КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)
Інформаційних технологій проєктування та прикладної математики
(назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «МАГІСТР»

на тему:
Розробка інформаційної системи захисту мережі
з використанням мережевих екранів

ХАСАНОВ ШАМІЛЬ
(прізвище, ім’я та по батькові студента повністю)

Київ 2025

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)
Інформаційних технологій проєктування та прикладної математики
(назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри

д.т.н., проф. Бородавка Є.В.

„___” _____2025 року

ПОЯСНЮВАЛЬНА ЗАПИСКА
ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «МАГІСТР»

Розробка інформаційної системи захисту мережі
з використанням мережевих екранів
(назва)

Виконав студент групи ІСТм-24

126 «Інформаційні системи та технології»
(спеціальність)
Хасанов Шаміль
(прізвище, ім’я та по батькові повністю)

Керівник Івахненко І.С.
(прізвище та ініціали)
професор, доктор економічних наук
(вчене звання, науковий ступінь)

Київ 2025

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: автоматизації і інформаційних технологій

Кафедра: інформаційних технологій проєктування та ПМ

Освітній рівень: «магістр за ОПП/ОНП»

Спеціальність: 126 «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ

Завідувач кафедри

д.т.н., проф. Бородавка Є.В.

„___”_____2025 року

З А В Д А Н Н Я
ДО ВИКОНАННЯ ЕВАЛІФІКАЦІЙНОЇ РОБОТИ
НА ЗДОБУТТЯ ОСВІТНЬОГО РІВНЯ «МАГІСТР»

Хасанов Шаміль

(прізвище, ім’я та по батькові студента)

1. Тема роботи: Розробка інформаційної системи захисту мережі з використанням мережевих екранів

затверджена наказом ректора КНУБА № 1619/23/25 від «29»09 2025 року

2. Керівник роботи Терентьєв О.О.

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

3. Строк подання студентом роботи до захисту 10.12.25 р.

4. Зміст пояснювальної записки за розділами:

Р. 1. ОСНОВНІ ТЕОРЕТИЧНІ І МЕТОДОЛОГІЧНІ ПОЛОЖЕННЯ. КОНЦЕПЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Р. 2. СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

Р. 3. БРАНДМАУЕР ЯК ІНСТРУМЕНТ УПРАВЛІННЯ МЕРЕЖЕВОЮ БЕЗПЕКОЮ

Р. 4. ВИБІР БРАНДМАУЕРА

Р. 5. ОПИС ТА ОБГРУНТУВАННЯ ОБРАНОЇ СИСТЕМИ ЗАХИСТУ

5. Графічний матеріал за розділами

Р. 1.6 рисунків

Р. 2. 6 рисунків

Р. 3. 5 рисунків

Р. 4. 13 рисунків

Р. 5. 3 рисунки

7. Календарний план виконання роботи: а) наукова частина; б) практична частина.

Види робіт та їх зміст	Дата виконання
Розділ 1. ОСНОВНІ ТЕОРЕТИЧНІ І МЕТОДОЛОГІЧНІ ПОЛОЖЕННЯ. КОНЦЕПЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	Жовтень 2025 р.
Розділ 2. СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ	Жовтень 2025 р.
Розділ 3. БРАНДМАУЕР ЯК ІНСТРУМЕНТ УПРАВЛІННЯ МЕРЕЖЕВОЮ БЕЗПЕКОЮ	Листопад 2025 р.
Розділ 4. ВИБІР БРАНДМАУЕРА	Листопад 2025 р.
Розділ 5. ОПИС ТА ОБГРУНТУВАННЯ ОБРАНОЇ СИСТЕМИ ЗАХИСТУ	Грудень 2025 р.
Остаточне оформлення роботи	Грудень 2025 р.
Направлення роботи на рецензування, перевірку на плагіат	Грудень 2025 р.
Попередній захист роботи на кафедрі	Грудень 2025 р.

8. Консультанти розділів атестаційної випускної роботи

Розділ	Прізвище, ініціали та посада консультанта	Перевірив	
		дата	підпис
Прийом програмного продукту	к.т.н. доц. Шабала Є.Є.		

9. Дата видачі завдання 22 вересня 2025 р.

Керівник _____ Івахненко І.С.
(підпис) (прізвище та ініціали)

Студент _____ Хасанов Шаміль
(підпис) (прізвище та ініціали)

РЕЗЮМЕ

Кваліфікаційна робота на здобуття освітнього рівня магістра складається зі вступу, п’яти розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 97 сторінки, має 33 рисунки, 1 таблицю в основному тексті. Список використаних джерел містить 29 найменувань і займає 6 сторінок.

Метою роботи є дослідження сучасних систем захисту мережі з використанням мережевих екранів.

У роботі проведено огляд сучасних та технологій захисту мереж та методів впливу зловмисників на них. Проаналізувано та систематизовано одержані результати; досліджено доцільність виконання кожного із розглянутих методів захисту захисту за конкретних умов; представлено результати дослідження у вигляді зручному для кінцевого користувача.

Актуальність – сьогодні повсюдне використання персональних комп'ютерів, на жаль, з появою програм, що самовідтворюються, віруси заважають нормальній роботі комп'ютера, руйнують файлову структуру диска, а також знищують інформацію, що зберігається на комп'ютері.

Все більше ЗМІ повідомляють про різноманітні піратські витівки комп’ютерних хуліганів, з’являються все складніші програми для самовідтворення. Хоча багато країн прийняли закони проти кіберзлочинності та розробили спеціальне програмне забезпечення для захисту від вірусів, кількість нових програмних вірусів все ще зростає. Це вимагає від користувачів персональних комп’ютерів розуміння природи вірусів, способів зараження та запобігання вірусам.

Практичне значення – реалізація запропонованого проекту дасть змогу користувачам обрати оптимальний спосіб захисту мережі в залежності від рівня секретності інформації.

Ключові слова: Мережеві екрани, мережа, файервол, брандмауер, захист.

RESUME

The attestation final work for the master's degree consists of an introduction, five sections, general conclusions, a list of used sources, the total volume of the work is 100 pages, has 33 figures, 1 table in the main text. The list of used sources contains 59 names and occupies 6 pages.

The aim of the work is to study modern network security systems using network screens.

The review of modern and technologies of network protection and methods of influence of malefactors on them is carried out in the work. The obtained results are analyzed and systematized; the expediency of performing each of the considered methods is investigated protection protection under specific conditions; the results of the study are presented in a form convenient for the end user.

Relevance - Today, the widespread use of personal computers, unfortunately, with the advent of self-replicating programs, viruses interfere with the normal operation of the computer, destroy the file structure of the disk, as well as destroy information stored on the computer.

More and more media are reporting various pirates of computer hooligans, and more and more complex programs for self-reproduction are appearing. Although many countries have passed anti-cybercrime laws and developed special software to protect against viruses, the number of new software viruses is still growing. This requires personal computer users to understand the nature of viruses, how to infect them, and how to prevent them.

Practical significance - the implementation of the proposed project will allow users to choose the best way to protect the network depending on the level of information secrecy.

Keywords: Firewalls, network, firewall, firewall, protection.

ЗМІСТ

ВСТУП

Актуальність дослідження. Захист інформації в комп'ютерних системах - складові успіху. Прогрес подарував людству безліч досягнень, але той же прогрес породив і масу проблем. Людський розум, вирішуючи одні проблеми, неодмінно стикається при цьому з іншими, новими, і цей процес приречений на нескінченність у своїй послідовності. Хоча, якщо вже бути точним, нові проблеми - це лише оновлена форма старих. Вічна проблема – захист інформації. На різних етапах свого розвитку людство вирішувало цю проблему з властивою даної епохи характерністю. Винахід комп'ютера та подальший бурхливий розвиток інформаційних технологій у другій половині 20 століття зробили проблему захисту інформації настільки актуальною та гострою, наскільки актуальною є сьогодні інформатизація для всього суспільства. Головна тенденція, що характеризує розвиток сучасних інформаційних технологій – зростання числа комп'ютерних злочинів та пов'язаних з ними розкрадань конфіденційної та іншої інформації, а також матеріальних втрат. За результатами одного дослідження, присвяченого питанням комп'ютерних злочинів, близько 58% опитаних постраждали від комп'ютерних зламів за останні 12 місяців. Приблизно 18% опитаних із цього числа заявляють, що втратили понад мільйон доларів під час нападів, понад 66 відсотків зазнали збитків у розмірі 50 тис. доларів. Понад 22% атак були націлені на промислові секрети або документи, що представляють інтерес передусім конкурентам. Сьогодні, напевно, ніхто не зможе з упевненістю назвати точну цифру сумарних втрат від комп'ютерних злочинів, пов'язаних із несанкціонованим доступом до інформації. Це пояснюється, перш за все, небажанням постраждалих компаній оприлюднити інформацію про свої втрати, а також тим, що не завжди втрати від розкрадання інформації можна оцінити в грошовому еквіваленті. Причин активізації комп'ютерних злочинів та пов'язаних з ними фінансових втрат досить багато, суттєвими з них є: перехід від традиційної «паперової» технології зберігання та передачі відомостей на електронну та недостатній при цьому розвиток технології

захисту інформації в таких технологіях; об'єднання обчислювальних систем, створення глобальних мереж та розширення доступу до інформаційних ресурсів; збільшення складності програмних засобів та пов'язане з цим зменшення числа їх надійності та збільшенням уразливостей.

Сьогодні повсюдне використання персональних комп'ютерів, на жаль, з появою програм, що самовідтворюються, віруси заважають нормальній роботі комп'ютера, руйнують файлову структуру диска, а також знищують інформацію, що зберігається на комп'ютері.

Все більше ЗМІ повідомляють про різноманітні піратські витівки комп’ютерних хуліганів, з’являються все складніші програми для самовідтворення. Хоча багато країн прийняли закони проти кіберзлочинності та розробили спеціальне програмне забезпечення для захисту від вірусів, кількість нових програмних вірусів все ще зростає. Це вимагає від користувачів персональних комп’ютерів розуміння природи вірусів, способів зараження та запобігання вірусам.

Метою роботи є дослідження сучасних систем захисту мережі з використанням мережевих екранів. **Завданнями** дослідження є:

1. Виконати огляд сучасних та технологій захисту мереж та методів впливу зловмисників на них. Проаналізувати та систематизувати одержані результати.

2. Дослідити доцільність виконання кожного із розглянутих методів захисту захисту за конкретних умов.

3. Представити результати дослідження у вигляді зручному для кінцевого користувача.

Об’єкт дослідження - безпека мереж.

Предмет дослідження - сучасні системи захисту мережі з використанням мережевих екранів.

Наукова новизна:

- Виконано дослідження і аналіз найновіших методів та засобів захисту інформації в мережах.

- Наведено ряд найбільш поширених засобів викрадення інформації з корпоративних мереж і запропоновано найбільш відповідні методи запобігання цьому.
- Результати досліджень узагальнено, систематизовано і подано у зручному вигляді для вибору користувачем оптимального способу захисту мережі в залежності від рівня секретності інформації.

РОЗДІЛ 1
ОСНОВНІ ТЕОРЕТИЧНІ І МЕТОДОЛОГІЧНІ ПОЛОЖЕННЯ. КОНЦЕПЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Можна сказати, що в нашій країні інформаційна безпека стала частиною корпоративної мережі, і є великі сумніви. Необхідність забезпечення надійної інформаційної безпеки визнають лише великі компанії, але донедавна вони усвідомлювали проблему лише з технічної сторони, яка могла захистити інформацію лише шляхом встановлення програмного забезпечення, такого як антивірусне програмне забезпечення, брандмауери, програми моніторингу та виявлення мережі. Вторгнення, несанкціонований доступ і віртуальні частини мережі. Згідно з рекомендаціями дослідницької компанії, основним напрямом безпеки має бути формування політики безпеки та відповідних документів. Стратегія безпеки є найдешевшим і найефективнішим засобом забезпечення інформаційної безпеки. Крім того, якщо політика сформульована, то це ще й керівництво для розвитку та вдосконалення системи безпеки[8].

Згідно з рекомендаціями дослідницької компанії, основним напрямом безпеки має бути формування політики безпеки та відповідних документів. Стратегія безпеки є найдешевшим і найефективнішим засобом забезпечення інформаційної безпеки. Крім того, якщо політика сформульована, то це ще й керівництво для розвитку та вдосконалення системи безпеки.

1.1 Загальні положення концепції інформаційної безпеки

Основною метою концепції є визначення методів і засобів захисту та безпеки інформації, що відповідають потребам України у використанні ресурсів глобальної мережі загальнодоступних даних для побудови корпоративних мереж безпеки та безпеки в сучасних умовах.

Ця концепція поєднує сучасну тенденцію розвитку мережевих інформаційних технологій, розвиток типів мережевих протоколів та їх взаємної інкапсуляції та спільного використання, а також формулює науково-технічні

принципи побудови системи захисту інформаційних ресурсів мережі підприємства.

Основними тенденціями розвитку сучасних комунікаційних мереж є глобалізація, комплексність та інтеграція. Інтеграція мережевих і комунікаційних технологій включає спільне використання та інтеграцію різних мережевих протоколів, спільне використання ресурсів постачальника зв'язку та засобів передачі даних, а також підключення послуг передачі та обслуговування.

Складність мережевих технологій пов'язана з розробкою нових функціональних протоколів зв'язку та передачі інформації, що забезпечують кращий і надійніший зв'язок і збільшення кількості та швидкості передачі інформації. Наприклад, з метою підвищення безпеки передачі інформації розроблено протокол IPSEC, який включено в нову версію протоколу IPv6[35].

Тенденція глобалізації визначається поєднанням і спільним використанням інформаційних ресурсів, розташованих у віддалених районах і країнах. Ці три основні тенденції розвитку мережевих інформаційних технологій привели до четвертої і вирішальної тенденції: «Ефективно та гнучко керуйте безпекою, а також захищайте передану та оброблену інформацію за допомогою централізованого розподілу».

Без взаємної довіри та інформаційної безпеки між провайдерами зв'язку неможливо здійснити ефективну інтеграцію. Інакше інтеграція призведе до економічної та моральної втрати однієї сторони та руйнування мережевої організації.

Комунікаційні технології стають дедалі складнішими, загрози інформаційної безпеки безмежно зростають, а інформаційні ресурси корпоративної мережі не мають кваліфікованої та гарантованої системи безпеки, що призводить до руйнування функцій мережі.

Глобалізація передбачає різке збільшення кількості інтерактивних об’єктів, що використовуються для обміну інформацією, що за відсутності контрольованої системи захисту інформації гарантує зворотний ефект – надає

несанкціонований доступ і перетворює цінну інформацію споживача на непотрібну інформацію[18].

1.2 Визначення корпоративної мережі. Особливості корпоративних мереж

Корпоративна мережа - набір взаємопов'язаних мереж, служб передачі даних і телекомунікаційних послуг, призначених для забезпечення єдиного безпечного кіберпростору, обмеженого компанією.

Основні особливості корпоративної мережі[5]:

1. Використовуйте ті ж інструменти, що й при використанні загальнодоступних мереж передачі даних.

2. Надавати доступ до інформації лише обмеженій групі клієнтів у внутрішній мережі організації. Внутрішня мережа — це локальна мережа, відокремлена від глобальної мережі брандмауером.

3. Розповсюдження інформації поділяється на три види: офіційні (формально дозволені та заохочуються на рівні організації), проектні або групові (для використання окремою групою співробітників, як правило, захищені) та неформальні (особисті) папки на сервері. або Каталог, Репозиторій послуг), нотатками та ідеями можна ділитися з іншими співробітниками компанії для взаємної вигоди, для обміну думками або в інших цілях.

4. Наявність централізованої системи управління (ефективністю, безпекою, живучістю) корпоративної мережі.

Існуюча система автоматизації підприємства має такі характеристики:

1. Компанія приймає модель розподілених обчислень. Однак за останні 5-10 років технологія тонкого клієнта стає все більш популярною в країні та за кордоном.

2. Програма підприємства невіддільна від функціональної одиниці підприємства і знаходиться на клієнтській станції як частина програмного коду.

3. Необхідно одночасно керувати кількома локальними мережами та обмінюватися інформацією між центральною консоллю та платформою керування.

4. Різні методи представлення, зберігання та передачі інформації.

5. Інтегрувати дані, що належать різним організаціям і використовуються для різних цілей, в одну базу даних. І розмістити необхідні дані для певних тем у віддаленому вузлі мережі (наприклад, текстовий звіт, що зберігається на робочій станції).

6. Абстрагувати власника даних від фізичної структури та розташування даних.

7. Брати участь в автоматизованому процесі обробки інформації для великої кількості різних типів користувачів і персоналу. Прямий і одночасний доступ до ресурсів (у тому числі інформації) великої кількості користувачів (відвідувачів) різних категорій.

8. Висока різноманітність комп'ютерних технологій і засобів зв'язку та програмного забезпечення.

9. Функціональному апаратному забезпеченню в системі відсутня спеціальна програмна та апаратна підтримка засобів захисту.

1.3 Класифікаційні ознаки корпоративних мереж

Відповідно до введеного визначення мережі компанії, її загальний склад складається з таких функціональних елементів:

Робоче місце (абонент) компанії може бути:

-Зосереджені або розташовані в будівлі;

-Розповсюджені або розкидані в деяких загалом не обмежених зонах[17].

Інформаційний сервер компанії призначений для зберігання та обробки інформаційних масивів (баз даних) різного функціонального призначення. Вони також можуть бути зосереджені або розподілені на великих ділянках компанії.

Телекомунікаційні засоби, що забезпечують взаємодію між робочими станціями та взаємодію з інформаційним сервером. Внутрішній телекомунікаційний метод компанії може бути:

-Виділ (або оренда), що належить підприємству;

-Загального призначення (існує поза мережею комунікацій компанії, а її кошти використовуються підприємством). Це кошти з існуючих публічних мереж.

Усередині компанії інформаційний вплив може бути реалізовано в межах однієї (телефон, телетекст, відеотекст, телекс), або кілька послуг (інтеграція сервісів) повинні надаватися через відповідні телекомунікаційні та користувацькі термінали[48].

Система управління продуктивністю мережі підприємства. Відповідно до набору послуг, реалізованого в корпоративній мережі, ви повинні використовувати власні засоби управління мережею, включаючи маршрутизацію та комутацію; засоби керування, реалізовані для ефективного використання мережевих ресурсів. Якщо можливо, управління мережевими елементами компанії можна виділити:

-Функціональні елементи, керовані всередині компанії (це власні або додаткові засоби, введені в мережу компанії);

-Чи керують функціональними елементами (особливо маршрутизаторами та комутаторами), які є частиною загальної підмережі, яку використовує компанія.

Система управління безпекою мережі підприємства. Необхідні служби безпеки мережі повинні бути реалізовані в корпоративній мережі, і відповідно до цього повинні використовуватися засоби безпеки.

Система надійності корпоративної мережі. Слід передбачити заходи для забезпечення працездатності всієї мережі або її фрагментів у разі відмови елемента мережі.

Система діагностики та контролю. У мережі компанії повинні бути передбачені засоби моніторингу роботи окремого функціонального елемента, система збору несправностей та інформації про несправності, а також система виживання, управління продуктивністю та управління безпекою. Необхідно розробити інструменти діагностики для корпоративної мережі та впроваджувати її на превентивній основі під час роботи мережі[20].

Операційна система. Крім цих функціональних елементів, мережа комунікацій підприємства також повинна мати план процесу розвитку (гіпотезу), який значною мірою визначає внутрішні функції, особливо з точки зору рівня протоколу взаємодії компонентів мережі та можливості інтеграції.

Узагальнюючи вступні характеристики мереж підприємства, отримуємо можливу класифікацію:

- по набору функціональних елементів (рис. 1.1);
- по ієрархії управління (рис. 1.2); тут під локальною підсистемою розуміється деяка функціональна підсистема, класифікація яких для системи управління безпекою наведена на рисунку 1.3, і де сама функціональна підсистема наведена на рисунку 1.4;
- по набору (типом і кількістю) об'єднуються в рамках корпоративної мережі підмереж загального користування;
- по набору (типом і кількістю) реалізуються в рамках корпоративної мережі телеслужби.

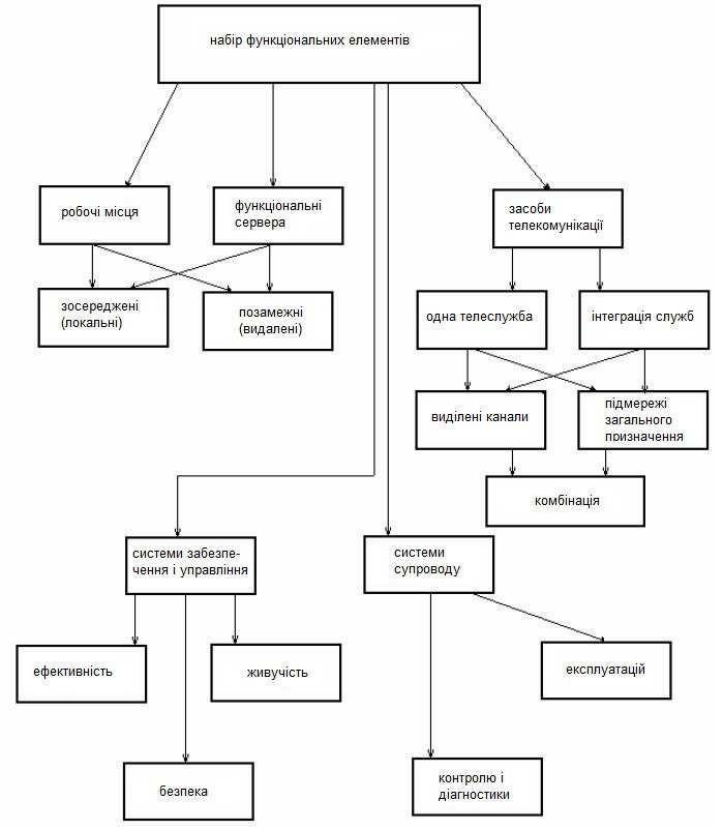

Рис. 1.1. Функціональні компоненти корпоративних мереж

Рис. 1.2. Класифікація по ієрархії управління

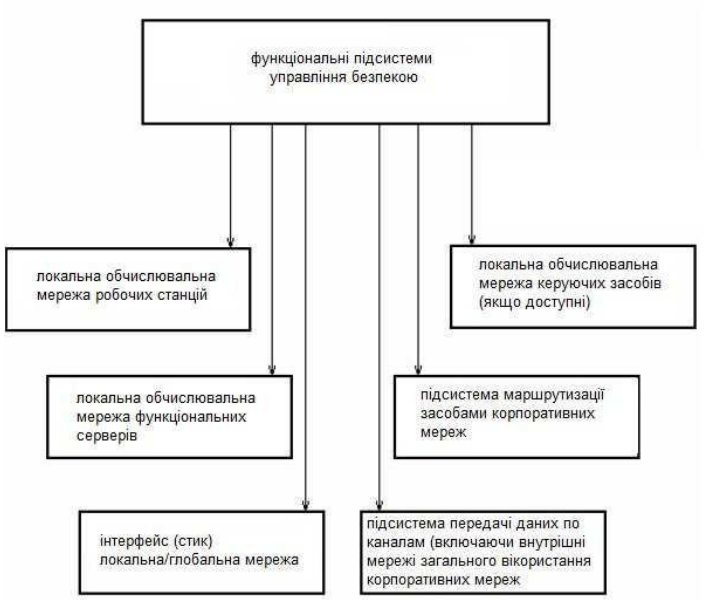

Рис.1.3 Класифікація функціональних підсистем управління безпекою

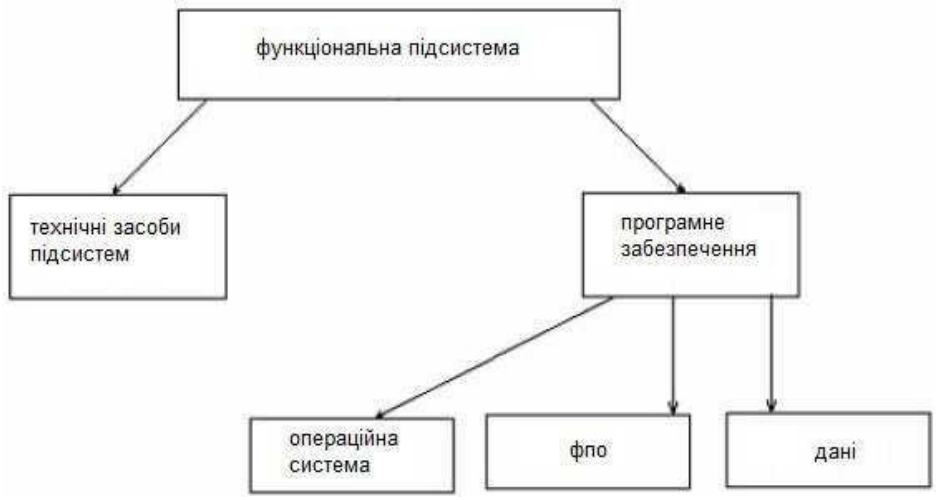

Рис. 1.4. Елементи функціональної підсистеми

1.4 Узагальнена структура корпоративної мережі. Загальні вимоги до адміністрування мережі

З урахуванням введених класифікаційних ознак можна отримати деяку узагальнену структуру мережі підприємства, як показано на рисунку 1.5. Фактично будь-яка корпоративна мережа буде містити фрагменти вищезгаданої загальної структури. У цій мережі повинна бути реалізована допоміжна мережа зв'язку - система управління, показана на рисунку 1.6. Тут також можна використовувати виділені канали (пунктирні лінії на рисунку 1.5 позначають функціональні з'єднання – фізичні канали маршрутизуються, захищені тощо (рис. 1.6)). Система управління мережею підприємства повинна дотримуватися таких принципів[60]:

- Об'єднання управління кожною функціональною підсистемою (питання ефективності не можна вирішити без урахування проблем живучості мережі, а питання безпеки не можна вирішити без врахування проблем ефективності та живучості) (іншими словами, при зміні рівня безпеки, наприклад, розглянути зміни та ефективність);

-Централізоване/розподілене управління, припускаючи, що основні завдання управління повинні вирішуватися з центру (основної частини мережі), другорядні завдання (наприклад, у віддаленому фреймворку) означає управління кожною підсистемою;

- У системі керування має бути реалізована функція автоматичної системи керування. Для підвищення ефективності реагування системи управління на особливо важливі події в системі слід реалізувати автоматичну обробку особливо важливих ефектів;

-Усередині системи безпеки адаптивне управління безпекою має бути реалізовано шляхом відповідної зміни пов'язаних подій (наприклад, система виявлення атак може заблокувати локальний порт, коли відбувається тип атаки). «Відмова в обслуговуванні»).

-З метою підвищення ефективності та надійності системи управління необхідно передбачити експертну систему-систему «нагадування» для розвитку контрольного ефекту різних подій.

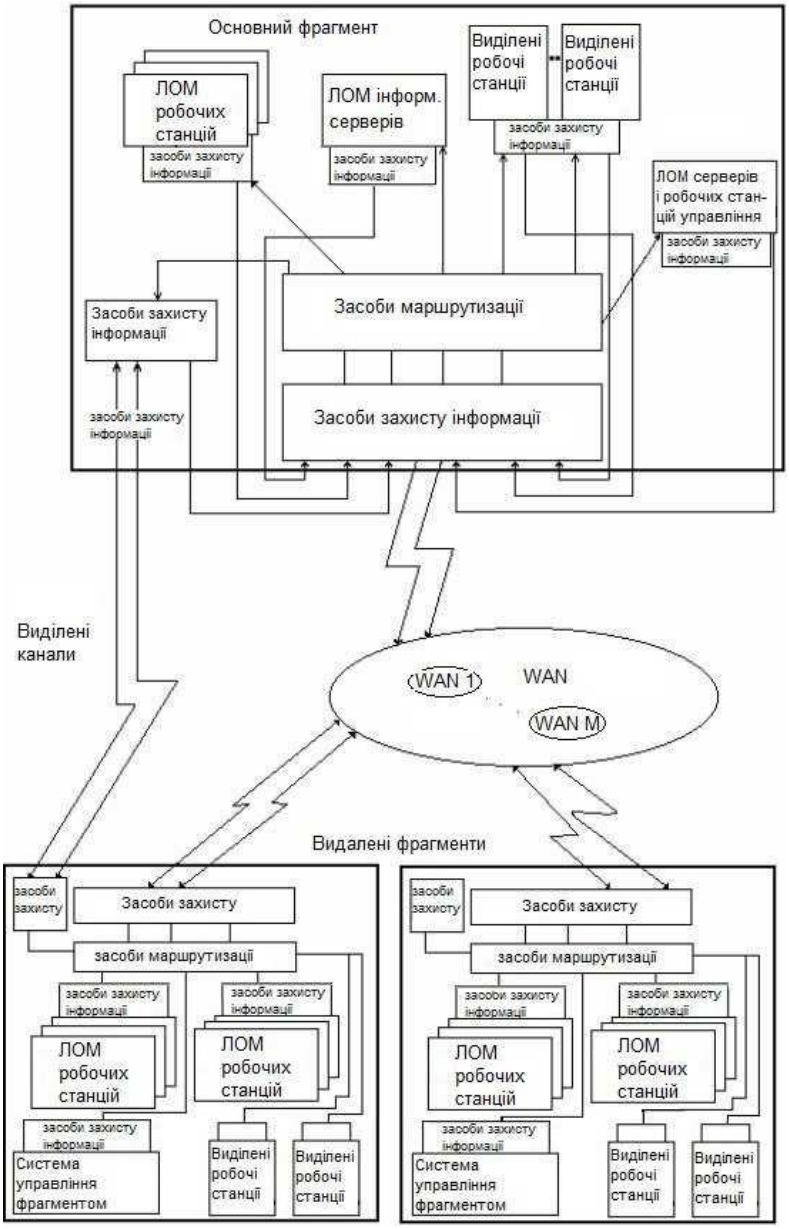

Рис. 1.5. Узагальнена структура корпоративної мережі

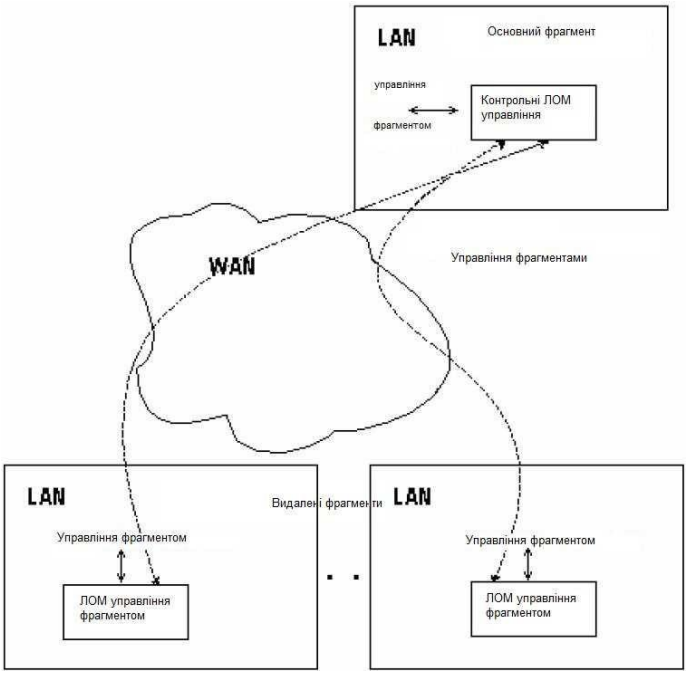

Рис. 1.6. Система управління корпоративною мережею

Рисунок 1.5 ілюструє загальну ситуацію, відмінність полягає в тому, що структура основного фрагмента і віддаленого фрагмента однакові (їх функції різні – основний фрагмент реалізує централізоване управління мережею зв’язку). Як правило, ці фрагменти мають різну складність. Слід зазначити, що спрощення структури мережі полягає в тому, щоб зменшити складність віддалених шардів і передати пов'язані функції елементам основного шарда (за його складністю)[1].

Спочатку це відбувається на наступних елементах:

-Інформаційні сервери (з точки зору безпеки мережі, має сенс централізувати всі інформаційні сервери та забезпечити їм необхідний захист за допомогою організаційно-технічних заходів);

-Управління всіма функціональними підсистемами мережі компанії з використанням обмеженої кількості додаткових інструментів для реалізації функціональних підсистем (наприклад, маршрутизаторів) можна зосередити в основному сегменті;

-Підключитися до загальнодоступної служби (Інтернет) з вибраної робочої станції основного сегмента (тут використовуються відповідні засоби захисту, і загалом підключення до глобальної мережі відрізняється від інших мереж).

1.5 Структура управління безпекою мережі. Основні вимоги

Система інформаційної безпеки повинна мати багаторівневу структуру, що включає такі рівні:

-Рівень захисту автоматизованого робочого місця (АРМ);

-Рівень захисту локальної мережі та інформаційного сервера;

-Рівень захисту корпоративних речників[33].

На рівні захисту автоматизованих робочих станцій слід виконувати ідентифікацію та аутентифікацію користувачів операційної системи. Управління доступом має здійснюватися: відповідно до матриці доступу, продуктивності реєстрації та всіх операційних записів суб'єкта доступу в журналі реєстрації суб'єкту надається доступ до об'єкта. Цілісність програмного середовища повинна забезпечувати регулярне тестування засобів захисту інформації. Такий захист повинен мати гнучкі засоби налаштування та можливості віддаленого керування.

Рівень захисту локальної мережі та мережевого сервера повинен забезпечувати:

-Ідентифікувати користувачів і встановити справжність систем і компонентів доступу;

-Захист даних аутентифікації;

-Встановити автентичність при зверненні до сервера;

-Передавати інформацію автентифікації від одного компонента до іншого без повторного встановлення автентичності доступу.

Механізм безпеки повинен мати можливість створювати, підтримувати (підтримувати) та запобігати модифікації або несанкціонованому доступу або знищенню інформації аутентифікації та об'єктів доступу до матриці.

Необхідно зареєструвати такі події:

-Використання механізмів ідентифікації та аутентифікації;

- Операції користувача над ключовими об'єктами;

- знищити предмети;

-Дії, вжиті системними операторами та адміністраторами та/або персоналом охорони;

Інші випадки безпеки.

Параметри реєстрації:

-Дата та час проведення заходу;

-Користувач;

- Тип корпусу;

-Успішні або невдалі додаткові спроби ідентифікації/аутентифікації;

-Джерело запиту (наприклад, локальна або мережева аутентифікація);

У разі знищення об'єкта та передачі інформації за місцем розташування адреса користувача, назва об'єкта.

Системний адміністратор повинен мати можливість вибірково керувати операціями будь-якого користувача або групи користувачів на основі особистих даних[51].

Інструменти інформаційної безпеки повинні мати модульну структуру, і кожен модуль повинен підтримувати область пам'яті для власної реалізації. Для кожного модуля системи інформаційної безпеки кожен компонент системи інформаційної безпеки поділяється на автоматизовану систему, при цьому має бути забезпечена ізоляція ресурсів, які потребують захисту, щоб на нього поширювалися вимоги контролю доступу та аудиту.

Регулярно перевіряйте правильність роботи апаратних, мікропрограмних і програмних систем інформаційної безпеки.

При відокремленні системи інформаційної безпеки необхідно забезпечити сповіщення керівного персоналу про збої, помилки та спроби несанкціонованого доступу, виявлені в окремих компонентах системи інформаційної безпеки. Протокол, реалізований в системі інформаційної безпеки, повинен бути розроблений таким чином, щоб забезпечити нормальну роботу у разі відмови (збою) мережі зв'язку або різних її компонентів.

Запобіжний механізм повинен бути перевірений і експлуатований відповідно до вимог документа. Рівень захисту системи автоматизації підприємства повинен забезпечувати[18]:

1. Цілісність інформації, що передається від джерела до одержувача:

- перевірити;

-Почесність у сфері спілкування;

-Неможливо відкинути той факт, що партнер по спілкуванню передає або отримує повідомлення.

2. Ненадання послуг:

Безперервність роботи;

- Протидіяти атакам відмови в обслуговуванні;

- Безпечний протокол передачі даних.

3. Запобігти несанкціонованому розголошенню інформації:

-Зберігати конфіденційність даних за допомогою механізмів шифрування;

- Вибір шляху передачі. Засоби захисту повинні забезпечувати:

-Конфіденційність вмісту (відправник повинен переконатися, що ніхто, крім конкретного одержувача, не прочитає повідомлення);

- Цілісність вмісту (одержувач повинен переконатися, що зміст повідомлення не було змінено);

- Цілісність послідовності повідомлень (одержувач повинен переконатися, що послідовність повідомлень не змінилася);

-Перевірка ідентичності джерела повідомлення (відправник повинен мати можливість аутентифікувати одержувача як джерела повідомлення та будь-який пристрій, через який вони проходять);

-Підтвердження доставки (відправник може переконатися, що повідомлення буде доставлено бажаному одержувачу в цілісності);

-Підтвердження подання (відправник може перевірити ідентичність пристрою, який використовувався для відправлення повідомлення);

-Помилка джерела (дозволяє відправнику довести одержувачу, що передане повідомлення належить йому);

-Помилка прийому (дозволяє відправнику повідомлення отримати повідомлення від пристрою, який надіслав повідомлення, щоб підтвердити, що повідомлення було отримане пристроєм і доставлено конкретному одержувачу);

-Помилка доставки (дозволяє відправнику отримати підтвердження отримання пошти від одержувача);

-Контроль контролю доступу (дозволяє двом компонентам системи обробки повідомлень встановлювати захищене з'єднання);

-Не допускати спроб розширити свої юридичні повноваження (доступ, формування, розповсюдження тощо), а також змінити (несанкціоновані) повноваження інших користувачів;

- Запобігайте модифікації програмного забезпечення шляхом додавання нових функцій.

1.6 Аналіз рівня захищеності корпоративної інформаційної системи. Поняття захищеності АС

При створенні інформаційної інфраструктури системи автоматизації підприємства (АС) на базі сучасних комп'ютерних мереж неминуче виникає проблема захисту інфраструктури від загроз інформаційної безпеки. А саме: наскільки адекватний механізм безпеки, запроваджений Африканським Союзом проти існуючих ризиків; чи можна довіряти цьому АС обробляти (зберігати та передавати) конфіденційну інформацію; чи містить поточна конфігурація АС помилки, які дозволяють потенційним зловмисникам обійти контроль доступу механізм; AU Чи містить програмне забезпечення, встановлене в AU, уразливості, які можна використовувати для захисту від злому; як оцінити рівень безпеки AU та як визначити, чи він достатній у цьому операційному середовищі; які контрзаходи дійсно підвищать рівень безпеки АС; якого типу оцінки безпеки слід дотримуватися Стандарт, який вид індексу безпеки слід використовувати[63].

Ці питання рано чи пізно піднімуть експерти з усіх IT-відділів, відділів інформаційної безпеки та інших підрозділів, відповідальних за функціонування

та обслуговування АС. Відповіді на ці питання далеко не очевидні. Проаналізувати безпеку АС від загроз інформаційної безпеки непросто. Вміння оцінювати та керувати ризиками, знання типових загроз і вразливостей, стандартів і методів аналізу безпеки, володіння методами аналізу та професійними інструментами, знання різноманітних програмно-апаратних платформ, що використовуються в сучасних комп'ютерних мережах – це не професійно. Повний перелік якостей, мають бути експерти, які керують роботою з аналізу безпеки АС. Аналіз безпеки є основним елементом наскрізних видів робіт, таких як сертифікація АС, аудит та інспекція безпеки.

Безпека є одним із найважливіших показників для вимірювання ефективності АС, а також таких показників, як надійність, відмовостійкість та продуктивність. Під безпекою АС ми розуміємо адекватність загрозам інформаційної безпеки механізму її реалізації [1]. Загрози інформаційній безпеці традиційно розуміли як можливість порушення конфіденційності, цілісності та доступності інформації.

На практиці завжди є багато неточних можливих оцінок можливих шляхів реалізації загроз безпеки ресурсам АС. В ідеалі кожен шлях загрози має бути заблокований відповідним механізмом захисту. Ця умова є першим фактором, який визначає безпеку колонок. Другим фактором є міцність існуючих механізмів захисту, які характеризуються стійкістю до спроб ухилитися або подолати їх. Третій фактор – це ступінь пошкодження власника АС, якщо загроза безпеки буде успішно реалізована[4].

На практиці отримати точне значення цих характеристик важко, оскільки поняття загрози, руйнування та опору механізму захисту важко виразити. Наприклад, оцінка збитків, завданих несанкціонованим доступом до політичної та військової інформації, взагалі не може бути визначена, а визначення можливості загрози не може базуватися на статистичному аналізі. Оцінка ступеня стійкості до захисних механізмів завжди суб'єктивна.

1.7 Нормативна база аналізу захищеності

Найбільш значущими нормативними документами в галузі інформаційної безпеки, визначальними критерії для оцінки захищеності АС, і вимоги, пропоновані до механізмів захисту, є[45]:

1. Загальні критерії оцінки безпеки IT (The Common Criteria for Information Technology Security Evaluation / ISO 15408).

2. Практичні правила управління інформаційної безпекою (Code of practice for Information Security Management / ISO 17799).

Крім того, в нашій країні першорядне значення мають керівні документи "Положення про технічний захист інформації в Україні" ISO15408: Common Criteria for Information Technology Security Evaluation.

Найбільш повно критерії для оцінки механізмів безпеки програмно-технічного рівня представлені в міжнародному стандарті ISO 15408: Common Criteria for Information Technology Security Evaluation (Загальні критерії оцінки безпеки інформаційних технологій), прийнятому в 1999 році.

Загальні критерії оцінки безпеки інформаційних технологій (далі «Загальні критерії») визначають функціональні вимоги безпеки (security functional requirements) і вимоги до адекватності реалізації функцій безпеки (security assurance requirements).

При проведенні робіт з аналізу захищеності АС, а також засобів обчислювальної техніки (ЗОТ) «Загальні критерії» доцільно використовувати в якості основних критеріїв, дозволяють оцінити рівень захищеності АС (ЗОТ) з точки зору повноти реалізованих в ній функцій безпеки та надійності реалізації цих функцій.

Хоча застосовність «Загальних критеріїв» обмежується механізмами безпеки програмно-технічного рівня, в них міститься певний набір вимог до механізмів безпеки організаційного рівня і вимог з фізичного захисту, які безпосередньо пов'язані з описуваними функціями безпеки[27].

Перша частина «Загальних критеріїв» містить визначення загальних понять, концепції, опис моделі та методики проведення оцінки безпеки IT. У ній

вводиться понятний апарат, і визначаються принципи формалізації предметної області.

Вимоги до функціональності засобів захисту приводяться в другої частини «Загальних критеріїв» і можуть бути безпосередньо використані при аналізі захищеності для оцінки повноти реалізованих в АС (ЗОТ) функцій безпеки.
Третя частина «Загальних критеріїв» містить класи вимог гарантій оцінки.
Процедура аудиту безпеки АС включає в себе перевірку наявності перелічених ключових засобів контролю, оцінку повноти та правильності їх реалізації, а також аналіз їх адекватності ризикам, існуючим в даному середовищі функціонування. Складовою частиною робіт з аудиту безпеки АС також є аналіз і управління ризиками[30].

Положення про захист інформаційних технологій України:

1. У цьому Положенні визначаються закони та організаційні засади захисту інформаційних технологій, що мають важливе значення для держави, суспільства та окремих осіб та охороняються державою відповідно до закону. Технічний захист інформації спрямований на державні органи, органи місцевого самоврядування, органи управління Збройних Сил України та інші військові організації, суміжні підприємства, установи та організації, створені відповідно до законодавства України (далі - підвідомчі установи).

2. Терміни, що використовуються в цьому Положенні, мають таке значення:

-Конфіденційність - атрибути інформації для запобігання несанкціонованому доступу;

- Цілісність - атрибути інформації для запобігання несанкціонованого спотворення, знищення;

-Доступність-атрибути інформації для запобігання несанкціонованого блокування;

-Захист інформаційних технологій (ТСІ) - діяльність інженерно-технічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації;

- Інформаційна система - система автоматизації, комп'ютерна мережа або система зв'язку;

-Ліцензія - документ, що дає право здійснювати роботи із захисту інформаційних технологій відповідно до власних потреб;

- Комплекс захисту інформаційних технологій - комплекс заходів та засобів, спрямованих на реалізацію захисту інформаційних технологій в інформаційних системах або об'єктах.

3. Правовою основою захисту інформаційних технологій в Україні є Конституція України (254к/96-ВР), закони України, Акт Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Управління Національної служби спеціального зв'язку та захисту інформації України та інших державних органів, Міжнародний договір України (обов'язковість якого ратифікована Верховною Радою України) про захист інформаційних технологій та ці положення. Указ Президента № 333/2008 (333/2008) від 11 квітня 2008 року зі змінами 3 ст.

4. Національна політика щодо захисту інформаційних технологій формується відповідно до законодавства та реалізується Державним агентством спеціального зв’язку та захисту інформації України (далі – Держспеціальне агентство України) у співпраці з підпорядкованими органами ТЗІ. Відповідно до Указу Президента від 11.04.2008 р. N 333/2008 (333/2008, ст. 4 змін.)

5. Організація технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, покладається на їх керівників.

6. Організаційно-технічні принципи, порядок впровадження захисту інформаційних технологій, процедури контролю у цій сфері, характеристики інформаційних загроз, стандарти та вимоги до захисту інформаційних технологій, а також процедури сертифікації та огляду захисту інформаційних технологій визначаються нормативно-правовими актами, прийнятими відповідними органами в встановленому порядку.

Нормативно-правові акти захисту інформаційних технологій повинні впроваджуватися всіма суб'єктами системи захисту інформаційних технологій.

7. Розроблення, видання нормативно-правових актів з питань технічного захисту інформації, а також роботи, пов'язані з розробленням і виконанням загальнодержавних програм розвитку системи технічного захисту інформації, здійснюються за рахунок коштів державного бюджету та інших джерел фінансування, не заборонених законодавством.

8. Суб'єктами системи технічного захисту інформації є:

- держспецзв'язку України; {Абзац другий пункту 8 із змінами, внесеними згідно з Указом Президента N333/2008 (333/2008) від 11.04.2008} органи, щодо яких здійснюється ТЗІ;

- Науково-виробнича організація Держспецзв’язку України, державного підприємства, що підпорядковується Держспецслужбі України, виконує завдання із захисту інформаційних технологій (п. 4 ст. 8, затверджено Указом Президента України № 333/2008) (333/2008) від 11 квітня 2008 р. переглянуто)

- Військові, підприємства, установи, організації різних форм власності, громадяни-підприємці здійснюють діяльність із захисту інформаційних технологій відповідно до відповідних дозволів або ліцензій;

- Навчальні заклади, які здійснюють підготовку, перепідготовку та підвищення кваліфікації спеціалістів із захисту інформаційних технологій. {Пункт 9 виключено на підставі Указу Президента N 333/2008 (333/2008) від 11.04.2008}{Пункт 10 втратив чинність на підставі Указу Президента N 1120/2000 (1120/2000) від 06.10.2000}

11. Основними завданнями організацій, пов'язаних з ТЗІ, є:

- Забезпечити захист інформаційних технологій відповідно до вимог законів та нормативних актів про захист інформаційних технологій;
- Рішення цих питань у межах своїх повноважень;
- Моніторинг стану технічного захисту інформації.

12. Органи, щодо яких здійснюється ТЗІ, відповідно до покладених на них завдань:

- створювати або визначати підрозділи, на які покладається забезпечення захисту інформаційних технологій та контроль за їх статусом, та погоджувати основні завдання та функції цих підрозділів;

- видають за погодженням з Адміністрацією Держспецзв'язку України та впроваджують нормативно-правові акти з питань технічного захисту інформації;

- погоджують з Адміністрацією Держспецзв'язку України проведення підприємствами, установами, організаціями тих науково-дослідних, дослідно-конструкторських і дослідно-технологічних робіт, спрямованих на розвиток нормативно-правової та матеріально-технічної бази системи технічного захисту інформації, які здійснюються за рахунок коштів

- державного бюджету;

- створюють або визначають за погодженням з Адміністрацією Держспецзв'язку України підприємства, установи та організації, що забезпечують технічний захист інформації;

- Забезпечити підготовку, перепідготовку та підвищення кваліфікації персоналу захисту з інформаційних технологій;

- надають Адміністрації Держспецзв'язку України за його запитами відомості про стан технічного захисту інформації. {Пункт 12 із змінами, внесеними згідно з Указом Президента N333/2008 (333/2008) від 11.04.2008}[24]

13. Основними завданнями інших суб'єктів системи технічного захисту інформації є:

- дослідження загроз для інформації на об'єктах, функціонування яких пов'язано з інформацією, що підлягає охороні;

- створення та виробництво засобів забезпечення технічного захисту інформації;

- розроблення, впровадження, супроводження комплексів технічного захисту інформації;

- підвищення кваліфікації фахівців з технічного захисту інформації.

14. Суб'єкти системи технічного захисту інформації мають право співробітничати з підприємствами, установами, організаціями іноземних держав, які здійснюють аналогічну діяльність, на основі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, та інших актів законодавства України.

15. Матеріально-технічна база системи технічного захисту інформації складається з технічних засобів загального призначення та спеціальних технічних засобів.

Технічні засоби загального призначення повинні мати документ, що засвідчує їх відповідність вимогам нормативно-правових актів з технічного захисту інформації, одержаний у порядку, що встановлюється Адміністрацією Держспецзв'язку України і Державним комітетом України з питань технічного регулювання та споживчої політики. {Абзац другий пункту 15 із змінами, внесеними згідно з Указом Президента N 333/2008 (333/2008) від 11.04.2008} {Пункт 15 із змінами, внесеними згідно з Указом Президента N333/2008 (333/2008) від 11.04.2008}[26]

16. Техніко-економічне обгрунтування, проектування будівництва та реконструкції об'єктів, проведення наукових досліджень та створення інформаційних систем, зразків озброєнь, військової та спеціальної техніки, критичних і небезпечних технологій виконуються за завданнями, до яких включаються вимоги з технічного захисту інформації, якщо під час виконання передбачених завданням робіт та у процесі функціонування зазначених об'єктів, систем, зразків і технологій циркулюватиме інформація, охорона якої забезпечується державою.

Під час віднесення замовником таких робіт до особливо важливих та створення інформаційних систем державних органів завдання та результати приймання їх етапів погоджуються з Адміністрацією Держспецзв'язку України. Фінансування створення цих систем здійснюється після такого погодження.

Витрати на заходи з технічного захисту інформації включаються до кошторисної вартості робіт. {Пункт 16 із змінами, внесеними згідно з Указом Президента N 333/2008 (333/2008) від 11.04.2008}

17. Під час розроблення і впровадження заходів з технічного захисту інформації використовуються засоби, дозволені Адміністрацією Держспецзв'язку України для застосування та включені до відповідних переліків. {Пункт 17 із змінами, внесеними згідно з Указом Президента N 333/2008 (333/2008) від 11.04.2008}

18. Контроль у сфері технічного захисту інформації полягає в перевірці виконання вимог цього Положення, інших нормативно-правових актів з питань технічного захисту інформації та в оцінюванні захищеності інформації на об'єкті, де вона циркулюватиме або циркулює.

Оцінювання захищеності інформації здійснюється шляхом атестації або експертизи комплексів технічного захисту інформації та інспекційних перевірок. За результатами атестації або експертизи комплексів технічного захисту інформації визначається можливість введення в експлуатацію об'єкта, де циркулюватиме інформація, охорона якої забезпечується державою.

19. Порядок експертизи та інспекційних перевірок захищеності інформації визначається відповідними нормативно-правовими актами.

20. Розроблення, впровадження, атестація та експлуатація комплексів технічного захисту інформації для власних потреб здійснюються відповідними підрозділами органів, щодо яких здійснюється ТЗІ, або військовими частинами, підприємствами, установами, організаціями, на які в установленому порядку покладено забезпечення технічного захисту інформації, за наявності у них відповідного дозволу.

До виконання цих робіт можуть бути залучені суб'єкти підприємницької діяльності, що мають відповідні ліцензії.

Результати атестації на державних об'єктах, віднесених замовником до особливо важливих, погоджуються з Адміністрацією Держспецзв'язку України.

{Пункт 20 із змінами, внесеними згідно з Указом Президента N333/2008 (333/2008) від 11.04.2008}

21. Роботи з технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, здійснюються за рахунок коштів, що виділяються на їх утримання, прибутку та інших джерел, не заборонених законодавством.

Керівники зазначених органів створюють належні умови для контролю за забезпеченням технічного захисту інформації.

22. У разі порушення вимог щодо забезпечення технічного захисту інформації посадові особи та громадяни несуть відповідальність згідно із законодавством України.

1.8 Методика аналізу захищеності

В даний час не існує стандартизованого методу аналізу безпеки АС, тому за певних обставин поведінкові алгоритми аудиторів можуть сильно відрізнятися. Проте все ще можна надати типовий метод аналізу безпеки корпоративної мережі. І хоча ця методика не претендує на універсальність, її ефективність неодноразово перевірена на практиці[44].

Типові методи передбачають використання таких методів:

-Дослідити вихідні дані мовця;

-Оцінити ризики, пов'язані з реалізацією загроз безпеки ресурсам АС;

-Аналіз організаційних механізмів безпеки, організаційної політики безпеки та організаційних та адміністративних документів для забезпечення систем інформаційної безпеки та оцінки їх відповідності вимогам чинних нормативних актів та їх відповідності існуючим ризикам;

- Вручну аналізувати файли конфігурації маршрутизаторів, МЕ та проксі-серверів, які керують мережевими взаємодіями, поштових і DNS-серверів та інших ключових елементів мережевої інфраструктури;

-Сканувати зовнішню ЛОМ-адресу локальної мережі з Інтернету;

-Сканувати ресурси локальної мережі зсередини;

-Використовуйте професійне програмне забезпечення для аналізу конфігурації локальної мережі серверів і робочих станцій.

Ці методи дослідження передбачають активне та пасивне тестування із застосуванням систем захисту. Активне тестування системи захисту полягає в імітації поведінки потенційних зловмисників для подолання механізму захисту. Пасивне тестування передбачає використання контрольних списків для аналізу конфігурації операційних систем і програм за допомогою шаблонів. Перевірку можна проводити вручну або за допомогою спеціального програмного забезпечення[3].

1.9 Вихідні дані обстежуваної АС

Відповідно до вимог захисту інформаційних технологій України, при проведенні сертифікації безпеки АС, у тому числі попередньої перевірки та аналізу безпеки інформаційних об’єктів, замовник повинен надати такі вихідні дані:

1. Повна і точна назва об'єкта інформатизації та його призначення.

2. (Технологія, економіка, виробництво, фінанси, військова, політика) Характер інформації та ступінь конфіденційності (конфіденційності) обробленої інформації визначаються на основі деяких списків (країн, галузей, відомств, підприємств).

3. Організаційна структура інформаційних об'єктів.

4. Перелік місць, структура комплексу технічних засобів (основних і допоміжних), вони є частиною інформаційного об'єкта, в якому (поверх) обробляється конкретна інформація.

5. Характеристики та розташування інформованих об'єктів вказують на межі контрольної зони.

6. Структура програмного забезпечення (обсяг системи та прикладна програма), що використовується для об’єктів аутентифікації інформації та використовується для обробки захищеної інформації, та використовуваний протокол обміну інформацією.

7. Загальна функціональна схема об'єкта інформатизації, включаючи план інформаційного потоку та спосіб обробки інформації, що захищається.

8. Існування та характер взаємодії з іншими інформаційними об'єктами.

9. Склад і структура системи захисту інформації об'єктів аутентифікації інформації.

10. Перелік захищених технологій виконання та програмних засобів, засобів захисту та контролю, що використовуються для об'єктів аутентифікації інформації та з відповідними сертифікатами та інструкціями з експлуатації.

11. Інформація про розробник системи захисту інформації, статус дозволу стороннього розробника (пов'язаного з компанією, де знаходиться об'єкт автентифікації інформації).

12. Наявність служб інформаційної безпеки та послуг адміністратора (системи автоматизації, мережі, бази даних) для інформаційних об'єктів (підприємство, де розташовані інформаційні об'єкти).

13. Існування та основні характеристики фізичного захисту інформаційних об'єктів у місцях обробки захищеної інформації та зберігання носіїв інформації).

14. Наявність та підготовка проектно-експлуатаційної документації об'єкта інформатизації та вихідних даних інших об'єктів аутентифікації інформатизації, що впливають на інформаційну безпеку[23].

1.10 Аналіз конфігурації засобів захисту інформації зовнішнього периметра ЛОМ та методи тестування системи захисту

При аналізі конфігурації та управління взаємоз'єднаннями периферійних засобів захисту локальної мережі зверніть особливу увагу на наступні аспекти, які визначаються їх конфігурацією:

-Встановити правила розмежування доступу (правила фільтрації мережевих пакетів) на МЕ та маршрутизаторі;

-Схема та налаштування використовуваних параметрів аутентифікації;

-Встановити параметри системи реєстрації подій;

-Використовувати механізми для приховування топології захищеної мережі, включаючи трансляцію мережевих адрес (NAT);

-Встановити механізм повідомлення про напади та реакції;

-Наявність та ефективність методів контролю цілісності;

-Версія використовуваного програмного забезпечення та наявність встановлених пакетів відновлення програмного забезпечення.

Система захисту АС тестується для перевірки ефективності застосовуваних у ній механізмів захисту, їх стійкості до можливих атак та виявлення вразливостей у захисті. Традиційно використовуються два основних методи тестування:

- Використання методу «чорного ящика» для тестування;

- Тестування методом «білого ящика».

Тестування методом «чорного ящика» означає, що тестер не володіє особливими знаннями про конфігурацію та внутрішню структуру об’єкта тестування. У цьому випадку на випробуваного будуть проведені всі відомі типи атак, а також перевіряється стабільність системи захисту від цих атак. Використаний метод тестування моделює поведінку потенційного зловмисника, який намагається скомпрометувати систему захисту. Основним методом тестування в даному випадку є мережевий сканер з базою даних відомих уразливостей[5].

Підхід «білого ящика» передбачає складання тестової програми на основі розуміння структури та конфігурації тестового об’єкта. Під час випробування перевірте наявність та ефективність механізму безпеки, чи відповідає склад і конфігурація системи захисту вимогам безпеки та наявним ризикам. Висновок про наявність вразливостей ґрунтується на аналізі використаних заходів безпеки та конфігурації програмного забезпечення системи, а потім перевіряється на практиці. Основним інструментом аналізу в цьому випадку є програмний агент інструмента аналізу безпеки на системному рівні.

РОЗДІЛ 2
СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

2.1 Міжмережеві екрани та їх класифікація

Брандмауер (МЕ) — це локальне або функціональне розподілене програмне забезпечення (апаратне забезпечення), яке контролює інформацію, яка надходить і/або виходить із системи автоматизації. Брандмауери та брандмауери також мають загальні назви. У будівельній галузі брандмауер (нім. brand-fire, mauer-wall) — вогнетривкий бар'єр, який використовується для відокремлення блоків у багатоквартирних будинках та запобігання поширенню вогню. МЕ виконує подібні функції в комп'ютерних мережах.

За визначенням МЕ діє як контрольна точка на кордоні двох мереж. У найбільш поширеному випадку ця межа проходить між внутрішньою та зовнішньою мережами організації, як правило, Інтернет (рисунок 2.1). Однак загалом МЕ можна використовувати для опису внутрішньої підмережі корпоративної мережі організації[49].

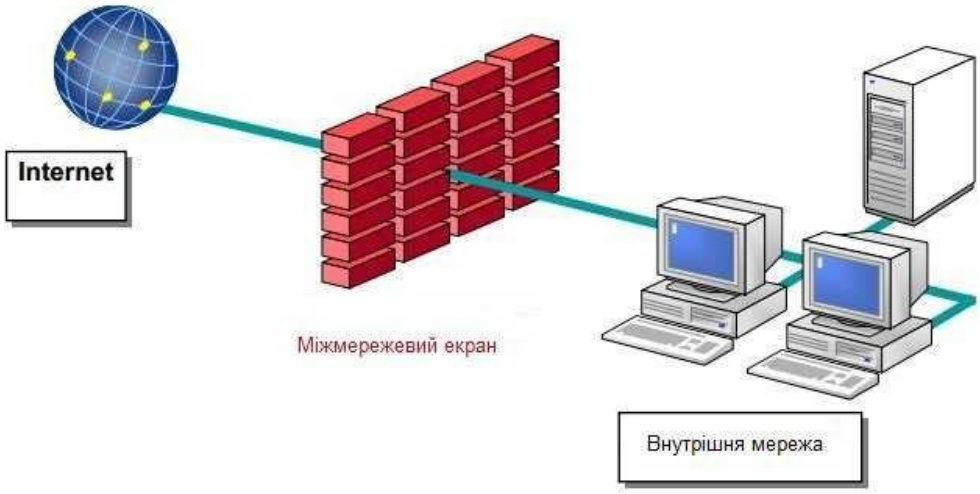

Рис. 2.1. Типове розміщення МЕ в корпоративній мереж

Завданнями МЕ як контрольної точки є:

-Контролювати весь трафік, що міститься у внутрішній мережі компанії;

-Контролювати весь трафік із внутрішньої мережі компанії.

Управління потоком інформації полягає у фільтрації та перетворенні його відповідно до набору правил. Оскільки в сучасних IU фільтрація може

виконуватися на різних рівнях відкритої системи (EMVOS, OSI) інтерактивної еталонної моделі, ІЕ зручно представити у вигляді системи фільтрації. Кожен фільтр приймає рішення на основі аналізу даних, які проходять через нього – передавати їх далі, викидати з екрану, блокувати чи трансформувати дані (рис. 2.2)[9].

Повною функцією МЕ є запис обміну інформацією. Ведення журналів дозволяє адміністраторам виявляти підозрілі операції, помилки в конфігурації МЕ та приймати рішення про зміну правил МЕ.

Рис. 2.2. Схема фільтрації в МЕ

За різними рівнями діяльності Мінприроди (OSI) класифікація МЕ виглядає наступним чином:

-Bridge екран (2 рівня OSI);

Фільтр-роутер (OSI рівня 3 і 4);

-Шлюз рівня сеансу (OSI рівень 5);

- Шлюз прикладного рівня (рівень OSI 7);

-Інтегрований екран (OSI рівень 3-7).

Мостові МЕ. Цей тип МЕ працює на рівні 2 моделі OSI і також називається прозорим (невидимим), прихованим, тіньовим МУ. Bridge МЕ з'явилися відносно пізно, що представляє собою перспективний напрямок розвитку технології брандмауера. Вони фільтрують трафік на рівні каналу, тобто МЕ використовує кадри (кадри, кадри). До переваг цього МЕ можна віднести:

-Немає необхідності змінювати налаштування корпоративної мережі та додаткової конфігурації мережевого інтерфейсу МЕ.

-Висока продуктивність. Оскільки це прості пристрої, вони не вимагають великих ресурсів. Ресурси потрібні для розширення можливостей машини або для більш глибокого аналізу даних.

- Прозорість. Ключ до цього пристрою полягає в тому, що він працює на 2 рівнях моделі OSI. Це означає, що мережевий інтерфейс не має IP-адреси. Ця функція важливіша за просте налаштування. Якщо IP-адреси немає, пристрій недоступний у мережі та не видимий для зовнішнього світу. Якщо такого ME немає, як атакувати? Зловмисник навіть не дізнається, що є ME, який перевіряє кожен їхній пакет. Схема фільтрації трафіку ME показана на рисунку 2.3[16].

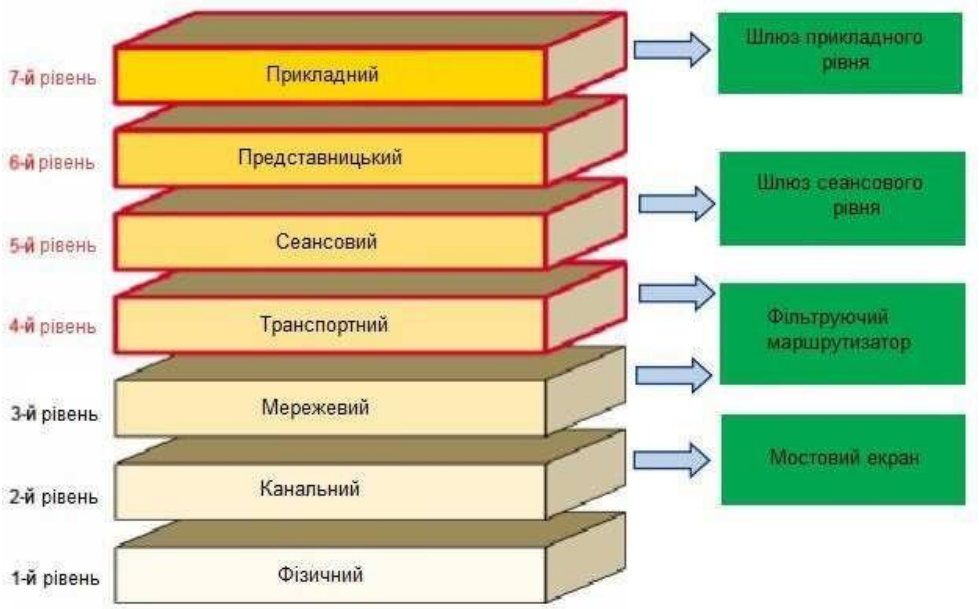

Рис. 2.3. Фільтрація трафіку ME на різних рівнях MBOS

Відфільтруйте роутер. Брандмауер для фільтрації пакетів — це маршрутизатор або комп’ютер, на якому запущено програмне забезпечення, яке налаштовано на фільтрацію певних типів вхідних та вихідних пакетів даних.

Фільтрація пакетів базується на інформації, що міститься в заголовках пакетів TCP і IP (адреси відправника і одержувача, номери їх портів тощо).

-Робота на 3 рівнях;

-Також відомий як ME на основі портів;

-Кожен пакет порівнюється зі списком правил (адреса джерела/отримання, порт джерела/отримання);

-Дешево і швидко (тому що це просто і ефективно), але найбільш небезпечно;

-Технологія 20 років тому;

-Приклад: список контролю доступу (ACL) маршрутизатор.

Шлюз на рівні сеансу. Шлюз рівня ланцюга – усуває брандмауер, який дозволяє клієнту взаємодіяти безпосередньо із зовнішнім хостом. Спочатку він приймає запити від надійних клієнтів на певні послуги, а після перевірки дійсності запитуваного сеансу встановлює з'єднання із зовнішнім хостом. Потім шлюз просто копіює пакет в обох напрямках, не фільтруючи його. На цьому рівні можна використовувати функцію трансляції мережевих адрес (NAT, трансляція мережевих адрес). Трансляція внутрішньої адреси виконується для всіх пакетів даних із внутрішньої мережі в зовнішню мережу. Для цих пакетів IP-адреса комп'ютера, який надсилає внутрішню мережу, автоматично перетворюється в одну IP-адресу, пов'язану із заблокованим ME[57].

Тому всі пакети, що залишають внутрішню мережу, відправляються в ME, тим самим усуваючи пряме з'єднання між внутрішньою і зовнішньою мережами.

IP-адреса шлюзу на рівні сеансу стає єдиною активною IP-адресою, яка входить у зовнішню мережу.

-Робота на 4 рівнях;

-Передача TCP-з'єднання на основі порту;

- Дешевше, але безпечніше, ніж пакетні фільтри;

- Зазвичай вимагають від користувачів працювати або налаштувати програму для повного запуску;

-Приклад: файрвол SOCKS.

Шлюз прикладного рівня. Шлюз прикладного рівня – усуває брандмауер, який дозволяє клієнту взаємодіяти безпосередньо із зовнішнім хостом, і фільтрує всі вхідні та вихідні пакети даних на прикладному рівні OSI. Агенти, пов'язані з програмою, пересилають інформацію, створену певними службами TCP/IP, через шлюз. Особливість:

-Розпізнавання та верифікація користувачів при спробі встановити з'єднання через МЕ;

-Фільтрація потоку повідомлень, наприклад, динамічне сканування вірусів і прозоре шифрування інформації;

-Реєстрація інцидентів та реагування на інцидент;

-Кешування даних, запитуваних із зовнішніх мереж.

На цьому рівні можуть використовуватися функції посередника (агента).

Для кожного обговорюваного протоколу прикладного рівня ви можете ввести програмний проксі-проксі HTTP, проксі FTP тощо. Кожен розповсюджувач послуг TCP/IP зосереджується на обробці повідомлень та виконанні функцій безпеки, пов’язаних із цією послугою. Як і шлюзи на рівні сеансу, шлюзи програм використовують відповідні агенти захисту для перехоплення вхідних і вихідних пакетів даних, копіювання та перенаправлення інформації через шлюз, а також діють як проміжні сервери, виключаючи прямі з’єднання між внутрішньою та зовнішньою мережами. Однак існують важливі відмінності між посередництвом, яке використовується шлюзом програми, і посередництвом каналу шлюзу на рівні сеансу. По-перше, проксі-сервери програмного шлюзу пов'язані з програмними серверами, що стосуються програми, а по-друге, вони можуть фільтрувати потік повідомлень на рівні програми моделі MBOS[4].

особливість:

-Робота на 7 рівнях;

- Специфічні для застосування;

-Ціна помірна, а швидкість повільніша, але безпечніше і дозволяє зареєстрованим користувачам;

- Для повного запуску потрібна робоча або конфігураційна програма користувача;

-Приклад: веб-проксі (http).

Експертний рівень МЕ. Брандмауер перевірки стану — це брандмауер експертного рівня, який перевіряє вміст отриманих пакетів даних на трьох рівнях

моделі OSI: мережа, сеанс і програма. При виконанні цього завдання використовується спеціальний алгоритм фільтрації пакетів, за допомогою якого кожен пакет порівнюється з відомим авторизованим шаблоном пакета.

-Триступінчаста фільтрація;

- Верифікація 4 рівня;

-5 рівнів огляду;

-Високий рівень вартості, захисту та складності;

-Приклад: брандмауер CheckPoint.

Деякі сучасні IU використовують комбінацію перерахованих вище методів і надають додаткові методи захисту мереж і систем.

«Особистий» я. Цей тип ME дозволяє додатково розширити захист, дозволяючи контролювати, які типи системних функцій або процесів можуть отримати доступ до мережевих ресурсів. Ці ME можуть використовувати різні типи підписів та умов, щоб дозволити або заборонити трафік.

Нижче наведено деякі загальні характеристики особистого ME:

-Блокування на рівні програми – лише певним програмам або бібліотекам дозволено виконувати мережеві операції або приймати вхідні з’єднання;

-Блокування на основі сигнатур

- Постійно відстежуйте мережевий трафік і блокуйте всі відомі атаки.

Через потенційно велику кількість систем, які можуть бути захищені персональними брандмауерами, додаткові елементи керування ускладнюють управління безпекою. Через неправильні налаштування це також підвищує ризик пошкодження та вразливості.

Динамічний ME.

Dynamic ME поєднує стандартні ME (перераховані вище) і методи виявлення вторгнень, щоб блокувати динамічні мережеві з’єднання, які відповідають певному сигнатурі, одночасно дозволяючи підключення до того самого порту з інших джерел. Наприклад, ви можете зупинити мережевих хробаків, не перериваючи звичайний трафік[18].

2.2 Схеми підключення МЕ

-Уніфікована схема захисту локальної мережі;

-Рішення захищене закритими підмережами, але не захищене відкритими підмережами;

-Схема роздільного захисту закритих і відкритих підмереж.

Єдина схема захисту локальної мережі

Найпростішим рішенням є брандмауер, щоб просто ізолювати локальну мережу від глобальної. У цьому випадку WWW-сервер, FTP-сервер, поштовий сервер та інші сервери також захищені брандмауером. Необхідно приділяти особливу увагу, щоб запобігти проникненню легкодоступних WWW-серверів у захищені станції локальної мережі.

Рішення захищено закритою підмережею, але не відкритою.

Щоб запобігти використанню ресурсів сервера WWW для доступу до локальної мережі, рекомендується підключатися до загальнодоступного сервера перед брандмауером. Цей метод має вищий рівень безпеки для локальної мережі, але нижчий для WWW і FTP-серверів. Схема захищена закритою підмережею і не захищена відкритою підмережею, як показано на рисунку 2.5.

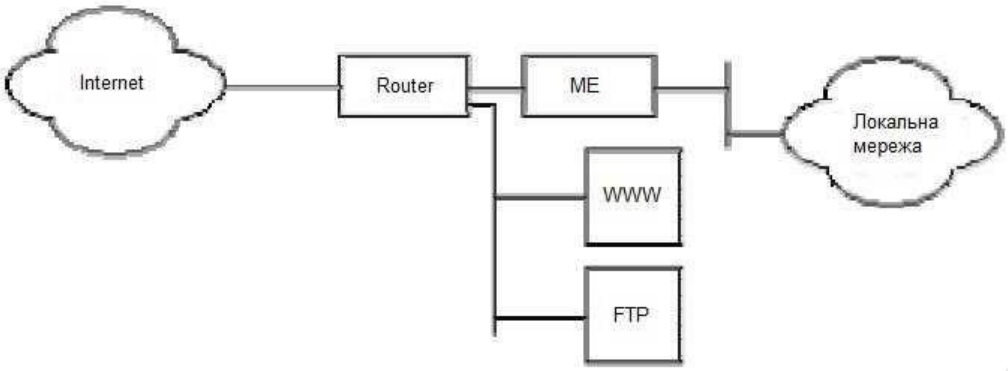

Рис. 2.5. Схема захищена закритою і не захищена відкритою підмережами

Схема роздільного захисту закритих і відкритих підмереж.

У порівнянні з розглянутими вище, ця схема підключення має найвищу безпеку. Схема заснована на використанні двох МЕ для захисту закритих і відкритих підмереж відповідно (рис. 2.6). Частина мережі між МЕ також називається екранованою підмережею або демілітаризованою зоною (DMZ)[6].

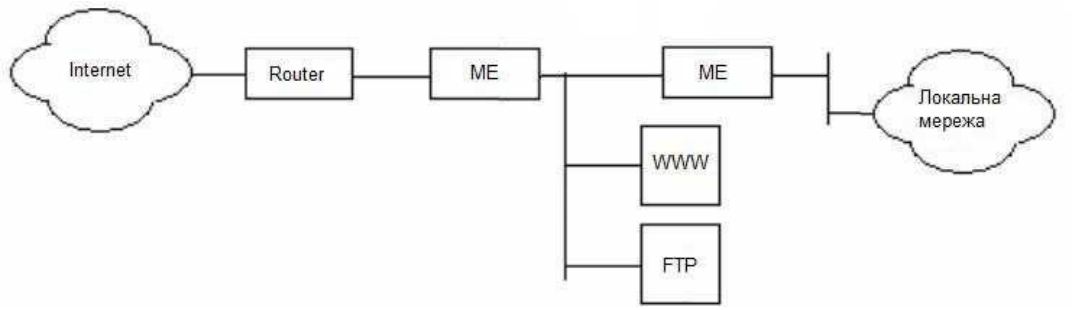

Рис. 2.6. Схема з роздільним захистом закритою і відкритою підмережею

2.3 Системи виявлення атак

На додаток до стандартного захисту неможливо уявити нормальну роботу АС (наприклад, ME, система резервного копіювання та антивірусні засоби), а також потрібен СВА (IDS, система виявлення атак або вторгнень), який є основним засобом протидії мережі напади [3].

В даний час СВА почав все більше використовуватися в корпоративній мережевій безпеці. Однак організації неминуче стикаються з багатьма проблемами при розгортанні системи виявлення атак. Ці проблеми роблять процес впровадження IDS дуже складним, а іноді навіть припиняють. Ось деякі з них[55]:

-Висока вартість комерційного СВА;

-Сучасна СВА має низьку ефективність, характеризується великою кількістю помилкових спрацьовувань і неоперацій (хибнопозитивних і хибнонегативних);

- Вимоги до ресурсів і іноді незадовільна продуктивність СВА в мережі 100 Мбіт/с;

-Недооцінювати ризики, пов'язані з кібератаками;

- Організації не вистачає методів аналізу ризиків та управління, вона не може повністю оцінити розмір ризику та виправдати витрати на впровадження управлінських контрзаходів;

- Для впровадження та розгортання СВА потрібні високоякісні експерти з виявлення атак.

Типова архітектура системи виявлення атак зазвичай включає такі компоненти:

1. Датчики (засоби збору інформації);

2. Аналізатор (інструмент аналізу інформації);

3. Інструменти реагування;

4. Контроль.

Звичайно, всі ці компоненти можна запустити на комп'ютері або навіть у програмі, але в більшості випадків вони розподілені за регіонами та функціями.

Небезпечно розміщувати компоненти СВА (такі як аналізатори та елементи керування) на ІЕ у зовнішній мережі, тому що якщо вони зламані, зловмисник може отримати доступ до інформації про внутрішню структуру мережі, яка захищена аналізом використовуваної бази правил СВА.

Типова архітектура системи виявлення атак показана на рисунку 2.7. Мережні датчики перехоплюють мережевий трафік, а хост-датчики використовуються як джерело інформації журналів подій, операційних систем, СУБД і програм. Датчик хоста також може отримувати інформацію про події безпосередньо з ядра операційної системи, IU або програми. Аналізатор, розміщений на захищеному сервері, централізовано збирає та аналізує інформацію, отриману від датчиків[2].

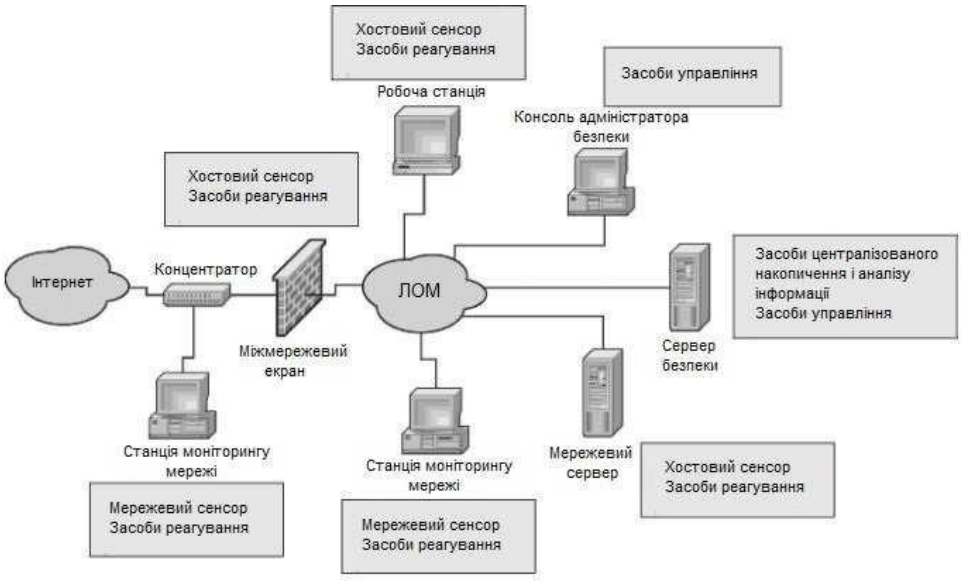

Рис. 2.7. Типова архітектура СВА

Відповідь може бути розміщена на станції моніторингу мережі, МЕ, сервері та робочій станції ЛОМ. Типовий набір дій у відповідь на атаку включає сповіщення адміністратора безпеки (через електронну пошту, консольне повідомлення або пейджер), блокування мережевих сеансів і журналів користувачів, щоб негайно припинити атаку, а також запис дій зловмисника.

Інструменти управління призначені для управління всіма компонентами системи виявлення атак, розробки алгоритмів виявлення і реагування на вразливості безпеки (політики безпеки), а також перегляду інформації про порушення та формування звітів[35].

2.4 Віртуальні приватні мережі. Функції та компоненти мережі VPN

Оскільки Інтернет, Інтранет та Екстранет широко використовуються при розробці та застосуванні розподілених інформаційних мереж і систем, одним із найактуальніших завдань є вирішення проблеми інформаційної безпеки [4].

За останні десять років завдяки швидкому розвитку Інтернету та мереж загального доступу у всьому світі відбувся якісний стрибок у поширенні та доступності інформації. Користувачі мають доступ до дешевих і доступних каналів зв'язку. Щоб заощадити гроші, компанії використовують ці канали для передачі важливої бізнес-інформації. Однак принципи побудови Інтернету відкривають перед зловмисниками можливість крадіжки або навмисного спотворення інформації. Неспроможність забезпечити належний і надійний захист для запобігання проникненню зловмисників у мережі компанії та відділів.

З метою ефективного протистояння мережевим атакам і забезпечення можливості активного і безпечного використання відкритих мереж у бізнесі зародився на початку 1990-х років і активно розвивається концепція побудови захищеної віртуальної приватної мережі-VPN (Virtual Private Networks)[38].

Захищена VPN — це поєднання локальної мережі та персонального комп’ютера через відкрите зовнішнє середовище для передачі інформації в єдину віртуальну мережу підприємства, забезпечуючи тим самим безпеку циркуляції даних.

Під час підключення корпоративної локальної мережі до відкритої мережі існує два основних типи загроз безпеки:

-Несанкціонований доступ до даних компанії під час передачі по відкритій мережі;

-Несанкціонований доступ до внутрішніх ресурсів локальної мережі компанії отримує зловмисник, який має несанкціонований доступ до мережі.

Захист інформації під час передачі по відкритих каналах зв'язку базується на таких основних функціях:

-Перевірка особистості взаємодіючої сторони;

-Шифрування переданих даних вимкнено (шифрування);

- Перевірити достовірність і повноту переданої інформації.

Характеристикою цих функцій є взаємозв’язок між собою. Їх реалізація заснована на використанні методів шифрування інформаційної безпеки[36].

Для захисту локальних обчислювальних мереж і персональних комп’ютерів від несанкціонованих операцій у зовнішньому середовищі зазвичай використовуються брандмауери, які підтримують безпеку інформаційної взаємодії шляхом фільтрації двосторонніх потоків повідомлень, виконують посередницькі функції в обміні інформацією. Брандмауер розташований на стику локальної мережі та відкритої мережі. Щоб захистити один віддалений комп’ютер, підключений до відкритої мережі, встановіть програмне забезпечення доступу до мережі на цьому ж комп’ютері. Такий брандмауер називається персональним екраном.

2.4.1 Тунелювання

Захист інформації в процесі передачі по відкритому каналу заснований на побудові захищеного віртуального каналу зв'язку, який називається зашифрованим тунелем захисту. Кожен такий тунель являє собою з'єднання, встановлене через відкриту мережу, через яку передаються зашифровані пакети повідомлень.

Створення захищеного тунелю виконується компонентами віртуальної мережі, які працюють на вузлах, що утворюють тунель. Ці компоненти називаються ініціатором і термінатором тунелю. Ініціатор тунелю інкапсулює (вбудовує) пакет даних у новий пакет даних, який разом із вихідними даними містить новий заголовок, що містить інформацію про відправника та одержувача. Хоча всі пакети даних, що передаються через тунель, є пакетами даних IP, інкапсульовані пакети даних можуть належати до будь-якого типу протоколу, включаючи пакети даних протоколів без маршрутизації, таких як NetBEUI[31].

Маршрут між ініціатором і термінатором тунелю визначається традиційною IP-мережею маршрутизації, яка може бути іншою, ніж Інтернет. Термінатор тунелю виконує процес зворотної інкапсуляції - він видаляє новий заголовок і пересилає кожен вихідний пакет до місця призначення в локальному стеку протоколів або локальній мережі.

Сама інкапсуляція не впливає на безпеку пакетів повідомлень, що передаються через тунель. Однак завдяки інкапсуляції можна виконати повний захист шифрування для інкапсульованого пакета даних. Конфіденційність інкапсульованих пакетів даних забезпечується їх криптографічним закриттям (тобто шифруванням), а також цілісністю та автентичністю (шляхом формування цифрового підпису). Оскільки існує багато способів захисту зашифрованих даних, дуже важливо, щоб ініціатор і термінатор тунелю використовували один і той же метод і могли координувати цю інформацію один з одним.

Крім того, щоб мати можливість розшифрувати дані та перевірити цифровий підпис при отриманні, ініціатор і термінатор тунелю повинні підтримувати функцію безпечного обміну ключами. Нарешті, щоб створювати тунелі лише між авторизованими користувачами, кінцеві точки взаємодії повинні бути аутентифіковані[5].

2.4.2 Класифікація VPN по робочому рівню EMBBC

Для технології безпечної передачі даних у загальнодоступній (небезпечній) мережі використовується загальний захищений іменем канал.

Системні інструменти, реалізовані на різних рівнях моделі перехресних посилань відкритої системи (EMVOS, OSI), можна використовувати для побудови безпечного каналу (табл. 2.1).

Таблиця 2.1

Рівні протоколів захищеного канала

<table>
<tr><td rowspan="7">Рівні протоколів захищеного канала</td><td>Прикладний</td><td rowspan="3">Впливають на додатки</td></tr>
<tr><td>Представницький</td></tr>
<tr><td>Сеансовий</td></tr>
<tr><td>Транспортний</td><td></td></tr>
<tr><td>Мережевий</td><td rowspan="3">Невидимі для додатків</td></tr>
<tr><td>Канальний</td></tr>
<tr><td>Фізичний</td></tr>
</table>

Функціональність реалізованої VPN та її сумісність із IP-додатками та сумісність з іншими засобами захисту значною мірою залежить від вибраного рівня OSI. За рівнем роботи моделі OSI виділяють такі групи VPN:

- VPN другого (канального) рівня;
- VPN третього (мережного) рівня;
- VPN п'ятого (сеансового) рівня.

VPN будуються на досить низьких рівнях моделі OSI. Причина цього в тому, що чим нижче в стеку реалізовані засоби захищеного каналу, тим простіше їх зробити прозорими для додатків і прикладних протоколів. Однак тут виникає інша проблема - залежність протоколу захисту від конкретної мережевої технології[17].

Якщо для захисту даних використовується протокол одного з верхніх рівнів (прикладного або представницького), то такий спосіб захисту не залежить від того, які мережі (IP або IPX, Ethernet або ATM) застосовуються для транспортування даних, що можна вважати безсумнівним гідністю. З іншого боку, додаток при цьому стає залежним від конкретного протоколу захисту, тобто для додатків подібний протокол не є прозорим.

Захищеному каналу на найвищому, прикладному рівні властивий ще один недолік це обмежена область дії. Угода захищає лише конкретні

мережеві служби - файли, гіпертекст або пошту. Наприклад, договір S/MIME захищає лише електронні листи. Тому для кожної служби необхідно розробити відповідну версію безпеки протоколу.

У верхньому рівні моделі OSI існує сильний зв'язок між використовуваним стеком протоколів і програмою.

VPN канального рівня

Інструменти VPN, що використовуються на рівні каналу моделі OSI, дозволяють інкапсуляцію різних типів трафіку третього рівня (і вищих рівнів) і побудову віртуальних тунелів, наприклад «точка-точка» (від маршрутизатора до маршрутизатора або з персонального комп'ютера на шлюз локальної мережі). Ця група включає продукти VPN, які використовують протоколи L2F (Layer 2 Forwarding) і PPTR (Point-to-Point Tunneling Protocol), а також нещодавно затверджений стандарт L2TP (Layer 2 Tunneling Protocol), спільно розроблений Cisco Systems і Microsoft[48].

Протокол безпечного каналу PPP заснований на протоколі PPP і забезпечує прозорі функції безпеки для програм і служб на прикладному рівні. Протокол PPTR може передавати пакети даних в мережі IP, а також може передавати пакети даних у мережі за допомогою протоколів IPX, DECnet або NetBEUI.

Протокол L2TP використовується для організації віддаленого доступу до локальної мережі (оскільки він в основному базується на Windows). У той же час, через недостатню масштабованість, коли потрібні кілька тунелів із загальнодоступними кінцевими точками, рішення другого рівня навряд чи матиме таке ж значення для взаємодії з локальною мережею.

VPN мережевого рівня

Продукти VPN мережевого рівня інкапсулюють IP в IP. Одним із відомих протоколів цього рівня є SKIP, який поступово замінюється новим протоколом IPSec, який призначений для аутентифікації, тунелювання та шифрування пакетів даних IP.

Мережевий протокол IPSec є компромісом. З одного боку, він прозорий

для програм, з іншого боку, він може працювати майже в усіх мережах, оскільки базується на широко використовуваному протоколі IP.

Протокол IPSec забезпечує стандартний метод ідентифікації користувача або комп'ютера під час ініціювання тунелю, стандартний метод використання шифрування кінцевої точки тунелю та стандартний метод обміну ключами шифрування та керування ними між кінцевими точками.

IPSec може працювати з L2TP, тому ці два протоколи забезпечують більш надійну ідентифікацію, стандартизоване шифрування та цілісність даних. Тунель IPSec між двома локальними мережами може підтримувати декілька окремих каналів даних, отримуючи тим самим переваги таких програм з точки зору розширення.

Говорячи про IPSec, необхідно зазначити, що протокол (IKE) дозволяє захистити передану інформацію від зовнішніх перешкод. Він вирішує проблему безпечного управління та обміну ключами шифрування між віддаленими пристроями.

VPN сеансового рівня

Деякі VPN використовують інший метод, який називається проксі-сервером. Цей метод працює на транспортному рівні і повторно передає трафік із захищеної мережі до загальнодоступного Інтернету для кожного сокета. (IP не має п'ятого рівня сеансу, але операції, орієнтовані на сокет, зазвичай називають операціями на рівні сеансу.)

Шифрування інформації, що передається між ініціатором і термінатором тунелю, зазвичай здійснюється шляхом захисту TLS транспортного рівня.
Щоб стандартизувати канал аутентифікації через брандмауер, альянс IETF визначив протокол під назвою SOCKS. Зараз для стандартизації реалізації каналу-посередника використовується SOCKS v.5.

У SOCKS версії 5 клієнтський комп'ютер використовує проксі-сервер для встановлення автентифікованого сокета (або сеансу). Цей проксі є єдиним способом зв'язку через брандмауер. Посередник виконує будь-яку операцію, яку запитує клієнт по черзі. Оскільки дилер знає трафік на рівні сокетів, він

може виконувати жорсткий контроль, наприклад блокувати певні програми користувача без необхідних дозволів[34].

2.4.3 Класифікація VPN з архітектури технічного рішення

За архітектурою технічного рішення існує три основних типи віртуальних приватних мереж:

-VPN з функцією віддаленого доступу;

-Внутрішня мережа VPN;

-VPN між підприємствами.

VPN віддаленого доступу призначений для забезпечення мобільного та/або віддаленого (домашнього офісу) співробітників компанії безпечним віддаленим доступом до інформаційних ресурсів компанії.

Внутрішньопідприємний VPN (Intranet VPN) має на меті забезпечити взаємодію безпеки між підрозділами всередині підприємства або між групою підприємств, підключених через корпоративну комунікаційну мережу (включаючи виділені лінії).

Міжпідприємний VPN (екстранет VPN) забезпечує співробітникам безпечний обмін інформацією зі стратегічними діловими партнерами, постачальниками, основними клієнтами, користувачами, клієнтами тощо.

Екстранет-VPN забезпечує прямий доступ з мережі однієї компанії до мережі іншої компанії, тим самим допомагаючи підвищити надійність зв'язку, що підтримується під час ділової співпраці. У мережах між підприємствами високо цінується контроль доступу через брандмауери та аутентифікація користувачів[57].

2.4.4 Класифікація VPN за способом технічної реалізації

За способом технічної реалізації VPN поділяється на такі категорії:

-VPN на основі мережевої операційної системи;

-VPN на основі брандмауера;

- VPN на основі маршрутизатора;

-VPN на основі програмних рішень;

-VPN на основі спеціального обладнання з вбудованим криптографічним процесором.

VPN на основі мережевої операційної системи

Візьмемо як приклад операційну систему Windows NT, розглянемо впровадження VPN на основі мережевої операційної системи. Для створення VPN Microsoft надає протокол PPTR, інтегрований у мережеву операційну систему Windows NT. Для організацій, які використовують Windows як корпоративну операційну систему, це рішення виглядає привабливим. VPN на базі Windows NT використовує клієнтську базу даних, що зберігається в первинному контролері домену (PDC).

Під час підключення до сервера PPTP користувач авторизується через протоколи PAP, CHAP або MS CHAP. Шифрування використовує нестандартний власний протокол шифрування «точка-точка», а 40-бітний ключ отримується після встановлення з'єднання.

Як перевагу цього рішення слід зазначити, що вартість рішення на базі мережевої операційної системи значно нижча, ніж вартість інших рішень.

Недосконалість цієї системи полягає в недостатній захищеності протоколу PPTP.

Маршрутизатор на основі VPN

Цей метод створення VPN передбачає використання маршрутизатора для створення безпечного каналу. Оскільки вся інформація, що надходить з локальної мережі, повинна проходити через роутер, природно покласти її та завдання шифрування на нього[61].

VPN на основі міжмережевих екранів

Брандмауери більшості виробників мають функції тунелювання та шифрування даних. До програмного забезпечення самого брандмауера додається модуль шифрування.

До недоліків цього підходу можна віднести високу вартість рішення на робочій станції та залежність від продуктивності обладнання, на якому працює

брандмауер. Використовуючи брандмауер на базі ПК, пам’ятайте, що цей параметр підходить лише для невеликих мереж з обмеженою інформацією.

Програмне забезпечення на основі VPN

Програмні рішення також використовуються для створення VPN. При реалізації таких програм використовується спеціальне програмне забезпечення, яке працює на виділеному комп’ютері і виконує в більшості випадків функцію проксі-сервера. Комп’ютери з таким програмним забезпеченням можуть перебувати за брандмауером.

VPN на основі спеціального обладнання з вбудованим криптографічним процесором

Варіант створення VPN на спеціальному обладнанні можна використовувати для мереж, які потребують високої продуктивності. Недоліком такого рішення є його висока вартість.

2.4.5 Технічні та економічні переваги впровадження технологій VPN в корпоративні мережі

Технологія VPN дозволяє ефективно вирішувати проблеми, пов'язані з обігом конфіденційної інформації в каналах зв'язку. Він забезпечує зв'язок між мережами та між віддаленими користувачами та мережами компанії через захищені канали (тунелі), «прокладені» у загальнодоступному Інтернеті.

Тому на цьому етапі, коли філії одного і того ж підприємства досить віддалені один від одного, потреба в своєчасному та надійному обміні інформацією стала найактуальнішою. Використання дорогих каналів зв'язку з високою пропускною здатністю не завжди є доцільним і економічно вигідним. Розвиток методів комунікації, особливо дешевих і найбільш легкодоступних (наприклад, Інтернет), призвів до того, що їх фактичне використання, особливо компаніями, стає все більш поширеним. У цьому випадку виникає спокуса використовувати їх для передачі цінної інформації компанії, а втрачені або спотворені збитки можуть негативно вплинути на діяльність компанії. Тому, враховуючи всі переваги безпечної VPN, використання

захищеної VPN стає все більш важливим і життєво важливим.

Концепція цього типу мережі дозволяє організувати вкрай необхідний обмін інформацією всередині компанії та з клієнтами з найкращим поєднанням продуктивності, ефективності, безпеки та вартості. Слід припустити, що такі технології, як VPN, будуть активно розвиватися, вдосконалюватися та популяризуватися[4].

РОЗДІЛ 3 БРАНДМАУЕР ЯК ІНСТРУМЕНТ УПРАВЛІННЯ МЕРЕЖЕВОЮ БЕЗПЕКОЮ

3.1 Міжмережевий екран

Міжмережевий екран або мережевий екран - це набір апаратного або програмного забезпечення, що використовується для моніторингу та фільтрації пакетів мережевих даних, що проходять через нього відповідно до заданих правил.

Основним завданням брандмауера є захист комп'ютерної мережі або окремого вузла від несанкціонованого доступу. Мережні екрани часто називають фільтрами, оскільки їх основне завдання — не пропускати (фільтрувати) пакети, які не відповідають критеріям, визначеним у конфігурації.

Деякі брандмауери також дозволяють динамічно замінювати адреси внутрішньої мережі (сірі) або порти зовнішніми адресами або портами, що використовуються поза локальною мережею[45].

3.1.1 Різновиди мережевих екранів

Брандмауери поділяються на різні типи за наступними характеристиками:

- Чи забезпечує екран з'єднання між вузлом і мережею, чи з'єднання між двома чи більше різними мережами;
- Мережевий протокол, на рівні якого здійснюється управління потоком даних;
- Чи слід контролювати стан активної речовини.

За охопленням контрольованого потоку даних брандмауери поділяються на:

- Цей метод створення VPN передбачає використання маршрутизатора для створення безпечного каналу. Оскільки вся інформація з локальної мережі проходить через роутер, то природно покласти її і завдання

шифрування на неї. Шлюз (сервер, який передає трафік між мережами) або апаратне рішення, яке контролює вхідні та вихідні потоки даних між підключеними мережами.

- Персональний брандмауер – програма, встановлена на комп'ютері користувача для запобігання несанкціонованого доступу лише до цього комп'ютера.
- Ситуація погіршення полягає в тому, що сервер використовує традиційний брандмауер для обмеження доступу до власних ресурсів[28].

За рівнем контролю доступу мережеві екрани поділяються на такі категорії:

- На мережевому рівні фільтрація базується на адресах відправника і одержувача пакета даних, номері порту транспортного рівня моделі OSI і статичних правилах, встановлених адміністратором;
- Рівень сеансу (також відомий як стан) – відстеження сеансів між програмами, які не доставляють пакети, що порушують специфікацію TCP/IP, ці пакети зазвичай використовуються для сканування ресурсів зловмисних операцій, викликаного неправильною реалізацією TCP/IP злом, відключення/уповільнення вниз, введення даних.
- На рівні програми фільтрація заснована на аналізі даних програми, переданих у пакеті даних. Ці типи екранів дозволяють блокувати передачу небажаної та потенційно небезпечної інформації на основі політик та налаштувань.

Деякі рішення, пов'язані з екранами на рівні програми, є проксі-серверами з деякими можливостями екрана для реалізації прозорих проксі-серверів, які спеціалізуються на протоколах. Функції проксі та багатопротокольна спеціалізація роблять фільтрацію набагато гнучкішою, ніж фільтрацію на традиційних веб-екранах, але такі програми мають усі недоліки проксі-серверів (наприклад, анонімізація трафіку).

Відповідно до відстеження активних з'єднань екран мережі виглядає

так:

- Без стану (проста фільтрація), не відстежує поточне з’єднання (наприклад, TCP), лише фільтрує потік даних відповідно до статичних правил;
- Перевірка пакетів із збереженням стану (SPI) (контекстно-чутлива фільтрація), яка відстежує поточне з’єднання та пропускає лише ті пакети, які відповідають логіці та алгоритму відповідного протоколу та програми.

Ці типи брандмауерів дозволяють ефективніше боротися з різними типами DoS-атак і вразливими місцями в певних мережевих протоколах. Крім того, вони забезпечують такі протоколи, як H.323, SIP, FTP тощо. Ці протоколи використовують складні схеми передачі даних між приймачами. Ці схеми важко описати статичними правилами, і їх зазвичай порівнюють зі стандартними брандмауерами без стану. Несумісні.[55]

3.1.2 Типові можливості

Типові функції включають:

- Фільтрувати доступ до раніше небезпечних служб;
- Не допускати отримання конфіденційної інформації із захищеної підмережі та внесення неправдивих даних до захищеної підмережі через уразливі сервіси;
- Контроль доступу до вузлів мережі;
- Всі спроби зовнішнього і внутрішнього доступу можуть бути зареєстровані, що дозволяє відстежувати використання доступу в Інтернет різними вузлами мережі;
- Стандартизувати порядок доступу до мережі;
- Повідомляти про підозрілу активність, спробу виявити або атакувати вузли мережі або сам екран;
- Через обмеження безпеки деякі необхідні служби користувача, такі як Telnet, FTP, SMB, NFS тощо, можуть бути заблоковані.

Тому для налаштування брандмауера необхідна участь експертів з мережевої безпеки. Якщо ні, шкода від неправильної конфігурації може переважити переваги.

Також слід зазначити, що використання брандмауера збільшить час відгуку та зменшить пропускну здатність, оскільки фільтрація не є миттєвою. Основне завдання брандмауера - перевіряти всі дані, що входять і виходять з комп'ютера. Інструмент діє як бар’єрний фільтр, відокремлюючи дані з комп’ютера від «зовнішнього світу» (точніше, Інтернету). Він перевіряє дані та дозволяє або забороняє надсилання залежно від типу даних, відправника та одержувача даних або їх обсягу. Але якщо ваша антивірусна програма вже виконує серію перевірок, навіщо потрібні додаткові заходи безпеки? Відповідь проста: загрози, що поширюються в Інтернеті, не обмежуються вірусами, хробаками та шпигунськими програмами; вони також включають різні спроби зловживання, включаючи використання програм захисту від уразливостей або використання незагальних сервісів[7].

Для виконання функції захисного бар’єру брандмауер використовує різноманітні методи фільтрації. Перший метод називається «фільтрація пакетів». Він включає в себе IP-адресу відправника та одержувача даних аналізу, тип пакету даних (в TCP) і номер порту, який використовується для передачі даних. Цей метод використовує «динамічну фільтрацію», яка виконує різні перевірки пакетів, але також контролює інші операції обміну даними. Для забезпечення більш надійного захисту більшість брандмауерів додатково використовують «фільтрацію на рівні програми», яка контролює передачу даних різними типами програм.

Коли буде виявлено спробу підключення, яка не відповідає вказаним правилам, брандмауер автоматично блокує спробу та попередить користувача. Наприклад, якщо користувач вирішить вимкнути службу FTP (оскільки це непотрібно або занадто ризиковано для комп’ютера), брандмауер блокуватиме всі спроби під’єднання за допомогою служби. Ви також можете використовувати брандмауери, щоб заборонити або дозволити доступ до

певних веб-сайтів і служб, наприклад, до завантажень або взаємодій між однорангом.

Брандмауер не може захистити від атак, які не виконуються через нього. Багато пов’язаних компаній дуже бояться витоку конфіденційних даних через цей канал. Керівництво багатьох організацій налякане підключенням до Інтернету і не знає, як захистити доступ до модему через комутовану лінію. Щоб брандмауер виконував свою функцію, він повинен бути частиною загальної системи безпеки, узгодженої в організації. Правила брандмауера мають бути реалістичними та відображати загальний рівень захисту всієї мережі.

Брандмауер не може захистити передачу команд (троянських коней) або неправильно написаних клієнтських програм через більшість протоколів прикладних програм. Брандмауер не є панацеєю, і його існування не позбавляє від необхідності контролю програмного забезпечення в локальній мережі або захисту хостів і серверів. Надсилання «поганих» повідомлень через HTTP, SMTP та інші методи дуже легко[13].

3.1.3 Проблеми, які не вирішуються файрволом

Сам брандмауер не є панацеєю від усіх кіберзагроз. Зокрема, він:

- Не захищає вузли мережі від проникнення через люк (англ. back door);
- Не забезпечує захист від багатьох внутрішніх загроз, особливо від витоку даних;
- Не захищає користувачів від завантаження шкідливого програмного забезпечення, включаючи віруси.

Для вирішення двох останніх проблем використовуються відповідні додаткові інструменти, включаючи антивірусне програмне забезпечення. Зазвичай вони підключаються до брандмауера і проходять через відповідну частину мережевого трафіку, діючи як прозорі проксі для інших вузлів мережі, або отримуючи копію всіх переданих даних від брандмауера. Однак цей аналіз вимагає багато апаратних ресурсів, тому зазвичай виконується незалежно на

кожному вузлі мережі[63].

3.2 Брандмауер

Брандмауер — це система або комбінація систем, яка дозволяє розділити мережу на дві або більше частин і реалізувати набір правил для визначення умов проходження пакетів даних з однієї частини в іншу. Ця межа зазвичай проводиться між локальною мережею компанії та Інтернетом, але її також можна провести в межах локальної мережі компанії. Тому брандмауер пропускає весь трафік через себе. Для кожного пакета, який проходить, брандмауер вирішує пропустити його або відкинути. Щоб брандмауер прийняв ці рішення, він повинен визначити набір правил. Нижче буде обговорено, як описати ці правила та які параметри використовуються для їх опису.

Як правило, брандмауери можуть працювати на будь-якій платформі UNIX — найпоширенішими є BSDI, SunOS, AIX, IRIX тощо, і рідше — DOS, VMS, WNT, Windows NT. З точки зору апаратної платформи, існують процесори R4400-R5000 серії INTEL, Sun SPARC, RS6000, Alpha, HP PA-RISC і RISC. На додаток до Ethernet, більшість брандмауерів також підтримують FDDI, token ring, 100Base-T, 100VG-AnyLan та різні послідовні пристрої. Вимоги до оперативної пам’яті та місця на жорсткому диску залежать від кількості машин у захищеному сегменті мережі, але зазвичай рекомендується мати принаймні 32 МБ оперативної пам’яті та 500 МБ місця на жорсткому диску[47].

Зазвичай в операційну систему, на якій працює брандмауер, вносяться зміни, щоб підвищити захист самого брандмауера. Ці зміни вплинуть на ядро операційної системи та відповідні файли конфігурації. Сам брандмауер не дозволяє облікові записи користувачів (тому можуть бути лазівки), лише облікові записи адміністратора. Деякі брандмауери працюють лише в режимі одного користувача. Багато брандмауерів мають системи перевірки цілісності програмного коду. Контрольна сума програмного коду зберігається в

безпечному місці та порівнюється на початку програми, щоб уникнути заміни програмного забезпечення. Всі брандмауери можна розділити на три типи:

- Пакетний фільтр
- Шлюз додатків
- Шлюз ланцюга

Усі типи можна зустріти одночасно в брандмауері.

3.2.1 Пакетні фільтри

Брандмауер фільтрації пакетів визначає, чи пропустити пакет, чи відкинути пакет, дивлячись на IP-адресу, прапор або номер порту TCP у заголовку пакета. IP-адреса та номер порту – це рівень мережі та транспортний рівень відповідно, але фільтр пакетів використовує інформацію прикладного рівня, оскільки всі стандартні послуги в TCP/IP пов’язані з певним номером порту.

Для того, щоб описати правила доставки пакетів, складаються такі типи таблиць:

- Поле «дія» можна пропустити або відкинути.
- Тип пакета - TCP, UDP або ICMP.
- Прапор – прапор із заголовка IP-пакету.
- Поля «Source Port» і «Destination Port» мають значення лише для пакетів TCP і UDP[47].

3.2.2 Сервера прикладного рівня

Брандмауер із сервером рівня програми використовує певний сервісний сервер — TELNET, FTP тощо. Проксі-сервер, який працює на брандмауері і пропускає весь трафік, пов’язаний з цією службою. Тому між клієнтом і сервером формуються два з'єднання: від клієнта до брандмауера і від брандмауера до місця призначення. Повний набір підтримуваних серверів відрізняється для кожного конкретного брандмауера, але найпоширенішими є сервери, які використовуються для таких служб:

- термінали (Telnet, Rlogin)
- передача файлів (FTP)
- електронна пошта (SMTP, POP3)
- WWW (HTTP)
- Gopher
- Wais
- X Window System (X11)
- Принтер
- Rsh
- Finger
- новини (NNTP) та ін.

Використання сервера рівня програми може вирішити важливе завдання — приховати структуру локальної мережі від зовнішніх користувачів, включаючи інформацію в поштових пакетах або заголовках служби доменних імен (DNS). Ще однією позитивною якістю є можливість аутентифікації на рівні користувача (ідентифікація — це процес підтвердження ідентичності чогось; в даному випадку — це процес підтвердження того, чи дійсно користувач є тим, за кого себе видає). Більше інформації про аутентифікацію буде описано нижче. Правила доступу описують ім’я служби, ім’я користувача, ефективний проміжок часу служби, комп’ютери, які можуть використовувати службу, схему аутентифікації та інші параметри. Сервер протоколу прикладного рівня забезпечує найвищий рівень захисту - за допомогою невеликої кількості програм для досягнення взаємодії із зовнішнім світом ці програми повністю контролюють весь вхідний і вихідний трафік[11].

3.2.3 Сервера рівня з’єднання

Сервер рівня з'єднання - це перетворювач з'єднань TCP. Користувач підключається до певного порту брандмауера, а останній підключається до місця призначення на іншій стороні брандмауера. Під час сеансу цей перетворювач копіює байти в обох напрямках, діючи як дріт.

Зазвичай місце призначення попередньо встановлено, а джерело може бути кількома (тип комбінації один-множинний). Можна створювати різні конфігурації, використовуючи різні порти.

Цей тип сервера дозволяє вам створити конвертер для будь-якої користувальницької служби на основі TCP, щоб контролювати доступ до служби та збирати статистику щодо її використання[5].

3.3 Порівняльна характеристика

Нижче наведено основні переваги та недоліки пакетних фільтрів і серверів рівня прикладних програм.

До переваг пакетних фільтрів можна віднести:

- Відносно невисока вартість
- Гнучкість у визначенні правил фільтрації
- Невелика затримка під час передачі пакетів
- Недоліками цього типу брандмауера є:
- Локальна мережа видима з ІНТЕРНЕТУ (маршрутизована)
- Правила фільтрації пакетів важко описати, потрібно добре розуміти технологію TCP та UDP
- Коли брандмауер вийде з ладу, всі комп’ютери за ним будуть повністю незахищені або недоступні
- аутентифікацію з використанням IP-адреси можна обдурити використанням IP-спуфінгу (атакуюча система видає себе за іншу, використовуючи її IP-адресу)
- відсутня автентифікація на рівні користувача

До переваг серверів прикладного рівня слід зарахувати такі:

- локальна мережа невидима з INTERNET
- при порушенні працездатності брандмауера пакети перестають проходити через брандмауер, тим самим не виникає загрози для машин, що захищаються ним.

- захист на рівні додатків дозволяє здійснювати велику кількість додаткових перевірок, знижуючи цим ймовірність злому з використанням дірок у програмному забезпеченні автентифікація на рівні користувача може бути реалізована система негайного попередження про спробу злому.

Недоліками цього є:

- Вищий, ніж пакетний фільтр;
- Не можна використовувати протоколи RPC та UDP;
- Продуктивність нижча, ніж у пакетного фільтра[13].

3.3.1 Віртуальні мережі

Былышість брандмауерів дозволяють організувати віртуальну приватну мережу (Virtual Private Network), яка об'єднує кілька локальних мереж, підключених до Інтернету, у віртуальну мережу. VPN дозволяє організовувати прозорі з’єднання для користувачів локальної мережі та підтримувати конфіденційність і цілісність інформації, що передається за допомогою шифрування. У цьому випадку шифруються не тільки дані користувача, а й мережева інформація-адреса мережі, номер порту тощо під час передачі через ІНТЕРНЕТ[40].

3.3.2 Схеми підключення

Для підключення брандмауерів використовують різні схеми. Брандмауер може використовуватися як зовнішній роутер, використовуючи підтримувані типи пристроїв для підключення до зовнішньої мережі (рис 3.1).

Рис.3.1 - Підключення до зовнішньої мережі

Іноді використовується схема, зображена на рис 3.2, однак користуватися нею слід тільки в крайньому випадку, оскільки потрібно дуже акуратне налаштування роутерів і невеликі помилки можуть утворити серйозні дірки в захисті.

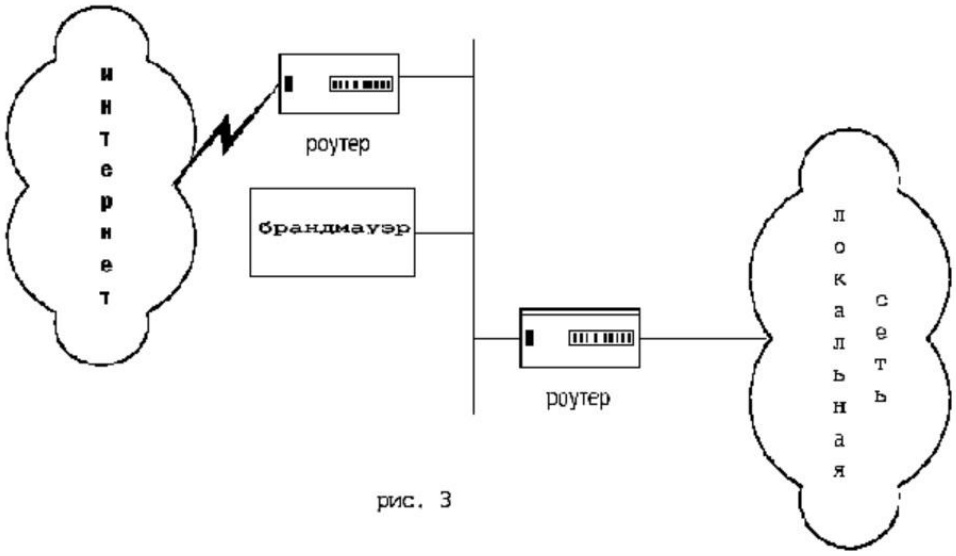

Рис. 3.2 – Підключення до роутера

Якщо брандмауер може підтримувати два інтерфейси Ethernet (так званий dual-homed брандмауер), то найчастіше підключення здійснюється через зовнішній маршрутизатор (рис.3.3).

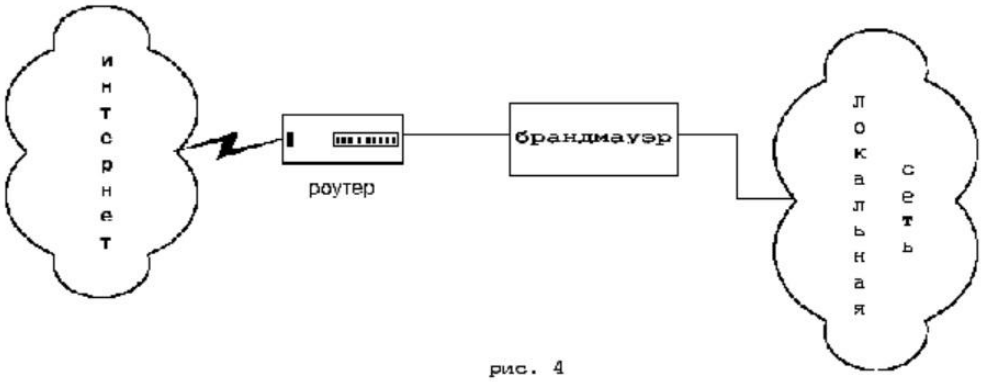

Рис. 3.3 - Підключення через зовнішній маршрутизатор

Однак між зовнішнім маршрутизатором і брандмауером є лише один шлях, тобто весь трафік. Зазвичай маршрутизатор налаштований так, що брандмауер є єдиною машиною, видимою ззовні. Ця схема є найкращою з точки зору безпеки та надійності захисту. Інше рішення показано на рисунку 3.4.

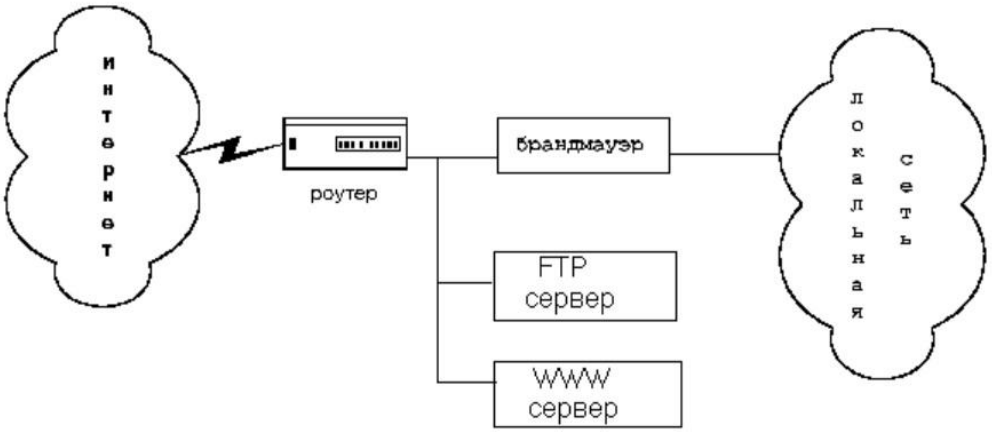

Рис. 3.4 – Шлях між маршрутизатором і брандмауером

У цьому випадку брандмауер захищає лише одну підмережу з кількох маршрутизаторів. У областях, не захищених брандмауерами, зазвичай є сервери (WWW, FTP тощо), які мають бути видимі ззовні. Деякі брандмауери пропонують розмістити ці сервери самостійно — це рішення не найкраще з точки зору безпеки завантажувального апарату та самого брандмауера.

Існують рішення (рис.3.5), які дозволяють організувати сервери, які повинні бути видимі з-за меж третьої мережі; це дозволяє контролювати доступ до них, зберігаючи рівень захисту, необхідний для машин в основній мережі[52].

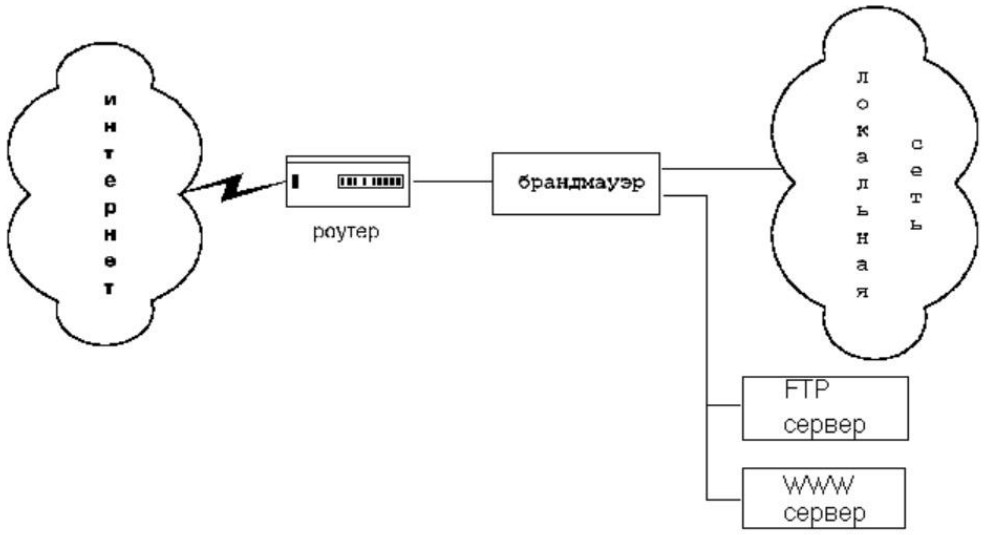

Рис.3.5 – Схема організації серверів

При цьому користувачі внутрішньої мережі не можуть ненавмисно чи свідомо відкрити лазівку в локальній мережі через ці сервери, що привернуло

велику увагу. Щоб підвищити рівень безпеки, можна використовувати кілька брандмауерів у мережі один за одним.

3.3.3 Адміністрування

Простота управління є одним із ключових факторів створення ефективної та надійної системи безпеки. Помилки в правилах доступу можуть спричинити лазівки, які можуть призвести до пошкодження системи. Тому більшість брандмауерів реалізують службові утиліти, які допомагають вводити, видаляти та змінювати набір правил. Наявність цих утиліт також дозволяє перевірити наявність граматичних або логічних помилок під час введення або редагування правил. Як правило, ці утиліти дозволяють переглядати інформацію, згруповану за будь-якими критеріями, наприклад, всю інформацію, пов’язану з певним користувачем або послугою[16].

3.3.4 Система збору статистики та попередження про атаку

Іншою важливою частиною брандмауера є система, яка використовується для збору статистики та попередження про атаки. Інформація про всі події-збої, вхідні та вихідні з’єднання, кількість переданих байтів, обслуговування, час підключення тощо. Більшість брандмауерів дозволяють гнучко визначати події, які потрібно реєструвати, описуючи дії брандмауера під час атаки або спроби несанкціонованого доступу – це може бути повідомлення, надіслане на консоль, повідомлення, надіслане системному адміністратору тощо. Якщо спроба успішна і зловмисник увійшов в систему, буде корисно негайно відобразити повідомлення про спробу злому на екрані консолі або адміністратора. Більшість брандмауерів включають генератори звітів для обробки статистичних даних. Вони дозволяють збирати статистичну інформацію про використання ресурсів конкретними користувачами, використання сервісів, збої, джерела спроб отримати несанкціонований доступ тощо[12].

3.3.5 Аутентифікація

Перевірка особи є одним з найважливіших компонентів брандмауера. Перш ніж надати користувачеві право користуватися сервісом, потрібно переконатися, що він є тим, за кого себе видає (припускаючи, що користувач дозволяє послугу: процес визначення дозволених послуг називається авторизацією. Авторизація зазвичай розглядається в контекстна аутентифікація - після автентифікації користувача. Отримавши запит на використання служби від імені будь-якого користувача, брандмауер перевірить, який метод аутентифікації визначено для користувача, і передасть контроль над сервером аутентифікації. Після того, як брандмауер отримує позитивну відповідь від сервера аутентифікації, з'єднання, запитане користувачем, формується.

Зазвичай використовується принцип «що він знає», тобто користувач знає деякі секретні слова, які він надсилає на сервер аутентифікації у відповідь на запит[22].

Однією із схем аутентифікації є використання стандартних паролів UNIX. Ця схема є найбільш вразливою з точки зору безпеки - пароль може бути перехоплений і використаний іншою особою.

Найчастіше використовується схема з одноразовим паролем. Навіть якщо він буде перехоплений, цей пароль не потрібен для наступної реєстрації. Отримання наступного пароля з попереднього пароля є надзвичайно складним завданням. Як програмні, так і апаратні генератори використовуються для створення одноразових паролів - останній є пристроєм, який підключається до комп'ютерного гнізда. Для роботи з цим пристроєм потрібно знати пароль. Багато брандмауерів підтримують Kerberos, який є одним із найпоширеніших методів аутентифікації. Деякі сценарії вимагають зміни клієнтського програмного забезпечення, і цей крок не завжди прийнятний. Як правило, усі комерційні брандмауери підтримують кілька різних сценаріїв, що дозволяє адміністраторам зробити вибір, який найкраще підходить для їх середовища.

Брандмауер може обмежити доступ третіх сторін до комп'ютера через Інтернет. Існує два типи брандмауерів, програмні та апаратні, і вони

допомагають запобігти спробам зловмисників отримати доступ до вашого комп’ютера в локальній мережі та Інтернеті (хакерські атаки, віруси, спам тощо).

Брандмауер необхідний для контролю вхідного та вихідного трафіку на комп’ютері чи локальній мережі, що дозволяє блокувати майже всі види мережевих атак, вирізати рекламу (відключати банери, рекламні скрипти, спливаючі вікна тощо), видаляти файли cookie, і не надавати іншим» інформація про сервер вашого комп’ютера робить «троянських коней» і методи віддаленого керування марними. Крім того, брандмауер допомагає запобігти участі вашого комп’ютера в таких атаках на інші комп’ютери без вашого відома. Використання брандмауера особливо важливо, коли ви часто підключаєтеся до Інтернету через кабельні, DSL або ADSL лінії[18].

Якщо на комп’ютері встановлено попередню версію Windows, рекомендується використовувати апаратний брандмауер. Багато точок бездротового доступу домашньої мережі мають вбудовані брандмауери та маршрутизатори. Підключити брандмауер до мережі так само просто, як підключити автовідповідач до телефону. Від’єднайте з’єднання Ethernet між кабельним або DSL-модемом і ПК та підключіть між ними брандмауер. (Це стосується більшості брандмауерів, але не всіх)

Можна придбати програмні брандмауери від кількох постачальників, щоб захистити комп’ютери з попередніми версіями Windows. Ці постачальники надають брандмауери, які можна використовувати в Windows XP.

Брандмауер підключення до Інтернету може не підходити для деяких мережевих програм, встановлених на комп’ютері. У більшості випадків цю несумісність можна вирішити, налаштувавши брандмауер підключення до Інтернету або звернувшись до свого програмного забезпечення чи постачальника послуг Інтернету. Іноді проблему можна вирішити шляхом встановлення новішої версії програмного забезпечення[2].

Попередження: брандмауер має бути чітко налаштований. Неправильна конфігурація призведе до неправильного запуску програм, які використовують мережевий трафік.

РОЗДІЛ 4 ВИБІР БРАНДМАУЕРА

Число кіберзлочинів зростає з кожним роком. Опитування показують, що вже зараз їхні жертви обчислюються мільйонами. У багатьох випадках неприємностей можна було б уникнути, якби на комп'ютері було встановлено гарний брандмауер. Але яку програму можна вважати такою? Щоб відповісти на це питання, проводяться деякі тести, які піддають брандмауери різноманітним атакам[6].

Відразу варто відзначити, що якщо професійні хакери будуть цілеспрямовано атакувати саме ваш комп'ютер, брандмауер може і не врятувати. Але відкинути атаки розумників з локальної мережі або автоматичні зломи, що виробляються вірусами, він цілком здатний.

Ідеальний персональний брандмауер повинен виконувати шість функцій:

- Запобігати зовнішнім атакам. В ідеалі брандмауер повинен блокувати всі відомі типи атак, включаючи сканування портів, підробку IP-адресів, DoS і DDoS, вибір пароля тощо.
- Зупинити витік інформації. Навіть якщо шкідливий код проникає в комп’ютер (не обов’язково через мережу, але у вигляді вірусу на придбаному піратському компакт-диску), брандмауер повинен запобігти витоку інформації, запобігаючи проникненню вірусу в мережу.
- Контроль програм. Наявність неминучих відкритих дверей (тобто відкритих портів) є однією з труднощів у запобіганні витоку інформації, і одним із найнадійніших способів запобігання проникненню вірусів через ці двері є контроль програм, які запитують доступ. На додаток до звичайної перевірки імені файлу, також дуже необхідно перевірити ідентичність програми.
- Підтримка зонального захисту. Робота в локальній мережі часто має на увазі практично повну довіру до локального контенту. Це відкриває унікальні можливості щодо використання новітніх (і, як правило, потенційно небезпечних) технологій. У той же час рівень довіри до

Інтернет-контенту значно нижчий, а отже, необхідний диференційований підхід до аналізу небезпеки того чи іншого змісту.

- Ведення журналу та попередження. Брандмауер повинен збирати необхідну кількість інформації. Занадто багато (і відсутність) інформації неприпустимо. Можливість налаштувати файл журналу та вказати причину привернення уваги користувачів.
- Максимальна прозорість. Ефективність і застосовність системи зазвичай обернено пропорційні складності її конфігурації, управління та обслуговування. Хоча традиційно скептично ставляться до користувацьких гідів та інших буржуазних трюків, навіть досвідчені адміністратори не будуть ігнорувати їх лише для економії часу.

4.1 Брандмауер Windows

Брандмауер (мережевий екран) можна представити у вигляді стіни або фільтра, що стоїть на варті локальної мережі або комп'ютера. Вперше брандмауер з'явився у Windows XP після впровадження другого службового пакета оновлень (Service Pack 2). Цей брандмауер був недосконалим і залишав відкритими всі порти вашого комп'ютера[16].

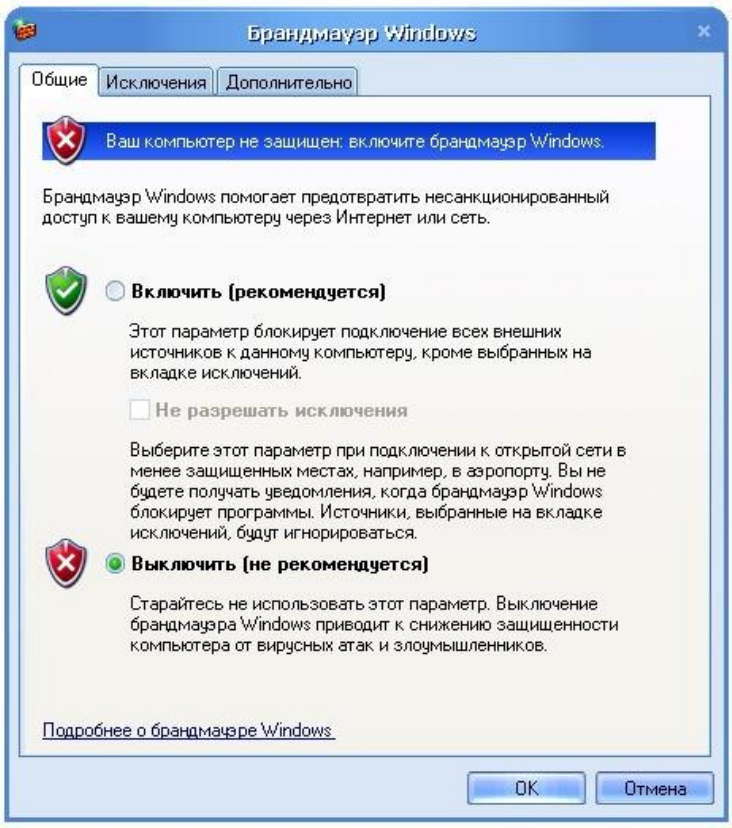

Рис.4.1- Брандмауер Windows

Брандмауер перевіряє кожне з'єднання між зовнішньою мережею, такою як Інтернет, та внутрішньою мережею, після чого або дозволяє, або забороняє його.

4.2 Tools Firewall Plus

Безкоштовний, простий у використанні, але ефективний персональний брандмауер для Windows, що захищає інформацію, що зберігається на вашому комп'ютері, від несанкціонованого доступу з локальних мереж або Інтернету. Контролюючи роботу різних програм, Firewall Plus припиняє спроби троянів, бекдорів, клавіатурних шпигунів та інших шкідливих програм завдати шкоди комп'ютеру та викрасти вашу конфіденційну інформацію.

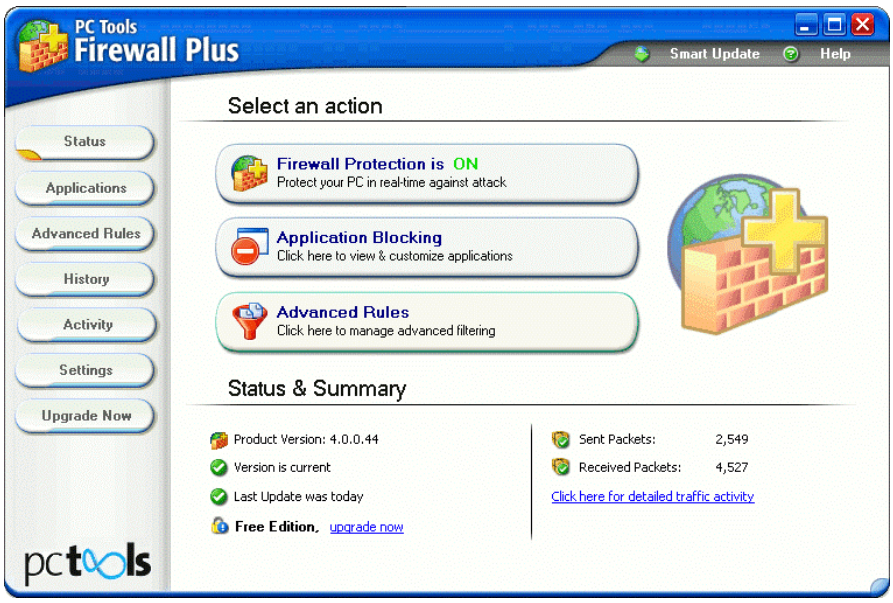

Рис. 4.2 - Tools Firewall Plus

Передова технологія PC Tools Firewall Plus була спеціально розроблена таким чином, щоб програмою могли користуватися не лише фахівці, а й пересічні користувачі. Потужний захист від атак та шкідливих програм активується за умовчанням. Все, що вам потрібно зробити – це інсталювати програму, і ваш комп'ютер негайно опиниться під постійним захистом. Досвідчені користувачі можуть також створювати власні ускладнені правила фільтрації пакетів, включаючи підтримку IPv6, щоб налаштувати мережевий захист на свій розсуд.

Основні переваги програми:

- захищає комп'ютер, коли ви працюєте, шукаєте щось в Інтернеті або граєте.
- автоматичний захист, що налаштовується без будь-яких проблем
- простота використання - програма призначена як для досвідчених, так і для користувачів-початківців.
- можливість створення додаткових правил підвищення рівня захисту ПК від поширених видів атак.

4.3 Comodo Firewall Pro 3.0.25.378

Офіційний сайт: comodo.com

Системні вимоги: Windows XP SP2, Vista, 7, 8, 10, 152 Мб RAM, 400 Мб на диску

Ліцензія: є безкоштовна версія та Pro

Вартість: безкоштовно або 39,99 доларів за Pro

Можливість обрати мову інтерфейсу: Ця програма здобула широку популярність ще в епоху Windows XP, коли Comodo Firewall був чи не найпоширенішим безкоштовним файрволом у Росії. Він користується популярністю і зараз. Що, загалом, не дивно: розробники обіцяють проактивний захист з HIPS, міжмережеве екранування, захист від переповнення буфера та несанкціонованого доступу, захист реєстру та системних файлів, а також інші смачні плюшки.

Однак під час встановлення файрвол викликав змішані почуття. Спочатку пропонував поставити розширення для Яндекс.Браузера.

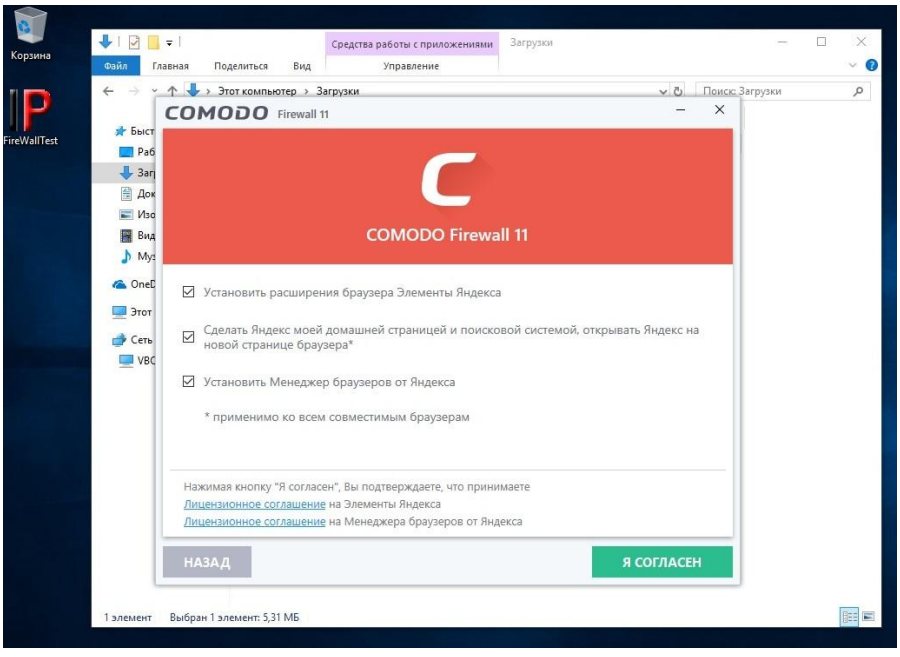

Рис. 4.3 - Comodo Firewall Pro 3.0.25.378

А потім, якщо не звернути увагу на «компоненти» і не вимкнути все непотрібне, інсталює інсталятор на комп’ютер.

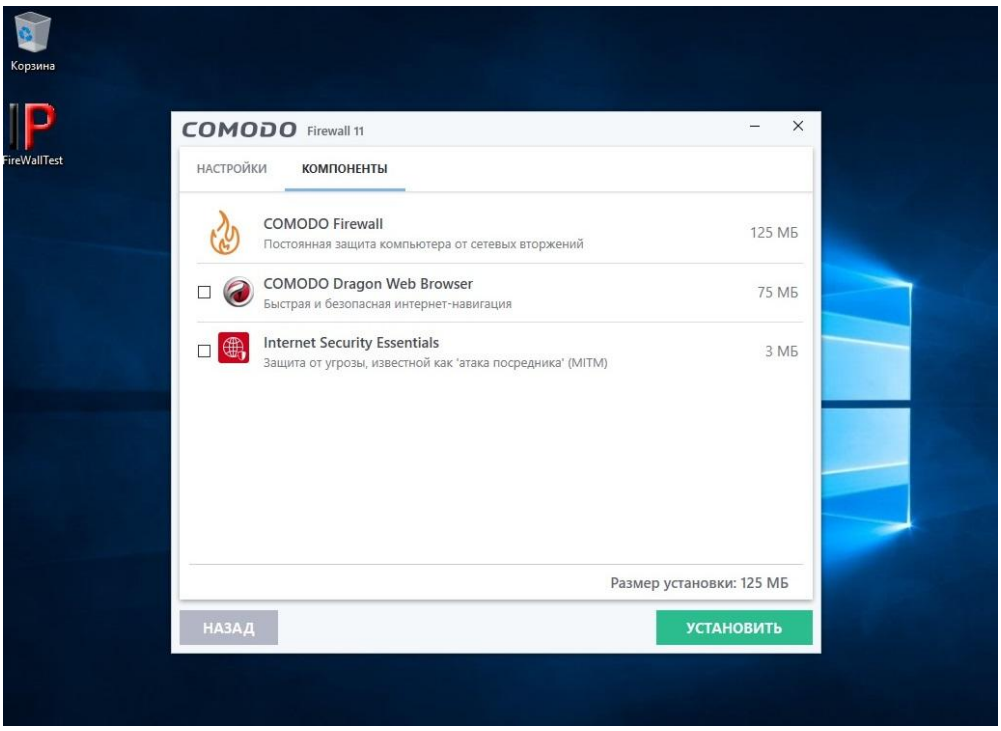

Рис.4.4 – Комоненти Comodo Firewall Pro 3.0.25.378

Робимо перший тест і Comodo пропускає нашу тулзу.

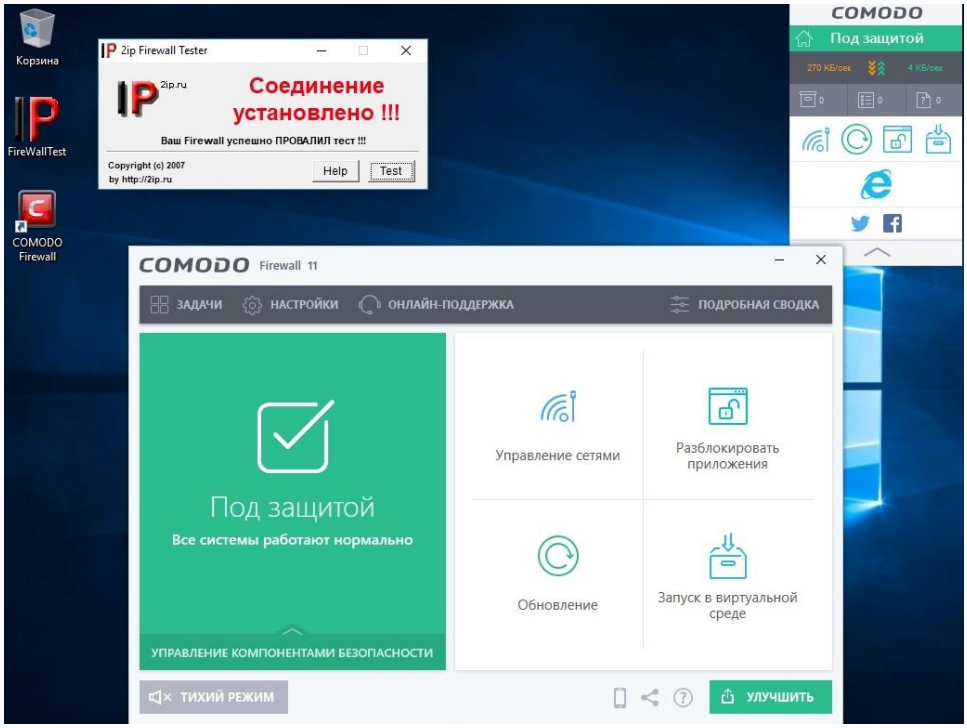

Рис.4.5 - Тест Comodo Firewall Pro 3.0.25.378

Включивши режим навчання в налаштуваннях - і файрвол чомусь ніяк не прореагував на тестову програму, яка успішно підключилася до віддаленого комп'ютера.

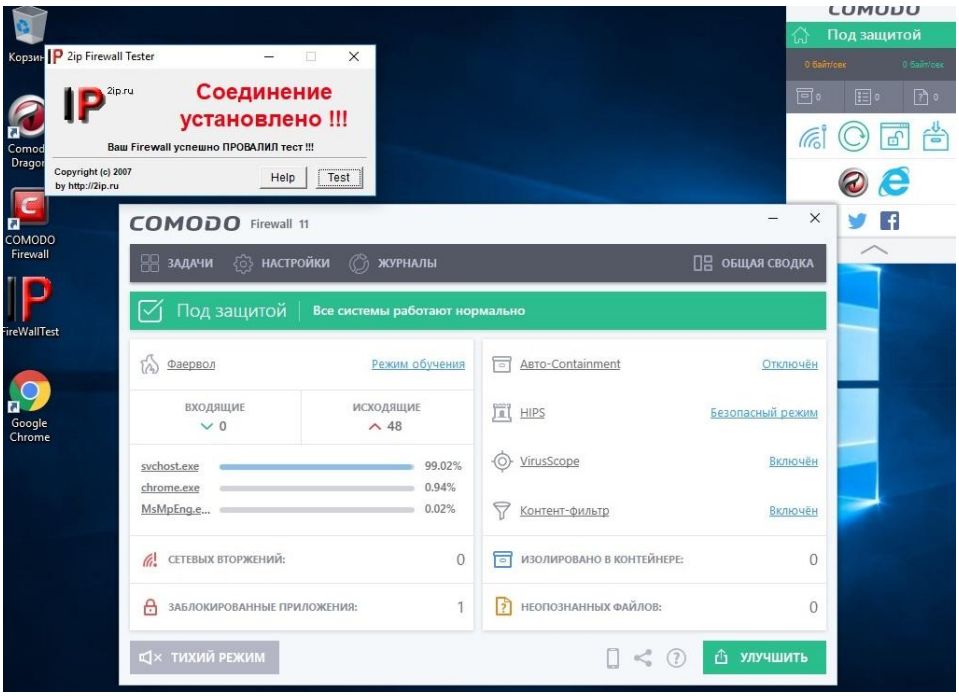

Рис. 4.6 – Блокування загрози

Тільки після складання білого списку тулзу, нарешті, вдалося заблокувати. Висновок напрошується суперечливий: Comodo Firewall - дуже відомий файрвол, але встановлення непотрібного софту псує все враження. А результати тесту виявилися сумними: для забезпечення безпеки програмі потрібне ґрунтовне налаштування.

4.4 Ashampoo Firewall

Безкоштовний, простий та зручний персональний брандмауер для операційних систем Windows. Вбудований модуль Configuration Assistant для легкої установки та налаштування програми під свої потреби та потреби. Режим роботи «Easy Mode» призначений для людей, які володіють невеликими технічними навичками в захисті ПК, але також є «Expert Mode» для професіоналів, які налаштовують власноруч налаштовувати програму.

Рис. 4.7 - Ashampoo Firewall

Маючи велику кількість додаткових інструментів, Ashampoo Firewall споживає трохи системних ресурсів і займає трохи місця в пам'яті комп'ютера. Ashampoo FireWall здійснює постійний моніторинг мережевої активності як вихідних, так і вхідних з'єднань, є режим самонавчання «Learning Mode», можливість налаштовувати правила роботи ПК, кнопка моментального блокування всіх з'єднань і т.д. Є російський інтерфейс.

4.5 Avast Premium Security

Офіційний сайт: avast.com/f-firewall

Системні вимоги: Windows XP SP3, Vista, 7, 8, 8.1, 10, 256+ Мбайт ОЗУ та 1,5 Гбайт на диску

Ліцензія: пробний період на 30 днів

Ціна: 1450 рублів на рік, є різні акції. При покупці на два або три роки ціна нижче

Хтось не чув про компанію Avast Sofware? Усі про неї чули. Однак, крім відомого антивірусу, Avast випускає ще й файрвол, який входить у платний набір програм Avast Premium Security (раніше він називався Avast Internet Security, але його перейменували - мабуть, щоб уникнути плутанини з програмою, яку розглянемо наступною). Тобто окремо завантажити та встановити файрвол не

вийде: він йде в навантаження до антивірусу, антиспам-модулю, модулю захисту бездротових мереж та набору інших фішок, платна ліцензія якого коштує 1450 рублів на рік на один ПК.

При встановленні пакету пропонують поставити ще й Google Chrome, але від нього хоча б можна безболісно відмовитись.

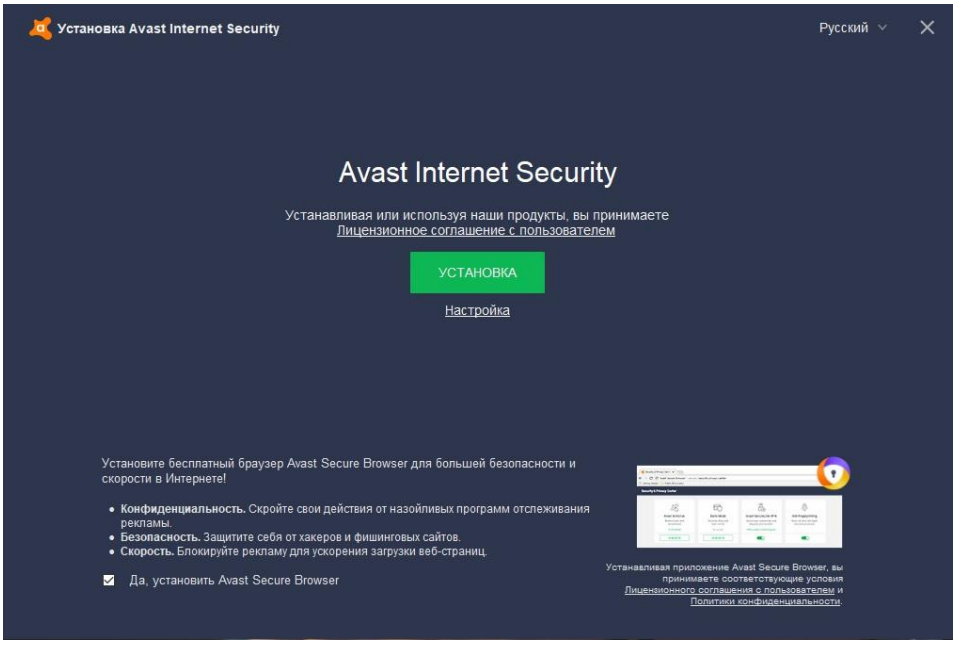

Рис. 4.8 - Avast Premium Security

Відразу після інсталяції дива не сталося: тулза успішно подолала файрвол та встановила з'єднання з віддаленим сервером.

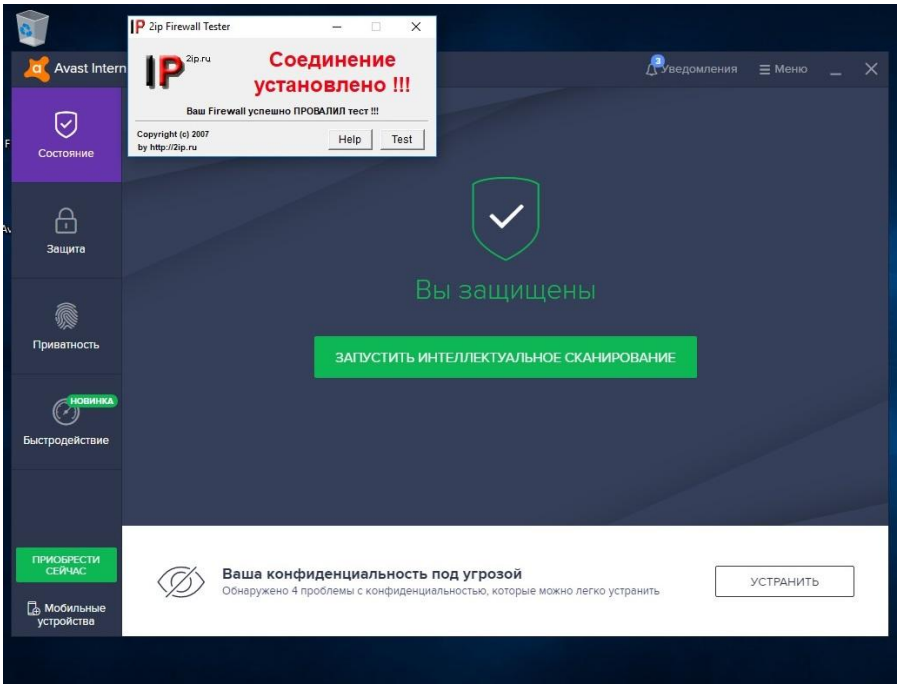

Рис. 4.9 – Встановлення з'єднання з віддаленим сервером

Після включення практично всіх можливих налаштувань та параметрів захисту нічого особливо не змінилося. Тільки змусивши файрвол параноїдально запитувати, як реагувати на кожен чх софта, що працює на комп'ютері, нарешті отримали очікуваний результат.

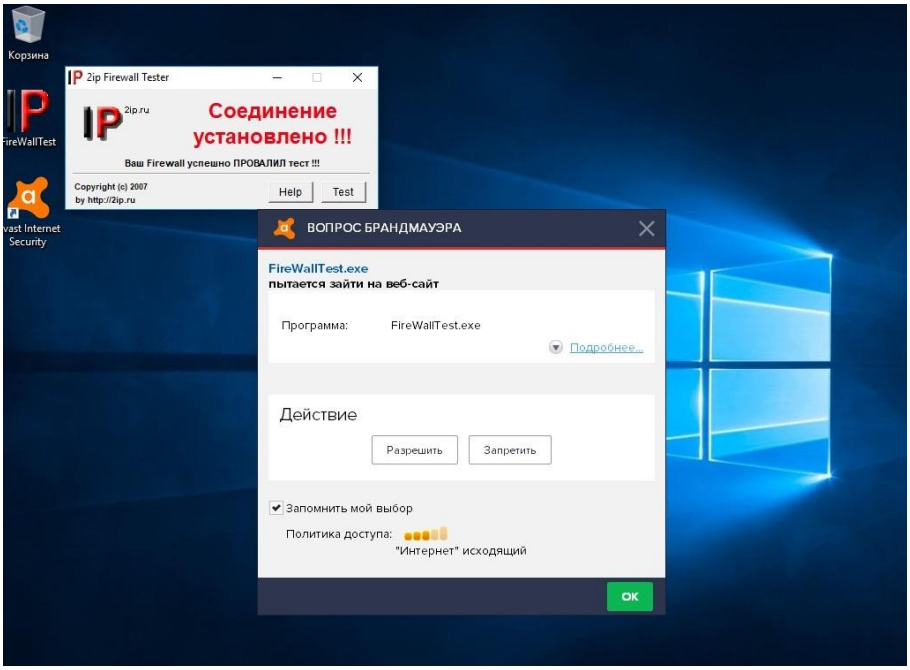

Рис.4.10 – Спроба зайти до сайту

Налаштування файрвола розкидані по різних меню, через що знайти з першого разу те, що потрібно дуже непросто. У комплекті поставки Avast Premium Security є безліч додаткових тулз для аналізу диска, реєстру, евристики, пошуку вірусів. Весь цей софт неможливо видалити, щоб залишити лише один брандмауер. Крім того, пробна версія продукту постійно просить оновитись до версії Pro та заплатити грошей.

4.6 AVG Internet Security

Офіційний сайт: avg.com

Системні вимоги: Windows XP SP3, Vista, 7, 8, 8.1, 10

Ліцензія: пробний період на 30 днів

Вартість: 1990 рублів за рік

Безкоштовний антивірус AVG також знайомий багатьом, правда про його ефективність існують різні думки. Файрвол (або, як його називають розробники,

«посилений брандмауер») теж не пропонується як окремий продукт, а йде в комплекті поставки AVG Internet Security, куди входить ще ціла купа різних утиліт, включаючи антивірус. Безкоштовної версії немає, але є можливість завантажити тріал та протестувати софтину протягом місяця.

Примітно, що антивірус AVG нещодавно був куплений компанією Avast Sofware, проте продовжує існувати в ролі самостійного продукту. Що ж, подивимося, чи є в ньому якісь суттєві відмінності від «материнського» проекту.

Установка AVG починається з впізнаваного віконця інсталера.

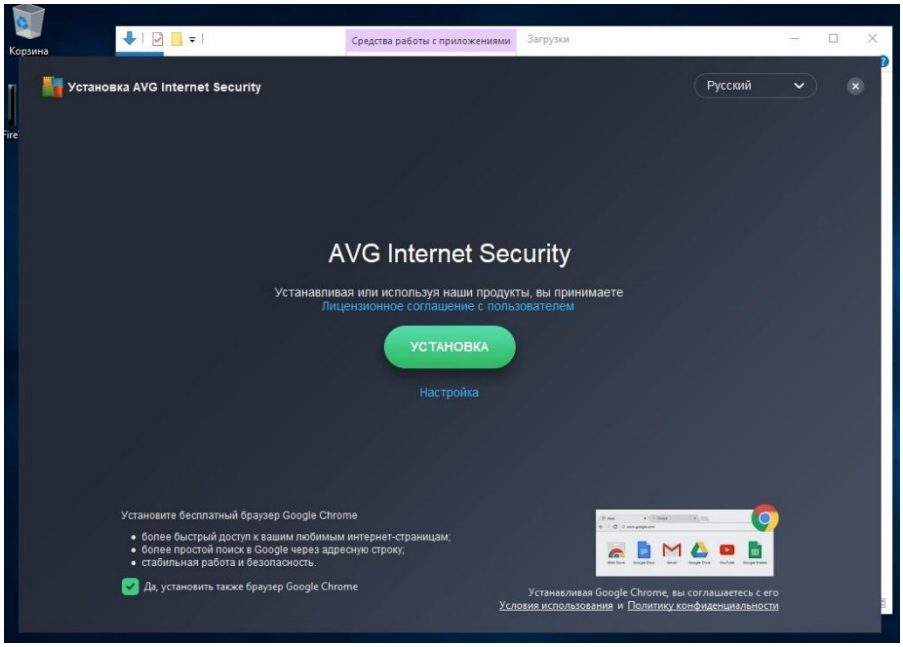

Рис.4.11 – Встановлення AVG Internet Security

При першому запуску бачимо вже знайому картинку.

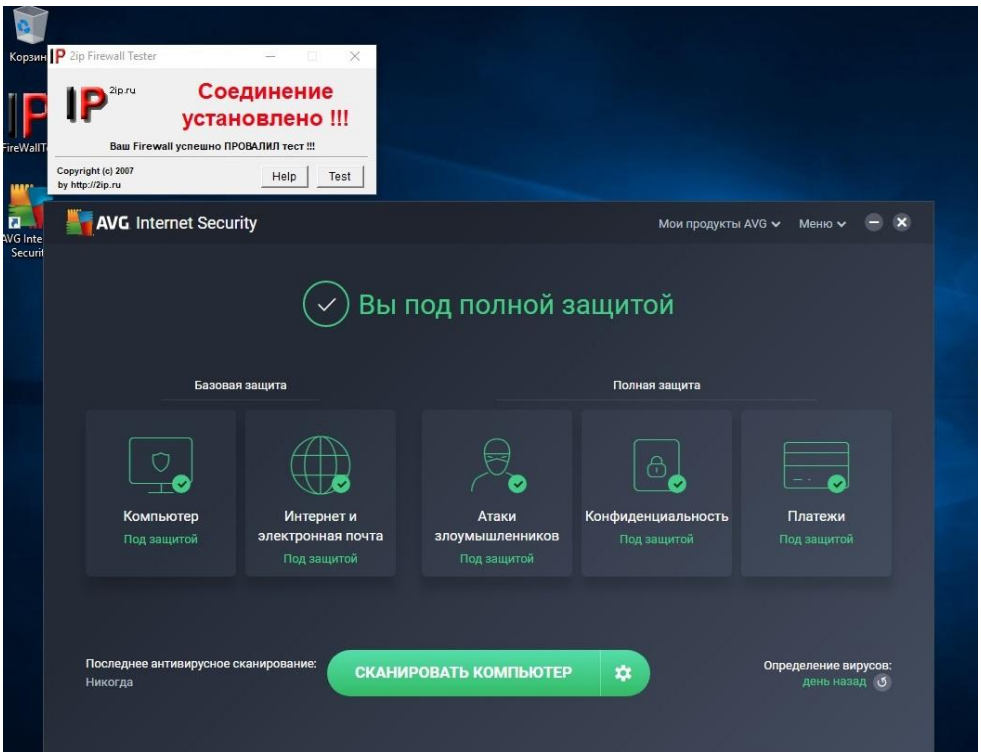

Рис.4.12 – Сканування AVG

Можна сміливо сказати, що AVG продемонстрував все те саме, що і Avast. І точно так само зумів розпізнати і заблокувати «шкідливу» тулзу тільки після примусового включення параноїдального режиму.

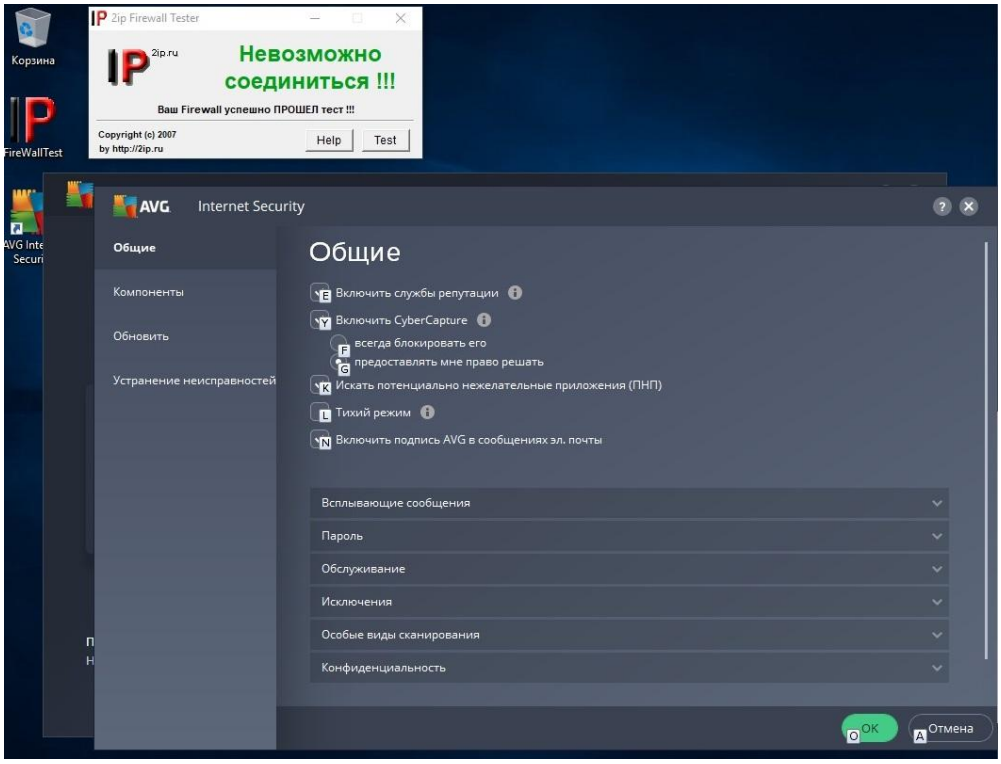

Рис. 4.13 – Тест AVG

4.7 CISCO PIX FIREWALL

Найпередовіший у галузі брандмауер (міжмережевий захисний екран), робота якого ґрунтується на трансляції мережевих адрес, забезпечує незрівнянну гнучкість при розробці проекту мережі.

Брандмауер PIX (Private Internet Exchange) Firewall фірми Cisco Systems забезпечує абсолютний захист внутрішньої мережі корпорації від несанкціонованого доступу із зовнішнього світу.

Функціонування PIX Firewall ґрунтується на ядрі операційної системи, абсолютно відмінному від UNIX; це ядро спрямоване на роботу в реальному масштабі часу і забезпечує принципово інший рівень безпеки. Забезпечення безпеки брандмауером PIX Firewall не ускладнює адміністративне керування мережею та не пов'язане з ризиком, властивим системам брандмауерного захисту на основі UNIX.

Мережевому адміністратору надаються всебічні можливості проведення аналізу всіх транзакцій, включаючи спроби несанкціонованого проникнення мережі корпорації. PIX Firewall забезпечує контрольований доступ до Internet. Програмне забезпечення брандмауера відрізняється можливістю масштабування та простотою конфігурування; на налаштування типової конфігурації потрібно не більше п'яти хвилин.

Для PIX Firewall характерними є висока продуктивність, невелика ціна, незначний обсяг технічного обслуговування. Цей брандмауер надійно захистить внутрішню мережу корпорації від несанкціонованого доступу.

Брандмауер PIX забезпечує безпечний доступ до Інтернету з приватної мережі. Брандмауер PIX використовує схему захисту трансляції з урахуванням стану (NAT) (трансляція мережевих адрес). Програма захищає внутрішню мережу компанії від Інтернету за допомогою надійного екранування та відстежує параметри підключення, такі як порти джерела та призначення, адреси, порядкові номери пакетів TCP та додаткові прапори TCP. Брандмауер PIX гарантує, що користувачі внутрішньої мережі вашої організації можуть отримати

доступ до Інтернету, одночасно захищаючи вашу внутрішню мережу від несанкціонованого зовнішнього доступу.

PIX Firewall також забезпечує додаткові переваги для вашої організації, надаючи можливість розширення та зміни конфігурації мереж TCP/IP, не турбуючись, чи вистачить для цього IP-адрес. NAT дозволяє використовувати будь-які з наявних IP-адрес або адреси з резервного пулу повноважної організації, що виділяє адреси в Internet (IANA - Internet Assigned Numbers Authority) (відповідно до RFC 1918).

У брандмауері є плата Cisco PIX Firewall Private Link, яка здійснює шифрування даних і забезпечує безпеку зв'язку при з'єднаннях по Internety між декількома системами PIX Firewall на основі стандарту шифрування даних DES (DES - Data Encryption Standard).

Адаптивна безпека:

Контролюються такі параметри вхідного трафіку:

- IP-адреси джерела та призначення
- Номери порту джерела та призначення
- Протокол
- Порядковий номер TCP
- Цілком забороняється доступ у внутрішню мережу із зовнішньої мережі
- Забезпечується параметрична безпека виконання транзакцій за протоколами TCP та UDP

Робота брандмауера ґрунтується на застосуванні схеми параметричного захисту Stateful Network Address Translation

Підтримується понад 16.000 одночасних з'єднань

Внутрішня мережа відгороджується від зовнішнього світу

Типова конфігурація налаштовується за допомогою п'яти команд протягом п'яти хвилин.

Безпечна динамічна та статична трансляція.

Трансляція мережевих адрес (Network Address Translation) здійснюється у повній відповідності до специфікацій RFC 1631.

Прозора підтримка всіх загальних сервісів TCP/IP Internet, таких як World Wide Web, FTP, Telnet, Archie, Gopher і Rlogin.

Програма безпеки займає менше 80 кбайт і діє в режимі реального часу.

Переваги:

- Брандмауер менш складний і надійніший, ніж фільтри пакетів
- Для його інсталяції не потрібно переривати роботу мережі
- Не потрібно проводити модернізацію хост-машин чи маршрутизаторів
- Не потрібне щоденне адміністративне управління брандмауером
- Повні можливості доступу із незареєстрованих хост-машин внутрішньої корпоративної мережі до Internet
- Для розширення мережі не потрібні додаткові зареєстровані IP-адреси
- Дозволяється використання як IP-адрес, що виділяються приватним мережам (відповідно до специфікації RFC 1918 - Address Allocation for Private Internets), так і наявних зареєстрованих IP-адрес
- Не створює перешкод для роботи користувачів, не погіршує функціонування локальних мереж.

РОЗДІЛ 5 ОПИС ТА ОБГРУНТУВАННЯ ОБРАНОЇ СИСТЕМИ ЗАХИСТУ

5.1 Simplewall - малий, але потужний мережевий екран

Для програмного фаєрвола Simplewall, що безкоштовно розповсюджується, має досить потужні функціональні можливості. Але відразу варто відзначити, що вбудований у Windows брандмауер має більший пріоритет у системі. Тобто, користувацькі установки в Simplewall можуть бути проігноровані операційною системою, якщо налаштування стандартного брандмауера суперечать таким у мережевого екрана, що розглядається. Тому перед використанням Simplewall розробником рекомендується вимкнути вбудований у Windows брандмауер. Втім, останній не заважає роботі функцій моніторингу мережевої активності Simplewall.

Відключати брандмауер вручну не потрібно - програма сама пропонує зробити це при активації функції міжмережевого екрану, а при деактивації - пропонує, навпаки, включити системний фаєрвол. Щоб це стало можливим, Simplewall слід запускати від імені адміністратора.

Simplewall – це простий, але досить функціональний фаєрволл – програма для обмеження доступу до інтернету програм та сервісів операційної системи. Простий інструмент для налаштування роботи Windows Filtering Platform.

Simplewall дозволяє обмежити доступ до інтернету будь-яким програмам та функціям операційної системи. Фаєрвол працює на основі правил, які вже включені в програму, так і створені користувачем. При активній функції фільтрації, simplewall блокуватиме доступ до інтернету всім програмам, і пропонуватиме користувачеві вибір подальших дій. У програмі доступний нескладний редактор правил, який дозволяє більш тонке налаштування, ніж можна/не можна.

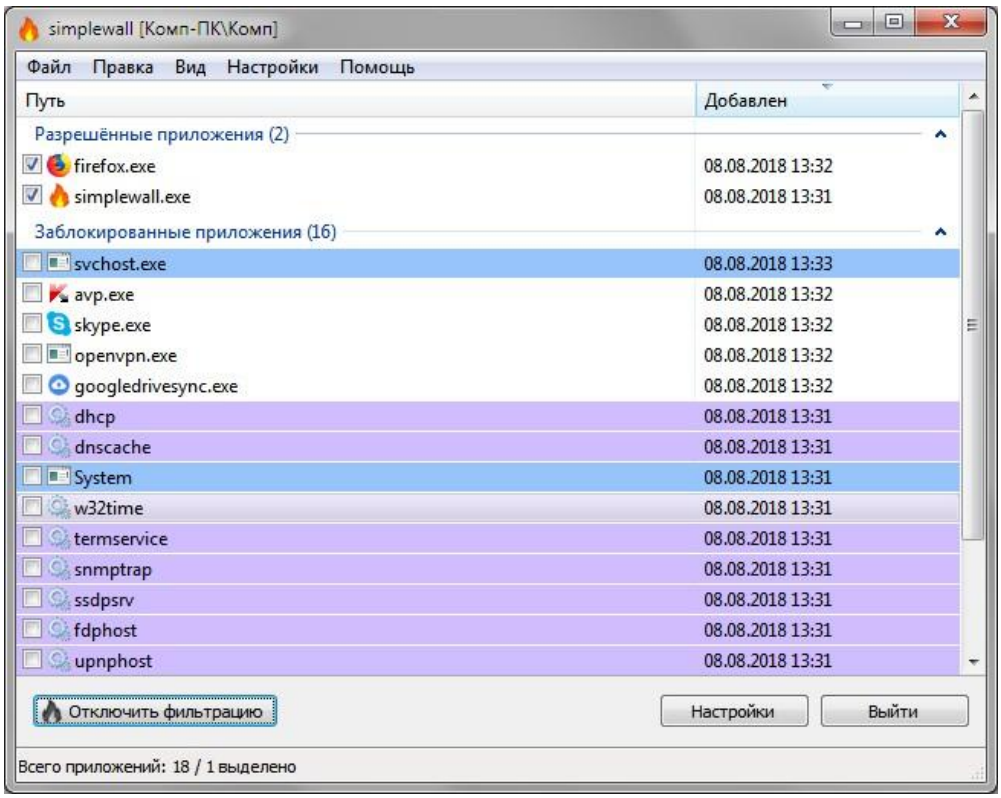

Рис. 5.1 Фільтрація Simplewall

У simplewall простий інтерфейс ділової програми - у ньому все у справі і без зайвих прикрас. В інтерфейсі перерахована вся мережна активність, з можливістю блокування доступу до інтернету будь-якої програми чи сервісу. Там є низка розділів з розсортованою інформацією про активність програм та сервісів, і користувачеві буде легко зорієнтуватися у тому, що відбувається. Програма включає ряд вбудованих правил, що блокують збір даних про користувача та подібну активність операційної системи та деяких програм.

Simplewall працює у Windows 7, 8, 8.1 та 10, має відкриті вихідні коди та важить менше мегабайта. Програма поширюється як у вигляді інсталяційного пакета, так і в Portable-версії (для потрібно створити simplewall.ini в директорії з програмою), що не потребує встановлення та дозволяє працювати прямо з флешки.

Що нового в simplewall 3.6.1:

- Підвищено швидкість запуску програми.
- Поліпшено підтримку DPI.
- Додано опцію для підтвердження дозволу роботи додатків.

- Додано фільтрацію списку програм.
- Реалізовано обхідний метод ініціалізації фаєрволу Windows.
- Додана фільтрація додатків та правил.
- Додано ім'я шару в балку.
- Список винятків перенесено на іншу сторінку налаштувань.
- Змінено значок створення правила.
- Оптимізовано сортування у списку.
- Дрібні косметичні виправлення.
- Виправлено безліч помилок.

Simplewall – крихітний захисник мережної активності, що дозволяє легко керувати службою фільтрації Windows (WFP).

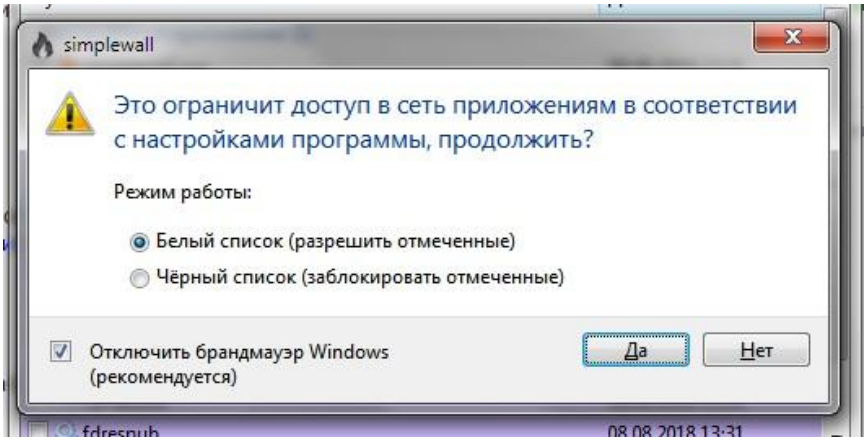

Рис.5.2 - «Білий список» Simplewall

Найнадійніший спосіб це «Білий список», спочатку блокується все, і коли якась програма «проситься» в інтернет, відразу створюється для нього правило, що дозволяє або забороняє.

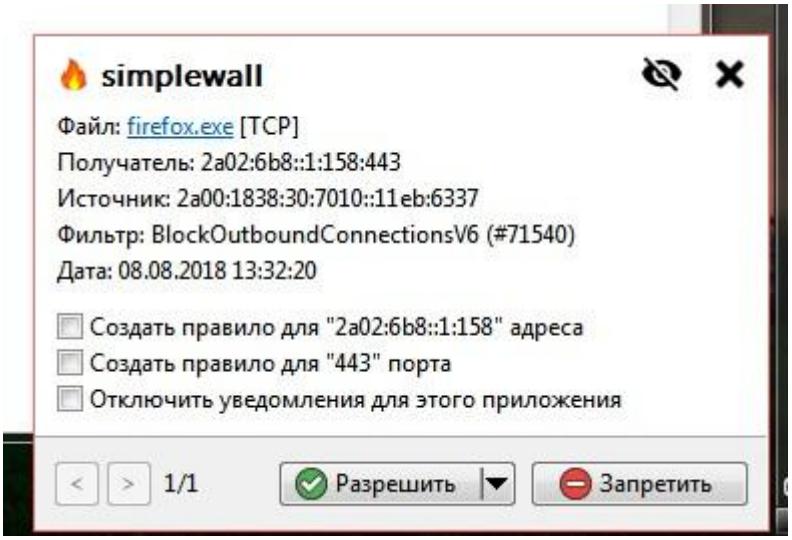

Рис.5.3 – Створення правила Simplewall

Очевидні переваги:

- Простий інтерфейс без дратівливих спливаючих вікон;
- редактор правил (створення власних правил);
- Внутрішні правила списку блокування (блокувати Windows spy/telemetry, тобто функції відстеження);
- У ручному режимі додавання файлів, процесів та служб до білого/чорного списку;
- Інформація про скинуті пакети з повідомленням та протоколюванням у файл;
- Інформація про дозволені пакети із записом у файл;
- Підтримка IPv6.

Фаєрвол Simplewall надає можливість застосування до будь-яких встановлених на комп'ютері програм та служб як системних, так і власних мережевих правил. Перші — це правила, які є у стандартному брандмауері Windows, звідки Simplewall їх імпортує і відображає у відповідній вкладці.

У списку власних мережевих правил фаєрволу спочатку є 8 їх одиниць. Будь-яке з них можна відредагувати, а при необхідності взагалі видалити. Користувач може створити необмежену кількість власних правил. Simplewall здатний блокувати активність додатків та служб за всіма затребуваними

мережевими протоколами: ICMP, IGMP, IPv4, IPv6, IPv6-ICMP, TCP, UDP, RDP, L2TP та SCTP.

Самі правила можуть мати різне написання (синтаксис), наприклад:

Вказівка IP-адрес та/або імен хостів (адреси сайтів) поодинці або через кому для блокування декількох одночасно. Також є можливість вказівки номерів через двокрапку після IP/імен хостів.

Вказує діапазон IP-адрес (також з можливістю вказівки блокованих портів).

Вказує діапазон блокованих мережних портів без IP-адрес або імен хостів.

Можливість використання методів безкласової IP-адресації як IPv4 CIDR, так і IPv6 CIDR (але це навряд чи стане в нагоді звичайним користувачам).

Створювані правила можуть мати глобальний характер (тобто. для всіх служб та додатків) або діяти лише на обрані користувачем елементи.

Моніторинг мережної активності

Програма Simplewall здатна відображати всі програми та системні служби (тут вони називається «сервісами», що є одне й те саме), хоча б раз звернулися до мережного інтерфейсу комп'ютера з моменту запуску фаєрволу. У відповідній вкладці програми користувач зможе ознайомитися з локальними та віддаленими IP-адресами, до яких зверталися програми та служби, використовувані ними типи мережевих протоколів та номери портів, а також поточний стан мережної активності.

Швидке блокування доступу до мережі

Фаєрвол Simplewall працює з програмами та службами окремо. За замовчуванням він блокує мережеву діяльність всіх запущених робіт. Тому користувач має не блокувати, а, навпаки, додавати їх до списку дозволених. Робиться це просто – достатньо встановити прапорець навпроти назв необхідних служб. Для зручності передбачена можливість додавання довіреного списку одночасно кількох елементів.

У випадку з програмами їх спочатку потрібно додати до списку контрольованих, що робиться з вкладки моніторингу їхньої мережної активності (також можливе додавання безлічі елементів одночасно).

У налаштуваннях основних параметрів можна змінити поведінку програми, запуск та оновлення. Далі за списком можна налаштувати інтерфейс та редагувати правила, та переглядати дозволені та заборонені пакети. Встановлення не потрібно, розпакували та запустили.

Легка програма для захисту системи від загроз з мережі, в парі з безкоштовним антивірусом (наприклад Kaspersky Free) буде надійним захистом для користувача, безкоштовно та ефективно.

В архіві, що додається до кваліфікаційної роботи, розміром близько 600 КБ, дві версії програми, для 32 та 64 бітних систем.

ВИСНОВКИ

У ході дипломної роботи проведено аналіз можливих загроз інформаційну безпеку користувачів послуг Інтернет. Розглянуто основні послуги мережі Інтернет, а також деструктивні фактори, існують у Мережі, та наслідки їх руйнівного впливу. Розглянуто класифікації, дано опис та характеристики найпоширеніших вірусів.

Дані описи та схеми підключення міжмережевих екранів, описані принципи роботи основних протоколів, що використовуються для захисту інформації та ПК.

Підсумовуючи, хотілося б підкреслити, що жодні апаратні, програмні та будь-які інші рішення не зможуть гарантувати абсолютну надійність та безпеку даних у комп'ютерних мережах. Водночас звести ризик втрат до мінімуму можливо лише за комплексного підходу до питань безпеки.

Незважаючи на широку поширеність антивірусних програм, віруси продовжують «плодитися». Щоб впоратися з ними, необхідно створювати більш універсальні та якісно-нові антивірусні програми, які включатимуть всі позитивні якості своїх попередників. На жаль, на даний момент немає такої антивірусної програми, яка б гарантувала захист від усіх різновидів вірусів на 100%, але деякі фірми, наприклад AntiVir на сьогоднішній день досягли непоганих результатів.

Що ж до брандмауерів, то за результатами численних тестів найкращим системою захисту мережі з використанням мережевих екранів з них був Simplewall.

Захищеність комп'ютера своєю чергою залежить від грамотності самого користувача, і лише за застосуванні всіх видів захисту можна досягти високого рівня безпеки комп'ютера, і, інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ньюман П. The Crash of the AT&T Network in 1990 [Електроний ресурс] // PhWorld: [сайт]. [2008]. URL: http://www.phworld.org/history/attcrash.htm
2. Колаковський Н. HP TouchPad Needs 6 to 8 Weeks for Additional Shipments [Електроний ресурс] // eWeek: [сайт]. [07]. URL: http://www.eweek.com/mobile/hp-touchpad-needs-6-to-8-weeks-for-additional-shipments
3. Netcraft Ltd. Web Server Survey [Електроний ресурс] // NetCraft: [сайт]. [2017]. URL: https://news.netcraft.com/archives/category/web-server-survey/
4. Говард М. IIS6 vs Apache2 Security Defects [Електроний ресурс] // Microsoft.com: [сайт]. [2004]. URL: https://blogs.msdn.microsoft.com/michael_howard/2004/10/15/iis6-vs-apache2-security-defects/
5. Говард М. Follow-up on IIS6 and Apache Security [Електроний ресурс] // Microsoft.com: [сайт]. [2004]. URL: https://blogs.msdn.microsoft.com/michael_howard/2004/10/18/follow-up-on-iis6-and-apache-security/
6. Google Inc. Google Testing Blog [Електроний ресурс] // GoogleBlog.com: [сайт]. URL: https://testing.googleblog.com/
7. softwaretestinghelp.com. Comprehensive Load Testing Tools List [Електроний ресурс] // Softwaretestinghelp: [сайт]. [2017]. URL: http://www.softwaretestinghelp.com/performance-testing-tools-load-testing-tools/
8. Брадтке Р. ISTQB 100 Success Secrets - ISTQB Foundation Certification Software Testing the ISTQB Certified Software Tester 100 Most Asked Questions. Emereo Publishing, 2008. 170 pp.
9. Microsoft Corporation. Performance Testing Guidance for Web Applications. ThriftBooks - Green Earth, 2007. 288 pp.
10. Байон Е. Performance Testing with Jmeter 2.9. ООО «Книга по Требованию», 2013. 138 pp.

11. Дохі Т., Накавага Т., та Стохастік Т. Reliability and Maintenance Modeling: Essays in Honor of Professor Shunji Osaki on his 70th Birthday. London: Springer, 2013. 360 pp.
12. Спілнер А., Лінз Т., Роснер Т., та Вінтер М. Software Testing Practice: Test Management: A Study Guide for the Certified Tester Exam ISTQB Advanced Level. Rocky Nook, 2007. 339 pp.
13. Колава А., Худжинга Д. Automated Defect Prevention: Best Practices in Software Management. Wiley-IEEE Computer Society Press, 2007.
14. Куджала С., "UX Curve: A method for evaluating long-term user experience," // Interacting With Computers, Vol. 23, No. 5, 2011.
15. IBM Design. Design in motion [Електроний ресурс] // IBM Design: [сайт]. [2015]. URL: http://www-01.ibm.com/software/ucd/designconcepts/ whatisUXD.html (дата звернення: 11.10.2017).
16. webstyleguide.com. Visual Design Web Style Guide 3 [Електроний ресурс] // Web Style Guide: [сайт]. [2015]. URL: http://webstyleguide.com/wsg3/7-page-design/3-visual-design.html (дата звернення: 11.10.2017).
17. Псомас С., "The Five Competencies of User Experience Design," // UX Matters, Листопад 2007.
18. Лонвгрен Д. Interaction Design - brief intro // Interaction Design. URL: http://www.interaction-design.org/encyclopedia/interaction_design.html
19. Маркус А. Design, User Experience, and Usability: Design Discourse. Springer, 2015. 672 pp.
20. Apache Foundation. Справочные материалы по программе JMeter [Електроний ресурс] // Сайт Apache Software Foundation: [сайт]. URL: https://jmeter.apache.org/ index.html (дата звернення: 5.11.2014).
21. Canonical Ltd. Ubuntu 16.04.3 LTS (Xenial Xerus) [Електроний ресурс] // Ubuntu.com: [сайт]. URL: https://wiki.ubuntu.com/XenialXerus/

ReleaseNotes?_ga=2.17724272.895013929.1508044866-1858907825.1508044866 (дата звернення: 15.10.2017).

22. Віксі П. MAN crontab [Електроний ресурс] // OpenNet.ru: [сайт]. URL: http://www.opennet.ru/man.shtml?topic=crontab&category=5 (дата звернення: 15.10.2017).
23. Oracle. Java SE Development Kit 9 [Електроний ресурс] // Oracle.com: [сайт]. URL: http://www.oracle.com/technetwork/java/javase/downloads/jdk9-downloads-3848520.html (дата звернення: 15.10.2017).
24. Вогель Л. REST with Java (JAX-RS) using Jersey [Електроний ресурс] // Jersey: [сайт]. [2017]. URL: http://www.vogella.com/tutorials/REST/article.html (дата звернення: 15.10.2017).
25. The Eclipse Foundation. Eclipse.com [Електроний ресурс] // Jetty HTTP Server: [сайт]. URL: https://www.eclipse.org/jetty/ (дата звернення: 15.10.2017).
26. Oracle. Why MySQL? [Електроний ресурс] // MySQL TM: [сайт]. URL: https://www.mysql.com/why-mysql/ (дата звернення: 15.10.2017).
27. Oracle. Java Docs (Oracle) [Електроний ресурс] // java.nio (Java SE7): [сайт]. URL: https://docs.oracle.com/javase/7/docs/api/java/nio/package-summary.html
28. Венерс Б. Object-Relational Mappings // Artima Developer. 2003. URL: http://www.artima.com/intv/abstract3.html (дата звернення: 2.12.2017).
29. MongoDB, Inc. What is MongoDB? [Електроний ресурс] // MongoDB: [сайт]. URL: https://www.mongodb.com/what-is-mongodb (дата звернення: 15.10.2017).