinţarea programului de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR", vă transmitem că punctele dumneavoastră de vedere au fost luate în calcul de către unele companii membre ale CCINA Constanţa şi vă susţinem în demersurile ce trebuie să le îndepliniţi pentru acreditarea acestui program de studii de masterat.

Membrii comunităţii de afaceri a judeţului Constanţa au conştientizat, în ultimii ani, importanţa şi necesitatea de a avea specialişti care să fie pregătiţi în a face faţă atacurilor cibernetice şi, totodată, de a avea competenţe în înţelegerea şi combaterea fenomenului criminalităţii informatice.

Numeroşi directori ai companiilor sunt îngrijoraţi de utilizarea, pe scară tot mai largă, a spaţiului cibernetic, de către grupări de hackeri, de înmulţirea cazurilor de spionaj cibernetic, dar şi de amploarea criminalităţii informatice ori imperativul protecţiei infrastructurilor critice.

Camera de Comerţ, Industrie, Navigaţie şi Agricultură Constanţa sprijină demersurile Universităţii Maritime din Constanţa, în înfiinţarea unei specializări de masterat prin care vor fi pregătiţi viitori specialişti, care să gestioneze adecvat riscurile din spaţiul cibernetic.

În concluzie, ne manifestăm convingerea privind utilitatea demersului de înfiinţare a acestui nou program de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR", în cadrul facultăţii Electromecanică Navală din Universitatea Maritimă din Constanţa şi pregătirea specialiştilor în domeniul de studii de masterat "INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE".

Cu stimă,
conf.univ.dr.ec. Ion Dănuţ Jugănaru
Director General
al
Camerei de Comerţ, Industrie, Navigaţie şi Agricultură Constanţa

INOMARCluster

Asociatia INOMAR Cluster
CIF 36324334
Str. Siretului nr. 63, Constanta

Către,

UNIVERSITATEA MARITIMĂ DIN CONSTANȚA
În atenția dlui Rector prof.univ.dr.ing. Cornel PANAIT

Având în vedere adresa prin care Universitatea Maritimă din Constanța solicită opinia INOMAR Cluster, Str. Siretului nr. 63A, 900675 Constanța, tel. +40 241 616 808, +40723790763, office@inomar.ro, cu privire la înființarea programului de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", vă transmitem că punctele dumneavoastră de vedere au fost luate în calcul de către membrii clusterului nostru și vă susținem în demersurile ce trebuie să le îndepliniți pentru acreditarea acestui program de studii de masterat.

Membrii companiilor din spațiul de business din Constanța constituiți în Clusterul INOMAR, au conștientizat în ultimii ani importanța și necesitatea de a avea specialiști care să fie pregătiți în a face față atacurilor cibernetice.

Clusterul INOMAR, sprijină demersurile Universității Maritime din Constanța, în înființarea unei specializări de masterat prin care vor fi pregătiți viitori specialiști care să gestioneze adecvat riscurile din spațiul cibernetic.

În concluzie suntem de acord cu înființarea acestui nou program de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", în cadrul facultății Electromecanică Navală din Universitatea Maritimă din Constanța și pregătirea specialiștilor în domeniul de studii de masterat "INGINERIE ELECTRONICĂ, TELECOMUNICAȚII ȘI TEHNOLOGII INFORMAȚIONALE".

Președinte
Stanica Enache

INOMAR CLUSTER
CIF36324334
Constanta
Romania

Str. Siretului nr. 63 - 900675 Constanta - Romania
Tel.: +40 241 616808 Cell.: +40 723 790763 | Skype: inomar_office | e-mail: office@inomar.ro
www.inomar.ro

Constanta
Port Business
Association

Constanta Port Business Association
Bd. Mamaia, nr. 182, parter, 900540, Constanța
Tel./Fax: 0241 484 836, E-mail: office@portbusiness.ro
www.portbusiness.ro

Nr. 22/21.01.2019

Către,

UNIVERSITATEA MARITIMĂ DIN CONSTANȚA
În atenția dlui Rector prof.univ.dr.ing. Cornel PANAIT

Având în vedere adresa prin care Universitatea Maritimă din Constanța solicită opinia organizației patronale „CONSTANTA PORT BUSINESS ASSOCIATION", organizație reprezentativa in sectorul de activitate „Transporturi maritime și servicii conexe. Transporturi aeriene și servicii conexe", având sediul în Constanta, Bd. Mamaia nr. 182, parter, Tel/Fax: 0241 484836, Email: office@portbusiness.ro, cu privire la înființarea programului de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", vă transmitem că punctele dumneavoastră de vedere au fost luate în calcul de către membrii asociației noastre și vă susținem în demersurile ce trebuie să le îndepliniți pentru acreditarea acestui program de studii de masterat.

Membrii companiilor din portul Constanța constituiți în Organizația Patronală CONSTANTA PORT BUSINESS ASSOCIATION, au conștientizat în ultimii ani importanța și necesitatea de a avea specialiști care să fie pregătiți în a face față atacurilor cibernetice.

Directorii de companii sunt îngrijorați de utilizarea pe scară tot mai largă a spațiului cibernetic de către grupări de hackeri, de înmulțirea cazurilor de spionaj cibernetic, dar și de amploarea criminalității informatice ori imperativul protecției infrastructurilor critice.

Organizația Patronală „CONSTANTA PORT BUSINESS ASSOCIATION", sprijină demersurile Universității Maritime din Constanța, în înființarea unei specializări de masterat prin care vor fi pregătiți viitori specialiști care să gestioneze adecvat riscurile din spațiul cibernetic.

În concluzie suntem de acord cu înființarea acestui nou program de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", în cadrul facultății Electromecanică Navală din Universitatea Maritimă din Constanța și pregătirea specialiștilor în domeniul de studii de masterat "INGINERIE ELECTRONICĂ, TELECOMUNICAȚII ȘI TEHNOLOGII INFORMAȚIONALE".

Cu stimă,
Viorel PANAIT
Președinte

CONSTANTA PORT BUSINESS ASSOCIATION ORGANIZAȚIE PATRONALĂ

GEMINI SOLUTIONS SRL
Bucureşti, Calea Dorobanti nr. 239, sector 1
J40/13485/2005
C.I.F. 17837325

GEMINI

Către,

UNIVERSITATEA MARITIMĂ DIN CONSTANȚA
În atenția dlui Rector prof.univ.dr.ing. Cornel PANAIT

Având în vedere adresa prin care Universitatea Maritimă din Constanța solicită opinia GEMINI SOLUTIONS S.R.L., cu sediul social în București, Calea Dorobanți 239, Et. 1, Sector 1, Cod Postal 010567, înregistrată la Registrul Comerțului cu nr. J40/13485/2005, Cod Unic de Identificare RO17837325, cu privire la înființarea programului de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", vă transmitem că punctele dumneavoastră de vedere au fost luate în calcul de către compania noastră și vă susținem în demersurile ce trebuie să le îndepliniți pentru acreditarea acestui program de studii de masterat.

Compania pe care o reprezint a conștientizat în ultimii ani importanța și necesitatea de a avea specialiști care să fie pregătiți în a face față atacurilor cibernetice, având în vedere prezența businessului nostru online care aduce totodată și posibilitatea de a fi atacat de infractorii cibernetici.

Managementul companiei noastre este îngrijorat de utilizarea pe scară tot mai largă a spațiului cibernetic de către grupări de hackeri, de înmulțirea cazurilor de spionaj cibernetic, dar și de amploarea criminalității informatice ori imperativul protecției infrastructurilor critice.

Salutăm și sprijinim inițiativa Universității Maritime din Constanța, care prin dotarea sa de excepție în domeniul securității cibernetice și a partenerilor cu care colaborează în acest domeniu, va pregăti viitori specialiști care să gestioneze adecvat riscurile din spațiul cibernetic, după absolvirea noul program de studii de masterat.

În concluzie suntem de acord cu înființarea acestui nou program de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", în cadrul facultății Electromecanică Navală din Universitatea Maritimă din Constanța și pregătirea specialiștilor în domeniul de studii de masterat "INGINERIE ELECTRONICĂ, TELECOMUNICAȚII ȘI TEHNOLOGII INFORMAȚIONALE".

Cu stimă,

SOCIETATEA COMERCIALĂ GEMINI SOLUTIONS S.R.L. BUCUREȘTI - ROMÂNIA

certSIGN

Bulevardul Tudor Vladimirescu nr. 29 A, AFI Tech Park 1, București
www.certSIGN.ro

Către,

CS 304
25 01 2018

UNIVERSITATEA MARITIMĂ DIN CONSTANȚA
În atenția dlui Rector prof.univ.dr.ing. Cornel PANAIT

Având în vedere adresa prin care Universitatea Maritimă din Constanța solicită opinia CERTSIGN S.A., cu sediul social în București, sector 4, Soseaua Oltenitei, nr. 107A, înregistrată la Registrul Comerțului cu nr. J40/484/2006, Cod Unic de Identificare, tel. 004-021-31.19.901, fax 004-021-31.19.905, e-mail office@certsign.ro, cu privire la înființarea programului de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", vă transmitem că punctele dumneavoastră de vedere au fost luate în calcul de către compania noastră și vă susținem în demersurile ce trebuie să le îndepliniți pentru acreditarea acestui program de studii de masterat.

Compania pe care o reprezint a conștientizat în ultimii ani importanța și necesitatea de a avea specialiști care să fie pregătiți în a face față atacurilor cibernetice.

Managementul companiei noastre este îngrijorat de utilizarea pe scară tot mai largă a spațiului cibernetic de către grupări de hackeri, de înmulțirea cazurilor de spionaj cibernetic, dar și de amploarea criminalității informatice ori imperativul protecției infrastructurilor critice.

Salutăm și sprijinim demersurile Universității Maritime din Constanța, în înființarea unei specializări de masterat prin care vor fi pregătiți viitori specialiști care să gestioneze adecvat riscurile din spațiul cibernetic.

În concluzie suntem de acord cu înființarea acestui nou program de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", în cadrul facultății Electromecanică Navală din Universitatea Maritimă din Constanța și pregătirea specialiștilor în domeniul de studii de masterat "INGINERIE ELECTRONICĂ, TELECOMUNICAȚII ȘI TEHNOLOGII INFORMAȚIONALE".

Cu stimă,

Director General CERTSIGN SA

Adrian FLOAREA

certSIGN
Cod fiscal **RO18288250**, Registrul Comerțului **J40/484/2006**, Capital social: **1,971,000**
Sediul social: Soseaua Olteniței Nr. 107 A , Corp C1, Parter, Sector 4, 041303, București, Telefon: +40 31 101 18 70; Fax: +40 21 311 99 05; E-mail: office@certsign.ro
ISO 9001-26325/06/R, ISO 14001-EMS 3928/R, OHSAS 18001 C-IS-957, ISO 27001-111/10: RINA SIMTEX-RENAR, ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806, ISO 27001-IT-850322: IQNET ISO 20000-1-ITSMS-31/13. ACCREDIA
Operator de date cu caracter personal înregistrat sub Nr. 3160

easydo Digital Innovator

Referinta
Nr.01_Doc_31/01/2019

UNIVERSITATEA MARITIMĂ DIN CONSTANȚA

În atenția dlui Rector prof.univ.dr.ing. Cornel PANAIT

Bucuresti la data de 31.01.2019

Având în vedere adresa prin care Universitatea Maritimă din Constanța solicită opinia EASYDO DIGITAL TECHNOLOGIES S.R.L., cu sediul social în Bucuresti, str. Coltei, nr. 38, Corp B2, Et. 1, Ap. 4, sector 3, înregistrată la Registrul Comertului sub nr. J40/12250/2018 cod fiscal nr. RO 39799672 , cu privire la înființarea programului de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", vă transmitem că punctele dumneavoastră de vedere au fost luate în calcul de către compania noastră și vă susținem în demersurile ce trebuie să le îndepliniți pentru acreditarea acestui program de studii de masterat.

Compania pe care o reprezint a conștientizat în ultimii ani importanța și necesitatea de a avea specialiști care să fie pregătiți în a face față atacurilor cibernetice, având în vedere prezența businessului nostru online care aduce totodată și posibilitatea de a fi atacat de infractorii cibernetici.

Managementul companiei noastre este îngrijorat de utilizarea pe scară tot mai largă a spațiului cibernetic de către grupări de hackeri, de înmulțirea cazurilor de spionaj cibernetic, dar și de amploarea criminalității informatice ori imperativul protecției infrastructurilor critice.

Salutăm și sprijinim inițiativa Universității Maritime din Constanța, care prin dotarea sa de excepție în domeniul securității cibernetice și a partenerilor cu care colaborează în acest domeniu, va pregăti viitori specialiști care să gestioneze adecvat riscurile din spațiul cibernetic, după absolvirea noul program de studii de masterat,.

În concluzie suntem de acord cu înființarea acestui nou program de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", în cadrul facultății Electromecanică Navală din Universitatea Maritimă din Constanța și pregătirea specialiștilor în domeniul de studii de masterat "INGINERIE ELECTRONICĂ, TELECOMUNICAȚII ȘI TEHNOLOGII INFORMAȚIONALE".

Cu stimă,

David Coyne

Administrator EASYDO Digital Technologies S.R.L.

SOCIETATEA 1 EASYDO DIGITAL TECHNOLOGIES SRL BUCUREȘTI - ROMÂNIA

ASOCIATIA ROMANA EDUCATIE CULTURA SECURITATE
ARECS

Către,

UNIVERSITATEA MARITIMĂ DIN CONSTANȚA
În atenţia dlui Rector prof.univ.dr.ing. Cornel PANAIT

Având în vedere adresa prin care Universitatea Maritimă din Constanța solicită opinia Asociației Române pentru Educație și Cultură de Securitate - ARECS, cu sediul în București, Cal. Floreasca, nr. 134, bl. 31, sc. C, et. 2, ap. 28, Sector 1, cod poștal 014456, tel. 0371121121, fax 0374090990, cod fiscal / C.I.F. 38675080, e-mail office@arecs.ro, www.arecs.ro, cu privire la înființarea programului de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", vă transmitem că punctele dumneavoastră de vedere au fost analizate în forurile asociației și vă susținem în demersurile ce trebuie să le îndepliniți pentru acreditarea acestui program de studii de masterat.

Salutăm şi susţinem iniţiativa Universităţii Maritime din Constanţa care, prin dotarea sa de excepţie în domeniul securităţii cibernetice şi prin calitatea partenerilor cu care colaborează în acest domeniu, poate pregăti viitori specialişti care să gestioneze adecvat riscurile din spațiul cibernetic, după absolvirea noului program de studii de masterat.

Membrii asociației noastre, susținători ai formelor de educație adecvate conștientizării și consolidării conceptului de cultură de securitate, în care este inclusă și securitatea cibernetică, sunt coștienți că evoluțiile tehnologice în spațiul cibernetic, pe lângă beneficii evidente, aduc și o largă paletă de riscuri de securitate, pentru a căror combatere este nevoie de tot mai mulți profesioniști cu o bună pregătire de specialitate.

Un program de studii de masterat cu tema aleasă de Universitatea Maritimă din Constanța este o foarte bună reprezentare a reacției mediului academic la cerințele cadrului european comun de răspuns la incidente de securitate cibernetică si de asigurare a securității rețelelor și sistemelor informatice ce deservesc activități vitale pentru economie și societate, în condițiile în care, la finele anului trecut, în România a fost adoptată legea care transpune Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016, ce are drept scop creșterea încrederii cetățenilor și stimularea dezvoltării Pieței Digitale Unice.

În concluzie, suntem de acord și susținem cu tărie înființarea acestui nou program de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ȘI MANAGEMENTUL RISCURILOR", în cadrul facultății Electromecanică Navală din Universitatea Maritimă din Constanța și pregătirea specialiștilor în domeniul de studii de masterat "INGINERIE ELECTRONICĂ, TELECOMUNICAȚII ȘI TEHNOLOGII INFORMAȚIONALE".

Cu deosebită stimă,

Dr.ing. Vasile Drăghici
Președinte A.R.E.C.S

ASOCIATIA ROMANA EDUCATIE CULTURA SECURITATE ARECS

București, str. Drum Pădurea Neagră, nr. 19-85, bl. 21A, ap. 11, Sector 1, 014044
www.arecs.ro 0742039206 office@arecs.ro

MINISTERUL EDUCAŢIEI NAŢIONALE
UNIVERSITATEA MARITIMĂ DIN CONSTANŢA
900663, CONSTANŢA, str. Mircea cel Bătrân, nr. 104, ROMÂNIA
Fax: +40-241-617260, Tel: +40-241-664740,
E-mail: info@imc.ro, Web: www.cmu-edu.eu

Analiza privind oportunitatea înființării programului de studii universitare de master

"Securitate cibernetică şi managementul riscurilor"

la

Universitatea Maritimă din Constanţa

Calificarea „*Securitate Cibernetică şi Managementul Riscurilor*" – studii de master, reprezintă o necesitate cerută de piaţa muncii, în urma numeroaselor discuţii purtate de Universitatea Maritimă Constanţa cu mediul socio-economic, cu specialişti din industrie şi din cadrul structurilor ce asigură Securitate cibernetică a României, la diverse reuniuni, workshop-uri, sau la cele 2 ediţii ale conferinţelor internaţionale de securitate cibernetică la Marea Neagră organizate de universitate.

Mediul virtual, generat de infrastructurile cibernetice, incluzând conținutul informațional procesat, stocat sau transmis, și acțiunile derulate de utilizatori, este deja o parte integrantă a vieții personale și profesionale, însă securitatea este un element luat în calcul mult prea rar. Noile tehnologii implică însă noi riscuri care pot afecta grav individul sau organizația, în condițiile în care există numeroase acțiuni ostile desfășurate în spațiul cibernetic de natură să afecteze disponibilitatea, integritatea și confidențialitatea funcționării sistemelor informatice.

Spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând deopotrivă atât oportunităţi de dezvoltare a societăţii informaţionale bazate pe cunoaştere, cât şi riscuri la adresa funcţionării acesteia (la nivel individual, statal şi chiar cu manifestare transfrontalieră).

Securitatea cibernetică este o prioritate pentru buna funcționare a sistemelor guvernamentale sau de control industrial (producția și distribuția de energie electrică, distribuția de apă) etc.

Pentru statul român, securitatea cibernetică este „starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic".

Securitatea cibernetică este un subiect discutat frecvent în ultimii ani, fiind un mediu dinamic. Tehnologiile folosite sunt înlocuite, actualizate și modificate constant, apărând astfel noi și noi provocări în contextul în care nivelul de conștientizare al utilizatorilor de Internet este încă unul foarte scăzut.

Mediul online are din ce în ce mai multe conexiuni cu spațiul fizic, iar multe dintre lucrurile pe care le facem în spațiul virtual au implicații în plan real. Astfel, când securitatea este compromisă în lumea virtuală, utilizatorii pot avea parte de consecințe dintre cele mai neplăcute în lumea reală.

Confruntată cu provocări de securitate cibernetică tot mai mari, UE trebuie să îmbunătățească gradul de conștientizare și capacitatea de reacție la atacurile cibernetice care vizează statele membre sau instituțiile UE (sursa www.consilium.europa.eu/ro/policies/cyber-security/).

„Internetul obiectelor" este deja o realitate, preconizându-se că, până în 2020, numărul dispozitivelor digitale conectate va fi de ordinul a zeci de miliarde.

În același timp, sistemele TIC actuale pot fi grav afectate de incidente de securitate precum defecțiunile de ordin tehnic și virușii. Aceste tipuri de incidente, denumite adesea incidente legate de rețele și de sisteme informatice (NIS), devin din ce în ce mai frecvente și mai dificil de abordat.

În plus, se estimează că atacurile cibernetice păgubesc anual economia globală cu 400 de miliarde EUR.

Multe întreprinderi și administrații publice din întreaga UE se bazează pe rețele și infrastructuri digitale pentru furnizarea serviciilor lor esențiale. Aceasta înseamnă că, atunci când apar, incidentele NIS pot avea un impact enorm prin compromiterea serviciilor și întreruperea funcționării corespunzătoare a întreprinderilor.

Prin urmare, un incident NIS dintr-o țară poate avea efecte în alte țări și chiar în întreaga UE.

Anul trecut, 7 din 10 calculatoare au fost atacate cibernetic. Asta înseamnă că aproximativ 3 milioane de computere au fost țintite de hackeri. Experţii au avut de gestionat peste 130 de milioane de alerte. Cu 25% mai multe, comparativ cu 2016 (sursa https://www.digi24.ro/stiri/actualitate/evenimente/greseala-grava-facuta-de-aproape-toti-expertii-in-securitate-cibernetica-la-un-test-al-sri-1011642).

În ceea ce priveşte existenţa infrastructurilor critice în Dobrogea, constatăm că economia municipiului Constanţa şi a întregii zone metropolitane are un caracter complex, principalele ramuri cu ponderi fiind: activitatea portuară şi transportul maritim, industria energiei electrice şi termice, industria construcţiilor de maşini, industria chimică şi petrochimică, industria de prelucrare a lemnului şi a producerii hârtiei, industria confecţiilor, etc.

Coordonarea activităţilor de producţie, distribuţie şi consum în zona metropolitană constănţeană implică aspecte legate de tipologia IoT, a unui mediu informaţional dinamic, bazat pe interoperabilitate şi servicii specifice societăţii informaţionale.

În Dobrogea există o serie de unităţi şi platforme economice, care prezintă un caracter critic din punct de vedere al securităţii cibernetice, putând deveni ţinta atacurilor informatice. Printre acestea se numără: Centrala Nuclearelectrică de la Cernavodă, rafinăria Petromidia Năvodari, porturile maritime Constanţa, Midia şi Mangalia.

Organizaţia Maritimă Internaţională (IMO) a transmis o serie de circulare prin care solicită instituţiilor de învăţământ superior şi actorilor de pe piaţa maritimă să acorde atenţie noilor riscuri apărute odată cu dezvoltarea industriei navale şi modernizarea echipamentelor de la bordul navelor. Nu numai navele au devenit ţinta atacurilor cibernetice, ci şi întregul lanţ logistic ce face posibil transportul maritim.

Pornind de la faptul ca la nivel european şi mondial, a căpătat o mare amploare studiul ameninţărilor cibernetice ce pot afecta siguranţa navigaţiei pe mare, diverşi cercetători şi specialişti din Europa au demonstrat vulnerabilitatea hărţilor electronice şi a sistemului GPS, uşurinţa cu care pot fi modificate pentru a induce în eroare ofiţerii de navigaţie.

Marea majoritate a problemelor apărute în ultimii ani, în sectorul maritim, s-a datorat nu atât factorului tehnic, cât mai ales celui uman, a personalului care opera echipamentele care nu aveau o pregătire complementară corespunzătoare în domeniul securităţii cibernetice, iar managerii nu au acordat suficientă atenţie acestui fenomen, fiind slab informaţi. Se marchează o importantă schimbare de paradigmă în privinţa apărării cibernetice colective, conferind spaţiului cibernetic acelaşi nivel de relevanţă cu mediile convenţionale de desfăşurare a acţiunilor militare.

Pornind de la aceste cerinţe, Universitatea Maritimă din Constanţa a construit un Simulator de securitate cibernetică în domeniul maritim, proiectat şi dotat cu resurse financiare şi umane proprii. Simulatorul dispune de mai multe servere înglobând peste 300 TerraBytes şi peste 200 de celule de procesare, 20 de laptopuri de instruire, un centru de coordonare al scenariilor, precum şi un video-wall format din 16 unităţi TV de 4K. În cadrul centrului se pot genera scenarii complexe privind ameninţările cibernetice ce pot afecta siguranţa navigaţiei pe mare, instalaţiile şi echipamentele de la bordul navelor, infrastructura portuară, şi nu numai.

Pentru a respecta directivele IMO, la masteratele internaţionale ale Universităţii Maritime se derulează deja cursuri de Securitate cibernetică în domeniul maritim.

Universitatea Maritimă din Constanţa a organizat deja 2 ediţii internaţionale pe Securitate cibernetică la Marea Neagră, iar în 2019 va organiza cea de a treia ediţie sub înaltul patronaj al Ministerului Afacerilor Externe şi al Preşedinţiei României la Consiliul UE.

În urma protocolului de colaborare pe Securitate cibernetică încheiat între Ministerul Comunicaţiilor şi Societăţii Informaţionale, în cadrul Universităţii Maritime Constanţa s-a înfiinţat "Centrul de excelenţă în securitate cibernetică în domeniul maritim".

Afiliaţi acestui centru sunt experţi de la diferite firme de IT din Constanţa şi din ţară, precum și Centru de Răspuns la Incidente de Securitate Cibernetice (CERT.RO). În cadrul centrului se derulează activităţi de cercetare direcţionate în vederea identificării posibilelor pericole cibernetice, precum și găsirea de soluții de creștere a securității.

Industria IT&C resimte problema creşterii insuficiente a numărului de absolvenţi şi trage semnale legate de cererea mare de specialişti de mulţi ani", spun reprezentanţii Bitdefender.

Iar lipsa resimţită în industria IT se poate observa şi în datele statistice, spre exemplu, facultăţile din România aduc în piaţa muncii circa 8.000 de absolvenţi de IT pe an, potrivit datelor de la INS, însă necesarul din piaţă este cel puţin dublu, iar a numărului de specialişti în securitate cibernetică de asemenea.

În urma analizării statisticilor şi studiilor efectuate de către firme de prestigiu de pe piaţa internaţională cum ar fi Deloitte (https://www2.deloitte.com/insights/us/en/topics/leadership/global-cio-survey.html), KPMG, KPMG CIO Survey is the world's largest IT leadership survey (https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/06/harvey-nash-kpmg-cio-survey-2018.pdf), s-a putut identifica (în mai toate statele unde s-a realizat colectarea datelor) faptul că cererea de specialişti în securitate cibernetică este tot mai mare, însoţită de cererea de specialişti în analiza datelor, potrivit ediţiei din acest an a CIO Survey realizat de Deloitte la nivel global.

Astfel, Calificarea „Securitate Cibernetică şi Managementul Riscurilor" – studii de master, reprezintă o necesitate cerută de piaţa muncii, iar acreditarea Programului de studii de master "*Securitate cibernetică şi managementul riscurilor*" în domeniul *Inginerie electronică, telecomunicaţii şi tehnologii informaţionale* se constituie într-un demers de rezolvarea a unei nevoi a mediului economic în ceea ce priveşte calificarea resursei umane.

Precizăm faptul că în cadrul domeniului *Inginerie electronică, telecomunicaţii şi tehnologii informaţionale,* la Universitatea Maritimă Constanţa se desfăşoară în prezent un singur program de studii

de master acreditat, cursuri de zi în limba română, şi anume: *"Circuite şi sisteme integrate de comunicaţii"*.

Cursurile *Programului de studii de master "Securitate cibernetică şi managementul riscurilor"* vin în completarea ofertei educaţionale locale şi nationale privind pregătirea masteranzilor în domeniul conştientizării fenomenului securităţii cibernetice, a criminalităţii informatice, precum şi al securizării echipamentelor digitizate din cadrul infrastructurilor critice din industrie, din cadrul companiilor şi nu în ultimul rând al echipamentelor de la bordul navelor, tocmai pentru a preîntâmpina atacurile cibernetice şi de a găsi soluţii şi masuri de diminuare a fenomenului.

Prin prisma investiţiilor făcute de Universitatea Maritimă din Constanţa în dotarea cu echipamente specifice în domeniul securităţii cibernetice, a resursei umane înalt calificate existente, precum şi a acordurilor de colaborare cu firme specializate în acest domeniu de nişă (a se vedea Anexa 5 – Acorduri de colaborare), universitatea îşi propune ca prin Programul de studii de master *"Securitate cibernetică şi managementul riscurilor"* să asigure competenţe specifice în domeniul securităţii cibernetice, a combaterii infracţiunilor informatice, pentru personalul executive din sectorul IT, pentru manageri de companii, pentru lucrătorii din administraţiile locale şi centrale, a lucrătorilor din sectoarele aferente infrastructurilor critice.

Calificarea „Securitate Cibernetică şi Managementul Riscurilor" obţinută în urma absolvirii Programului de studii de master *"Securitate cibernetică şi managementul riscurilor"* cu durata de doi ani, având forma de învăţământ cursuri cu frecvenţă în limba română, va rezolva o nevoie a mediului economic dobrogean, de specialişti care să aibă cunoştinţe specializate în domeniul securităţii cibernetice, precum şi de manageri care să fie avizaţi în acest domeniu de nişă.

Înfiinţarea acestui nou program de studii de masterat, cu durata de 2 ani, denumit "SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR", în cadrul facultăţii Electromecanică Navală din Universitatea Maritimă din Constanţa şi pregătirea specialiştilor în domeniul de studii de masterat "INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE", întruneşte aprobarea Senatului universităţii (a se vedea anexa 9).

04.02.2019

Conf.univ.dr.ing. Gabriel RAICU

Prorector cu activitatea de Cercetare şi Inovare Ştiinţifică

UNIVERSITATEA MARITIMĂ CONSTANŢA

România
MINISTERUL EDUCAŢIEI NAŢIONALE
Ministry of National Education
UNIVERSITATEA MARITIMA DIN CONSTANŢA [1)]
CONSTANTA MARITIME UNIVERSITY

SUPLIMENT LA DIPLOMĂ
DIPLOMA SUPPLEMENT

[2)] Acest supliment însoţeşte diploma
cu seria _____ nr. _____
The Supplement is for diploma
series _____ *no.* _____

1. DATE DE IDENTIFICARE A TITULARULUI DIPLOMEI
INFORMATION IDENTIFYING THE HOLDER OF THE DIPLOMA

Numele de familie din certificatul de naştere
Family name(s) of the birth certificate
1.1a

Numele de familie după căsătorie (dacă este cazul)
Family name(s) (after marriage) (if applicable)
1.1b

Iniţiala (iniţialele) prenumelui (prenumelor) tatălui/mamei
Initial(s) of father's/ mother's first name(s)
1.2a XXXXXX

Prenumele
First name(s)
1.2b YYYYYYY

Data naşterii (anul/luna/ziua)
Date of birth (year/month/day)
1.3a AA LL ZZ

Locul naşterii (localitatea, judeţul, ţara)
Place of birth
1.3b ZZZZZ

Numărul matricol
Student enrolment number
1.4 NNNN

Codul numeric personal (CNP)
Personal identification number
saallzznnnnnn

Anul înmatriculării
Year of enrolment
1.5 AAAA

2. INFORMAŢII PRIVIND CALIFICAREA
INFORMATION IDENTIFYING THE QUALIFICATION

Denumirea calificării şi titlul acordat
Name of qualification and title awarded
2.1 **SECURITATE CIBERNETICĂ SI MANAGEMENTUL RISCURILOR / MASTER**
CYBER SECURITY AND RISKS MANAGEMENT / Master of Science

Domeniul de studii
Field of study
2.2a **Inginerie electronică, telecomunicaţii şi tehnologii informationale**
Electronics engineering. telecommunications and informational technologies

Programul de studii
Programme of study
2.2b **Securitate cibernetică şi managementul riscurilor**
Cyber Security and Risks Management

Numele şi statutul instituţiei de învăţământ superior care eliberează diploma (în limba română)
Name and status of awarding institution
2.3a **Universitatea Maritima din Constanţa**
CONSTANTA MARITIME UNIVERSITY

Facultatea care organizează examenul de finalizare a studiilor (în limba română)
Faculty administering the final examination
2.3b **Facultatea de Electromecanică Navală**
Faculty of Marine Engineering

Numele şi statutul instituţiei de învăţământ superior care a asigurat şcolarizarea (dacă diferă de 2.3a, în limba română)
Name and status of institution administering studies (if different from 2.3a)
2.4a -

Facultatea care a asigurat şcolarizarea (dacă diferă de 2.3b, în limba română)
Faculty administering studies (if different from 2.3b)
2.4b -

Limba (limbile) de studiu / examinare
Language(s) of instruction / examination
2.5 **Română**, *ROMANIAN*

3. INFORMAŢII PRIVIND NIVELUL CALIFICĂRII
INFORMATION ON THE LEVEL OF THE QUALIFICATION

Nivelul calificării
Level of qualification
3.1 **Ciclul II - Studii universitare de masterat , 7 EQF, 7CEC**
2nd Cycle- Master Studies, 7EQF, 7 CEC

Durata oficială a programului de studii şi numărul de credite de studii transferabile (conform ECTS/SECT)
Official length of the programme of study and number of ECTS/SECT credits
3.2 **4 Semestre, 120 credite**
4 Semesters, 120 credits

L.S.

Condiţiile de admitere
Access requirement(s)

3.3 **STUDII DE LICENŢĂ/LUNGĂ DURATĂ+EXAMEN DE ADMITERE**
BACHELOR OF SCIENCE DEGREE + ADMISSION EXAM

4. INFORMAŢII PRIVIND CURRICULUMUL ŞI REZULTATELE OBŢINUTE
INFORMATION ON THE CURRICULUM AND RESULTS GAINED

Forma de învăţământ
Mode of study

4.1 **CU FRECVENŢĂ**
FULL TIME

Competenţele asigurate prin programul de studii
Learning outcomes of the study programme

4.2 **Competenţe profesionale:**
Folosirea creativă a conceptelor fundamentale din telecomunicaţii şi tehnologia informaţiilor, a metodelor de modelare şi simulare, pentru realizarea modelelor unor sisteme electronice de comunicaţii;
Aplicarea creativă a cunoştinţelor şi metodelor specifice domeniului telecomunicaţii şi tehnologiei informaţiei;
Însușirea și interpretarea conceptelor și termenilor folosiți în domeniul securității cibernetice;
Capacitatea de corelare și realizare de conexiuni logice între două sau mai multe prevederi legislative din diferite state europene;
Identificarea compatibilităților, a diferențelor și a elementelor contradictorii dintre prevederile legislației naționale și ale celei europene în vederea analizării și identificării metodelor și mecanismelor de cooperare transnațională;
Cunoașterea modului de organizare și desfășurare a proceselor de management al riscurilor de securitate asociate infrastructurilor cibernetice;
Aplicarea metodologiilor și utilizarea în mod corespunzător a instrumentelor tehnice specializate de evaluare a securității sistemelor informatice;
Implementarea unor soluţii noi de securitate, eficiente, care să asigure un nivel adecvat de protecție în cazul unor atacuri cibernetice complexe;
Cunoșterea și aplicarea prevederilor și procedurilor legale pentru investigarea incidentelor de securitate cibernetică;
Utilizarea în mod corect a instrumentele de colectare a probelor digitale si cunoasterea mecanismelor și a tehnicilor de investigare a acestora;

Professional competences:
Creative use of fundamental concepts in telecommunications and information technology, modeling and simulation methods, for the realization of electronic communications systems models;
Creative application of knowledge and methods specific to the field of telecommunication and information technology;
Acquiring and interpreting the concepts and terms used in the field of cyber security;
Ability to link and make logical connections between two or more legislative provisions across European countries;
Identify the compatibility, differences and contradictory elements between national and European legislation to analyze and identify transnational cooperation methods and mechanisms;
Know how to organize and deploy the security risk management processes associated with cyber infrastructures;
Application of methodologies and appropriate use of specialized technical tools to assess the security of IT systems;
Implementing new, cost-effective security solutions to ensure an adequate level of protection against complex cyber attacks;
Knowledge and enforcement of legal provisions and procedures for investigating cyber security incidents;
Proper use of digital evidence collection tools and knowledge of mechanisms and techniques for investigating them;

Detaliile programului absolvit, calificativele / notele / creditele ECTS/SECT obţinute (conform Registrului matricol al facultăţii volumul nr. 1 MASTER - IM - 2019-2021 / 1)
Programme details and the individual grades / marks / number of ECTS/SECT obtained (according to Faculty Student Records, volume no. 1 MASTER - ME - 2019-2021 / 1)

L.S.

Sistemul de notare şi, dacă sunt disponibile, informaţii privind distribuţia statistică a notelor

Grading scheme and, if available, grade distribution guidance

4.4 **Notarea unei discipline se face pe o scală de la 10 la 1, notele acordate fiind numere întregi;nota minimă de promovare este 5, iar nota maximă este 10; Media minimă de promovare a anilor de studii pentru promoţia 2021, domeniul de studii Inginerie electronică, telecomunicaţii şi tehnologii informaţionale, programul de studii Securitate cibernetică şi managementul riscurilor este _____, iar media maximă este _____, titularul fiind clasat pe locul ___ dintr-un total de ____ absolvenţi.**

Grades are integer numbers and given on a scale from 10 (the highest grade) to 1 (the lowest grade); the lowest passing grade is 5. The passing overall average grades for the class of 2021, field of study Electronics engineering. telecommunications and informational technologies, study programme in Cyber Security and Risks Management, are : lowest average ____ (out of 10) and highest average ____ (out of 10), the degree holder is ranked ___ out of ___ graduates.

L.S.

4.3

Nr. *No*	*Subject*	[3] Total ore *Number of hours*		Nota/ *Grade*		Nr. credite *Number of ECTS/SECT credits*	
		C	**S, LP, P**	**Sem I 1st sem**	**Sem II 2nd sem**	**Sem I 1st sem**	**Sem II 2nd sem**
	Anul I (anul universitar **2019-2020**) *1st year of study (**2019-2020** academic year)*						
1	Principii fundamentale de securitate cibernetică în tehnologia informaţiei / Cyber Security Fundamentals in information technology	28	28			4	-
2	Securitatea informaţională şi tehnologii criptografice / Information security and Cryptographic Technologies	28	28			4	-
3	Protocoale şi interfeţe de comunicare aferente infrastructurilor critice în energetică, transporturi şi servicii / Protocols and communication interfaces for critical infrastructures in energy, transport and services	28	14			5	-
4	Practică I /Pratics I	-	84			4	-
5	Sisteme electronice de navigaţie / Electronic navigational systems Managementul securităţii cibernetice / Cyber Security Management	28	14			4	-
6	Taxonomia riscurilor de securitate cibernetică în tehnologiile informaţionale / Cyber Security Taxonomy Threats in Information Technologies	28	28			4	-
7	Antene, arhitecturi de comunicaţii şi riscuri cibernetice / Antennas, communication architectures and cyber risks Managementul tehnologiei informaţiilor prin prisma ameninţărilor hibride / Information Technology Hybrid Threat Management	28	28			5	-
8	Securitatea cibernetică a sistemelor de control industrial (SCADA, PLC, DPC) / Cyber security of industrial control systems (SCADA, PLC, DPC)	28	42			-	5
9	Cultura organizaţională de securitate / Organizational culture of security	28	28			-	5
10	Securitatea cibernetică a dispozitivelor mobile şi riscurile asociate IoT / Cyber Security Risks Associated with Mobile Devices and IoT	28	28			-	6
11	Siguranţa tehnicilor de programare şi securitatea aplicaţiilor şi sistemelor informatice / Safety Programming Techniques and Security Applications and Informatics Systems	28	28			-	5
12	Practică II /Pratics II	-	112			-	4
13	Sisteme de comunicaţii subacvatice / Underwater communication systems Infracţiuni informatice în legislaţia penală română / Computer crimes in Romanian criminal law	28	14			-	5
Promovat cu media: [4] *Pass, average grade per academic year*		Total credite: Total ECTS/SECT credits:				60	
	Anul II (anul universitar **2020-2021**) *2nd year of study (**2020-2021** academic year)*						
1	Vulnerabilităţile tehnologiilor utilizate în Internet, analiză malware şi IT Forensic / Vulnerabilities of Internet technologies, malware analysis and Forensic IT	28	42			5	-
2	Protecţia datelor şi legislaţia privind securitatea / Data protection and security legislation	28	28			4	-
3	Managementul riscului în tehnologiile informaţionale / Risk Management of Information Technologies	28	28			4	-
4	Tehnologia informaţiei şi Industria 4.0 / Information Technologies and Industry 4.0	28	28			5	-
5	Etică şi integritate academică / Ethics and academic integrity	-	14			4	-
6	Practică III /Pratics III	-	112			4	-
7	Echipamente radio definite software / Defined radio equipment Factorul uman, ingineria socială şi criminalitatea cibernetică / Human factor, social engineering and cybercrime	28	14			4	-
8	Calculul evolutiv în tehnologia informaţiei / Progressive Computing in Information Technology	28	28			-	5
9	Tehnici şi instrumente de evaluare a securităţii cibernetice, hacking etic şi audit de securitate / Techniques and tools for assessing cyber security, ethical hacking and security audit	28	28			-	5
10	Competitive & Business Intelligence şi mecanisme de răspuns la crize din perspectiva Cyber Security / Competitive & Business Intelligence and Crisis Response Mechanisms from the Cyber	28	28				5
11	Limbaje de descriere hardware / Hardware description languages Investigarea infracţiunilor informatice / Investigating cybercrime						5
12	Practică IV / Pratics IV	-	42			-	5
13	Practică pentru pregătirea lucrării de disertaţie / Practice for preparing the dissertation paper	-	112				5
14	Elaborarea şi Susţinerea lucrării de disertaţie / Elaboration and defending of the dissertation paper	-	28				10
Promovat cu media: [4] *Pass, average grade per academic year*		Total credite: Total ECTS/SECT credits:				60 +10	

Promovat: DA *YES* *Pass:*	Media aritmetică a anilor de studii [5]: *The arithmetic mean of the study years:*	Total credite: 120+10 *Total ECTS/SECT credits:*

5. INFORMAŢII SUPLIMENTARE
ADDITIONAL INFORMATION

	Informaţii suplimentare *Additional information*		Alte surse pentru obţinerea mai multor informaţii *Further information sources*
5.1	**Studentul a fost înmatriculat, având numărul matricol 01. Conform deciziei xxx/01.10.2019** The student was enrolled, having the registration number 01. According to the decision xxx / 01.10.2019	5.2	**900663, Constanţa** **Str. Mircea cel Bătrân, nr. 104** **Tel./Fax:+40-241-664740/617260** **www.cmu-edu.eu** *www.cmu-edu.eu*

6. INFORMAŢII PRIVIND DREPTURILE CONFERITE DE CALIFICARE ŞI DE TITLU (dacă este cazul)
INFORMATION ON THE FUNCTION OF THE QUALIFICATION AND DEGREE (if applicable)

Posibilităţi de continuare a studiilor (după promovarea examenului de finalizare)
Access to further study (after passing the final examination)

6.1 **STUDII DE DOCTORAT**
PhD studies

Statutul profesional (dacă este cazul)
Professional status (if applicable)

6.2 **Ocupaţii posibile conform COR :**
215222 - Inginer sisteme de Securitate
215220 - Specialist mentenanţă electromecanică-automatică echipamente industriale
215227 - Inginer de cercetare în comunicaţii
251402 - Specialist în proceduri şi instrumente de securitate a sistemelor informatice

Possible professions according to the Romanian Code of Professions:
215222 – Security systems engineer
215220 - Specialist for electromechanical and automatic maintenance of industrial equipment
215227 - Communications Research Engineer
251402 - Security procedures and Security IT Tools Specialist,

L.S.

7. LEGALITATEA SUPLIMENTULUI
CERTIFICATION OF THE SUPPLEMENT

	Funcţia *Position*	Semnătura *Signature*		Funcţia *Position*	Semnătura *Signature*
7.1	**RECTOR** ***RECTOR*** **Prof. univ. dr. ing. Cornel Panait**		7.2	**Secretar şef universitate** ***University Registrar*** **Edith Pădineanu**	
7.3	**DECAN** ***DEAN*** **Conf. univ.dr.ing. Ion Omocea**		7.4	**Secretar şef facultate** ***Faculty Registrar*** **Nicolae Anca**	

	[6] Nr. şi data eliberării *No., dated.*		Ştampila sau sigiliul oficial *Official stamp or seal*
7.5	_____/_____ **Acest document conţine un număr de 7 pagini.** *This document consists of 7 pages.*	7.6	L.S.

1) Denumirea ministerului şi a instituţiei de învăţământ superior care a asigurat şcolarizarea şi care eliberează suplimentul la diplomă.
1) Name of ministry and institution administering studies and provided diploma supplement.
2) Se va completa de către instituţia de învăţământ superior care eliberează diploma. Aceasta trebuie să verifice legalitatea tuturor înscrisurilor de pe diplomă şi de pe suplimentul la diplomă.
2) To be filled in by the awarding institution that must check the legality of all information provided in the diploma and diploma supplement.
3) Se va menţiona numărul total de ore, din care: numărul total de ore de curs (C); numărul total de ore de seminar (S); numărul total de ore de lucrări practice (LP); numărul total de ore de proiect (P); etc.
3) It shall be mentioned the total hours of which total hours for courses (C), seminars (S), practical courses (LP), projects (P).
4) Media anuală, cu două zecimale, fără rotunjire.
4) Average grade per academic year, with two decimals and without rounding off.
5) Media aritmetică a anilor de studii, cu două zecimale, fără rotunjire.
5)The arithmetic mean of the study years with two decimals and without rounding off.
6) Se va completa de către instituţia care a asigurat şcolarizarea titularului.
6) To be filled in by the institution administering studies.

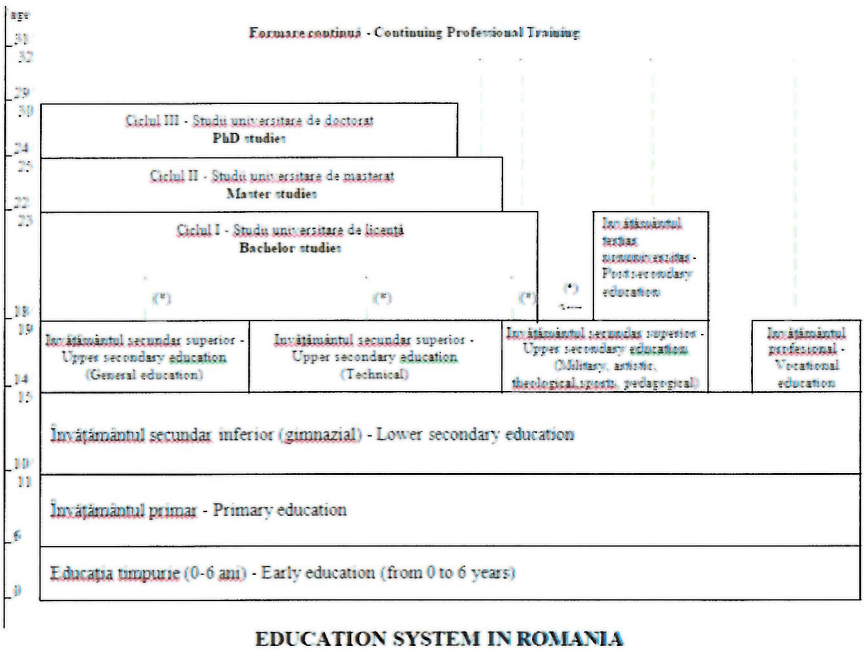
Suplimentul la diplomă se va redacta pe format A4 (faţă/verso), se va numerota şi se va ştampila pe fiecare pagină, pe colţul din dreapta jos (L.S.), cu acelaşi specimen de la 7.6.

Diploma supplement shall be printed on both sides of an A4 paper format and shall be numbered and stamped on each page on the right bottom corner (L.S.), with the same specimen from 7.6.

Punctul 4.3 "Detalii privind programul absolvit (conform Registrului matricol al facultăţii, volumul nr. .../...)" va fi completat cu durata corespunzătoare programului de studii universitare de master sau cu durata profesiilor reglementate.

The point 4.3 'Programme details and the individual grades/marks/ECTS/SECT credits obtained (according to Faculty Student Records, volume no./)' will be completed with the appropriate duration of university master's program or with the duration of regulated professions.

8. INFORMAŢII PRIVIND SISTEMUL NAŢIONAL DE ÎNVĂŢĂMÂNT
INFORMATION ON THE NATIONAL EDUCATION SYSTEM



EDUCATION SYSTEM IN ROMANIA

PREZENTARE GENERALĂ A SISTEMULUI NAŢIONAL DE ÎNVĂŢĂMÂNT SUPERIOR
Overview of the national higher education system

Accesul în învăţământul superior se bazează pe diploma de bacalaureat (obţinută la sfârşitul învăţământului secundar superior), iar accesul la programe de master se bazează pe diploma obţinută după finalizarea studiilor de licenţă (BA/BSc/BEng).
Access to higher education is based on the baccalaureate diploma (obtained at the end of upper secondary education) and access to master programmes is based on the bachelor degree (BA/BSc/BEng).
Studiile universitare de licenţă (BA/BSc/BEng) presupun 180 - 240 de puncte de credit, calculate în conformitate cu sistemul european de credite transferabile (ECTS/SECT) şi se finalizează prin nivelul 6 din cadrul european al calificărilor pentru învăţare pe tot parcursul vieţii (EQF/CEC).
Bachelor studies (BA/BSc/BEng) presuppose 180-240 credit points, calculated in accordance with the European Credit Transfer System (ECTS/SECT), and ends with the level 6 from the European Qualifications Framework for lifelong learning (EQF/CEC).
Studiile universitare de master (MA/MSc/MEng) presupun 60-120 puncte de credit, calculate în conformitate cu sistemul european de credite transferabile (ECTS/SECT) şi se finalizează prin nivelul 7 din EQF/CEC.
Master studies (MA/MSc/MEng) presuppose 60-120 credit points, calculated in accordance with the European Credit Transfer System (ECTS/SECT), and ends with the level 7 EQF/CEC.
Pentru profesii reglementate prin norme, recomandări sau bune practici europene, studiile universitare de licenţă şi masterat pot fi oferite comasat, într-un program unitar de studii universitare cu o durată cuprinsă între 5 şi 6 ani, la învăţământul cu frecvenţă, diplomele obţinute fiind echivalente diplomei de master (în următoarele domenii de studiu: Medicină - 360 de ECTS/SECT, Medicină dentară - 360 de ECTS/SECT, Farmacie - 300 ECTS/SECT, Medicină Veterinară - 360 ECTS/SECT, Arhitectură - 360 ECTS/SECT, Arhitectură de interior - 300 ECTS/SECT, Design de produs - 300 ECTS/SECT).
For professions regulated by European norms, regulations or good practices, bachelor (BA/BSc/BEng) and master studies (MA/MSc/MEng) can be provided as part of a 5 to 6 year full time programme of study, thus diplomas are recognized as master's degree certificates (the following fields of study are considered:Medicine - 360 ECTS/SECT, Dentistry - 360 ECTS/SECT, Pharmacy - 300 ECTS/SECT, Veterinary Medicine - 360 ECTS/SECT, Architecture - 360 ECTS/SECT, Architecture of inside - 300 ECTS/SECT, Design of product - 300 ECTS/SECT).
Studiile universitare de doctorat conduc la o teza de doctorat, iar candidaţii care finalizează primesc diploma de doctor. Studiile universitare de doctorat permit dobândirea unei calificări de nivelul 8 din EQF/CEC.
PhD studies result in a doctoral research thesis, while successful candidates are awarded a PhD diploma. Doctoral studies allow obtaining a qualification at level 8 EQF/CEC.

L.S.

Sistemul de învăţământ superior românesc este un sistem deschis. Toate universităţile din România folosesc Sistemul European de Credite Transferabile (ECTS/SECT).

The Romanian higher education system is an open system. All Romanian universities use the European Credit Transfer System (ECTS/SECT).

Programele de studii universitare pot fi organizate, după caz, conform reglementărilor legale în vigoare, la următoarele forme de învăţământ: cu frecvenţă, cu frecvenţă redusă şi la distanţă.

University programs can be organized, as appropriate, according to legal regulations, at the following forms of education:full time, part time and distantly.

De asemenea, universităţile oferă programe de formare profesională continuă, pe baza cererilor de pe piaţa muncii. Universities also provide continuing professional training programmes based on the market demands.

(*) În conformitate cu Legea nr. 1/2011

According to Law no. 1/2011

L.S.

FACULTATEA DE ELECTROMECANICĂ NAVALĂ

Departamentul de Ştiinţe Generale Inginereşti

STUDII UNIVERSITARE DE MASTER

Domeniul: INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE

Specializarea: *SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR*

APROBĂ
RECTOR,
prof. univ.dr.ing. Cornel PANAIT

PLAN DE ÎNVĂŢĂMÂNT
Cu începere din anul universitar 2019-2020

Facultatea de ELECTROMECANICĂ NAVALĂ
Domeniul: *INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE*
Specializarea de masterat: ***SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR***
Durata studiilor: 2 ani
Forma de învăţământ: cursuri de zi
Titlul absolventului: Master

MISIUNEA PROGRAMULUI DE STUDII

În contextul actual, în care sistemele informatice sunt supuse la ameninţări multiple, iar datele personale ale utilizatorilor sunt privite ca produse ce pot fi tranzacţionate pe piaţă, este necesar ca la nivelul sistemelor informatice să fie asigurată o securitate minimă predictibilă şi să existe o informare a utilizatorilor în privinţa riscurilor existente.

Astfel, securitatea cibernetică trebuie privită din perspectiva rolului pe care sistemul îl are în cadrul infrastructurii (cerere de servicii, oferire de servicii, echipament de reţea), fiecare rol necesitând diferite soluţii şi metode de asigurare a securităţii.

Domeniul securității cibernetice a început să capete dimensiuni noi odată cu creșterea gradului de automatizare a nivelului tehnologic și extinderea și amplificarea amenințărilor/atacurilor cibernetice.

Administratorii de securitate din orice organizație au misiunea dificilă de a încerca să facă față tuturor amenințărilor cibernetice cu care se confruntă și de a minimiza posibilitățile de compromitere a infrastructurii IT. În acest sens, este necesar a fi optimizat procesul de monitorizare și detecție a evenimentelor de securitate, în scopul prevenirii, detecției și răspunsului optim la incidentele de securitate cibernetică.

Misiunea programului de masterat constă în familiarizarea managerilor, a specialiştilor care lucrează în diferite companii şi instituţii care gestionează infrastructuri critice, din domeniile tehnice inginereşti şi IT, cu provocările induse de vulnerabilităţile echipamentelor şi sistemelor tehnologice digitizate în faţa atacurilor cibernetice.

Programul de masterat oferă cursanţilor cunoştinţele teoretice şi deprinderile practice necesare pentru:

- cunoaşterea principalelor coordonate ale securizării rețelelor și sistemelor informatice, în vederea identificării rapide a atacurilor cibernetice,
- înţelegerea și recunoașterea comportamentului aplicaţiilor malware
- cunoașterea metodelor și tehnologiilor criptografice
- cunoaşterea principalelor ameninţări din spaţiul cibernetic şi a metodelor de atac cel mai des folosite
- auditarea și evaluarea securităţii cibernetice a sistemelor informatice utilizate în cadrul companiilor și infrastructurilor critice
- prevenirea și combaterea criminalității informatice
- îmbunătăţirea sistemului de management al securităţii informaţiilor

OBIECTIVE GENERALE

Obiectivele generale sunt reprezentate de însuşirea de către participanţii la programul de pregătire de masterat a cunoştinţelor teoretice pe baza cărora aceştia să poată contribui la asigurarea unui nivel adecvat de securitate cibernetică, prevenirea și combaterea criminalității informatice, îmbunătăţirea sistemului de management al securităţii informaţiilor.

OBIECTIVE SPECIFICE

Obiectivele specifice sunt reprezentate de însuşirea de către participanţii la programul de pregătire de masterat a cunoştinţelor teoretice şi deprinderile practice necesare pentru:

- cunoaşterea principalelor coordonate ale securizării rețelelor și sistemelor informatice, în vederea identificării rapide a atacurilor cibernetice,
- înţelegerea și recunoașterea comportamentului aplicaţiilor malware
- cunoașterea metodelor și tehnologiilor criptografice
- cunoaşterea principalelor ameninţări din spaţiul cibernetic şi a metodelor de atac cel mai des folosite
- auditarea și evaluarea securităţii cibernetice a sistemelor informatice utilizate în cadrul companiilor și infrastructurilor critice
- prevenirea și combaterea criminalității informatice
- îmbunătăţirea sistemului de management al securităţii informaţiilor

COMPETENŢE

Competenţe profesionale

1. Cunoştinţe specifice de telecomunicaţii şi tehnologia informaţiilor
   - Folosirea creativă a conceptelor fundamentale din telecomunicaţii şi tehnologia informaţiilor, a metodelor de modelare şi simulare, pentru realizarea modelelor unor sisteme electronice de comunicaţii;
   - Aplicarea creativă a cunoştinţelor şi metodelor specifice domeniului telecomunicaţii şi tehnologiei informaţiei;
2. Comprehensiunea şi interpretarea actelor normative care reglementează domeniul de referință
   - Însușirea și interpretarea conceptelor și termenilor folosiți în domeniul securității cibernetice;
   - Capacitatea de corelare și realizare de conexiuni logice între două sau mai multe prevederi legislative din diferite state europene;
   - Identificarea compatibilităților, a diferențelor și a elementelor contradictorii dintre prevederile legislației naționale și ale celei europene în vederea analizării şi identificării metodelor şi mecanismelor de cooperare transnațională;
   - Cunoaşterea modului de organizare şi desfăşurare a proceselor de management al riscurilor de securitate asociate infrastructurilor cibernetice;
3. Elaborarea a noi inițiative în domeniul prevenirii și combaterii criminalității cibernetice
   - Aplicarea metodologiilor și utilizarea în mod corespunzător a instrumentelor tehnice specializate de evaluare a securităţii sistemelor informatice;
   - Implementarea unor soluţii noi de securitate, eficiente, care să asigure un nivel adecvat de protecție în cazul unor atacuri cibernetice complexe;
4. Răspunsul la incidentele de securitate cibernetică
   - Cunoșterea și aplicarea prevederilor și procedurilor legale pentru investigarea incidentelor de securitate cibernetică;
   - Utilizarea în mod corect a instrumentele de colectare a probelor digitale si cunoasterea mecanismelor și a tehnicilor de investigare a acestora;

Competenţe transversale

- Abilitatea de a comunica în diferite medii manifestînd toleranţa; exprimarea şi înţelegerea diferitelor puncte de vedere; negocierea şi abilitatea de a crea încredere şi de a manifesta empatie; abilitatea de a face faţă stresului şi frustrării precum şi abilitatea de a le exprima în mod constructiv.

- Dezvoltarea competenţelor civice şi a deprinderilor civice prin implicarea alături de ceilalţi în domeniul public, solidaritate şi interes în rezolvarea problemelor care afectează comunitatea; reflectarea critică şi creativă şi participarea constructivă în activităţile comunităţii, precum şi în luarea deciziilor cu privire la securitatea organizaţională şi a sistemelor de infractructuri critice.

- Aplicarea, în mod responsabil, a principiilor, normelor şi valorilor eticii profesionale în realizarea sarcinilor profesionale şi identificarea obiectivelor de realizat, a resurselor disponibile, a etapelor de
- a duratelor de execuţie, a termenelor de realizare aferente şi a riscurilor aferente.

- Identificarea rolurilor şi responsabilităţilor într-o echipă pluridisciplinară şi aplicarea de tehnici de relaţionare şi muncă eficientă în cadrul echipei

- Autoevaluarea obiectivă a nevoii de formare profesională continuă în domeniul telecomunicaţiilor şi tehnologiei informaţionale, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia.

- Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale.

- Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

REPARTIZAREA FONDULUI DE TIMP PE ANI DE STUDII, CATEGORII DE PREGĂTIRE ŞI DISCIPLINE

PLAN DE ÎNVĂŢĂMÂNT

UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea de ELECTROMECANICĂ NAVALĂ
Domeniul: ***INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE***
Program de masterat: ***SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR***
Durata de studii: 2 ani
Forma de studiu: cursuri de zi
Titlul obţinut: Master

Aprobat
RECTOR,
prof. univ.dr.ing. Cornel PANAIT

CURRICULUM

Anul de studii : I - începând cu anul universitar 2019-2020

CURSURI OBLIGATORII

Nr. crt.	Denumirea Disciplinei	Cod	Tip disc.	Semestrul 1 - 14 săptămâni							Semestrul 2 - 14 săptămâni						
				C	S	L	P	SI	FV	PC	C	S	L	P	SI	FV	PC
1	Principii fundamentale de securitate cibernetică în tehnologia informaţiei	CYSEC 1.1.1	DA	2	-	2	-	64	E	4							
2	Securitatea informaţională şi tehnologii criptografice	CYSEC 1.2.1	DA	2	-	2	-	16	C	4							
3	Protocoale şi interfeţe de comunicare în industrie aferente infrastructurilor critice în energetică, transporturi şi servicii	CYSEC 1.3.1	DS	2	-	1	-	78	E	5							
4	Practică I	CYSEC 1.4.1	DS				6		C	4							
5	Sisteme de conducere a proceselor industriale şi protecţie cibernetică (SCADA, PLC, DPC)	CYSEC 1.5.2	DS								2	-	2	1	64	E	5
6	Cultura organizaţională de securitate	CYSEC 1.6.2	DC								2	2	-	-	64	E	5
7	Securitatea cibernetică a dispozitivelor mobile şi riscurile asociate IoT	CYSEC 1.7.2	DS								2	-	2	-	64	E	6
8	Siguranţa tehnicilor de programare şi securitatea aplicaţiilor şi sistemelor informatice	CYSEC 1.8.2	DA								2	-	2	-	64	E	5
9	Practică II	CYSEC 1.9.2	DS											8		C	4
Total ore (puncte credit) pe săptămână				6	-	5	6		2E+2C	17	8	2	6	9		4E+C	25
				17							25						

Legendă: C – curs; S – seminar; L – laborator; P – proiect; SI – ore de studiu individual; FV – forma de verificare ; PC – puncte credit atribuite

DECAN,
Conf.univ.dr.ing. Ion OMOCEA

DIRECTOR DEPARTAMENT,
Conf.univ.dr.ing. Alexandra RAICU

UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea de ELECTROMECANICĂ NAVALĂ
Domeniul: ***INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE***
Program de masterat: ***SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR***
Durata de studii: 2 ani
Forma de studiu: cursuri de zi
Titlul obţinut: Master

Aprobat
RECTOR,
prof. univ.dr.ing. Cornel PANAIT

CURRICULUM

Anul de studii : I – începând cu anul universitar 2019-2020

CURSURI OPŢIONALE

Nr. crt.	Denumirea Disciplinei	Cod	Tip disc.	Semestrul 1 - 14 săptămâni							Semestrul 2 - 14 săptămâni						
				C	S	L	P	SI	FV	PC	C	S	L	P	SI	FV	PC
PACHETUL A																	
1	Sisteme electronice de navigaţie	CYSEC 1.5.1	DS	2	-	1	-	62	C	4							
2	Analiza şi clasificarea riscurilor de securitate cibernetică în tehnologiile informaţionale	CYSEC 1.6.1	DA	2	-	1	1	64	E	4							
3	Antene, arhitecturi de comunicaţii şi riscuri cibernetice	CYSEC 1.7.1	DA	2	-	2		48	E	5							
4	Sisteme de comunicaţii subacvatice	CYSEC 1.10.2	DS								2	-	1	-	62	C	5
	Total ore (puncte credit) pe săptămână			6	-	4	1		2E+C	13	2	-	1			C	5
				11							3						
PACHETUL B																	
1	Managementul securităţii cibernetice	CYSEC 1.5.1	DS	2	1	-	-	30	C	4							
2	Analiza şi clasificarea riscurilor de securitate cibernetică în tehnologiile informaţionale	CYSEC 1.6.1	DA	2	-	1	1	64	E	4							
3	Managementul tehnologiei informaţiilor prin prisma ameninţărilor hibride	CYSEC 1.7.1	DA	2	2	-	-	48	E	5							
4	Infracţiuni informatice în legislaţia penală română	CYSEC 1.10.2	DS								2	1	-	-	30	C	5
	Total ore (puncte credit) pe săptămână			6	3	1	1		2E+C	13	2	1	-	-		C	5
				11							3						
Total ore (puncte credit) pe săptămână cursuri obligatorii şi opţionale				28					4E+3C	30	28					4E+2C	30

Legendă: C – curs; S – seminar; L – laborator; P – proiect; SI – ore de studiu individual; FV – forma de verificare ; PC – puncte credit atribuite

DECAN,
Conf.univ.dr.ing. Ion OMOCEA

DIRECTOR DEPARTAMENT,
Conf.univ.dr.ing. Alexandra RAICU

UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea de ELECTROMECANICĂ NAVALĂ
Domeniul: ***INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE***
Program de masterat: ***SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR***
Durata de studii: 2 ani
Forma de studiu: cursuri de zi
Titlul obţinut: Master

Aprobat
RECTOR,
prof. univ.dr.ing. Cornel PANAIT

CURRICULUM

Anul de studii : I - începând cu anul universitar 2019-2020

CURSURI FACULTATIVE

Nr. crt.	Denumirea Disciplinei	Cod	Tip disc.	Semestrul 1 - 14 săptămâni							Semestrul 2 - 14 săptămâni						
				C	S	L	P	SI	FV	PC	C	S	L	P	SI	FV	PC
1	Cadrul naţional şi european de reglementare al securităţii cibernetice	CYSEC 1.11.2	DC								2	2	-	-	64	C	5
Total ore (puncte credit) pe săptămână											**2**	**2**	**-**	**-**		**C**	**5**
											4						

Legendă: C – curs; S – seminar; L – laborator; P – proiect; SI – ore de studiu individual; FV – forma de verificare ; PC – puncte credit atribuite

DECAN,
Conf.univ.dr.ing. Ion OMOCEA

DIRECTOR DEPARTAMENT,
Conf.univ.dr.ing. Alexandra RAICU

UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea de ELECTROMECANICĂ NAVALĂ
Domeniul: ***INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE***
Program de masterat: ***SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR***
Durata de studii: 2 ani
Forma de studiu: cursuri de zi
Titlul obţinut: Master

Aprobat
RECTOR,
prof. univ.dr.ing. Cornel PANAIT

CURRICULUM

Anul de studii : II, începând cu anul universitar 2019-2020

CURSURI OBLIGATORII

Nr. crt.	Denumirea Disciplinei	Cod	Tip disc.	Semestrul 1 - 14 săptămâni							Semestrul 2 - 14 săptămâni						
				C	S	L	P	SI	FV	PC	C	S	L	P	SI	FV	PC
1	Vulnerabilitățile tehnologiilor utilizate în Internet, analiză malware şi IT Forensic	CYSEC 2.1.1	DA	2	-	2	1	74	E	5							
2	Legislația privind securitatea şi criminalitatea economico financiară	CYSEC 2.2.1	DC	2	-	2	-	88	E	4							
3	Managementul riscului în tehnologiile informaționale	CYSEC 2.3.1	DC	2	2	-	-	40	C	4							
4	Aplicarea tehnologiei informației şi comunicațiilor pentru a monitoriza şi controla procesele fizice	CYSEC 2.4.1	DC	2	2	-	-	88	E	5							
5	Etică şi integritate academică	CYSEC 2.5.1	DC	1	-	-	-	90	C	4							
6	Practică III	CYSEC 2.6.1	DS	-	-	-	7		C	4							
7	Calculul evolutiv în tehnologia informației	CYSEC 2.7.2	DA								2	-	2	-	64	E	5
8	Tehnici şi instrumente de evaluare a securității cibernetice, hacking etic şi audit de securitate	CYSEC 2.8.2	DS								2	-	2	-	64	E	5
9	Mecanisme de răspuns la crize din perspectiva Cyber Security	CYSEC 2.9.2	DS								2	2	-	-	64	E	5
10	Practică IV	CYSEC 2.10.2	DS								-	-	-	3	-	C	5
11	Practică pentru pregătirea lucrării de disertație	CYSEC 2.11.2	DS											8		C	5
12	Elaborarea şi Susținerea lucrării de disertație	CYSEC 2.12.2	DS											2			10
Total ore (puncte credit) pe săptămână				9	4	4	8		3E+3C	26	6	2	4	13		3E+2C	25+10
				25							25						

Legendă: C – curs; S – seminar; L – laborator; P – proiect; SI – ore de studiu individual; FV – forma de verificare ; PC – puncte credit atribuite

DECAN,
Conf.univ.dr.ing. Ion OMOCEA

DIRECTOR DEPARTAMENT,
Conf.univ.dr.ing. Alexandra RAICU

UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea de ELECTROMECANICĂ NAVALĂ
Domeniul: ***INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE***
Program de masterat: ***SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR***
Durata de studii: 2 ani
Forma de studiu: cursuri de zi
Titlul obţinut: Master

Aprobat
RECTOR,
prof. univ.dr.ing. Cornel PANAIT

CURRICULUM

Anul de studii : II –începând cu anul universitar 2019-2020

CURSURI OPŢIONALE

Nr. crt.	Denumirea Disciplinei	Cod	Tip disc.	Semestrul 1 - 14 săptămâni							Semestrul 2 - 14 săptămâni						
				C	S	L	P	SI	FV	PC	C	S	L	P	SI	FV	PC
PACHETUL A																	
1	Echipamente radio definite software	CYSEC 2.7.1	DS	2	-	1	-	62	C	4							
2	Limbaje de descriere hardware	CYSEC 2.13.2	DS								2	-	1	-	62	E	5
	Total ore (puncte credit) pe săptămână			**2**	**-**	**1**	**-**		**C**	**4**	**2**	**-**	**1**	**-**		**E**	**5**
				3							**3**						
PACHETUL B																	
1	Implicarea factorului uman în securitatea cibernetică maritimă	CYSEC 2.7.1	DS	2	1	-	-	54	C	4							
2	Investigarea infracţiunilor informatice	CYSEC 2.13.2	DS								2	1	-	-	78	E	5
	Total ore (puncte credit) pe săptămână			**2**	**1**	**-**	**-**		**C**	**4**	**2**	**1**		**-**		**E**	**5**
				3							**3**						
Total ore (puncte credit) pe săptămână cursuri obligatorii şi opţionale				**28**					**3E+4C**	**30**	**28**					**3E+2C**	**30**

Legendă: C – curs; S – seminar; L – laborator; P – proiect; SI – ore de studiu individual; FV – forma de verificare ; PC – puncte credit atribuite

DECAN,
Conf.univ.dr.ing. Ion OMOCEA

DIRECTOR DEPARTAMENT,
Conf.univ.dr.ing. Alexandra RAICU

NOTĂ 1: Numărul de ore de studiu individual /disciplină /semestru se calculează cu formula: **SI = PC x 24 – 14** x(**C+S+L+P**)

NOTĂ 2: Pentru **Susţinerea lucrării de dizertaţie** se acordă 10 puncte de credite transferabile, peste totalul celor 120 alocate programului de studii.

STRUCTURA ANULUI UNIVERSITAR (ÎN SĂPTĂMÂNI)

	Activităţi didactice		Sesiune de examene			Vacanţe		
	Sem. I	Sem. II	Iarnă	Vară	Restanţe	Iarnă	Primăvară	Vară
Anul I	14	14	4	4	2	2	1	12
Anul II	14	14	4	4	2	2	1	12

NOTE EXPLICATIVE CU PRIVIRE LA ACTIVITATEA DE CERCETARE ŞTIIŢIFICĂ

La **Facultatea de Electromecanică Navală**, specializarea de masterat **„SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR”, activitatea** de cercetare şi elaborare a lucrării de disertaţie a studenţilor masteranzi se desfăşoară pe toată durata semestrului patru de studiu.

Activitatea de cercetare ştiinţifică în care sunt implicaţi studenţii masteranzi, se organizează şi se desfăşoară prin proiecte şi teme, finanţate sau nefinanţate, cuprinse în programe corelate cu *Planurile Strategice* şi *Operaţionale* ale **Facultăţii de Electromecanică Navală** şi cu *Planul Activităţii de Cercetare Ştiinţifică* al **Departamentul de Ştiinţe Generale Inginereşti,** coordonator al programului de studii universitare de masterat.

În principal, activităţile de cercetare ştiinţifică sunt derulate prin **Centrul de Securitate Cibernetică în Domeniul Maritim** entitate aparţinătoare **Universităţii Maritime din Constanţa**, care are drept obiectiv să răspundă diverselor cerinţe privind managementul educaţional şi profesional, de cercetare ştiinţifică universitară, de diseminare a informaţiilor şi consultanţă tehnico-economică, pe termen mediu şi lung, corespunzător nevoilor mediului economic şi industrial în domeniul securităţii cibernetice.

FINALIZAREA STUDIILOR

La **Facultatea de Electromecanică Navală**, pentru specializarea de studii universitare de masterat **„SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR”,** finalizarea studiilor se realizează în două etape:

1. Cercetare ştiinţifică pentru dizertaţie prin stagiile de practică care se desfăşoară pe parcursul fiecărui semestru;
2. Studiu pentru elaborarea lucrării de dizertaţie din ultimul semestru de studiu.

În principiu, **Departamentul de Ştiinţe Generale Inginereşti** al **Facultăţii de Electromecanică Navală,** aduce la cunoştinţă studenţilor propunerile pentru temele **Lucrărilor de Dizertaţie**, la începutul semestrului doi. Temele trebuie să abordeze problematica aferentă procesului de pregătire pe parcurs şi ele se constituie în studii teoretice, aplicative şi practice pentru soluţionarea unor probleme inginereşti şi manageriale specifice proiectării, construcţiei şi exploatării utilajelor, instalaţiilor, sistemelor şi echipamentelor caracteristice industriei marine sau de offshore.

În cadrul **Examenului de Dizertaţie**, absolvenţii trebuie să dovedească însuşirea competenţelor şi abilităţilor profesionale specifice specializării **„ SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR”.**

BILANŢ GENERAL					
Nr. crt.	**Discipline**	**Număr de ore**	**%**	**Număr de Credite**	**%**
1	Total ore	1568		120	100
2	Discipline complementare (DC)	238	15,18	22	18,33
3	Discipline de specialitate (DS)	924	58,93	66	55,00
4	Discipline de aprofundare (DA)	406	25,89	32	26,66
5	Discipline facultative (DFac)	4	2	5	4
6	Ore curs	574	36,61		
7	Ore aplicative (seminar + laborator +proiect)	518	33,04		
8	Ore practică incluzând practica pentru elaborarea lucrării de disertaţie	476	30,35		
9	Raport ore aplicative / ore curs	1,11			

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Principii fundamentale de securitate cibernetică în tehnologia informaţiei				
Titularul activităţilor de curs	Conf.univ.dr.ing. Raicu Gabriel				
Titularul activităţilor de seminar	Conf.univ.dr.ing. Raicu Gabriel				
Anul de studiu	1	Semestrul	1	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DA
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	-	Laborator	2	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	-	Laborator	28	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	26
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	20
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	10
II d) Tutoriat	8
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	64
Total ore pe semestru (Ib+II+III+IV)	122
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	• Cunoaşterea unei limbi străine

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• Masteranzii trebuie să respecte normele de conduită academică • Masteranzii nu se vor prezenta la prelegeri cu telefoanele mobile deschise; • Nu va fi tolerată întârzierea masteranzilor la curs; • Data susţinerii examenului se va stabili de titular de comun acord cu masteranzii.
Desfăşurare aplicaţii	Seminar	• Trebuie să respecte normele de conduită academică; • Nu se vor prezenta la seminare cu telefoanele mobile deschise; • Nu va fi tolerată întârzierea la seminare; • Termenele de predare şi susţinere a lucrărilor de seminar sunt stabilite de titular de comun acord cu masteranzii. Nu se vor accepta cererile de amânare a acestora pe motive altfel decât obiectiv întemeiate. De asemenea, nu se acceptă cererile doar de predare a temelor de seminar fără ca acestea să se susţină în faţa colegilor.

	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	• Însușirea și interpretarea conceptelor și termenilor folosiți în domeniul securității cibernetice; • Aplicarea metodologiilor și utilizarea în mod corespunzător a instrumentelor tehnice specializate de evaluare a securității sistemelor informatice • Implementarea unor soluţii noi de securitate, eficiente, care să asigure un nivel adecvat de protecţie în cazul unor atacuri cibernetice complexe • Acordarea de asistența necesară în cazul unor atacuri informatice factorilor responsabili în domeniu • Analiza caracteristicilor esenţiale ale principalelor incidente de securitate cibernetică. • Să utilizeze spațiul virtual pentru o conduită specifică care să îi asigure un nivel corespunzător de securitate și diminuare a amenințărilor informatice • Să valorifice cunoştinţele acumulate în vederea integrării în viitoarea activitate profesională şi viaţa socială; • Să participe la elaborarea proiectelor de desfăşurare a diferitelor activităţi profesionale la nivelul sistemului public / privat;
Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Cunoaşterea şi înţelegerea problematicii securităţii cibernetice în administrația publică / mediul antreprenorial / societăţi capital privat, a practicilor specifice în organizaţii, a procedurilor şi mecanismelor de management a amenințărilor informaticee pentru realizarea securității cibernetice cu alte entităţi specifice organizaţiei din care face parte

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
1. Concepte generale privind securitatea informatiei	2	Prelegere orală	
2. Securitatea informatiei in medii heterogene	2	Prelegere orală	
3. Arhitecturi de retea reziliente	6	Prelegere orală	3 ședințe x 2hrs
4. Retele wireless si modele de securitate	2	Prelegere orală	
5. Arhitectura retelei Internet	2	Prelegere orală	
6. Sisteme distribuite si concepte generale de securitate	2	Prelegere orală	
7. Securitatea sistemelor izolate	2	Prelegere orală	
8. Criptografie generala	4	Prelegere orală	2 ședințe x 2hrs
9. Pentesting si identificare vulnerabilitati	2	Prelegere orală	
10. Raspunsul la incidentele de securitate cibernetica	2	Prelegere orală	
11. Politici, standarde si managementul riscului	2	Prelegere orală	

Bibliografie

1. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.
2. "Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian
3. Stevens, Tim (2018-06-11). "Global Cybersecurity: New Directions in Theory and Methods". Politics and Governance. 6 (2): 1–4. doi:10.17645/pag.v6i2.1569.
4. "Computer Security and Mobile Security Challenges". researchgate.net. 3 December 2015. Archived from the original on 12 October 2016. Retrieved 4 August 2016.
5. "Distributed Denial of Service Attack". csa.gov.sg. Archived from the original on 6 August 2016. Retrieved 12 November 2014.
6. "Legion cyber-attack: Next dump is sansad.nic.in, say hackers". The Indian Express. 12 December 2016. Archived from the original on 29 December 2016. Retrieved 29 December 2016.
7. "15k patients' info shared on social media from NH Hospital data breach". RT International. Archived from the original on 29 December 2016. Retrieved 29 December 2016.

8. "Former New Hampshire Psychiatric Hospital Patient Accused Of Data Breach". CBS Boston. 27 December 2016. Archived from the original on 29 September 2017. Retrieved 29 December 2016.
9. "Texas Hospital hacked, affects nearly 30,000 patient records". Healthcare IT News. 4 November 2016. Archived from the original on 29 December 2016. Retrieved 29 December 2016.
10. Becker, Rachel (27 December 2016). "New cybersecurity guidelines for medical devices tackle evolving threats". The Verge. Archived from the original on 28 December 2016. Retrieved 29 December 2016.
11. "Postmarket Management of Cybersecurity in Medical Devices" (PDF). 28 December 2016. Archived (PDF) from the original on 29 December 2016. Retrieved 29 December 2016.
12. Brandt, Jaclyn (2018-06-18). "D.C. distributed energy proposal draws concerns of increased cybersecurity risks". Daily Energy Insider. Retrieved 2018-07-04.

Aplicații (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observații
1. Securitatea informatiei, exemple si aplicatii	2	problematizare, exercitiu	
2. Schimbul de date in medii eterogene	2	problematizare, exercitiu	
3. Arhitecturi de retea si elemente de propagare a riscurilor	2	problematizare, exercitiu	
4. Sisteme criptografice, algortimi si viteza de calcul	2	problematizare, exercitiu	
5. Securitatea informatiei, tehnici de obfuscare si teganografie	2	problematizare, exercitiu	
6. Pentesting. Exemple si aplicatii live	2	problematizare, exercitiu	
7. Adresarea riscurilor si paradigme legislative asociate	2	problematizare, exercitiu	

Bibliografie

13. Wireless mouse leave billions at risk of computer hack: cyber security firm Archived 3 April 2016 at the Wayback Machine
14. "Multi-Vector Attacks Demand Multi-Vector Protection". MSSP Alert. July 24, 2018.
15. Millman, Renee (December 15, 2017). "New polymorphic malware evades three quarters of AV scanners". SC Magazine UK.

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

Elaborarea fișei disciplinei a avut loc în urma discutării conținutului disciplinei și a cerințelor practice cu specialiști și practicieni din domeniu care își desfășoară activitatea în sectorul public și privat (manageri publici, funcționari publici de conducere și de execuție, personal contractual etc.), dar și pornind de la competențele profesionale cerute de piața muncii (prin însușirea noțiunilor teoretico-metodologice și a aspectelor practice din cadrul disciplinei, masteranzii dobândesc cunoștințe, în concordanță cu competențele parțiale cerute pentru ocupațiile posibile prevăzute în Grila RNCIS).

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	- Să cunoască termenii de specialitate și să înțeleagă conceptele privind securitatea cibernetică și interacțiunilor individului în spațiul virtual; - Să explice principiile operațiilor informaționale - Să identifice abordările decizionale pentru activitatea structurilor de specialitate - Să utilizeze spațiul virtual pentru comunicarea specifică	Examen scris	70%
Seminar	• Realizarea temelor de seminar • Prezența la curs și seminar	Evaluare continuă	30%
Laborator			
Proiect			
Standard minim de performanță			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	Conf.univ.dr.ing. Raicu Gabriel	Conf.univ.dr.ing. Raicu Gabriel

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Securitatea informaţională şi tehnologii criptografice				
Titularul activităţilor de curs	Prof.univ.dr.ing. Eliodor Constantinescu				
Titularul activităţilor de seminar	Prof.univ.dr.ing. Eliodor Constantinescu				
Anul de studiu	I	Semestrul	I	Tipul de evaluare	C

Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară	DA
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)	DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	-	Laborator	2	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	-	Laborator	28	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	6
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	2
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	4
II d) Tutoriat	4
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	16
Total ore pe semestru (Ib+II+III+IV)	74
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• Sala cu calculatoare
Desfăşurare aplicaţii	Seminar	• Sala cu calculatoare
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Cunoasterea conceptelor de baza si a principiilor securitatii informatiei Utilizarea corecta a primitivelor si a sistemelor criptografice Studiul principalelor primitive criptografice actuale Analizarea securitatii sistemelor criptografice

Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Prezentarea unor algoritmi matematici folositi în criptografie
	Algoritmi numerici şi algebrici vor fi studiaţi şi implementaţi în proiecte

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
1. Noţiuni de complexitatea algoritmilor, congruente	2	expunere, algoritmizare	
2. Primalitate şi factorizare	2	expunere, algoritmizare	
3. Resturi pătratice	2	expunere, algoritmizare	
4. Corpuri finite şi logaritmi discreţi	2	expunere, algoritmizare	
5. Sisteme clasice de criptare	2	expunere, algoritmizare	
6. Criptografie cu cheie private	2	expunere, algoritmizare	
7. Cifruri pe blocuri	2	expunere, algoritmizare	
8. Cifruri pe şiruri	2	expunere, algoritmizare	
9. Criptosistemul RSA	2	expunere, algoritmizare	
10. Criptosistemul ElGamal	2	expunere, algoritmizare	
11. Funcţii hash	2	expunere, algoritmizare	
12. Semnături digitale	2	expunere, algoritmizare	
13. Protocoale legate de chei	2	expunere, algoritmizare	
14. Criptografie cuantică	2	expunere, algoritmizare	

Bibliografie

1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
2. C. Gherghe, D. Popescu, Criptografie. Coduri. Algoritmi, Editura Univ. Bucuresti, 2005.
3. D. Kahn, The Codebreakers, Macmillan, 1967.
4. N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.
5. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997. [http://www.cacr.math.uwaterloo.ca/hac]

Bibliografie minimală

A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997. [http://www.cacr.math.uwaterloo.ca/hac]

Aplicaţii (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observaţii
1. Notiuni de complexitatea algoritmilor, congruente	4	problematizare, exercitiu	
2. Primalitate	4	problematizare, exercitiu	
3. Factorizare	4	problematizare, exercitiu	
4. Resturi patratice	4	problematizare, exercitiu	
5. Corpuri finite si logaritmi discreti	4	problematizare, exercitiu	
6. Criptografie cu cheie privata	4	problematizare, exercitiu	
7. Criptografie cu cheie publica	4	problematizare, exercitiu	

Bibliografie

1. S. Crivei, A. Marcus, C. Sacarea, C. Szanto, Computational algebra with applications to coding theory and cryptography, Editura EFES, Cluj-Napoca, 2006.
2. N. Koblitz, A Course in Number Theory and Cryptography, Springer-Verlag, 1994.
3. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997. [http://www.cacr.math.uwaterloo.ca/hac]

Bibliografie minimală

A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997.

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

- Conţinutul este orientat către aspecte practice ale criptografiei. Subiectul este prezent în mai multe programe de master în domenii ale informaticii aplicate în securitatea cibernetică în domeniul maritime din alte universităţi.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Cunoasterea sistemelor de criptare si a tehnicilor de criptanaliza prezentate pe parcursul cursului Abilitatea de a aplica cunostintele dobandite pe cazuri particulare Abilitatea de a argumenta utilizarea / inutilizarea unui anumit sistem criptografic in diferite scenarii Abilitatea de a analiza securitatea unui algoritm criptografic	Lucrare scrisă	60%
Seminar	Capacitatea de a aplica cunostintele dobandite in cadrul cursului pentru rezolvarea problemelor propuse	Teme de casă	40%
Laborator			
Proiect			
Standard minim de performanţă			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	Prof.univ.dr.ing. Eliodor Constantinescu	Prof.univ.dr.ing. Eliodor Constantinescu

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Protocoale şi interfeţe de comunicare în industrie aferente infrastructurilor critice în energetică, transporturi şi servicii				
Titularul activităţilor de curs	Prof.univ.dr.ing. Hnatiuc Bogdan				
Titularul activităţilor de seminar	Prof.univ.dr.ing. Hnatiuc Bogdan				
Anul de studiu	1	Semestrul	1	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	3	Curs	2	Seminar	-	Laborator	1	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	42	Curs	28	Seminar	-	Laborator	14	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	20
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	20
II d) Tutoriat	28
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	78
Total ore pe semestru (Ib+II+III+IV)	122
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		Sală cu tablă şi videoproiector
Desfăşurare aplicaţii	Seminar	•
	Laborator	Sala BNE119
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Capacitatea de a aplica cunoştinţele privind configurarea, monitorizarea şi comanda la distanţă a echipamentelor din infrastructurile critice energetice Optimizarea şi simularea comutării echipamentelor electrice de putere incluse în sistemele automate de distribuţie şi transport a energiei electrice
Competenţe	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a

transversale	abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Dobândirea cunoştinţelor teoretice şi practice necesare în domeniul echipamentelor electrice şi protocoalelor de comunicare specifice pentru infrastructura utilizată în energetică prin orele de curs şi laborator Asimilarea unor cunoştinţe la nivel operaţional cu privire la funcţionarea şi configurarea sistemelor de tip SCADA

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
Capitolul 1. Interfeţe de comunicare pentru echipamente industriale protocoale industriale (Ethernet, RS232, RS485, Bluetooth)	4	Prezentare cu ajutorul videoproiectorului, Expunere şi demonstraţii pe tablă	
Capitolul 2. Tipuri de protocoale utilizate pentru echipamentele electrice în procesele industriale (MODBUS, PROFIBUS, DEVICENET, CUBIBUS)	4	Prezentare cu ajutorul videoproiectorului, Expunere şi demonstraţii pe tablă	
Capitolul 3. Softuri dedicate pentru control şi comandă la distanţă (SCADA, EkipView, SD-View 2000, etc.)	6	Prezentare cu ajutorul videoproiectorului, Expunere şi demonstraţii pe tablă	
Capitolul 4. Configurarea unităţilor de tip Electronic Trigger Unit prevăzute cu interfeţe de proces	4	Prezentare cu ajutorul videoproiectorului, Expunere şi demonstraţii pe tablă	
Capitolul 5. Echipamente capabile de a fi integrate în sisteme de comanda şi monitorizare la distanţă (întrerupătoare, separatoare, contactoare, ruptoare, sisteme de plottere pentru reglarea tensiunii (auto)transformatoarelor, relee)	10	Prezentare cu ajutorul videoproiectorului, Expunere şi demonstraţii pe tablă	

Bibliografie

1. Hortopan G., *Aparate electrice*, Editura Didactica si Pedagogica, Bucuresti, 1980. (1996)
2. Asandei D., *Protecţia sistemelor electrice*, Bucureşti, Matrix Rom, 1999
3. Cataloage Schrack
4. Datasheet ABB, Moeller, Omron
5. Hnatiuc B., Note de curs (format ppt)

Aplicaţii (laborator)	Nr. ore	Metode de predare	Observaţii
Laborator 1: Introducere. Simboluri ale echipamentelor electrice în schemele utilizate de softurile de comandă şi monitorizare la distanţă a infrastructurii critice în energetică	2	Standuri cu montaje practice, tablă, videoproiector	
Laborator 2 : Studiul funcţionării întrerupătoarelor automate din familiile NZM7 şi MZ1	2	Standuri cu montaje practice, tablă, videoproiector	
Laborator 3: Studiul interfeţelor şi protocoalelor de transmitere a datelor la distanţă	2	Standuri cu montaje practice, tablă, videoproiector	
Laborator 4: Relee. Circuite pentru controlul, comanda şi protecţia motoarelor trifazate	2	Standuri cu montaje practice, tablă, videoproiector	
Laborator 5 : Programarea şi funcţionarea releelor numerice inteligente Zelio Logic SR2A101FU şi	2	Standuri cu montaje practice, tablă, videoproiector	
Laborator 6 : Logică programabilă cu relee pentru driver NVBDL_CNC	2	Standuri cu montaje practice, tablă, videoproiector	
Laborator 7: Studiul declanşatorului electronic SACE PR332/P	2	Standuri cu montaje practice, tablă, videoproiector	

Bibliografie

Hnatiuc B., Aparate electrice – Indrumar de aplicaţii, Editura Nautica, 2016, ISBN 978-606-681-077-7

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

- Pregătirea în cadrul disciplinei permite integrarea absolvenților în orice societate care se ocupă de monitorizarea și comanda la distanță a echipamentelor incluse în infrastructura critică din domeniul energetic. Profilul unor astfel de firme se regăsește în cele de producere a energiei electrice din surse neconvenționale (eoliene, celule fotovoltaice), convenționale (centrale hidroelecrice, atomoelectrice, termoelectrice), a celor care se ocupă cu sistemul energetic național și a celor care supraveghează integritatea sistemelor critice.
- Conţinutul este orientat către aspectele practice ale sistemelor de monitorizare și comandă la distanță a echipamentelor electrice de putere, cu însușirea celor mai noi tehnici care sunt aplicate în întreaga lume.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Examen	Probă scrisă	70%
Seminar			
Laborator	Referate individuale	Evaluare continuă	30%
Proiect			
Standard minim de performanţă			
• **Obținerea a 5 puncte din 10 posibile (Nota minimă: 5)**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	Prof.univ.dr.ing. Hnatiuc Bogdan	Prof.univ.dr.ing. Hnatiuc Bogdan

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Practică I				
Titularul activităţilor de curs					
Titularul activităţilor de seminar					
Anul de studiu	1	Semestrul	1	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	6	Curs	-	Seminar	-	Laborator	-	Proiect	6
I b) Totalul de ore pe semestru din planul de învăţământ	84	Curs	-	Seminar	-	Laborator	-	Proiect	84

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	
II d) Tutoriat	
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	
Total ore pe semestru (Ib+II+III+IV)	86
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	Cunoştinţe de bază în domeniul ştiinţelor inginereşti
Competenţe	Utilizarea adecvată a cunoştinţelor tehnice în propunere de soluţii

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Utilizarea principiilor generale de securitate şi aplicarea regulilor de securitate la nivelul componentelor sistemului informatic. Dobândirea unui spirit atitudinal-afectiv pozitiv faţă de amploarea şi complexitatea prospectiv-ştiinţifică oferită de domeniul securităţii cibernetice.
Competenţe transversale	Întărirea capacităţilor de lucru în colectiv, comunicare cu alte colective tehnice în vederea analizării şi identificării soluţiilor constructive.

	Dezvoltarea unui mod de comunicare clar şi concis în cadrul prezentării propriilor poziţii. Adaptarea la situaţii noi de lucru. Adaptarea la un colectiv nou.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Corelarea şi aplicarea cunoştinţelor teoretice în activitatea practică specifica masterului.
	Cunoaşterea instituţiei şi activităţii unde se desfăşoară stagiul de practică. Cunoaşterea şi aprofundarea elementelor practice specific soluţionării documentaţiei tehnice. Aprofundarea cunoştinţelor dobândite prin activităţi practice.

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
Bibliografie			

Conţinut programa de practică	Nr. ore	Metode de predare	Observaţii
Se vor urmă cu predilecţie următoarele aspecte specifice : Cunoaşte principiile generale de securitate şi aplicarea regulilor de securitate la nivelul componentelor sistemului informatic. Cunoaşterea planificării şi organizării activităţilor de Securitate în cadrul unei organizaţii. Identificarea principiilor generale de securitate şi aplicarea regulilor de securitate la nivelul componentelor sistemului informatics. Înţelege modul de planificare şi organizare a activităţilor de Securitate cibernetică într-o societate comercială. Să poată să elaboreze şi să implementeze planul de comunicare (alertare) şi de răspuns la apariţia (sau numai la suspiciunea) unui incident de securitate	84	Studierea documentaţiei tehnice puse la dispoziţie de către firma unde se face stagiul de practică.	
Bibliografie			

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

- Disciplina oferă studenţilor posibilitatea de a pune în practică în interiorul unei instituţii de pe piaţa muncii cunoştinţele şi competenţele dobândite specific programului masteral.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Practică	Evaluare finală (proiect + apreciere unitate de practică) întrebări şi răspunsuri în faţa comisiei	Prezentarea portofoliului elaborat ca urmare a efectuării stagiului de practică	100%
Standard minim de performanţă			

- **Nota 5**
  Pentru a obţine nota minimă de promovare studentul trebuie să prezinte următoarele documente :
  - Convenţia de practică parafată de compania unde a efectuat stagiul de practică şi
  - Caietul de practică

  Nota propusă de tutorele de practică trebuie să fie de minim 5, iar studentul trebuie să demonstreze în cadrul colocviului cunoştinţe minimale despre aspectele specifice securităţii cibernetice.
- **Nota 10**

Nota maximă poate fi obţinută în condiţiile în care studentul dovedeşte la colocviu, cunoştinţe solide, documentate, argumentate şi de detaliu, are un caiet de practică complet şi tutorele de practică a apreciat activitatea pe durata stagiului de practică drept Foarte Bună.

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018		

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Sisteme de conducere a proceselor industriale şi protecţie cibernetică (SCADA, PLC, DPC)				
Titularul activităţilor de curs	Conf.univ.dr.ing. Sintea Sorin				
Titularul activităţilor de seminar	Conf.univ.dr.ing. Sintea Sorin				
Anul de studiu	1	Semestrul	2	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	5	Curs	2	Seminar	-	Laborator	2	Proiect	1
I b) Totalul de ore pe semestru din planul de învăţământ	70	Curs	28	Seminar	-	Laborator	28	Proiect	14

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	26
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	20
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	10
II d) Tutoriat	8
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	64
Total ore pe semestru (Ib+II+III+IV)	136
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	• Automate programabile.
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Capacitatea de a aplica cunoştinţele privind configurarea, monitorizarea şi comanda la distanţă a echipamentelor din infrastructurile critice energetice Optimizarea şi simularea comutării echipamentelor electrice de putere incluse în sistemele automate de distribuţie şi transport a energiei electrice
Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea

	personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Dobândirea cunoştinţelor teoretice şi practice necesare în domeniul echipamentelor electrice şi protocoalelor de comunicare specifice pentru infrastructura utilizată în energetică prin orele de curs şi laborator Asimilarea unor cunoştinţe la nivel operaţional cu privire la funcţionarea şi configurarea sistemelor de tip SCADA

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
1. Introducere. Era industriala si dezvoltarea ei in spatiul cibernetic. Transferul de tehnologie din aria industriala in spatiul cibernetic.	2	Prelegere orală	
2. Sisteme de control industrial. Arhitecturi actuale de control industrial (SCADA, DCS). Unitatea arhitectonica de control a echipamentelor industriale (sisteme dedicate si AP-uri).	4	Prelegere orală	
3. Spatiul cibernetic. Suport pentru accesarea tehnologiilor industriale din spatiul cibernetic.	2	Prelegere orală	
4. Transferul sistemelor si tehnologiilor industriale in spatiul cibernetic. Utilizarea platformelor IoT si Industry IV pentru dezvoltarea de sisteme de control industrial. Convergenta tehnologiilor de control utilizand sisteme arhitectonice de management a datelor (BigData).	4	Prelegere orală	
5. Retele industriale conectate la spatiul cibernetic. Asigurarea securitatii retelei industriale la conectarea la spatiul cibernetic.	4	Prelegere orală	
6. Structura arhitectonica a unui automat programabil. Dezvoltarea acestuia pentru a putea fi integrat in spatiul cibernetic. Tehnologii de protectie a informatiei si de securitate a retelelor cu automate programabile.	6	Prelegere orală	
7. Magistrale logice de comunicatii din spatiul real in spatiul virtual. Gateway-uri de date pentru interfata cu spatiul cibernetic. Asigurarea securitatii gateway-urilor de date.	2	Prelegere orală	
8. Conectarea de controlere dedicate la spatiul cibernetic. Controllere dedicate conectate in spatiul cibernetic. Asigurarea securitatii controlerelor dedicate conectate in spatiul cibernetic.	2	Prelegere orală	
9. Servere de date de tip OPC conectate in spatiul cibernetic. Securizarea serverelor de tip OPC.	2	Prelegere orală	

Bibliografie

1. GSMA. Understanding the Internet of Things (IoT). July 2014. https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf
2. Dave Evans. CISCO. The Internet of Things. How the Next Evolution of the Internet Is Changing Everything. April 2011. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
3. Sintea Sorin. "Automate programabile industriale". Editura Nautica. Constanta. 2018
4. Henry Hui, Kieran McLaughlin, "Investigating Current PLC Security Issues Regarding Siemens S7 Communications and TIA Portal", https://ewic.bcs.org/upload/pdf/ewic_icscsr18_paper8.pdf, Jan. 2019

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

- Conţinutul este orientat către aspecte practice ale tehnologiilor de lucru cu echipamente industriale, în concordanţă cu cele mai noi tehnici care sunt aplicate în întreaga lume.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Examen	Examen scris	70%

Seminar			
Laborator	Referate individuale	Evaluare continuă	15%
Proiect		Nota Proiect	15%
Standard minim de performanţă			
• Nota 5			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
17.10.2018	Conf.univ.dr.ing. Sintea Sorin	Conf.univ.dr.ing. Sintea Sorin

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Cultura organizațională de securitate				
Titularul activităţilor de curs	Dr.ing. Vasile Drăghici				
Titularul activităţilor de seminar	Dr.ing. Vasile Drăghici				
Anul de studiu	1	Semestrul	2	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DC
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	2	Curs	2	Seminar	2	Laborator	-	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	28	Laborator	-	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	10
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	8
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	7
II d) Tutoriat	5
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	30
Total ore pe semestru (Ib+II+III+IV)	88
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	- Cunoaştere şi înţelegerea conceptelor de cultură de securitate, securitate organizaţională, politici de securitate, ameninţări de securitate, incidente de securitate ş.a.; - Înţelegerea principalelor direcţii de abordare a culturii de securitate ca fundament al securităţii organizaţionale şi adaptarea elementelor culturale la schimbările de paradigmă; - Cunoaşterea, înţelegerea şi implementarea reglementărilor legale care vizează securitatea organizaţiei; - Aplicarea unor metode moderne de evaluare a măsurilor de securitate şi a răspunsului adecvat al

	organizației la amenințările de securitate; - Stabilirea politicilor de securitate ale organizației și dimensionarea sistemului de securitate pe baza analizei riscurilor; - Cunoașterea și utilizarea transdiciplinară a unor principii și mecanisme pentru prevenirea sau soluționarea incidentelor de securitate; - Stăpânirea problematicii securității organizației și determinarea conținutului și formelor de educație pentru consolidarea culturii de securitate organizațională;
Competențe transversale	- Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităților lingvistice, a cunoștințelor de tehnologia informației și a comunicării pentru dezvoltarea personală si profesională, în scopul inserției pe piața muncii și al adaptării la dinamica cerințelor acesteia. - Utilizarea eficientă a resurselor și tehnicilor de învățare, în scopul dezvoltării personale și profesionale continue în domeniul telecomunicațiilor și tehnologiei informaționale, operarea cu informații și tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. - Planificarea, organizarea, conducerea în cadrul unei echipe și demonstrarea abilităților de comunicare.

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

7.1. Obiectivul general al disciplinei	Formarea unei viziuni cuprinzătoare privind cultura organizatională de securitate, înțelegerea rolurilor și cunoașterea actorilor implicați în asigurarea securității organizației, dezvoltarea deprinderilor necesare pentru elaborarea politicilor de securitate și implementarea unui sistem integrat de securitate organizațional
7.2. Obiective specifice	- Înțelegerea și interpretarea evoluției conceptului de cultură de securitate organizațională, dezvoltarea capacității de analiză critică, sinteză și predicție a dimensiunilor securității organizației; - Dezvoltarea abilităților în utilizarea metodelor de evaluare a măsurilor de securitate și analiză a riscurilor; - Formarea și dezvoltarea atitudinii pozitive, responsabile, față de pregătirea continuă, cunoașterea și identificarea tendințelor actuale de evoluție a mediului de securitate organizațional;

8. **Conținuturi**

Curs	Nr. ore	Metode de predare	Observații
1. Cultura de securitate in limitele culturii organizației	2	Prelegere, prezentare ppt.	
2. Evoluții ale mediilor de securitate organizațională în spațiul european și euro-atlantic	2	Prelegere, prezentare ppt.	
3. Fundamentele securității organizaționale	2	Prelegere, prezentare ppt.	
4. Abordări sistemice și holistice ale securității organizaționale	2	Prelegere, prezentare ppt.	
5. Modele culturale specifice și politici de securitate organizațională	2	Prelegere, prezentare ppt.	
6. Organizarea securității organizației. Valori, actori și principii generale	2	Prelegere, prezentare ppt.	
7. Securitatea personalului. Selectarea, verificarea și pregătirea	2	Prelegere, prezentare ppt.	
8. Securitatea fizică. Sisteme de securitate integrate	2	Prelegere, prezentare ppt.	
9. Securitatea informațiilor și suporturilor fizice	2	Prelegere, prezentare ppt.	
10. Securitatea sistemelor informatice și de comunicații pentru informații sensibile	2	Prelegere, prezentare ppt.	
11. Securitatea industrială. Protecția activităților contractuale	2	Prelegere, prezentare ppt.	
12. Costurile implementării și eficiența măsurilor de securitate	2	Prelegere, prezentare ppt.	
13. Amenințările și vulnerabilitățile organizației. Analiza riscurilor de securitate.	2	Prelegere, prezentare ppt.	
14. Educația de securitate. Prevenirea și tratarea incidentelor de securitate	2	Prelegere, prezentare ppt.	

Bibliografie

- Drăghici V., Iliescu C., *Sisteme de protecţie a informaţiilor clasificate în spaţiul euro-atlantic – actori, principii, evoluţii,* Editura Academiei Tehnice Militare, Bucureşti, 2013
- Patterson D., Fay J., *Contemporary Security Management, 4th Edition,* Butterworth-Heinemann, Oxford, 2017.
- Kaldor M., *Securitatea umană: reflexii asupra globalizării şi intervenţiei*, Editura CA Publishing, Cluj Napoca, 2010;
- Gariup M., *European Security Culture: Language, Theory, Policy*, Ashgate, 2009.
- Hutter B.M., Power M. - *Organizational Encounters With Risk*, Cambridge University Press, Cambridge, 2005.
- Banisar D, *Freedom of information around the world*, Privacy International, London, 2006.
- Tipton H.F., Krause M., *Information Security Management Handbook*, Taylor & Francis Routledge, Londra, 2005.
- * * * C-M(2002)49 - *Security within the North Atlantic Treaty Organisation (NATO)*, Corrigendum 9 dated 5 February 2013, Public Disclosure - PDN(2010)0003-ADD1 dated 6 July 2010.
- * * * *Council Guide, Internal document, III. Delegates' Handbook*, General Secretariat of the Council, September 2000
- * * * *Instruction générale interministérielle sur la protection du secret de la défense nationale N°1300 /SGDSN/PSE/PSD*, Paris, 23.07.2010
- * * * *The Cabinet Manual - A guide to laws, conventions and rules on the operation of government*, UKCabinet Office, October 2011

Aplicaţii (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observaţii
1. Securitatatea organizaţiilor mari. Politici de securitate în cadrul UE şi NATO	4	Studiu de caz, dezbatere, conversaţie, prezentări ppt	
2. Politici nationale de securitate în spaţiul European	4	Studiu de caz, dezbatere, conversaţie, prezentări ppt	
3. Repere legislative în reglementarea unor standarde minime de securitate	4	Studiu de caz, dezbatere, conversaţie, prezentări ppt	
4. Confidenţialitatea, integritatea şi disponibilitatea informaţiilor	4	Studiu de caz, dezbatere, conversaţie, prezentări ppt	
5. Abordarea proactivă a securităţii organizaţiei. Managementul măsurilor de securitate	4	Studiu de caz, dezbatere, conversaţie, prezentări ppt	
6. Metode de evaluare a măsurilor de securitate	4	Studiu de caz, dezbatere, conversaţie, prezentări ppt	
7. Incidente de securitate	4	Studiu de caz, dezbatere, conversaţie, prezentări ppt	

Bibliografie

- Drăghici V., Iliescu C., *Sisteme de protecţie a informaţiilor clasificate în spaţiul euro-atlantic – actori, principii, evoluţii,* Editura Academiei Tehnice Militare, Bucureşti, 2013
- Patterson D., Fay J., *Contemporary Security Management, 4th Edition,* Butterworth-Heinemann, Oxford, 2017.
- Kaldor M., *Securitatea umană: reflexii asupra globalizării şi intervenţiei*, Editura CA Publishing, Cluj Napoca, 2010;
- Gariup M., *European Security Culture: Language, Theory, Policy*, Ashgate, 2009.
- Hutter B.M., Power M. - *Organizational Encounters With Risk*, Cambridge University Press, Cambridge, 2005.
- Banisar D, *Freedom of information around the world*, Privacy International, London, 2006.
- Tipton H.F., Krause M., *Information Security Management Handbook*, Taylor & Francis Routledge, Londra, 2005.
- * * * C-M(2002)49 - *Security within the North Atlantic Treaty Organisation (NATO)*, Corrigendum 9 dated 5 February 2013, Public Disclosure - PDN(2010)0003-ADD1 dated 6 July 2010.
- * * * *Council Guide, Internal document, III. Delegates' Handbook*, General Secretariat of the Council, September 2000

- * * * *Instruction générale interministérielle sur la protection du secret de la défense nationale N°1300 /SGDSN/PSE/PSD*, Paris, 23.07.2010
- * * * *The Cabinet Manual - A guide to laws, conventions and rules on the operation of government*, UKCabinet Office, October 2011

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

- Disciplina a fost elaborată în concordanţă cu lucrările din domeniu, publicate în ţară şi străinatate;
- Unele teme din cadrul cursului cuprind aspecte relevante, ce fac obiectul preocuparilor instituţiilor de profil sau al unor conferinte stiintifice naţionale şi internaţionale, inclusiv dezbateri în cadrul revistelor de specialitate la nivel naţional şi internaţional.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	- Cunoașterea conceptelor şi a metodelor de evaluare; - Calitatea argumentării; - Capacitatea de analiză critică şi sinteză; - Acuratețea limbajului;	Examen oral	60%
Seminar	- Capacitarea de înțelegere a tematicii şi bibliografiei cursului; - Abilitățile de comunicare; - Capacitatea de argumentare	Evaluare continuă	40%
Laborator			
Proiect			
Standard minim de performanță			
- Nota 5 (cinci) ; - Prezența la 75% din seminarii (5 din 7); - Utilizarea adecvată a aparatului critic şi bibliografic conform normelor academice impuse la prima întâlnire a masteratului;			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
23.10.2018	Dr.ing. Vasile Drăghici	Dr.ing. Vasile Drăghici

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Securitatea cibernetică a dispozitivelor mobile şi riscurile asociate IoT				
Titularul activităţilor de curs	Conf.univ.dr.ing. Gabriel Raicu				
Titularul activităţilor de seminar	Conf.univ.dr.ing. Gabriel Raicu				
Anul de studiu	1	Semestrul	2	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	-	Laborator	2	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	-	Laborator	28	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	29
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	15
II d) Tutoriat	10
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	64
Total ore pe semestru (Ib+II+III+IV)	122
Numărul de credite	6

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Realizarea si operarea arhitecturilor IoT la scara extinsa Lucrul in medii eterogene cin punct de vere al arhitecturilor de calcul Configurari avansate ale retelelor IoT Intelegerea conceptelor de proiectare sigura a retelelor care intereaza IoT
Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea

	personală si profesională, în scopul inserției pe piața muncii și al adaptării la dinamica cerințelor acesteia. Utilizarea eficientă a resurselor și tehnicilor de învățare, în scopul dezvoltării personale și profesionale continue în domeniul telecomunicațiilor și tehnologiei informaționale, operarea cu informații și tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe și demonstrarea abilităților de comunicare.

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

Obiectivul general al disciplinei	Crearea competentelor necesare pentru intelegerea, operarea si proiectarea retelelor care includ IoT

8. Conținuturi

Curs	Nr. ore	Metode de predare	Observații
1. Principii de operare IoT. Platforme si arhitecturi	4	Prelegere orală	
2. Riscuri de securitate cibernetica asociate IoT	4	Prelegere orală	
3. Securitatea tehnicilor de programare	4	Prelegere orală	
4. Configurare si protectie pe termen lung pentru IoT	4	Prelegere orală	
5. Integrarea avansata a dispozitivelor IoT in sisteme la scara mare – vurnerabilitati distribuite	4	Prelegere orală	
6. Riscurile operarii platformelor eterogene	4	Prelegere orală	
7. Proiectarea IoT. Conceptul de"secure by design"	4	Prelegere orală	

Bibliografie

1. Arcos Sergio. "Social Engineering" (PDF). Archived (PDF) from the original on 3 December 2013.
2. Scannell, Kara (24 February 2016). "CEO email scam costs companies $2bn". Financial Times (25 Feb 2016). Archived from the original on 23 June 2016. Retrieved 7 May 2016.
3. "Bucks leak tax info of players, employees as result of email scam". Associated Press. 20 May 2016. Archived from the original on 20 May 2016. Retrieved 20 May 2016.
4. "What is Spoofing? – Definition from Techopedia". Archived from the original on 30 June 2016.
5. spoofing. Oxford Reference. Oxford University Press. 2016-01-21. doi:10.1093/acref/9780199688975.001.0001. ISBN 9780199688975. Retrieved 8 October 2017.
6. Marcel, Sébastien; Nixon, Mark; Li, Stan, eds. (2014). Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks (PDF). Advances in Computer Vision and Pattern Recognition. London: Springer. doi:10.1007/978-1-4471-6524-8. ISBN 978-1-4471-6524-8. ISSN 2191-6594. LCCN 2014942635. Retrieved 8 October 2017 – via Penn State University Libraries.

Aplicații (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observații
1. Arhitecturi IoT functionalitati comparate	2	problematizare, exercitiu	
2. Riscuri OS related versus riscuri arhitecturale	2	problematizare, exercitiu	
3. Configurarea IoT in retele locale	2	problematizare, exercitiu	
4. Configurarea IoT in retele extinse	2	problematizare, exercitiu	
5. Integrare multipltforma	2	problematizare, exercitiu	
6. Operare IoT in medii eterogene	2	problematizare, exercitiu	
7. Concepte de securizare in industria IoT		problematizare, exercitiu	

Bibliografie

1. Gallagher, Sean (14 May 2014). "Photos of an NSA "upgrade" factory show Cisco router getting implant". Ars Technica. Archived from the original on 4 August 2014. Retrieved 3 August 2014.
2. Lim, Joo S., et al. "Exploring the Relationship between Organizational Culture and Information Security Culture." Australian Information Security Management Conference.
3. K. Reimers, D. Andersson (2017) POST-SECONDARY EDUCATION NETWORK SECURITY: THE END USER CHALLENGE AND EVOLVING THREATS, ICERI2017 Proceedings, pp. 1787-1796.

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

- Conținutul este orientat către aspecte practice ale tehnologiilor de lucru sub apă, în concordanță cu cele mai noi tehnici care sunt aplicate în întreaga lume.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs		Examen scris	70%
Seminar		Evaluare continuă	30%
Laborator			
Proiect			
Standard minim de performanţă			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
17.10.2018.	Conf.univ.dr.ing. Gabriel Raicu	Conf.univ.dr.ing. Gabriel Raicu

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Siguranţa tehnicilor de programare şi securitatea aplicaţiilor şi sistemelor informatice					
Titularul activităţilor de curs	Ş.l.univ.dr.ing. Alexandru Pescaru					
Titularul activităţilor de seminar	Ş.l.univ.dr.ing. Alexandru Pescaru					
Anul de studiu	1	Semestrul	2	Tipul de evaluare	E	
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară					DA
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)					DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	-	Laborator	2	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	-	Laborator	28	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	29
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	15
II d) Tutoriat	10
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	64
Total ore pe semestru (Ib+II+III+IV)	122
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Folosirea cunoştinţelor multidisciplinare pentru integrarea tehnicilor de programare a aplicatiilor in sistemele informatice; Identificarea şi descrierea tehnicilor, metodelor, metodologiilor şi tehnologiilor necesare în programarea sistemelor informatice; Utilizarea de concepte, principii, tehnici, metodologii şi tehnologii de programare a aplicatiilor si sistemelor informatice; Stabilirea criteriilor relevante privind calitatea şi securitatea aplicatiilor si sistemelor informatice Utilizarea unor concepte şi metode noi pentru asigurarea securităţii, siguranţei şi uşurinţei în exploatare a sistemelor informatice integrate Realizarea de proiecte de cercetare- dezvoltare interdisciplinare cu respectarea standardelor de calitate, securitate şi siguranţă
Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Analiza principiilor, metodelor si tehnologiilor de securitate si siguranta a sistemelor informationale; studierea cailor de evaluare a nivelului securitatii si identificarea amenintarilor si vulnerabilitatii sistemelor informatice; promovarea noilor tehnologii de protectie a sistemelor de baze de date.

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
1. Notiuni introductive privind siguranţa tehnicilor de programare şi securitatea aplicaţiilor şi sistemelor informatice	2	Prelegere orală	
2. Clasificarea informatiilor si a tehnicilor de programare.	2	Prelegere orală	
3. Particularitati ale sistemelor informationale	4	Prelegere orală	
3.1. Vulnerabilitatea calculatoarelor			
3.2. Forme de manifestare a pericolelor in sistemele informationale aparute in sistem, din cauze naturale sau actiuni voite ale omului;			
3.3. Asigurarea securitatii sistemelor informatice si mecanisme de aparare.			
4. Protectia informatiilor prin clasificarea lor. Protejarea suporturilor informationale.	2	Prelegere orală	
5. Controlul accesului in sistemele informatice - tipuri de control; identificarea si autentificarea; control prin parole.	2	Prelegere orală	
6. Politici, standarde, norme si proceduri de securitate -	4	Prelegere orală	
6.1. Mecanisme utilizate in securizarea retelelor - firewall, proxy, filtre de pachete, retele VPN, PPTP, L2TP			
7. Criptografia	2	Prelegere orală	
8. Modele si programe de securitate.	2	Prelegere orală	
9. Siguranta si securitatea retelelor de calculatoare	2	Prelegere orală	
10. Strategii de securitate ale razboiului informational.	2	Prelegere orală	
11. Asigurarea sigurantei si securitatii sistemelor informationale publice si private	2	Prelegere orală	
11.1. Siguranta si securitatea locului de amplasare;			
11.2. Siguranta si securitatea echipamentelor;			
11.3. Siguranta si securitatea software-ului			
12. Aspecte juridice prind protectia, siguranta si securitatea sistemelor informatice.	2	Prelegere orală	
Bibliografie			

1. Anderson, R., *Security engineering: A guide to building dependable distributed systems*, NY, 2001
2. Andress, M., *Surviving security*, SAMS, 2001
3. Bishop,M., *Introduction to computer security*, Addison Wesly Professional, 2004.
4. Mihai, I. C., *Securitatea sistemului informatic*, Galati, 2007.
5. Mojzi, M., *Securitatea sistemelor de calcul si a retelelor de calculatoare*
6. Northcutt, S. and Novak, J., *Network intrusion detection*: An nalyst's Handbook, 2000
7. Oprea D., *Protectia si securitatea sistemului informational*, Iasi, 2009.
8. Pfleeger, Ch.P., Pfleeger,S.L., *Security in Computing*, Prentice Hall, 2002.
9. Popa, S.E., *Securitatea sistemelor informatice*, 2007.
10. Zwicky E., et. al. *Building Internet Firewalls*, 2nd. Edition, 2000.

Aplicaţii (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observaţii
1. Ascunderea unui fisier si descoperirea unui fisier ascuns	4	problematizare, exercitiu	
2. Asigurarea securitatii sistemelor informatice si mecanisme de aparare.	2	problematizare, exercitiu	
3. Controlul accesului in sistemele informatice - tipuri de control; identificarea si autentificarea; control prin parole	2	problematizare, exercitiu	
4. Modele si programe de securitate.	2	problematizare, exercitiu	
5. Firewall	4	problematizare, exercitiu	
6. Proxy server	2	problematizare, exercitiu	
7. Proxy server Squid pe sisteme de operare Linux	2	problematizare, exercitiu	
8. Open VPN (retea virtuala privata)	4	problematizare, exercitiu	
9. Strategii de securitate ale razboiului informational.	2	problematizare, exercitiu	
10.Criptografie	4	problematizare, exercitiu	
Bibliografie			

1. Anderson, R., *Security engineering: A guide to building dependable distributed systems*, NY, 2001
2. Andress, M., *Surviving security*, SAMS, 2001
3. Bishop,M., *Introduction to computer security*, Addison Wesly Professional, 2004.
4. Mihai, I. C., *Securitatea sistemului informatic*, Galati, 2007.
5. Mojzi, M., *Securitatea sistemelor de calcul si a retelelor de calculatoare*
6. Northcutt, S. and Novak, J., *Network intrusion detection*: An nalyst's Handbook, 2000
7. Oprea D., *Protectia si securitatea sistemului informational*, Iasi, 2009.
8. Pfleeger, Ch.P., Pfleeger,S.L., *Security in Computing*, Prentice Hall, 2002.
9. Popa, S.E., *Securitatea sistemelor informatice*, 2007.
10. Zwicky E., et. al. *Building Internet Firewalls*, 2nd. Edition, 2000.

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

- Conţinutul este orientat către aspecte practice ale tehnologiilor de lucru sub apă, în concordanţă cu cele mai noi tehnici care sunt aplicate în întreaga lume.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Abilitatea de rezolvare a unor probleme specifice domeniului. Participarea activa la orele de curs.	Examen scris	70%
Seminar			
Laborator	Abilitatea de rezolvare a unor probleme specifice domeniului. Participarea activa la orele de laborator	Evaluare continuă. Analiza si notarea rezultatelor lucrarilor de laborator si a aplicatiilor.	30%
Proiect			
Standard minim de performanţă - Rezolvarea corecta, in proportie de 70% asubiectelor de examen, a temelor si aplicatiilor date			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
23.10.2018	Ş.l.univ.dr.ing. Alexandru Pescaru	Ş.l.univ.dr.ing. Alexandru Pescaru

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Practică II				
Titularul activităţilor de curs					
Titularul activităţilor de seminar					
Anul de studiu	1	Semestrul	2	Tipul de evaluare	C

Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară	DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)	DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	8	Curs	-	Seminar	-	Laborator	-	Proiect	8
I b) Totalul de ore pe semestru din planul de învăţământ	112	Curs	-	Seminar	-	Laborator	-	Proiect	112

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	
II d) Tutoriat	
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	
Total ore pe semestru (Ib+II+III+IV)	114
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	Cunoştinţe de bază în domeniul ştiinţelor inginereşti
Competenţe	Utilizarea adecvată a cunoştinţelor tehnice în propunere de soluţii

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Utilizarea principiilor generale de securitate şi aplicarea regulilor de securitate la nivelul componentelor sistemului informatic. Dobândirea unui spirit atitudinal-afectiv pozitiv faţă de amploarea şi complexitatea prospectiv-ştiinţifică oferită de domeniul securităţii cibernetice.
Competenţe transversale	Întărirea capacităţilor de lucru în colectiv, comunicare cu alte colective tehnice în vederea analizării şi identificării soluţiilor constructive.

	Dezvoltarea unui mod de comunicare clar şi concis în cadrul prezentării proprilor poziţii. Adaptarea la situaţii noi de lucru. Adaptarea la un colectiv nou.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Corelarea şi aplicarea cunoştinţelor teoretice în activitatea practică specifica masterului.
	Cunoaşterea instituţiei şi activităţii unde se desfăşoară stagiul de practică. Cunoaşterea şi aprofundarea elementelor practice specific soluţionării documentaţiei tehnice. Aprofundarea cunoştinţelor dobândite prin activităţi practice.

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
Bibliografie			

Conţinut programa de practică	Nr. ore	Metode de predare	Observaţii
Se vor urmă cu predilecţie următoarele aspecte specifice : Cunoaştere şi înţelegerea conceptelor de cultură de securitate, securitate organizaţională, politici de securitate, ameninţări de securitate, incidente de securitate ş.a.; Înțelegerea principalelor direcții de abordare a culturii de securitate ca fundament al securității organizaționale și adaptarea elementelor culturale la schimbările de paradigmă; Folosirea cunoştinţelor multidisciplinare pentru integrarea tehnicilor de programare a aplicatiilor in sistemele informatice; Identificarea şi descrierea tehnicilor, metodelor, metodologiilor şi tehnologiilor necesare în programarea sistemelor informatice; Utilizarea de concepte, principii, tehnici, metodologii şi tehnologii de programare a aplicatiilor si sistemelor informatice; Managementului prin proiecte în domeniul securităţii cibernetice , respectând cerinţele impuse de principiile de certificare internă şi de omologare – auditare a sistemelor IT&C, de standarde specifice ISO 17799, standarde de evaluare şi omologare internă a securităţii echipamentelor şi sistemelor ISO 15408	112	Studierea documentaţiei tehnice puse la dispoziţie de către firma unde se face stagiul de practică.	
Bibliografie			

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

- Disciplina oferă studenţilor posibilitatea de a pune în practică în interiorul unei instituţii de pe piaţa muncii cunoştinţele şi competenţele dobândite specific programului masteral.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Practică	Evaluare finală (proiect + apreciere unitate de practică) întrebări şi răspunsuri în faţa comisiei	Prezentarea portofoliului elaborat ca urmare a efectuării stagiului de practică	100%
Standard minim de performanţă			
• **Nota 5** Pentru a obţine nota minimă de promovare studentul trebuie să prezinte următoarele documente : - Convenţia de practică parafată de compania unde a efectuat stagiul de practică şi			

- Caietul de practică

Nota propusă de tutorele de practică trebuie să fie de minim 5, iar studentul trebuie să demonstreze în cadrul colocviului cunoştinţe minimale despre aspectele specifice securităţii cibernetice.

- **Nota 10**

Nota maximă poate fi obţinută în condiţiile în care studentul dovedeşte la colocviu, cunoştinţe solide, documentate, argumentate şi de detaliu, are un caiet de practică complet şi tutorele de practică a apreciat activitatea pe durata stagiului de practică drept Foarte Bună.

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
23.10.2018		

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Sisteme Electronice de Navigaţie				
Titularul activităţilor de curs	S.L. univ.dr. ing. Ana SAVU				
Titularul activităţilor de seminar	S.L. univ.dr. ing. Ana SAVU				
Anul de studiu	1	Semestrul	1	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DOA

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	3	Curs	2	Seminar	-	Laborator	1	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	42	Curs	28	Seminar	-	Laborator	14	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	30
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	17
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	15
II d) Tutoriat	
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	62
Total ore pe semestru (Ib+II+III+IV)	106
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	Senzori, Traductoare şi Achiziţii de Date. Circuite Electronice
Competenţe	C.1 Aplicarea creativă a cunoştinţelor şi metodelor specifice domeniului ingineriei electronice

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• Nu este cazul
Desfăşurare aplicaţii	Seminar	• -
	Laborator	• Prezenţa obligatorie • Calculatoare cu licenţă Matlab • Sistem hibrid GPS/INS
	Proiect	• -

6. Competenţe specifice acumulate

Competenţe profesionale	**C1.2.** Identificarea şi descrierea funcţională a elementelor sistemelor electronice în contextul utilizarii in domeniul telecomunicaţiilor **C 1.5.** Dezvoltarea si implementarea unor abordari creative in formularea de solutii tipice si elementare de exploatare asociate instalatiilor specifice domeniului inginerie electronică **C3.1** Descrierea conceptelor fundamentale ce stau la baza metodologiilor de proiectare si realizare a sistemelor electronice de radionavigatie şi a sistemelor de comunicaţii prin fibre optice

Competenţe transversale	

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Disciplina studiază sisteme electronice de navigaţie, având în vedere caracterizarea, tehnologia, proiectarea, modelarea, simularea, măsurarea şi utilizarea acestora.
	Familiarizarea studenţilor cu principalele tipuri de sisteme electronice de navigaţie. Realizarea unor măsurători şi experimentări specifice acestor sisteme.

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
1. Navigaţia inerţială 1.1 Aplicaţii ale sistemelor de navigaţie inerţială 1.1 Sisteme inerţiale în navigaţia maritimă 1.3 Senzori utilizaţi în navigaţia inerţială	6	Predarea (definiţii, demonstraţii, proprietăţi) principalelor noţiuni teoretice este efectuată folosind metoda clasică (la tablă). Pentru înlesnirea înţelegerii fenomenelor fizice, anumite proprietăţi/caracteristici sunt prezentate folosind videoproiectorul, acoperind astfel funcţia de comunicare demonstrativă. .	
2. Unitatea de măsurări inerţiale (IMU) 2.1 Schemă bloc 2.2 Descriere şi funcţionare	2		
3. Sistemul referenţial de atitudine şi direcţie (AHRS) 3.1 Schemă bloc 3.2 Descriere şi funcţionare	2		
4 Sistemul de poziţionare dinamică (DPS) 4.1 Schemă bloc 4.2 Descriere şi funcţionare	2		
5. Sistemul de navigaţie inerţială (INS) 5.1 Schemă bloc 5.2 Descriere şi funcţionare 5.3 Grade de precizie pentru diferitele tipuri de INS. 5.4 Erori în estimarea poziţiei 5.5 Senzori inerţiali pe 3,6 şi 9 axe 5.6 Platforme de achiziţie şi prelucrare a datelor pentru navigaţia inerţială 5.7 Descumpunerea informaţiei provenite de la un sistem de navigaţie inerţială utilizând metoda momentelor	8		
6. Radionavigaţia 6.1 Determinarea poziţiei cu ajutorul undelor radio si a unor dispozitive electronice specifice 6.2 Sisteme de radionavigaţie costieră 6.3 Sisteme de radionavigaţie aeriană 6.1 Sistemul global de poziţionare prin sateliţi (GPS)	8		

Bibliografie

1. Teză de doctorat "Utilizarea microsenzorilor în sistemele de navigaţie inerţială" A. Dumitraşcu
2. J. Farrell and M. Barth, *The Global Positioning System and Inertial Navigation. McGraw-Hill*, 1999.
3. D.H. Titertton, J.L.Weston, *Strapdown Inertial Navigation Technology*, MPG Books Ltd, 2004.
4. S. Y.Yurish, M. Teresa S.R. Gomes, *Smart Sensors and MEMS*, Proceedings of the NATO Advanced Study Institute on Smart Sensors and MEMS Povoa de Varzim, Portugal, 2003.
5. C. T. Leondes, *MEMS/NEMS, Handbook Techniques and Applications*, Springer 2006.

Bibliografie minimală

1. Teză de doctorat "Utilizarea microsenzorilor în sistemele de navigaţie inerţială" A. Dumitraşcu
2. J. Farrell and M. Barth, *The Global Positioning System and Inertial Navigation. McGraw-Hill*, 1999.

3. D.H. Titertton, J.L.Weston, *Strapdown Inertial Navigation Technology*, MPG Books Ltd, 2004.
•

Aplicaţii (Laborator)	Nr. ore	Metode de predare	Observaţii
Senzori pentru navigaţia inerţială	2	metoda de comunicare orală utilizată este metoda problematizării,utilizate frontal. Studenţii testează şi evaluează independent aceleaşi probleme prin utilizarea continuă a platformelor de laborator. Materialele didactice sunt reprezentate, în principal, de îndrumarul de laborator în variantă tipărită şi electronică (pe campusul virtual).	
Achiziţia şi prelucrarea datelor în navigaţia inerţială	2		
Descumpunerea informaţiei provenite de la un sistem de navigaţie inerţială utilizând metoda momentelor	2		
Erori în estimarea poziţiei	2		
Sisteme de navigaţie prin satelit	2		
Sisteme de navigaţie costieră şi aeriană	2		
Verificare de laborator	2		

Bibliografie

1. Teză de doctorat "Utilizarea microsenzorilor în sistemele de navigaţie inerţială" A. Dumitraşcu
2. J. Farrell and M. Barth, *The Global Positioning System and Inertial Navigation. McGraw-Hill*, 1999.
3. D.H. Titertton, J.L.Weston, *Strapdown Inertial Navigation Technology*, MPG Books Ltd, 2004.
4. S. Y.Yurish, M. Teresa S.R. Gomes, *Smart Sensors and MEMS*, Proceedings of the NATO Advanced Study Institute on Smart Sensors and MEMS Povoa de Varzim, Portugal, 2003.
5. C. T. Leondes, *MEMS/NEMS, Handbook Techniques and Applications*, Springer 2006.
1.

Bibliografie minimală

1. Teză de doctorat "Utilizarea microsenzorilor în sistemele de navigaţie inerţială" A. Dumitraşcu
2. J. Farrell and M. Barth, *The Global Positioning System and Inertial Navigation. McGraw-Hill*, 1999.
3. D.H. Titertton, J.L.Weston, *Strapdown Inertial Navigation Technology*, MPG Books Ltd, 2004.

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

- Performanţele sistemelor de navigaţie au fost îmbunătăţite în permanenţă. Se poate afirma că precizia şi stabilitatea acestora a crescut în ultimii 10 de ani de aproape 10 de ori. Miniaturizarea şi creşterea frecvenţelor de lucru a circuitelor electronice a impus crearea şi dezvoltarea de noi configuraţii de sisteme, crescând interesul pentru acestea, atât pentru firmele de specialitate, dar şi pentru institute de cercetare şi universităţile tehnice. Obiectivul cursului este însuşirea de către viitorii ingineri a sistemelor de navigaţie inerţială dar şi a sistemelor integrate (INS/GPS). Cursul are un puternic caracter aplicativ având în vedere caracterizarea, proiectarea, modelarea, simularea, măsurarea şi utilizarea acestor sisteme în concordanţă cu tehnologiile moderne ce stau la baza realizării produselor electronice din domeniu.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	- Cunoaşterea noţiunilor teoretice fundamentale - Cunoaşterea modului de aplicare a teoriei la probleme specifice - Analiza critică şi comparativă a tehnicilor şi modelelor teoretice	Examen programat în sesiune. Subiectele acoperă în totalitate programa analitică a disciplinei, realizând o sinteză între parcurgerea teoretică comparativă a cursului şi explicitarea prin exerciţii a	**50%**

		modelelor de aplicaţie.	
Seminar			
Laborator		Colocviu final de laborator, cuprinzând o componentă teoretică şi o componentă practică. Componenta teoretică constă în răspunsul dat de fiecare student la un set distinct de întrebări; componenta practică constă în determinarea unor parametrii fundamentali ai componentelor.	**50%**
Proiect			
Standard minim de performanţă			
• Înțelegerea principiilor care stau la baza funcționării sistemelor de navigație inerțială • Posibilitatea evaluării performanţelor tehnice ale sistemelor de navigație inerțială			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	S.L. univ. dr. ing. Ana SAVU	S.L.univ. dr. ing. Ana SAVU

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Ion Omocea

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Analiza şi clasificarea riscurilor de securitate cibernetică în tehnologiile informaţionale				
Titularul activităţilor de curs	Conf.univ.dr.ing. Sintea Sorin				
Titularul activităţilor de seminar	Conf.univ.dr.ing. Sintea Sorin				
Anul de studiu	I	Semestrul	I	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DA
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DOA

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	-	Laborator	1	Proiect	1
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	-	Laborator	14	Proiect	14

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	26
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	20
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	10
II d) Tutoriat	8
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	64
Total ore pe semestru (Ib+II+III+IV)	122
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	• Să cunoască termenii de specialitate şi să înţeleagă conceptele privind managementul ameninţărilor informatice în contextul securităţii cibernetice, performanţele de calificare a unui angajat pentru relaţionarea corectă în spaţiul virtual şi social-media; • Să cunoască şi să interpreteze strategii şi tehnici specifice ameninţărilor informatice; • Să caracterizeze teoriile managementului ameninţărilor informatice în contextul securităţii cibernetice;

	• Să aplice principiile managementului ameninţărilor informatice în contextul securităţii cibernetice pentru analiza organizaţiei • Să înţeleagă specificul procesului de management al ameninţărilor informatice în contextul securităţii cibernetice în cadrul organizaţiei în care activează • Să cunoască funcţiile procesului de securitate cibernetică şi să stabilească diferenţieri între tipurile de riscuri în vederea aplicării acestora în managementul managementului ameninţărilor informatice
Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Cunoaşterea şi înţelegerea problematicii managementului ameninţărilor informatice în contextul securităţii cibernetice în administraţia publică / mediul antreprenorial / societăţi capital privat, a practicilor specifice în organizaţii, a procedurilor şi mecanismelor de management a ameninţărilor informatice pentru realizarea securităţii cibernetice cu alte entităţi specifice organizaţiei din care face parte, compararea structurii şi funcţionalităţii compartimentelor de profil, elaborarea unei strategii de securitate cibernetică şi management a ameninţărilor informatice

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
1. Introducere. Dezvoltarea sistemelor informatice. Deschiderea si dezvoltarea continua a spatiului cibernetic. Necesitatea analizei riscurilor in sistemele cibernetice.	2	Prelegere orală	
2. Natura incidentelor care afecteaza spatiul cibernetic.	4	Prelegere orală	
3. Cauzele principale ce afecteaza spatiul cibernetic.	4	Prelegere orală	
4. Severitatea atacurilor din spatiul cibernetic	2	Prelegere orală	
5. Impactul atacurilor din spatiul cibernetic	2	Prelegere orală	
6. Impactul atacurilor din spatiul ciberntic in diverse sectoare de activitate	6	Prelegere orală	
7. Nivelul de impact al atacurilor din spatiul cibernetic	4	Prelegere orală	
8. Perspectiva, prognoza cu privire la impactul atacului cibernetic asupra societatii si economiei	2	Prelegere orală	
9. Impactul atacului cibernetic in societatea moderna asupra securitatii nationale si a componentelor socio-economice	2	Prelegere orală	

Bibliografie

1. NIS Cooperation Group - Cybersecurity Incident Taxonomy - July 2018
2. col.drd. Cătălin-Iulian BALOG – "RISCURI DE SECURITATE ÎN SPAŢIUL CIBERNETIC" - Buletinul Universităţii Naţionale de Apărare „Carol I", sept 2014
3. G.C. Kessler, J.P. Craiger, J.C. Haass – "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System" – TransNav, Vol 12, Nr 3, Sept 2018
4. James J. Cebula, Lisa R. Young – "A Taxonomy of Operational Cyber Security Risks" – Software Engineering Institute, TECHNICAL NOTE CMU/SEI-2010-TN-028, Dec. 2010

Aplicaţii (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observaţii
1. Introducere. Prezentare laborator.	2	problematizare, exercitiu	
2. Pierderea accesului la spatiul cibernetic datorat unor evenimente provocate de statii locale	2	problematizare, exercitiu	
3. Pierderea accesului la spatiul cibernetic datorat unor evenimente provocate de caderea infrastructurii	2	problematizare, exercitiu	
4. Pierderea accesului la spatiul cibernetic datorat unor evenimente provocate de caderea zonei de protectie la accesul in spatiul informatic	2	problematizare, exercitiu	
5. Limitarea accesului la spatiul cibernetic datorat unor	2	problematizare, exercitiu	

atacurilor din spatiul cibernetic			
6. Pierderea accesului la spatiul cibernetic datorat unor atacurilor din spatiul cibernetic	2	problematizare, exercitiu	
7. Evaluare laborator	2	problematizare, exercitiu	

Bibliografie

1. NIS Cooperation Group - Cybersecurity Incident Taxonomy - July 2018
2. col.drd. Cătălin-Iulian BALOG – "RISCURI DE SECURITATE ÎN SPAȚIUL CIBERNETIC" - Buletinul Universității Naționale de Apărare „Carol I", sept 2014
3. G.C. Kessler, J.P. Craiger, J.C. Haass – "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System" – TransNav, Vol 12, Nr 3, Sept 2018
4. James J. Cebula, Lisa R. Young – "A Taxonomy of Operational Cyber Security Risks" – Software Engineering Institute, TECHNICAL NOTE CMU/SEI-2010-TN-028, Dec. 2010

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

- Conținutul este orientat către aspecte practice ale tehnologiilor de lucru in domeniul informatic, în concordanță cu cele mai noi tehnici care sunt aplicate în întreaga lume.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Să cunoască termenii de specialitate și să înțeleagă conceptele de bază în ceea ce privește contextul securității cibernetice și interacțiunilor individului în spațiul virtual; Să caracterizeze teoriile amenințărilor informatice; Să explice principiile operațiilor informaționale Să înțeleagă specificul procesului de realizare a acțiunilor ostile de influențare Să identifice abordările decizionale pentru activitatea structurilor de specialitate Să utilizeze spațiul virtual pentru comunicarea specifică	Examen scris	70%
Seminar			
Laborator	Realizarea temelor de laborator	Evaluare continuă	10%
Proiect	Realizarea temei de proiect	Evaluare proiect	20%
Standard minim de performanță			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
18.10.2018	Conf.univ.dr.ing. Sintea Sorin	Conf.univ.dr.ing. Sintea Sorin

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Antene, arhitecturi de comunicaţii şi riscuri cibernetice				
Titularul activităţilor de curs	Prof.univ.dr. ing. Răzvan TAMAŞ				
Titularul activităţilor de seminar	Prof. univ.dr. ing. Răzvan TAMAŞ				
Anul de studiu	1	Semestrul	1	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DA
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DOA

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	-	Laborator	2	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	-	Laborator	28	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	35
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	8
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	5
II d) Tutoriat	
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	48
Total ore pe semestru (Ib+II+III+IV)	106
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	• Bazele electrotehnice, Semnale şi sisteme, Teoria transmisiunii informaţiei, Decizie şi estimare în prelucrarea informaţiilor
Competenţe	C3.3 Utilizarea soft-urilor profesionale pentru proiectarea sistemelor electronice de telecomunicaţii C3.4 Simularea şi evaluarea sistemelor electronice de telecomunicaţii proiectate cu ajutorul modelărilor numerice şi softurilor profesionale

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• Nu este cazul
Desfăşurare aplicaţii	Seminar	•
	Laborator	• Prezenţa obligatorie
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	C3 Folosirea creativa a conceptelor fundamentale din electronică, a metodelor de modelare si simulare, pentru realizarea modulelor unor sisteme electronice de telecomunicaţii.
Competenţe	C1. Îndeplinirea sarcinilor profesionale cu identificarea exactă a obiectivelor de realizat, a unor factori

transversale	potenţiali de risc, a resurselor disponibile, a aspectelor economico-financiare, condiţiilor de finalizare a acestora, etapelor de lucru, timpului de lucru şi termenelor de realizare aferente.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Rezolvarea problemelor specifice pentru caracterizarea şi modelarea canalelor de propagare. Clasificarea mecanismelor de propagare; Clasificarea reţelelor radio; Topologii de reţele şi clasificarea ariilor de serviciu; Cunoaşterea conceptelor de propagare, a comportamentului unui canal radio, a bugetului legăturii radio, înţelegerea fenomenului de fading; Identificarea specificului organismelor de standardizare şi reglementare privind emisiile în cadrul reţelelor radio;
	Utilizarea principalilor parametri de calitate şi a tehnicilor de măsură specifice mediilor de propagare şi transmisie. Obiectivele specifice asigurate de disciplină se referă la prezentarea principiilor propagării undelor radio.

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
1. Definiţii 1.1. Terminologie 1.2. Scenarii de propagare 1.3. Metode de măsură pentru canale radio	2	Predarea se bazează pe folosirea videoproiectorului (acoperind funcţia de comunicare şi demonstrativă); metoda de comunicare orală utilizată este metoda problematizării,utilizate frontal. Studenţii simulează, implementează, testează şi evaluează independent aceleaşi probleme prin utilizarea continuă a calculatorului şi a mediului software, sau prin rotaţie, utilizând platformele de laborator. Materialele didactice sunt reprezentate, în principal, de îndrumarul de laborator în variantă tipărită şi electronică (pe campusul virtual).	
2. Modelarea canalelor 2.1 Modele stocastice 2.2 Modele bazate pe topologia reţelei 2.3 Modele simplificate	4		
3. Parametrii şi modele de canal 3.1 Modele pentru atenuarea de propagare 3.2 Generarea coeficienţilor canalului 3.3 Tranziţia între condiţiile de propagarii	4		
4. Folosirea modelelor de canal în simulări	2		
5. Metode pentru caracterizarea canalelor radio 5.1 În interiorul clădirilor 5.2 Micro celule 5.3 Macro celule	2		
6. Metode pentru sinteza antenelor	2		
7. Metoda ecuaţiei integrale	2		
8. Dipoli de bandă largă şi tehnici de adptare 8.1. Antena biconică 8.2. Dipolul cilindric 8.3. Tehnici de adaptare	2		
9. Antene cu undă progresivă	2		
10. Antene independente de frecvenţă	2		
11. Antene planare, Sisteme de antene, Antene inteligente, Antenă distribuită	2		
12. Măsurarea antenei 12.1 Măsurarea caracteristicii de radiaţie 12.2 Măsurarea câştigului 12.3 Măsurarea directivităţii 12.4 Măsurarea impedanţelor 12.5 Măsurarea curentului 12.6 Măsurarea polarizaţiei 12.7 Măsurarea modelelor la scară	2		
Bibliografie			

- R. Tamaş, „Antene, propagare şi diversitate", suport de curs disponibil pe campusul virtual al UMC
- R. Tamaş, „Antenna theory: traditional versus modern approach", Ed. Nautica, 2011
- R.E. Collin, "Antennas and Radiowave Propagation", McGraw-Hill Book Company Inc., New York, 1985
- E. Nicolau, "Antene şi propagare", Editura Didactică şi Pedagogică, Bucureşti, 1982
- C. A. Balanis, "Antenna Theory – Analysis and Design", John Wiley & Sons, Inc., 1997

Bibliografie minimală

•

Aplicaţii (Laborator)	Nr. ore	Metode de predare	Observaţii
L.1 Modele pentru atenuarea de propagare I	2	Predarea se bazează pe folosirea videoproiectorului (acoperind funcţia de comunicare şi demonstrativă); metoda de comunicare orală utilizată este metoda problematizării,utilizate frontal. Studenţii simulează, implementează, testează şi evaluează independent aceleaşi probleme prin utilizarea continuă a calculatorului şi a mediului software, sau prin rotaţie, utilizând platformele de laborator. Materialele didactice sunt reprezentate, în principal, de îndrumarul de laborator în variantă tipărită şi electronică (pe campusul virtual).	
L.2 Modele pentru atenuarea de propagare II	2		
L.3 Canal radio mobil I	2		
L.4 Canal radio mobil II	2		
L.5 Diversitate spaţială I	2		
L.6 Diversitate spaţială II	2		
L.7 Arie de dipoli I	2		
L.8 Arie de dipoli II	2		
L.9 Antenă microstrip I	2		
L.10 Antenă microstrip II	2		
L.11 Impedanţa de intrare I	2		
L.12 Impedanţa de intrare II	2		
L.13 Antene inteligente I	2		
L.14 Antene inteligente II	2		

Bibliografie

1. R. Tamaş, „Antene, propagare şi diversitate", suport de curs disponibil pe campusul virtual al UMC
2. R.E. Collin, "Antennas and Radiowave Propagation", McGraw-Hill Book Company Inc., New York, 1985
3. E. Nicolau, "Antene şi propagare", Editura Didactică şi Pedagogică, Bucureşti, 1982
4. C. A. Balanis, "Antenna Theory – Analysis and Design", John Wiley & Sons, Inc., 1997

Bibliografie minimală

•

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

- Dezvoltarea fără precedent a sistemelor de radiocomunicaţii, a senzorilor radio şi a sistemelor de detecţie şi localizare prin mijloace electromagnetice a făcut ca echipamentele radio să fie omniprezente. În structura oricărui sistem radio există cel puţin o antenă. Tendinţa de miniaturizare a echipamentelor sau cea de creştere a eficienţei spectrale reclamă dezvoltarea de noi tipuri si variante de antene. Industria are o cerere importantă de ingineri calificaţi, cu specializări radio şi cu un fundament solid în domeniul antenelor şi modelării canalelor radio, capabili să dezvolte noi produse şi servicii.
- Programa cursului răspunde concret acestor cerinţe actuale de dezvoltare şi evoluţie, subscrise economiei europene a serviciilor din domeniul Inginerie Electronică şi Telecomunicaţii, programul de studii Tehnologii şi sisteme de telecomunicaţii (TST). În contextul progresului tehnologic actual al echipamentelor de radiofrecvenţă, domeniile de activitate vizate sunt practic nelimitate, cum ar fi aplicaţiile şi bunurile de larg consum (terminale mobile de tip "smart-phone"), domeniul medical (tratament, imagistică), domeniul militar (sisteme de comunicaţii speciale integrate, sisteme de radiolocaţie şi radioghidaj), domeniul de securitate (sisteme de supraveghere), domeniul extrem de actual al comunicaţiilor profesionale şi altele.
- Se asigură astfel absolvenţilor ciclului de învăţământ universitar de master competenţe în concordanţă cu necesităţile calificărilor actuale, precum şi o pregătire ştiinţifică şi tehnică modernă, de calitate şi competitivă, care să le permită după absolvire o angajare rapidă. Acest lucru este conform politicii Universităţii Maritime din Constanţa, atât din punctul de vedere al conţinutului şi structurii, cât şi din punctul de vedere al aptitudinilor şi deschiderii internaţionale oferite absolvenţilor.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	- Prezentarea metodelor de analiză şi proiectare a antenelor. Cunoşterea tipurilor de antene folosite in tehnologiile de acces şi transport radio, antene	Examen programat în sesiune. Subiectele acoperă în totalitate programa analitică a	**50%**

	pentru staţiile de bază pentru terminale fixe, mobile sau portabile. Parametrii fundamentali ai canalului radio fix, mobil sau cu diversitate. Prezentarea proprietăţilor canalelor radio şi a metodelor de analiză.	disciplinei, realizând o sinteză între parcurgerea teoretică comparativă a cursului şi explicitarea prin exerciţii a modelelor de aplicaţie.	
Seminar	-	-	-
Laborator	- Studiul unor antene folosite in terminale mobile şi staţii de bază. Sisteme de antene, antene inteligente, sistem de antenă distribuită.	Colocviu final de laborator, cuprinzând o componentă teoretică şi o componentă practică. Componenta teoretică constă în răspunsul dat de fiecare student la un set distinct de întrebări; componenta practică constă în determinarea unor parametrii fundamentali ai antenelor.	**50%**
Proiect			
Standard minim de performanţă			
- Crearea abilităţilor de a analiza şi proiecta antene pentru staţii de bază şi terminale fixe sau portabile. - Cunoaşterea modelelor uzuale folosite pentru caracterizarea canalului radio fix sau mobil. - Abilitatea de a măsura şi caracteriza un canal radio. Capacitatea de a genera specificaţii pentru antene simple sau sisteme de antene.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	Prof. univ. dr. ing. Răzvan Tamaş	Prof. univ. dr. ing. Răzvan Tamaş

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Ion Omocea

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Sistemele de comunicaţii subacvatice				
Titularul activităţilor de curs	Conf.univ. dr. ing. Alin DANISOR				
Titularul activităţilor de seminar	Ş.L.univ. dr. ing. Ana SAVU				
Anul de studiu	1	Semestrul	2	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DOA

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	3	Curs	2	Seminar	-	Laborator	1	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	42	Curs	28	Seminar	-	Laborator	14	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	30
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	20
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	12
II d) Tutoriat	-
III Examinări	2
IV Alte activităţi (precizaţi):	-

Total ore studiu individual II (a+b+c+d)	62
Total ore pe semestru (Ib+II+III+IV)	106
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	Semnale si Sisteme, Prelucrarea Digitala a Semnalelor, Decizie si Estimare in Prelucrarea Informatiei
Competenţe	Studentii capata abilitatea de a analiza semnale din mediul subacvatic in vederea detectiei tintelor subacvatice si estimarea parametrilor acestora. Vor capata abilitatea de analiza a schemelor bloc a sistemelor SONAR. Partea finala a cursului prezinta probleme specifice referitoare la comunicatiile subacvatice si modurile de solutionare a acestora.

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• Nu este cazul
Desfăşurare aplicaţii	Seminar	•
	Laborator	• Prezenţa obligatorie
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	C3 - Folosirea creativa a conceptelor fundamentale din electronică, a metodelor de modelare si simulare, pentru realizarea modulelor unor sisteme electronice de comunicaţii
Competenţe	CT1 - Îndeplinirea sarcinilor profesionale cu identificarea exactă a obiectivelor de realizat, a unor factori

transversale	potenţiali de risc, a resurselor disponibile, a aspectelor economico-financiare, condiţiilor de finalizare a acestora, etapelor de lucru, timpului de lucru şi termenelor de realizare aferente.

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Disciplina asigură studenţilor o pregătire generală in domeniul analizei semnalelor submarine si implementatrea acesteia in sistemele SONAR si sistemele de comunicatii subacvatice.Sunt prezentate aspectele fizice ale propagarii undelor acustice in mediul submarin.
	Directiile specifice ale disciplinei constau in abordarea aspectelor specifice ale propagarii sunetelor in mediul subacvatic. Cursul abordeaza metodele moderne de prelucrare a semnalelor in sistemele SONAR si schemele bloc ale sistemelor dedicate.Sunt tratate de asemenea aspectele specifice comunicatiilor submarine.

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
1. Oscilatii si unde acustice 1.1. Oscilatoare liniare. Concepte de baza 1.2. Oscilatoare mecanice legate in paralel 1.3. Oscilattile libere ale oscilatoarelor mecanice legate in paralel 1.4. Oscilattile fortate ale oscilatoarelor mecanice legate in paralel 1.5. Energia oscilatoarelor mecanice 1.6. Sisteme acustice 1.7. Rezonatorul Helmholtz	2	Predarea principalelor noţiuni teoretice, a schemelor de principiu şi caracteristicilor acestora este efectuată folosind videoproiectorul, în timp ce deducerile relaţiilor matematice şi demonstraţiile sunt efectuate folosind metoda clasică (la tablă).	
2. Traductoare electromecanice si electroacustice 2.1. Ecuatiile traductoarelor electroacustice 2.2. Cuplarea traductoarelor electroacustice 2.3.Traductoare de presiune si de gradient de presiune	4	Predarea principalelor noţiuni teoretice, a schemelor de principiu şi caracteristicilor acestora este efectuată folosind videoproiectorul, în timp ce deducerile relaţiilor matematice şi demonstraţiile sunt efectuate folosind metoda clasică (la tablă).	
3. Decizia in acustica submarina 3.1. Detectie si estimare 3.2. Teoria clasica a detectiei 3.3. Filtre adaptate 3.4. Estimarea parametrilor si a semnalelor	4	Predarea principalelor noţiuni teoretice, a schemelor de principiu şi caracteristicilor acestora este efectuată folosind videoproiectorul, în timp ce deducerile relaţiilor matematice şi demonstraţiile sunt efectuate folosind metoda clasică (la tablă).	

4. Zgomotul mediului submarin 4.1. Zgomotul ambiant 4.2. Zgomotul propriu si radiant al navei 4.3. Reverberatia	2	Predarea principalelor noțiuni teoretice, a schemelor de principiu și caracteristicilor acestora este efectuată folosind videoproiectorul, în timp ce deducerile relațiilor matematice și demonstrațiile sunt efectuate folosind metoda clasică (la tablă).	
5. Arii de traductoare 5.1. Unde elastice si prelucrarea semnalelor aferente 5.2. Arii de traductoare adaptate 5.3. Arii de traductoare de inalta rezolutie	2	Predarea principalelor noțiuni teoretice, a schemelor de principiu și caracteristicilor acestora este efectuată folosind videoproiectorul, în timp ce deducerile relațiilor matematice și demonstrațiile sunt efectuate folosind metoda clasică (la tablă).	
6. SONAR activ 6.1. Efectul canalului de propagre 6.2. Functia de incertitudine 6.3. Alegerea formelor de unda	4	Predarea principalelor noțiuni teoretice, a schemelor de principiu și caracteristicilor acestora este efectuată folosind videoproiectorul, în timp ce deducerile relațiilor matematice și demonstrațiile sunt efectuate folosind metoda clasică (la tablă).	
7. SONAR pasiv 7.1. Procesarea semnalelor acustice de banda larga 7.2. Procesarea semnalelor acustice de banda ingusta 7.3. Postprocesarea 7.4. Metode de localizare si urmarire	4	Predarea principalelor noțiuni teoretice, a schemelor de principiu și caracteristicilor acestora este efectuată folosind videoproiectorul, în timp ce deducerile relațiilor matematice și demonstrațiile sunt efectuate folosind metoda clasică (la tablă).	
8. Comunicatii subacvatice 8.1. Introducere in comunicatiile subacvatice 8.2. Codarea si decodarea 8.3. Comunicatii cu spectru imprastiat	6	Predarea principalelor noțiuni teoretice, a schemelor de principiu și	

8.4 Egalizarea canalelor de comunicatii subacvatice		caracteristicilor acestora este efectuată folosind videoproiectorul, în timp ce deducerile relaţiilor matematice şi demonstraţiile sunt efectuate folosind metoda clasică (la tablă).	

Bibliografie

2. Hodges R. - *Underwater acoustics,* Wiley &Sons 2010
3. Qihu Li - *Digital sonar design in underwater acoustics*, Springer 2012
2. Hodges R. - *Underwater acoustics,* Wiley &Sons 2010

Bibliografie selectiva

1. Danisor A. - *Underwater locating and communications systems, course notes,* https://campus.cmu-edu.eu/

Aplicaţii (Laborator)	Nr. ore	Metode de predare	Observaţii
1. Zgomotul in acustica subacvatica. Parametrii	2	Predarea se bazează pe folosirea videoproiectorului (acoperind funcţia de comunicare şi demonstrativă); metoda de comunicare orală utilizată este metoda problematizării, utilizate frontal. Studenţii simulează, implementează, testează şi evaluează independent aceleaşi probleme prin utilizarea continuă a calculatorului şi a mediului software. Materialele didactice sunt reprezentate, în principal, de îndrumarul de laborator în variantă tipărită şi electronică (pe campusul virtual).	
2. Decizia in sistemle SONAR. Filtre adaptate	2		
3. Sonare active. Proiectarea formelor de unda	2		
4. Procesarea cu arii de antene	2		
5. Studiul sonarelor pasive	2		
6. Comunicatii subacvatice. Codarea si decodarea	2		
7. Comunicatii subacvatice. Spectru imprastiat	2		

Bibliografie

1. Hann B., & all - *Essential Matlab for Engineers and Scientists,* Elsevier Ltd. 2010

Bibliografie minimală

1. Savu A. - *Underwater locating and communication systems. Applications,* https://campus.cmu-edu.eu/

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

Crearea de abilitati in aplicarea cunostintelor generale in domeniul prelucrarii digitale a semnalelor. Se urmareste dezvoltarea capabilitatilor in scopul obtinerii celor mai bune performante in domeniul prelucrarii digitale a semnalelor pentru rezolvarea efectiva a problemelor din domeniu. Disciplina are un puternic caracter aplicativ in sensul proiectarii, modelarii si simularii semnalelor reale in concordanta cu metodele moderne de prelucrare.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Cunoasterea fenomenelor de propagare a semnalelor ultra-acustice in mediul subacvatic, a metodelor de prelucrare a semnalelor subacvatice si a principiilor si metodelor comunicatiilor subacvatice .	Examen programat în sesiune. Subiectele acoperă în totalitate programa analitică a disciplinei, realizând o sinteză între parcurgerea teoretică comparativă a cursului şi explicitarea prin exerciţii a modelelor de aplicaţie.	**60%**
Seminar			
Laborator	Abilitatea de aplicare a celor mai bune metode in prelucrarea semnalelor subacvatice, modelarea sistemelor SONAR si de comunicatii subacvatice.	Referat de laborator conținând rezultatele experimentelor efectuate și răspunsurile la problemele/exercițiile aferente acestora.	**40%**
Proiect			
Standard minim de performanţă			
Cunoasterea minimala a fenomenelor propagarii sunetelor in mediul submarin, a prelucrarii de baza a semnalelor in sistemele SONAR si de comunicatii subacvatice si cunoasterea elementelor fundamentale a structurii acestor sisteme.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	Conf. univ.dr. ing. Alin Danisor	Ș.L.univ. dr. ing. Ana Savu

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ. dr. ing. Ion Omocea

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Managementul securităţii cibernetice				
Titularul activităţilor de curs	Daniel Ioniţă				
Titularul activităţilor de seminar	Daniel Ioniţă				
Anul de studiu	1	Semestrul	1	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DOA

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	3	Curs	2	Seminar	1	Laborator	-	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	42	Curs	28	Seminar	14	Laborator	-	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	16
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	4
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	4
II d) Tutoriat	6
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	30
Total ore pe semestru (Ib+II+III+IV)	74
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Să cunoască şi să interpreteze strategii şi tehnici specifice ameninţărilor informatice; Să caracterizeze teoriile managementului ameninţărilor informatice în contextul securităţii cibernetice; Să aplice principiile managementului ameninţărilor informatice în contextul securităţii cibernetice pentru analiza organizaţiei Să cunoască cerinţele generale ale sistemului de management al securităţii Să înţeleagă specificul procesului de management al ameninţărilor informatice în contextul securităţii

	cibernetice în cadrul organizației în care activează
Competențe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităților lingvistice, a cunoștințelor de tehnologia informației și a comunicării pentru dezvoltarea personală si profesională, în scopul inserției pe piața muncii și al adaptării la dinamica cerințelor acesteia. Utilizarea eficientă a resurselor și tehnicilor de învățare, în scopul dezvoltării personale și profesionale continue în domeniul telecomunicațiilor și tehnologiei informaționale, operarea cu informații și tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe și demonstrarea abilităților de comunicare.

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

Obiectivul general al disciplinei	Cunoașterea principalelor aspecte referitoare la managementul securității cibernetice la nivel național și la nivelul oricărei entități economico-administrative în conformitate și cu respectarea prevederilor de management din domeniul de referință

8. Conținuturi

Curs	Nr. ore	Metode de predare	Observații
1. Identificarea nevoilor de securitate cibernetică la nivel național	**4**	Prelegere orală	
2. Identificarea principalelor amenințări de securitate cibernetică la adresa securității naționale	**4**	Prelegere orală	
3. Vectori de propagare a amenințărilor cibernetice	**2**	Prelegere orală	
4. Managementul vulnerabilităților în securitate cibernetică	**2**	Prelegere orală	
5. Incidente de securitate cibernetică - prevenire, identificare, analiză și răspuns	**4**	Prelegere orală	
6. Măsuri de sporire a nivelului de securitate cibernetică în plan național	**2**	Prelegere orală	
7. Evaluarea riscurilor de securitate cibernetică la nivelul instituțiilor publice și întocmirea planurilor de răspuns	**4**		
8. Capabilități de răspuns la incidente de securitate cibernetică la nivel național	**2**	Prelegere orală	
9. Capabilități de răspuns la incidente de securitate cibernetică la nivel internațional	**2**	Prelegere orală	
10. Programe de educare și formare în securitate cibernetică	**2**	Prelegere orală	

Bibliografie

1. Managementul securității cibernetice
2. Cyber readiness index 2.0 – Potomac Institute for Policies Studies
3. HG494/2011 – Organizarea și funcționarea CERT-RO
4. ISO 17799,
5. Personally identifiable information (PII)
6. ISO 27001
7. ITIL

Aplicații (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observații
Seminar 1 - Analiza principalilor vectori de propagare a amenințărilor cibernetice	2	problematizare, exercitiu	
Seminar 2 - Măsuri de sporire a nivelului de securitate cibernetică în plan național	2	problematizare, exercitiu	
Seminar 3 – Elaborarea politicilor de securitate	2		
Seminar 4 - Evaluarea riscurilor de securitate cibernetică la nivelul unei instituții publice sau a unei entități private din sectoarele reglementate de Legea 362/2019	2	problematizare, exercitiu	
Seminar 5 - Întocmirea unui plan de răspuns la amenințări de securitate cibernetică pe baza riscurilor evaluate	2	problematizare, exercitiu	
Seminar 6 - Certificarea la nivel european in securitate cibernetica -	2	problematizare, exercitiu	
Seminar 7 – Cybersecurity Operation Centre – rol, atribuții, organizare si funcționare	2	problematizare, exercitiu	

Bibliografie

1. Managementul securităţii cibernetice
2. Cyber readiness index 2.0 – Potomac Institute for Policies Studies
3. HG494/2011 – Organizarea şi funcţionarea CERT-RO
4. Legea 362/2019 privind un nivel comun ridicat de securitate a reţelelor şi sistemelor informatice
5. ISO 17799
6. Personally identifiable information (PII)
7. ISO 27001
8. Cyber Security Act – Regulation on ENISA and on communication and information technology cybersecurity certification

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

- Conţinutul este orientat către aspecte practice ale evaluării riscurilor de securitate cibernetică la nivelul unei instituţii, derivată din managementul national al riscurilor de securitate cibernetică în vederea managementului acestora.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Să cunoască cerinţele generale ale sistemului de management al securităţii Să înţeleagă specificul procesului de management al ameninţărilor informatice în contextul securităţii cibernetice în cadrul organizaţiei în care activează Să poată evalua şi aprecia calitativ şi cantitativ incidentele de securitate cibernetică complexe şi poate interpreta rezultatele. Să poată implementa proceduri de testare / verificare a conformităţii cu obiectivele din strategia de securitate privind informaţia; Să poată elabora setul de criterii de evaluare a gradului de îndeplinire a obiectivelor din strategia de Securitate; Să poată să propună machete / şabloane etalon pentru monitorizarea aplicării măsurilor de securitate	Examen scris	70%
Seminar	Realizarea temelor de seminar Prezenţa la curs şi seminar	Evaluare continuă	30%
Laborator			
Proiect			
Standard minim de performanţă			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
12.10.2018	Daniel Ioniţă	Daniel Ioniţă

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Managementul riscului în tehnologiile informaţionale				
Titularul activităţilor de curs	Prof.univ.dr.ing. Stanca Costel				
Titularul activităţilor de seminar	Prof.univ.dr.ing. Stanca Costel				
Anul de studiu	2	Semestrul	1	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DC
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	2	Laborator	-	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	28	Laborator	-	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	15
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	10
II d) Tutoriat	5
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	40
Total ore pe semestru (Ib+II+III+IV)	98
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Înţelegerea riscurilor din organizaţie Analiza cantitativă a riscului Aplicarea metodelor de gestiune a riscurilor
Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia.

	Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Studentii vor fi capabili să analizeze, să utilizeze tehnicile de cuantificare şi de tratare a riscurilor organizaţionale

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
Introducere in managementul riscurilor	2	Prelegere orală	
Evaluarea riscurilor – elemente de baza	4	Prelegere orală	
Evaluarea cantitativa a riscurilor	4	Prelegere orală	
Controlul riscurilor	4	Prelegere orală	
Managementul riscului în tehnologia informaţiei	4	Prelegere orală	
Managementul riscului în proiecte	4	Prelegere orală	
Familia de standarde ISO 27000	6	Prelegere orală	

Bibliografie

ALBU IONEL, AUDITUL INTERN ŞI MANAGEMENTUL RISCURILOR, ÎN: TRIBUNA ECONOMICĂ, V. 19, NR. 8, P. 56-60, 2008;
BĂRBULESCU SEVASTIAN, GESTIONAREA RISCURILOR - FUNCŢIE MANAGERIALĂ LA NIVELUL UNEI ORGANIZAŢII PUBLICE, ÎN: REVISTA FINANŢE PUBLICE ŞI CONTABILITATE, V. 19, NR. 4, P. 24-30, 2008;
BJELIC ALEKSANDAR, RISCUL - COMPONENTĂ A ORGANIZAŢIILOR. ÎN: TRIBUNA ECONOMICĂ, V. 18, NR. 22, P. 25-28, 2007;
CHORAFAS DIMITRIS N, MANAGING RISK IN THE NEW ECONOMY, NEW YORK: NEW YORK INSTITUTE OF FINANCE, 2001;
CIOCOIU CARMEN NADIA, MANAGEMENTUL RISCULUI,: VOL 1: TEORII, PRACTICI, METODOLOGII, BUCUREŞTI: EDITURA ASE, 2008;
CIOCOIU CARMEN NADIA, MANAGEMENTUL RISCULUI, VOL 2: MODELE ECONOMICO-MATEMATICE, INSTRUMENTE ŞI TEHNICI, BUCUREŞTI: EDITURA ASE, 2008;
LAM, JAMES, ENTERPRISE RISK MANAGEMENT, FROM INCENTIVES TO CONTROLS, HOBOKEN: JOHN WILEY & SONS, 2003;
OPRAN CONSTANTIN, MANAGEMENTUL RISCULUI, EDITURA COMUNICARE.RO, BUCURESTI, 2004;
WATERS DONALD, SUPPLY CHAIN RISK MANAGEMENT, VULNERABILITY AND RESILIENCE IN LOGISTICS, LONDON: KOGAN PAGE, 2007.
STANDARDELE ISO 27000

Aplicaţii (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observaţii
Evaluarea riscurilor – elemente de baza	6	problematizare, exercitiu	
Evaluarea riscurilor – distributia normala	4	problematizare, exercitiu	
Evaluarea riscurilor – distirbutia binomiala	4	problematizare, exercitiu	
Evaluarea riscurilor – distributia Poisson	6	problematizare, exercitiu	
Familia de standarde ISO 27000	8	problematizare, exercitiu	

Bibliografie

ALBU IONEL, AUDITUL INTERN ŞI MANAGEMENTUL RISCURILOR, ÎN: TRIBUNA ECONOMICĂ, V. 19, NR. 8, P. 56-60, 2008;
BĂRBULESCU SEVASTIAN, GESTIONAREA RISCURILOR - FUNCŢIE MANAGERIALĂ LA NIVELUL UNEI ORGANIZAŢII PUBLICE, ÎN: REVISTA FINANŢE PUBLICE ŞI CONTABILITATE, V. 19, NR. 4, P. 24-30, 2008;
BJELIC ALEKSANDAR, RISCUL - COMPONENTĂ A ORGANIZAŢIILOR. ÎN: TRIBUNA ECONOMICĂ, V. 18, NR. 22, P. 25-28, 2007;
CHORAFAS DIMITRIS N, MANAGING RISK IN THE NEW ECONOMY, NEW YORK: NEW YORK INSTITUTE OF FINANCE, 2001;
CIOCOIU CARMEN NADIA, MANAGEMENTUL RISCULUI,: VOL 1: TEORII, PRACTICI, METODOLOGII, BUCUREŞTI: EDITURA ASE, 2008;
CIOCOIU CARMEN NADIA, MANAGEMENTUL RISCULUI, VOL 2: MODELE ECONOMICO-MATEMATICE, INSTRUMENTE ŞI TEHNICI, BUCUREŞTI: EDITURA ASE, 2008;
STANDARDELE ISO 27000

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

- Conţinutul este orientat către aspecte practice ale tehnologiilor de lucru sub apă, în concordanţă cu cele mai noi tehnici care sunt aplicate în întreaga lume.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Cunoaşterea terminologiei de specialitate, a sistemului conceptual cu care operează disciplina Capacitatea de utilizare adecvată a principiilor, normelor şi metodelor de operare impuse de disciplină Probarea argumentaţiei logice (prin argumente pro şi contra), pe baza unei strategii de evaluare conştientă a realităţii	Examen scris, axat pe elemente de corelare a cunoştinţelor teoretice cu cele concrete, practice	70%
Seminar	Însuşirea abilităţilor de gândire în evaluarea unor situaţii tip „dilemă" în dezvoltarea economico-socială asimetrică (diminuarea disparităţilor economico-sociale) Executarea unor sarcini complexe, interdisciplinare (studii de caz) Capacitatea de corelare a aspectelor teoretice cu cele practice	Răspunsuri la seminar, din tematica anunţată anterior	30%
Laborator			
Proiect			
Standard minim de performanţă			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
22.10.2018	Prof.univ.dr.ing. Stanca Costel	Prof.univ.dr.ing. Stanca Costel

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Managementul tehnologiei informaţiilor prin prisma ameninţărilor hibride				
Titularul activităţilor de curs	Dr. Mihai - Liviu Dănilă				
Titularul activităţilor de seminar	Dr. Mihai - Liviu Dănilă				
Anul de studiu	1	Semestrul	1	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DA
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DOA

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	2	Laborator	-	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	28	Laborator	-	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	16
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	18
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	8
II d) Tutoriat	6
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	48
Total ore pe semestru (Ib+II+III+IV)	106
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	• Cunoaşterea unei limbi străine

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• Masteranzii trebuie să respecte normele de conduită academică • Masteranzii nu se vor prezenta la prelegeri cu telefoanele mobile deschise; • Nu va fi tolerată întârzierea masteranzilor la curs; • Data susţinerii examenului se va stabili de titular de comun acord cu masteranzii.
Desfăşurare aplicaţii	Seminar	• Trebuie să respecte normele de conduită academică; • Nu se vor prezenta la seminare cu telefoanele mobile deschise; • Nu va fi tolerată întârzierea la seminare; • Termenele de predare şi susţinere a lucrărilor de seminar sunt stabilite de titular de comun acord cu masteranzii. Nu se vor accepta cererile de amânare a acestora pe motive altfel decât obiectiv întemeiate. De asemenea, nu se acceptă cererile doar de predare a temelor de seminar fără ca acestea să se susţină în faţa colegilor.
	Laborator	•

	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	• Să cunoască termenii de specialitate şi să înţeleagă conceptele privind managementul ameninţărilor hibride în contextul securităţii cibernetice, performanţele de calificare a unui angajat pentru relaţionarea corectă în spaţiul virtual şi social-media; • Să cunoască şi să interpreteze strategii şi tehnici specifice ameninţărilor hibride; • Să caracterizeze teoriile managementului ameninţărilor hibride în contextul securităţii cibernetice; • Să aplice principiile managementului ameninţărilor hibride în contextul securităţii cibernetice pentru analiza organizaţiei • Să înţeleagă specificul procesului de management al ameninţărilor hibride în contextul securităţii cibernetice în cadrul organizaţiei în care activează • Să cunoască funcţiile procesului de securitate cibernetică şi să stabilească diferenţieri între tipurile de riscuri în vederea aplicării acestora în managementul managementului ameninţărilor hibride • Să cunoască şi să înţeleagă etapele proiectării şi reproiectării unei strategii de management a ameninţărilor hibride în contextul securităţii cibernetice, în interiorul propriei organizaţii • Să identifice abordările decizionale pentru activitatea structurilor de management a ameninţărilor hibride în contextul securităţii cibernetice • Să utilizeze spaţiul virtual pentru o conduită specifică care să îi asigure un nivel corespunzător de securitate şi diminuare a ameninţărilor hibride • Să valorifice cunoştinţele acumulate în vederea integrării în viitoarea activitate profesională şi viaţa socială; • Să participe la elaborarea proiectelor de desfăşurare a diferitelor activităţi profesionale la nivelul sistemului public / privat; • Să participe la elaborarea proiectelor de cercetare ştiinţifică în domeniul managementului ameninţărilor hibride în contextul securităţii cibernetice.
Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Cunoaşterea şi înţelegerea problematicii managementului ameninţărilor hibride în contextul securităţii cibernetice în administraţia publică / mediul antreprenorial / societăţi capital privat, a practicilor specifice în organizaţii, a procedurilor şi mecanismelor de management a ameninţărilor hibride pentru realizarea securităţii cibernetice cu alte entităţi specifice organizaţiei din care face parte, compararea structurii şi funcţionalităţii compartimentelor de profil, elaborarea unei strategii de securitate cibernetică şi management a ameninţărilor hibride

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
1. Ameninţări hibride vs. ameninţări asimetrice: definire	2	Prelegere orală	
2. Categorii de ameninţări asimetrice şi hibride	2	Prelegere orală	
3. Operaţiile informaţionale – OI; OI ofensive; OI defensive	6	Prelegere orală	3 şedinţe x 2hrs
4. Operaţiile netradiţionale (nesupunerea civilă, utilizarea terorii etc.)	2	Prelegere orală	
5. Caracteristicile ameninţărilor hibride şi impactul de intelligence	2	Prelegere orală	
6. Dimensiuni, forme şi procedee ale ameninţărilor hibride	2	Prelegere orală	
7. Impactul ameninţărilor hibride în contextul securităţii cyber	2	Prelegere orală	
8. Social media din perspectiva ameninţărilor hibride; cazuistică	4	Prelegere orală	2 şedinţe x 2hrs
9. Modalităţi de contracarare a ameninţărilor hibride	2	Prelegere orală	
10. Aspecte juridice ale acţiunilor hibride în context cyber	2	Prelegere orală	
11. Mediile de dezvoltare a ameninţărilor hibride şi contramăsuri	2	Prelegere orală	
Bibliografie			

1. CRUCERU, Valerică, „Despre conceptul de război hibrid în gândirea militară americană", în Buletinul UNAp., nr. 3/2014, Bucureşti, Editura UNAp, 2014, p. 29-33.
2. FLYNN, Michael T., Fixing Intel - A blueprint for making intelligence relevant in Afghanistan, Center for a New American Security, Washington DC, 2010, 26 p.
3. HOFFMAN, Frank G., „Hybrid Warfare and Challenges", Joint Forces Quarterly/ Issue 52, 1st quarter 2009, p. 34-39, http://www.ndupress.ndu.edu.
4. LOWENTHAL, Mark M., Intelligence-from secrets to policy, Third edition, CQ Press, 2006.
5. KORKISCH, Friedrich W., NATO Gets „Better Intelligence", Strategy Paper 1-2010, Vienna, 2010, 75 p.
6. *** "NATO's Readiness Action Plan" – fact sheet, December 2014.
7. *** BI-SC Collective Training and Exercise Directive 075-003, 02 October 2013.
8. www.nato.int
9. www.stratfor.com
10. Chifu, Iulian, „Prospective of Ukrainian crisis. Scenarios for a mid-long term evolution", Editura Institutului de Ştiinţe politice şi Relaţii Internaţionale al Academiei Române, Bucureşti, 2014.
19. Chifu, Iulian, „Hybrid war, a limited and unlimited war", in Rethinking social action, Core Values, 16-19 april 2015, Iaşi, Editura Lumen, 2015, p.158.
20. Chifu, Iulian, „Hybrid warfare, lawfare, informational war. The wars of the future", in Stan Anton, Iuliana Simona Ţuţuianu, Proceedings International Scientifi c Conference Strategies XXI. The Complex Dynamic Nature of the Security Environment, 11-12 iunie 2015, Universitatea Naţională de Apărare Carol I, pp. 203-211.
21. Kissinger, Henry, Diplomaţia, op. cit.

Aplicaţii (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observaţii
1. Conceptul ameninţărilor hibride: definire şi categorii	2	problematizare, exercitiu	
2. Operaţiile informaţionale	2	problematizare, exercitiu	
3. Tipologia operaţiilor informaţionale	2	problematizare, exercitiu	
4. Operaţiile netradiţionale	2	problematizare, exercitiu	
5. Ameninţările hibride – provocare pentru Intelligence	2	problematizare, exercitiu	
6. Impactul amininţărilor hibride	2	problematizare, exercitiu	
7. Măsuri de diminuare a ameninţărilor hibride în contextual realizării securităţii cibernetice	2	problematizare, exercitiu	

Bibliografie

1. McLENDON, J.W., „Battlefi eld on the Future: Information War Impact and Concerns", http://www. totse.com;
2. POPA, Radu, „Abordări moderne privind războiul informaţional pe timp de pace, criză sau război", Buletinul Universităţii Naţionale de Apărare „Carol I", nr. 4, 2007, Bucureşti, p. 453-458; 3.SZAFRANSKI, R., „A Theory of Information Warfare", Air University, 1995, http://www.airpower. maxwel.af.mil/airchronicles/apj/szfran.html;
4. TOFFLER, Alvin şi TOFFLER, Heidi, Război şi antirăzboi. Supravieţuirea în zorii secolului XXI, Editura Antet, 1995;
5. TOPOR, Sorin, Războiul informaţional, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2006;
6. WALTZ, Eduard, Information Warfare: Principles and Operations, Artech House, Boston, 1998;
7. AJP-3.10, Allied Joint Doctrine for Information Operations, 2006;
8. FM 34-10-2, Intelligence and Electronic Warfare Equipment Handbook, Headquarters Department of the Army, Washington D.C.;
9. FM 34-1, Intelligence and Electronic Warfare Operations, Headquarters Department of the Army, Washington D.C.;
10. J.Pub. 3-13, „Joint Doctrine for Command and Control Warfare".

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

Elaborarea fişei disciplinei „Managementul ameninţărilor hibride în contextul securităţii cibernetice" a avut loc în urma discutării conţinutului disciplinei şi a cerinţelor practice cu specialişti şi practicieni din domeniu care îşi desfăşoară activitatea în sectorul public şi privat (manageri publici, funcţionari publici de conducere şi de execuţie, personal contractual etc.), dar şi pornind de la competenţele profesionale cerute de piaţa muncii (prin însuşirea noţiunilor teoretico-metodologice şi a aspectelor practice din cadrul disciplinei, masteranzii dobândesc cunoştinţe, în concordanţă cu competenţele parţiale cerute pentru ocupaţiile posibile prevăzute în Grila RNCIS).

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	- Să cunoască termenii de specialitate şi să	Examen scris	70%

	înţeleagă conceptele privind Managementul ameninţărilor hibride în contextul securităţii cibernetice şi interacţiunilor individului în spaţiul virtual; - Să cunoască şi să interpreteze strategiile persuasive şi tehnicile specifice; - Să caracterizeze teoriile ameninţărilor hibride; - Să explice principiile operaţiilor informaţionale - Să înţeleagă specificul procesului de realizare a acţiunilor ostile de influenţare - Să cunoască contextul procesual al managementului ameninţărilor hibride în contextul securităţii cibernetice şi să stabilească diferenţieri între acestea în vederea aplicării contramăsurilor - Să cunoască şi să înţeleagă etapele proiectării şi reproiectării unei strategii de management - Să identifice abordările decizionale pentru activitatea structurilor de specialitate - Să utilizeze spaţiul virtual pentru comunicarea specifică		
Seminar	• Realizarea temelor de seminar • Prezenţa la curs şi seminar	Evaluare continuă	30%
Laborator			
Proiect			
Standard minim de performanţă			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
19. 10. 2018	Dr. Mihai - Liviu Dănilă	Dr. Mihai - Liviu Dănilă

Data avizării în departament	Semnătura directorului de departament
12. 11. 2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21. 11. 2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Infracţiuni informatice în legislaţia penală română				
Titularul activităţilor de curs	Prof.univ.dr. Drăghici Vasile				
Titularul activităţilor de seminar	Prof.univ.dr. Drăghici Vasile				
Anul de studiu	1	Semestrul	2	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DOA

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	3	Curs	2	Seminar	1	Laborator	-	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	42	Curs	28	Seminar	14	Laborator	-	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	10
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	5
II d) Tutoriat	5
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	30
Total ore pe semestru (Ib+II+III+IV)	74
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	- Cunoaşterea şi înţelegerea conceptelor de criminalitate informatică ; - Cunoaşterea termenilor de specialitate definiţi în legislaţia penală ; - Cunoaşterea tipurilor de infracţiuni informatice incriminate de legislatia penală; - Implementarea metodologiei privind analiza teoretică şi practică a infracţiunilor informatice; - Înţelegerea principalelor direcţii de abordare în vederea prevenirii şi combaterii criminalităţii informatice; - Cunoaşterea şi înţelegerea instrumentelor internaţionale privind prevenirea şi combaterea criminalităţii

	informatice; - Cunoaşterea şi utilizarea transdiciplinară a unor principii şi mecanisme pentru prevenirea şi combaterea criminalităţii informatice; - Identificarea şi utilizarea mecanismelor de cooperare judiciară internaţională folosite în combaterea şi prevenirea criminalităţii informatice;
Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Prezentarea generală a reglementărilor internaţionale şi interne referitoare la criminalitatea informatică. Cunoaşterea tuturor tipurilor de infracţiuni în sfera criminalităţii informatice. Prevenirea şi combaterea infracţiunilor informatice

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
1. Elemente de drept penal – partea generală	4 ore	Prelegere orală	
2. Concept, trăsături, evoluţie – criminalitate informatică	2 ore	Prelegere orală	
3. Aspecte criminologice ale criminalităţii informatice	2 ore	Prelegere orală	
4. Prezentarea generală a reglementărilor internaţionale şi interne referitoare la criminalitatea informatică	2 ore	Prelegere orală	
5. Convenţia europeană a criminalităţii informatice – Budapesta 2001 şi modul de implementare a acesteia în legislaţia penală română	2 ore	Prelegere orală	
6. Fraude comise prin sisteme informatice şi mijloace de plată electronice	4 ore	Prelegere orală	
7. Falsul informatic	2 ore	Prelegere orală	
8. Infracţiuni contrasiguranţei şi integrităţii sistemelor şi datelor informatice	4 ore	Prelegere orală	
9. Pornografia infantilă	2 ore	Prelegere orală	
10. Alte fapte penale susceptibile a fi încadrate în sfera criminalităţii informatice	2 ore	Prelegere orală	
11. Cooperarea judiciară internaţională pentru prevenirea şi combaterea criminalităţii informatice	2 ore	Prelegere orală	

Bibliografie

1. Cod penal – Legea nr. 286/2009
2. Noul Cod de procedură penală – Legea nr. 135/2010
3. Vintilă Dogaru ş.a., Explicaţii ale Codului penal roman, parte general vol. I – III, Bucureşti, Editura Academiei Române, 2003
4. George Antoniu, Constantin, Tudorel Toader (coordonatori), Costică Bulai, Bogdan Nicolae Bulai, Constantin Duvac, Ioan Griga, Ion Ifrim, Gheorghe Ivan, Constantin Mitrache, Ioan Molnar, Ilie Pascu, Viorel Paşca, Ovidiu Predescu (autori), Explicaţiile noului cod penal, ISBN 978-606-673-338-0, Editura Universul Juridic, Bucureşti, 2015
5. Vasile Drăghici, Drept penal. Parte general, Ediţia III, Editura Pro-Universitaria, Bucureşti 2010
6. Alexandru Boroi, Drept penal. Parte special, Editura C.H. Beck, bucureşti 2016
7. Mariana Zainea, Raluca Simianu, Infracţiuni în domeniul informatic, Culegere de practică judiciară, Editura C.H.Beck , Bucureşti , 2009
8. Ghid introductiv pentru aplicarea dispoziţiilor legale referitoare la criminalitatea informatică, Bucureşti, 2004, proiect RITI dot-gov , www.riti-internews.ro, 2010
9. Dan Cimpoeru, Dreptul internetului, Ediţia 2, Editura C. H. Beck, Bucureşti 2013
10. Mihai Adrian ş.a., Infracţiuni prevăzute în legi penale speciale, Ediţia 2, Editura C. H. Beck, Bucureşti 2010
11. AnaMaria Trancă, Dumitru Cristian Trancă, Infracţiuni informatice în noul cod penal, Editura Universul Juridic , Bucureşti, 2014
12. Gheorghe Iulian Ioniţă, Infracţiuni din sfera criminalităţii informatice, Ediţia III revizuită şi adăugită, Universul Juridic, Bucureşti 2018

Aplicații (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observații
1. Definiția dreptului penal. Principii fundamentale de drept penal. Definirea infracțiunii. Concept sancțiuni	2 ore	problematizare, exercitiu	
2. Conceptul de criminalitate informatică caracteristici, evoluție. Factori care influențează evoluția criminalității informatice, amenințări actuale.	2 ore	problematizare, exercitiu	
3. Teorii criminologice privind subculturile criminalității informatice actuale. Tipurile de subculturi ale criminalității informatice actuale	2 ore	problematizare, exercitiu	
4.Convenția de la Berna 1886, Tratatul OMTI – Geneva 1996, regula UE 910/2014 al Parlamentului European și al Consiliului, 2014, Directiva 2009/24/CE/ 23.04.2009, Alte instrumente europene internaționale	2 ore	problematizare, exercitiu	
5. Adoptarea convenției europene privind criminalitatea informatică Budapesta 23.11.2001. Structura convenției. Protocolul additional referitor la incriminarea actelor de natură rasistă și xenofobă săvarșită prin intermediul sistemelor informatice	2 ore	problematizare, exercitiu	
6. Frauda informatică – art. 249 Cod Penal. Efectuarea de operațiuni financiaare în mod fraudulos art. 250 Cod Penal. Acceptarea operațiunilor financiare detectate în mod fraudulos art. 251 Cod Penal. Tentativa art. 252 Cod Penal.	2 ore	problematizare, exercitiu	
7. Accesul illegal la un sistem informatics art. 360 Cod Penal. Interceptarea ilegală a unei transmisii de date informatice art. 361 Cod Penal. Alterarea integrității datelor informatice art. 362 Cod Penal. Perturbarea funcționării sistelor informatice art. 363 Cod Penal. Transferul neautorizat de date informatice art. 364 Cod Penal. Operațiuni ilegale cu dispozitiv sau programe informatice.	2 ore	problematizare, exercitiu	

Bibliografie

1. Cod penal – Legea nr. 286/2009
2. Noul Cod de procedură penală – Legea nr. 135/2010
3. Vintilă Dongoroz ş.a., Explicații ale Codului penal roman, parte general vol. I – III, București, Editura Academiei Române, 2003
4. George Antoniu, Tudorel Toader (coordonatori), Costică Bulai, Bogdan Nicolae Bulai, Constantin Duvac, Ioan Griga, Ion Ifrim, Gheorghe Ivan, Constantin Mitrache, Ioan Molnar, Ilie Pascu, Viorel Pașca, Ovidiu Predescu (autori), Explicațiile noului cod penal, ISBN 978-606-673-338-0, Editura Universul Juridic, București, 2015
5. Vasile Drăghici, Drept penal. Parte general, Ediția III, Editura Pro-Universitaria, București 2010
6. Alexandru Boroi, Drept penal. Parte special, Editura C.H. Beck, bucureşti 2016
7. Mariana Zainea, Raluca Simion, Infracțiuni în domeniul informatic, Culegere de practică judiciară, Editura C.H.Beck , București , 2009
8. Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică, București, 2004, proiect RITI dot-gov , www.riti-internews.ro, 2010
9. Dan Cimpoeru, Dreptul internetului, Ediția 2, Editura C. H. Beck, București 2013
10. Mihai Adrian Hotca ş.a., Infracțiuni prevăzute în legi penale speciale, Ediția 2, Editura C. H. Beck, București 2010
11. AnaMaria Trancă, Dumitru Cristian Trancă, Infracțiuni informatice în noul cod penal, Editura Universul Juridic , București, 2014
12. Gheorghe Iulian Ioniță, Infracțiuni din sfera criminalității informatice, Ediția III revizuită și adăugită, Universul Juridic, București 2018

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

- Conținutul este orientat către aspecte practice ale tratării infracțiunilor de criminalitate informatică, în acord cu legislația penală română, precum și cu cele mai noi reglementări internaționale.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Să cunoască termenii de specialitate cu privire la infracţiunile informatice reglementate de codul penal; Să cunoască şi să interpreteze faptele care sunt incriminate de legislaţia penală română cu privire la criminalitatea informatică; Să explice tipurile de infracţiuni cibernetice; Să înţeleagă specificul faptelor penale susceptibile a fi încadrate în sfera criminalităţii informatice; Să cunoască reglementările europene şi internaţionale referitoare la criminalitatea informatică; Să cunoască metodele de cooperare judiciară internaţională pentru prevenirea şi combaterea criminalităţii informatice.	Examen scris	70%
Seminar	Realizarea temelor de seminar Prezenţa la seminar	Evaluare continuă	30%
Laborator			
Proiect			
Standard minim de performanţă			
• **Nota 5** Cunoaşterea tipurilor de infracţiuni şi fraude informatice. Realizarea unui referat cu privire la încadrarea unui tip de infracţiune de criminalitate informatică în acord cu codul penal şi procedură penală română.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
19.10.2018	Prof.univ.dr. Drăghici Vasile	Prof.univ.dr. Drăghici Vasile

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Cadrul naţional şi european de reglementare al securităţii cibernetice				
Titularul activităţilor de curs	Daniel Ioniţă				
Titularul activităţilor de seminar	Daniel Ioniţă				
Anul de studiu	1	Semestrul	2	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DC
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DL

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	2	Laborator	-	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	28	Laborator	-	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	29
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	15
II d) Tutoriat	10
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	64
Total ore pe semestru (Ib+II+III+IV)	122
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Să aibă cunoştinţe cu privire la elementele ale strategiei europene de securitate cibernetică, respectiv a celei naţionale Să cunoască domeniile de aplicare a prevederilor cadrului de reglementare în domeniul securităţii cibernetice Să cunoască care sunt obligaţiile operatorilor de servicii esenţiale şi a furnizorilor de servicii digitale Să cunoască modul de aplicare a securităţii cibernetice pentru porturi şi sisteme portuare

	Să cunoască modul de aplicare a securității cibernetice pentru nave Să poată să revizuiască tabloul măsurilor de securitate privind informația aplicabile organizației; Să poată întocmi studii, emite rapoarte de evoluție și progres, poate formula soluții și poate elabora strategii cu privire la rezolvarea unor incidente cibernetice, corelat cu cerințele de mediu, siguranță, securitate și sănătate specifice domeniului tehnologiei informației;
Competențe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităților lingvistice, a cunoștințelor de tehnologia informației și a comunicării pentru dezvoltarea personală si profesională, în scopul inserției pe piața muncii și al adaptării la dinamica cerințelor acesteia. Utilizarea eficientă a resurselor și tehnicilor de învățare, în scopul dezvoltării personale și profesionale continue în domeniul telecomunicațiilor și tehnologiei informaționale, operarea cu informații și tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe și demonstrarea abilităților de comunicare.

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

Obiectivul general al disciplinei	Cunoașterea cadrului de reglementare al securității cibernetice în vederea stabilirii modului de derulare al activităților curente în cadrul oricărei entități economico-administrative în conformitate și cu respectarea prevederilor legale din domeniul de referință.

8. **Conținuturi**

Curs	Nr. ore	Metode de predare	Observații
1. Organisme și organizații internaționale cu atribuții și responsabilități în domeniul securității cibernetice (ONU, UE, NATO, OSCE, ITU)	**4**	Prelegere orală	
2. Cadrul european de reglementare a securității cibernetice	**10**		
2.1 Actori și domenii de competență potrivit Strategiei europene de securitate cibernetică	2	Prelegere orală	
2.2 Directiva NIS – subiecți, criterii, praguri și activități obligatorii	2	Prelegere orală	
2.3 Capabilități europene de securitate cibernetică	6		
3. Cadrul național de reglementare a securității cibernetice	**10**	Prelegere orală	
3.1 Securitatea cibernetică componentă a securității naționale	2	Prelegere orală	
3.2 Asigurarea unui nivel comun de securitate a rețelelor și sistemelor informatice – prevederi legale referitoare la stabilirea subiecților, a atribuțiilor și măsurilor legale ce se impun	6	Prelegere orală	
3.3 Cadrul de reglementare a capabilităților de securitate cibernetică existente la nivel național	2	Prelegere orală	
4. Cooperarea în domeniul securității cibernetice – asociații profesionale, modele de cooperare și documente suport	**2**	Prelegere orală	
5. Instrumente financiare pentru derularea proiectelor de securitate cibernetică – europene și naționale	**2**	Prelegere orală	

Bibliografie

1. Strategia Europeană de securitate cibernetică
2. Directiva NIS
3. Strategia de Securitate cibernetică a României – HG 271/2013
4. Legea 362/2019
5. HG494/2011 – Organizarea și funcționarea CERT-RO
6. The European Union Agency for Network and Information Security (ENISA) regulation
7. Horizon Europe and Digital Europe Programme – instrumente financiare parte a Programului cadru multianual de finanțare al UE (MFF) a proiectelor din domeniul de referință la nivel european.

Aplicații (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observații
Seminar 1- Identificarea ariilor de competență a entităților din domeniul de referință potrivit Strategiei europene de securitate cibernetică	2	problematizare, exercitiu	
Seminar 2 - Identificarea ariilor de competență a entităților din domeniul de referință potrivit Strategiei de securitate cibernetică a României	2	problematizare, exercitiu	
Seminar 3 – Îmbunătățirea capabilităților de securitate cibernetică la nivel național	2	problematizare, exercitiu	
Seminar 4 – Domeniile de aplicare a prevederilor cadrului de	2	problematizare, exercitiu	

reglementare în domeniul securității cibernetice			
Seminar 5 - Identificarea operatorilor de servicii esențiale	2	problematizare, exercitiu	
Seminar 6 – Obligațiile Operatorilor de servicii esențiale și a furnizorilor de servicii digitale	2	problematizare, exercitiu	
Seminar 7 – Obligativitatea raportării incidentelor de Securitate cibernetică de către operatorii de servicii esențiale si furnizorii de servicii digitale.	2	problematizare, exercitiu	
Seminar 8 – Tipurile de incidente de Securitate cibernetică ce trebuie raportate autorităților naționale și entităților europene	2	problematizare, exercitiu	
Seminar 9 – Securitatea cibernetică în sectorul maritim	4	problematizare, exercitiu	
Seminar 10 – Securitatea cibernetică pentru porturi și sisteme portuare – abordare generala	4	problematizare, exercitiu	
Seminar 11 – Securitatea cibernetică a navelor - abordare generală	4	problematizare, exercitiu	

Bibliografie

1. Strategia Europeană de securitate cibernetică
2. Directiva NIS
3. Strategia de Securitate cibernetică a României – HG 271/2013
4. Legea 362/2019
5. HG494/2011 – Organizarea și funcționarea CERT-RO
6. The European Union Agency for Network and Information Security (ENISA) regulation
7. Horizon Europe and Digital Europe Programme – instrumente financiare parte din Programul cadru multianual de finanțare al UE (MFF) a proiectelor din domeniul de referință la nivel european.

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

- Conținutul este orientat către aspecte practice ale legislației în domeniul de referință în vederea identificării celor mai bune practici de derulare a activităților cu respectarea prevederilor legale.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Să cunoască ariile de competență a entităților din domeniul de referință potrivit Strategiei europene de securitate cibernetică, respectiv a celei naționale Să cunoască domeniile de aplicare a prevederilor cadrului de reglementare în domeniul securității cibernetice Să cunoască care sunt obligațiile Operatorilor de servicii esențiale și a furnizorilor de servicii digitale Să cunoască modul de aplicare a securității cibernetice pentru porturi și sisteme portuare Să cunoască modul de aplicare a securității cibernetice pentru nave	Examen scris	70%
Seminar	• Realizarea temelor de seminar • Prezența la curs și seminar	Evaluare continuă	30%
Standard minim de performanță			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
17.10.2018	Daniel Ioniță	Daniel Ioniță

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra
Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Vulnerabilităţile tehnologiilor utilizate în Internet, analiză malware şi IT Forensic				
Titularul activităţilor de curs	Conf.univ.dr.ing.GABRIEL RAICU				
Titularul activităţilor de seminar	Conf.univ.dr.ing.GABRIEL RAICU				
Anul de studiu	2	Semestrul	1	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DA
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	5	Curs	2	Seminar	-	Laborator	2	Proiect	1
I b) Totalul de ore pe semestru din planul de învăţământ	70	Curs	28	Seminar	-	Laborator	28	Proiect	14

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	15
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	39
II d) Tutoriat	10
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	74
Total ore pe semestru (Ib+II+III+IV)	144
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Poate să utilizeze în mod corespunzător instrumentele tehnice specializate de evaluare a securităţii sistemelor informatice; Poate să realizeze securitatea bazelor de date, securitatea în faţa viruşilor informatici, smart card-uri identifice; Cunoaşte modul de control al securităţii accesului, controlul accesului la resurse, securitatea prin parole, drepturi, restricţii, privilegii, autentificarea utilizatorilor, metode de autentificare, certificate;

	Ştie să aplice prevederile şi procedurile legale pentru investigarea incidentelor de securitate cibernetică; Ştie să utilizezea în mod corect instrumentele de colectare a probelor digitale;
Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Cursul îşi propune să ofere cunoştinţele teoretice şi deprinderile practice necesare pentru a identifica rapid şi a răspunde la diferite tipuri de atacuri cibernetice. Acest curs construieşte o bază solidă pentru analiza codului malware, folosind o varietate de aplicaţii de monitorizare a sistemului şi a reţelei, aplicaţii de dezasamblare, debug şi multe alte instrumente. Cursul oferă instrumentele de răspuns în situaţia producerii unui atac cibernetic, adică devin necesare răspunsurile la întrebările "5W" (Who, What, When, Where, Why?).

8. **Conţinuturi**

Curs	**Nr. ore**	**Metode de predare**	**Observaţii**
Modul I. Noţiuni introductive a. Definiţii şi istoric aplicaţii malware b. Tipuri de fişiere şi modalităţi de rulare (fişiere executabile, scripturi, fişiere web, compilatoare, interpretoare, stagii intermediare) c. Clasificare malware d. Tehnici de propagare ale aplicaţiilor malware e. Vectori de atac şi infecţie f. Incident Response g. Analiză malware şi Reverse engineering - generalităţi h. Dezasamblare şi Decompilare i. Antivirus - generalităţi j. Importanţa unui timeline al evenimentelor în cazul unui incident	2	Prelegere orală	
Modul II. Tehnici de analiză malware a. Instalare laborator de analiză malware şi sandbox b. Sisteme de operare c. Sisteme de fişiere d. Arhitectura calculatoarelor e. Limbajul de asamblare f. Structura PE (Portable Executable) g. Windows API h. Aplicaţii utilizate în procesul de analiză malware i. Analiza caracteristicilor statice j. Analiză comportamentală k. Sandbox şi Honeypot l. Analiză statică şi dinamică avansate (analiza codului şi debugging)	2	Prelegere orală	
Modul III. Inginerie inversă - Aplicaţii executabile a. Concepte de bază b. Funcţii de asamblare c. Control Flow d. API Patterns în malware e. Stack f. Metode de protecţie utilizate de aplicaţiile malware (packing, obfuscare, metode anti-reverse, etc.) g. 64-bit code	2	Prelegere orală	
Modul IV. Analiză scripturi, documente şi fişiere web a. Analiză fişiere web (php, javascript)	2	Prelegere orală	

b. Analiză log-uri web c. Deobfuscare scripturi d. Analiză documente PDF maliţioase e. Analiză macro/swf din documente Office f. Analiză documente RTF			
Modul V. Analiză memorie a. Înţelegerea modului de funcţionare al memoriei b. Dump de fişiere din memorie c. Analiză memorie (achiziţie, analiză) d. Debug pentru executabile protejate de packere e. Injectare cod şi API Hooking	2	Prelegere orală	
Modul VI. Analiză Trafic a. Research - adrese de domeniu, adrese IP b. Malware networking (topologii, DGA, tunneling) c. Snort, Wireshark	2	Prelegere orală	
Modul VII. Automatizare şi hunting a. Surse online de hunting b. Automatizare c. Indicatori de compromitere (IoCs) d. Reguli YARA, yarGen şi Loki	2	Prelegere orală	
Modul VIII IT Forensics	2	Prelegere orală	
Modul IX. Achiziţia datelor de pe dispozitivele de stocare a. Hardware (LogicCube, Tableau, etc) b. Software (FTK Imager, EnCase, DD, Paladin, LiveBoot) c. Prin reţea (F-Response, Netcat, GRR)	2	Prelegere orală	
Modul X. Tehnici şi instrumente folosite pentru achiziţia memoriei RAM de pe toate sistemele de operare a. Windows (Magnet, FTK Imager, Memdump, DumpIT) b. Linux (LiME- Linux Memory Extractor)	2	Prelegere orală	
Modul XI. Analiza memoriei RAM a. Analiza fişierelor Pagefile.sys, Hiberfil.sys, Swapfile.sys b. Extragerea fişierelor shimcache si prefatch c. Extragerea artefactelor utilizând Volatility, Rekall, Redline d. Analiza conexiunilor efectuate de sistemul de calcul (connscan, sockets, connections, netscan) e. Analiza proceselor extrase din memoria RAM (Pslist, Pstree, Psscan, memdump) f. Analiza codului injectat în memoria RAM (malfind, ldrmodules) g. Extragerea informaţiilor de interes din regiştri prin intermediul plugin-urilor (Hivelist, Hivedump, Printkey, Userassist, Hashdump) h. Automatizarea procesului de analiză a memoriei RAM prin folosirea programelor MemGator si Voldiff	2	Prelegere orală	
Modul XII. Analiza fişierelor de jurnalizare de pe sistemele de operare a. Windows Event Logs i. System Event Logs ii. Application Event Logs iii. Security Event Logs b. Linux Logs i. OS Logs (messages.log, daemon.log, dmsg, security, cron, kern.log) ii. Apache Logs (acces.log, error.log) iii. Autentificare (auth.log, wtmp.log, lastlog.log, btmp) iv. Mysql Database (mysqld.log)	2	Prelegere orală	
Modul XIII. Analiza artefactelor de tip forensics de pe sistemele de operare a. Analiza regiştrilor b. Analiza utilizatorilor c. Analiza conexiunilor la reţea	2	Prelegere orală	

d. Analiza dispozitivelor USB e. Analiza de tip timeline f. Analiza volum shadow copy			
Modul XIV. Tehnici de identificare a metodelor antiforensics a. Sistemul de fişiere NTFS b. Anomalii ale fişierului timeline c. Fişiere şterse, chei de regiştri d. Timestamp alterat	2	Prelegere orală	

Bibliografie

Bază de date cu site-urile mari de CTF-uri: https://www.wechall.net/
şi write-ups cu toate CTF-urile: https://github.com/ctfs
Practical Malware Analysis: The Hands-On Guide to Dissection Malicious Software (Michael Sikorski, Andrew Honig)
•The IDA PRO Book (Chris Eagle)
•SANS GIAC610 – Reverse-Engineering Malware
•yara.readthedocs.io/en/v3.8.1
https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
•https://www.sans.org/reading-room
•https://www.forensicfocus.com/
•https://www.dfir.training/
•https://forensiccontrol.com/wp-content/uploads/2018/08/Free-Computer-Forensic-Software.pdf
•https://aboutdfir.com/
•http://windowsir.blogspot.com/

Aplicaţii (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observaţii
Clasificare malware. Tehnici de propagare ale aplicaţiilor malware. Vectori de atac şi infecţie	2	problematizare, exercitiu	
Tehnici de analiză malware	2	problematizare, exercitiu	
Metode de protecţie utilizate de aplicaţiile malware (packing, obfuscare, metode anti-reverse, etc.)	2	problematizare, exercitiu	
Analiză scripturi, documente şi fişiere web	2	problematizare, exercitiu	
Dump de fişiere din memorie. Analiză memorie (achiziţie, analiză)	2	problematizare, exercitiu	
Analiză Trafic	2	problematizare, exercitiu	
Surse online de hunting	2	problematizare, exercitiu	
Indicatori de compromitere (IoCs). Reguli YARA, yarGen şi Loki	2	problematizare, exercitiu	
Achiziţia datelor de pe dispozitivele de stocare	2	problematizare, exercitiu	
Tehnici şi instrumente folosite pentru achiziţia memoriei RAM de pe toate sistemele de operare	2	problematizare, exercitiu	
Analiza memoriei RAM	2	problematizare, exercitiu	
Analiza fişierelor de jurnalizare de pe sistemele de operare	2	problematizare, exercitiu	
Analiza artefactelor de tip forensics de pe sistemele de operare	2	problematizare, exercitiu	
Tehnici de identificare a metodelor antiforensics	2	problematizare, exercitiu	

Bibliografie

Bază de date cu site-urile mari de CTF-uri: https://www.wechall.net/
şi write-ups cu toate CTF-urile: https://github.com/ctfs
Practical Malware Analysis: The Hands-On Guide to Dissection Malicious Software (Michael Sikorski, Andrew Honig)
•The IDA PRO Book (Chris Eagle)
•SANS GIAC610 – Reverse-Engineering Malware
•yara.readthedocs.io/en/v3.8.1
https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
•https://www.sans.org/reading-room
•https://www.forensicfocus.com/
•https://www.dfir.training/
•https://forensiccontrol.com/wp-content/uploads/2018/08/Free-Computer-Forensic-Software.pdf
•https://aboutdfir.com/
•http://windowsir.blogspot.com/

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

- Conţinutul este orientat către aspecte practice ale tehnologiilor de lucru sub apă, în concordanţă cu cele mai noi tehnici care sunt aplicate în întreaga lume.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Are cunoştinţe în : Clasificare malware. Tehnici de propagare ale aplicaţiilor malware. Vectori de atac şi infecţie Tehnici de analiză malware Metode de protecţie utilizate de aplicaţiile malware (packing, obfuscare, metode anti-reverse, etc.) Analiză scripturi, documente şi fişiere web Surse online de hunting Indicatori de compromitere (IoCs). Reguli YARA, yarGen şi Loki Achiziţia datelor de pe dispozitivele de stocare Tehnici şi instrumente folosite pentru achiziţia memoriei RAM de pe toate sistemele de operare Analiza memoriei RAM	Examen practic	60%
Seminar			
Laborator	Poate face identificarea şi clasificare unui atac cibernetic	Evaluare continuă	40%
Proiect			
Standard minim de performanţă			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
12.10.2018	Conf.univ.dr.ing.GABRIEL RAICU	Conf.univ.dr.ing.GABRIEL RAICU

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Protecţia datelor şi legislaţia privind securitatea				
Titularul activităţilor de curs	Prof.univ.dr. Popa George				
Titularul activităţilor de seminar	Prof.univ.dr. Popa George				
Anul de studiu	2	Semestrul	1	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DC
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	-	Laborator	2	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	-	Laborator	28	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	25
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	25
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	30
II d) Tutoriat	8
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	88
Total ore pe semestru (Ib+II+III+IV)	146
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• Studenţii se vor prezenta la prelegeri, seminarii/laboratoare cu materialele necesare pt preluarea datelor/informatiilor transmise de profesor, avand telefoanele mobile inchise. De asemenea, nu vor fi tolerate convorbirile în timpul cursului, nici părăsirea de către studenţi a sălii de curs în vederea preluării apelurilor telefonice personale; Nu se vor tolera intarzieri si activitati care ar putea afecta buna desfasurare a cursurilor/laboratoarelor/seminariilor.
Desfăşurare aplicaţii	Seminar	• Studenţii se vor prezenta la prelegeri, seminarii/laboratoare cu materialele necesare pt preluarea datelor/informatiilor transmise de profesor, avand telefoanele mobile inchise. De asemenea, nu vor fi tolerate convorbirile în timpul cursului, nici părăsirea de către studenţi a sălii de curs în vederea preluării apelurilor telefonice personale; Nu se vor tolera intarzieri si activitati care ar putea afecta buna desfasurare a cursurilor/laboratoarelor/seminariilor.

	Laborator	• Studenții se vor prezenta la prelegeri, seminarii/laboratoare cu materialele necesare pt preluarea datelor/informatiilor transmise de profesor, avand telefoanele mobile inchise. De asemenea, nu vor fi tolerate convorbirile în timpul cursului, nici părăsirea de către studenți a sălii de curs în vederea preluării apelurilor telefonice personale; Nu se vor tolera intarzieri si activitati care ar putea afecta buna desfasurare a cursurilor/laboratoarelor/seminariilor.
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	• Dobandirea cunostintelor necesare angajării cu succes şi dovedirea unei inalte eficiente pe piaţa muncii capacitatea dovedită de a selecta, combina şi utiliza adecvat cunoştinţe, abilităţi şi alte achiziţii (valori şi atitudini) simultan cu imbunatatirea capacitatii de analiza si sinteza • Capacitatea de organizare si de coordonare accentuata. • Cunoştinţe generale de baza, comunicare scrisa si orala in termeni de specialitate. • Capacitatea de a soluţiona probleme de specialitate. • Capacitatea de a lua decizii in domeniul de specialitate. • Capacitatea de a susţine public un discurs coerent, logic si retoric in domeniul respectiv.
Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor aferente protectiei datelor cu caracter personal şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul de referinta, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Să se familiarizeze cu principalele curente și abordări din domeniul acestei discipline si sa stapaneasca regulile legale din acest domeniu.

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
1. Regulamentul UE 2016/679 privind protectia datelor cu caracter personal	2	Prelegere orală	
2. Principalele obligatii pentru operatorii de date in aplicarea Regulamentului UE 2016/679	2	Prelegere orală	
3. Cartografierea datelor cu caracter personal	2	Prelegere orală	
4. Principalele riscuri la adresa datelor cu caracter personal	2	Prelegere orală	
5.Drepturile persoanelor vizate de prelucrarea datelor	2	Prelegere orală	
6.Evaluarea impactului asupra protectiei datelor cu caracter personal	2	Prelegere orală	
7.Responsabilul cu protectia datelor cu caracter personal	2	Prelegere orală	
8.Sarcinile responsabilului cu protectia datelor cu caracter personal	2	Prelegere orală	
9.Principiile prelucrarii datelor cu caracter personal	2	Prelegere orala	
10. Autoritatea Nationala de Suprveghere	2	Prelegere orala	
11.Legea nr.190/18 iulie 2018 privind prelucrarea datelor personale	2	Prelegere orala	
12. Legea nr.190/18 iulie 2018 privind prelucrarea datelor personale	2	Prelegere orala	
13.Plenarele Comitetului European pt protectia datelor	2	Prelegere orala	
14.Plenarele Comitetului European pt protectia datelor	2	Prelegere orală	

Bibliografie

1. Regulamentul UE privind protectia datelor – Regulamentul UE 2016/679
2. Legea nr.190/18 iulie 2018 privind prelucrarea datelor personale
3. Ghidurile ANSDCP privind protectia datelor cu caracter personal

Aplicaţii (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observaţii
1. Dezbateri, prezentare practica privind Regulamentul UE 2016/679 privind protectia datelor personale	2	problematizare, exercitiu	
2. Dezbateri, prezentare practica privind pricipalele obligatii privind protectia datelor personale	2	problematizare, exercitiu	

3. Dezbateri, prezentari practice privind cartografierea datelor cu caracter personal	2	problematizare, exercitiu	
4. Dezbateri, prezentari practice principalele riscuri la adresa datelor cu caracter personal	2	problematizare, exercitiu	
5. Dezbateri, prezentari practice privind drepturile persoanelor vizate de prelucrare de date	2	problematizare, exercitiu	
6. Dezbateri, prezentari practice privind evaluarea impactului asupra datelor personale	2	problematizare, exercitiu	
7. Dezbateri, prezentari practice privind responsabilul cu protectia datelor cu caracter personal	2	problematizare, exercitiu	
8. Dezbateri, prezentari practice privind sarcinile si atributiile DPO	2	problematizare, exercitiu	
9. Dezbateri, prezentari practice privind principiile prelucrarii datelor cu caracter personal	2	problematizare, exercitiu	
10. Dezbateri, prezentari practice privind ANSPDC	2	problematizare, exercitiu	
11. Dezbateri, prezentari practice privind Legea 190/18	2	problematizare, exercitiu	
12. Dezbateri, prezentari practice privind Legea 190/18	2	problematizare, exercitiu	
13. Dezbateri, prezentari practice privind practicile UE	2	problematizare, exercitiu	
14. Dezbateri, prezentari practice privind practicile UE	2	problematizare, exercitiu	
Bibliografie			
Regulamentul UE privind protectia datelor – Regulamentul UE 2016/679 Legea nr.190/18 iulie 2018 privind prelucrarea datelor personale Ghidurile ANSDCP privind protectia datelor cu caracter personal			

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

- În vederea schițării conținuturilor, alegerii metodelor de predare/învățare titularul disciplinei a participat la mai multe întâlniri cu specialisti si alte cadre didactice din domeniu, titulare în alte instituții de învățământ superior. Întâlnirea a vizat identificarea nevoilor și așteptărilor asociatiilor profesionale, angajatorilor din domeniu și coordonarea cu alte programe similare din cadrul altor instituții de învățământ superior.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Cunoaşterea terminologiei utilizate in cadrul acestei disciplinei, capacitatea de utilizare adecvată a noţiunilor, insuşirea raporturilor juridice specifice, cunoasterea institutiilor juridice din acest doemniu, intelegerea mecanismelor si rapoartelor juridice din acest domeniu si in domeniile conexe.	Examen scris	70%
Seminar			
Laborator	Însuşirea problematicii tratate la curs şi laborator. Capacitatea de a utiliza corect metodele, modelele şi notiunile predate la curs.	Evaluare continua	30%
Proiect			
Standard minim de performanţă			
• **Nota 5** Cunoaşterea în linii mari a notiunilor, institutiilor si a raporturilor juridice specifice acestei discipline.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
15.10.2018	Prof.univ.dr. jur. Popa George	Prof.univ.dr. jur. Popa George

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Răicu Alexandra
Data aprobării în Consiliul academic	**Semnătura decanului**
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Aplicarea tehnologiei informației și comunicațiilor pentru a monitoriza și controla procesele fizice				
Titularul activităţilor de curs	Prof.univ.dr.ing. Zăgan Remus				
Titularul activităţilor de seminar	Prof.univ.dr.ing. Zăgan Remus				
Anul de studiu	2	Semestrul	1	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DC
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	2	Laborator	-	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	28	Laborator	-	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	40
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	20
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	20
II d) Tutoriat	8
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	88
Total ore pe semestru (Ib+II+III+IV)	146
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Să cunoască termenii de specialitate şi să înţeleagă conceptele privind tehnologiile industriei 4.0; Să cunoască și să interpreteze strategii și tehnici specifice mecanismelor de răspuns la crize; Să cunoască și să înțeleagă sistemele cyber-fizice pentru a monitoriza și controla procesele fizice. Să aplice tehnologia informației și comunicațiilor pentru a digitiza informația și integra sisteme la concepție, dezvoltare, fabricație și utilizarea produselor.

	Să cunoască noi tehnologii software pentru modelare, simulare, virtualizare și fabricație digitală. Să înțeleagă specificul noilor tehnologii ICT, precum Big Data, AI(inteligenta artificiala) sau IoT(Internet of Things). Să utilizeze spațiul virtual pentru o conduită specifică care să îi asigure un nivel corespunzător de securitate și diminuare a crizelor în spațiul cyber. Să valorifice cunoștințele acumulate în vederea integrării în viitoarea activitate profesională și viața socială. Să participe la elaborarea proiectelor de desfășurare a diferitelor activități profesionale la nivelul sistemului public / privat.
Competențe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităților lingvistice, a cunoștințelor de tehnologia informației și a comunicării pentru dezvoltarea personală si profesională, în scopul inserției pe piața muncii și al adaptării la dinamica cerințelor acesteia. Utilizarea eficientă a resurselor și tehnicilor de învățare, în scopul dezvoltării personale și profesionale continue în domeniul telecomunicațiilor și tehnologiei informaționale, operarea cu informații și tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe și demonstrarea abilităților de comunicare.

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

Obiectivul general al disciplinei	Cunoașterea și înțelegerea problematicii managementului securității cibernetice în industria 4.0. Cunoașterea și înțelegerea sistemelor și tehnologiilor aferente industriei 4.0. Identificarea și abordarea riscurilor cibernetice emergente în ecosistemul industrial. Evaluarea riscurilor, monitorizarea amenințărilor cibernetice, planul de răspuns la atacurile cibernetice

8. Conținuturi

Curs	Nr. ore	Metode de predare	Observații
Modulul 1: Introducere în industria 4.0 1.1 Diferitele revoluții industriale 1.2 Digitalizarea și economia în rețea 1.3 Evoluțiile în domeniu industriei 4.0 în lume 1.4 Tendințe ale datelor industriale mari și analiza predictivă pentru transformarea inteligentă a afacerilor	2	Prelegere orală	
Modulul 2: Drumul către industria 4.0 2.1 Internetul obiectelor (Internetul de obiecte) și Internetul interactiv al lucrurilor (IIoT) și Internetul serviciilor 2.2 Producția inteligentă 2.3 Dispozitivele inteligente și produsele 2.4 Logistica inteligentă 2.5 Orașele inteligente	3	Prelegere orală	
Modulul 3: Sisteme și tehnologii aferente industriei 4.0 3.1 Sisteme ciberfizice 3.2 Automatizarea robotului și robotul colaborativ 3.3 Sistemul de suport pentru industria 4.0 3.4 Computere mobile	5	Prelegere orală	
Modulul 4: Rolul datelor, informațiilor, cunoștințelor și colaborării în cadrul organizațiilor viitoare 4.1 Vizualizarea bazată pe resurse a unei firme 4.2 Date ca o resursă nouă pentru organizații 4.3 Utilizarea și schimbul de cunoștințe în cadrul organizațiilor 4.4 Cloud Computingul și industria 4.0	3	Prelegere orală	
Modulul 5: Studii de caz IoT	2	Prelegere orală	
Modulul 6: Business issues în industria 4.0 6.1 Oportunități și provocări 6.2 Viitorul resursei umane și competențelor acestora în industria 4.0 6.3 Strategii pentru a concura într-o industrie 4.0	4	Prelegere orală	
Modulul 7: Riscuri inerente în sistemele de control industrial	3	Prelegere orală	
Modulul 8: Securitatea versus producție	2	Prelegere orală	
Modul 9: Identificarea și abordarea riscurilor cibernetice emergente în ecosistemul industrial	2	Prelegere orală	
Modul 10: Evaluarea riscurilor, monitorizarea amenințărilor cibernetice,	2	Prelegere orală	

planul de răspuns la atacurile cibernetice			

Bibliografie

Arnold, C.; Kiel, D.; Voigt, K.-I. How the industrial internet of things changes business models in different manufacturing industries. Int. J. Innov. Manag. 2016, 20, 1640015.
Bordeleau, F.-E.; Mosconi, E.; Santa-Eulalia, L.A. Business Intelligence in Industry 4.0: State of the art and research opportunities. In Proceedings of the 51st Hawaii International Conference on System Sciences, Waikoloa Village, HI, USA, 2–6 January 2018; pp. 3944–3953.
Eric D. Knapp and Raj Samani , Applied Cyber Security and the Smart Grid, ISBN 978-1-59749-998-9, 2013 Elsevier
David Willson, Cyber Security Awareness for CEOs and Management, ISBN 978-0-12-804754-5, Elsevier, 2016
Lee, J.; Kao, H.-A.; Yang, S. Service innovation and smart analytics for industry 4.0 and big data environment. Procedia CIRP 2014
Oesterreich, T.D.; Teuteberg, F. Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry. Comput. Ind. 2016, 83, 121–139
PwC. Industry 4.0-Building the Digital Enterprise; PricewaterhouseCoopers LLP: Berlin, Germany, 2016; Available online: https://www.google.com/search?q=PwC+%282016%29%3A+Industry+4.0+-+Building+the+digital+enterprise.+PricewaterhouseCoopers+LLP+Hermann%2C+M.%2C+Pentek%2C+T.%2C+Otto%2C+B.+%282016%29%3A+Design+principles+for+industrie+4.0+scenarios.+In+System+Sciences+%28HICSS%29%2C+2016+49th+Hawaii+International+Conference+on+%28p.+392&ie=utf-8&oe=utf-8&client=firefox-b

Aplicații (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observații
Internetul obiectelor (Internetul de obiecte) și Internetul interactiv al lucrurilor (IIoT) și Internetul serviciilor	2	problematizare, exercitiu	
Sisteme și tehnologii aferente industriei 4.0	4	problematizare, exercitiu	
Rolul datelor, informațiilor, cunoștințelor și colaborării în cadrul organizațiilor viitoare	4	problematizare, exercitiu	
Viitorul resursei umane și competențelor acestora în industria 4.0	2	problematizare, exercitiu	
Riscuri inerente în sistemele de control industrial	4	problematizare, exercitiu	
Identificarea și abordarea riscurilor cibernetice emergente în ecosistemul industrial	4	problematizare, exercitiu	
Evaluarea riscurilor, monitorizarea amenințărilor cibernetice, planul de răspuns la atacurile cibernetice	4	problematizare, exercitiu	
Studii de caz IoT	4	problematizare, exercitiu	

Bibliografie

Arnold, C.; Kiel, D.; Voigt, K.-I. How the industrial internet of things changes business models in different manufacturing industries. Int. J. Innov. Manag. 2016, 20, 1640015
Bordeleau, F.-E.; Mosconi, E.; Santa-Eulalia, L.A. Business Intelligence in Industry 4.0: State of the art and research opportunities. In Proceedings of the 51st Hawaii International Conference on System Sciences, Waikoloa Village, HI, USA, 2–6 January 2018; pp. 3944–3953.
Oesterreich, T.D.; Teuteberg, F. Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry. Comput. Ind. 2016, 83, 121–139

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

- Conținutul este orientat către aspecte practice ale tehnologiilor de lucru sub apă, în concordanță cu cele mai noi tehnici care sunt aplicate în întreaga lume.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Să cunoască termenii de specialitate și să înțeleagă conceptele privind tehnologiile industriei 4.0; Să cunoască și să interpreteze strategii și tehnici specifice mecanismelor de răspuns la crize; Să cunoască și să înțeleagă sistemele cyber-fizice	Examen scris	70%

	pentru a monitoriza și controla procesele fizice. Să aplice tehnologia informației și comunicațiilor pentru a digitiza informația și integra sisteme la concepție, dezvoltare, fabricație și utilizarea produselor. Să cunoască noi tehnologii software pentru modelare, simulare, virtualizare și fabricație digitală. Să înţeleagă specificul noilor tehnologii ICT, precum Big Data, AI(inteligenta artificiala) sau IoT(Internet of Things). Să utilizeze spațiul virtual pentru o conduită specifică care să îi asigure un nivel corespunzător de securitate și diminuare a crizelor în spațiul cyber.		
Seminar	Prezenţă la curs şi atitudine proactive la activităţile de seminarizare.	Evaluare continuă	30%
Laborator			
Proiect			
Standard minim de performanţă			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	Prof.univ.dr.ing. Zăgan Remus	Prof.univ.dr.ing. Zăgan Remus

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Etică și integritate academică				
Titularul activităţilor de curs	Conf. univ. dr. Surugiu Felicia				
Titularul activităţilor de seminar	-				
Anul de studiu	2	Semestrul	1	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DC
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	1	Curs	1	Seminar	-	Laborator	-	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	14	Curs	14	Seminar	-	Laborator	-	Proiect	-

II Distribuţia fondului de timp pe semestru:	Ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	50
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	25
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	15
II d) Tutoriat	
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	90
Total ore pe semestru (Ib+II+III+IV)	106
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• Sala cu video-proiector
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	-
Competenţe transversale	**C1.** Îndeplinirea sarcinilor profesionale cu identificarea exactă a obiectivelor de realizat, a unor factori potenţiali de risc, a resurselor disponibile, a aspectelor economico-financiare, condiţiilor de finalizare a acestora, etapelor de lucru, timpului de lucru şi termenelor de realizare aferente. **C2** Distribuirea rolurilor şi responsabilităţilor într-o echipă, asigurarea coordonării şi controlului activităţii

	echipei pentru atingerea obiectivelor prevăzute **C3**. Utilizarea eficientă a surselor informaţionale şi a resurselor de comunicare şi formare profesională continuă pentru îndeplinirea planului personal de dezvoltare a carierei

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Disciplina permite familiarizarea studenţilor cu problemele, conceptele şi aspectele privind etica şi deontologia academică, precum şi cu moralitatea politicilor întâlnite în mediul de afaceri care pot să provoace imense daune si prejudicii indivizilor, comunităţilor şi mediului.

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
Cap. 1 Cercetarea ştiinţifică şi standarde privind evaluarea calităţii academice de către aracis	2	Prelegere, dezbatere, slide-uri ppt.	
Cap.2 Etica universitară si codurile de etică universitare	2		
Cap.3 Integritatea academică	2		
Cap.4 Integritatea în sistemul de învătământ si cercetarea stiintifică	2		
Cap.5 Buna conduită în cercetarea stiintifică	2		
Cap.6 Plagiatul si identificarea plagiatului în lucrările cu caracter stiintific	2		
Cap.7 Programe utilizate in vederea stabilirii gradului de similitudine in lucrarile stiintifice	2		

Bibliografie

1. Elena Emilia STEFAN , Etica afacerilor si integritate academica, Editura Pro Universitaria 2018
2. Avram, Laurenţia, Etica afacerilor, Suport de curs, Univ. Spiru Haret, Câmpulung Muscel, 2008
3. Bihan, Christine, Marile probleme ale eticii, Institutul European Iaşi, 1997
4. Macintyre, Alasdaire, Tratat de morală, Humanitas, 1998
5. Miroiu, Adrian (ed.), Etica aplicată, Editura Alternative, Bucureşti, 1995
6. Miroiu, Mihaela, Blebea Nicolae, Gabriela, Introducere în etica profesională, Editura Trei, 2001
7. Sârbu, Tănase, Etică: valori şi virtuţi morale, Editura Societăţii Academice „Matei Teiu Botez", Iaşi, 2005

Bibliografie minimală

1. Elena Emilia STEFAN , Etica afacerilor si integritate academica, Editura Pro Universitaria 2018

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

Disciplina Etică şi integritate academică conţine noţiuni teoretice, metode şi tehnici de lucru care sunt solicitate de societate, comunitatea epistemică, asociaţiile profesionale şi angajatori în transporturi.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Întocmirea şi prezentarea de referate cu teme specifice disciplinei	Examen grilă	100%
Seminar			
Laborator			
Proiect			
Standard minim de performanţă			
• Cunoştinţe pentru nota 5 – 50 % din materia predată			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	Conf. univ. dr. Felicia SURUGIU	

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf. univ. dr. ing. Alexandra Raicu

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf. univ. dr. ing. Ion Omocea

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Practică III				
Titularul activităţilor de curs					
Titularul activităţilor de seminar					
Anul de studiu	2	Semestrul	1	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	7	Curs	-	Seminar	-	Laborator	-	Proiect	7
I b) Totalul de ore pe semestru din planul de învăţământ	98	Curs	-	Seminar	-	Laborator	-	Proiect	98

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	
II d) Tutoriat	
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	
Total ore pe semestru (Ib+II+III+IV)	100
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	Cunoştinţe de bază în domeniul ştiinţelor inginereşti
Competenţe	Utilizarea adecvată a cunoştinţelor tehnice în propunere de soluţii

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Utilizarea principiilor generale de securitate şi aplicarea regulilor de securitate la nivelul componentelor sistemului informatic. Dobândirea unui spirit atitudinal-afectiv pozitiv faţă de amploarea şi complexitatea prospectiv-ştiinţifică oferită de domeniul securităţii cibernetice.
Competenţe transversale	Întărirea capacităţilor de lucru în colectiv, comunicare cu alte colective tehnice în vederea analizării şi identificării soluţiilor constructive.

	Dezvoltarea unui mod de comunicare clar şi concis în cadrul prezentării proprilor poziţii. Adaptarea la situaţii noi de lucru. Adaptarea la un colectiv nou.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Corelarea şi aplicarea cunoştinţelor teoretice în activitatea practică specifică masterului.
	Cunoaşterea instituţiei şi activităţii unde se desfăşoară stagiul de practică. Cunoaşterea şi aprofundarea elementelor practice specific soluţionării documentaţiei tehnice. Aprofundarea cunoştinţelor dobândite prin activităţi practice.

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
Bibliografie			

Conţinut programa de practică	Nr. ore	Metode de predare	Observaţii
Se vor urmă cu predilecţie următoarele aspecte specifice : Cunoaştere şi înţelegerea terminologiei utilizate in cadrul protectiei datelor personale, capacitatea de utilizare adecvată a noţiunilor, insuşirea raporturilor juridice specifice, cunoasterea institutiilor juridice din acest doemniu, intelegerea mecanismelor si rapoartelor juridice din acest domeniu si in domeniile conexe. Capabilitatea de a monitoriza, detecta, preîntâmpina, minimiza si raporta acţinui specifice atacurilor cibernetice, care exploatează factorul uman, în vederea infectării/disruperii unui ehipament/sistem sau retea computerizată. Cunoasterea şi aplicarea metodelor de prevenire, minimizare şi combatere riscurilor de securitate cibernetica din perspeciva factorului uman.	98	Studierea documentaţiei tehnice puse la dispoziţie de către firma unde se face stagiul de practică.	
Bibliografie			

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

- Disciplina oferă studenţilor posibilitatea de a pune în practică în interiorul unei instituţii de pe piaţa muncii cunoştinţele şi competenţele dobândite specific programului masteral.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Practică	Evaluare finală (proiect + apreciere unitate de practică) întrebări şi răspunsuri în faţa comisiei	Prezentarea portofoliului elaborat ca urmare a efectuării stagiului de practică	100%
Standard minim de performanţă			

- **Nota 5**
  Pentru a obţine nota minimă de promovare studentul trebuie să prezinte următoarele documente :
  - Convenţia de practică parafată de compania unde a efectuat stagiul de practică şi
  - Caietul de practică

  Nota propusă de tutorele de practică trebuie să fie de minim 5, iar studentul trebuie să demonstreze în cadrul colocviului cunoştinţe minimale despre aspectele specifice securităţii cibernetice.
- **Nota 10**
  Nota maximă poate fi obţinută în condiţiile în care studentul dovedeşte la colocviu, cunoştinţe solide, documentate, argumentate şi de detaliu, are un caiet de practică complet şi tutorele de practică a apreciat activitatea pe durata stagiului de practică drept Foarte Bună.

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018		

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Calculul evolutiv în tehnologia informaţiei				
Titularul activităţilor de curs	Lector.univ.dr.Simona Dinu				
Titularul activităţilor de seminar	Lector.univ.dr.Simona Dinu				
Anul de studiu	2	Semestrul	2	Tipul de evaluare	E

Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară	DA
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)	DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	-	Laborator	2	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	-	Laborator	28	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	20
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	24
II d) Tutoriat	10
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	64
Total ore pe semestru (Ib+II+III+IV)	122
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	• Cursuri de programare calculatoare, algoritmi şi structuri de date
Competenţe	• Abilităţi de programare în C++

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	- Înţelegerea principiilor fundamentale ale Calculului Evolutiv; - Formularea unei probleme practice ca o problemă de căutare/optimizare în vederea soluţionării utilizând Algoritmi Evolutivi; - Compararea diferitelor abordări evolutive în soluţionarea problemelor care sunt dificil de abordat prin algoritmi de optimizare tradiţionali.
Competenţe	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a

transversale	abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Cursul prezintă concepte specifice, tehnici, algoritmi şi metode moderne de calcul, inspirate din procesele evolutive şi biologice. În particular, cursul va aborda componenta de bază a Calculului Evolutiv şi anume Algoritmii Genetici - tehnici de optimizare stohastică, bazate pe metafora evolutivă şi adaptarea speciilor la mediul înconjurător. Aplicaţiile Calculului Evolutiv pentru rezolvarea unor probleme practice din domeniul IT şi Telecomunicaţii vor fi implementate în limbajul C++.

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
Calculul Inteligent (CI) – o nouă paradigmă în domeniul IT: principii de bază, direcţii de studiu, exemple şi posibilităţi de utilizare a tehnicilor CI în proiecte şi aplicaţii din lumea reală.	2	Prelegere orală	
Modelarea si rezolvarea problemelor, optimizare: conceptul de optimizare; formularea unei probleme de optimizare, aspecte generale şi caracteristici particulare ale problemelor de optimizare, tipuri de probleme de optimizare.	2	Prelegere orală	
Algoritmi şi aplicaţii ale calculului "soft computing" versus calculul convenţional - "hard computing" pentru rezolvarea unor probleme complexe	2	Prelegere orală	
Tehnici Evolutive de optimizare - domenii de cercetare şi aplicaţii: Algoritmi Genetici, Strategii Evolutive, Programare Evolutivă, Programare Genetică (prima parte).	2	Prelegere orală	
Tehnici Evolutive de optimizare - domeniile de cercetare şi aplicaţii: Algoritmi Genetici, Strategii Evolutive, Programare Evolutivă, Programare Genetică (continuare).	2	Prelegere orală	
Algoritmi Genetici: concepte de bază, structură şi particularităţi de implementare.	2	Prelegere orală	
Algoritmi Genetici: metode şi operatori avansaţi; noi perspective de implementare.	2	Prelegere orală	
Rezolvarea problemelor de optimizare cu restricţii folosind Algoritmi Genetici.	2	Prelegere orală	
Controllere fuzzy utilizate pentru configurarea parametrilor unui Algoritm Evolutiv	2	Prelegere orală	
Modele de Algoritmi Evolutivi pentru optimizare multicriterială	2	Prelegere orală	
Analiza complexităţii: metrici pentru evaluarea performanţelor unui Algoritm Evolutiv	2	Prelegere orală	
Meta-euristici hibride - noi abordări de optimizare în spaţii complexe	2	Prelegere orală	
Modele paralele şi distribuite ale Algoritmilor Evolutivi	2	Prelegere orală	
Alte metode de calcul inspirate din natură: calculul de tip Swarm („Swarm Intelligence") bazat pe studiul comportamentelor colectivelor cu organizare socială din lumea animală (colonii de furnici, stoluri de păsări, bancuri de peşti, colonii de albine, colonii de bacterii).	2	Prelegere orală	

Bibliografie

1. Alba, E. şi alţii " Optimization Techniques For Solving Complex Problems", Ed. Wiley, 2009.
2. Dumitrescu, D. "Algoritmi genetici şi strategii evolutive: aplicaţii în inteligenţa artificială şi în domenii conexe", Ed. Albastră, 2006.
3. Eremia, M. şi alţii "Tehnici de inteligenţă artificială în conducerea sistemelor electroenergetice", Ed. Agir, 2006.
4. Gen, M., Yu, X. "Introduction to Evolutionary Algorithms", Ed. Springer, 2010.
5. Yang, X. şi alţii " Bio-Inspired Computation in Telecommunications", Ed. Elsevier, 2015.

Aplicații (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observații
Calculul Inteligent (CI) – o nouă paradigmă în domeniul IT: principii de bază, direcții de studiu, exemple și posibilități de utilizare a tehnicilor CI în proiecte și aplicații din lumea reală.	2	problematizare, exercitiu	
Modelarea si rezolvarea problemelor, optimizare: conceptul de optimizare; formularea unei probleme de optimizare, aspecte generale și caracteristici particulare ale problemelor de optimizare, tipuri de probleme de optimizare.	2	problematizare, exercitiu	
Algoritmi și aplicații ale calculului "soft computing" versus calculul convențional - "hard computing" pentru rezolvarea unor probleme complexe	2	problematizare, exercitiu	
Tehnici Evolutive de optimizare - domenii de cercetare și aplicații: Algoritmi Genetici, Strategii Evolutive, Programare Evolutivă, Programare Genetică (prima parte).	2	problematizare, exercitiu	
Tehnici Evolutive de optimizare - domeniile de cercetare și aplicații: Algoritmi Genetici, Strategii Evolutive, Programare Evolutivă, Programare Genetică (continuare).	2	problematizare, exercitiu	
Algoritmi Genetici: concepte de bază, structură și particularități de implementare.	2	problematizare, exercitiu	
Algoritmi Genetici: metode și operatori avansați; noi perspective de implementare.	2	problematizare, exercitiu	
Rezolvarea problemelor de optimizare cu restricții folosind Algoritmi Genetici.	2	problematizare, exercitiu	
Controllere fuzzy utilizate pentru configurarea parametrilor unui Algoritm Evolutiv	2	problematizare, exercitiu	
Modele de Algoritmi Evolutivi pentru optimizare multicriterială	2	problematizare, exercitiu	
Analiza complexității: metrici pentru evaluarea performanțelor unui Algoritm Evolutiv	2	problematizare, exercitiu	
Meta-euristici hibride - noi abordări de optimizare în spații complexe	2	problematizare, exercitiu	
Modele paralele și distribuite ale Algoritmilor Evolutivi	2	problematizare, exercitiu	
Alte metode de calcul inspirate din natură: calculul de tip Swarm („Swarm Intelligence") bazat pe studiul comportamentelor colectivelor cu organizare socială din lumea animală (colonii de furnici, stoluri de păsări, bancuri de pești, colonii de albine, colonii de bacterii).	2	problematizare, exercitiu	

Bibliografie

1. Chambers, L.D. "The Practical Handbook of Genetic Algorithms: Applications", Ed. Chapman & Hall, 2001.
2. Ghosh, A. și alții "Advances in Evolutionary Computing: Theory and Applications", Ed. Springer, 2003.
3. Popa, R. "Genetic Algorithms in Applications", Ed. InTech, 2012.
4. Roeva, O. "Real-World Applications of Genetic Algorithms", Ed. InTech, 2012.

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

- Conținutul este orientat către aspecte practice ale calculului evolutiv, în concordanță cu cele mai noi descoperiri în domeniu.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Însușirea noțiunilor și aspectelor teoretice și practice prezentate în cadrul cursului	Examen scris	70%
Seminar			
Laborator	Teme și scenarii de lucru	Evaluare continuă	30%

Standard minim de performanţă
• **Nota 5**

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	Lector.univ.dr.Simona Dinu	Lector.univ.dr.Simona Dinu

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra
Data aprobării în Consiliul academic	**Semnătura decanului**
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Tehnici şi instrumente de evaluare a securităţii cibernetice, hacking etic şi audit de securitate				
Titularul activităţilor de curs	Lector.univ.dr.Simona Dinu				
Titularul activităţilor de seminar	Lector.univ.dr.Simona Dinu				
Anul de studiu	2	Semestrul	2	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	-	Laborator	2	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	-	Laborator	28	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	20
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	24
II d) Tutoriat	10
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	64
Total ore pe semestru (Ib+II+III+IV)	122
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Poate analiza gradul în care sistemul de securitate existent în organizaţie răspunde strategiei de securitate privind informaţia, ameninţărilor şi riscurilor identificate; Poate să proiecteze tabloul măsurilor de securitate privind informaţia aplicabile organizaţiei; Poate sintetiza şi interpreta informaţiile tehnice, legislative şi comerciale şi le poate aplica în mod creativ în procesele de proiectare a procedurilor de securitate cibernetică;

	Poate evalua şi aprecia calitativ şi cantitativ incidentele de securitate cibernetică complexe şi poate interpreta rezultatele. Poate implementa proceduri de testare / verificare a conformităţii cu obiectivele din strategia de securitate privind informaţia; Poate elabora teste etalon pentru controlul aplicării măsurilor de securitate şi pentru evaluarea rezultatelor; Poate elabora setul de criterii de evaluare a gradului de îndeplinire a obiectivelor din strategia de Securitate; Poate să propună machete / şabloane etalon pentru monitorizarea aplicării măsurilor de securitate
Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Cursul prezintă etapele esenţiale ale procesului de audit, alături de tehnici de auditare şi instrumentele prin care un atacator poate compromite un sistem informatic

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
Modul I Planificarea, definirea domeniului de audit şi tehnici de recunoaştere - Principii ale auditului de securitate cibernetică - Tipuri de audit de securitate - Metodologia procesului de audit şi reguli de angajare - Definirea domeniului de testare - Procesul de recunoaştere - Extragere informaţii folosind motoare de căutare - Raportare	5	Prelegere orală	
Modul II Scanare şi culegere de informaţii - Scopul culegerilor de informaţii şi tipuri de scanări - Scanare de porturi - Identificare sisteme de operare şi servicii active - Identificare vulnerabilităţi Web şi de Reţea	6	Prelegere orală	
Modul III Exploatare - Categorii de exploit-uri - Exploatarea vulnerabilităţilor Web şi reţea	6	Prelegere orală	
Modul IV Post-Exploatare şi Pivotare - Colectare de fişiere şi informaţii de pe terminalele compromise - Powershell şi Bash pentru pentesting - Atacuri asupra parolelor: definiţii şi metodologii	6	Prelegere orală	
Modul V Hacking etic - Înţelegerea conceptului de hacking etic - Analiza vulnerabilităţilor, Scanarea reţelelor, Ameninţări Malware, Social engineering	5	Prelegere orală	

Bibliografie

Information Security Forum , "Information Risk Assessment Methodology 2," 2016 , https://www.securityforum.org/tool/information-risk-assessment-methodologyiram2/
Stouffer, K., Falco, J. and Scarfone, K. Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). Special Publication 800-82 (Final Public Draft), NIST, Gaithersburg, MD, September 29, 2008.
Scarfone, K., Souppaya, M., Cody, A. and Orebaugh, A. Technical Guide to Information Security Testing and Assessment. Special Publication 800-115, NIST, Gaithersburg, MD, September 2008.
Ethical Hacking: Student Courseware, Ec-Council ISBN 0972936211
Michael Simpson , Hands-On Ethical Hacking and Network Defense, ISBN: 0-619-21708-1 , 2006
Ankit Fadia , The Unofficial Guide to Ethical Hacking, Second Edition, ISBN: 1-59863-062-8 , 2006
https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_tutorial.pdf

Aplicaţii (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observaţii
Principii ale auditului de securitate cibernetică	4	problematizare, exercitiu	
Metodologia procesului de audit	4	problematizare, exercitiu	
Scopul culegerilor de informaţii şi tipuri de scanări	4	problematizare, exercitiu	
Identificare sisteme de operare şi servicii active	4	problematizare, exercitiu	
Exploatarea vulnerabilităţilor Web şi de reţea	4	problematizare, exercitiu	
Colectare de fişiere şi informaţii de pe terminalele compromise	4	problematizare, exercitiu	
Hacking etic – comportament şi analiză	4	problematizare, exercitiu	

Bibliografie

Information Security Forum , "Information Risk Assessment Methodology 2," 2016 , https://www.securityforum.org/tool/information-risk-assessment-methodologyiram2/
Stouffer, K., Falco, J. and Scarfone, K. Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). Special Publication 800-82 (Final Public Draft), NIST, Gaithersburg, MD, September 29, 2008.
Scarfone, K., Souppaya, M., Cody, A. and Orebaugh, A. Technical Guide to Information Security Testing and Assessment. Special Publication 800-115, NIST, Gaithersburg, MD, September 2008.
Ethical Hacking: Student Courseware, Ec-Council ISBN 0972936211
Michael Simpson , Hands-On Ethical Hacking and Network Defense, ISBN: 0-619-21708-1 , 2006
Ankit Fadia , The Unofficial Guide to Ethical Hacking, Second Edition, ISBN: 1-59863-062-8 , 2006
https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_tutorial.pdf

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

- Conţinutul este orientat către aspecte practice ale auditului de securitate cibernetică, în concordanţă cu cele mai noi tehnici care sunt aplicate în întreaga lume.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Are cunoştinţe despre: - Principii ale auditului de securitate cibernetică şi Metodologia procesului de audit - Identificare sisteme de operare şi servicii active - Hacking etic – comportament şi analiză	Examen scris	70%
Seminar			
Laborator	Teme şi scenarii de lucru	Evaluare continuă	30%
Standard minim de performanţă			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	Lector.univ.dr.Simona Dinu	Lector.univ.dr.Simona Dinu

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra
Data aprobării în Consiliul academic	**Semnătura decanului**
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Mecanisme de răspuns la crize din perspectiva Cyber Security				
Titularul activităţilor de curs	Dr. Mihai - Liviu Dănilă				
Titularul activităţilor de seminar	Dr. Mihai - Liviu Dănilă				
Anul de studiu	2	Semestrul	2	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	4	Curs	2	Seminar	-	Laborator	2	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	56	Curs	28	Seminar	-	Laborator	28	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	20
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	24
II d) Tutoriat	10
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	64
Total ore pe semestru (Ib+II+III+IV)	122
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	• Cunoaşterea unei limbi străine

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• Masteranzii trebuie să respecte normele de conduită academică; • Masteranzii nu se vor prezenta la prelegeri cu telefoanele mobile deschise; • Nu va fi tolerată întârzierea masteranzilor la curs; • Data susţinerii examenului se va stabili de titular de comun acord cu masteranzii.
Desfăşurare aplicaţii	Seminar	• Trebuie să respecte normele de conduită academică; • Nu se vor prezenta la seminare cu telefoanele mobile deschise; • Nu va fi tolerată întârzierea la seminare; • Termenele de predare şi susţinere a lucrărilor de seminar sunt stabilite de titular de comun acord cu masteranzii. Nu se vor accepta cererile de amânare a acestora pe motive altfel decât obiectiv întemeiate. De asemenea, nu se acceptă cererile doar de predare a temelor de seminar fără ca acestea să se

		acceptă cererile doar de predare a temelor de seminar fără ca acestea să se susțină în fața colegilor.
	Laborator	•
	Proiect	•

6. Competențe specifice acumulate

Competențe profesionale	• Să cunoască termenii de specialitate și să înțeleagă conceptele privind Competitive & Business Intelligence din perspectiva Cyber Security, performanțele de calificare a unui angajat pentru relaționarea corectă în spațiul economic/comercial și social; • Să cunoască și să interpreteze strategii și tehnici specifice mecanismelor de răspuns la crize; • Să caracterizeze teoriile managementului crizelor din perspectiva Cyber; • Să aplice principiile de Competitive & Business Intelligence și mecanisme de răspuns la crize din perspectiva Cyber Security pentru analiza organizației • Să cunoască și să înțeleagă etapele proiectării și reproiectării unei strategii de Competitive & Business Intelligence din perspectiva Cyber Security, în interiorul propriei organizații • Să identifice abordările decizionale pentru activitatea structurilor de management a mecanismelor de răspuns la crize din perspectiva Cyber Security • Să înțeleagă specificul procesului de Competitive & Business Intelligence și mecanisme de răspuns la crize în cadrul organizației în care activează • Să cunoască funcțiile procesului de securitate cibernetică și să stabilească diferențieri între tipurile de riscuri în vederea aplicării acestora în Competitive & Business Intelligence și mecanisme de răspuns la criză • Să utilizeze spațiul virtual pentru o conduită specifică care să îi asigure un nivel corespunzător de securitate și diminuare a crizelor în spațiul cyber • Să valorifice cunoștințele acumulate în vederea integrării în viitoarea activitate profesională și viața socială; • Să participe la elaborarea proiectelor de desfășurare a diferitelor activități profesionale la nivelul sistemului public / privat; • Să participe la elaborarea proiectelor de cercetare științifică în domeniile de Competitive & Business Intelligence și cele specifice mecanismelor de răspuns la crize din perspectiva Cyber Security.
Competențe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităților lingvistice, a cunoștințelor de tehnologia informației și a comunicării pentru dezvoltarea personală si profesională, în scopul inserției pe piața muncii și al adaptării la dinamica cerințelor acesteia. Utilizarea eficientă a resurselor și tehnicilor de învățare, în scopul dezvoltării personale și profesionale continue în domeniul telecomunicațiilor și tehnologiei informaționale, operarea cu informații și tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe și demonstrarea abilităților de Competitive & Business Intelligence și de răspuns la crize din perspectiva Cyber Security.

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

Obiectivul general al disciplinei	Cunoașterea și înțelegerea problematicii managementului amenințărilor hibride în contextul securității cibernetice în administrația publică / mediul antreprenorial / societăți capital privat, a practicilor specifice în organizații, a procedurilor și mecanismelor de management a amenințărilor hibride pentru realizarea securității cibernetice cu alte entități specifice organizației din care face parte, compararea structurii și funcționalității compartimentelor de profil, elaborarea unei strategii de securitate cibernetică și management a amenințărilor hibride

8. Conținuturi

Curs	Nr. ore	Metode de predare	Observații
1. Competitive & Business Intelligence – conceptualizare, definire	4	Prelegere orală	2 ședințe x 2hrs
2. Competitive & Business Intelligence în teoria managementului	2	Prelegere orală	
2.1 Competitive Intelligence și managementul organizației	2	Prelegere orală	
2.2 Business Intelligence și managementul corporatist	2	Prelegere orală	
3. Caracteristicile de intelligence ale mediului de business competitiv	2	Prelegere orală	
4. Analiza specifică mediului de Competitive & Business Intelligence	4	Prelegere orală	2 ședințe x 2hrs
5. Aspecte juridice ale Competitive & Business Intelligence sfera cyber	2	Prelegere orală	

6. Managementul crizelor – definire, conceptualizări, școli de gândire	4	Prelegere orală	2 ședințe x 2hrs
7. Mecanisme de răspuns la crize specifice mediului cyber	4	Prelegere orală	2 ședințe x 2hrs
8. Aspecte juridice ale mecanismelor de răspuns la crize	2	Prelegere orală	

Bibliografie

1. John F. Prescott, Stephen H. Miller, Proven Strategies in Competitive Intelligence: Lessons from the Trenches, Society of Competitive Intelligence Professionals – 2002;
2. Jay Liebowitz, *Strategic Intelligence, Business Intelligence, Competitive Intelligence, and Knowledge Management*, Auerbach Publications, ebook, 2006;
3. Craig Fleisher, Babette Bensoussan, *STRATEGIC AND COMPETITIVE ANALYSIS: Methods and Techniques for Analyzing Business Competition*, Prentice Hall, 2002;
4. TOFFLER, Alvin şi TOFFLER, Heidi, Război şi antirăzboi. Supraviețuirea în zorii secolului XXI, Editura Antet, 1995;
5. LOWENTHAL, Mark M., Intelligence-from secrets to policy, Third edition, CQ Press, 2006;
6. TOPOR, Sorin, Războiul informațional, Editura Universității Naționale de Apărare „Carol I", București, 2006.

Aplicații (Seminar / **laborator** / proiect)	Nr. ore	Metode de predare	Observații
1. Competitive Intelligence – definire, impact societal	4	problematizare, exercițiu	2 ședințe x 2hrs
2. Business Intelligence – impact global, vectorul corporatist	4	problematizare, exercițiu	2 ședințe x 2hrs
3. Impactul de intelligence în piața globală - specificități regionale ale mediului de business	4	problematizare, exercițiu	2 ședințe x 2hrs
4. Modalități de analiză specifice mediilor de business competitiv din perspectiva cyber security	4	problematizare, exercițiu	2 ședințe x 2hrs
5. Tipologii de criză – situațiile speciale de urgență	4	problematizare, exercițiu	2 ședințe x 2hrs
6. Mecanisme generale de răspuns la crize ale actorilor globali	4	problematizare, exercițiu	2 ședințe x 2hrs
7. Mecanisme specifice mediului cyber de răspuns la crize	4	problematizare, exercițiu	2 ședințe x 2hrs

Bibliografie

1. https://www.consilium.europa.eu/ro/policies/ipcr-response-to-crises/;
2. Crăciun, Ion, *Prevenirea conflictelor și managementul crizelor*, Ed. UNAp, „CAROL I", București, 2006;
3. Jay Liebowitz, *Strategic Intelligence, Business Intelligence, Competitive Intelligence, and Knowledge Management*, Auerbach Publications, ebook, 2006;
4. Badrus, Ghe., Globalitate și Management, ed. All Beck, București, 2000;
5. KORKISCH, Friedrich W., NATO Gets „Better Intelligence", Strategy Paper 1-2010, Vienna, 2010;
6. www.stratfor.com.

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

Elaborarea fișei disciplinei „Competitive & Business Intelligence şi mecanisme de răspuns la crize din perspectiva Cyber Security" a avut loc în urma discutării conținutului disciplinei şi a cerințelor practice cu specialiști şi practicieni din domeniu care îşi desfăşoară activitatea în sectorul public şi privat (manageri publici, funcționari publici de conducere şi de execuție, personal contractual etc.), dar şi pornind de la competențele profesionale cerute de piața muncii (prin însuşirea noțiunilor teoretico-metodologice şi a aspectelor practice din cadrul disciplinei, masteranzii dobândesc cunoştințe, în concordanță cu competențele parțiale cerute pentru ocupațiile posibile prevăzute în Grila RNCIS).

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	- Să cunoască termenii de specialitate şi să înțeleagă conceptele privind Competitive & Business Intelligence şi mecanisme de răspuns la crize din perspectiva Cyber Security; - Să cunoască şi să interpreteze strategiile persuasive şi tehnicile specifice; - Să caracterizeze teoriile Competitive & Business Intelligence din perspectiva Cyber Security; - Să explice principiile Competitive & Business Intelligence din perspectiva Cyber Security - Să înțeleagă specificul procesului de realizare a mecanismelor de răspuns la crize din perspectiva Cyber Security	Examen scris	70%

	- Să cunoască contextul procesual de Competitive & Business Intelligence și să stabilească diferențieri între acestea în vederea aplicării lor în piață - Să cunoască și să înțeleagă etapele proiectării și reproiectării unei strategii de răspuns la criză - Să identifice abordările decizionale pentru activitatea structurilor de specialitate - Să utilizeze spațiul virtual pentru o comunicarea specifică		
Seminar	• Realizarea temelor de seminar • Prezența la curs și seminar	Evaluare continuă	30%
Laborator			
Proiect			
Standard minim de performanță			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
12.10.2018.	Dr. Mihai - Liviu Dănilă	Dr. Mihai - Liviu Dănilă

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Practică IV				
Titularul activităţilor de curs					
Titularul activităţilor de seminar					
Anul de studiu	2	Semestrul	2	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	3	Curs	-	Seminar	-	Laborator	-	Proiect	3
I b) Totalul de ore pe semestru din planul de învăţământ	42	Curs	-	Seminar	-	Laborator	-	Proiect	42

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	
II d) Tutoriat	
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	
Total ore pe semestru (Ib+II+III+IV)	44
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	Cunoştinţe de bază în domeniul ştiinţelor inginereşti
Competenţe	Utilizarea adecvată a cunoştinţelor tehnice în propunere de soluţii

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Utilizarea principiilor generale de securitate şi aplicarea regulilor de securitate la nivelul componentelor sistemului informatic. Dobândirea unui spirit atitudinal-afectiv pozitiv faţă de amploarea şi complexitatea prospectiv-ştiinţifică oferită de domeniul securităţii cibernetice.
Competenţe transversale	Întărirea capacităţilor de lucru în colectiv, comunicare cu alte colective tehnice în vederea analizării şi identificării soluţiilor constructive.

	Dezvoltarea unui mod de comunicare clar şi concis în cadrul prezentării proprilor poziţii. Adaptarea la situaţii noi de lucru. Adaptarea la un colectiv nou.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Corelarea şi aplicarea cunoştinţelor teoretice în activitatea practică specifica masterului.
	Cunoaşterea instituţiei şi activităţii unde se desfăşoară stagiul de practică. Cunoaşterea şi aprofundarea elementelor practice specific soluţionării documentaţiei tehnice. Aprofundarea cunoştinţelor dobândite prin activităţi practice.

8. Conţinuturi

Curs	Nr. ore	Metode de predare	Observaţii
Bibliografie			

Conţinut programa de practică	Nr. ore	Metode de predare	Observaţii
Se vor urmă cu predilecţie următoarele aspecte specifice : Să poată analiza şi identifica modificările apărute în modelul ameninţărilor şi al vulnerabilităţilor. Să poată să revizuiască tabloul măsurilor de securitate privind informaţia aplicabile organizaţiei; Să poată întocmi studii, emite rapoarte de evoluţie şi progres, poate formula soluţii şi poate elabora strategii cu privire la rezolvarea unor incidente cibernetice, corelat cu cerinţele de mediu, siguranţă, securitate şi sănătate specifice domeniului tehnologiei informaţiei Să aibă cunoştinţe avansate de securitatea serverelor şi a clienţilor, segmentarea reţelelor; Să aibă cunoştinţe avansate de securitatea aplicaţiilor, controlul modificărilor; Să aibă cunoştinţe avansate privind accesul şi securitatea accesului in Internet şi Intranet; Să aibă cunoştinţe avansate de securitatea sistemelor de operare şi a serviciilor;	42	Studierea documentaţiei tehnice puse la dispoziţie de către firma unde se face stagiul de practică.	
Bibliografie			

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

- Disciplina oferă studenţilor posibilitatea de a pune în practică în interiorul unei instituţii de pe piaţa muncii cunoştinţele şi competenţele dobândite specific programului masteral.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Practică	Evaluare finală (proiect + apreciere unitate de practică) întrebări şi răspunsuri în faţa comisiei	Prezentarea portofoliului elaborat ca urmare a efectuării stagiului de practică	100%
Standard minim de performanţă			
• **Nota 5** Pentru a obţine nota minimă de promovare studentul trebuie să prezinte următoarele documente : - Convenţia de practică parafată de compania unde a efectuat stagiul de practică şi - Caietul de practică Nota propusă de tutorele de practică trebuie să fie de minim 5, iar studentul trebuie să demonstreze în cadrul colocviului cunoştinţe minimale despre aspectele specifice securităţii cibernetice			

Nota maximă poate fi obţinută în condiţiile în care studentul dovedeşte la colocviu, cunoştinţe solide, documentate, argumentate şi de detaliu, are un caiet de practică complet şi tutorele de practică a apreciat activitatea pe durata stagiului de practică drept Foarte Bună.

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
17.10.2018		

Data avizării în departament	Semnătura directorului de departament
12-11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Practica pentru pregătirea lucrării de dizertaţie				
Titularul activităţilor de curs					
Titularul activităţilor de seminar					
Anul de studiu	2	Semestrul	2	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DO

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	8	Curs	-	Seminar	-	Laborator	-	Proiect	8
I b) Totalul de ore pe semestru din planul de învăţământ	112	Curs	-	Seminar	-	Laborator	-	Proiect	112

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	20
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	30
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	10
II d) Tutoriat	10
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	70
Total ore pe semestru (Ib+II+III+IV)	184
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	Cunoştinţe de bază în domeniul ştiinţelor inginereşti
Competenţe	Utilizarea adecvată a cunoştinţelor tehnice în propunere de soluţii

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Utilizarea principiilor generale de securitate şi aplicarea regulilor de securitate la nivelul componentelor sistemului informatic. Cunoştinţe avansate de aplicare instrumente, programe utilitare pentru: supravegherea reţelelor, supravegherea traficului de date, monitorizarea performanţelor sistemelor şi a reţelelor, detectarea alterării performanţelor. Cunoştinţe avansate de aplicare a standardelor specifice: ISO 17799, ISO 27000

	Cunoştinţe avansate privind instrumente, programe utilitare pentru: supravegherea reţelelor, supravegherea traficului de date, monitorizarea performanţelor sistemelor şi a reţelelor, detectarea alterării performanţelor; Cunoştinţe avansate privind instrumente, programe utilitare pentru verificarea conformităţii sistemelor cu machete etalon de securitate Poate să proiecteze tabloul măsurilor de securitate privind informaţia aplicabile organizaţiei; Poate să elaboreze şi să implementeze proceduri noi de securitate şi le îmbunătăţeşte pe cele existente
Competenţe transversale	Asumarea cu responsabilitate, a principiilor, normelor şi valorilor profesionale în executarea sarcinilor de serviciu – stabilirea obiectivelor, identificarea resusrselor, dimensionarea judicioasă a etapelor de lucru, stabilirea raţională a termenelor. Autoevaluarea competenţelor şi a nivelului de pregătire profesională, conştinetizarea necesităţii formării profesionale continue şi durabile, identificarea oportunităţilor de dezvoltare personal şi profesională şi utilizarea lor eficientă (cursuri de formare continua, cursuri on-line şi de învăţământ la distanţă, portaluri de internet, aplicaţii software de specialitate, etc). Abilitatea de a lucra independent şi/sau în echipă pentru a rezolva probleme în diverse contexte profesionale

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	În principiu, temele de disertaţie trebuie să abordeze problematica aferentă procesului de pregătire pe parcurs. Ele se constituie în studii aplicative teoretice şi practice privind soluţionarea problemelor de securitate cibernetică. Prin temele alese absolvenţii se înscriu în activitatea de cercetare a departamentului coordonator în conformitate cu reperele din planurile de cercetare ale acestuia şi/sau în activitatea de cercetare individuală (în conformitate cu propunerile proprii acceptate).
Obiective specifice	Conexarea cunoştinţelor teoretice şi tehnico-aplicative dobândite pe parcursul anilor de studii cu activitatea desfăşurată în sectoarele productive / administrative. Cunoaşterea stadiului actual în domeniu şi a tuturor informaţiilor de natură specifică în domeniul securităţii cibernetice. Dobândirea deprinderii de a utiliza corect noţiunile teoretice, adaptate condiţiilor concrete din practică.

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
Bibliografie			

Stagiu de pregătire	Nr. ore	Metode de predare	Observaţii
Se vor urmă cu predilecţie următoarele aspecte specifice : 1. Fundamente privind analiza şi identifica modificările apărute în modelul ameninţărilor şi al vulnerabilităţilor. 2. Fundamentarea privind întocmirea de studii, emite rapoarte de evoluţie şi progres, formularea de soluţii şi elaborarea de strategii cu privire la rezolvarea unor incidente cibernetice, corelat cu cerinţele de mediu, siguranţă, securitate şi sănătate specifice domeniului tehnologiei informaţiei. 3. Fundamentarea privind tabloul măsurilor de securitate privind informaţia aplicabile organizaţiei. 4. Fundamente privind tematica specifică lucrării de disertaţie. 5. Fundamente privind tehnica de calcul asistată de calculator specifică lucrării de disertaţie. 6. Sintetizarea documentaţiei şi a informaţiilor cumulate. 7. Finalizarea componentelor teoretice, applicative şi grafice a lucrării de disertaţie.	112	Studiu individual	
Bibliografie			

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

- Disciplina oferă studenţilor posibilitatea de a pune în practică în interiorul unei instituţii de pe piaţa muncii cunoştinţele şi competenţele dobândite specific programului masteral.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Practică	Evaluare finală (proiect + apreciere unitate de practică) întrebări şi răspunsuri în faţa comisiei	Prezentarea portofoliului elaborat ca urmare a efectuării stagiului de practică	100%
Standard minim de performanţă			
• **Nota 5** Cunoaşterea, înţelegerea şi explicarea principiilor de bază în analizarea şi identificarea modificărilor apărute în modelul ameninţărilor şi al vulnerabilităţilor. Întocmirea de studii, emite rapoarte de evoluţie şi progres, formularea de soluţii şi elaborarea de strategii cu privire la rezolvarea unor incidente cibernetice, corelat cu cerinţele de mediu, siguranţă, securitate şi sănătate specifice domeniului tehnologiei informaţiei.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018		

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Echipamente radio definite prin software				
Titularul activităţilor de curs	Ș.L.univ. dr. ing. Mirel PĂUN				
Titularul activităţilor de seminar	Ș.L. univ.dr. ing. Mirel PĂUN				
Anul de studiu	2	Semestrul	1	Tipul de evaluare	C
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DOA

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	3	Curs	2	Seminar	-	Laborator	1	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	42	Curs	28	Seminar	-	Laborator	14	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	50
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	6
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	6
II d) Tutoriat	
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	62
Total ore pe semestru (Ib+II+III+IV)	106
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	• Antene și propagare. Semnale și sisteme. Prelucrarea digitală a semnalelor. Analiza și sinteza circuitelor.
Competenţe	C4.1. Formularea, dezvoltarea și implementarea creativă de soluții pentru probleme tipice și elementare, în contexte bine definite, asociate proiectării și utilizării echipamentelor radio definite prin software.

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• Nu este cazul
Desfăşurare aplicaţii	Seminar	•
	Laborator	• Prezenţa obligatorie
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	C4. Proiectarea şi optimizarea subsistemelor complexe și sistemelor de radiocomunicaţii.
Competenţe transversale	CT1. Îndeplinirea sarcinilor profesionale cu identificarea exactă a obiectivelor de realizat, a unor factori potenţiali de risc, a resurselor disponibile, a aspectelor economico-financiare, condiţiilor de finalizare a

	acestora, etapelor de lucru, timpului de lucru şi termenelor de realizare aferente.

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Disciplina asigură studenţilor o pregătire generală în domeniul echipamentelor radio definite prin software.
	Obiectivele specifice asigurate de disciplină se referă la prezentarea principalelor arhitecturi utilizate de către echipamentele radio definite prin software precum și analiza și caracterizarea acestora în funcție de domeniile de aplicabilitate.

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
1. Noțiuni introductive • 1.1. Definiție • 1.2. Utilitate • 1.3. Schema de principiu a unui ERDS • 1.4. Evoluția ERDS • 1.5. Arhitectura software și hardware	2	Predarea principalelor noțiuni teoretice, a schemelor de principiu și caracteristicilor acestora este efectuată folosind videoproiectorul și diapozitive animate, în timp ce deducerile relațiilor matematice și demonstrațiile sunt efectuate folosind metoda clasică (la tablă).	
2. Parametrii secțiunii analogice • 2.1. Structura secțiunii analogice • 2.2. Zgomotul • 2.3. Distorsiunile neliniare • 2.4. Convertorul A/D	4	Predarea principalelor noțiuni teoretice este efectuată folosind videoproiectorul și diapozitive animate, deducerile relațiilor matematice și demonstrațiile sunt efectuate folosind metoda clasică (la tablă).	

3. Secțiunea digitală
• 3.1. Structura secțiunii digitale
• 3.2. Operațiile efectuate de unitatea de prelucrare în banda de bază
  o 3.2.1. Operații pe bit
  o 3.2.2. Modulare / Demodulare
  o 3.2.3. Filtre de formare
• 3.3. Structura și operațiile implementate de secțiunea frontală digitală
  o 3.3.1. Schimbarea de frecvență și supraeșantionarea
  o 3.3.2. Reducerea vârfurilor de amplitudine
  o 3.3.3. Predistorsionarea digitală
  o 3.3.4. Schimbarea de frecvență și decimarea
  o 3.3.5. Tehnica subeșantionării
  o 3.3.6. Caracteristicile arhitecturii homodină
  o 3.3.7. Reglajul automat al amplificării
  o 3.3.8. Sincronizarea receptorului
	20	Predarea principalelor noțiuni teoretice este efectuată folosind videoproiectorul și diapozitive animate, deducerile relațiilor matematice și demonstrațiile sunt efectuate folosind metoda clasică (la tablă).	

4. Implementări practice • 4.1. USRP N200	2	Predarea principalelor noțiuni teoretice este efectuată folosind videoproiectorul și	

• 4.2. Stația de bază pentru telefonia mobilă ZTE		diapozitive animate.	

Bibliografie

- M. Păun, „Echipamente radio definite prin software", suport de curs disponibil pe campusul virtual al UMC
- Walter Tuttlebee, "Software Defined Radio - Enabling Technologies", John Wiley & Sons, New York, 2002
- Tony Rouphael, "RF and Digital Signal Processing for Software-Defined Radio", Newnes, 2008

Bibliografie minimală

- M. Păun, „Echipamente radio definite prin software", suport de curs disponibil pe campusul virtual al UMC

Aplicații (Laborator)	Nr. ore	Metode de predare	Observații
1. Scanarea spectrului radio folosind echipament radio definit prin software	2	Predarea se bazează pe folosirea videoproiectorului (acoperind funcția de comunicare și demonstrativă); metoda de comunicare orală utilizată este metoda problematizării, utilizate frontal. Studenții simulează, implementează, testează și evaluează independent aceleași probleme prin utilizarea continuă a calculatorului și a mediului software. Materialele didactice sunt reprezentate, în principal, de îndrumarul de laborator în variantă tipărită și electronică (pe campusul virtual).	
2. Implementarea emisiei FM folosind echipamentul USRP	2		
3. Implementarea recepției FM folosind echipamentul USRP	2		
4. Implementarea unui sistem de comunicație OOK folosind echipamentul USRP	2		
5. Implementarea unui sistem de comunicație BPSK folosind echipamentul USRP	2		
6. Implementarea unui sistem de comunicație QPSK folosind echipamentul USRP	2		
7. Implementarea unui sistem de comunicație QAM folosind echipamentul USRP	2		

Bibliografie

1. M. Păun, „Echipamente radio definite prin software - Îndrumar de laborator", Ed. Nautica, 2017
2. Simona Halunga-Fratu, Octavian Fratu, „Simularea sistemelor de transmisiune analogice și digitale folosind mediul MATLAB / Simulink", Matrix Rom, București, 2004

Bibliografie minimală

1. M. Păun, „Echipamente radio definite prin software - Îndrumar de laborator", Ed. Nautica, 2017

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

- Domeniul telecomunicațiilor este unul dintre cele mai dinamice din sectorul tehnologiei, cerințele pieței în materie de acoperire și viteză fiind într-o continuă creștere. Aproape toate domeniile activității umane din prezent beneficiază de pe urma dezvoltării telecomunicațiilor, iar radiocomunicațiile sunt fundamentale pentru asigurarea mobilității și creșterii acoperirii geografice cu servicii de calitate. Cea mai nouă tehnologie pentru implementarea sistemelor de comunicații radio este cea a echipamentelor radio definite prin software, care prin flexibilitatea și capacitatea sa de reconfigurare oferă suportul fizic pentru implementarea sistemelor radio inteligente care se adaptează în mod automat și autonom la mediul de transmisiune, realizând așa numitul radio cognitiv.
- Programa cursului răspunde concret acestor cerințe actuale de dezvoltare și evoluție, subscrise economiei europene a serviciilor din domeniul Inginerie Electronică și Telecomunicații.
- Se asigură astfel absolvenților ciclului de învățământ universitar de masterat competențe în concordanță cu necesitățile calificărilor actuale, precum și o pregătire științifică și tehnică modernă, de calitate și competitivă, care să le permită după absolvire o angajare rapidă. Acest lucru este conform politicii Universității Maritime din Constanța, atât din punctul de vedere al conținutului și structurii, cât și din punctul de vedere al

aptitudinilor şi deschiderii internaţionale oferite absolvenţilor.

4. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	- Cunoaşterea noţiunilor teoretice fundamentale - Cunoaşterea modului de aplicare a teoriei la probleme specifice - Analiza critică şi comparativă a tehnicilor şi modelelor teoretice	Examen programat în sesiune. Subiectele acoperă în totalitate programa analitică a disciplinei, realizând o sinteză între parcurgerea teoretică comparativă a cursului şi explicitarea prin exerciţii a modelelor de aplicaţie.	**50%**
Seminar			
Laborator	- Cunoașterea structurii și a pricipalelor caracteristici ale echipamentului radio definit prin software - Programarea și utilizarea echipamentului radio definit prin software pentru a implementa un sistem de comunicații	Referat de laborator conținând rezultatele experimentelor efectuate și răspunsurile la problemele/exercițiile aferente acestora.	**50%**
Proiect			
Standard minim de performanţă			
• Cunoașterea structurii și a pricipalelor caracteristici ale echipamentului radio definit prin software • Utilizarea echipamentului radio definit prin software			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	Ș.L.univ. dr. ing. Mirel Păun	Ș.L.univ. dr. ing. Mirel Păun

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf. univ. dr. ing. Alexandra Raicu

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf. univ.dr. ing. Ion Omocea

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Limbaje de descriere hardware				
Titularul activităţilor de curs	Conf. univ.dr. ing. Mihaela HNATIUC				
Titularul activităţilor de seminar	Conf. univ.dr. ing. Mihaela HNATIUC				
Anul de studiu	2	Semestrul	2	Tipul de evaluare	E

Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară	DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)	DOA

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	3	Curs	2	Seminar	-	Laborator	1	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	42	Curs	28	Seminar	-	Laborator	14	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	50
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	6
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	6
II d) Tutoriat	
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	62
Total ore pe semestru (Ib+II+III+IV)	106
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	Circuite integrate digitale, Programare, Microcontrolere
Competenţe	**C3.3.** Utilizarea soft-urilor profesionale pentru proiectarea sistemelor electronice de telecomunicaţii **C 3.5.** Proiectarea sistemelor electronice de telecomunicaţii utilizând alături de metodele consacrate şi softurile profesionale

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		• Nu este cazul
Desfăşurare aplicaţii	Seminar	•
	Laborator	• Prezenţa obligatorie
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	**C3.** Folosirea creativa a conceptelor fundamentale din electronică, a metodelor de modelare si simulare, pentru realizarea modulelor unor sisteme electronice de telecomunicaţii
Competenţe transversale	CT3. Utilizarea eficientă a surselor informaţionale şi a resurselor de comunicare şi formare profesională continuă pentru îndeplinirea planului personal de dezvoltare a carierei

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Descrierea circuitelor cu logică programabilă şi prezentarea arhitecturii FPGA. - prezentarea limbajelor specifice proiectării şi verificării circuitelor digitale pentru FPGA. - prezentarea criteriilor de selectie a FPGA pe baza specificaţiilor de proiectare. - descrierea conceptelor şi metodelor de proiectare, testare şi implementare FPGA. - proiectarea şi analiza componentelor combinaţionale şi secvenţiale, prezentarea arhitecturilor de implementare şi a maşinilor de stări finite asincrone/ sincrone. Descrierea structurală sau comportamentală în VHDL. - studierea metodelor de optimizare a ariei şi/sau vitezei corespunzătoare unui circuit digital. - parcurgerea completă a etapelor specifice implementării circuitelor digitale pe FPGA (selecţia chipului, editarea codului sursă, editarea codurilor de test şi verificarea la nivel de bloc şi sistem, sinteza, generarea fişierelor de constragere, implementarea, validarea implementarii, generarea fişierelor de configurare, verificarea post-implementare). - prezentarea celor mai cunoscute unelte software aferente fiecarei etape (ModelSIM, Specman, Xilinx XST, Xilinx ISE, ChipScope). - proiectarea şi implementarea unor circuite uzuale în sistemele digitale (convertoare S/P si P/S, interfete seriale si paralele, calcul CRC, etc).
	- parcurgerea completă a etapelor specifice implementării circuitelor digitale pe FPGA (selecţia chipului, editarea codului sursă, editarea codurilor de test şi verificarea la nivel de bloc şi sistem, sinteza, generarea fişierelor de constragere, implementarea, validarea implementarii, generarea fişierelor de configurare, verificarea post-implementare). -prezentarea celor mai cunoscute unelte software aferente fiecarei etape

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
Circuite cu logică programabilă 1.1. Circuite SPLD (PLA si PAL) 1.2. Circuite CPLD 1.3. Circuite FPGA	2	Predarea (definiţii) principalelor noţiuni teoretice este efectuată folosind metoda Proiectare pe ecran LCD, acoperind astfel funcţia de comunicare demonstrativă.	
Reprezentarea numerelor în precizie finită 2.1. Intreg fară semn 2.2. Intreg cu semn - semn şi modul 2.3 Complement faţă de 1 si faţă de 2 2.4 Virgulă mobilă	2	Predarea (definiţii) principalelor noţiuni teoretice este efectuată folosind metoda Proiectare pe ecran LCD, acoperind astfel funcţia de comunicare demonstrativă.	
Limbajul VHDL 3.1. Concepte de bază 3.2. Sintaxa limbajului VHDL 3.3. Descriere comportamentală 3.4. Descriere structurală	6	Predarea (definiţii) principalelor noţiuni teoretice este efectuată folosind metoda Proiectare pe ecran LCD, acoperind astfel funcţia de comunicare demonstrativă.	
Instanţierea componentelor fizice şi logice dedicate 4.1. Componente fizice 4.1.1. Blocuri memorie 4.1.2. Blocuri de aritmetică 4.2. Componente logice	6	Predarea (definiţii) principalelor noţiuni teoretice este efectuată folosind metoda Proiectare pe ecran LCD, acoperind astfel funcţia de comunicare demonstrativă.	
Verificarea codului VHDL 5.1. Verificare la nivel de modul 5.1.1. Verificare funcţională 5.1.2. Verificare temporală 5.2. Verificare la nivel de sistem	2	Predarea (definiţii) principalelor noţiuni teoretice este efectuată folosind metoda Proiectare pe ecran LCD, acoperind astfel funcţia de comunicare demonstrativă.	

Sinteza codului VHDL 6.1. Descrierea procesului de sinteză 6.2. Reguli de configurare a sintezei 6.3. Interpretarea rezultatelor şi reguli de optimizare	4	Predarea principalelor noţiuni teoretice este efectuată folosind metoda Proiectare pe ecran LCD, acoperind astfel funcţia de comunicare demonstrativă	
Implementarea codului VHDL 7.1. Biblioteci de componente hardware 7.2. Reguli de configurare a implementării 7.3. Validarea proiectării 7.4. Generarea fişierelor de configurare	4	Predarea este efectuată folosind metoda Proiectare pe ecran LCD, acoperind astfel funcţia de comunicare demonstrativă	
Metode de testare post-implementare 8.1. Simulare post- implementare 8.2. Verificare prin achiziţie în timp real	2	Predarea este efectuată folosind metoda Proiectare pe ecran LCD, acoperind astfel funcţia de comunicare demonstrativă	
Bibliografie			
Volnei Pedroni, „Circuit Design with VHDL", MIT Press Taek Kwon, VHDL, Sintax referece, FPGA prototyping by VHDL examples, Xilinx SpartanTM-3Version			
Bibliografie minimală			
Meher Krishna Patel, FPGA designs with VHDL, 2017			

Aplicaţii (Laborator)	Nr. ore	Metode de predare	Observaţii
VHDL Prezentare generală	2	Studenţii simulează, implementează, testează şi evaluează independent aceleaşi probleme prin utilizarea continuă a calculatorului, mediului software şi a placilor FPGA. Materialele didactice sunt reprezentate, în principal, de îndrumarul de laborator în variantă tipărită şi electronică (pe campusul virtual).	
Tipul de date	2		
Modelarea fluxului de date	2		
Modelarea comportamentală	2		
Proceduri, funcţii şi pachete	2		
Verificări vizuale ale modelelor	2		
Stari masină finite	2		
Bibliografie			
- DEO-NANO, User Manual			
Bibliografie minimală			
Meher Krishna Patel, FPGA designs with VHDL, 2017			

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

- Dezvoltarea fără precedent a sistemelor de calcul a făcut ca FPGA-urile să fie utilizate în toate domeniile.
- Industria are o cerere importantă de ingineri calificaţi, cu specializări în sisteme împachetate şi cu un fundament solid în domeniul programării şi schemelor electronice, capabili să dezvolte noi produse şi servicii.
- Programa cursului răspunde concret acestor cerinţe actuale de dezvoltare şi evoluţie, subscrise economiei europene a serviciilor din domeniul Inginerie Electronică şi Telecomunicaţii, programul de studii Circuite şi sisteme integrate de comunicaţii (CSIC). În contextul progresului tehnologic actual al echipamentelor de achiziţii de date, domeniile de activitate vizate sunt practic nelimitate.
- Se asigură astfel absolvenţilor ciclului de învăţământ universitar de masterat competenţe în concordanţă cu necesităţile calificărilor actuale, precum şi o pregătire ştiinţifică şi tehnică modernă, de calitate şi competitivă, care să le permită după absolvire o angajare rapidă. Acest lucru este conform politicii Universităţii Maritime din Constanţa, atât din punctul de vedere al conţinutului şi structurii, cât şi din punctul de vedere al aptitudinilor şi deschiderii internaţionale oferite absolvenţilor.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	- Cunoaşterea noţiunilor teoretice fundamentale - Cunoaşterea modului de aplicare a teoriei la probleme specifice - Analiza critică şi comparativă a tehnicilor şi modelelor	Examen programat în sesiune. Subiectele acoperă în totalitate programa analitică a disciplinei, realizând o sinteză	**55%**

	teoretice	între parcurgerea teoretică comparativă a cursului şi explicitarea prin exerciţii a modelelor de aplicaţie.	
Seminar			
Laborator	- Cunoașterea noțiunilor teoretice - Realizarea de circuite digitale în VHDL - Realizarea de programe în VHDL	Colocviu final de laborator, cuprinzând o componentă teoretică şi o componentă practică. Componenta teoretică constă în răspunsul dat de fiecare student la un set distinct de întrebări; componenta practică constă în realizarea unor teme de casă.	**45%**
Proiect			
Standard minim de performanţă			
• Cunoaşterea arhitecturilor circuitelor logice programabile • Realizarea de scheme electronice, citirea lor și programarea in VHDL			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10.10.2018	Conf. univ.dr. ing. Mihaela HNATIUC	Conf. univ.dr. ing. Mihaela HNATIUC

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf. univ. dr. ing. Alexandra Raicu

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.dr.ing. Ion Omocea

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Implicarea factorului uman în securitatea cibernetică maritimă				
Titularul activităţilor de curs	Conf.univ.dr.ing. Hanzu Radu				
Titularul activităţilor de seminar	Conf.univ.dr.ing. Hanzu Radu				
Anul de studiu	2	Semestrul	1	Tipul de evaluare	C

Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară	DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)	DOA

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	3	Curs	2	Seminar	1	Laborator	-	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	42	Curs	28	Seminar	14	Laborator	-	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	29
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	10
II d) Tutoriat	5
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	54
Total ore pe semestru (Ib+II+III+IV)	98
Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	Familiarizarea cu terminologia specifică. Capabilitatea de a monitoriza, detecta, preîntâmpina, minimiza si raporta acţinui specifice atacurilor cibernetice, care exploatează factorul uman, în vederea infectării/disruperii unui ehipament/sistem sau retea computerizată. Cunoasterea şi aplicarea metodelor de prevenire, minimizare şi combatere riscurilor de securitate cibernetica din perspeciva factorului uman.

Competenţe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităţilor lingvistice, a cunoştinţelor de tehnologia informaţiei şi a comunicării pentru dezvoltarea personală si profesională, în scopul inserţiei pe piaţa muncii şi al adaptării la dinamica cerinţelor acesteia. Utilizarea eficientă a resurselor şi tehnicilor de învăţare, în scopul dezvoltării personale şi profesionale continue în domeniul telecomunicaţiilor şi tehnologiei informaţionale, operarea cu informaţii şi tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe şi demonstrarea abilităţilor de comunicare.

7. **Obiectivele disciplinei** (reieşind din grila competenţelor specifice acumulate)

Obiectivul general al disciplinei	Cunoasterea și aplicarea metodelor de prevenire, minimizare și combatere riscurilor de securitate cibernetica din perspeciva factorului uman

8. **Conţinuturi**

Curs	Nr. ore	Metode de predare	Observaţii
1. Dimensiunea socio-umana a criminalităţii cibernetice.	**6**	Prelegere orală	
1.1. Perspectivă asupra conflictelor si criminalităţii in cel de-al 5-lea spaţiu de conflict – "Cyberspace" 1.2. IOT-Internetul Lucrurilor între oportunitate, inovare şi vulnerabilităţi. Conceptul "secure by design" şi factorul uman. 1.3. Atacatorii. Cine sunt şi ce îi motivează.		Prelegere orală	
2. Ingineria Socială relaţionată la Criminalitatea Cibernetică.	**8**	Prelegere orală	
2.1. Evitarea controalelor tehnice (anti-malware) prin atactul asupra factorului uman intr-o organizaţie. 2.2. Varietatea atacurilor si tendinţele actuale de intensificare şi diversificare ale acestora. 2.3. Reţelele sociale intre nevoile de marketing, business şi ingineria socială "de zi cu zi".		Prelegere orală	
3. Informatiile din surse deschise, profilingul psiho-social, amprenta şi identitatea digitală.	**4**	Prelegere orală	
3.1. Întelegerea "Existenţei Online" 3.2. Agregarea datelor generate online si profilarea utilizatorilor. 3.3. De ce online e mai usor?...		Prelegere orală	
4. Prevenirea şi minimizarea riscurilor în cazul atacurilor de criminalitate cibernetica.	**10**	Prelegere orală	
Bibliografie			
ISO/IEC 27001 Information Security Management Standard Europea NIS Directive European General Data Protection Regulation (GDPR) National Cyber Security Centre - GCHQ Note de Training Acreditat dr. John McCarthy			

Aplicaţii (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observaţii
Studiu de caz – "Vishing" via phone spoofing	2	problematizare, exercitiu	
Geolocarea in ingineria socială – studiu de caz	2	problematizare, exercitiu	
Telefonul tau este "gură mare"! – informatii obtinute vs. daruite	2	problematizare, exercitiu	
Prietenii prietenilor – Studiu Practic	2	problematizare, exercitiu	
Profiling – metode si modalitati practice	2	problematizare, exercitiu	
Metode de prevenire si aparare	4	problematizare, exercitiu	
Bibliografie			
ISO/IEC 27001 Information Security Management Standard Europea NIS Directive European General Data Protection Regulation (GDPR) National Cyber Security Centre - GCHQ Note de Training Acreditat dr. John McCarthy			

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

- Conţinutul este orientat către aspecte practice ale tehnologiilor de lucru sub apă, în concordanţă cu cele mai noi tehnici care sunt aplicate în întreaga lume.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Cunoaşterea terminologiei utilizate in cadrul acestei disciplinei, capacitatea de utilizare adecvată a noţiunilor. Cunoasterea dimensiunii socio-umana a criminalităţii cibernetice. Cunoasterea tehnicilor de prevenire şi minimizare a riscurilor în cazul atacurilor de criminalitate cibernetica.	Examen scris	70%
Seminar	Însuşirea problematicii tratate la curs. Capacitatea de a utiliza corect metodele, modelele şi notiunile predate la curs.	Evaluare continuă	30%
Laborator			
Proiect			
Standard minim de performanţă			
• **Nota 5**			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
26.10.2018	Conf.univ.dr.ing. Hanzu Radu	Conf.univ.dr.ing. Hanzu Radu

Data avizării în departament	Semnătura directorului de departament
12.11.2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21.11.2018	Conf.univ.dr.ing. Omocea Ion

FIŞA DISCIPLINEI

1. Date despre program

Instituţia de învăţământ superior	UNIVERSITATEA MARITIMĂ CONSTANŢA
Facultatea	ELECTROMECANICĂ NAVALĂ
Departamentul	ŞTIINŢE GENERALE INGINEREŞTI
Domeniul de studii	INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE
Ciclul de studii	MASTER
Programul de studii/calificarea	SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR

2. Date despre disciplină

Denumirea disciplinei	Investigarea infracţiunilor informatice				
Titularul activităţilor de curs	Prof.univ.dr. Drăghici Vasile				
Titularul activităţilor de seminar	Prof.univ.dr. Drăghici Vasile				
Anul de studiu	2	Semestrul	2	Tipul de evaluare	E
Regimul disciplinei	Categoria formativă a disciplinei DA – de aprofundare/cunoaştere avansată, DS - de sinteză, DC - complementară				DS
	Categoria de opţionalitate a disciplinei: DO - obligatorie (impusă), DOA - opţională (la alegere), DL - facultativă (liber aleasă)				DOA

3. Timpul total estimat (ore alocate activităţilor didactice)

I a) Număr de ore pe săptămână	3	Curs	2	Seminar	1	Laborator	-	Proiect	-
I b) Totalul de ore pe semestru din planul de învăţământ	42	Curs	28	Seminar	14	Laborator	-	Proiect	-

II Distribuţia fondului de timp pe semestru:	ore
II a) Studiul după manual, suport de curs, bibliografie şi notiţe	30
II b) Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	10
II c) Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	28
II d) Tutoriat	10
III Examinări	2
IV Alte activităţi (precizaţi):	

Total ore studiu individual II (a+b+c+d)	78
Total ore pe semestru (Ib+II+III+IV)	122
Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

Curriculum	•
Competenţe	•

5. Condiţii (acolo unde este cazul)

Desfăşurare a cursului		•
Desfăşurare aplicaţii	Seminar	•
	Laborator	•
	Proiect	•

6. Competenţe specifice acumulate

Competenţe profesionale	- Cunoaştere şi înţelegerea conceptelor de criminalitate informatică; - Cunoaşterea modurilor de săvârşire a infracţiunilor de criminalitatea informatică; - Cunoaşterea tipurilor de procedee tehnice şi tactice de investigare a infracţiunilor informatice; - Înţelegerea problematicii privind mijloacele de probă necesare probării infracţiunilor de criminalitate informatică; - Cunoaşterea şi înţelegerea standardelor şi procedeelor internaţionale folosite în investigarea criminalităţii informatice;

	- Cunoașterea și utilizarea transdiciplinară a unor principii și mecanisme pentru prevenirea și combaterea criminalității informatice;
Competențe transversale	Autoevaluarea obiectivă a nevoii de formare profesională continuă, precum si utilizarea eficientă a abilităților lingvistice, a cunoștințelor de tehnologia informației și a comunicării pentru dezvoltarea personală si profesională, în scopul inserției pe piața muncii și al adaptării la dinamica cerințelor acesteia. Utilizarea eficientă a resurselor și tehnicilor de învățare, în scopul dezvoltării personale și profesionale continue în domeniul telecomunicațiilor și tehnologiei informaționale, operarea cu informații și tehnici de gestionare a acestora, angajarea clară pe calea propriei dezvoltări profesionale. Planificarea, organizarea, conducerea în cadrul unei echipe și demonstrarea abilităților de comunicare.

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

Obiectivul general al disciplinei	Prezentarea generală a noțiunilor de criminalitate informatică, evoluție, trăsături, tipuri. Cunoașterea procedeelor tehnice și tactice de investigare a infracțiunilor informatice, a mijloacelor de probă necesare probării comiterii infracțiunilor informatice. Standardele și procedeele internaționale folosite în investigarea criminalității informatice

8. **Conținuturi**

Curs	Nr. ore	Metode de predare	Observații
1. Elemente de criminalistică	2 ore	Prelegere orală	
2. Riscuri și amenințări referitoare la securitatea sistemelor informatice	2 ore	Prelegere orală	
3. Noțiunea de criminalitate informatică, evoluție, trăsături, tipuri	2 ore	Prelegere orală	
4. Organisme, structuri specializate în prevenirea și combaterea criminalității informatice; competența acestora	2 ore	Prelegere orală	
5. Moduri de săvârșire ale infracțiunilor informatice	2 ore	Prelegere orală	
6. Procedee tehnice și tactice de investigare a infracțiunilor informatice	8 ore	Prelegere orală	
7. Probleme principale apărute în cadrul investigării infracțiunilor informatice	2 ore	Prelegere orală	
8. Mijloacele de probă necesare probării comiterii infracțiunilor informatice	2 ore	Prelegere orală	
9. Particularități ale investigării fraudelor cu carduri	4 ore	Prelegere orală	
10. Standardele și procedeele internaționale folosite în investigarea criminalității informatice	2 ore	Prelegere orală	

Bibliografie

1. Cod penal – Legea nr. 286/2009
2. Noul Cod de procedură penală – Legea nr. 135/2010
3. Emilian Stancu, Tratat criminalistică, Ediția 5, Universul Juridic, București 2010
4. Emilian Stancu, Petruț Ciobanu, Criminalistică – Metodologia criminalistică, Universul Juridic, București 2018
5. Dan Cimpoeru, Dreptul internetului, Ediția 2, Editura C. H. Beck, București 2013
6. Gheorghe Iulian Ioniță, Infracțiuni din sfera criminalității informatice, Ediția III revizuită și adăugită, Universul Juridic, București 2018
7. Adrian Cristian Moise, Metodologia investigării criminalității a infracțiunilor informatice, Universul Juridic, București 2011
8. Vasiu Ioana, Criminalitatea informatică, Ediția 2, Editura Nemira, București 2001
9. Amza I., Amza C.P., Criminalitatea informatică, Editura Lumina Lex, București 2003

Aplicații (Seminar / laborator / proiect)	Nr. ore	Metode de predare	Observații
1. Noțiuni, concepte criminalistice, principii, obiect criminalistică. Principalele taxonomii din sfera securității sistemelor informatice.	2 ore	problematizare, exercitiu	
2. Cercetarea la fața locului a infracțiunilor informatice. Efectuarea percheziției informatice. Acte de urmărire penală efectuate în investigarea infracțiunilor informatice.	4 ore	problematizare, exercitiu	
3. Identificarea obiectelor ce au fost folosite s-au destinate la săvârșirea infracțiunilor informatice. Identificarea hardware-ului ca rezultat al comiterii infracțiunii informatice.	2 ore	problematizare, exercitiu	
4. Urma electronică. Informația virtuală. Hardware-ul	2 ore	problematizare, exercitiu	
5. Folosirea cărților de credit. Plățile online. Operațiuni de skimming, phishing, vishing, pharming.	2 ore	problematizare, exercitiu	

6. Falsificarea unui card. Tipuri de fraudă cu cardul.	2 ore	problematizare, exercitiu	

Bibliografie

1. Cod penal – Legea nr. 286/2009
2. Noul Cod de procedură penală – Legea nr. 135/2010
3. Emilian Stancu, Tratat criminalistică, Ediţia 5, Universul Juridic, Bucureşti 2010
4. Emilian Stancu, Petruţ Ciobanu, Criminalistică – Metodologia criminalistică, Universul Juridic, Bucureşti 2018
5. Dan Cimpoeru, Dreptul internetului, Ediţia 2, Editura C. H. Beck, Bucureşti 2013
6. Gheorghe Iulian Ioniţă, Infracţiuni din sfera criminalităţii informatice, Ediţia III revizuită şi adăugită, Universul Juridic, Bucureşti 2018
7. Adrian Cristian Moise, Metodologia investigării criminalităţii a infracţiunilor informatice, Universul Juridic, Bucureşti 2011
8. Vasiu Ioana, Criminalitatea informatică, Ediţia 2, Editura Nemira, Bucureşti 2001
9. Amza I., Amza C.P., Criminalitatea informatică, Editura Lumina Lex, Bucureşti 2003

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

- Conţinutul este orientat către aspecte practice ale investigării infracţiunilor de criminalitate informatică, în acord cu legislaţia penală română, precum şi cu cele mai noi reglementări internaţionale şi europene.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Să cunoască şi înţelegerea elementelor de criminalistică informatică; Să cunoască riscurile şi ameninţările la securitatea informatică; Să cunoască tipurile de procedee tehnice şi tactice de investigare a infracţiunilor informatice; Să cunoască problematica privind mijloacele de probă necesare probării comiterii infracţiunilor de criminalitate informatică; Să cunoască standardele şi procedeele internaţionale folosite în investigarea criminalităţii informatice;	Examen scris	70%
Seminar	Realizarea temelor de seminar Prezenţa la seminar	Evaluare continuă	30%
Laborator			
Proiect			

Standard minim de performanţă

Nota 5

Cunoaşterea tipurilor de procedee tehnice şi tactice de investigare a infracţiunilor informatice. Realizarea unui referat cu privire la modul prin care se utilizează mijloacele de probă necesare probării comiterii unui tip de infracţiune de criminalitate informatică.

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10. 10. 2018	Prof.univ.dr. Drăghici Vasile	Prof.univ.dr. Drăghici Vasile

Data avizării în departament	Semnătura directorului de departament
12. 11. 2018	Conf.univ.dr.ing. Raicu Alexandra

Data aprobării în Consiliul academic	Semnătura decanului
21. 11. 2018	Conf.univ.dr.ing. Omocea Ion

Institutia: UNIVERSITATEA MARITIMA DIN CONSTANTA
Domeniul Fundamental: STIINTE INGINERESTI
Domeniul de studii: INGINERIE ELECTRONICA, TELECOMUNICATII SI TEHNOLOGII INFORMATIONALE
Programul de studii: Master SECURITATE CIBERNETICA SI MANGEMENTUL RISCURILOR

LISTA PERSONALULUI DIDACTIC LA STRUCTURA ACADEMICA EVALUATE

CONFORM STATELOR DE FUNCTIUNI ALE DEPARTAMENTELOR

Nr. crt.	Nume şi prenume	Funcţia postului ocupat	Specialitatea cadrului didactic	Titlul ştiinţific	Gradul didactic	Instituţia unde are norma de baza	Acordul Personal pentru a preda	Alte institutii unde îşi desfăşoară activitatea
1	Tamaş Răzvan	Profesor	Radiocomunicaţii	Dr.ing.	Profesor	UMC	DA	
2	Hnatiuc Bogdan	Profesor	Electrotehnică (Inginerie Electrică)	Dr.ing.	Profesor	UMC	DA	
3	Constantinescu Eliodor	Profesor	Cercetări operaţionale (cibernetică)	Dr.mat.	Profesor	UMC	DA	
4	Popa George	Profesor	Economie specializare în prevenirea şi combaterea infracţionalităţii economico-financiare	Dr.ec.	Profesor	UMC	DA	
5	Stanca Costel	Profesor	Inginerie Navala	Dr.ec.	Profesor	UMC	DA	
6	Zăgan Remus	Profesor	Inginerie Industrială	Dr.ing.	Profesor	UMC	DA	
7	Surugiu Felicia	Profesor	Economie	Dr.ec.	Profesor	UMC	DA	
8	Drăghici T Vasile	Profesor	Drept	Dr.jr	Profesor	Parchetul Curţii de Apel Cţa	DA	Universitatea Ovidius Constanţa
9	Raicu Gabriel	Conferenţiar	Cibernetica, Informatică Economică	Dr.ing.	Confere nţiar	UMC	DA	-

10	Sintea Sorin	Conferenţiar	Ştiinţa calculatoarelor	Dr.ing.	Conferenţiar	UMC	DA	-
11	Hanzu-Pazara Radu	Conferenţiar	Inginerie mecanică	Dr.ing.	Conferenţiar	UMC	DA	
12	Dănişor Alin	Conferenţiar	Inginerie mecanică	Dr.ing.	Conferenţiar	UMC	DA	
13	Hnatiuc Mihaela	Conferenţiar	Inginerie electronică şi telecomunicaţii	Dr.ing.	Profesor	UMC	DA	
14	Pescaru Alexandru	Şef lucrări	Automatică	Dr.ing.	Lector	UMC	DA	-
15	Dinu Simona	Lector	Informatică			UMC	DA	
16	Savu Ana	Şef lucrări	Inginerie electronică şi telecomunicaţii			UMC	DA	
17	Păun Mirel	Şef lucrări	Inginerie electronică şi telecomunicaţii			UMC	DA	-
18	Dănilă Mihai Liviu	Conferenţiar Asociat	Doctor în Ştiinţe militare MBA- Management Strategic	Dr.	-	Pensionar militar	DA	-
19	Drăghici V. Vasile	Conferenţiar Asociat	Inginerie electronică şi telecomunicaţii	Dr.ing.	-	Pensionar militar	DA	-
20	Ioniţă Daniel	Lector asociat	Managementul Educaţional în Cultura de Securitate	Expert	-	Pensionar militar	DA	

Rector,

Prof. univ.dr. ing. Cornel PANAIT

Director departament,

Conf.univ.dr. ing. Alexandra RAICU

ANEXA 5

Instituţia: UNIVERSITATEA MARITIMĂ DIN CONSTANŢA
Facultatea ELECTROMECANICĂ NAVALĂ
Domeniul de masterat: ***INGINERIE ELECTRONICĂ, TELECOMUNICAŢII ŞI TEHNOLOGII INFORMAŢIONALE***
Programul de studii: ***SECURITATE CIBERNETICĂ ŞI MANAGEMENTUL RISCURILOR***

TABEL PRIVIND INDEPLINIREA INDICATORULUI

„Cadrele didactice titulare* au pregătirea iniţială, sunt doctori / doctoranzi şi cercetează în domeniul în care se includ disciplinele din postul ocupat"

Nr crt	Gradul didactic, numele şi prenumele titularului vârsta / vechimea în învăţământul superior	Disciplinele din cadrul programului de studii incluse în postul didactic şi tipul activităţii desfăşurate (curs, seminar, lucrări, proiect)	Competenţa cadrului didactic titular în disciplinele din postul didactic			Constatări privind îndeplinirea indicatorului
			Universitatea/ facultatea/ specializarea absolvită	Specializarea la masterat/ doctorat	Numărul de cărţi, numărul de lucrări ştiinţifice, numărul de brevete în domeniul disciplinelor din postul didactic ** conform Anexelor 5.1, 5.2 etc	
1	Prof.univ.dr.ing. Tamaş Răzvan 49/24	Antene, arhitecturi de comunicaţii şi riscuri cibernetice (curs şi laborator)	Universitatea Politehnica Bucureşti Facultatea de Electronică şi Telecomunicaţii Specializarea: Radiocomunicaţii	Abilitare (Habilitation à Diriger de Recherches) în Radiofrecvenţă (Grenoble INP, Franţa) Doctorat în Optică, Optoelectronică şi Microunde (cotutelă cu Grenoble INP, Franţa) **Doctorat în inginerie electronică şi telecomunicaţii (UPB)** Masterat în Radiocomunicaţii, Microunde şi Comunicaţii Optice	Teza de abilitare (A1), Teza de doctorat (A2); 3 cărţi (B1, B2, B3); 49 lucrări indexate ISI/BDI (C1 – C49);	Îndeplinit
2	Prof. univ.dr. ing. Hnatiuc Bogdan 45/22	Protocoale şi interfeţe de comunicare în industrie aferente infrastructurilor critice în energetică, transporturi şi servicii	Universitatea Tehnică "Gheorghe Asachi" Iaşi	Doctorat în Inginerie Electrica	Teza de doctorat (A); 7 cărţi (B1-B7); 3 brevete (E1, E2, E3) 18 lucrări indexate ISI/BDI (C1 – C18); 8 lucrări publicate în ultimii 10 ani în	Îndeplinit

		(curs şi laborator)	Facultatea de Electrotehnică		reviste şi volume de conferinţe (D2, D4, D6, D9, D10, D11,D14, D16)	
3	Prof. univ.dr. Constantinescu Eliodor 55/31	Securitatea informaţională şi tehnologii criptografice	Universitatea Bucureşti/Facultatea Matematică/Matematică şi Informatică	Doctorat în Cibernetica, Informatica Economica	4 cărţi (B5, B6, B7, B8) 6 lucrări indexate ISI/BDI (C2, C3, C4, C10, C11, C12); 5 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D5, D8, D9, D10, D11);	Îndeplinit
4	Prof.univ.dr.ing. Stanca Costel 45/20	Managementul riscului în tehnologiile informaţionale (curs şi laborator)	Universitatea Maritimă Constanţa Facultatea de Navigaţie şi Transport Naval Specializarea Navigaţie şi Transport Maritim şi Fluvial	Doctorat în Economie	Teza de doctorat (A); 3cărţi (B2, B4 şi B5); 9 lucrări indexate ISI sau BDI (C1, C3, C5, C8, C9, C11, C12, C18, C20); 4 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D3, D4, D5, D6);	Îndeplinit
5	Prof.univ.dr. Popa George 50/10	Legislaţia privind securitatea şi criminalitatea economico financiară (curs şi laborator)	Academia de Poliţie „Al. I. Cuza", Bucuresti Facultatea de Drept	Doctorat în Economie/ Specializare în prevenirea şi combaterea infracţionalităţii economico-financiare	Teza de doctorat (A); 3 cărţi (B1, B5, B6); 8 lucrări indexate ISI sau BDI (C2, C3, C4, C6, C9, C11, C15, C19); 6 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D1, D2, D7, D8, D9,D10);	Îndeplinit
6	Prof. univ.dr. ing. Zăgan Remus 52/26	Aplicarea tehnologiei informaţiei şi comunicaţiilor pentru a monitoriza şi controla procesele fizice (curs şi laborator)	Institutul Politehnic „Gh. Asachi" Iaşi Facultatea de Tehnologia Construcţiilor de Maşini Specializarea Tehnologia Construcţiilor de Maşini	Doctorat în Inginerie Industrială Specializări în domeniul securităţii cibernetice în 2016, 2017, 2018	Teza de doctorat (A); 6 cărţi (B7, B8, B9, B11, B12, B15); 15 lucrări indexate ISI (C5, C7, C8, C9, C10, C11, C12, C13, C14, C15, C18, C19, C30, C34, C37); 6 lucrari indexate BDI (C40, C41, C44, C45, C46, C49); 5 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D41, D42, D46, D47, D54)	Îndeplinit

7	Prof.univ.dr.ing. Drăghici T Vasile 53/27	Infracţiuni informatice în legislaţia penală română (curs şi seminar)	Universitatea Bucureşti/ Facultatea de drept	Doctorat în Drept/ Specializare in Managementul securităţii informaţiei Specializări în domeniul securităţii cibernetice în 2016, 2017, 2018	Teza de doctorat (A); 4 cărţi (B1, B3, B5, B6, B11, B17); 10 lucrări indexate BDI C13, C17, C18, C23,C24, C26, C28, C38, C40, C41); 2 articole publicate în extenso, în volume ale sesiunilor ştiinţifice internaţionale pe domeniul infracţionalităţii cibernetice (C40, C41);	Îndeplinit
		Investigarea infracţiunilor informatice (curs şi seminar)			Teza de doctorat (A); 4 cărţi (B1, B3, B5, B6, B11, B17); 10 lucrări indexate BDI (C13, C17, C18, C23,C24, C26, C28, C38, C40, C41); 2 articole publicate în extenso, în volume ale sesiunilor ştiinţifice internaţionale pe domeniul infracţionalităţii cibernetice (C40, C41);	
8	Prof. univ.dr. Surugiu Felicia 52/26	Etică şi integritate academică (curs)	Universitatea Creştină Dimitrie Cantemir – Licenţă Academia de Studii Economice Bucureşti Specializarea: Management Turistic şi Comercial	Doctorat în Economie	Teza de doctorat (A); 1 carte B3; 2 lucrări indexate ISI/BDI (C1,C2,C5); 3 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D10, D11, D12);	Îndeplinit
9	Conf.univ.dr.ing. Raicu Gabriel 45 / 19	Principii fundamentale de securitate cibernetică în tehnologia informaţiei (curs şi laborator)	Universitatea Maritimă Constanţa Facultatea de Navigaţie şi Transport Naval	Doctorat în Cibernetică, Informatică Economică/ Specializări în domeniul securităţii cibernetice vezi secţiunea G în	Teza de doctorat (A); 1 carte B4; 2 lucrări indexate ISI/BDI (C1-C2); 7 Lucrări prezentate în plen la sesiuni ştiinţifice internaţionale : F1, F2, F3, F4, F5, F6, F7	îndeplinit

		Tehnologii utilizate în Internet, analiză malware și IT Forensic (curs şi laborator)	Specializarea Navigație și Transport Maritim și Fluvial	2016, 2017, 2018	2 Carti B3, B4; lucrări indexate ISI/BDI (C4, C7,C9, C12,C13,C14,C21, C25) 7 Lucrări prezentate în plen la sesiuni ştiinţifice internaţionale : F1, F2, F3, F4, F5, F6, F7	
		Securitatea cibernetică a dispozitivelor mobile și riscurile asociate IoT (curs şi laborator)			Teza de doctorat (A); 1 carte B4; 2 lucrări indexate ISI/BDI (C9,C24,); 7 Lucrări prezentate în plen la sesiuni ştiinţifice internaţionale : F1, F2, F3, F4, F5, F6, F7	
10	Conf.univ.dr.ing. Sintea Sorin 52 / 27	Analiza şi clasificarea riscurilor de securitate cibernetică în tehnologiile informaţionale (curs şi laborator)	Universitatea „Transilvania" Braşov Facultatea de Electrotehnică	Doctorat în Ştiinţa calculatoarelor/ Certificat Operator General radio in sistemul GMDSS	Teza de doctorat (A); 4 cărţi (B4, B6,B8, B10); 4 lucrări indexate ISI/BDI (C1, C2, C3, C4, C6); 10 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D1-D10);	Îndeplinit
		Sisteme de conducere a proceselor industriale şi protecţie cibernetică (SCADA, PLC, DPC) (curs şi laborator)			Teza de doctorat (A); 5 cărţi (B1, B2, B5, B6,B9); 4 lucrări indexate ISI/BDI (C2,C3, C5, C6); 7 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D1, D3, D5, D6, D7, D8, D10);	
11	Conf.univ.dr.ing. Hanzu-Pazara Radu 43/15	Implicarea factorului uman în securitatea cibernetică maritimă (curs şi seminar)	Universitatea Maritimă Constanţa/ Facultatea de Navigaţie şi Transport Naval/ Navigaţie şi Transport Maritim şi Fluvial	Doctorat în Inginerie mecanică Specializări în domeniul securităţii cibernetice în 2016, 2017, 2018	Teza de doctorat (A); 5 cărţi (B5,B6,B8,B9, B10); lucrări indexate ISI/BDI (C1, C2, C8, C9, C12, C19, C23, C28); 4 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D1,D5,D7, D8);	Îndeplinit

12	Conf.univ.dr.ing. Dănişor Alin 55/26	Sisteme de comunicaţii subacvatice (curs)	Universitatea Politehnica Bucureşti / Facultatea de Electronică, Telecomunicații și Tehnologii Informaționale	Doctorat în inginerie electronică și telecomunicații	Teza de doctorat (A); 1 carte (B1), 7 lucrări indexate ISI/BDI (C1, C2, C3, C4,C6 ,C7, C8, C11, C13 ,C15 ,C16); 5 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D1, D2, D3, D4, D5);	Îndeplinit
13	Conf. univ.dr. ing. Hnatiuc Mihaela 47/16	Limbaje de descriere hardware (curs şi laborator)	Universitatea Tehnică din Iași / Facultatea de Electronică și Telecomunicații Specializarea: Electronică aplicată	Doctorat în inginerie electronică și telecomunicații/ Master în Inginerie Biomedicală	Teza de doctorat (A); 4 cărţi (B1-B4); 18 lucrări indexate ISI/BDI (C1-29); 1 brevet de invenţie (E1);	Îndeplinit
14	Şef lucrări univ. dr.ing. Pescaru Alexandru 44/18	Siguranța tehnicilor de programare și securitatea aplicațiilor și sistemelor informatice (curs şi laborator)	Universitatea Maritimă Constanța Facultatea de Navigație și Transport Naval Specializarea Navigație și Transport Maritim și Fluvial	Doctorat în Automatică	Teza de doctorat (A); 1 carte (B1); 8 lucrări indexate ISI sau BDI (C1,C2,C3, C4, C5, C6, C7, C8) 3 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D4, D8, D9)	Îndeplinit
15	Lector univ.dr. Dinu Simona 51 / 19	Calculul evolutiv în tehnologia informaţiei (curs şi laborator)	Universitatea București / Facultatea de Matematică / Informatică	Doctorat în Cibernetica, Informatica Economica	Teza de doctorat (A); 2 cărţi (B2,B3); 27 lucrări indexate ISI/BDI (C2, C6, C8,C9, C11, C17, C19, C23);	îndeplinit
		Tehnici și instrumente de evaluare a securității cibernetice, hacking etic și audit de securitate (curs şi laborator)			Teza de doctorat (A); 4 cărţi (B1, B4, B5,B6); 27 lucrări indexate ISI/BDI (C3, C7, C10, C11, C14,C15, C22, C25,C27);	

16	Şef lucrări univ. dr.ing. Savu Ana 44/14	Sisteme de comunicaţii subacvatice (laborator)	Universitatea Maritimă din Constanța / Facultatea de Electromecanică Navală Specializarea: Electrotehnică	Doctorat în inginerie electronică și telecomunicații	Teza de doctorat (A); 4 lucrări indexate ISI/BDI (C1, C4, C6, C7, C14, C15); 2 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D1, D6)	Îndeplinit
		Sisteme electronice de navigaţie (curs şi laborator)			Teza de doctorat (A); 6 lucrări indexate ISI/BDI (C2, C5, C8, C9, C11, C12); 2 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe (D1, D5);	
17	Şef lucrări univ. dr.ing. Păun Mirel 33/10	Echipamente radio definite software (curs şi laborator)	Universitatea OVIDIUS din Constanța / Facultatea de Fizică, Chimie, Electronică și Tehnologia petrolului Specializarea: Electronică Aplicată	Doctorat în inginerie electronică și telecomunicații Master în telecomunicații	Teza de doctorat (A); 1 carte (B1); 8 lucrări indexate ISI/BDI (C1, C8-C14);	Îndeplinit
18	Dr. Dănilă Mihai Liviu 55/20	Managementul amenințărilor hibride în contextul securității cibernetice (curs şi seminar)	Universitatea Naţională de Apărare „Carol I" Bucureşti Facultate Militară, Aviaţie şi Apărare antiaeriană Universitatea „Babeş-Bolyai" – Facultatea de Ştiinţe Economice Facultatea Management si administrarea afacerilor/ Metode Moderne de Management	Doctorat în Ştiinţe militare MBA, Management Strategic	Teza de doctorat (A); 6 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe D1-D6 Lista lucrări conferinţe neclasificata F1 Alte certificări Secţiunea G : Responsabil cadrul mecanismului de răspuns politic integrat la crize și implementarea cauzei de solidaritate în platforma IPCR – SCI a Consiliul UE (cu hub-uri cyber și hybrid)	Îndeplinit
		Mecanisme de răspuns la crize din perspectiva Cyber Security			Teza de doctorat (A); 6 lucrări publicate în ultimii 10 ani în reviste şi volume de conferinţe D1-D6 Lista lucrări conferinţe neclasificata F1 Alte certificări Secţiunea G : Responsabil cadrul mecanismului de răspuns politic integrat la crize și implementarea cauzei de solidaritate în platforma IPCR – SCI a Consiliul UE (cu hub-uri cyber și hybrid)	

19	Dr.ing Drăghici V. Vasile 60/20	Cultura organizațională de securitate (curs şi laborator)	Academia Tehnică Militară/ Facultatea Electronică şi Electrotehnică Şcoala Naţională de Studii Politice şi Administrative/ Masterat în administraţie publică	Doctorat în inginerie electronică și telecomunicații	Teza de doctorat (A); Cărţi – B1 şi B2 Lucrări neclasificate C1-C3 Alte certificări Secţiunea G – Expert în structurile de securitate ale NATO şi UE pentru schimbul de informaţii clasificate	Îndeplinit
20	expert Ioniţă Daniel 50/10	Managementul securităţii cibernetice (curs şi seminarr) **Disciplina facultativă** Cadrul naţional şi european de reglementare al securităţii cibernetice (curs şi seminar)	Academia Forțelor Aeriene / Management organizatii militare Academia Națională de Informații – București Universitatea Ovidius din Constanţa/ Facultatea de Drept	Master în Managementul Educaţional în Cultura de Securitate	Teza de Master în Managementul Educational în Cultura de Securitate A se vedea CV-ul anexat Lista de lucrări neclasificată: B1-B7 Lista lucrări conferinţe neclasificata F1—F11 Alte cursuri şi certificări – secţiunea G	Îndeplinit

*Din statul de funcţii cumulativ al tuturor disciplinelor şi tuturor activităţilor didactice desfăşurate în cadrul programului de studii evaluat.

** Se indică numărul pe următoarele tipuri de lucrări: A – teza de doctorat B – cărţi şi capitole în cărţi publicate în ultimii XX ani C – lucrări indexate ISI/BDI publicate în ultimii XX ani	D – lucrări publicate în ultimii XX ani în reviste şi volume de conferinţe cu referenţi (neindexate); E – brevete acordate în întreaga activitate. Persoanele incluse în tabelul de mai sus anexează cîte o listă de lucrări după modul de mai jos.

Rector,
Prof. univ.dr. ing. Cornel PANAIT

Director departament,
Conf.univ.dr. ing. Alexandra RAICU