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

A N U N Ţ

UNIVERSITATEA MARITIMĂ DIN CONSTANŢA organizează concurs pentru ocuparea a 5 funcţii contractuale vacante de **experţi în domeniul securităţii cibernetice** (***specialişti în proceduri şi instrumente de securitate a sistemelor informatice***), pe perioadă nedeterminată, cu studii superioare, cu timp parţial de lucru (2/4/6 ore/zi), în cadrul **Centrului de Excelenţă în securitate cibernetică maritimă**, astfel :

postul 1 - specialist Managementul securităţii organizaţionale (normă de **6 ore/zi**) :

- **nivelul studiilor**: absolvirea, cu diplomă, a unei instituţii de învăţământ superior de profil (*Tehnologia informaţiei, Electronică şi calculatoare, Electronică şi telecomunicaţii*, etc.);
- **vechime în muncă**:
  - experienţa necesară (cumulativ) în funcţii manageriale - minim 10 ani;
  - experienţă anterioară relevantă în administraţia publică centrală ca *director/coordonator/şef structură de securitate, cooperare internaţională, acreditarea sistemelor de securitate, control şi audit de securitate;*
- **alte cerinţe** :
  - deţinerea titlului de *Doctor in inginerie;*

postul 2 - specialist Cadrul naţional şi european de reglementare al securităţii cibernetice (normă de **2 ore/zi**) :

- **nivelul studiilor**: absolvirea, cu diplomă, a unei instituţii de învăţământ superior (*Drept, Apărare, Management, Informaţii, Tehnologia informaţiei*, etc.);
- **vechime în muncă** :
  - experienţă relevantă minimă de 7 ani în *domeniul securităţii cibernetice şi al cooperării internaţionale în acest domeniu, la nivel managerial (director/preşedinte); expertiză internaţională la nivel, cel puţin, de coordonator în politicile de securitate cibernetică* :

postul 3 – specialist în Managementul tehnologiei informaţiilor în context hibrid, mecanisme de răspuns la crizele de securitate cibernetică (normă de **4 ore/zi**)

- **nivelul studiilor** : absolvirea, cu diplomă, a unei instituţii de învăţământ superior de profil (*Apărare, Management, Tehnologia informaţiei,* etc.);
- **vechime în muncă** :
  -experienţă relevantă minimă de 10 ani în *domeniul managementului informaţiilor, situaţiilor speciale de urgenţă şi crizelor, diplomaţie şi afaceri europene la nivel de director/coordonator/şef structură;*
- **alte cerinţe** :
  - deţinerea titlului de *Doctor în ştiinţe militare;*

postul 4 – specialist în Managementul riscului în tehnologiile informaționale și securitate cibernetică (normă de **2 ore/zi**) :

- **nivelul studiilor** : absolvirea, cu diplomă, a unei instituții de învățământ superior de profil (*Apărare, Tehnologia informației,* etc.); constituie avantaj absolvirea unor studii postuniversitare în domeniul informațiilor și securității naționale;
- **vechime în muncă** : experiență relevantă minimă de 10 ani în *domeniul managementului informațiilor, planificării strategice și cooperării internaționale, experiență de conducere la nivel managerial de minim 4 ani în instituții de învățământ superior în domeniul educației în securitate și informații*.
- **alte cerințe** :
  - deținerea titlului de *Doctor în inginerie/studii inginerești;*

postul 5 – specialist tehnologii avansate în securitate cibernetică (normă de **6 ore/zi**) :

- **nivelul studiilor**: absolvirea, **cu diplomă, a unei instituţii de învăţământ superior** de profil (***Informatica, Automatica, Informatica economica, Tehnologia informației, Electronică și calculatoare***, etc.);

- **vechime în muncă :**

  -experiență de minim 10 ani în Full Stack and Mobile Development;
  -experiență de minim 5 ani pentru Angular/NativeScript (Typescript) and NodeJS;
- **alte cerințe :**

  - doctorat în Computer Science;
  - experiență managerială ca CTO sau Tech Lead în cadrul unor companii internaționale de profil;
  - protocoale:TLS, SSL,HTTPS, SSH;
  - experiență în :
    - criptografie: AES-256, RSA-2048, SHA-256;
    - aplicații în timp real folosind protocolul Websockets Secure și JWT;
    - cloud security protocols: Secure Single-Sign-On Protocol, Key Management Protocol, Cloud Trust Protocol, Secure Cloud Transmission Protocol, Secure Sessions Protocol.

- **Data limită de depunere a actelor pentru concurs**: **16.02.2022**, ora 14.00, Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța;

- **Data de desfășurare a concursului**: - **24.02.2022,** ora 10.00 (**proba practică)**, Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța;

- **01.03.2022,** ora 10.00, *estimativ* (**interviu**), Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța;

- **Relații privind concursul**: tel. 0241/664.740, interior 125, Serviciul Resurse Umane, dna. Popescu Anca, Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța și pe site-ul universității la adresa **https://cmu-edu.eu/cariera/didactic-auxiliar**.

A. CALENDARUL DE DESFĂȘURARE A CONCURSULUI

Etapa I:

1.Selecția dosarelor de concurs ale candidaților: **18.02.2022.**

2.Afișarea rezultatelor selectării dosarelor de înscriere:**21.02.2022 ora 14.00**, Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța, precum și pagina de internet la adresa: **http://www.cmu-edu.eu**.

3.Termenul limită pentru depunerea contestațiilor cu privire la rezultatul selectării dosarelor: **22.02.2022, ora 14.00,** Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța – Rectorat.

4.Comunicarea rezultatelor la contestațiile depuse: **23.02.2022, ora 14.00,** Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța, precum și pagina de internet la adresa: **http://www.cmu-edu.eu**.

Etapa a II-a

1. **Proba practică: 24.02.2022, ora 10.00**, Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța.

- Timp de lucru: maxim **120 minute**.

- Punctajul minim: **50 de puncte**.

2. Afișarea rezultatelor obținute de candidați la **proba practică**: **24.02.2022, ora 14.00** (oră estimativă).

3.Termenul limită pentru depunerea contestațiilor cu privire la rezultatul obținut la proba practică: **25.02.2022, ora 14.00*,** Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța – Rectorat.

* Termenul limită de depunere a contestațiilor se va corela cu ora afișării rezultatelor obținute de candidați la **proba practică** și va fi comunicat candidaților prin afișare la Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța, precum și pagina de internet la adresa: **http://www.cmu-edu.eu**.

4.Comunicarea rezultatelor la contestațiile depuse: **28.02.2022, ora 14.00,** Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța, precum și pagina de internet la adresa: **http://www.cmu-edu.eu**.

Etapa a III-a

1. Interviu și testare abilități : **01.03.2022, ora 10.00 (**estimare**)**, Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța.

- Punctajul minim: **50 de puncte**;

2. Afișarea rezultatelor obținute de candidați în urma testării abilităţilor, aptitudinilor şi motivaţiei candidaţilor: **02.03.2022, ora 10.00 (**estimare**)**, Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța, precum și pagina de internet la adresa: **http://www.cmu-edu.eu**.

3 Termenul limită pentru depunerea contestațiilor privind rezultatele obținute de candidați în urma testării abilităţilor, aptitudinilor şi motivaţia candidaţilor: **03.03.2022, ora 10.00,** Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104 – Rectorat.

4. Comunicarea rezultatelor la contestațiile depuse: **04.03.2022, ora 10.00,** Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța, precum și pagina de internet la adresa: **http://www.cmu-edu.eu**.

Depunere contestații

După afişarea rezultatelor obţinute la selecţia dosarelor, proba scrisă şi/sau proba practică şi interviu, după caz, candidaţii nemulţumiţi pot depune contestaţie în termen de cel mult o zi lucrătoare de la data afişării rezultatului selecţiei dosarelor, respectiv de la data afişării rezultatului probei scrise şi/sau a probei practice şi a interviului, sub sancţiunea decăderii din acest drept.

Rezultatele la contestațiile depuse:

În situaţia contestaţiilor formulate faţă de rezultatul probei scrise sau a interviului și/sau testării abilităţilor, aptitudinilor şi motivaţiei candidaţilor, comisia de soluţionare a contestaţiilor va analiza lucrarea sau consemnarea răspunsurilor la interviu doar pentru candidatul contestatar în termen de maximum o zi lucrătoare de la expirarea termenului de depunere a contestaţiilor.

- Comunicarea rezultatelor la contestațiile depuse se va efectua prin afișare la Sediul Central al Universității Maritime din Constanța, str. Mircea cel Bătrân, nr. 104, Constanța, precum și pagina de internet la adresa: **http://www.cmu-edu.eu**.

B. DOCUMENTE SOLICITATE

Pentru înscrierea la concurs candidaţii vor prezenta un dosar de concurs care va conţine următoarele documente:

1**. cerere de înscriere** la concurs adresată Rectorului universității;

2. **copia actului de identitate** sau orice alt document care atestă identitatea, potrivit legii, după caz. Documentul va fi prezentat şi în original în vederea verificării conformităţii copiei cu originalul;

3. **copiile documentelor** care să ateste ***nivelul studiilor*** şi ale altor acte care atestă ***efectuarea unor specializări***, precum şi copiile documentelor care atestă îndeplinirea condiţiilor specifice ale postului respectiv.
Documentele **vor fi prezentate şi în original** în vederea verificării conformităţii copiilor cu acestea;

4. **carnetul de muncă** sau, după caz, adeverinţele care atestă ***vechimea în muncă şi/sau în specialitatea studiilor***, în copie.
Documentele **vor fi prezentate şi în original** în vederea verificării conformităţii copiilor cu acestea;

5. **cazierul judiciar** sau o declaraţie pe propria răspundere că nu are antecedente penale care să-l facă incompatibil cu funcţia de **expert securitate cibernetică.**

Candidatul declarat admis la selecţia dosarelor, care a depus la înscriere o declaraţie pe propria răspundere că nu are antecedente penale, are obligaţia de a completa dosarul de concurs cu originalul cazierului judiciar, cel mai târziu până la data primei probe a concursului, respectiv, până la data de **24.02.2022.**

6. **adeverință medicală** care să ateste starea de sănătate corespunzătoare, eliberată cu ***cel mult 6 luni*** anterior derulării concursului de către medicul de familie al candidatului sau de către unităţile sanitare abilitate. Adeverinţa care atestă starea de sănătate conţine, în clar, numărul, data, numele emitentului şi calitatea acestuia, în formatul standard stabilit de Ministerul Sănătăţii.

7. curriculum vitae.

C. BIBLIOGRAFIE ȘI TEMATICĂ

Postul nr. 1 – specialist Managementul securității organizaționale

Tematica

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

Bibliografie

1. Drăghici V., Iliescu C., S*isteme de protecţie a informaţiilor clasificate în spaţiul euro-atlantic – actori, principii, evoluţii,*Editura Academiei Tehnice Militare, București, 2013
2. Patterson D., Fay J., *Contemporary Security Management, 4th Edition,* Butterworth-Heinemann, Oxford, 2017.
3. Kaldor M., *Securitatea umană: reflexii asupra globalizării şi intervenţiei*, Editura CA Publishing, Cluj Napoca, 2010;
4. Gariup M., *European Security Culture: Language, Theory, Policy*, Ashgate, 2009.
5. Hutter B.M., Power M. - *Organizational Encounters With Risk*, Cambridge University Press, Cambridge, 2005.
6. Banisar D, *Freedom of information around the world*, Privacy International, London, 2006.
7. Tipton H.F., Krause M., *Information Security Management Handbook*, Taylor & Francis Routledge, Londra, 2005.
8. * * * 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.
9. * * * *Council Guide, Internal document, III. Delegates' Handbook*, General Secretariat of the Council, September 2000
10. * * * *Instruction générale interministérielle sur la protection du secret de la défense nationale N°1300 /SGDSN/PSE/PSD*, Paris, 23.07.2010
11. * * * *The Cabinet Manual - A guide to laws, conventions and rules on the operation of government*, UKCabinet Office, October 2011

Postul nr. 2 - specialist Cadrul naţional şi european de reglementare al securităţii cibernetice

Tematica

1. Organisme și organizații internaționale cu atribuții și responsabilități în domeniul securității cibernetice (ONU, UE, NATO, OSCE, ITU)
2. Cadrul european de reglementare a securității cibernetice
3. Strategii europene de securitate cibernetică - actori, domenii de competență , responsabilități
4. Directiva NIS – subiecți, criterii, praguri și activități obligatorii
5. Norme europene de certificare standardizare și capabilitățile de implementare a acestora
6. Cadrul național de reglementare a securității cibernetice
7. Securitatea cibernetică componentă a securității naționale
8. 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
9. Cadrul de reglementare a capabilităților de securitate cibernetică existente la nivel național
10. Cooperarea în domeniul securității cibernetice – asociații profesionale, modele de cooperare și documente suport
11. Instrumente financiare pentru derularea proiectelor de securitate cibernetică – europene și naționale
12. Identificarea nevoilor de securitate cibernetică la nivel național
13. Identificarea principalelor amenințări de securitate cibernetică la adresa securității naționale
14. Generatori și vectori de propagare a amenințărilor cibernetice – globali, regionali, naționali.
15. Capabilități de răspuns la incidente de securitate cibernetică la nivel internațional – rol, atribuții, responsabilități.
16. Capabilități naționale de răspuns la incidente de securitate cibernetică – rol, atribuții, responsabilități.
17. Tipuri de Echipe de Răspuns la Incidente de Securitate Cibernetică (CSIRT/CERT) – rol, constituență, abilități și limite.
18. Modalități de înființare, dezvoltare și operaționalizare a structurilor de tip CERT/CSIRT
19. Tipuri de servicii furnizate de echipele de tip CERT/CSIRT în conformitate cu prevederile legale și regulamentele asociațiilor profesionale
20. Incidente de securitate cibernetică - prevenire, identificare, analiză și răspuns
21. Programe de educare și formare în securitate cibernetică

Bibliografie

1. Strategia Europeană de securitate cibernetică
2. Directiva NIS - Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.
3. Strategia de Securitate cibernetică a României – HG 271/2013
4. Legea 362/2018
5. HG 963/2020 pentru aprobarea Listei serviciilor esențiale.
6. HG 976/2020 privind aprobarea valorilor de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor şi sistemelor informatice ale operatorilor de servicii esenţiale.
7. HG494/2011 – Organizarea și funcționarea CERT-RO
8. The European Union Agency for Network and Information Security (ENISA) regulation
9. Ordonanță de Urgență nr. 119 din 22 iulie 2020 pentru modificarea și completarea Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.
10. 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.
11. Managementul securității cibernetice
12. Cyber readiness index 2.0 – Potomac Institute for Policies Studies
13. HG494/2011 – Organizarea și funcționarea CERT-RO
14. OUG104/2021- Înființarea Directoratului Național de Securitate Cibernetică
15. ISO 17799
16. Personally identifiable information (PII)
17. GDPR, ISO 27001, ITIL

<u>Postul nr. 3</u> – specialist în Managementul tehnologiei informațiilor în context hibrid, mecanisme de răspuns la crizele de securitate cibernetică

Tematică

1. Amenințări hibride vs. amenințări asimetrice: definire
2. Categorii de amenințări asimetrice și hibride
3. Operațiile informaționale – OI; OI ofensive; OI defensive
4. Operațiile netradiționale (nesupunerea civilă, utilizarea terorii etc.)
5. Caracteristicile amenințărilor hibride și impactul de intelligence
6. Dimensiuni, forme şi procedee ale amenințărilor hibride
7. Impactul amenințărilor hibride în contextul securității cyber
8. Social media din perspectiva amenințărilor hibride; cazuistică
9. Modalităţi de contracarare a amenințărilor hibride
10. Aspecte juridice ale acțiunilor hibride în context cyber
11. Mediile de dezvoltare a amenințărilor hibride și contramăsuri
12. Competitive & Business Intelligence – conceptualizare, definire
13. Competitive & Business Intelligence în teoria managementului
14. Competitive Intelligence și managementul organizației
15. Business Intelligence și managementul corporatist
16. Caracteristicile de intelligence ale mediului de business competitiv
17. Analiza specifică mediului de Competitive & Business Intelligence
18. Aspecte juridice ale Competitive & Business Intelligence sfera cyber
19. Managementul crizelor – definire, conceptualizări, școli de gândire
20. Mecanisme de răspuns la crize specifice mediului cyber
21. Aspecte juridice ale mecanismelor de răspuns la crize

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.
11. Chifu, Iulian, „Hybrid war, a limited and unlimited war“, in Rethinking social action, Core Values, 16-april 2015, Iaşi, Editura Lumen, 2015, p.158.
12. 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.
13. Kissinger, Henry, Diplomația, op. cit.

Postul nr. 4 – specialist în Managementul riscului în tehnologiile informaționale și securitate cibernetică

Tematică

1. Stabilirea contextelor de management al riscului de securitate cibernetică
2. Modele de management al riscului în tehnologiile informaționale
3. Procesul de management al riscului în tehnologiile informaționale
4. Identificarea riscului de securitate cibernetică în tehnologiile informaționale
5. Analiza complexă și evaluarea globală a riscului în tehnologiile informaționale
6. Tratarea riscului de securitate cibernetică în tehnologiile informaționale
7. Monitorizare și comunicare în managementul riscului
8. Managementul riscului în managementul proiectelor de tehnologia informației
9. Stabilirea contextelor de risc în tehnologiile informaționale

10. Proiectarea unui model de management al riscului în securitatea cibernetică
11. Planul de management al riscurilor în tehnologiile informaționale
12. Etica în managementul riscului de securitate cibernetică

Bibliografie

1. Ballard, G.M., 1992. Industrial risk: Safety by design. In: Ansell, J., Wharton, F. (Eds.), Risk: Analysis. Assessment and Management. John Wiley & Sons, Chichester.
2. Breakwell, G.M., 2007. The Psychology of Risk. Cambridge University Press, Cambridge.
3. Ciocoiu Carmen Nadia, Managementul Riscului, Vol 1: Teorii, Practici, Metodologii, București: Editura ASE, 2008.
4. Ciocoiu Carmen Nadia, Managementul Riscului, Vol 2: Modele Economico-Matematice, Instrumente și Tehnici, București: Editura ASE, 2008.
5. Clifton L. Smith; David J. Brooks, 2013. Security Science. The Theory and Practice of Security, Butterworth-Heinemann is an imprint of Elsevier, ISBN 978-0-12-394436-8
6. Koller, G., 1999. Risk Assessment and Decision Making in Business and Industry: A Practical Guide. CRC Press, Boca Raton, FL.
7. Koller, G., 2000. Risk Modeling for Determining Value and Decision Making. Chapman and Hall/CRC Press, Boca Raton, FL.
8. Lupton, D., 1999. Risk. Routledge, New York.
9. Roper, C.A., 1999. Risk Management for Security Professionals. Butterworth-Heinemann, Boston.
10. Vaughan, E.J., 1997. Risk Management. John Wiley & Sons, New York.
11. SR ISO 31000, Managementul riscului. Linii directoare
12. SR BS 31100:2013, Managementul riscului. Cod de practică și îndrumare pentru implementarea standardului SR ISO 31000
13. SR EN 31010:2010, Managementul riscului. Tehnici de evaluare a riscurilor
14. SR GHID ISO 73:2010, Managementul riscului. Vocabular

<u>Postul nr. 5</u> – specialist Tehnologii avansate în securitate cibernetică

Tematica

1. Web Development (Javascript/Typescript/Angular/NodeJS/PHP/Python)
2. Mobile Development (Android/Swift)
3. Software Development (C/C++, C#, Java)
4. Arhitecturi avansate de calculatoare
5. Cloud computing
6. Sisteme paralele și distribuite
7. Decision Making Blockchain
8. Structuri Avansate VLSI,
9. Circuite inteligente bazate pe logica fuzzy
10. Sisteme cu microprocesoare avansate
11. Metode și tehnici de programare în High Performance Computing
12. AWS/Microsoft Cloud security
13. Protocoale:TLS, SSL,HTTPS, SSH
14. - Criptografie: AES-256, RSA-2048, SHA-256
15. - Aplicatii in timp real folosind protocolul Websockets Secure si JWT
16. - Cloud security protocols: Secure Single-Sign-On Protocol, Key Management Protocol,
17. Cloud Trust Protocol, Secure Cloud Transmission Protocol, Secure Sessions Protocol
18. - Familiarity with existing and emerging EM tool technologies: SolarWinds, SCOM, and
19. Splunk, Zenoss ZenPack, Zabbix
20. Cloud Security Solutions: Cloud Workload Protection Platform, Cloud Security Posture
21. Management, Cloud Access Security Broker, eXtended Detection and Response(XDR)
22. - AWS cloud monitoring: AWS CloudTrail, AWS CloudWatch, AWS Certificate Manager

Bibliografie

1. "Application Development (AppDev) Defined and Explained". Bestpricecomputers.co.uk. 13 August 2007. Retrieved 5 August 2012.
2. System Development Methodologies for Web-Enabled E-Business: A Customization Framework Linda V. Knight (DePaul University, USA), Theresa A. Steinbach (DePaul University, USA) and Vince Kellen (Blue Wolf, USA)
3. Alan M. Davis. Great Software Debates (October 8, 2004), pp:125-128 Wiley-IEEE Computer Society Press
4. Otero, Carlos. "Software Design Challenges". IT Performance Improvement. Taylor & Francis LLC. Retrieved 19 October 2017.
5. Web Development vs. Software Development
6. Kuhn, D.L (1989). "Selecting and effectively using a computer-aided software engineering tool". Annual Westinghouse computer symposium; 6-7 Nov 1989; Pittsburgh, PA (USA); DOE Project.
7. "Incident Response Policy and Procedure | iCIMS". iCIMS | The Leading Cloud Recruiting Software. Retrieved 13 March 2021.
8. CASE Archived 2012-02-18 at the Wayback Machine definition In: Telecom Glossary 2000 Archived 2005-11-22 at the Wayback Machine. Retrieved 26 Oct 2008.
9. "Incident Response Policy and Procedure | iCIMS". iCIMS | The Leading Cloud Recruiting Software. Retrieved 13 March 2021.
10. "A Framework for a Vulnerability Disclosure Program for Online Systems". Cybersecurity Unit, Computer Crime & Intellectual Property Section Criminal Division U.S. Department of Justice. July 2017. Retrieved 9 July 2018.
11. "Mission and Vision". www.cybercom.mil. Retrieved 20 June 2020.

RECTOR,

Prof.univ.dr.ing. **Violeta Vali CIUCUR**

afișat azi, 02.02.2022, pe site-ul propriu/la avizier