MD-2045, CHIŞINĂU, STR. Studenţilor, 9/7, TEL: 022 50-99-08 [www.utm.md](http://www.utm.md)

**SECURITATEA REȚELELOR INFORMATICE**

1. **Date despre unitatea de curs/modul**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Facultatea** | Calculatoare, Informatică şi Microelectronică | | | | |
| **Catedra/departamentul** | Ingineria Software şi Automatică | | | | |
| **Ciclul de studii** | Studii superioare de master, ciclul II | | | | |
| **Programul de studii** | 061 Tehnologii ale informației și comunicațiilor | | | | |
| **Programul de master** | Tehnologia Informaţiei pentru afaceri | | | | |
| **Anul de studii** | **Semestrul** | **Tip de evaluare** | **Categoria formativă** | **Categoria de opţionalitate** | **Credite ECTS** |
| II (învăţământ cu frecvenţă); | 3; | E | S – unitate de curs de specialitate | O - unitate de curs obligatorie | 5 |

1. **Timpul total estimat**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Total ore în planul de învăţământ | Din care | | | | | |
| Ore auditoriale | | Lucrul individual | | | |
| Curs | Laborator | | Proiect de an | Studiul materialului teoretic | Pregătire aplicaţii |
| 150 | 20 | 20 | | - | 50 | 60 |

1. **Precondiţii de acces la unitatea de curs/modul**

|  |  |
| --- | --- |
| Conform planului de învăţământ | Matematică superioară. Programarea calculatoarelor. Structuri de date și algoritmi. Sisteme de Operare. Administrarea rețelelor. |
| Conform competenţelor | Cunoștințe medii de utilizare și cunoștințe minime de instalare și configurare a sistemelor de operare (Windows, Linux, MacOS). Accesarea și folosirea liniei de comandă.  Abilități de instalare, configurare și utilizare a aplicațiilor de sistem.  Elemente ale teoriei algoritmilor, teoriei grafurilor și ale teoriei așteptării. |

1. **Condiţii de desfăşurare a procesului educaţional pentru**

|  |  |
| --- | --- |
| Curs | Pentru prezentarea materialului teoretic în sala de curs este nevoie de tablă, proiector, PC/laptop și acces la Internet. Nu vor fi tolerate întârzierile studenţilor, precum şi convorbirile telefonice în timpul cursului. |
| Laborator/ seminar | Studenții vor fi evaluați prin teste teoretice, lucrări practice și, în funcție de caz, rapoarte electronice. Evaluările vor avea loc cel puțin peste o săptămână după ce materialul a fost predat la curs.  Termenul de susținere a testelor și/sau a lucrărilor de laborator este de cel mult două săptămâni după finalizarea acestora. Pentru susținerea cu întârziere a testelor sau a lucrărilor de laborator, evaluarea lor se va depuncta cu 1pct./săptămână de întârziere. |

1. **Competenţe specifice acumulate**

|  |  |
| --- | --- |
| Competenţe profesionale | **C5*.*** **Competențe privind arhitectura și infrastructura sistemelor de calcul**   * Identificarea și definirea de componente arhitecturale hardware, software și de comunicații, precum și celor necesare la descrierea unei infrastructuri de calcul. * Explicarea interacțiunii și funcționării componentelor arhitecturale și de infrastructură. * Aplicarea metodelor de bază pentru specificarea de soluții arhitecturale și de infrastructură pentru probleme tipice de calcul. * Utilizarea de criterii și metode de evaluare a caracteristicilor funcționale și nefuncționale ale componentelor de sistem. * Implementarea unei soluții arhitecturale și de infrastructură în baza unor constrângeri enunțate. |
| Competenţe transversale | **CT2*.*** Identificarea, descrierea și derularea activităţilor organizate într-o echipă cu dezvoltarea capacităţilor de comunicare și colaborare, dar și cu asumarea diferitelor roluri (de execuție și conducere).  **CT3*.*** Identificarea necesităților de formare profesională continuă, inclusiv utilizând eficient resursele online de comunicare şi formare profesională (e-mail, cursuri on-line și alte resurse Internet). |

1. **Obiectivele unităţii de curs/modulului**

|  |  |
| --- | --- |
| Obiectivul general | Studierea aspectelor teoretice și formarea abilităților practice de bază privind analiza, funcționarea, și înțelegerea principiilor de securitate, ale tehnologiilor și ale procedurilor utilizate pentru apărarea rețelelor de calculatoare contra atacurilor cibernetice.  Formarea abilităţilor de identificare și soluționare a proceselor care sunt vulnerabile la atacuri cibernetice. |
| Obiectivele specifice | Înțelegerea caracteristicilor criminalilor și eroilor din domeniul securității cibernetice.  Identificarea principiilor confidențialității, integrității și disponibilității în ceea ce privește starea datelor și contramăsurile de securitate cibernetică.  Însușirea tacticilor, tehnicilor și procedurilor folosite de infractorii cibernetici.  Descrierea și aplicarea modului în care tehnologiile, produsele și procedurile sunt utilizate pentru a asigura integritatea.  Determinarea modului în care tehnologiile, produsele și procedurile asigură o disponibilitate ridicată.  Identificarea modului în care profesioniștii în securitate cibernetică folosesc tehnologiile, procesele și procedurile pentru a apăra toate componentele rețelei.  Explicarea scopului legilor legate de securitatea cibernetică |

1. **Conţinutul unităţii de curs/modulului**

|  |  |  |
| --- | --- | --- |
| Tematica activităţilor didactice | Numărul de ore | |
| învăţământ cu frecvenţă | învăţământ cu frecvenţă redusă |
| **Tematica prelegerilor** | | |
| T1. Securitatea Cibernetică – O Lume de Experți și Criminali  Noţiuni generale privind securitatea cibernetică: definiţie, structură, concepte și rolul criminalilor și eroilor în securitatea informaţională. Evoluţia structurii securității cibernetice, a resurselor și aptitudinilor de combatere a atacurilor. | 2 | 1 |
| T2. Cubul de securitate cibernetică  Noțiuni generale, funcțiile de bază ale cubului cibernetic. Dimensiunile cubului cibernetic : principiile securității, stările datelor, contramăsuri de protecție. Cunoașterea cadrului de management al securității. | 3 | 1,5 |
| T3. Amenințări, vulnerabilități și atacuri de securitate cibernetică  Varietatea atacurilor de securitate cibernetică lansate de infractori cibernetici. Tipurile de amenințări, identificarea vulnerabilităților și măsuri de prevenire. | 3 | 1,5 |
| T4. Arta de a proteja parolele secrete  Modelele și tipurile de control ale accesului la date. Compararea algoritmilor de criptare, simetrici și asimetrici. Tehnicile de mascare a datelor : steganografia și obfuscarea. | 2 | 1 |
| T5. Arta de a asigura integritatea  Instrumente de verificare a autenticității mesajelor și documentelor: algoritmi de hash, prelucrarea parolei și a codului de autentificare a mesajelor cu cheie. Aplicarea integrității bazelor de date. | 3 | 1,5 |
| T6. Conceptul Five Nines  Servicii oferite pentru asigurarea disponibilității sistemului. Plan de recuperare a datelor în cazul furturilor de date. | 2 | 1 |
| T7. Protejarea unui domeniu de securitate cibernetică  Tehnologiile, procesele și procedurile folosite pentru apărarea sistemelor, dispozitivelor și datelor care alcătuiesc infrastructura de rețea. Securizarea accesului administrativ, menținerea parolelor și implementarea comunicațiilor securizate. | 2 | 1 |
| T8. Devină un specialist în securitatea cibernetică  Noțiuni generale privind legile care afectează cerințele de tehnologie și securitate cibernetică. Legile : FISMA, GLBA, FERPA, SOX, CIPA. Capacitățile și aptitudinile necesare pentru a deveni specialist în securitatea cibernetică | 3 | 1 |
| **Total prelegeri:** | **20** | **10** |

|  |  |  |
| --- | --- | --- |
| Tematica activităţilor didactice | Numărul de ore | |
| învăţământ cu frecvenţă | învăţământ cu frecvenţă redusă |
| **Tematica lucrărilor de laborator** | | |
| LL1. Specialiști în securitatea cibernetică. | 2 | 1 |
| LL2. Amenințări commune. Arene de amenințare. | 2 | 1 |
| LL3. Certificări de Securitate cibernetică. | 2 | 1 |
| LL4. Modelul ISO al securității cibernetice. | 2 | 1 |
| LL5. Atacuri cibernetice. | 2 | 1 |
| LL6. Obscurizarea datelor. Ofuscarea datelor. Steganografia datelor. | 2 | 1 |
| LL7. Tipuri de controale de integritate a datelor. | 4 | 1 |
| LL8. Protejarea domeniului securității cibernetice. Securitatea fizică. | 2 | 0,5 |
| LL9. Integrarea competențelor în profesia securității cibernetice. | 2 | 0,5 |
| **Total lucrări de laborator:** | **20** | **8** |

1. **Referinţe bibliografice**

|  |  |
| --- | --- |
| Principale | 1. E-learning platform netacad.com 2. CCNA-Routing and Switching – Practice Tests. 3. CCNA-Routing-and-Switching-Complete-Study-Guide-Exam-100-105-Exam-200-105-Exam-200-125-PDF. 4. Donahue, G. Network warrior. – O’Reilly Media, 2011. – 788 p. 5. Balchunas, Aaron. Cisco CCNA Study Gide. 2014. – 321 p. 6. Tomai, N.; Silaghi, Gh.C. Tehnologii şi aplicaţii mobile. – Cluj-Napoca: Risoprint, 2012. – 7. Moise, G.; Constantinescu, Z.; Vlădoiu, M.; Dumitru, M. Networking şi securitate. – Ploiesti: Editura Universității Petrol-Gaze, 2015. |
| Suplimentare | 1. ПОЛНЫЙ КУРС ПО КИБЕРБЕЗОПАСНОСТИ ТОМ 1 СЕКРЕТЫ ХАКЕРОВ, Нейтан Хаус CISSP. CISM. CISA. SCF. Сертифицированный ведущий аудитор ISO 27001  2. The Complete Cyber Security Course, Volume I-VIII HACKERS Exposed |

1. **Evaluare**

|  |  |  |  |
| --- | --- | --- | --- |
| Curentă | | Proiect de an | Examen final |
| Atestarea 1 | Atestarea 2 |
| 30% | 30% | - | 40% |
| Standard minim de performanţă | | | |
| Prezenţa şi activitatea la prelegeri şi lucrări de laborator;  Obţinerea notei minime de „5” la fiecare dintre atestări şi lucrări de laborator;  Susținerea examenului final cu nota „5”. | | | |