

**Universitatea Tehnică a Moldovei**

**MANAGEMENTUL SECURITĂȚII REȚELELOR CORPORATIVE**

**Masterand:  
Dilevschi Sergiu**

**Conducător:  
Prof. univ., dr. hab.  
Guțuleac Emilian**

**Chișinău – 2016**

**Ministerul Educației al Republicii Moldova**  
**Universitatea Tehnică a Moldovei**  
**Facultatea Calculatoare, Informatică**  
**și Microelectronică**  
**Catedra Calculatoare**

**Admis la susținere**

Șef de catedră: conf. univ, dr. V. Sudacevski

---

„\_\_” \_\_\_\_\_ 2016\_

**MANAGEMENTUL SECURITĂȚII REȚELELOR CORPORATIVE**

**Teză de master în**  
**Calculatoare**

---

*(programul de masterat)*

**Masterand:** \_\_\_\_\_ (S. Dilevski \_\_)

**Conducător:** \_\_\_\_\_ (E. Guțuleac \_\_)

**Chișinău – 2016**

## **Declarația de onestitate**

## Adnotare

La teza de master cu tema “Managementul securității rețelelor corporative”, prezentată de către masterantul Dilevschi Sergiu, este scrisă în limba română și este desfășurată pe trei capitole.

Această teză este dedicată studiului tehnologiilor utilizate pentru implementarea și întreținerea managementului securității rețelelor corporative bazată pe cercetarea rețelelor a două companii diferite după necesități, structură, sistem de operare și licențiere. Scopul acestei lucrare este studiului modelelor de securizare a rețelelor.

Motivul principal de a executa cercetarea dată constă interesul deosebit față de sistemele de securizare și metodelor de combatere a infracțiunilor electronice, care este o problemă actuală, unde zi de zi apar noi tehnologii atât de securizare cât și combatere a acestor tehnologii.

Teza include: introducerea în domeniul tehnologiilor de administrare a rețelelor; analiza situației în domeniul respectiv; analiza sistemelor de operare, lideri în domeniu; analiza riscurilor; managementul riscurilor; metode și tehnici de securizare a datelor în cazurile excepționale; analiza tipurilor de atacuri și metodelor de combatere a acestora; analiza comparativă în baza a două exemple cu structură și funcționalitate complet diferite, dar cu aceleași scopuri de funcționalitate, a managementului securității rețelor bazate pe exemple.

Lucrarea de master include 3 capitole pe 68 de pagini text de bază, 1 anexă, 7 listinguri și 27 de figuri.

Cuvintele cheie: Securitate; Sistem de operare; Rețele; Servicu; Firewall; Management.

## **Annotation**

This Thesis Corporate network security management presented by Sergiu Dilevschi as Master project is written in Romanian and is developed in three chapters.

This thesis is dedicated to analyze used technologies for implementation and maintenance of corporate networks management, based on networks researching of two different companies in structure, necessities, operating system and software licencing.

The main reason to perform this research is particular interest beside method of cybercrime and data securization, which is an current problem and in this domain every day are new technologies so as to secure and combat these technologies.

This thesis includes: network management technologies ; domain analysis of the situation in the field; operating systems description and analysis, leaders in the world; risks analysis ; risks management; methods and techniques of data security in different cases; Analysis of network attacks and methods to combat them; Comparative analysis on two examples of completely different structure and functionality, but with the same goals, security management, network based on.

Master thesis includes three chapters on 68 pages basic text, 1 annex, 7 listings and 27 figures.

Thesis keywords: Security; Operating system; Networking; Service; Firewall; Management.

## Cuprins

Lista figurilor.....	6
Abrevieri.....	7
Introducere .....	8
1. Analiza situației domeniului de proiectare.....	11
1.1. Noțiuni introductive .....	11
1.2. Sistemele de operare.....	12
1.2.1. Sistemul de operare „MS Windows” .....	12
1.2.2. Sistemul de operare „MAC OS” .....	14
1.2.3. Sistemul de operare „Linux” .....	14
1.2.4. Selectarea sistemului de operare. ....	16
1.3. Securitatea și Vulnerabilitatea rețelelor .....	17
1.4. Firewall.....	24
1.5. Limitarea accesului fizic la rețea, DHCP serverul. ....	27
2. Metode, tehnici și tehnologii pentru combatere a riscurilor, securizarea rețelelor și datelor.....	29
2.1. Analiza riscurilor.....	30
2.2. Managementul riscurilor. ....	32
2.3. Metode și tehnici de securizare a datelor la nivel local.....	35
2.3.1. RAID (Redundant Array of Inexpensive Disks). ....	36
2.3.2. Criptarea datelor.....	38
2.4. Tipuri de atacuri a rețelelor și metodele de combatere a lor. ....	39
3. Analiza comparativă a securității corporative prin exemple, abordarea practică securității rețelelor.....	45
3.1. Analiza sistemului firewall, iptables în cauză. ....	45
3.2. Serviciile DHCP și DNS. ....	48
3.2.1. Serviciul DHCP.....	48
3.2.2. Serviciul DNS. ....	50
3.3. Filtrarea traficului prin proxy server. ....	51
3.4. Calculatoarele utilizatorilor, restricționarea accesurilor. ....	54
3.5. Accesul de la distanță.....	59
3.5. Managementul serviciilor și tehnicii.....	65
3.5.1. Serviciul NetMan. ....	65
3.5.2. Serviciul OCS Inventory. ....	69
3.5. Analiza fișierelor Log.....	72
3.5. Generalități.....	73
Concluzii .....	75
Bibliografie.....	76
Anexa 1. Codul script Generate.sh.....	77

## Lista figurilor

1.1 Clasificarea tipurilor de incidente.....	23
1.2 Dispunerea unui firewall.....	24
2.1 RAID 0.....	37
2.2 RAID 1.....	37
2.3 RAID 5.....	38
3.1 Fluxul datelor prin iptables.....	46
3.2 Permisunile structurate pe mape.....	52
3.3 Directoriul ce conține imagini ale sistemelor de operare.....	54
3.4 Logarea utilizatorului.....	55
3.5 Directoriul ce conține scripturile.....	57
3.6 Scriptul sync_users.sh fără parametri.....	58
3.7 Cronurile.....	59
3.8 Power management unit control.....	61
3.9 Elemente din sshd_config.....	64
3.10 Conecțiunea prin telnet-ssh.....	64
3.11 Adăugarea dispozitivului.....	65
3.12 Interfața de bază a NetMan-ului.....	66
3.13 Raportul DHCP.....	67
3.14 Fișierul de acces al serviciului squid.....	68
3.15 NetMant activity report.....	68
3.16 OCS, activitatea calculatoarelor.....	69
3.17 OCS, informația despre “Hardware”.....	70
3.18 OCS, informația despre un dispozitiv.....	70
3.19 OCS, Selecția în baza criteriilor.....	71
3.20 Conținutul raportului de avertizare.....	72
3.21 Structura rețelei, MS Windows.....	73
3.22 Structura rețelei, Linux.....	74