МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 004.022

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____ к.т.н. Г.В. Шуклін
«____» _____ 2022 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: «ЗАХИСТ ВІДДАЛЕНОГО СЕРВЕРУ ВІД ПРОНИКНЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ»

студент групи СЗД-42 Савиченко Марія Сергіївна _____
(підпис)

Науковий керівник: к.т.н., доцент Пепа Юрій Володимирович _____
(підпис)

Нормоконтроль: Гребенніков Асаді Болдхоядович _____
(підпис)

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»

Завідувач кафедри СІКЗ

_____ к.т.н. Г.В. Шуклін

(підпис)

«_____»_____ 2022 р.

ЗАВДАННЯ

на атестаційну роботу

студенту: Савиченко Марії Сергіївні

1. Тема роботи: «Захист віддаленого серверу від проникнення шкідливого програмного забезпечення», затверджена наказом по університету від « » 2022 р. за № .

2. Термін здачі студентом оформленої роботи « 2 » червня 2022 р.

3. Об'єкт дослідження: система виявлення шкідливих програмних засобів у системі безпеки серверу.

4. Предмет дослідження: методи та засоби захисту на програмно-апаратному рівні серверної частини.

5. Мета роботи: розробити архітектуру серверної частини та запропонувати програмне забезпечення, яке дозволить підвищити захищеність інформації у базах даних сервера.

6. Перелік питань, які мають бути розроблені:

1. Провести аналіз сучасних програмних засобів захисту від стороннього вторгнення;

2. Розробити архітектуру серверної частини;

3. Виробити рекомендації щодо налаштувань програмного забезпечення, яке унеможливлює потрапляння шкідливого програмного коду на сервер.

7. Перелік публікацій:

8. Перелік ілюстративного матеріалу. Презентація виконана на слайдах для подання за допомогою світлопроекторів та комп'ютерних засобів.

9. Дата видачі завдання «____» _____ 2022 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «16» лютого 2022 р.

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Огляд літератури	до 29.03.22 р.	виконано
2	Написання першого розділу роботи	до 10.04.22 р.	виконано
3	Написання другого розділу роботи	до 27.04.22 р.	виконано
4	Написання третього розділу роботи	до 08.05.22 р.	виконано
5	Оформлення атестаційної роботи	до 16.05.22 р.	виконано
6	Підготовка слайдів	до 20.05.22 р.	виконано

Студент: СЗД-42 Савиченко М.С. _____
(підпис)

Науковий керівник: к.т.н., доц. Пепа Ю.В. _____
(підпис)

Нормоконтроль: Гребенніков А.Б. _____
(підпис)

РЕФЕРАТ

Текстова частина бакалаврської роботи складається з: 52 сторінки, 17 рисунків, 1 таблиці та 11 джерел.

Об'єкт дослідження – система виявлення шкідливих програмних засобів у системі безпеки серверу.

Предмет дослідження – методи та засоби захисту на програмно-апаратному рівні серверної частини.

Мета роботи – розробити архітектуру серверної частини та запропонувати програмне забезпечення, яке дозволить підвищити захищеність інформації у базах даних сервера.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації програмних засобів, робота з софтом відомих розробників захисного програмного забезпечення.

Практичне значення одержаних результатів: запропоновані рекомендації щодо налаштування програмного забезпечення можуть бути використані у сфері кіберзахисту важливої електронної інформації.

Галузь використання – кібербезпека, інформаційні технології, захист інформації.

Ключові слова: СЕРВЕР, ПРОГРАМНИЙ КОД, АТАКА, АНАЛІЗ БЕЗПЕКИ, ЗАХИЩЕНА СИСТЕМА, ВІДДАЛЕНИЙ КОРИСТУВАЧ, КОНТРОЛЬ.

ЗМІСТ

ВСТУП

В даний час, у більшості організацій використовуються локальні обчислювальні мережі. Чим більше організація, тим більш розгалужена та складніша мережа. З ростом організації росте обчислювальна мережа, переходячи в більш територіально рознесену, з'являються сервера і клієнти віддаленого доступу, контролери доменів, файл-сервера, сервера баз даних, ускладнюється активне мережеве устаткування, додаються протоколи мережевої і міжмережевої взаємодії, будуються VLAN, налагоджуються канали Frame-Relay і VPN, уся ця структура зветься – корпоративна мережа.

Одним з найпоширеніших способів обмежити взаємодію корпоративної мережі з зовнішнім світом є побудова захисту безпосередньо на кожній клієнтській машині (хості) за допомогою персонального антивірусу або недорогого персонального брандмауера і файєрвола.

Сама топологія корпоративних мереж майже завжди залишає бажати кращого, частенько використовуються застарілі мережеві топології (наприклад 10base-T, TokenRing), мережеве активне устаткування (концентратори невідомих фірм, та застаріли моделі маршрутизаторів).

Порушнику досить легко пробитися в таку мережу використовуючи безліч відомих вразливостей, неточності в написанні програмного забезпечення, недбалість обслуговуючого персоналу, відсутність грамотно описаної процедури протидії порушнику.

1 ЗАГАЛЬНІ ПРИНЦИПИ І ПІДХОДИ ДО СИСТЕМ ЗАХИСТУ

1.1 Поділ об'єкта на зони безпеки

Багатозональність забезпечує диференційований санкціонований доступ різних категорій співробітників і відвідувачів до джерел інформації й реалізується шляхом поділу простору, займаного об'єктом захисту (організацією, підприємством, фірмою або будь-якою іншою державною й комерційною структурою) на зони безпеки (контрольовані зони). Типовими зонами є:

- територія, що займає організація і обнесена забором або умовною зовнішньою границею;

- будинок на території;

- приміщення (службові, кабінет, кімната, зал, технічні приміщення, склад і ін.);

- шафи, сейфи, сховища.

Один з варіантів розташування зон безпеки об'єкта, що захищається, показаний на рис. 1.1.

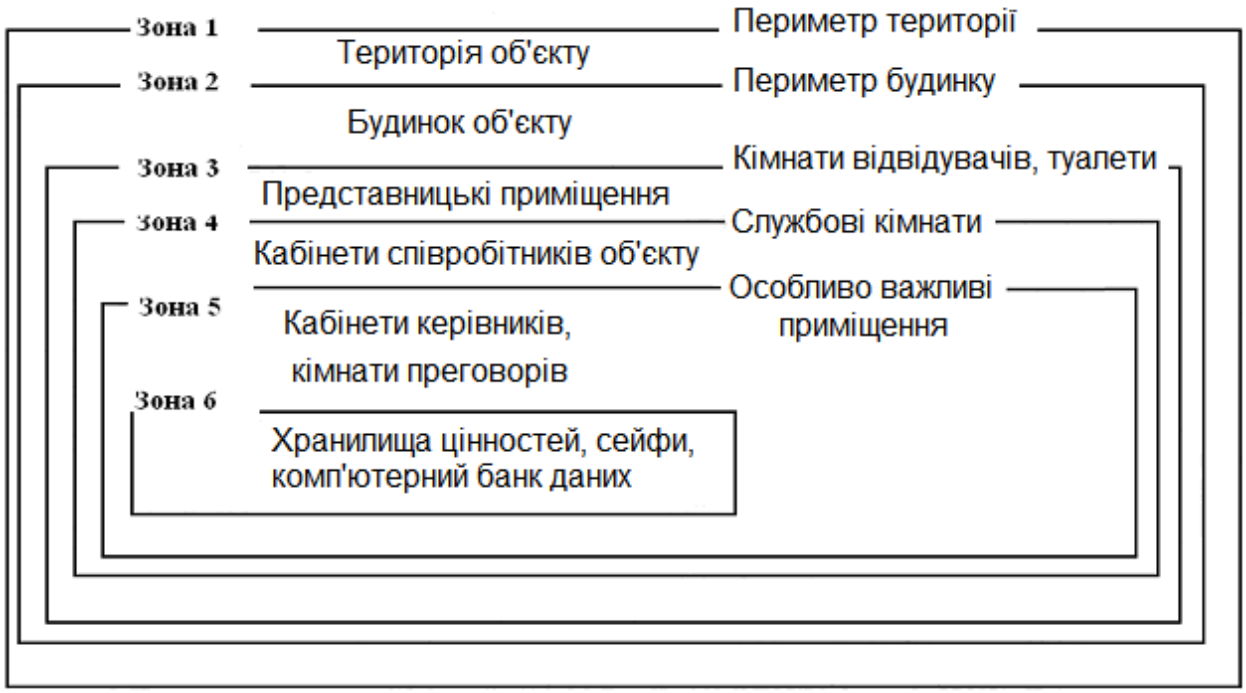

Рисунок 1.1 – Розташування зон безпеки об'єкта, що захищається

Варіант забезпечення безпеки (охорони) території такого об'єкта показаний на рис. 1.2.

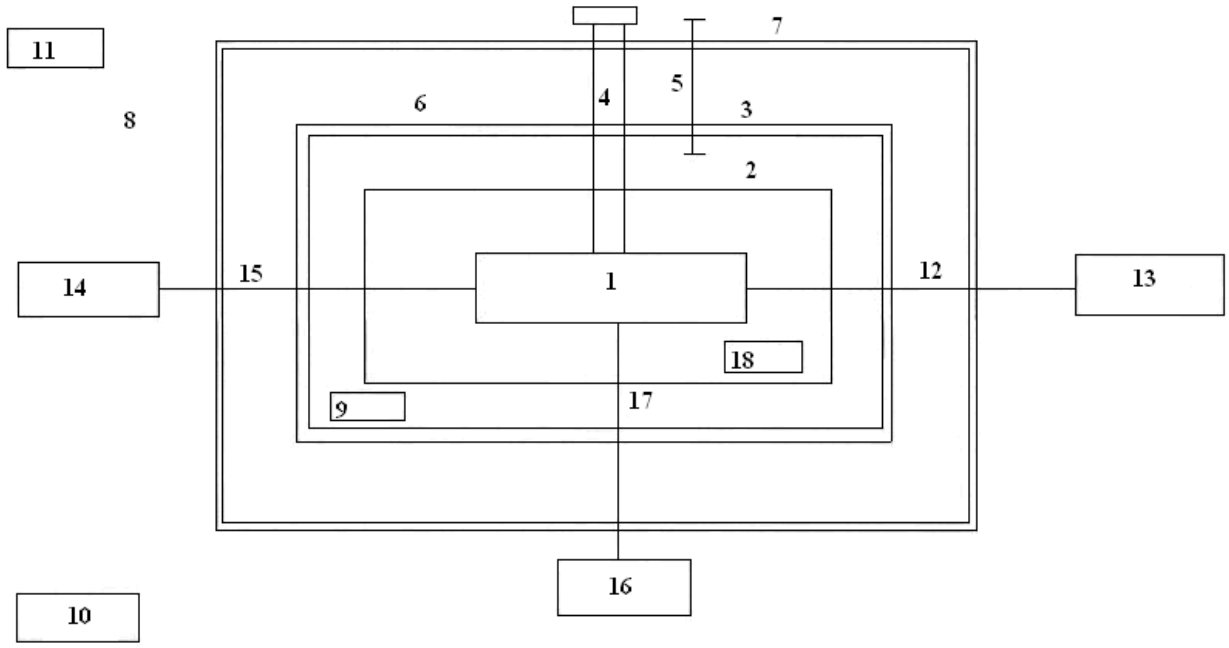

Рисунок 1.2 – Варіант системи забезпечення безпеки (охорони) об'єкта

На рис. 1.2 прийняті наступні позначення: 1) охороняємий об'єкт (серверна); 2) затримуюче огородження; 3) огородження, що виявляє порушників; 4) контрольований вхід; 5) зона оцінки; 6) нейтральна зона; 7) огорожа; 8) віддалений захист; 9) сили внутрішньої охорони; 10) сили зовнішньої охорони; 11) рухливий патруль; 12) канал зв'язку; 13) зовнішній об'єкт; 14) електропідстанція; 15) лінія електропередач; 16) об'єкти технічного забезпечення; 17) інженерні комунікації; 18) радіосигналізація.

Засоби протидії рекомендується розміщати на концентричних колах, що перетинають всі можливі шляхи супротивника до кожного з об'єктів. Кожний рубіж оборони варто створювати таким чином, щоб затримати нападаючого на час, достатній для прийняття персоналом охорони відповідних дій.

У тому випадку, якщо усередині будинку розташовуються об'єкти з істотно різними вимогами до безпеки, застосовується поділ будинку на відсіки, що дозволяє виділити внутрішні периметри усередині загального контрольованого простору й створити внутрішні захисні засоби від

несанкціонованого доступу. Периметр звичайно виділяється фізичними перешкодами, прохід через які контролюється електронним способом або за допомогою спеціальних процедур.

Зони можуть бути: незалежними (будинку організації, приміщення будинків), що перетинаються й вкладеними (сейф усередині кімнати, кімнати усередині будинку, будинку на території організації).

З метою запобігання проникненню зловмисника в зону на її границі створюються, як правило, один або кілька рубежів захисту. Особливістю захисту границі зони є вимога рівної міцності рубежів на границі й наявність контрольно-перепускних пунктів або постів, що забезпечують керування доступом у зону людей і автотранспорту.

Приклад вибору зон безпеки й побудови рубежів охорони наведений на рис. 1.3.

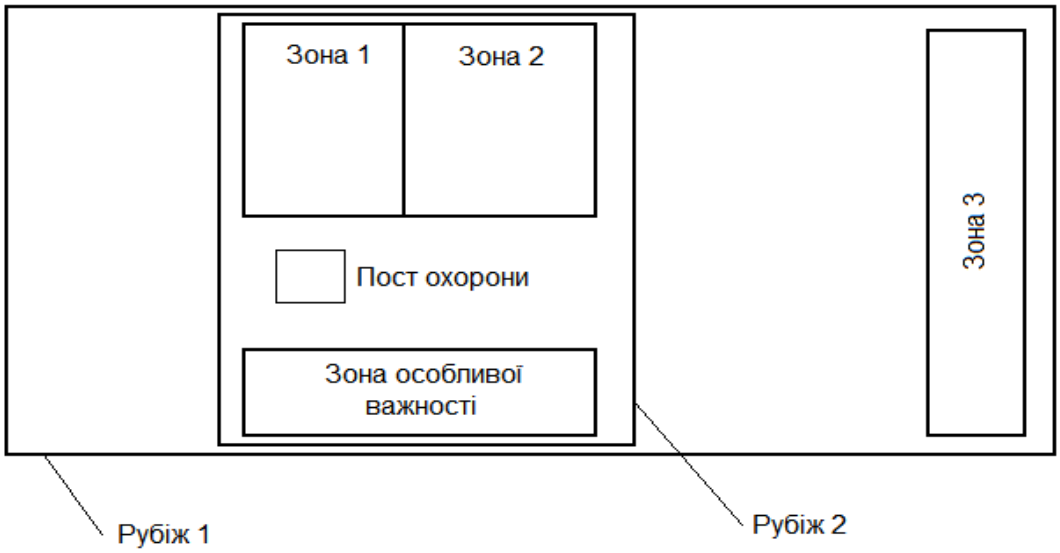

Рисунок 1.3 – Принципи багатозональності й багаторубіжності захисту інформації

Рубежі захисту створюються й усередині зони на шляху можливого руху зловмисника або поширення інших носіїв, насамперед, електромагнітних і акустичних полів. Наприклад, для захисту акустичної інформації від підслуховування в приміщенні може бути встановлений рубіж захисту у вигляді акустичного екрану.

Кожна зона характеризується рівнем безпеки інформації, що перебуває в ній. Безпека інформації в зоні залежить від:

- відстані від джерела інформації (сигналу) до зловмисника або його засобу добування інформації;

- кількості й рівня захисту рубежів на шляху руху зловмисника або поширення іншого носія інформації;

- ефективності способів і засобів керування допуском людей і автотранспорту в зону;

- заходів по захисту інформації усередині зони.

Чим більша дальність джерела інформації від місця знаходження зловмисника або його засобів добування інформації й чим більше рубежів захисту, тим більший час руху зловмисника до джерела й ослаблення носія у вигляді поля або електричного струму. Кількість і інше розташування зон і рубежів вибираються таким чином, щоб забезпечити необхідний рівень безпеки захисту інформації, як від зовнішніх (що перебувають поза територією організації), так і внутрішніх (що проникли на територію зловмисників і співробітників). Чим більш коштовною є інформація, тим більшою кількістю рубежів і зон доцільно оточувати її джерело й тем складніше зловмисникові забезпечити розвідувальний контакт із її носіями.

Безпека інформації в і-*й* зоні оцінюється ймовірністю $Q_i(\tau)$ забезпечення заданого рівня безпеки інформації протягом певного часу τ. Для незалежних зон значення цих ймовірностей незалежні:

$$Q_1(\tau) < Q_2(\tau) < Q_3(\tau) < Q_4(\tau) < Q_5(\tau),$$

де $Q_1 \ldots Q_5$ – імовірності забезпечення заданого рівня безпеки інформації відповідно для території, будинку, поверху, приміщення й сейфа.

Об’єкт можна класифікувати за ступенем захищеності зон (табл. 1.1).

Таблиця 1.1

Класифікація зон за ступенем захищеності

Категорія	**Найменування зони**	**Функціональне призначення зони**	**Умови доступу співробітників**	**Умови доступу відвідувачів**
0	Вільна	Місця вільного відвідування	Вільний	Вільний
I	Спостережувана	Кімнати прийому відвідувачів, секретаріат	Вільний	Вільний
II	Реєстраційна	Кабінети співробітників служб і відділів	Вільний	З реєстрацією по посвідченню особи
III	Режимна	Комп'ютерні зали, архіви	По іденти-фікаційним картам	По разових пропусках
IV	Посиленого захисту	Операційні зали обробки фінансової та звітної інформації, склади цінностей	По спец-документам	По спец-перепусткам
V	Вищого захисту	Шафи, сейфи, хранилищ	По спец-документам, біометрія	По спец-перепусткам, біометрія

Якщо безпека інформації в кожній зоні забезпечується тільки рубежем на її границі, то для доступу зловмисника, наприклад до документа, що зберігається в спеціальному сховищі, йому необхідно перебороти 5 рубежів: границю території, увійти в будинок, у коридор потрібного поверху, у приміщення й відкрити сховище. У цьому випадку безпека інформації в *k*-ій зоні Q_k оцінюється величиною:

$$Q_k(\tau) = 1 - \left[\left(1 - Q_1(\tau)\right) \cdot \left(1 - Q_2(\tau)\right) \cdot \left(1 - Q_3(\tau)\right) \cdot \left(1 - Q_4(\tau)\right) \cdot \left(1 - Q_5(\tau)\right) \cdot \ldots\right].$$

Виходячи із загальної теорії об'єктів, що захищаються, інформаційної діяльності, можна зробити висновок, що наш об'єкт надійно захищений.

1.2 Розробка моделі погроз даним серверної

Головною метою будь-якої системи інформаційної безпеки є забезпечення стійкого функціонування об'єкта, запобігання погроз його безпеки, захист законних інтересів замовника від протиправних зазіхань, недопущення розкрадання фінансових звітів, розголошення, втрати, витоку, перекручування й знищення інформації, забезпечення нормальної виробничої діяльності всіх підрозділів підприємства. Іншою метою системи інформаційної безпеки є підвищення якостей послуг і гарантій безпеки, майнових прав і інтересів клієнтів, які надаються.

Досягнення заданих цілей можливо в ході рішення наступних основних завдань:

- віднесення інформації до категорії обмеженого доступу (конфіденційна);

- прогнозування й своєчасне виявлення погроз безпеки інформаційним ресурсам, причин і умов, що сприяють нанесенню фінансового, матеріального й морального збитку, порушенню його нормального функціонування й розвитку;

- створення умов функціонування з найменшою вірогідністю реалізації погроз безпеки інформаційним ресурсам і нанесення різних видів збитку;

- створення умов для максимально можливого відшкодування й локалізації збитків, що наноситься неправомірними діями фізичних і юридичних осіб, послаблення негативного впливу наслідків порушення інформаційної безпеки на досягнення стратегічної мети.

При виконанні робіт зі створення інформаційної системи безпеки можна використовувати наступну модель (рис. 1.4).

Ця модель відповідає нормативним документам по забезпеченню інформаційної безпеки, прийнятим в Україні, міжнародному стандарту ISO/IEC 15408 "Інформаційна технологія – методи захисту – критерії оцінки інформаційної безпеки", і враховує тенденції розвитку вітчизняної нормативної бази.

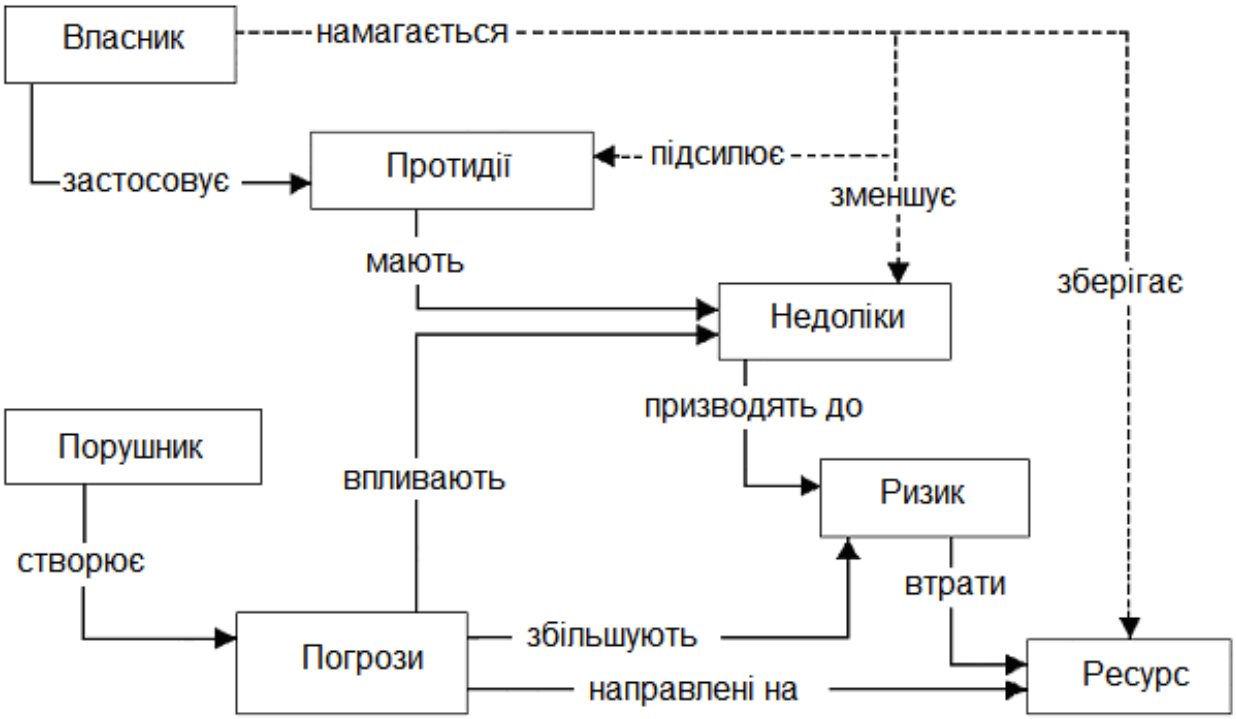

Рисунок 1.4 – Модель забезпечення інформаційної безпеки об'єкта

Запропонована модель інформаційної безпеки – це сукупність об'єктивних зовнішніх і внутрішніх факторів і їхній вплив на стан інформаційної безпеки на об'єкті й на збереження матеріальних або інформаційних ресурсів.

Розглядаються наступні об'єктивні фактори:

- погрози інформаційної безпеки, які характеризуються вірогідністю виникнення й вірогідністю реалізації;

- уразливість інформаційної системи або системи контрзаходів (системи інформаційної безпеки), що впливає на вірогідність реалізації погрози;

- ризик – це фактор, що відображає можливий збиток організації в результаті реалізації погроз інформаційної безпеки: втрати інформації і її неправомірного використання (ризик в остаточному підсумку відображає достовірні фінансові втрати – прямі або непрямі).

Пропонована методика дозволяє:

- повністю проаналізувати й документально оформити вимоги, пов'язані із забезпеченням інформаційної безпеки;

- уникнути витрат на зайві заходи безпеки, можливі при суб'єктивній оцінці ризиків;

- надати допомогу в плануванні й здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем;

- забезпечити проведення робіт у стислий термін;

- представити обґрунтування для вибору заходів протидії;

- оцінити ефективність контрзаходів, порівняти різні варіанти контрзаходів.

Для того щоб побудувати збалансовану систему інформаційної безпеки передбачається спочатку провести аналіз можливих погроз в області інформаційної безпеки. Потім, на підставі аналізу погроз, що існують у системі вразливостей, повинні бути описані вимоги для комплексу засобів захисту інформації від цих погроз. На підставі виконаної роботи повинні бути вироблені заходи захисту, перетворення яких у життя дозволило б знизити рівень можливих погроз.

Отже, перед тим як запропонувати заходи захисту, спочатку опишемо вимоги до них:

1. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їхнього експорту й імпорту;

2. Перш ніж користувач або процес зможе одержати у своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що втримується в даному об'єкті, повинна стати недосяжною;

3. Повинен виконуватися аналіз схованих каналів з метою виявлення й усунення потоків інформації, які існують, але не контролюються;

4. Комплекс засобів захисту повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що втримується на об'єкті. Запити на призначення або зміну рівня захищеності повинні оброблятися

комплексом засобів захисту тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження;

5. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності повинні бути представлені правила збереження атрибутів доступу до об'єктів під час їхнього експорту й імпорту. Запити на зміну прав доступу до об'єкта повинні оброблятися комплексом засобів захисту на підставі атрибутів доступу користувача, що ініціює запит до об'єкта;

6. Запити на зміну прав доступу повинні оброблятися комплексом засобів захисту тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження;

7. Комплекс засобів захисту повинен надавати можливість адміністраторові або користувачеві, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування приналежністю користувачів, процесів і об'єктів до відповідної доменам визначити конкретні процеси й/або групи процесів, які мають право модифікувати об'єкт;

8. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачеві або процесу відкликати або скасувати певний набір (безліч) операцій, виконаних над захищеним об'єктом за певний проміжок часу;

9. Повинен забезпечувати можливість виявлення порушення цілісності інформації, що втримується на об'єкті, що передається, а також фактів його видалення або дублювання;

10. Повинна існувати можливість установлювати обмеження таким чином, щоб комплекс засобів захисту мав можливість запобігти діям, які можуть привести до неможливості доступу інших користувачів до функцій комплексу засобів захисту або захищених об'єктів. Комплекс засобів захисту повинен контролювати такі дії, здійснювані з боку окремого користувача;

11. Відмова одного захищеного компонента не повинна приводити до неприступності всіх послуг, а повинен у найгіршому разі проявлятися в зниженні характеристик обслуговування;

12. Комплекс засобів захисту повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори й користувачі, яким надані відповідні повноваження, повинні мати у своєму розпорядженні засоби перегляду й аналізу журналу реєстрації;

13. Політика ідентифікації й аутентифікації, що реалізується комплексом засобів захисту, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися комплексом засобів захисту;

14. Політика достовірного каналу, що реалізується комплексом засобів захисту, повинна визначати механізми встановлення достовірного зв'язку між користувачем і комплексом засобів захисту;

15. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, які підтверджують прийняття їм цієї ролі;

16. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс комплексу засобів захисту й всі запити на доступ до захищених об'єктів контролюються їм;

17. Політика самотестування, що реалізується комплексом засобів захисту, повинна описувати властивості інформаційної системи й реалізовані процедури, які можуть бути використані для оцінки правильності функціонування комплексу засобів захисту;

18 .Комплексом засобів захисту, перш ніж почати обмін даними з іншим комплексом засобів захисту, повинен ідентифікувати й аутентифікувати цей комплекс із використанням захищеного механізму.

Аналіз представленої класифікації об'єктів захисту й загальних характеристик моделі погроз дозволяє зробити наступні виводи.

По-перше, без знання моделей об'єктів захисту може бути розроблена тільки перша модель погроз – модель інформаційно-технічної розвідки.

По-друге, розробка інших всіх моделей в цілому, а також вишукування шляхів і засобів захисту об'єктів доцільно, як єдиний процес, першим етапом якого є розробка моделі погроз.

По-третє, вихідними даними для моделі погроз є модель інформаційно-технічної розвідки і моделі об'єктів, що захищаються.

По-четверте, проблема ТЗІ є науково-технічною проблемою й повинна вирішуватися як така.

Відповідно до прийнятої методики перейдемо до керування доступом. Отже, обираємо функціональний профіль захищеності, що виявляє собою перелік мінімально необхідних рівнів послуг, які повинен реалізувати комплекс засобів захисту інформаційної системи, щоб задовольнити висунуті вимоги.

2 ЗАХИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

2.1 Архітектура сервера

Конфігурація сервера: Intel Xeon 3.2GHz (HT), Dual, DDR IV 64 GB / SSD 500 GB. Дана конфігурація серверного хоста дозволяє швидко обробляти багато задач й обробляти великі запити до бази даних і WEB-порталу компанії. Так само за рахунок організації на апаратному рівні Hyper Threading навантаження на CPU буде зменшена.

Встановлене програмне забезпечення на сервері:

- операційна система Windows Server 2003;
- WEB-сервер Apache 2.2.x + PHP 5.x.;
- база даних MySQL 5.x або MSSQL;
- мережевий фільтр;
- антивірусне програмне забезпечення;
- поштовий сервер;
- FTP-сервер;
- проксі-сервер;
- програмне забезпечення для виявлення „троянів”.

2.2 Мережева безпека сервера

Для забезпечення мережевої безпеки серверного хоста, необхідно відкрити наступні порти:

1. **80 порт** WEB-сервера;
2. **8080 порт** proxy-сервера;
3. **21 порт FTP**-сервер;
4. **25 порт SMTP**-сервер;
5. **110 порт POP3** для прийому листів;
6. **3306 порт MySQL**-сервера (дозволити керування тільки для виділених IP);

7. **3381 порт RPC** віддалене адміністрування (дозволити керування тільки для виділених IP).

Виходячи з мір безпеки в мережі, всі інші порти повинні бути закриті, або відкриті тільки для довірених IP адрес. Дану задачу за контролем над доступом до портів виконує в нас мережевий фільтр. Так само за допомогою мережевого фільтру ми повинні встановити контроль за додатками запущеними на сервері для обліку – з якими портами ці додатки працюють, а також який мережевий протокол вони використовують.

Так само для загальної безпеки рекомендується закрити **ECHO порт** (через пінг хоста можлива організація флуд атаки, що може привести до не стабільної роботи всього хоста).

2.3 Сучасні охоронні брандмауери

Більшість організацій працюють із операційною системою Windows, перекладаючи всі можливі проблеми з безпекою під час своєї присутності в мережі на її плечі.

Однак, як показує практика, з питанням безпеки в Microsoft, незважаючи на всі її зусилля, існують чималі проблеми. Тому зараз і виходить на перший план питання охорони особистої інформації користувача сторонніми засобами.

Мережа надає прекрасні можливості для існування й розмноження різного роду шкідливих програм: хробаків, вірусів, троянських коней. Крім того, звичайно, дуже неприємна діяльність спливаючої реклами й спаму. Чого коштують, хоча б, недавні наслідки діяльності багатостраждального Blaster'a. І тільки завдяки відсутності у автора цього вірусу деструктивних помислів, величезна кількість людей крім морального збитку не одержали більше серйозних наслідків, одним з найстрашніших, звичайно, могла б бути втрата інформації.

Однак, зараження можна було б уникнути при наявності програм, що мають назву firewall (файєрвол), здатними позбавити користувача від багатьох

проблем, пов'язаних з особистою безпекою. Ці програми дозволяють користувачеві самому визначати, чи дозволяти одержання або, навпаки, відправлення TCP/IP-пакетів з робочого комп'ютера.

Можна настроїти доступ до Інтернет тільки дозволеним програмам, наприклад, Web-браузеру, клієнтові електронної пошти, менеджерові закачування, ICQ або IRC. Таким чином, інші програми, які раніше могли самовільно приймати або пересилати дані на віддалений комп'ютер, не зможуть зробити свої дії. Крім того, файєрвол здатний відслідковувати доступ до машини через відкриті порти.

Користувач сам може настроїти безпечні з'єднання, забороняючи, таким чином, потенційно небезпечні. Безумовно, в епоху інформаційного розвитку, клас таких програм користується величезною популярністю. І гідних продуктів на ринку чимало.

Для розгляду я взяв декілька продуктів, що б вибрати найбільш корисніший:

- Sunbelt Kerio Personal Firewall;
- McAfee Firewall;
- Norton Personal Firewall;
- Outpost;
- Sygate Pro's firewall;
- ZoneAlarm Pro;

2.3.1 Sunbelt Kerio Personal Firewall

Sunbelt Kerio Personal Firewall – представляє собою надійну, легку у використанні персональну технологію безпеки, яка повністю захищає персональний комп’ютер від хакерських атак та витоку даних.

Кожний Windows-комп’ютер, під’єднаний до Інтернету надсилає та одержує деякі дані (рис. 2.1). Sunbelt Kerio Personal Firewall представляє користувачам огляд того, які додатки відправляють дані, а які одержують.

Рисунок 2.1 – Огляд Інтернет з’єднань

Sunbelt Kerio Personal Firewall не пропонує попередньо встановлену універсальну політику безпеки (рис. 2.2), скоріше він постачає засобами для створення та дотримання такої політики.

Рисунок 2.2 – Створення політики безпеки

Перший крок в створенні політики безпеки – це визначення того, який тип доступу до Інтернету є дозволеним. Sunbelt Kerio Personal Firewall точно знає, які додатки намагаються вийти в Інтернет. Користувачі можуть дозволити доступ до Інтернету для надійних додатків, і в той час блокувати інші.

Наприклад, додаткам для спілкування доступ може бути дозволеним, а для програм, що використовують розділені файлові ресурси – заборонений.

«Продвинуті» користувачі або мережеві адміністратори можуть створювати правила фільтрації пакетів, які блокують або лімітують трафік для визначених портів, протоколів або IP-адрес, надаючи рівень контролю та безпеки, який можна знайти тільки в складних мережевих файєрволах.

Огляд трафіку показує, що комп'ютер робить у визначений момент часу, відображаючи, що блокується та що дозволено. Це допомагає користувачу легко бачити чи необхідно коригувати правила. Історія трафіку може бути записана з використанням настоюваного рівня деталізації та відправлена на віддалений сервер для огляду адміністратором.

2.3.2 McAfee Firewall

Коментар: McAfee Firewall – легкий в установці й використанні firewall. Після першого запуску файєрвола, "Помічник" допомагає без особливих проблем настроїти програму.

Після того, як файєрвол був встановлений, він автоматично запускається в режимі "Стандартної безпеки" (рис. 2.3), блокуючи будь-який сумнівний трафік з Інтернету і відзначаючи все це в журналі безпеки. Щоб змінити режим, варто нажати правою клавішею миші на іконку McAfee Firewall, вибрати "Personal Firewall", а потім вибрати "Set Security Level".

Рисунок 2.3 – Зовнішній вигляд McAfee Firewall

Вікно програми складається з верхнього меню й поля інформації, де з лівої сторони традиційно доступні елементи меню, а праворуч – їхній зміст.

McAfee Firewall містить наступні пункти меню: Summary (загальна статистика, останні подія, останні новини), Internet Applications – програми, що намагаються з'єднатися з Інтернет, Inbound Events (вхідні події, потенційно – спроби атаки), Utilities (додаткові утиліти).

З підменю в "Personal Firewall" можна також вибрати наступні:

- View Summary – перегляд загальної повної статистики блокованого трафіку й атак на комп'ютер;

- View Applications – перегляд дозволених і блокованих додатків, що робили спробу доступу до Інтернет;

- View Events – перегляд історії подій.

У процесі роботи, McAfee показав відкритість 139 порту (NetBIOS) при всіх скануваннях, залишаючи, таким чином, машину уразливою до дослідження програмами ShieldsUP!, PC Flank, SMBDie й Retina. Хоча сканування від NAT і спроби атаки від SMBDie були виявлені й блоковані.

У цілому, відкриття 139 порту в настроюваннях за замовчуванням – погана ідея. Retina також знайшла відкритий 1025 порт (потрібний для роботи мережевих доступів, що використовується деякими троянськими кіньми).

Діяльність spyware (шпигунського програмного забезпечення) була виявлена в додатках SaveNow, Adware й Brilliant, однак, блокування їхньої діяльності було дуже слабким, або було відсутнє зовсім.

McAfee також дозволяє браузеру збирати й пересилати cookies з потенційно особистою інформацією, небажаної для розголосу.

У цілому, McAfee – легкий у використанні, і є непоганим захистом від діяльності розповсюджених експлоїтів. Це гарний вибір для початківців, яким складно розбиратися з тонкостями настроювання програми, однак занадто спрощений і неповноцінний для досвідчених користувачів.

До додаткових можливостей програми можна віднести:

- надбудовані візуальні й звукові попередження;

- безкоштовна технічна підтримка по електронній пошті або в режимі реального часу (Chat);

- автоматичне оновлення через Інтернет.

2.3.3 Norton Personal Firewall

Коментар: Norton Personal Firewall – досить простий для домашнього користувача firewall, має проте необхідні тонкі настроювання для більше досвідчених користувачів.

При першому запуску програма відкриває "Помічника", що допомагає встановити програму, проробивши наступне його настроювання, без яких-небудь проблем. Подібно McAfee, NPF (рис. 2.4) поділяє жорсткий диск на додатки, що працюють з Інтернет, але на відміну від конкурента, може автоматично надавати доступ.

Рисунок 2.4 – Зовнішній вигляд Personal Firewall

Можна також призначити пароль для зміни настроювань. На жаль, "Помічник" не зміг визначити домашню мережу, повідомляючи про незнайдені адаптери для настроювання з'єднання з мережею. Проте,

незважаючи на це повідомлення, комп'ютер міг з'єднуватися з Інтернет, розділяючи для віддаленого використання також файли й принтери.

Всі інші установки виробляються вже в процесі роботи Norton Personal Firewall. На скриншоті показане основне вікно програми, де основні настроювання програми для користувача здійснюються на рівні on-off (включене/виключене):

- захист комп'ютера від вторгнень через Інтернет (Security);
- захист даних від спроб несанкціонованого доступу (Personal Firewall);
- виявлення й відбиття атак (Intrusion Detection);
- блокування банерів і рекламних блоків (Ad blocking).

Тут же за допомогою повзунка виставляється низький, середній або високий рівень захисту.

Верхнє піктограмне меню програм дозволяє вибирати між Монітором Захисту (Security Monitor), Блокуванням Трафіку (Block Traffic), Оновленням через Інтернет (Live Update), і Настроюваннями (Options). При необхідності однією кнопкою з головного вікна можна заблокувати/розблокувати доступ в Інтернет всіх програм.

NPF – єдиний файєрвол, що повністю запобігає пересиланню особистої інформації на віддалений комп'ютер. Він також виявляє й блокує будь-яку спробу атаки на машину. При скануванні кожен порт був закритий від очей хакера, cookies були блоковані. Відмінно організована робота перелогів-файлів, що надають детальну інформацію і ясні пояснення подій, що відбулися. Ця інформація надалі може допомогти в ідентифікації атакуючіх.

Зручне невелике функціональне вікно, у якому з'являється гістограма поточного трафіку, виводяться повідомлення про атаки й доступні всі основні функції програми.

На відмінність від більшості інших файєрволів, які лише повідомляють про атаку, NTF дозволяє оцінити характер і серйозність погрози й порадити виконати необхідні дії. Подібний консультативний підхід був впроваджений

також у визначення роботи spyware, хоча його блокування було недостатньо гарним, а часами було відсутнє повністю.

2.3.4 OutPost

Коментар: створений як самий "просунутий" файєрвол (рис. 2.5) для Windows (має величезну кількість опцій, що набудовуються,), OutPost використовується в домашніх умовах, хоча й розроблений переважно для фахівців.

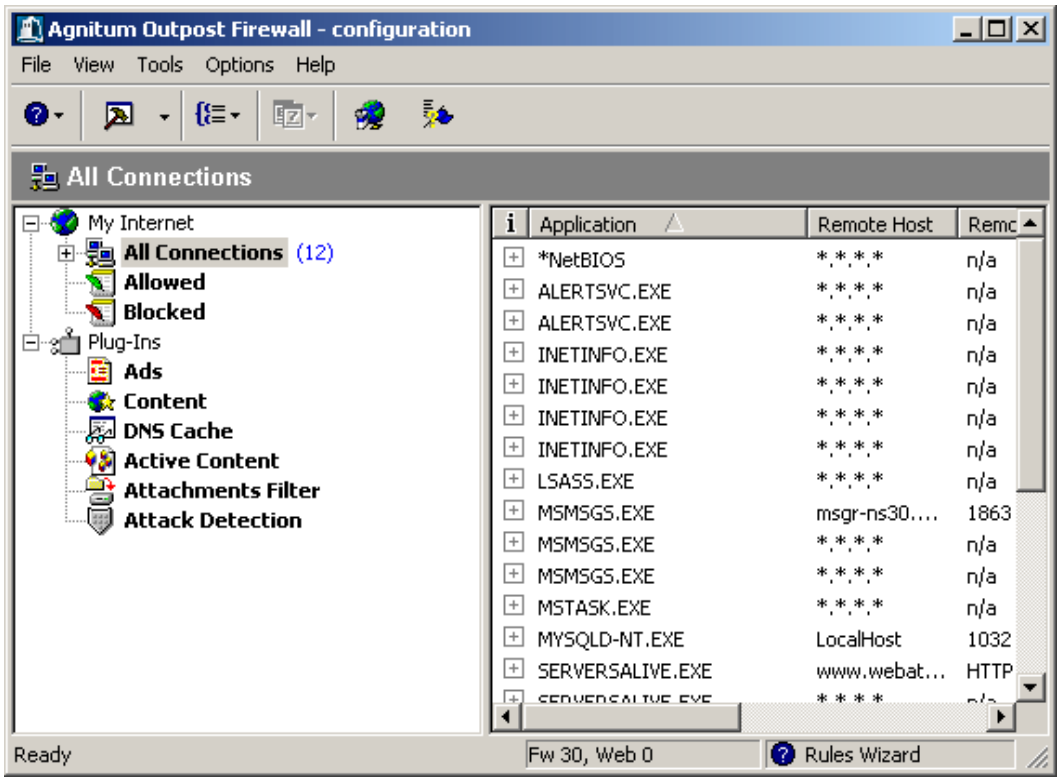

Рисунок 2.5 – Зовнішній вигляд OutPost

Настроювання для файєрвола передбачається через завантаження з офіційного сайту розроблювача в Інтернеті, які надалі можуть бути доповнені досвідченими користувачами через вбудовані програмні засоби. Призначення "Помічника" настроювання досить специфічне: він не дозволяє визначати вам власні настроювання для файєрвола, даючи лише інформацію з використання продукту.

Вікно програми складається з верхнього меню, меню піктограм, куди винесені найбільш необхідні функції й вікна З'єднання. Ліворуч у цьому вікні перебуває меню, а праворуч – виводиться інформація з кожного пункту. У меню у вікні З'єднання 2 більші закладки: My Internet – статистика по з'єднанню з Інтернет і Plug-Ins, що підключають модулі, серед яких, варто відзначити:

- ADS – модуль видалення рекламних блоків при відображенні в браузері Web-сайтів. Він має доповнювати базу стандартних для реклами рядків гіпертексту й розмірів найбільш використовуваних блоків реклами (100x100, 125x125, 468x60, 470x60, 234x60, 120x80, 88x31 пікселів), по яких і відбувається фільтрація. Використання цієї функції дозволяє значно збільшити швидкість завантаження сайтів;

- Content – блокування доступу до Web-сайтів з певними адресами або вбудованими в html-коді певними рядками;

- Active Content – блокування активних елементів Web-сайтів, наприклад виконання Active, сценаріїв, написаних на Java й Visual Basic;

- Attachments Filter – виведення повідомлення при спробі одержання/запуску файлу, що виконується;

- Attack Detection – детектор і блокування атак. При використанні цієї функції можна вибрати один із трьох режимів безпеки: блокування IP-адреси атакуючого (у випадку точної ідентифікації атаки), блокування спроби сканування декількох портів або порту з певним номером, блокування спроби сканування одного порту, можливе також блокування DoS-атак.

Тестування OutPost Retin'ой показало відкритими порти 135, 1025 й 5000 (універсальний Plug and Play), залишаючи машину потенційно уразливою. ShieldsUP! також показав відкритий 5000 порт, однак PC Flank не виявив ніяких відкритих портів. Cookies також не блокуються, незважаючи на твердження розроблювачів про відсутність можливості Web-сайтів збирати й пересилати інформацію про переваги користувачів при серфінгу. У настроюваннях за замовчуванням спливаючі вікна не показуються, хоча й

відзначаються в перелогах-файлах. Це не дуже зручно, тому що не кожен користувач буде заглядати в історію подій. Крім того, організація перелогів-файлів прорoблена недостатньо чітко, записуючи лише факт атаки, не залишаючи навіть дати й часу нападу.

Діяльність KaZa прирівняна до spyware, тому для роботи із цим сервісом користувач повинен вибирати між блокуванням сервісу або роботою з ним без якого-небудь захисту. Розглянута версія – перший випуск даного продукту, що має безліч додаткових корисних настроювань, малопридатна для початківців, тому що робота програми з настроюваннями за замовчуванням майже безглузда.

2.3.5 Sygate Pro’s firewall

Коментар: Sygate Pro's firewall настроюється за допомогою відповідей користувача, на можливість певних додатків мати доступ до Інтернет: коли додаток запускається – файєрвол виводить вікно діалогу для вибору доступу цього додатка: дозволити або заборонити. Користувач може створювати власний список правил (по порту, за адресою).

Передбачається, що технічно користувач непогано підкований, хоча по цьому питанню є додаткова система допомоги.

Користувачеві надаються журнали всіх дій, що відбуваються під час виконання програми:

- журнал атак, сканування портів комп'ютера й інших зазіхань на його безпеку;

- журнал з найдокладнішою інформацією по вхідному й вихідному трафіку із вказівкою програми, IP-адреси, порту, часу початку й закінчення процесу;

- журнал проходження пакетів;

- журнал запуску й закриття брандмауера.

Настроювання програми включають наступні основні функції:

- захист настроювань програми паролем для запобігання несанкціонованої зміни їх іншими користувачами комп'ютера;

- включення/відключення детектора сканування портів й інших видів найпоширеніших атак;

- завдання часу, протягом якого буде блокуватися надходження інформації з IP-адреси атакуючого;

- автоматичне відсилання інформації про атаку на певну електронну адресу;

- завдання максимального розміру журналів роботи;

- автоматичне оновлення через Інтернет.

На екрані користувачеві надається інформація в графічному виді (рис. 2.6) про вхідний/вихідний трафік, про напади.

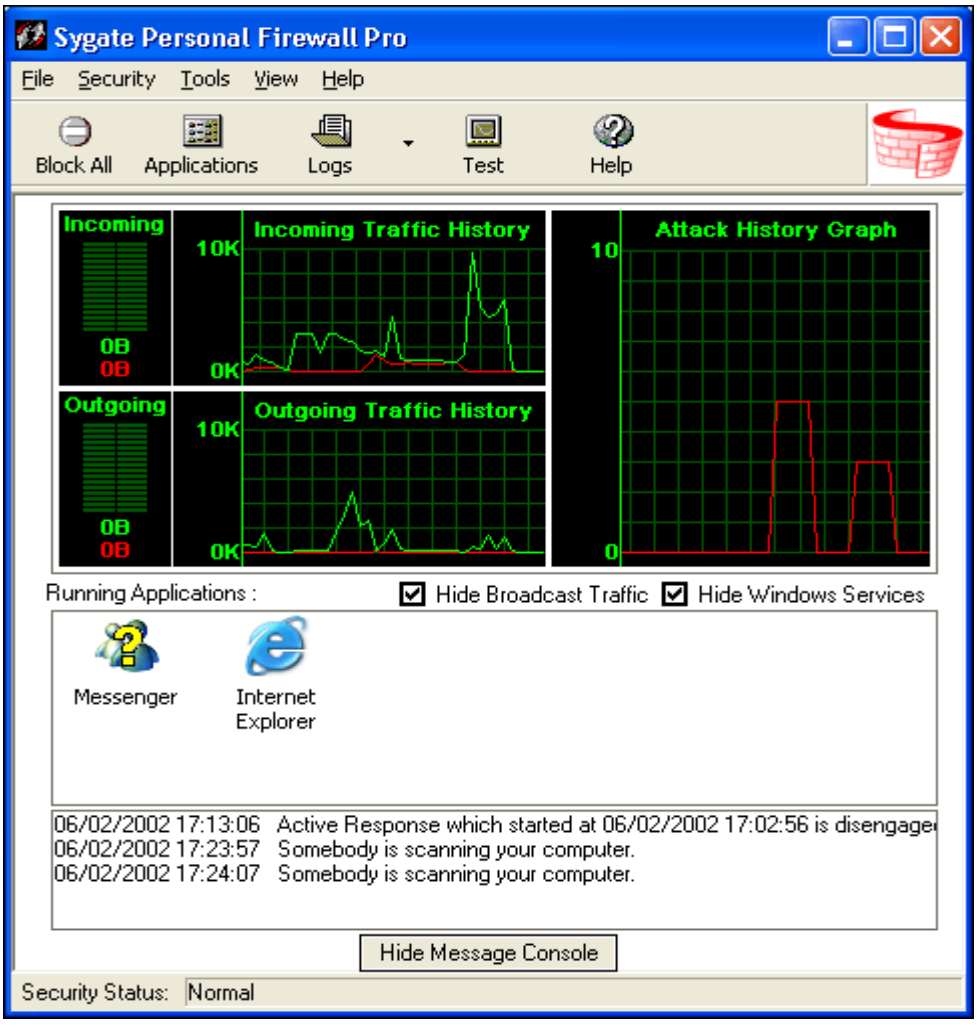

Рисунок 2.6 – Зовнішній вигляд Sygate Pro's

Цей файєрвол добре захищає машину від проникнення з боку порушника, автоматично виявляючи й забороняючи доступ атакуючого на певний, заданий проміжок часу.

Порти 5000 й 135 при скануванні здалися відкритими, однак вторгнення PC Flank й ShieldsUP! були блоковані. Інші порти були закриті й невидимі для хакерів. DoS-атаки, NAT сканування й експлойти SMBDie були дозволені з довіреної зони, однак, повністю блоковані із зовнішньої сторони. Виявлення діяльності spyware відмінне, отриманої інформації досить для блокування цих програм.

Просунуті користувачі, безперечно, залишаться задоволені гарною організацій перелогів-файлів, роботою з електронною поштою, прихованню системної панелі й блокуванню TCP й IPX-трафіку. У цілому, цей файєрвол дуже гарний, не вважаючи відкритих за замовчуванням уразливих портів, "закриття" яких може викликати труднощі для більшості користувачів.

2.3.6 ZoneAlarm Pro

Коментар: ZoneAlarm Pro – значно вдосконалена версія ZoneAlarm, з організацією особистого захисту машини, безліччю можливостей, що набудовують самі користувачі, захистом електронної пошти й Інтернет-гейтів (рис. 2.7).

Рисунок 2.7 – Зовнішній вигляд ZoneAlarm Pro

Незважаючи на додаткові можливості, розмір дистрибутива усе ще перебуває в межах 4 Мбайт. При установці всю роботу виконує "Помічник", крім того, опції роботи з cookies задаються вже при інсталяції.

Настроювання спрощене в порівнянні з вільно розповсюджуваною версією файєрвола (ZoneAlarm): менше спливаючих діалогів, що запитують дії користувача для якоїсь програми.

Основне (і єдине) функціональне вікно розділене на дві частини. У верхній, меншій за розміром містяться:

- графічно представлені відомості про обсяг вхідної і вихідної інформації. Ця ж гістограма є присутня як значок ZoneAlarm Pro у нижньому правому куті екрана поруч із годинниками;

- кнопка блокування доступу в Інтернет;

- піктограма, що відображає наявність підключення до Інтернету й IP-адресу;

- інформація про програми, що працюють із Інтернетом у даний момент.

Нижня, більша за розміром, частина вікна містить усілякі настроювання й інформацію, розділену по групах:

- Overview (огляд) включає відомості про число відбитих атак і кількість програм, що мають доступ в Інтернет; дані про ZoneAlarm Pro (реєстрації, версії й т.д.), короткі настроювання програми: установка пароля на користувальницькі настроювання, включення автоматичного (або ручного) оновлення ZoneAlarm через Інтернет, включення автоматичного запуску ZoneAlarm Pro після завантаження комп'ютера, режиму приховання IP-адреси й т.д.;

- Firewall (захист від несанкціонованого доступу) включає змінювані за допомогою повзунка установки захищеності (високий рівень, коли всі підозрілі пакети й інформація блокуються, а комп'ютер при спробах його ідентифікації ззовні "небачимий"; середній рівень, коли ПК за тих самих умов ззовні "бачимий", але ресурси його блокуються; низький рівень – захист відключений). Режими встановлюються окремо для трьох зон, дві з яких

визначаються користувачем. Це так званий "білий" список, що включає комп'ютери, інформація з яких не блокується й вважається безпечною, наприклад, комп'ютери тієї ж локальної мережі. У так званий "чорний" список входять комп'ютери з небезпечною інформацією. Сюди користувач звичайно заносить ті IP-адреси, з яких він раніше був атакований. Третя зона, не обумовлена користувачем, – це всі інші сервери, що не ввійшли ні в "білий", ні в "чорний" список. Крім того, тут утримується інформацію про з'єднання з Інтернетом, IP-адресу, маску під мережі;

- **Program Control** (контроль над програмами) включає вибір рівня контролю над програмами: високий припускає, що всі програми запитують доступ в Інтернет і встановлений контроль над використовуваними програмами динамічно підключеними бібліотеками (dll), при середньому всі програми запитують доступ в Інтернет, а контроль над використовуваними dll-файлами перебуває в режимі навчання (ZoneAlarm Pro запитує користувача про необхідність контролю в конкретних випадках), низький рівень має на увазі, що й контроль над програмами, і контроль над dll-файлами перебуває в режимі навчання, коли всілякий контроль відключений. Program Control також містить список програм із вказівкою наявності доступу в Інтернет і перелік всіх бібліотек, що підключають динамічно, використовуваних програмами;

- **Alerts & Logs** (сигнали й журнали) визначає рівень установки виводу сигналів при атаках і ведеться журнал з повною інформацією про них. Можливе відображення сигналів при всіх атаках, тільки при особливо небезпечних або при відсутності відображення. Аналогічно настроюється ведення журналу з описом виду атаки, позначенням її часу й дати, а також IP-адреси що атакує й порту, на який йде атака;

- **Privacy** (таємність) користувач вибирає режим роботи з інформаційними файлами. Можливе блокування всіх інформаційних файлів (що напевно спричинить проблеми з відображенням деяких Web-сайтів), блокування надходження даних з перерахованих користувачем сайтів і відсутність блокування;

- E-mail protection (захист електронної пошти). Спеціальна функція MailSafe перевіряє всі прийняті по електронній пошті файли на наявність вірусів й інших деструктивних об'єктів і попереджає про них користувача.

Pro-версія надає прекрасне настроювання для завдання доступу до Інтернет кожного додатка (можливість доступу по портах).

ZoneAlarm Pro добре виявив себе при рясних атаках, виявляючи й блокуючи будь-яку спробу проникнення. Всі порти були закриті, NetBIOS-доступ, так само як і більшість cookies, були заборонені. Блокування спливаючої реклами також працювало, причому іноді надмірно агресивно, порушуючи нормальну роботу деяких скриптів браузера Internet Explorer'a. Організація перелогів-файлів – чудова. Інформація там деталізована, існує навіть можливість пошуку географічного місця розташування нападника. Spyware виявляє добре, KaZa функціонує, причому програма не здатна завантажити рекламу з http або ftp.

ZoneAlarm Pro – один із кращих файєрволов огляду, досить простий і зручний для починаючих користувачів, але проте, він має тонкі й детальні настроювання для більше досвідчених користувачів.

2.4 Програмне забезпечення для виявлення вторгнень

Проблема інформаційної безпеки стає усе більше актуальною з кожним днем, а шкода, заподіювана вірусами нового покоління, усе більше відчутною.

Розроблювачам антивірусного ПЗ дуже складно оперативно випускати оновлення для своїх продуктів, а системні адміністратори не завжди встигають вчасно реагувати на нові епідемії.

Основна категорія комп'ютерів, що ризикують піддатися вірусній атаці – робочі станції в офісах різних організацій, об'єднані в локальні мережі.

Причини можуть бути найрізноманітнішими: висока вартість подібного програмного забезпечення, неможливість установки програм на малопотужні комп'ютери, тому що це спричинить значне зменшення швидкості роботи системи й ін.

Подібне відношення до питань безпеки нерідко стає причиною зараження комп'ютерів. І отоді встає питання лікування. Боротися з наслідками шкідливої дії вірусу, що потрапив у локальну мережу, часто буває дуже складно.

Один з найефективніших способів – використання невеликих спеціалізованих утиліт, спрямованих на виявлення й видалення певного типу вірусів, а також на відновлення ушкоджених файлів. Подібні програмні рішення мають дуже багато переваг:

- інсталяція, як правило, не потрібна;

- дистрибутив настільки невеликого розміру, що він уміщається на звичайну дискету.

Скачати ж його можна швидко, навіть використовуючи невисоку швидкість з'єднання:

- утиліти мають безкоштовний статус;

- перевірка здійснюється тільки на наявність самих популярних у цей момент вірусів, що істотно прискорює процес сканування;

- робота цих програм не вимагає великої кількості системних ресурсів.

Подібні утиліти можна назвати швидкою допомогою для зараженого комп'ютера або ж для такого, котрий підозрюється в зараженні. Випуском подібних утиліт займаються відомі антивірусні компанії, такі як Symantec, MacAfee й ін. Кілька утиліт були випущені в самій Microsoft.

У цьому невеликому огляді ми розглянемо самі актуальні на сьогоднішній день програми, здатні допомогти у вирішенні подібного роду проблем.

Почнемо з утиліт від Symantec. Отут ми розглянемо лише трохи із програм, випущених цією компанією. Повний список інструментів для видалення самих популярних вірусів, що випускають компанією Symantec, можна знайти в Інтернеті.

2.4.1 W32.Novarg@mm/W32.Mydoom@mm Fix Tool

Остання версія утиліти від компанії Symantec. Ця програма виявляє й видаляє віруси типу W32.Mydoom із зараженого комп'ютера. У процесі аналізу системи, програма видаляє самі файли, а також зміни в системному реєстрі, які були зроблені після зараження. Утиліта підтримує наступні модифікації вірусу:

W32.Mydoom.A@mm,

W32.Mydoom.B@mm,

W32.Mydoom.F@mm,

W32.Mydoom.G@mm,

W32.Mydoom.H@mm,

W32.Mydoom.L@mm,

W32.Mydoom.M@mm,

W32.Mydoom.Q@mm,

Backdoor.Zincite.A,

W32.Zindos.A,

Backdoor.Nemog,

W32.Bofra.A@mm (renamed from W32.Mydoom.AI@mm),

W32.Bofra.C@mm (renamed from W32.Mydoom.AK@mm),

W32.Bofra.D@mm (renamed from W32.Mydoom.AH@mm).

Вірус цього типу являє собою поштового хробака, що поширюється у вигляді атачмента з розширенням: .bat, .cmd, .exe, .pif, .scr і .zip. Коли комп'ютер інфікований, хробак відкриває на комп'ютері TCP порти від 3127 до 3198, що дозволяє потенційному недоброзичливцеві підключитися до комп'ютера й використати його як проксі для одержання доступу до мережених ресурсів.

2.4.2 Backdoor.Agent.B removal tool

Утиліта від Symantec для пошуку на комп'ютері вірусу Backdoor.Agent.B і його видалення. Цей вірус був виявлений наприкінці липня цього року. Після

відвідування користувачем певних сайтів вірус установлює файл.dll, що дозволяє шкідливим додаткам робити на комп'ютері різні дії.

Як і попередня утиліта, ця програма дуже проста у використанні (рис. 2.8).

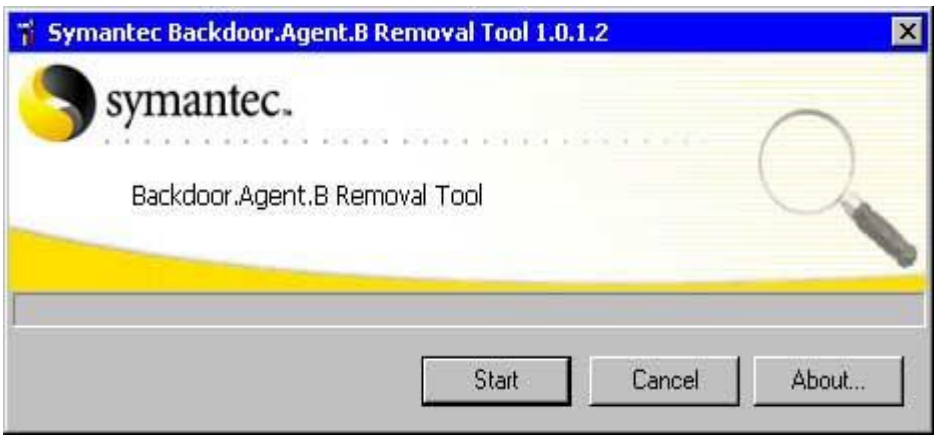

Рисунок 2.8 – Зовнішній вигляд Backdoor.Agent.B removal tool

Однак потрібно пам'ятати про те, що оскільки вірус, що вона видаляє, поширюється через інтернет і локальну мережу, перед її використанням необхідно відключити комп'ютер від всіх мереж.

2.4.3 Trojan.Vundo Removal Tool

Утиліта від Symantec для виявлення й видалення модуля Trojan.Vundo. Цей вірус був виявлений зовсім недавно.

Vundo – це компонент рекламного модуля, що закачує і відображає рекламні оголошення у вигляді pop-up вікон.

Крім закриття всіх додатків від відключення комп'ютера від Інтернету й локальної мережі, перед використанням цієї утиліти в середовищі Windows, необхідно також відключити опцію System Restore.

2.4.4 W32.Bofra@mm FixTool

Утиліта від Symantec для виявлення й видалення одного з найпоширеніших у світі на сьогоднішній день сімейства вірусів Bofra. Bofra

використає поки незакриті уразливості браузера Internet Explorer для поширення.

Bofra – це нова модифікація вірусу MyDoom. Перша інформація про виникнення цього вірусу з'явилася в перших числах листопада минулого року. Ще тоді співробітники компанії McAfee попереджали, що у вірусу є всі шанси для того, щоб стати значимим. Уже наприкінці листопада було оголошено, що по ступені поширеності Bofra посідає шосте місце у світі.

Саме через цей вірус співробітники Міністерства зв'язку Фінляндії рекомендували не використати Internet Explorer службовцям на підприємствах. Підхопити Bofra можна, просто клацнувши по посиланню у вікні браузера IE. Вірус також поширюється поштою.

W32.Bofra@mm FixTool видаляє наступні різновиди вірусу:

W32.Bofra.A@mm (renamed from W32.Mydoom.AI@mm),

W32.Bofra.B@mm (renamed from W32.Mydoom.AJ@mm),

W32.Bofra.C@mm (renamed from W32.Mydoom.AK@mm),

W32.Bofra.D@mm (renamed from W32.Mydoom.AH@mm).

2.4.5 Win32.Sobig.F@mm Removal Tool

Утиліта для видалення вірусу Win32.Sobig.F від компанії BitDefender. Даний вірус поширюється поштою. Його можна одержати в листах з темами:

"Re: That movie",

"Re: Wicked screensaver",

"Re: Your application",

"Re: Re: My details",

"Re: Thank you!".

Тіло зараженого листа звичайно виглядає так: "Please see the attached file for details".

Утиліта Win32.Sobig.F@mm Removal Tool (рис. 2.9) визначає всі відомі версії вірусу, видаляє інфіковані файли, видаляє процес із пам'яті, а також виправляє внесені вірусом зміни до реєстру Windows.

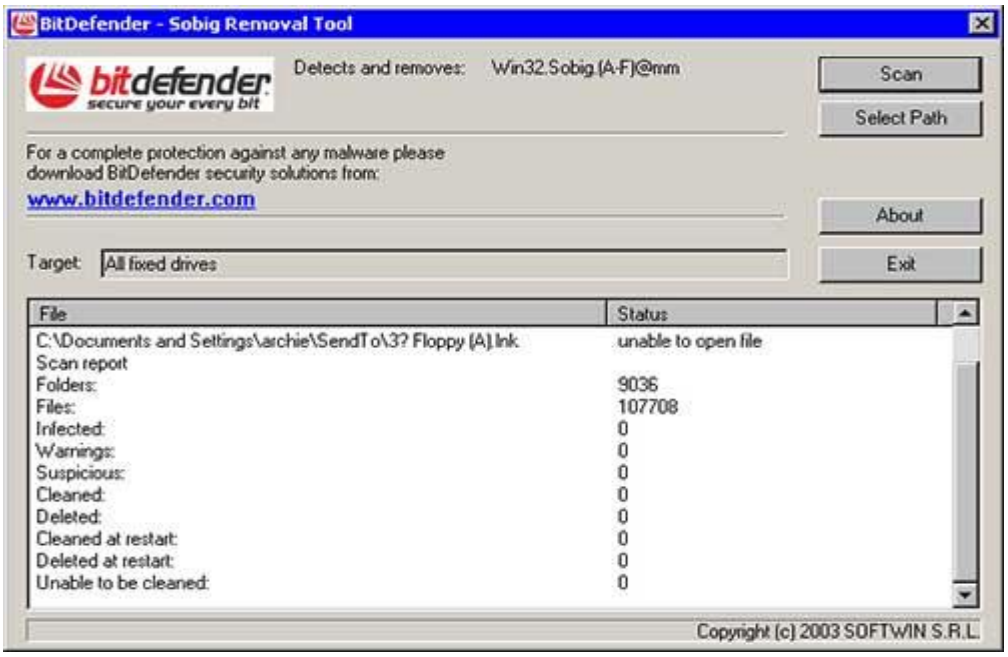

Рисунок 2.9 – Зовнішній вигляд Win32.Sobig.F@mm Removal Tool

2.4.6 McAfee AVERT Stinger

Одна із самих популярних і часто обновлюваних антивірусних утиліт, що випускає компанія McAffee. Вона допомагає відшуковувати й видаляти віруси різних типів. На даний момент у базі програми більше сорока самих популярних у Мережі шкідливих модулів. Це всі відомі варіанти таких вірусів:

BackDoor-AQJ,

BackDoor-CFB,

BackDoor-CHR,

BackDoor-JZ,

Bat/Mumu.worm,

Exploit-DcomRpc,

IPCScan,

IRC/Flood.ap,

IRC/Flood.bi,

IRC/Flood.cd,

NTServiceLoader,

PWS-Narod,

PWS-Sincom.dll,

W32/Anig.worm,

W32/Bagle@MM,

W32/Blaster.worm(Lovsan),

W32/Bugbear@MM,

W32/Deborm.worm.gen,

W32/Doomjuice.worm,

W32/Dumaru,

W32/Elkern.cav,

W32/Fizzer.gen@MM,

W32/FunLove, W32/Klez,

W32/Korgo.worm,

W32/Lirva,

W32/Lovgate,

W32/Mimail,

W32/MoFei.worm,

W32/Mumu.b.worm,

W32/MyDoom,

W32/Nachi.worm,

W32/Netsky,

W32/Nimda,

W32/Pate,

W32/Polybot,

W32/Sasser.worm,

W32/Sdbot.worm.gen,

W32/SirCam@MM,

W32/Sober,

W32/Sobig,

W32/SQLSlammer.worm,

W32/Swen@MM,

W32/Yaha@MM,

W32/Zafi,

W32/Zindos.worm.

Програма не вимагає інсталяції й дуже проста у використанні (рис. 2.10).

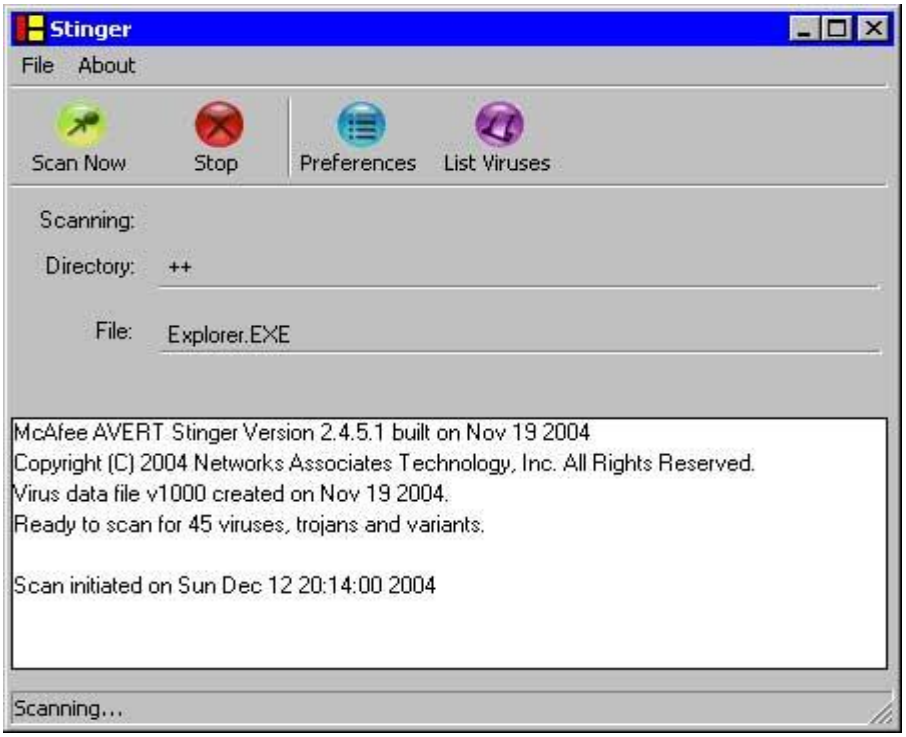

Рисунок 2.10 – Зовнішній вигляд McAfee AVERT Stinger

Її особливістю є можливість настроювання деяких параметрів за допомогою кнопки Preferences. Так, можна визначити поводження утиліти у випадку виявлення вірусу на комп'ютері, настроїти параметри сканування. Також програма може відображати в процесі сканування всі файли, які були перевірені.

Навряд для кого-небудь секретом є той факт, що комп'ютери потрібно захищати. Особливо якщо ви використовуєте сервер на базі Windows 2000 для виходу в Інтернет. Це типово для багатьох організацій. Windows 2000 набагато простіше й зручніше в настроюванні, чим різні версії Unix. А при належному настроюванні ця система не менш стійка до злому й стабільна. Втім, багато аматорів Unix можуть із цим не погодитися, але це моя думка. Звичайно до сервера Windows 2000 підключається модем виділеної лінії (або будь-який

інший пристрій), паралельно з локальною мережею. При цьому організується або роздача з'єднання з Інтернетом по локальній мережі (Internet Connection Sharing, найпростіший варіант NAT), або встановлюється проксі-сервер. Кожний із цих варіантів має свої плюси й мінуси, але з погляду гнучкості керування й обліку діяльності користувачів я предпочитаю другий. У кожному разі потрібно ясно зрозуміти – сервер прийдеться захищати. Саме дивне, що системи Windows мають багаті вбудовані можливості з захисту.

3 СИСТЕМИ І ЗАСОБИ РЕАЛІЗАЦІЇ СЕРВЕРНИХ ДОДАТКІВ

3.1 Функціонал серверної системи

Виходячи з аналізу предметної області і вимог до інформаційної системи, побудуємо функціональну схему серверної частини Інтернет-системи на об’єкті інформаційної діяльності (рис. 3.1).

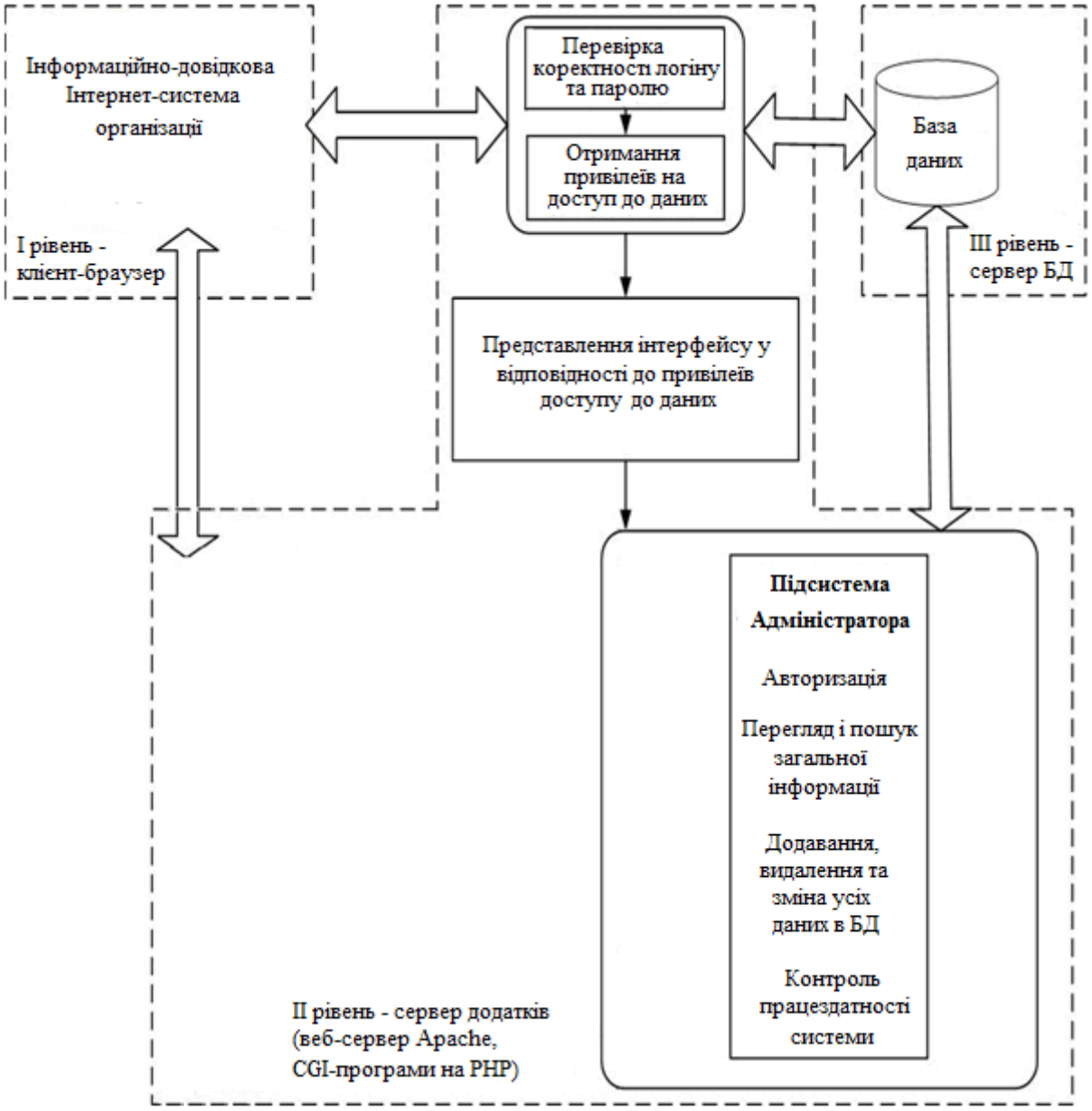

Рисунок 3.1 – Функціональна модель серверної частини системи

Як видно з рис. 3.1, при створенні серверної частини Internet-системи необхідно створити підсистему адміністратора. Для реалізації серверної

частини інформаційно-довідкової Інтернет-системи серверної частини необхідний один продуктивний хост, що підтримує базу даних, Web-сервер і технологію формування динамічних Web-сторінок для підготовки документів за результатами запитів до бази даних і відображення їх в браузерах у клієнтів. Інформаційно-довідкова система серверу повинна забезпечувати зручну роботи і можливість здійснення адміністрування серверної частини системи.

Сучасні програмні додатки та інформаційні системи досягли високого рівня розвитку і термін або поняття «архітектура» у застосуванні до них дозволяє грамотно побудувати і сконструювати інформаційну систему в цілому, забезпечуючи її ефективне і надійне функціонування.

Архітектура інформаційної системи – концепція, яка визначає модель, структуру, виконувані функції і взаємозв'язок компонентів інформаційної системи.

В процесі розвитку програмних систем все більшого значення набуває їх інтеграція один з одним з метою побудови єдиного інформаційного простору підприємства. Для того щоб побудувати правильну і надійну архітектуру і спроектувати інтеграцію програмних систем необхідно чітко слідувати сучасним стандартам в цих областях. Без цього велика ймовірність, створити архітектуру, яка нездатна задовольняти зростаючим потребам користувачів. Класифікація програмних систем за їх архітектурою представляється таким чином:

- централізована архітектура;
- архітектура «файл-сервер»;
- дворівнева архітектура «клієнт-сервер»;
- багаторівнева архітектура «клієнт-сервер»;
- архітектура розподілених систем;
- архітектура Web-додатків;
- сервіс-орієнтована архітектура.

Дана інформаційно-довідкова Інтернет-система розроблена як клієнт-серверна система. Клієнт-серверна система характеризується наявністю двох взаємодіючих самостійних процесів клієнта і сервера, які, в загальному випадку, можуть виконуватися на різних хостах, обмінюючись даними по мережі. За такою схемою можуть бути побудовані системи обробки даних на основі СУБД, поштові та інші системи.

Додаток на робочій станції виконує важливі функції – відповідає за формування інтерфейсу користувача, логічну обробку даних і за безпосереднє маніпулювання даними. Файловий сервер надає послуги тільки найнижчого рівня – відкриття, закриття і модифікацію файлів. Таким чином, безпосередньою обробкою даних займається кілька незалежних і неузгоджених між собою процесів.

Інформаційно-довідкова Інтернет-система серверу представляє собою трирівневу архітектуру, що припускає наявність наступних компонентів програми: клієнтський додаток («тонкий клієнт» або термінал) підключений до сервера додатків, який в свою чергу підключений до сервера бази даних (рис. 3.2).

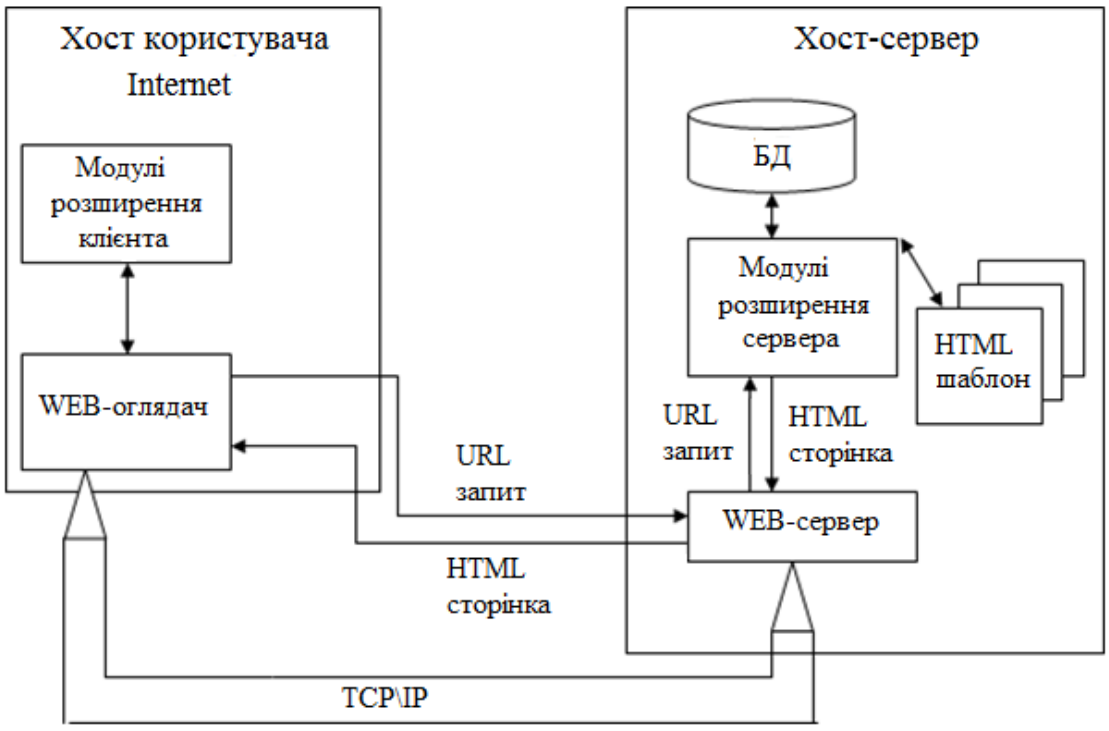

Рисунок 3.2 – Архітектура інформаційної системи сервера

Робоча станція (клієнт) призначена для безпосередньої роботи користувача або категорії користувачів і володіє ресурсами, відповідними локальним потребам даного користувача. Сервер повинен володіти ресурсами, відповідними його функціональному призначенню і потребам.

Інформаційно-довідкова Інтернет-система серверу передбачає публікацію веб-додатку в мережі Інтернет та забезпечення віддаленого доступу користувачів до інформації. Архітектура WEB-додатків публікує бази даних і включає додаткові рівні, такі як сервер бази даних, сервер додатків, джерела даних. Залежно від того, як розподіляються ланки інформаційної системи на вузлах комп'ютерної мережі, можуть бути визначені дворівневі, трирівневі або N-рівневі архітектури WEB-додатків.

Перший рівень не повинен мати прямих зв’язків з базою даних (за вимогами безпеки), бути навантаженим основною роботою (за вимогами масштабованості) і зберігати стан додатків (за вимогами надійності). На перший рівень зазвичай виноситься найпростіша схема: інтерфейс авторизації, алгоритми шифрування, перевірка введених значень на допустимість і відповідність формату, нескладні операції (сортування, угруповання, підрахунок значень) з даними, вже завантаженими на термінал. Сервер додатків розташовується на другому рівні. На другому рівні зосереджена також велика частина інформації. Поза увагою залишаються фрагменти, що експортуються на термінали, а також занурені в третій рівень збережені процедури і тригери. Сервер бази даних забезпечує зберігання даних і виноситься до третього рівню. Зазвичай це стандартна реляційна або об'єктно-орієнтована СУБД. Якщо третій рівень являє собою базу даних разом з збереженими процедурами, тригерами і схемою, яка описує додаток в термінах реляційної моделі, то другий рівень будується програмний інтерфейс, що зв'язує клієнтські компоненти з прикладної логікою бази даних. У спрощеній конфігурації фізично сервер додатків може бути поєднаний з сервером бази даних на одному комп'ютері, до якого по мережі підключається один або декілька терміналів.

Дана інформаційно-пошукова система розроблена з використанням сервера Apache. Завдяки тому, що сервер Apache має ряд переваг, а саме: є програмою з відкритим вихідним кодом, безкоштовно розповсюджуваний в Internet. Програмісти постійно додають в сервер нові функціональні можливості, створюючи модулі, які працюють з кодом ядра Apache, з використанням Apache API. Назва Apache виходить з його природи – «a patchy Web Server» (Web-сервер, що виправляється). Переваги, простота протоколу HTTP і взаємодія «сервер/клієнт». У модулях активно використовується Apache API, істотно спрощуючи базові операції. Єдина складність в розумінні фаз обробки – з'ясування того, коли Apache використовує команди з компонентних функцій модуля. Основні переваги Web-сервера Apache:

- для установки Web-сервера Apache досить мати персональний комп'ютер, що працює під управлінням однієї з популярних операційних систем Windows;

- безкоштовно розповсюджуваний програмний продукт, легко конфігурувати;

- Apache дозволяє встановити для роботи інтерпретатори Perl і PHP;

- веб-сервер Apache надає мінімальні вимоги до системи: швидкодія комп'ютера, обсяг оперативної і дискової пам'яті і так ін.

Так само, однією з переваг цього сервера є той факт, що адміністратору додатків не потрібно налаштовувати глобальний файл конфігурації сервера для забезпечення локальних налаштувань, а достатньо лише створити свій локальний файл конфігурації .htaccess. Багато розробників модифікують код Apache, вносячи додаткові функції, і пропонують для вільного розповсюдження свої розробки. Зокрема, є версії Apache, в які додані функції для роботи з документами з урахуванням різних кодувань кирилиці. Будучи безкоштовною відкритої програмою, призначеної для безкоштовних Unix-систем (FreeBSD, Linux і ін.), Apache за функціональними можливостями і надійності не поступається комерційним серверам, а широкі

можливості конфігурації дозволяють налаштувати його для роботи практично з будь-якої конкретною системою.

Відповідно до технології WWW, сервер протоколу HTTP Apache, працюючий, як правило, по 80-му порту стека протоколів TCP/IP, приймає запити від користувача за допомогою клієнтських програм перегляду гіпертекстових документів. Формалізований доступ до даних в рамках інформаційної системи здійснюється на основі HTML-форм. З їх допомогою введені в поля форми дані передаються на сервер Apache, який викликає зазначену у формі PHP-програму для обробки цих параметрів і передає їй управління. PHP-скрипт за допомогою функцій прикладного інтерфейсу перетворює дані в SQL-запит, встановлює з'єднання з сервером СУБД і передає йому запит на виконання. Сервер СУБД виконує запит, звертаючись до бази даних, і повертає результат PHP-скрипту, який, в свою чергу формує динамічний HTML-документ і через сервер Apache передає його клієнту.

3.2 Скриптова мова програмування PHP

В даний час однієї з найпопулярніших сценарних мов в Web є PHP. PHP (PHP: Hypertext Preprocessor – гіпертекстовий препроцесор), була створена для генерації HTML-сторінок на стороні Web-сервера. PHP є одною з найпоширеніших мов, що використовуються у сфері Web-розробок разом з Java, Perl, Python. PHP підтримується переважною більшістю хостинг-провайдерів. Проект, за якими був створений PHP – проект з відкритими програмними кодами.

PHP інтерпретується Web-сервером в HTML-код, який передається на сторону клієнта. На відміну від таких мов програмування, як JavaScript, користувач не має доступу до PHP-коду, що є перевагою з точки зору безпеки, але значно погіршує інтерактивність сторінок. Але ніщо не забороняє використовувати PHP для генерування та JavaScript-кодів, які виконаються вже на стороні клієнта.

Для реалізації інформаційно-довідкової системи серверу була обрана об'єктно-орієнтована мова PHP. PHP – мова, яка вбудована безпосередньо в html-код сторінок, які, в свою чергу будуть коректно оброблені PHP-інтерпретатором. Механізм PHP просто починає виконувати код після першої екрануючої послідовності (<?) і продовжує виконання до того моменту, коли він зустріне парну послідовність (?>). Велика розмаїтість функцій PHP дають можливість уникнути написання багаторядкових призначених для користувача функцій на C або Pascal. Перевагами мови PHP є:

- наявність інтерфейсів до багатьох баз даних. У PHP вбудовані бібліотеки для роботи з MySQL, PostgreSQL, mSQL, Oracle, dbm, Hyperware, Informix, InterBase, Sybase;

- через стандарт відкритого інтерфейсу зв'язку з базами даних (Open Database Connectivity Standard – ODBC) можна підключатися до всіх баз даних, в яких існує драйвер;

- традиційність.

Ефективність є винятково важливим фактором при програмуванні для багатокористувацьких середовищ, до яких належить і Web-середовище. Дуже важлива перевага PHP полягає в його трансльованому інтерпретаторі. Такий пристрій дозволяє обробляти сценарії з достатньо високою швидкістю. За деякими оцінками, більшість PHP-сценаріїв обробляються швидше за аналогічні їм програми, написані на Perl. Продуктивність PHP цілком достатня для створення цілком серйозних Web-додатків.

З точки зору типізації, PHP є мовою програмування з динамічною типізацією. Немає необхідності явного визначення типу змінних, хоча така можливість існує. У разі звернення до змінної, ядро PHP трактує її тип відповідно до контексту. При необхідності можливе приведення змінної певного типу за допомогою відповідних конструкцій мови. Це може знадобитися, якщо врахувати, що значення змінної можуть трактуватись по різному залежно від її типу.

PHP постійно вдосконалюється, працює на UNIX та Windows платформах, допускає роботу з більшістю СУБД, має широкий набір функцій, допускає об'єктно-орієнтоване програмування, здатний використовувати протоколи: HTTP, FTP, SNMP, NNTP, POPS. Дозволяє працювати з файлами графіки. Можна також запускати PHP-скрипти, які інтерпретуються файли і компілювати виконувані додатки.

Для побудови програмних комплексів, можливо, використовувати модульний підхід, виконуючи розділення різнорідного коду. При необхідності, можливе виконання підключення необхідних модулів, причому операція виконання може бути і умовною.

Протокол HTTP, засобами якого, як правило, обмінюються інформацією клієнт і Web-сервер не надає можливість зберегти стан сеансу взаємодії. Це випливає з того, що між клієнтом і сервером не встановлюється постійне з'єднання, і клієнт не надає жодних відомостей, які можуть виділити його серед інших активних. Альтернативою cookies є концепція сесій, яка знайшла свою реалізацію в PHP. У сесії можна зберігати різні дані, включаючи об'єкти.

3.3 Управління базами даних на сервері

Для розробки інформаційно-довідкової Інтернет-системи серверу публікують базу даних в Інтернет, тому доцільно використовувати СУБД середнього масштабу і продуктивності. На сьогоднішній день СУБД MySQL є однією з найвідоміших, безкоштовних, надійних і швидких з усього сімейства існуючих СУБД.

MySQL написаний під десятки видів операційних систем. Це iFreeBSD, OpenBSD, MacOS, OS/2, SunOS, Windows, Unix, Linux. Сьогодні MySQL особливо поширена на платформах Linux і Windows, причому на останній зустрічається набагато рідше.

Принцип роботи СУБД MySQL аналогічний принципу роботи будь СУБД, що використовує SQL (Structured Query Language, мова

структурованих запитів), як командну мову для створення/видалення баз даних, таблиць, для поповнення таблиць даними, для здійснення вибірки даних.

MySQL, як і будь-яка інша СУБД являє собою програму-сервер, яка знаходиться в пам'яті комп'ютера і обслуговує TCP порт. А клієнтська програма, будь то CGI-додаток на Perl або програмний продукт на C, з'єднується з СУБД з цього порту і посилає йому рядки на SQL. Той у свою чергу їх інтерпретує, виконуючи необхідні дії, і відсилає результати запиту назад клієнтові. Таким способом відбувається спілкування сервера баз даних з клієнтськими програмами.

Для запуску MySQL-сервера необхідно виконати файл mysqld.exe. Сервер запускається як, без віконний фоновий процес. При цьому він залишається в пам'яті і обробляє запити від клієнтських додатків. Для зупинки сервера слід виконати команду mysqladmin – u root shutdown. Якщо сервер не був зупинений коректно, то при наступному запуску у файлі mysql.err буде додано запис про збої. Коректна зупинка сервера необхідна для збереження всіх даних, які знаходяться в кешах MySQL.

MySQL має розвинену систему доступу до баз даних. Користувачеві бази даних може бути наданий доступ до всієї бази даних, окремих таблиць і окремих стовпців таблиць. Є розмежування на дії, які може виробляти користувач із записами. Для організації такої, складною структури доступу використовується декілька таблиць в системній базі даних. На підставі значень цих таблиць налаштовується політика надання доступу. Схема обробки запитів СУБД MySQL наведена на рис. 3.3.

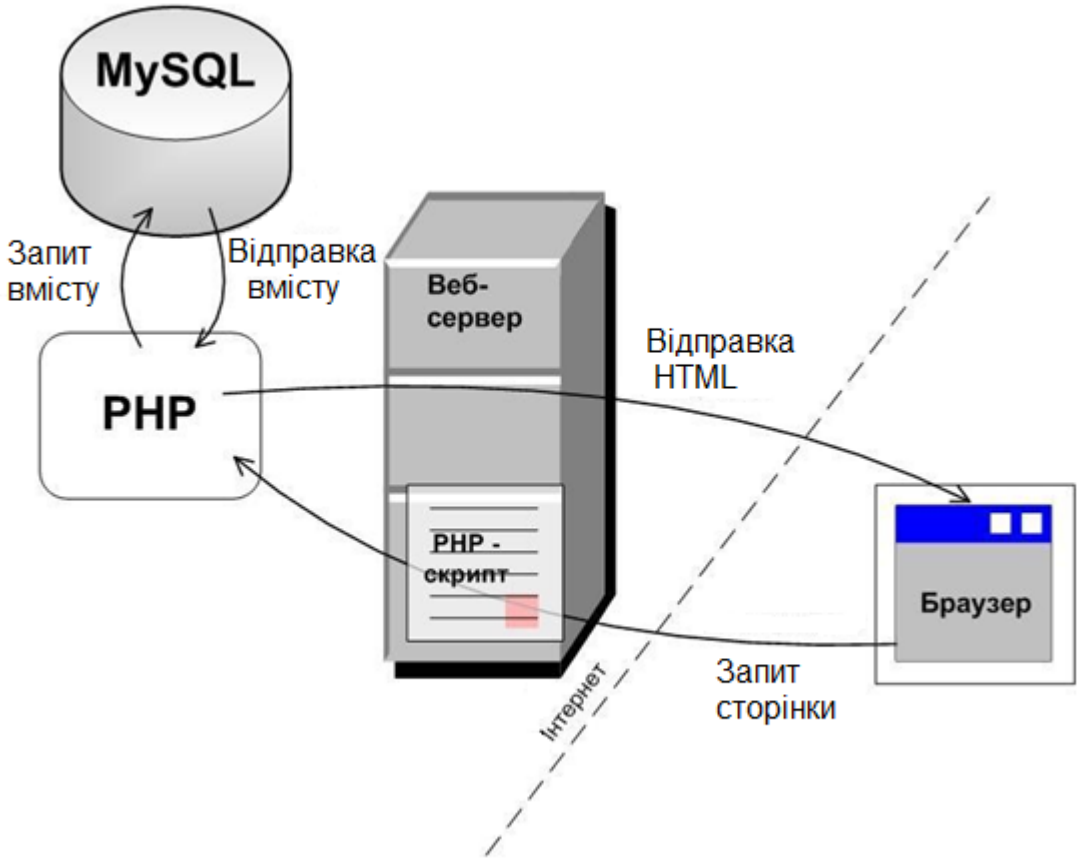

Рисунок 3.3 – Схема обробки запитів СУБД MySQL

База даних, яку сервер MySQL використовує для зберігання внутрішньою інформації про користувачів, за замовчуванням має ім'я mysql. У цій базі даних певні таблиці для зберігання інформації користувача облікових записів.

Підсистема для Користувача-Адміністратора, який виконує функції управління даними предметної області та даними зареєстрованих користувачів, здійснює контроль працездатності всієї Internet-системи і її безпеки в цілому.

ВИСНОВКИ

В даній роботі розглянута та приділена особлива увага інформаційній безпеці в мережі за допомогою апаратного та програмного забезпечення.

У цій роботі було розглянуто систему захисту віддаленого хосту у мережі за допомогою програмного забезпечення та раціональної побудові топології мережі. Для цього створена мережа на підприємстві, що складається з сервера та віддалених хостів.

В рамках дипломної роботи мною розроблена система захисту інформації у системі, що забезпечила комплексний захист даних на всіх рівнях. Система складається з комплексу заходів та засобів захисту інформації: аутентифікації, авторизації, засобів перевірки даних, що працюють в середині мережі, захисту даних локальних користувачів та сервера, захисту каналу передачі даних.

Розроблена система захисту інформації:

1) Забезпечує захист створеної мережі (сервера та користувачів мережі).

2) Відповідає принципам забезпечення безпеки інформації системах та мережах.

3) Захищає інтереси користувачів і співробітників підприємства.

4) Дозволяє запобігти можливих збитків від атак на компоненти і ресурси системи.

Цією роботою я показав, що захист мережі можливий не тільки дорогими технічними засобами (маршрутизатори, комутатори, „залізні” файєрволи та інше) але й доступними засобами, такими як Outpost firewall, та антивірусами.

ПЕРЕЛІК ПОСИЛАНЬ

1. Detection of Anomalous Computer Session Activity [Електронний ресурс]. – 1989. – Режим доступу до ресурсу: http://people.scs.carleton.ca/~soma/id-2007w/readings/vaccaro-wisdom+sense.pdf.

2. Detecting Intruders in Computer Systems [Електронний ресурс]. – 1993. – Режим доступу до ресурсу: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.43.7289.

3. Береза А.М. Основи створення інформаційних систем [навч. посіб.]. – К.: КНЕУ, 1998. – 140 с.

4. Харрингтон Д. Проектирование реляционных баз данных. – М.: Лори, 2004. – 241 с.

5. Коннолли Т., Бегг К., Страчан А. Базы данных: проектирование, реализация и сопровождение. Теория и практика [учеб. пособ.]. – М.: «Вильямс», 2000. – 761 с.

6. Дунаев В. Сценарии для Web-сайта. PHP и JavaScript. – М.: БХВ-Петербург, 2008. – 576 с.

7. Веллинг Л., Томсон Л. Разработка веб-приложений с помощью PHP и MySQL. – М.: Вильямс, 2010.– 848 с.

8. Computer Security Threat Monitoring and Surveillance [Електронний ресурс]. – 1980. – Режим доступу до ресурсу: https://csrc.nist.gov/csrc/media/publications/conferencepaper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cspapers/ande80.pdf.

9. An Intrusion Detection Model [Електронний ресурс]. – 1986. – Режим доступу до ресурсу: https://www.academia.edu/8674514/An_Intrusion-Detection_Model.

10. Бенкен Е. PHP, MySQL, XML. Программирование для Интернета. – СПб.: БХВ-Петербург, 2007.– 336 с.

11. Хольцнер С. PHP в примерах. – М.: «Бином-Пресс», 2007. – 352 с.