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

ЛОМОНОСОВ МИХАЙЛО ВАСИЛЬОВИЧ

УДК 004.73; 004.77

ОПТИМІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ СЕРВЕРІВ SUN MICROSYSTEMS

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: доктор технічних наук, професор кафедри комп'ютерних наук
Приймак Микола Володимирович,
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. 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 окремий 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.

При зберіганні, підтримці і наданні доступу до будь-якого інформаційного об'єкту його власник, або уповноважена ним особа, накладає явно або самоочевидно набір правил по роботі із нею. Навмисне їх порушення класифікується як атака на інформацію.

Із масовим впровадженням комп'ютерів у всі сфери діяльності людини об'єм інформації, що зберігається в електронному вигляді виріс в тисячі разів. І тепер скопіювати за півхвилини і понести дискету із файлом, що містить план випуску продукції, набагато простіше, ніж зкопіювати або переписати кіпу паперів. А із появою комп'ютерних мереж навіть відсутність фізичного доступу до комп'ютера перестала бути гарантією збереження інформації.

Які можливі наслідки атак на інформацію? В першу чергу, звичайно, нас цікавитимуть економічні втрати:

1. Розкриття комерційної інформації може привести до серйозних прямих збитків на ринку
2. Звістка про крадіжку великого об'єму інформації зазвичай серйозно впливає на репутацію фірми, приводячи побічно до втрат в об'ємах торгових операцій
3. Фірми-конкуренти можуть скористатися крадіжкою інформації, якщо та залишилася непоміченою, для того, щоб повністю розорити фірму, нав'язуючи їй фіктивні або свідомо збиткові операції
4. Підміна інформації як на етапі передачі, так і на етапі зберігання у фірмі може привести до величезних збитків
5. Багатократні успішні атаки на фірму, що надає будь-який вид інформаційних послуг, знижують довіру до фірми у клієнтів, що позначається на об'ємі доходів.

Природно, комп'ютерні атаки можуть принести і величезний моральний збиток. Поняття конфіденційного спілкування давно вже стало "притчею во язицех". Само собою зрозуміло, що ніякому користувачеві комп'ютерної мережі не хочеться, щоб його листи окрім адресата отримували ще 5-10 чоловік, або, наприклад, ваш текст, що набирається на клавіатурі ЕОМ, копіювався в буфер, а потім при підключенні до Інтернету відправлявся на певний сервер. А саме так і відбувається в тисячах і десятках тисяч випадків.

Декілька цікавих цифр про атаки на інформацію. Вони були отримані дослідницьким центром DataPro Research в 1998 році. Основні причини пошкоджень електронної інформації розподілилися таким чином: ненавмисна помилка людини – 52% випадків, умисні дії людини - 10% випадків, відмова техніки – 10% випадків,

пошкодження в результаті пожежі - 15% випадків, пошкодження водою – 10% випадків. Як видно, кожен десятий випадок пошкодження електронних даних пов'язаний з комп'ютерними атаками.

Хто був виконавцем цих дій: у 81% випадків – поточний кадровий склад установ, тільки в 13% випадків – абсолютно сторонні люди, і в 6% випадків – колишніх працівників цих же установ. Частка атак, вироблюваних співробітниками фірм і підприємств, просто приголомшує і примушує пригадати не тільки про технічні, але і про психологічні методи профілактики подібних дій.

І, нарешті, що ж саме роблять зловмисники, діставшись до інформації: у 44% випадків взлому були проведені безпосередні крадіжки грошей з електронних рахунків, в 16% випадків виводилося з ладу програмне забезпечення, так же часто – в 16% випадків – проводилася крадіжка інформації з різними наслідками, в 12% випадків інформація була сфальсифікована, в 10% випадків зловмисники за допомогою комп'ютера скористалися або замовили послуги, до яких в принципі не повинні були мати доступу.

Актуальністю роботи є застосування систем захисту конфіденнційної 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 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, 8 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 168 арк. формату А4, графічна частина – 10 аркушів формату А1

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.

Загрози комп'ютерної безпеки діляться на явні і приховані. Під явними розуміємо такі погрози, які зрозумілі і однозначно передбачені. Вони не вимагають для протидії їм будь-яких додаткових відомостей про статистику погроз і неочевидних припущень про можливі атаки зловмисника.

Критерії оцінки захисту комп'ютера встановлюють базові вимоги щодо контролю комп'ютерної безпеки вбудованої в обчислювальну систему, використовуються, щоб оцінювати, класифікувати та обирати комп'ютерні системи, які використовуються для обробки, зберігання та надання доступу до класифікованої інформації.

Критерії оцінки інформаційної безпеки є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності.

З допомогою критеріїв можливо порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем.

Компанія Sun - один з основних виробників серверів, які грають провідну роль в сегменті серверів Інтернету. Ця компанія грає важливу роль в розробці деяких важливих програмних пакетів, використовуваних на веб-сайтах, таких як мова Java і переносні застосування, засновані на Java.

Операційна система Solaris встановлена на всіх комп'ютерах Sun – від настільних комп'ютерів до найбільших корпоративних серверів (еквівалент мейнфрейму компанії Sun). Операційна система Solaris 10 включає ряд інструментальних засобів управління сервером, наведених нижче. Ці інструменти

призначені не лише для управління локальною системою, фактично багато хто з них сприяє перетворенню системи Solaris на універсальну консоль управління.

Компанія Sun класифікує сервери відповідно до кількості підтримуваних клієнтів. Інші виробники серверів засновують свої оцінки виходячи з кількості процесорів в сервері. Але в реальному житті все буває набагато складніше. Так, наприклад, сервер класу 1U – це ряд блоків, щільно "упакованих" на стійці, або 16, або 20 коміркових серверів, поміщених в серверній шафі. Тому компанія Sun виробила свій підхід до класифікації серверів, що дозволяє уникнути неоднозначності.

Для роботи буде встановлено сервер початкового рівня Sun Fire V40z з використання операційної системи Microsoft Windows Server 2008 R2.

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. М. Ломоносов. Дослідження основних соціальних мереж / Ломоносов М. – 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. 79-80.

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

Lately a report is about attacks on information, about hackers and computer взломи filled all mass medias. That such the "attack on information"? To give determination to this action in actual fact very difficultly, as information, especially in an electronic kind, presented by hundreds of different kinds. It is possible to consider a separate file, and database, and one record information in her, and complete programmatic complex. And all these objects can yield and yield to the attacks from the side of some task force of persons.

At storage, support and grant to access to any information holding object his proprietor, or a person is authorized to them, lays on obviously or self-evident set of rules on work with her. Intentionally their violation is classified as an attack on information.

With mass introduction of computers in all spheres of activity of man there is a volume of information which is kept in an electronic kind grew in thousand one times. And now to copy for a half-minute and bear a diskette with a file which contains the plan of producing of products, far simpler than copy or to rewrite the stack of papers. And with appearance of computer networks even absence of physical access to the computer left off to be the guarantee of maintenance of information.

Are there what possible consequences of attacks on information? First of all, certainly, us economic losses will interest:

1. Opening of commercial information can result in serious proximate damages at the market.
2. Information about the theft of high-cube of information usually in earnest influences on reputation of firm, resulting side in losses in the volumes of trade operations.
3. Firms-competitors can take advantage of theft of information, if and remained unnoticed, in an order fully to bring to ruin a firm, imposing dummy or consciously unprofitable activities to her.
4. Substitution of information both on the stage of transmission and on the stage of storage in a firm can result in enormous losses.
5. Frequent successful attacks on a firm which gives any type of informative services reduce a trust to the firm for clients, that affects volume of profits.

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