

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

СЕНИК ВАЛЕНТИН ВІКТОРОВИЧ

УДК 004.73

**РОЗРОБЛЕННЯ МЕТОДИКИ СИСТЕМИ ЗАХИСТУ КОМП'ЮТЕРНОЇ
МЕРЕЖІ З ВИКОРИСТАННЯМ СЕРВЕРІВ STANFORD UNIVERSITY
NETWORK**

122 «Комп'ютерні науки»

Автореферат

дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2019

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

Керівник роботи: кандидат технічних наук, професор кафедри комп'ютерних наук
Харченко Олександр Григорович,
Тернопільський національний технічний університет імені Івана Пулюя

Рецензент: кандидат педагогічних технічних наук, доцент кафедри кібербезпеки
Кареліна Олена Володимирівна,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 27 грудня 2019 р. о 9-00 годині на засіданні екзаменаційної комісії №33 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська 56, навчальний корпус №1, ауд. 702.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Останнім часом повідомлення про атаки на інформацію, про хакерів і комп'ютерні взломи наповнили всі засоби масової інформації. Що ж таке "атака на інформацію"? Дати визначення цій дії насправді дуже складно, оскільки інформація, особливо в електронному вигляді, представлена сотнями різних видів. Інформацією можна вважати і окремих файл, і базу даних, і один запис в ній, і повний програмний комплекс. І всі ці об'єкти можуть піддатися і піддаються атакам з боку деякої соціальної групи осіб.

Актуальністю роботи є застосування систем захисту конфіденційної інформації в діючих комп'ютерних системах.

Мета роботи: проаналізувати роботу діючої мережі підприємства та вдосконалити її захист; використати при запровадженні оптимізації сервер Sun Microsystems.

Об'єкт, методи та джерела дослідження. Діюча комп'ютерна мережа.

Практичне значення отриманих результатів.

Проведено аналіз об'єктів загроз, аналіз критеріїв оцінки інформаційної безпеки, аналіз існуючих категорій серверів; розроблено методику вибору варіанту системи захисту за критерієм живучості в умовах невизначеності впливу дестабілізуючих факторів, розроблено методику використання систем захисту конфіденційної інформації.

Апробація. Окремі результати роботи доповідались на VIII Міжнародній науково-технічній конференції молодих учених та студентів „Актуальні задачі сучасних технологій“, Тернопіль, ТНТУ, 27-28 листопада 2019. — Т. : ТНТУ, 2019. — С. 53-54. — (Том 2).

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 – 147 арк. формату А4.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі розглянуто актуальність використання систем захисту в локальних комп'ютерних мережах.

В першому розділі розглянуто основи систем захисту інформації.

В другому розділі проаналізовано сервери Sun Microsystems.

В третьому розділі описано процедуру розробки методики захисту. Для роботи встановлено сервер початкового рівня Sun Fire V40z з використання операційної системи Microsoft Windows Server 2008 R2.

В розділі “Спеціальна частина” описано спосіб пошуку Malware.

В частині “Обґрунтування економічної ефективності” проведено економічні розрахунки, спрямовані на визначення економічної ефективності від оптимізації системи захисту локальної мережі з використанням серверів Sun Microsystems, а також прийнято рішення щодо подальшого розвитку. Розраховано значення економічної ефективності становить 0,559, 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 психологію безпеки праці і ергономіку; характеристику вогнегасних речовин та підвищення стійкості роботи об'єктів господарської діяльності у воєнний час.

В частині “Екологія” проведено аналіз сучасних програмних продуктів для опрацювання великих масивів екологічної інформації та розглянуто кореляційний аналіз зв'язків в екології.

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

ВИСНОВКИ

В результаті проведених досліджень можна зробити наступні висновки.

Щодо системи захисту, то:

1. Розроблено метод вибору варіанту системи захисту для КМЗ за критерієм живучості в умовах невизначеності впливу ДФ. Для цього використано теорії підтримки прийняття рішень, що дає змогу знайти оптимальне вирішення, що найкраще відповідатиме змісту та умовам задачі у випадку трьох інформаційних ситуацій про ймовірності появи подій A_k .

2. Проаналізовано особливості і сформульовано задачі вибору варіанту системи захисту інформації в КМЗ за критерієм живучості в умовах невизначеності впливу ДФ у вигляді задачі умовної оптимізації вибору конкретного ефективного рішення (живучішої системи захисту) для кожної конкретної реалізації сценарію розвитку зовнішнього середовища.

3. Вдосконалено та досліджено математичну модель і алгоритми формування множини альтернатив для задачі вибору варіанта системи захисту інформації в КМЗ за критерієм живучості в умовах невизначеності впливу ДФ, яку доцільно на практиці використовувати як вихідну інформацію для прийняття рішень про структуру СЗІ, яка має властивість живучості в умовах ризику та невизначеності.

4. Використано систему захисту конфіденційної інформації PGP.

5. Описано застосовані засоби протидії несанкціонованому доступу.

6. На мережевому рівні застосовано два основні алгоритми захисту: SKIP і IPSec.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Сенік В.В. Методи оптимізації програми / В.В. Сенік // Матеріали VIII Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій“, 27-28 листопада 2019. — Т. : ТНТУ, 2019. — С. 53-54. — (Том 2).

АНОТАЦІЯ

Об'єкт аналізу – діюча комп'ютерна мережа.

Мета роботи – аналіз роботи діючої мережі підприємства та вдосконалення її захисту; використання при запровадженні оптимізації сервера Sun Microsystems.

Основні результати – проведено аналіз об'єктів загроз, аналіз критеріїв оцінки інформаційної безпеки, аналіз існуючих категорій серверів; розроблено методику вибору варіанту системи захисту за критерієм живучості в умовах невизначеності впливу дестабілізуючих факторів, розроблено методику використання систем захисту конфіденційної інформації.

Ключові слова: ЗАГРОЗА, ЗАХИСТ, СИСТЕМА, ОБ'ЄКТ, СЕРВЕР, АРХІТЕКТУРА, ДЕСТАБІЛІЗУЮЧИЙ ФАКТОР, МЕТОДИКА, КОНФІДЕНЦІЙНИЙ, НЕСАНКЦІОНОВАНИЙ ДОСТУП.

ANNOTATION

The object of analysis is a functioning computer network.

The purpose of the work is to analyze the operation of the existing enterprise network and improve its protection; use when implementing Sun Microsystems server optimization.

The main results are the analysis of the objects of threats, the analysis of criteria for assessment of information security, the analysis of existing categories of servers; the technique of choosing a variant of the system of protection by the criterion of survivability in the conditions of uncertainty of influence of destabilizing factors is developed, the method of using the systems of protection of confidential information is developed.

Key words: THREAT, DEFENCE, SYSTEM, OBJECT, SERVER, ARCHITECTURE, DESTABILIZING FACTOR, METHODS, CONFIDENTIAL, UNAUTHORIZED DIVISION.