МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА КОМП’ЮТЕРНИХ НАУК

ОСТРОЖИНСЬКИЙ СЕРГІЙ ВІКТОРОВИЧ

УДК 004.73; 004.77

ДОСЛІДЖЕННЯ РОБОТИ ІНФОРМАЦІЙНО-ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ СТРУКТУРНИХ ПІДРОЗДІЛІВ ТЕРНОПІЛЬСЬКОЇ ОБЛАСТІ

8.05010101 «Інформаційні управляючі системи та технології»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2017

Роботу виконано на кафедрі комп'ютерних наук Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат фізико-математичних наук, доцент кафедри фізики
Скоренький Юрій Любомирович,
Тернопільський національний технічний університет імені Івана Пулюя

Рецензент: кандидат технічних наук, доцент кафедри інформатики та математичного моделювання
Гащин Надія Богданівна,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 23 лютого 2017 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії №31 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 46, навчальний корпус №1, ауд.701.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Безпеку інформаційної взаємодії локальних мереж окремих комп'ютерів через відкриті мережі, наприклад, через глобальну мережу Internet, вимагає якісного рішення двох базових задач:

– захисту підключених до публічних каналів зв'язку локальних мереж і окремих комп'ютерів від несанкціонованих дій з боку зовнішнього середовища;

– захисту інформації в процесі передачі по відкритих каналах зв'язку.

Рішення першої задачі засноване на використанні міжмережевих екранів (МЕ), що підтримують безпеку інформаційної взаємодії шляхом фільтрації двостороннього потоку повідомлень, а також виконання функцій посередництва при обміні інформацією. Для захисту локальних мереж МЕ розташовують на стику між локальною і відкритою мережею. Для захисту окремого віддаленого комп'ютера, підключеного до відкритої мережі, програмне забезпечення МЕ встановлюється на цьому ж комп'ютері, а сам МЕ в цьому випадку називають персональним.

Захист інформації в процесі передачі по відкритих каналах зв'язку заснований на виконанні наступних функцій:

– аутентифікації (встановлення достовірності) взаємодіючих сторін;

– шифруванні передаваних даних;

– підтвердженні достовірності і цілісності доставленої інформації;

– захисту від повтору, затримки і видалення повідомлень;

– захисту від заперечення фактів відправлення і прийому повідомлень.

Перераховані функції багато в чому пов'язані один з одним, і їх реалізація заснована па криптографічному захисті передаваних даних. Висока ефективність такого захисту забезпечується за рахунок спільного використання симетричних і асиметричних криптографічних систем.

Мета роботи: розробка інформаційно-обчислювальної мережі структурних підрозділів Тернопільської області, що включає в себе.

Об’єкт, методи та джерела дослідження. Канали передачі даних.

Практичне значення отриманих результатів.

Проаналізовано дискретні канали передачі інформації без перешкод і з перешкодами, проаналізовано можливість використання протоколу IPSec при розробці мережі, сформовано послідовність інсталяції мережі з використанням тунелів VPN, проведено експериментальну перевірку ефективності її використання.

Апробація. Окремі результати роботи доповідались на IX Всеукраїнській студентській науково-технічній конференції «Природничі та гуманітарні науки. Актуальні питання» (20-21 квітня 2016 р., м. Тернопіль).

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 6 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 127 арк. формату А4, графічна частина – 8 аркушів формату А1

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі розглянуто актуальність захищених каналів зв’язку для об’єднання різних підрозділів в одне ціле.

В першому розділі розглянуто основи функціонування VPN, а саме, звернуто увагу на тунелювання, протоколи, цифрові сертифікати.

В другому розділі розглянуто описано процес інсталяції мережі, наведено комутаційне обладнання, описано процедуру підключення з використанням ОС Windows 7.

В частині “Спеціальна частина” розглянуто перелік можливих атак на вузли мережі.

В частині “Обґрунтування економічної ефективності” проведено економічні розрахунки, спрямовані на визначення економічної ефективності від дослідження роботи інформаційно-обчислювальної мережі, а також прийнято рішення щодо подальшого розвитку. Розраховано значення економічної ефективності становить 0,56, що є високим значенням. Так само нормальним є термін окупності. Для даного дослідження він становить 1.78 року.

В частині “Охорона праці та безпека в надзвичайних ситуаціях” розглянуто електробезпеку; першу допомогу при ураженні електричним струмом; фактори, що впливають на функціональний стан користувачів комп'ютерів.

В частині “Екологія” розглянуто статистичні показники екологічних явищ; статистичне оцінювання екологічного стану навколишнього природного середовища та закономірностей його розподілу.

У загальних висновках щодо дипломної роботи описано прийняті в роботі технічні рішення.

ВИСНОВКИ

Віртуальні приватні мережі, або захищені віртуальні мережі (Virtual Private Network, VPN), – це підключення, встановлене по існуючій загальнодоступній інфраструктурі і використовує шифрування і аутентифікацію для забезпечення безпеки змісту передаваних пакетів.

Віртуальна приватна мережа створює віртуальний сегмент між будь-якими двома точками доступу до мережі. Вона може проходити через загальнодоступну інфраструктуру локальної обчислювальної мережі, підключення до глобальної мережі (Wide area Network, WAN) або Інтернет.

Підключення по протоколу IPSec має два основні режими: транспортний (transport) і тунельний (tunnel).

Транспортний режим – це форма зв'язку типу вузол-вузол, де застосовується шифрування тільки змістовної частини пакету. Через двоточковий характер зв'язку відповідне програмне забезпечення необхідно завантажити (встановити) на всі вузли мережі, які зв’язуються між собою, що є досить серйозною проблемою. Цей режим VPN зручно використовувати для зашифрованого зв'язку між вузлами однієї мережі.

Режим тунелювання застосовується при створенні більшості VPN, тому що він шифрує увесь оригінальний пакет. Режим тунелювання може застосовуватися для організації зв'язку типу вузол-вузол, вузол-шлюз або шлюз-шлюз. При

організації зв'язку типу шлюз-шлюз значно спрощується зв'язок між мережами, не вимагається встановлення спеціального ПЗ на вузлах мережі.

На останньому етапі було описано процес інсталяції мережі, наведено комутаційне обладнання, описано процедуру підключення з використанням ОС Windows 7, сформовано перелік можливих атак на вузли мережі.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. С. Острожинський. Про поняття «соціальні мережі» / Острожинський С. – Тези доповіді на IX Всеукраїнській студентській науково-технічній конференції «Природничі та гуманітарні науки. Актуальні питання». Том I, Тернопіль, 20-21 квітня 2016 року. – Тернопіль, ТНТУ, 2016. – с. 92-93.

АНОТАЦІЯ

Дипломна робота присвячена питанням побудови захищеного каналу зв’язку між структурними підрозділами.

Захист інформації в процесі передачі по відкритих каналах зв'язку заснований на виконанні наступних функцій:

- аутентифікації (встановлення достовірності) взаємодіючих сторін;
- шифруванні передаваних даних;
- підтвердженні достовірності і цілісності доставленої інформації;
- захисту від повтору, затримки і видалення повідомлень;
- захисту від заперечення фактів відправлення і прийому повідомлень.

Перераховані функції багато в чому пов'язані один з одним, і їх реалізація заснована па криптографічному захисті передаваних даних. Висока ефективність такого захисту забезпечується за рахунок спільного використання симетричних і асиметричних криптографічних систем.

Об’єкт аналізу – канали передачі даних.

Мета роботи – розробка інформаційно-обчислювальної мережі структурних підрозділів Тернопільської області.

Основні результати — проаналізовано дискретні канали передачі інформації без перешкод і з перешкодами, проаналізовано можливість використання протоколу IPSec при розробці мережі, сформовано послідовність інсталяції мережі з використанням тунелів VPN, проведено експериментальну перевірку ефективності її використання.

Ключові слова: ІНФОРМАЦІЯ, КАНАЛ, ДИСКРЕТНИЙ, ПРОТОКОЛ, ТУНЕЛЮВАННЯ, ТЕОРЕМА, ЗВ’ЯЗОК, ЗАХИЩЕНИЙ, СЕРТИФІКАТ, ІНСТАЛЯЦІЯ, АТАКА.

ANNOTATION

A priv in the process of transmission on open communication channels is based on implementation of next functions :

- authentifications (establishment of authenticity) of interactive parties;
- enciphering of transferrable data;

- validifying and integrity of the delivered information;
- to protecting from repetition, delay and moving away of reports;
- to protecting from the denial of facts of sending and pick up messages.

The transferred functions are in a great deal related to each other, and their realization is founded to the step cryptographic protection of transferrable data. High efficiency of such defence is provided due to the general use of the symmetric and asymmetric cryptographic systems.

An object of analysis is channels of data.

A purpose of work is development of information-calculating network of structural subdivisions of the Ternopil area.

Basic results - the discrete channels of information transfer are analysed without obstacles and with obstacles, possibility of the use of protocol of IPSec is analysed at development of network, the sequence of installation of network is formed with the use of tunnels of VPN, experimental verification of efficiency of her use is conducted.

Keywords: INFORMATION CHANNEL, DISCRETE, PROTOCOL, TUNNELING, THEOREMS, US-PROTECTED CERTIFICATES, INSTALLATIONS, ATTACK.