UNIVERSITATEA TEHNICĂ A MOLDOVEI

SISTEM DE DETECTARE ȘI PREVENIRE A ATACURILOR CIBERNETICE

Masterand:

Nour Iurie

Conducător:

conf.dr. Sudacevschi Viorica

Chișinău - 2018

ADNOTARE

Nour Iurie, “ Sistem de detectare și prevenire a atacurilor cibernetice”, teză de masterat, Universitatea Tehnică a Moldovei, or. Chişinău, 2018.

Teza cuprinde introducere, trei compartimente, concluzii şi recomandări, bibliografia de 17 titluri şi este perfectată pe 80 pagini, din care 72 pagini partea de bază, inclusiv 23 figuri, şi 5 tabele.

Cuvintele cheie: securitatea rețelelor informaționale, analiza riscurilor şi vulnerabilităților, instrumentele securității, securitatea informației, procesul modelării informaţionale, politica de securitate; sistem de management al securităţii informaţiei, securitatea VPN, detecţie şi prevenţie a intruziunilor.

Scopul şi obiectivele lucrării. Constă în determinarea unor priorităţi de consolidare a securității sistemului informațional, prin eficientizare utilizării instrumentelor de securizare a informaţiei şi creşterea performanţei prin implementarea sistemului de detecție ale intruziunilor și monitorizarea securității rețelelor.

Asigurarea scopului propus presupune realizarea următoarelor *obiective*: stabilirea, analiza şi verificarea vulnerabilităţii SI, evaluarea riscurile de securitate a informaţiei, şi implementarea sistemul de detecție și prevenție ale intruziunilor și monitorizarea securității rețelei informaționale.

Această lucrare reprezintă un studiu ce ține de asigurarea securității informaționale în rețelele informaționale, fiind abordate subiectele referitoare la importanţa protejării reţelelor de comunicaţii şi organizarea securităţii informaţionale, precum și respectarea culturii securităţii informaţiei, prin intermediul iniţiativelor, angajaţilor la ridicarea nivelului de protecție a Sistemelor Informaţionale .

Un rol deosebit în lucrare îl ocupă partea teoretică, unde sunt descrise aspectele legate de organizarea și modelarea securității informaționale, politicile și procedurile de securitate, pericolele la care sunt expuse rețelele de comunicații, instituţiile Republicii Moldova implicate în procesul de asigurare a securităţii informaţionale și cadrul normativ de asigurare a securităţii informaționale. De asemenea se relatează că orice sistem informaţional este vulnerabil chiar şi într-o reţea cu securitate ridicată, însă politica de securitate este cea care, pe baza analizei de securitate a unei rețele, exprimă cel mai bine principiile care stau la baza adoptării unei anumite strategii de securitate, implementată prin diverse măsuri specifice, cu tehnici şi protocoale adecvate.

În partea practică a tezei este propusă o metodă de detecţie şi prevenţie a intruziunilor (IDPS) ce pot servi ca suport într-un studiu mai aprofundat în securitatatea reţelei şi gestionarea conturilor de utilizator, securitatea aplicaţiilor şi a datelor, nivelurile de securitate în sistemele de operare Windows al unui sistemului informaţional. Evenimentele provocate până în prezent de breşele de securitate din reţelele de comunicaţii demonstrează că indiferent de cât de sigur pare a fi un sistem, un nivel adecvat de securitate poate fi atins doar dacă este protejat şi mediul de transmisie.

ANNOTATION

Nour Iurie " Cyber attack detection and prevention system ", master thesis, Technical Universities of Moldova, Chisinau, 2018.

The thesis contains an introduction, three chapters, conclusions and recommendations, bibliography of 17 titles and is perfect on 80 pages, 72 pages main part, including 23 figures and 5 tables.

Keywords: security of information networks, analyze risks and vulnerabilities, security tools, information security, information modeling process, security policy; information security management system, security, VPN, intrusion detection and prevention.

The purpose and objectives. It is to determine priorities for strengthening information system security by efficient use of information security tools and increased performance through the implementation of intrusion detection system and network security monitoring.

Ensuring purpose involves the following objectives: establish, analysis and verification vulnerability, assess information security risks, and implementation of intrusion detection system and network security monitoring information.

This work is a study related to information security in information networks, addressing topics related to the importance of protecting communications networks and organization of information security and compliance culture of information security through initiatives, employees from raising protection Information Systems.

A special role in the work is granted by theoretical part, which describes aspects of the organization and shaping information security policies and security procedures, the dangers posed to communications networks, institutions of the Republic of Moldova involved in information security and regulatory framework, the information security of the country. Also it is reported that any information system is vulnerable even in a network with high security, but security policy is what, based on the security of a network, best expresses the principles underlying the adoption of a particular strategy security measures implemented by various specific techniques and appropriate protocols.

In the practical part of the thesis proposes a method of detection and intrusion prevention (IDPS) that can serve as support in further study in securitatatea network and managing user accounts, application security and data security levels in systems Windows operating system information. The events caused so far by security breaches in communications networks demonstrates that no matter how secure a system seems to be an appropriate level of security can be achieved only if it is protected and the transmission medium.

CUPRINS