**FACULTATEA CALCULATOARE, INFORMATICĂ ȘI MICROELECTRONICĂ**

**DEPARTAMENTUL INGINERIA SOFTWARE ȘI AUTOMATICĂ**

|  |  |  |
| --- | --- | --- |
| **APROBAT**  **la şedinţa Departamentului ISA nr.\_\_\_\_din\_\_\_\_\_\_\_\_\_\_\_\_**  **Șef departament**  **FIODOROV Ion**  **conf. univ., dr.**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | **APROBAT**  **la şedinţa Consiliului Facultăţii CIM**  **nr.\_\_\_\_din\_\_\_\_\_\_\_\_\_\_\_\_**  **Președintele Consiliului CIM**  **CIORBĂ Dumitru,**  **conf. univ., dr.**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
|  |  |  |

|  |  |
| --- | --- |
| **Program de studii:** | 0613.1 Tehnologia informației |
| **Cod, Denumirea modulului:** | D.O.007 Tehnologii ale securității informaționale |
| **Beneficiari:** | studenții anului II universitar, învățământ cu frecvență la zi |
| **Ciclul de învățământ:** | I licență |
| **Numărul de credite ECTS:** | 4 |

**Titularul disciplinei**

lect.univ, ALEXEI Arina

*Nume, prenume, semnătura titularului*

**PRELIMINARII**

Acest curs își propune să ofere o introducere și o privire de ansamblu asupra conceptelor de vulnerabilități, amenințări, atacuri, proceduri și mecanisme de securitate atât în ​​sistemele informatice, cât și în rețelele de calculatoare.

Obiectivele cursului:

* *Analiza atacurilor care se bazează pe factorul uman;*
* *Cunoașterea și utilizarea tehnologiilor pentru asigurarea securității informaționale;*
* *Evaluarea modelelor de amenințări și influența acestora asupra unei organizații;*
* *Crearea politicilor de securitate relevante organizației și mediului;*
* *Compararea diferitelor utilizări și abordări ale criptografiei;*
* *Pregătirea și răspunsul la incidentele de securitate, securizarea sistemelor informaționale;*
* *Studierea atacurilor comune în rețea, controlul accesului.*

1. **PRECONDIŢII DE ACCES LA DISCIPLINĂ**

Pentru a atinge obiectivele cursului studenţii trebuie să posede cunoștințe aferente următoarelor cursuri universitare: Programarea calculatoarelor, Algebra liniară, Matematica discretă.

1. **COMPETENŢELE CARE URMEAZĂ A FI DEZVOLTATE**

**Competenţe profesionale**

***CP1. Elaborarea și proiectarea arhitecturii***

**2P.** Cerințele arhitecturii sistemelor: performanță, mentenabilitate, extensibilitate, scalabilitate, disponibilitate, securitate și accesibilitate.

**4P.** Arhitectura întreprinderii și standardele interne ale companiei.

**15P*.*** Utilizează cunoștințele sale tehnologice din diferite domenii pentru a elabora şi implementa arhitectura întreprinderii.

***CP3. Integrarea componentelor***

**1P.** Componente/module hardware/software, indiferent dacă sunt vechi, existente sau noi.

**18P.** Securizează și face backup-ul datelor pentru a asigura integritatea lor în timpul integrării datelor sau a sistemului.

***CP5. Implementarea soluțiilor***

**5P.** Tehnologiile și standardele care se utilizeză în timpul implementării/ /desfăşurării.

***CP7. Ingineria sistemelor***

**6P.** Bazele securităţii informaţiei

**16P.** Conduce auditurile de gestionare a riscurilor și acționează pentru a reduce impactul acestora.

**17P.** Aplică arhitecturi software și/sau hardware adecvate.

***CP8. Managementul problemelor***

**17P.** Alocă resurse adecvate activităților de întreținere, luând în considerare costurile și riscurile.

**Competențe transversale**

**22 T.** Demonstrează executarea responsabilă a sarcinilor profesionale în condiţii de autonomie.

**24 T.** Conştientizează nevoia de formare continuă cu utilizarea eficientă a resurselor şi tehnicilor de învăţare pentru dezvoltarea personală şi profesională.

1. **ADMINISTRAREA DISCIPLINEI/MODULULUI**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cod** | **Anul** | **Semestrul** | **Numărul de ore** | | | | | | **Credite** |
| **Curs** | **Seminar** | **Lucrări de laborator** | **Lucrări practice** | **Proiectare** | **Lucrul individual** |
| D.O.007 | **Învăţământ cu frecvenţă** | | | | | | | | |
| II | IV | 30 |  | 30 |  |  | 60 | 4 |

1. **REZULTATELE ÎNVĂŢĂRII, CONŢINUTURI ŞI METODE DIDACTICE APLICATE**

| **Rezultatele învăţării.**  **Studentul trebuie:** | **Conţinuturi** | | **Metode de predare** | **Realizarea în timp (ore)** | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Curs** | **Lucrări de laborator** |  | **învăţământ cu frecvenţă** | | | |
| **curs** | **sem** | **lab** | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | |
| ***În rezultatul însuşirii temei studentul trebuie:***  ***să cunoască:***   * + *Domeniile cibernetice,*   + *Tipuri de date și starea datelor în sistemele cibernetice,*   + *Criminalii în securitate cibernetică,*   + *Amenințările comune, răspândire și complexitate,*   + *Instrumente utile pentru atenuarea atacurilor cibernetice.*   ***să fie capabil:***   * *Analizeze atacurile cibernetice la nivel internațional,* * *Analizeze și exemplifice tehnicile și tacticile atacatorilor ce utilizează ingineria socială,* * *Configureze un server FTP, WEB server, server Email, server DNS, server NTP, server AAA.* | 1. Prezentare generală a securității informaționale. | LL1. Analiza incidentelor de securitate cu impact major din ultimii 5 ani. | * Expunerea materialului, * Prezentare PowerPoint cu utilizarea tablei interactive, * Materiale video demonstrative de pe Youtube, * Demonstrații în timp real * Mediul de simulare PacketTracer. | **2** |  | **2** | |
| 2. Bazele securității informaționale și importanța factorului uman | LL2. Explorarea tehnicilor de inginerie socială. | **2** |  | **2** | |
| 3. Securitatea informației în sistemele informaționale | LL3. Configurarea unui mediu cibernetic protejat. | **2** |  | **2** | |
| ***În rezultatul însuşirii temei studentul trebuie:***  ***să cunoască:***   * *Dimensiunile cubului de securitate informațională,* * *Principiul de Confidențialitate și principalele provocări,* * *Principiul de Integritate și principalele provocări,* * *Principiul de Disponibilitate și principalele provocări,* * *Tehnologii de securizare,* * *Politici și proceduri de securitate informațională,* * *Modelul ISO de securitate informațională,* * *Legile, directivele, strategiile, HG ale RM aferent securității informaționale.*   ***să fie capabil:***   * *Transmite email între utilizatori,* * *Încarce/descarce fișiere folosind FTP,* * *Acceseze la distanță routerul organizației folosind Telnet,* * *Acceseze la distanță routerul organizației folosind SSH,* * *Instaleze mașini virtuale,* * *Configureze în Ubuntu mecanisme de autentificare, autorizare și contabilizare.* | 4. Securitatea informației pentru dispozitivele terminale | LL4. Configurarea politicilor locale de securitate în Windows | * Expunerea materialului, * Prezentare PowerPoint cu utilizarea tablei interactive, * Materiale video demonstrative de pe Youtube, * Demonstrații în timp real * Mediul de simulare PacketTracer, * Mașina virtuală. | **2** |  | **2** | |
| 5. Tehnologii ale securității informaționale: Firewall și VPN | LL5. Configurare Windows Firewall. Configurarea modului de transport VPN | **2** |  | **2** | |
| 6. Tehnologii ale securității informaționale: Sisteme de detecție a intruziunilor, controlul accesului și alte instrumente | LL6. Instalarea mașinii virtuale Ubuntu pe PC. Configurarea mecanismelor de autentificare, autorizare și contabilizare. | **2** |  | **2** | |
| 7. Securitatea informației și criptografia | LL7. Criptarea fișierelor și datelor. | **2** |  | **2** | |
| ***În rezultatul însuşirii temei studentul trebuie:***  ***să cunoască:***   * *Tipurile programelor malițioase,* * *Tipurile atacurilor cibernetice la email și browser,* * *Tipurile atacurilor cibernetice în rețea,* * *Tipurile atacurilor cibernetice în rețelele wireless și dispozitivele mobile,* * *Tipurile atacurilor cibernetice la aplicații,* * *Securitatea sistemelor de operare,* * *Soluții anti-malware,* * *Managementul patch-urilor,* * *Firewalluri bazate pe host și sisteme de detecție a intruziunilor,* * *Comunicații sigure,* * *Controlul accesului la fișiere,* * *Criptarea fișierelor,* * *Protecția fizică a unei stații de lucru,*   ***să fie capabil:***   * *Configureze politici de securitate locale,* * *Configureze firewall,* * *Configureze VPN,* * *Aplice instrumente pentru detectarea amenințărilor și vulnerabilităților de securitate,* * *Configureze comunicațiile wireless,* * *Cripteze date simetric și asimetric,* * *Utilizeze semnăturile digitale.* | 8. Criptografia simetrică. Algoritmi și standarde de criptare simetrică | LL8. Utilizarea criptării simetrice. | * Expunerea materialului, * Prezentare PowerPoint cu utilizarea tablei interactive, * Materiale video demonstrative de pe Youtube, * Demonstrații în timp real * Mediul de simulare PacketTracer, * Mașina virtuală. | **2** |  | **2** | |
| 9. Criptografia asimetrică. Algoritmi și standard de criptare asimetrică | LL9. Utilizarea verificărilor de integritate a datelor și fișierelor | **2** |  | **2** | |
| 10. Integritatea datelor și semnătura digitală | LL10. Utilizarea semnăturilor digitale | **2** |  | **2** | |
| 11. Riscul managementului de securitate | LL11. Identificarea activelor informaționale. Detectarea amenințărilor și vulnerabilităților de securitate | **2** |  | **2** | |
| 12. Aspecte practice ale managementului riscului | LL12. Evaluarea riscului informațional. Completarea planului de tratare a riscului informațional | **2** |  | **2** | |
| 13. Managementul riscului de Securitate într-o organizație | LL13. Crearea unui SMSI pentru o organizație | **2** |  | **2** | |
| 14. Politici, proceduri și standarde de securitate | LL14. Crearea unei politici generice și a unei politici specifice pentru organizație | **2** |  | **2** | |
| 15. Discuții finale | LL15. Prezentarea rezultatelor obținute | **2** |  | **2** | |

1. **SUGESTII PENTRU ACTIVITATEA INDIVIDUALĂ A STUDENŢILOR**

| **Nr. crt.** | **Capitol, temă** | **Conținut activitate individuală** | **Durataore** | **Forma de control** | **Termeni de control (perioada)** |
| --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** |
|  | 1. Prezentare generală a securității informaționale.  LL1. Analiza incidentelor de securitate cu impact major din ultimii 5 ani. | Crearea unui mindmap la temă. Identificare informații suplimentare.  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
| 1. **2** | 2. Bazele securității informaționale și importanța factorului uman  LL2. Explorarea tehnicilor de inginerie socială. | Crearea unui mindmap la temă. Identificare informații suplimentare.  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 3. Securitatea informației în sistemele informaționale  LL3. Configurarea unui mediu cibernetic protejat. | Crearea unui mindmap la temă. Identificare informații suplimentare.  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 4. Securitatea informației pentru dispozitivele terminale  LL4. Configurarea politicilor locale de securitate în Windows | Crearea unui mindmap la temă. Identificare informații suplimentare.  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 5. Tehnologii ale securității informaționale: Firewall și VPN  LL5. Configurare Windows Firewall. Configurarea modului de transport VPN | Crearea unui mindmap la temă. Identificare informații suplimentare.  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 6. Tehnologii ale securității informaționale: Sisteme de detecție a intruziunilor, controlul accesului și alte instrumente  LL6. Instalarea mașinii virtuale Ubuntu pe PC. Configurarea mecanismelor de autentificare, autorizare și contabilizare. | Crearea unui mindmap la temă. Identificare informații suplimentare.  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 7. Securitatea informației și criptografia  LL7. Criptarea fișierelor și datelor. | Crearea unui mindmap la temă. Identificare informații suplimentare.  Rezolvarea exercițiilor  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 8. Criptografia simetrică. Algoritmi și standarde de criptare simetrică  LL8. Utilizarea criptării simetrice. | Crearea unui mindmap la temă. Identificare informații suplimentare.  Rezolvarea exercițiilor  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 9. Criptografia asimetrică. Algoritmi și standard de criptare asimetrică  LL9. Utilizarea verificărilor de integritate a datelor și fișierelor | Crearea unui mindmap la temă. Identificare informații suplimentare.  Rezolvarea exercițiilor  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 10. Integritatea datelor și semnătura digitală  LL10. Utilizarea semnăturilor digitale | Crearea unui mindmap la temă. Identificare informații suplimentare.  Rezolvarea exercițiilor  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 11. Riscul managementului de securitate  LL11. Identificarea activelor informaționale. Detectarea amenințărilor și vulnerabilităților de securitate | Crearea unui mindmap la temă. Identificare informații suplimentare.  Rezolvarea exercițiilor  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 12. Aspecte practice ale managementului riscului  LL12. Evaluarea riscului informațional. Completarea planului de tratare a riscului informațional | Crearea unui mindmap la temă. Identificare informații suplimentare.  Rezolvarea exercițiilor  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 13. Managementul riscului de Securitate într-o organizație  LL13. Crearea unui SMSI pentru o organizație | Crearea unui mindmap la temă. Identificare informații suplimentare.  Cercetarea și Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 14. Politici, proceduri și standarde de securitate  LL14. Crearea unei politici generice și a unei politici specifice pentru organizație | Crearea unui mindmap la temă. Identificare informații suplimentare.  Elaborarea raportului și pregătirea pentru susținerea lucrării de laborator | 2  2 | Încărcarea pe platforma MOODLE  Susținere lucrare de laborator | 1 săptămână |
|  | 15. Discuții finale  LL15. Prezentarea rezultatelor obținute | Pregătirea prezentării portofoliului  Prezentarea portofoliului | 2  2 | Încărcarea pe platforma MOODLE | 1 săptămână |
| **Total** | | | 60 |  |  |

1. **EVALUAREA DISCIPLINEI**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Periodică** | | **Curentă** | **Studiu individual** | **Proiect/teză** | **Examen** |
| **EP 1** | **EP 2** |
| **Învăţământ cu frecvenţă** | | | | | |
| 15% | 15% | 15% | 15% |  | 40% |
| **Învăţământ cu frecvenţă redusă** | | | | | |
| 25% | | | 25% | | 50% |
| Standard minim de performanță:   * Prezenţa şi activitatea la cursuri, lucrări de laborator; * Obţinerea notei minime de „5” la evaluările periodice, activitatea curentă, lucrul individual; * Obţinerea notei minime de „5” la examenul final. | | | | | |

**VIII. CRITERII DE EVALUARE**

| **Denumire** | **Modul de desfăşurare** | **Pondere pe componente de conţinut** |
| --- | --- | --- |
| **Învăţământ cu frecvenţă** | | |
| **Evaluare curentă** |  | **15%** |
|  | ***Susținerea lucrărilor de laborator*** | *50%* |
| ***Implicarea în procesul de învățare activă la cursuri*** | *25%* |
| ***Rezultatele mini-testelor curente realizate la orele de curs*** | *25%* |
| **Studiu individual** |  | **15%** |
| Sarcina 1: Crearea mindmap-urilor la temele studiate la curs | Prezentare la temă  Rezolvarea exercițiilor | *50%* |
| Sarcina 2: Realizarea a 2 politici de securitate pentru o organizație | Portofoliu prezentat spre evaluare | *50%* |
| **Evaluare periodică** |  |  |
| EP 1 | Test pe platforma Moodle | **15%** |
| EP 2 | Test pe platforma Moodle | **15%** |
| **Proiect/teză** |  |  |
| **Examen semestrial** | Scris, în baza biletului individual | **40%** |

**IX. LISTA DE SUBIECTE PENTRU EVALUĂRI PERIODICE ŞI CEA FINALĂ**

**Chestionar pentru EP I**

**Va include subiectele temelor 1-7**

1. Prezentare generală a securității informaționale:

* Definirea securității informaționale
* Exemple relevante despre incidentele de securitate
* Managementul securității informaționale

2. Bazele securității informaționale și importanța factorului uman

* Principiile fundamentale ale securității informaționale
* Terminologie de bază în securitatea informațională
* Importanța factorului uman
* Profilul infractorilor cibernetici
* Tehnici de inginerie socială

3. Securitatea informației în sistemele informaționale

* Amenințări comune și specifice ale sistemelor informaționale
* Atacuri în sistemele informaționale
* Atacuri la servere: WEB, Email, FTP, NTP, AAA
* Tacuri de refuz al serviciului
* Atacuri în rețelele informaționale de comunicații

4. Securitatea informației pentru dispozitivele terminale

* Atacuri și contamăsuri pentru dispozitivele terminale
* Programe malițioase
* Infectarea dispozitivelor terminale

5. Tehnologii ale securității informaționale: Firewall și VPN:

* Tipuri de firewall
* Configurare firewall
* Tipuri de VPN
* Configurare VPN

6. Tehnologii ale securității informaționale: Sisteme de detecție a intruziunilor, controlul accesului și alte instrumente:

* Tipuri de sisteme de detecție a intruziunilor
* Configurare server AAA

7. Securitatea informației și criptografia:

* Cerințe pentru comunicații securizate
* Definirea termenilor specifici criptografie
* Criptografia clasică
* Criptografia modernă

**Chestionar pentru EP a II-a**

**Va include subiectele temelor 8-14**

1. Criptografia simetrică. Algoritmi și standarde de criptare simetrică:

* Concepte de bază și definirea termenilor
* Algoritmi de criptare simetrică
* Tipuri de criptare simetrică
* Utilizarea în sistemele informaționale

1. Criptografia asimetrică. Algoritmi și standard de criptare asimetrică:

* Concepte de bază și definirea termenilor
* Algoritmi de criptare asimetrică
* Tipuri de criptare asimetrică
* Utilizarea în sistemele informaționale

1. Integritatea datelor și semnătura digitală:

* Funcții hash
* Algoritmi de generare a semnăturilor digitale

1. Riscul managementului de securitate:

* Procesul de management al riscului
* Identificarea activelor informaționale importante
* Analiza metodelor de realizare a evaluării riscului informațional
* Tratarea riscului informațional

1. Aspecte practice ale managementului riscului:

* Calcularea valorii activelor informaționale dintr-o organizație
* Utilizarea unei metode de calcul al riscului
* Cerințe de securitate

1. Managementul riscului de Securitate într-o organizație:

* Guvernanța securității informaționale
* Sisteme de management a securității informaționale SMSI

1. Politici, proceduri și standarde de securitate:

* Politici, proceduri și standarde de securitate informațională
* Evaluarea securității informaționale

**Chestionar pentru examen**

1. Prezentare generală a securității informaționale.

2. Bazele securității informaționale și importanța factorului uman

3. Securitatea informației în sistemele informaționale

4. Securitatea informației pentru dispozitivele terminale

5. Tehnologii ale securității informaționale: Firewall și VPN

6. Tehnologii ale securității informaționale: Sisteme de detecție a intruziunilor, controlul accesului și alte instrumente

7. Securitatea informației și criptografia

8. Criptografia simetrică. Algoritmi și standarde de criptare simetrică

9. Criptografia asimetrică. Algoritmi și standard de criptare asimetrică

10. Integritatea datelor și semnătura digitală

11. Riscul managementului de securitate

12. Aspecte practice ale managementului riscului

13. Managementul riscului de Securitate într-o organizație

14. Politici, proceduri și standarde de securitate

**X. REFERINŢE BIBLIOGRAFICE**

**Obligatorii**

1. Michael E. Whitman and Herbert J. Mattord - Principles of Information Security, ISBN-13: 978-1337102063, 2013.
2. Christof Paa and Jan Pelzl - Understanding Cryptography: A Textbook for Students and Practitioners, 2010. Springer.
3. www.netacad.com,
4. Anderson R. – Security Engineering : A Guide to Building Dependable Distributed Systems, NY,2001;
5. Andress, M. – Surviving Security: How to Integrate People, Process and Technology, SAMS, Indianapolis, 2002;
6. Davis D. – "The Problems Catch Up With The Solution", in Card Technology, April 2003;
7. Ioan-Cosmin MIHAI – Securitatea informațiilor, Editura Sitech, 2012;

ISBN 978-606-11-29203-4;

1. King, C.M., Dalton, C.E., Osmanaglu, T.E. – Security Arhitecture: Design, Deployment&Operations,Osborne/McGraw-Hill, New York, 2001;
2. Krutz R.L, Vines R.D. – The CISSP Prep Guide – Mastering the Ten Domains of Computer Security, Wiley & Sons, Inc. New York, 2001;
3. Schwartan W. – Information Warfare, 2nd Edition , Thunder's Mouth Press, New York,

1996;

1. Ioan-Cosmin MIHAI – Securitatea sistemului informatic, Editura Dunărea de Jos, 2007

ISBN 978-973-627-369-8;

1. Victor Valeriu PATRICIU, Monica Ene PIETROSANU, Ion BICA, Justin PRIESCU –

Semnături electronice și securitate informatică, Editura All, 2006;

1. Aurel Serb, Constantin Baron, Narcisa Isaila, Securitatea informatica in societatea

informationala, Bucuresti: Pro Universitaria, 2013;

1. Smart N. Информационная безопасность, Moscova, Tehnosfera 2006;
2. Steven M. Bellovin, Michael Merritt - Limitations of the Kerberos Authentication System, AT&T Bell Labs,2010;

**Suplimentare**

1. Leitner Achim, "Reţele WLAN sigure, cu un tunel OpenVPN criptat", Linux Magazin, nr. 22, iunie 2005;
2. OpenVPN: http:// openvpn. sourceforge. Net;
3. Biblioteca LZO: http:// www. oberhumer. com/opensource/ lzo/;
4. Proiect OpenSSL: http:// www. openssl. org/;

Driver TUN/ TAP: http:// vtun. sourceforge. net/ tun/;

1. Thomas T., Primii paşi în securitatea reţelelor, Corint, Bucureşti, 2005;
2. Lachi A., Securitatea Sistemelor Informaționale, Partea I, Îndrumar de laborator, UTM,

Chișinău, 2011;

1. Lachi A., Securitatea Sistemelor Informaționale, Partea I, Îndrumar de laborator, UTM,

Chișinău, 2015;

1. www.squid-cache.org
2. http://www.wingate.com/download.php