

Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра управління проектами, інформаційних технологій та телекомунікацій

«Допущено до захисту»
Завідувач кафедри
д.т.н., професор
_____ С. В. Мартин
“ ___ ” _____ 20__ року

ДИПЛОМНА РОБОТА МАГІСТРА

на тему: «Удосконалення системи захисту комп'ютерних
інформаційних мереж»

Виконав:
слухач VI курсу, КН-61м
спеціальності 122 «Комп'ютерні науки
та інформаційні технології»

(комп'ютерні науки та
інформаційні технології)

(шифр і назва спеціальності)
Пушкар В.Я.

(прізвище та ініціали)

Керівник Борзов Ю.О.

(прізвище та ініціали)

Рецензент Рак Т.Є.

(прізвище та ініціали)

Львів – 2017 року

Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

Кафедра управління проектами, інформаційних технологій та телекомунікацій

Освітньо-кваліфікаційний рівень магістр

Спеціальність 122 «Комп'ютерні науки та інформаційні технології» (комп'ютерні науки та інформаційні технології)

ЗАТВЕРДЖУЮ

Завідувач кафедри УПІТтаТ

д.т.н., професор

_____ Є. В. Мартин

“ ___ ” _____ 20__ року

ЗАВДАННЯ

на дипломну роботу

Студенту _____ Пушкарю Володимирі Ярославовичу

(прізвище, ім'я, по батькові)

1. Тема: Удосконалення системи захисту комп'ютерних інформаційних мережева
керівник роботи _____ Борзов Юрій Олексійович, к.т.н.

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ЛДУ БЖД від “_26_” _вересня_ 2017_ року №_112од_

2. Термін подання слухачем роботи _____ 01 грудня 2017 року

3. Початкові дані до роботи

1. Концепція технічного захисту інформації в Україні. Постанова Кабінету Міністрів України № 1126 від 8 жовтня 1997 р.

2. Кульгін М. Технології корпоративних мереж. Енциклопедія. — СПб.: Питер, 2000. — 704 с.

3. Олифер В. Г., Олифер Н. А. Комп'ютерні мережі. Принципи, технології, протоколи: Учебник для вузів. — СПб.: Питер, 2001. — 672 с.

4. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін - К.: "МК-Прес", 2005. - 432 с., іл..

4. Зміст дипломної роботи/проекту (перелік питань, які потрібно розробити)

Вступ

Розділ 1. Характеристика об'єкта проектування

Розділ 2. Огляд літературних джерел

Розділ 3. Системний аналіз об'єкту проектування

Розділ 4. Програмне рішення

Розділ 5. Охорона праці

Висновки

Список використаних джерел

Додатки

5. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 26.09.2017**КАЛЕНДАРНИЙ ПЛАН**

№ з/п	Назва етапів виконання дипломної роботи/проекту	Термін виконання етапів роботи	Примітка
1	Характеристика об'єкта проектування		
2	Огляд літературних джерел		
3	Системний аналіз об'єкту проектування		
4	Програмне рішення		
5	Охорона праці		

Студент

(підпис)

Пушкар В.Я.

(прізвище та ініціали)

Керівник роботи

(підпис)

Борзов Ю.О.

(прізвище та ініціали)

АНОТАЦІЯ

Пушкар В.Я. «Удосконалення системи захисту комп'ютерних інформаційних мереж». Дипломна робота за спеціальністю 122 «Комп'ютерні науки та інформаційні технології» складається з основної частини, що містить 5 розділів, обсягом 70 сторінок і містить 18 ілюстрацій, 1 таблицю та 22 джерел використаної літератури.

Метою роботи є розробка програмного рішення класу мережевий екран, який призначений для організації захищених комунікацій у комп'ютерних інформаційних системах.

Об'єктом дослідження є комунікаційні процеси у комп'ютерних мережах.

Основні завдання дипломного проекту є такі:

- Аналіз роботи комунікаційних протоколів
- Аналіз роботи мережевих підсистем платформи Windows.
- Аналіз роботи підсистем WinSocket та Berkeley Sockets.
- Вивчення технологій
- Проектування мережевого екрану.
- Розробка структур даних для забезпечення роботи мережевого екрану.
- Розробка потоку управління комунікаційними потоками
- Розробка завершеного програмного рішення

Одним з традиційних способів несанкціонованого доступу є перепопнення мережевих пакетів для подальшої обробки та аналізу. Тому важливо і нагальним завданням є створення простих програмних систем, які автоматично забезпечать безпечний сеанс зв'язку.

Ключові слова: інформаційні технології, інформаційна безпека, автоматизована система, комунікаційний протокол, мережевий екран, віртуальна приватна мережа.

SUMMARY

V. Pushkar “Improvement of the system of protection of computer information networks”. Thesis specialty 122 “Computer Science and Information Technology“ consists of main body containing 5 chapters of 70 pages, 18 illustrations, 1 table and 22 sources of information.

The aim of the diploma project is to develop a software solution class firewall that is designed for organizations secure communications in computer information systems.

Therefore, the main object of the diploma project is communication processes in komp'yutenyh networks.

The main objectives of the diploma project are:

- Analysis of communication protocols
- Analysis of network subsystems platform Windows.
- Analysis of the subsystems WinSocket and Berkeley Sockets.
- Learning Technologies
- Designing firewall.
- Development of data structures to support the work firewall.
- Design flow management communication flows
- Develop a complete prohramanoho decision.

One of the traditional methods of unauthorized access is merehoplennya network packets for further processing and analysis. Therefore it is important and urgent task is to build a simple software systems that would automatically would provide secure communication session.

Key words: IT (information technology), information security, automated systems, communication protocol, network screen, VPN (Virtual Private Network).

Зміст

Вступ.....	8
Постановка задачі.....	10
1. Характеристика об'єкта проектування.....	11
1.1. Проблема забезпечення безпеки інформаційних мереж.....	11
1.2. ТЗІ в комунікаційних системах на мережевому рівні.....	13
2. Огляд літературних джерел.....	15
2.1. Захист інформації.....	15
2.2. Загрози інформації.....	15
2.3. Аналіз загроз безпеки інформації в автоматизованих системах.....	18
2.4. Віртуальні приватні мережі як засіб безпеки в комунікаційних сеансах.....	23
2.4.1. Класифікація VPN.....	24
2.4.2. Класифікація VPN за типом використовуваного середовища.....	27
2.4.2. Алгоритми хешування і шифрування. Переваги та недоліки VPN.....	31
2.5. Криптографічні методи захисту інформації.....	32
2.5.1 Криптографія. Основні поняття і визначення.....	32
2.5.2. Вимоги до криптографічних систем.....	35
2.5.3. Принципи побудови й схеми криптологічних систем.....	36
2.5.4. Класифікація алгоритмів шифрування.....	38
3. Системний аналіз.....	43
3.1. Дерево цілей.....	43
3.2. Дерево проблем.....	45
4. Програмне рішення.....	48

4.1. Схема функціонування програмного рішення	48
4.2. Архітектура програмного рішення	50
4.3. Опис прикраних функціональностей програми	53
5. Охорона праці	61
5.1. Загальні положення	61
5.2. Санітарно-гігієнічні вимоги	61
5.3. Вимоги до організації робочого місця.....	62
5.4. Освітленість	63
5.5. Мікроклімат.....	64
5.6. Рекомендації щодо поліпшення умов праці	65
5.7. Вимоги безпеки при аварійних ситуаціях	65
Висновки	8
Література.....	10
Додатки.....	71
Додаток А – файл проекту.....	71
Додаток В – код основного модуля	72
Додаток В – код ініціалізації мережевої підсистеми.....	74

Висновки

За результатами дипломного проектування можна зробити такі висновки. Отримане програмне рішення дає можливість забезпечити захищені комунікаційні сеанси з достатньо високим ступенем захисту в повністю автоматичному режимі. Фактично від користувача потребується виконання лише однієї дії, а саме встановлення режиму функціонування. Така реалізація дає можливість використання програмного продукту у організаціях з дуже обмеженим бюджетом. Тепер зникають потреби на розгортання важких систем тунелювання, які тягнуть за собою витрати на підтримку та адміністрування.

Розгортання розробленої системи є повністю автоматичним і також не потребує яких небудь особливих знань в області інформаційних технологій.

Ще однією перевагою розробленого програмного рішення є можливості динамічного розширення методів шифрування. Для підмикання в програму нових методів необхідно лише в каталог програми розмістити нову версію бібліотеки `encrypt.dll`. Структура бібліотеки є достатньо простою і складається із двох функцій методу ініціалізації та методу шифрування. Дотримання цих правил дозволить привнести в програму нові методи шифрування без перероблення усієї програми.

Подальший розвиток програмного продукту має два шляхи. За першим шляхом це портація програмного продукту на платформу Windows. Це не дуже розширить ринок використання, оскільки більшість малих і середніх підприємств на сьогодні розгортають свої системи на платформі WinTEL. Проте у майбутньому це дасть можливість використання програми в кросплатформених мережевих системах.

За другим напрямом розвиток полягає в захопленнях для захисту Web-портів. В комунікаційних сеансах інтернету відсутність підтримки цих протоколів не є проблемою, оскільки існує захищений протокол `https`, який працює подібно до нашої програми. Підтримка Web-протоколів може дати перевагу у випадку

використання користувацьких тунелів на базі протоколу http. Оскільки на практиці такі технології використовуються рідко (перевага віддається стандартизованим тунелям), то протокол http не розглядався як протокол, який потребує захисту

Література

1. Концепція технічного захисту інформації в Україні. Постанова Кабінету Міністрів України № 1126 від 8 жовтня 1997 р.
2. Богущ В. М. Інформаційна безпека держави / В. М. Богущ, О. К. Юдін - К.: "МК- Прес", 2005. - 432 с., іл.
3. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
4. Положення про технічний захист інформації в Україні. Указ Президента України № 1229 від 27 вересня 1999 р.
5. НД ТЗІ 3.6-001- 200. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
7. Методы и средства защиты информации. В 2-х томах / Ленков С. В., Перегудов Д. А., Хорошко В. А., Под ред. В. А. Хорошко. - К.: Арин, 2008. - 464 с.
8. Бабак В. П. Теоретичні основи захисту інформації: Підруч. / В. П. Бабак - К. : Книжкове вид-во НАУ, 2008. - 752 с.
9. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
10. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
11. <http://uk.wikipedia.org/wiki>
12. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР — zakon.rada.gov.ua
13. A Framework for IP Based Virtual Private Networks [Электронный документ] / В. Gleeson, А. Lin, J. Heinanen. — <http://www.ietf.org/rfc/rfc2764.txt>

14. VPN и IPSec на пальцах [Электронный документ] / Dru Lavigne. — <http://www.nestor.minsk.by/sr/2005/03/050315.html>
15. Алексей Лукацкий Неизвестная VPN // Компьютер Пресс.- 2001.- № 10
<http://abn.ru/inf/compress/network4.shtml>
16. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. — М.: КУДИЦ-ОБРАЗ, 2001. — 368 с.
17. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000. — 704 с.
18. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. — СПб.: Питер, 2001. — 672 с.
19. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. — М: Радио и связь, 2002. — 328 с.
20. Правила охорони праці під час експлуатації електронно-обчислювальних машин : НПАОП 0.00.-1.31-10. — [Чинний від 2010-03-26]. — К. : Держнагляд охорон праці України, 2010. — 7 с. — (Національні стандарти України).
21. Природне і штучне освітлення : ДБН В.2.5-28:2015 — [Чинний від 2015-01-01]. — К. : Міністерство будівництва, архітектури та житлово-комунального господарства України, 2015. — 171 с. — (Національні стандарти України).
22. Санітарні норми мікроклімату виробничих приміщень : ДСН 3.3.6.042-99. — [Чинний від 2000-01-01]. — К. : МОЗ України, 2000. — 42 с. — (Національні стандарти України).