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

ДЯЧИШИН АНДРІЙ РОМАНОВИЧ

УДК 004.04

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ТА ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ В ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

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 технічних наук, доцент кафедри комп'ютерних наук
Гладьо Юрій Богданович,
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: кандидат технічних наук, доцент кафедри кібербезпеки
Загородна Наталя Володимирівна,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 20 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 56, навчальний корпус №1, ауд. 701

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Пропорційно розвитку комп'ютерних технологій також зростає й рівень злочинності в комп'ютерному середовищі. У зв’язку з цим, використання локальних мереж для передачі та зберігання інформації, вимагає побудови ефективної системи захисту.

Тому створення системи захисту інформації, у даний час, стає невід’ємною частиною політики безпеки будь-якої організації. Для правильного функціонування системи захисту необхідні знання можливих дій порушника, а отже, можливих загроз КС.

Мета роботи: підвищення рівня безпеки мережевої взаємодії шляхом створення комплексної системи захисту на основі протоколів різних рівнів моделі OSI.

Об’єкт, методи та джерела дослідження. Вбудовані протоколи захисту ОС Windows.

Наукова новизна отриманих результатів:

- розглянути модель порушника та основні класи загроз безпеки в КС;
- провести аналіз протоколів захисту інформації в автоматизованих системах різних рівнів моделі OSI;
- практично виконати налаштування протоколів захисту інформації.
- виконано техніко-економічне обґрунтування прийнятих рішень;
- охорони праці, безпеки в надзвичайних ситуаціях те екології.

Практичне значення отриманих результатів. Все більше актуальною стає побудова комплексної системи захисту, що використовує всі можливі методи та способи захисту, в тому числі й ті, що входять до складу операційних систем. Вбудовані засоби дозволяють зменшити витрати на побудову системи захисту. Мова йде про так звані специфічні протоколи захисту, тобто протоколи та алгоритми, які забезпечують конфіденційність та цілісність інформації, яка передається.

Таким чином, аналіз таких протоколів є передумовою обґрунтованого відбору протоколів для побудови на їх основі комплексної системи захисту, що є актуальною задачею в загальній проблемі забезпечення інформаційної безпеки сучасних об’єктів інформаційної діяльності.

Апробація. Окремі результати роботи доповідались на V міжнародній науково-технічна конференція молодих вчених та студентів 17-18 листопада 2016 року.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 7 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 128 арк. формату А4, графічна частина – 8 аркушів формату А1

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі проведено огляд сучасного стану комп'ютерних і телекомунікаційних технологій та охарактеризовано основні завдання, які необхідно вирішити.

В частині аналітичний огляд літературних та інших джерел описано, що з найважливіших проблем забезпечення безпеки комп'ютерних систем є визначення, аналіз і класифікація можливих загроз безпеки КС. Перелік загроз, оцінка вірогідності їх реалізації, а також модель порушника виступають основою побудови комплексної системи захисту КМ.

У розділі зроблено аналіз, сучасних комп'ютерних систем обробки інформації, який показав, що в загальному випадку КС є територіально розподіленими багатокористувацькими системами, складові яких інтенсивно взаємодіють між собою, використовуючи інтеграцію даних різного призначення та широкий спектр способів уявлення, зберігання й передачі інформації.

В частині аналіз протоколів захисту інформації проведено теоретичний аналіз вбудованих засобів захисту операційних систем. Виходячи зі специфіки мережевої взаємодії, на кожному рівні моделі взаємодії відкритих систем, можна застосовувати відповідні протоколи.

Показано, що на канальному рівні використовуються протоколи тунелювання (PPTP, L2TP), які дозволяють виконати тунелювання PPP-з'єднань по IP-мережах та забезпечити захист інформації, яка передається, від загроз конфіденційності та цілісності, шляхом створення VPN. Розглянуті схеми включення: провайдер-маршрутизатор та клієнт-маршрутизатор. Формування захищеного каналу відбувається в три етапи: установлення з'єднання клієнта із сервером віддаленого доступу, аутентифікація користувача, конфігурування захищеного тунелю. Особливістю функціонування L2TP є те, що він потребує спеціалізованого ключа отриманого із центру сертифікації.

В частині практичне налаштування протоколів захисту інформаціїї було практично налаштовано та продемонстровано правильність роботи таких протоколів захисту: IPSec, SSL, PPTP та L2TP. Усі ці протоколи забезпечуються надійний захист від загроз конфіденційності та цілісності.

Для практичного розгляду використовується спеціальне програмне забезпечення VMware Workstation, на якому встановлені операційні системи Windows Server та Windows XP та налаштована мережева взаємодія між ними. Для аналізу мережевої взаємодії застосовується програмний продукт Wireshark.

Для налаштування протоколу IPsec на всі види ключової інформації на сервері (Windows Server) встановлено сервер доменних імен (DNS), WEB-сервер, контролер доменних імен, Active Directory та центр сертифікації. Основою правильної роботи IPSec є Security Association, яка налаштовується на клієнтські та серверній машині та визначає алгоритми аутентифікації та шифрування. Налаштування даної асоціації включає в себе такі етапи: створення політики IP-фільтрації, створення політики IP-безпеки, конфігурування політики IP-безпеки. Аналіз мережевої взаємодії показав, що IP пакети інкапсулюються в захищені пакети ESP, зміст яких розібрати неможливо.

В спеціальній частині з розглянутої проблеми виділені та розглянуті сучасні найбільш поширені методи криптографічного захисту інформації від несанкціонованого доступу.

В новітніх інформаційних системах для шифрування повідомлень, які передаються, використовуються симетричні алгоритми шифрування, зважаючи на велику обчислювальну здатність асиметричних алгоритмів, їх застосовують для генерації та поширення сеансових ключів. Усунути основні недоліки, властиві як симетричним, так і асиметричним методам криптографічного захисту інформації, дозволяє їх комбіноване використання.

В частині «Обґрунтування економічної ефективності» розглянуто питання організації виробництва і проведено розрахунки техніко-економічної ефективності проектних рішень.

В частині «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто вимоги до розміщення елементів на робочому місці, принципи та заходи захисту в умовах надзвичайної ситуації, завдання першої допомоги, надання першої допомоги при обмороженнях.

В частині «Екологія» проаналізовано роль матеріало- та ресурсозбереження у вирішенні екологічних проблем та основні методи екологічної статистики.

Розглянуто що таке екологічна статистика, що являє собою статистика стану і забруднення атмосферного повітря. Визначено основне завдання статистики стану і забруднення атмосферного повітря.

Проаналізовано статистику стану, використання й охорони водних ресурсів, статистику землекористування і земельних угідь, статистику охорони і захисту лісу, статистику знешкодження відходів.

У загальних висновках щодо дипломної роботи наведено отримані технічні рішення і запропоновано організаційно-технічні заходи, які забезпечують виконання поставленого завдання.

ВИСНОВКИ

У результаті виконання роботи розглянуто основні проблеми захисту КС та проведено теоретичний та практичний аналіз вбудованих засобів захисту інформації.

Зроблено аналіз, сучасних автоматизованих систем обробки інформації. Який показав, що уразливими є буквально всі основні структурно-функціональні елементи розподілених КС: робочі станції, сервери (Host-машини), міжмережеві мости (шлюзи, центри комутації), канали зв'язку.

Виходячи з основних нормативних документів із захисту інформації розглянуто чотири основних класи загроз: порушення конфіденційності, цілісності, доступності, спостережності. Інформаційна безпека КС забезпечена у випадку, якщо для будь-яких інформаційних ресурсів в системі підтримується певний рівень конфіденційності, цілісності, доступності та спостережності.

Розглянуто модель загроз, згідно з якою всі потенційні загрози за природою їх виникнення розділяється на два класи: природні (об'єктивні) і штучні (суб'єктивні). А джерела загроз по відношенню до КС можуть бути зовнішніми або внутрішніми.

Виходячи з можливих загроз та суб'єктів їх вчинення, розглянута модель порушника, в якій відбиваються його практичні і теоретичні можливості – важлива складова для побудови надійної системи захисту.

З розглянутого широко спектру загроз інформаційної безпеки випливає, що тільки комплексний підхід до захисту інформації може забезпечити сучасні вимоги безпеки в КС. Він має на увазі комплексний розвиток усіх методів і засобів захисту.

Елементами комплексної системи захисту КМ є засоби, механізми яких входять до складу мережевих операційних систем. Їх використання є доцільним, оскільки не потребує затрат коштів та робочої сили. Виходячи зі специфіки мережевої взаємодії, на кожному рівні моделі взаємодії відкритих систем, можна застосовувати свої відповідні протоколи.

Для безпечної мережевої взаємодії на основі вбудованих засобів захисту інформації необхідним є практичний аналіз протоколів захисту інформації, що включає налаштування серверів, клієнтів, служб, протоколів та з'єднань.

В роботі практично налаштовано та продемонстровано правильність функціонування таких протоколів захисту: IPSec, SSL, PPTP та L2TP. Всі ці протоколи забезпечуються надійний захист від загроз конфіденційності та цілісності.

Результатами роботи є розглянуті особливості сучасних загроз і уразливість інформації в КМ та забезпечення безпеки. Проведений аналіз протоколів захисту інформації різних рівнів моделі OSI. Практично налаштовані протоколи захисту інформації в КС.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Дячишин А.Р. Особливості сучасних КС як об'єкту захисту [Текст] / Дячишин А.Р., Шимчук Г.В. Тези доповіді на V міжнародна науково-технічна конференція молодих вчених та студентів – Тернопіль, ТНТУ, 2016. – с. 39.

2. Дячишин А.Р. Уразливість основних структурних елементів розподілених КС [Текст] / Дячишин А.Р., Шимчук Г.В. Тези доповіді на V міжнародна науково-технічна конференція молодих вчених та студентів – Тернопіль, ТНТУ, 2016. – с. 40-41.

АНОТАЦІЯ

У дипломній роботі проведено дослідження методів захисту в локальних комп'ютерних мережах для забезпечення безпеки інформації.

Розглянуто особливості сучасних КС як об'єкту захисту, уразливість основних структурних елементів розподілених КС, загрози безпеки інформації в КС, основні класи загроз безпеки, загрози конфіденційності, цілісності, доступності та спостережності в КМ, неформальну модель порушника, сучасні методи й засоби забезпечення безпеки в КМ, програмно-апаратні засоби захисту комп'ютерної інформації.

Проаналізовано протоколи захисту в КС, розглянуто еталонну модель OSI та протоколи захисту інформації на кожному з рівнів, розглянуто захист інформації на

канальному, мережевому, транспортному та прикладному рівнях моделі взаємодії відкритих систем.

Практично налаштовано протоколи захисту інформації, а саме: IPSec, SSL, PPTP, L2TP.

Ключові слова: ЕОМ, АС, ЛОМ, СЕРВЕР, ПРОТОКОЛ, TCP, PPTP, DNS, IP ЗАХИСТ, МЕТОД, МЕРЕЖА, БЕЗПЕКА, ЗАГРОЗА, МОДЕЛЬ, АЛГОРИТМ, OSI

ANNOTATION

In the thesis work studied the methods of protection of local computer networks for security information.

The features modern COP as an object of protection, vulnerability main structural elements distributed COP, information security threats to the Constitutional Court, the main classes of threats to security threats to confidentiality, integrity, availability and observability in KM, informal model of the offender, modern methods and means of ensuring security KM, software and hardware information protection.

The analysis protocols to protect the COP considered OSI reference model and protocols of information security at each of the levels considered data protection for data link, network, transport and application level model of open systems.

Almost configured information security protocols, such as: IPSec, SSL, PPTP, L2TP.

Key words: COMPUTERS, AS, LAN, SERVER, PROTOCOL, TCP, PPTP, DNS, IP, PROTECTION, METHOD, NETWORK, SECURITY, THREAT, MODEL, ALGORITHM, OSI