

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicații și Sisteme Electronice

Admisă la susținere
Șefa departament TSE:
conf.univ., dr. Valentina Tîrșu

” _____ ” _____ 2024

Analiza schimbului de date securizat în rețelele de comunicații

Proiect de licență

Studenta: _____ **Șevcenco Tatiana, grupa IMTC-191**

Coordonator: _____ **Nistiriuc Pavel, conf.univ., dr.**

Consultant: _____ **Grițco Maria, asistentă univ.**

Chișinău, 2024

ADNOTARE

Șevcenco Tatiana, studenta grupei IMTC-191

Tema proiectului: Analiza schimbului de date securizat în rețelele de comunicații.

Proiectul de licență este constituit din introducere, trei capitole, concluzii și bibliografie.

Cuvintele cheie: rețele de comunicații, schimb de date securizat, steganografie, firewall, openVPN.

Scopul proiectului constă în studiul și aplicarea diferitor tehnici și tehnologii de asigurare a schimbului de date securizat în rețelele de comunicații ce va contribui la buna funcționare a obiectelor supuse riscurilor și la elaborarea politicilor și managementului de securitate.

Utilizarea eficientă a tehnicilor și tehnologiilor de asigurare a informației în rețelele de comunicații este determinată de următoarele obiective:

1. Familiarizarea cu tehnica și utilizarea unei aplicații de ascundere a informației în rețelele de comunicații prin steganografie;
2. Analiza funcționării, rolului și configurării unui firewall în securitatea rețelelor de comunicații;
3. Analiza funcționalității rețelelor virtuale private, tunelelor între două sisteme pe Internet și configurarea Open VPN.

Au fost efectuate ascunderea unui fișier de text în spatele unei imagini, care poate fi JPG, BMP, TIF, PGN etc. prin utilizarea ferestrei de deschidere a aplicației de steganografie și descoperirea unui fișier ascuns. A fost efectuată verificarea stării Windows Firewall și adăugarea unei excepții în Windows Firewall. Au fost determinate problemele de compatibilitate cu ISP, hardware și software, modalitățile de păcălire a Firewall/IDS-urilor și de ascundere a identității. Pentru rețelele de comunicații cu comutații de etichete a fost instalat OpenVPN cu configurarea unui tunel între sistemul server VPN și sistemul client VPN cu verificarea funcționalității tunelului creat și determinarea metodelor de autentificare bazate pe certificate, smart-carduri, chei unice etc și modalitățile de portabilitate cu asigurarea suportului pentru diferite platforme ca Linux, Windows, OpenBSD etc. La fel au fost determinate cerințele ergonomice către locul de muncă și valorile utilităților de ansamblu pentru a elabora relația de preferință, care va confirma varianta optimă de justificare economică a proiectului.

ANNOTATION

Sevcenco Tatiana, student of IMTC-191 group

Project theme: Analysis of secure data exchange in communication networks.

The draft license consists of an introduction, three chapters, conclusions and a bibliography.

Keywords: communication networks, secure data exchange, steganography, firewall, openVPN.

The purpose of the project consists in the study and application of different techniques and technologies to ensure secure data exchange in communication networks that will contribute to the proper functioning of objects subject to risks and to the development of security policies and management.

The effective use of information assurance techniques and technologies in communication networks is determined by the following objectives:

1. Familiarization with the technique and use of an application for hiding information in communication networks through steganography;
2. Analysis of the operation, role and configuration of a firewall in the security of communication networks;
3. Analysis of the functionality of virtual private networks, tunnels between two systems on the Internet and Open VPN configuration.

Hiding a text file behind an image, which can be JPG, BMP, TIF, PGN, etc., has been performed. by using the opener of the steganography application and discovering a hidden file. Windows Firewall status check was performed and an exception was added to Windows Firewall. ISP, hardware and software compatibility issues, ways to fool Firewall/IDS and hide identity have been determined. For communication networks with label switching, OpenVPN was installed with the configuration of a tunnel between the VPN server system and the VPN client system with the verification of the functionality of the created tunnel and the determination of authentication methods based on certificates, smart cards, unique keys, etc. and the portability methods with providing support for different platforms such as Linux, Windows, OpenBSD, etc. In the same way, the ergonomic requirements for the workplace and the overall utility values were determined in order to elaborate the relationship of preference, which will confirm the optimal variant of the economic justification of the project.

CUPRINS

INTRODUCERE	10
1 DESCRIEREA SCHIMBULUI DE DATE SECURIZAT ÎN REȚELELE DE COMUNICAȚII	12
1.1 Steganografia.....	12
1.2 Mecanisme utilizate în securitatea rețelelor de comunicații.....	13
1.3 Rețelele de comunicații VPN.....	20
2 STUDII DE CAZ	26
2.1 Steganografia ca metodă de securitate a informațiilor.....	26
2.2 Analiza Firewall-urilor.....	29
2.3 OpenVPN.....	39
2.4 Cerințele ergonomice către locul de muncă.....	44
3 JUSTIFICAREA ECONOMICĂ A PROIECTULUI	46
3.1 Analiza axiomelor metodei utilităților.....	46
3.2 Elaborarea matricei criteriilor de apreciere.....	46
3.3 Determinarea utilităților pentru fiecare soluție.....	48
CONCLUZII	50
BIBLIOGRAFIE	51

INTRODUCERE

Societatea îmbrățișează din ce în ce mai mult tehnologia informației. Informația care până nu de mult avea la bază hârtia, îmbracă acum forma electronică. Informația pe suport de hârtie mai este încă rezervată documentelor oficiale, acolo unde este necesară o semnătură sau o stampilă. Adoptarea semnăturii electronice deschide însă perspectiva digitizării complete a documentelor, cel puțin din punct de vedere funcțional.

Acest nou mod de lucru, în care calculatorul a devenit un instrument indispensabil și un mijloc de comunicare prin tehnologii precum poșta electronică sau Internetul, atrage după sine riscuri specifice. O gestiune corespunzătoare a documentelor în format electronic face necesară implementarea unor măsuri specifice. Măsurile ar trebui să asigure protecția informațiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Cel mai sensibil aspect este acela de a asigura securitatea informației gestionată de sistemele informatice în noul context tehnologic.

Securitatea informației este un concept mai larg care se referă la asigurarea integrității, confidențialității și disponibilității informației. Dinamica tehnologiei informației induce noi riscuri pentru care organizațiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea memoriilor portabile de capacitate mare, induce riscuri de copiere neautorizată sau furt de date. Lucrul în rețea și conectarea la Internet induc și ele riscuri suplimentare, de acces neautorizat la date sau chiar fraudă.

Dezvoltarea tehnologică a fost acompaniată și de soluții de securitate, producătorii de echipamente și aplicații incluzând metode tehnice de protecție din ce în ce mai performante. Totuși, în timp ce în domeniul tehnologiilor informaționale schimbarea este exponențială, componenta umană rămâne neschimbată. Asigurarea securității informațiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană. Majoritatea incidentelor de securitate sunt generate de o gestiune și organizare necorespunzătoare, și mai puțin din cauza unei deficiențe a mecanismelor de securitate.

Este important ca organizațiile să conștientizeze riscurile asociate cu utilizarea tehnologiei și gestionarea informațiilor și să abordeze pozitiv acest subiect printr-o conștientizare în rândul angajaților a importanței securității informațiilor, înțelegerea tipologiei amenințărilor, riscurilor și vulnerabilităților specifice mediilor informatizate și aplicarea practicilor de control.

Scopul proiectului constă în studiul și aplicarea diferitor tehnici și tehnologii de asigurare a schimbului de date securizat în rețelele de comunicații ce va contribui la buna funcționare a obiectelor supuse riscurilor și la elaborarea politicilor și managementului de securitate.

Utilizarea eficientă a tehnicilor și tehnologiilor de asigurare a informației în rețelele de comunicații este determinată de următoarele obiective:

1. Familiarizarea cu tehnica și utilizarea unei aplicații de ascundere a informației în rețelele de comunicații prin steganografie;
2. Analiza funcționării, rolului și configurării unui firewall în securitatea rețelelor de comunicații;
3. Analiza funcționalității rețelelor virtuale private, tunelelor între două sisteme pe Internet și configurarea Open VPN.

BIBLIOGRAFIE

1. GLICK, M., LING, LIAO, SCHMIDTKE, K. Integrated Photonics for Data Communication Applications. Academic Press/Elsevier, 2023.
2. AGRAWAL, G. Fiber-Optic Communication Systems. John Wiley & Sons. 2021.
3. KEISER, GERSD. Fiber Optic Communications. Academic Press, 2021.
4. TOGAN, M. Infrastructuri de Securitate pentru servicii electronice în Internet. București: Matrix Rom, 2017.
5. CATRINA, O. Cryptographic algorithm and protocols. București: Matrix Rom, 2016.
6. MOISE, G. Networking și Securitate. Ploiești: Editura Universitatea Petrol-Gaze din Ploiești, 2015.
7. STANCIU, V. Securitatea informației: principii și bune practice. București: Editura ASE, 2015.
8. ВАСИЛЬКОВ, А., В. Информационные системы и их безопасность. Москва: Форум, 2014.
9. БАРАНОВА, Е., К. Информационная безопасность и защита информации. Москва: ИНФРА-М, 2014.
10. ШАНЬГИН, В., Ф. Информационная безопасность компьютерных систем и сетей. Москва: ИНФРА-М, 2014ю
11. ЗАТУРАНОВ, М., Н. Построение информационных систем на основе принципа виртуализации. Москва: Техносфера, 2014.
12. CONSTANTINESCU, Z. Criptarea informației: Ghid practic. Ploiești: Editura Universitatea Petrol-Gaze din Ploiești, 2013.
13. ȘERB, A., BARON, C. Securitatea informatică în societatea informațională. București: Pro Universitatea, 2013.
14. CITTADINI, L. MPLS Virtual Private Networks. Cisco Press, 2013.
15. РАССЕЛ, ДЖ. Волоконно-оптические системы. Москва: VSD, 2013.
16. ЗАПЕЧНИКОВ, С., В. Основы построения виртуальных частных сетей. Москва: Радио и связь, 2012.
17. OLARU, E. Securitatea și sănătatea în muncă. Chișinău: UTM, 2012.
18. FLONTA, S. Metode criptografice pentru sisteme structurate. Cluj-Napoca: U.T.Press, 2011.
19. GANGAN, S. Justificarea economică a lucrării de diploma. Exemple numerice de studii manageriale. Îndrumar metodic. Partea 2. Chișinău: UTM, 2006.