ЗМІСТ

ВСТУП

В наш час велику популярність набули глобальні мережі особливо Internet. І в зв'язку з цим виникли проблеми з захистом інформації. Питання захисту інформації стало невід'ємною частиною любої системи яка працює з комерційно значущою інформацією. При використанні Internet в комерційних межах а також для з'єднання частин компаній і організацій виникають проблеми захищеності інформації яка проходить через мережу і обмеження доступу зовнішніх користувачів до внутрішніх мереж. Захист інформації стоїть на першому місці по актуальності і поставлених задач.

Актуальність теми

Основною актуальністю захисту інформації в корпоративних мережах є запобігання викрадення інформації. Все більше і більше людей отримують доступ до мережі Internet, а хакерів і "script kiddes" на сьогоднішній день більше ніж колись. Питання захисту корпоративної мережі не варто відкладувати на майбутнє адже це може обернутись трагедією для компанії.

2 листопада 1988 року був зафіксованих перший випадок появи мережевого хробака, що паралізував роботу шести тисяч інтернет-вузлів в США. Це був хробак Морріса, названий в честь автора. Збиток від нього поніс близько 96 мільйонів доларів.

3 жовтня 1994 року Володимир Левін проник в внутрішню мережу американського банку Citibank зламавши аналогове підключення банку і отримав доступ до деяких рахунків, викравши при цьому майже 11 мільйонів доларів.

30 червня 1999 року Джеймс Джозеф атакував NASA. Він отримав доступ взломавши пароль сервера, що належав урядовій установі, розташованому в штаті Алабама. Ціна викраденого програмного забезпечення 1,7 мільйона доларів.

Гарі Мак Кіннон – переконаний що воєнні приховують докази про НЛО в 2002 році взламав комп'ютери що належали армії, ВМС, Міністерству оборони, ВВС і Пентагону. В загальному Мак Кіннон отримав доступ до 97 комп'ютерів.

20 лютого 2004 року в компанії Microsoft викрали вихідний код операційної системи Windows 2000, який згодом був викладений в мережу.

Інтернет став невід'ємною частиною і постійно розвиваючою мережею, яка змінила вид діяльності багатьох людей і організацій. Багато організацій були атаковані або зондів ані зловмисниками що привело до великих втрат. Мережі організацій що не знають або ігнорують ці проблеми піддають себе великому ризику бути атакованими зловмисниками.

Також є багато других причин, наприклад вразливість сервісів TCP/IP. Ряд сервісів TCP/IP можуть бути скомпрометовані зловмисниками, сервіси які використовуються для покращення управління мережею особливо вразливі.

Мета і завдання дослідження. Метою роботи є дослідження сучасних інформаційних загроз захищених корпоративних мереж. Завданнями дослідження є:

1. Виконати огляд сучасних та технологій захисту корпоративних 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 захищених корпоративних мереж.

Предмет дослідження - методи і засоби захисту корпоративних мереж.

Наукова новизна

- Виконано дослідження і аналіз найновіших методів та засобів захисту інформації в корпоративних 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 корпоративної мережі в залежності від рівня секретності інформації.

Апробація результатів роботи. Результати досліджень оприлюднені на XVII Международной заочной научно-практической конференции «Научная дискуссия: вопросы технических наук».

Публікації. Результати роботи опубліковані у збірнику тез XVII Международной заочной научно-практической конференции «Научная дискуссия: вопросы технических наук».

РОЗДІЛ 1
ОСНОВНІ ТЕОРЕТИЧНІ І МЕТОДОЛОГІЧНІ ПОЛОЖЕННЯ. КОНЦЕПЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Говорити про те, що інформаційна безпека стала частиною корпоративних мереж в нашій країні можна з великим сумнівом. Необхідність забезпечувати надійну безпеку інформації освідомили тільки великі компанії, але й вони до недавнього часу сприймали проблеми тільки з технічної сторони, яка була поставленна тільки з сторони встановлення програмного забезпечення для захисту інформації такого як антивірусного програмного забезпечання, міжмережевих екранів, програм для моніторингу мереж і виявлення вторгнень, несанкціонованого доступу і віртуальних частин мереж.

За рекомендаціями дослідницьких фірм, основним напрямком забезпечення безпеки слід спрямувати на розробку політики безпеки і супутніх їй документів. Політика безпеки є найдешевшим і одночасно найефективнішим засобом забезпечення інформаційної безпеки. Крім того, якщо політика сформульована, то вона є і керівництвом щодо розвитку і вдосконалення системи захисту.

1.1 Загальні положення концепції інформаційної безпеки

Основна мета концепції - визначення методів і засобів захисту та забезпечення безпеки інформації, що відповідають інтересам, вимогам і законодавству України в сучасних умовах необхідності використання ресурсів глобальних мереж передачі даних загального користування для побудови корпоративних захищених і безпечних мереж.

Концепція формулює науково-технічні принципи побудови систем забезпечення безпеки інформаційних ресурсів корпоративних мереж з урахуванням сучасних тенденцій розвитку мережевих інформаційних технологій, розвитку видів мережевих протоколів, їх взаємної інкапсуляції та спільного використання.

Основною сучасною тенденцією розвитку мереж зв'язку є їх глобалізація, ускладнення та інтеграція. Інтеграція мережевих і комунікаційних технологій полягає у спільному використанні та інтеграції різноманітних мережевих протоколів, у взаємному використанні комунікаційними провайдерами ресурсів і засобів передачі даних і стикуванні транспортних і сервісних послуг.

Ускладнення мережевих технологій пов'язаний з розробкою нових функціональних протоколів зв'язку і передачі інформації, забезпечують більш якісний, і надійний зв'язок, збільшення обсягів і швидкості переданої інформації. Наприклад, для підвищення безпеки передачі інформації був розроблений протокол IPSEC, який входить в нову версію протоколу IPv6.

Тенденція глобалізації визначається необхідністю об'єднання і взаємного використання інформаційних ресурсів, розташованих у віддалених районах і країнах. Ці три основні тенденції розвитку мережевих інформаційних технологій призводять до четвертої і визначальної тенденції: «Ефективне і гнучке управління безпекою та захистом переданої і оброблюваної інформації засобами централізовано-розподіленого управління».

Ефективна інтеграція неможлива без взаємної довіри і гарантій з безпеки інформації комунікаційних провайдерів. В іншому випадку, інтеграція призводить до фінансових і моральних втрат однієї зі сторін та організаційному руйнування мережі.

Зростання складності комунікаційних технологій призводить до необмеженого росту загроз безпеки інформації, що в умовах відсутності кваліфікованої та гарантованої система забезпечення безпеки інформаційних ресурсів корпоративних мереж призводить до функціонального руйнування мережі.

Глобалізація передбачає різке збільшення числа взаємодіючих суб'єктів обміну інформацією, що при відсутності керованої системи захисту інформації гарантує зворотній від бажаного ефект - гарантії з несанкціонованого доступу і перетворенню цінної для клієнтів інформації в марно перекачуєме інформаційне сміття.

1.2 Визначення корпоративної мережі. Особливості корпоративних мереж

Корпоративна мережа - взаємопов'язана сукупність мереж, служб передачі даних і Телеслужби, призначена для надання єдиного захищеного мережевого простору обмеженому рамками корпорації колу користувачів.

Основними особливостями корпоративних мереж є:

1. Використання того ж інструментарію, що і при роботі з мережею передачі даних загального користування.

2. Доступ до інформації надається тільки обмеженій групі клієнтів у внутрішній мережі організації. Внутрішня мережа представляє з себе локальну мережу, відокремлену від глобальних мереж міжмережевими екранами.

3. Циркулює інформація трьох типів: офіційна (поширення якої офіційно санкціонується і заохочується на рівні організації), проектна або групова (призначена для використання окремою групою співробітників, як правило, підлягає захисту) і неофіційна (особиста папка або каталог на сервері, службовим сховищем статей, заміток і ідей, з якими можна поділитися з іншими співробітниками підприємства в спільних інтересах для обміну зауваженнями чи якихось інших цілей.

4. Наявність централізованої системи управління (ефективністю функціонування, безпекою, живучістю) корпоративною мережею.

Для існуючих корпоративних автоматизованих систем властиво:

1. Використання корпораціями розподіленої моделі обчислень. Однак в останні 5-10 років у нашій країні і за кордоном набирають популярність технології тонкого клієнта.

2. Невіддільність корпоративних додатків від функціональних підрозділів корпорації, оскільки частина прикладного коду розташовується на станції-клієнті.

3. Необхідність одночасного контролю декількох локальних обчислювальних мереж, необхідність обміну центральній консолі повідомленнями з платформами адміністрування.

4. Широкий спектр використовуваних способів подання, зберігання і передачі інформації.

5. Інтеграція даних різного призначення, що належать різним суб'єктам, в рамках єдиних баз даних. І розміщення необхідних деяким суб'єктам даних у віддалених вузлах мережі (приклад, текстові звіти, збережені на робочих станціях).

6. Абстрагування власників даних від фізичних структур і місця розміщення даних.

7. Участь у процесі автоматизованої обробки інформації великої кількості користувачів і персоналу різних категорій. Безпосередній і одночасний доступ до ресурсів (у тому числі і інформаційним) великої кількості користувачів (суб'єктів доступу) різних категорій.

8. Високий ступінь різнорідності засобів обчислювальної техніки і зв'язку, а також програмного забезпечення.

9. Відсутність спеціальної програмно-апаратної підтримки засобів захисту у функціональних технічних засобах, які у системі.

1.3 Класифікаційні ознаки корпоративних мереж

Відповідно до введеним визначенням корпоративної мережі її склад в загальному випадку утворюють такі функціональні елементи:

Робочі місця (абоненти) корпорації, які можуть бути:

- зосередженими, або розташовуватися в рамках однієї будівлі;
- розподіленими, або розосередженими на деякій в загальному випадку необмежено великій території.

Інформаційні сервери корпорації, призначені для зберігання і обробки інформаційних масивів (баз даних) різного функціонального призначення. Вони також можуть бути зосередженими або розподіленими на великій території корпорації.

Засоби телекомунікації, що забезпечують взаємодію між собою робочих станцій та їх взаємодія з інформаційним серверами. Засоби телекомунікації в рамках корпорації можуть бути:

- виділеними (або орендованими), які є приналежністю корпорації;
- загального призначення (існуючі поза корпорацією мережі зв'язку, кошти яких використовуються корпорацією). Це кошти існуючих мереж загального користування.

У рамках корпорації інформаційний вплив може бути реалізовано в рамках однієї (телефонія, телетекст, відеотекст, телефакс); або декількох служб (інтеграція служб), що має забезпечуватися відповідними засобами телекомунікації та абонентських закінчень.

Система управління ефективністю функціонування корпоративної мережі. Залежно від реалізованого набору служб в корпоративній мережі повинні використовуватися свої засоби управління мережею, зокрема кошти маршрутизації і комутації; засоби адміністрування, реалізовані з метою ефективного використання мережевих ресурсів. По можливості управління елементами корпоративної мережі можна виділити:

- керовані в рамках корпорації функціональні елементи (це власні, або додатково вводяться в рамках корпоративної мережі засоби);
- чи не керовані в рамках корпорації функціональні елементи, (зокрема, маршрутизатори і комутатори), які є приналежністю використовуваних корпорацією підмереж загального призначення.

Система управління безпекою функціонування корпоративної мережі. У корпоративній мережі повинні бути реалізовані необхідні мережеві служби безпеки, повинні використовуватися відповідно засоби безпеки.

Система забезпечення надійності корпоративної мережі. Повинні бути передбачені засоби забезпечення працездатності всеї мережі, або її фрагментів при відмовах елементів мережі.

Система діагностики та контролю. В рамках корпоративної мережі повинні бути передбачені засоби контролю працездатності окремих функціональних елементів, система збору інформації про відмови і збої та

надання її систем забезпечення живучості; управління ефективністю функціонування; управління безпекою. Для корпоративної мережі повинні бути розроблені засоби діагностики, реалізовані як в процесі функціонування мережі, так і профілактично.

Система експлуатації. Крім перерахованих функціональних елементів, корпоративні мережі зв'язку повинні мати план (гіпотезу) процесу розвитку, великою мірою визначають закладені в неї функціональні можливості, зокрема на рівні протоколів взаємодії мережевих компонентів і можливості їх інтеграції.

Узагальнюючи введені ознаки корпоративних мереж, отримаємо можливу їх 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.

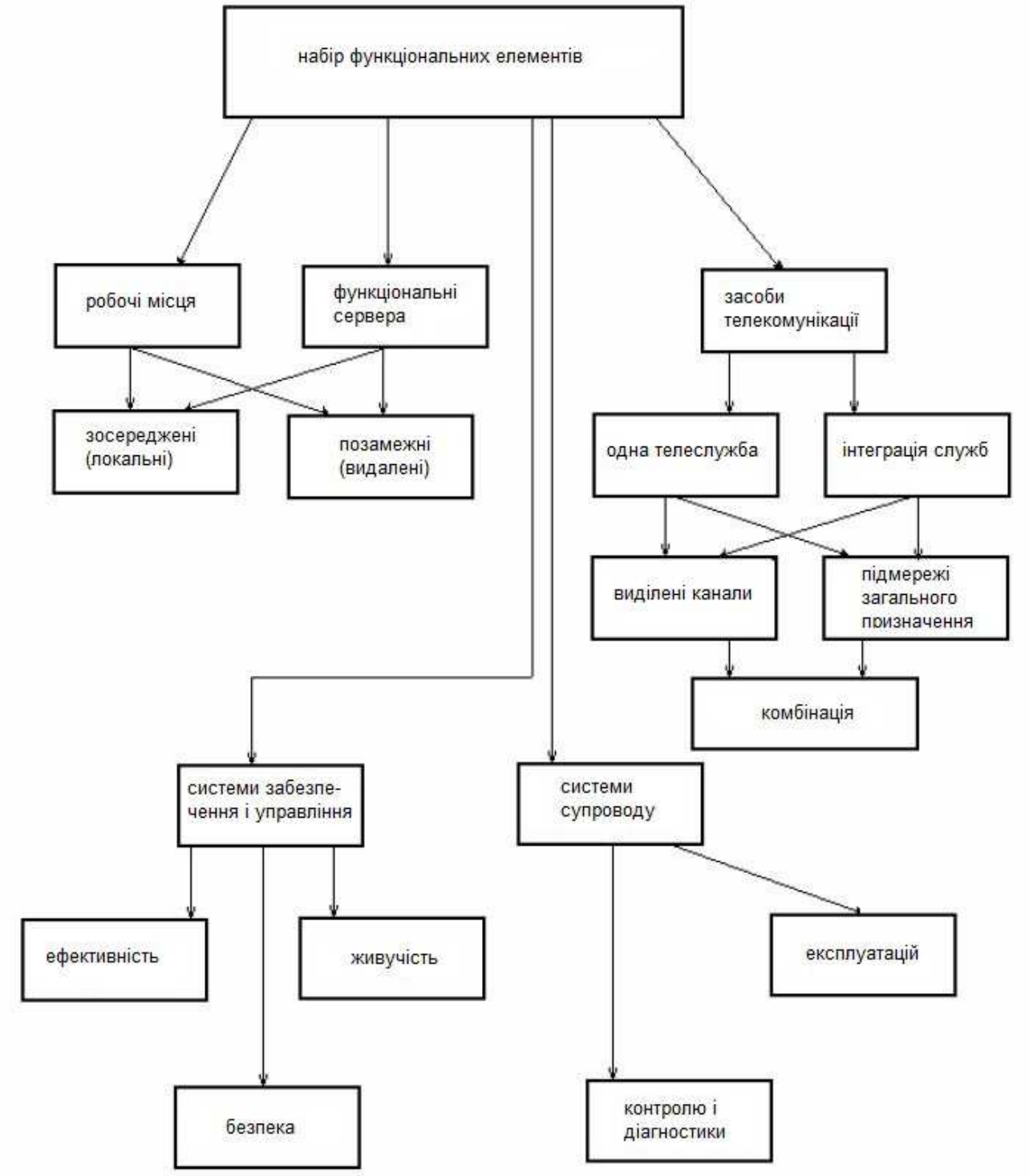

Рис. 1.1. Функціональні компоненти корпоративних мереж

Рис. 1.2. Класифікація по ієрархії управління

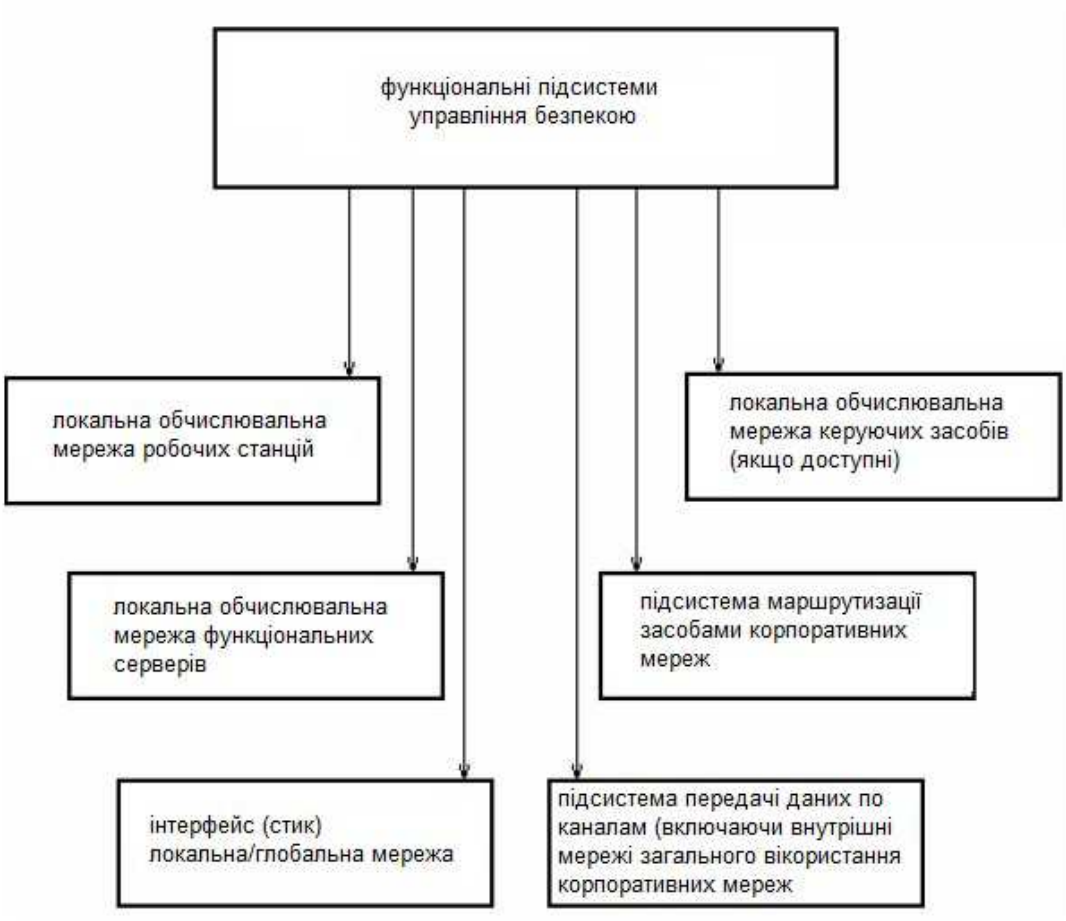

Рис.1.3 Класифікація функціональних підсистем управління безпекою

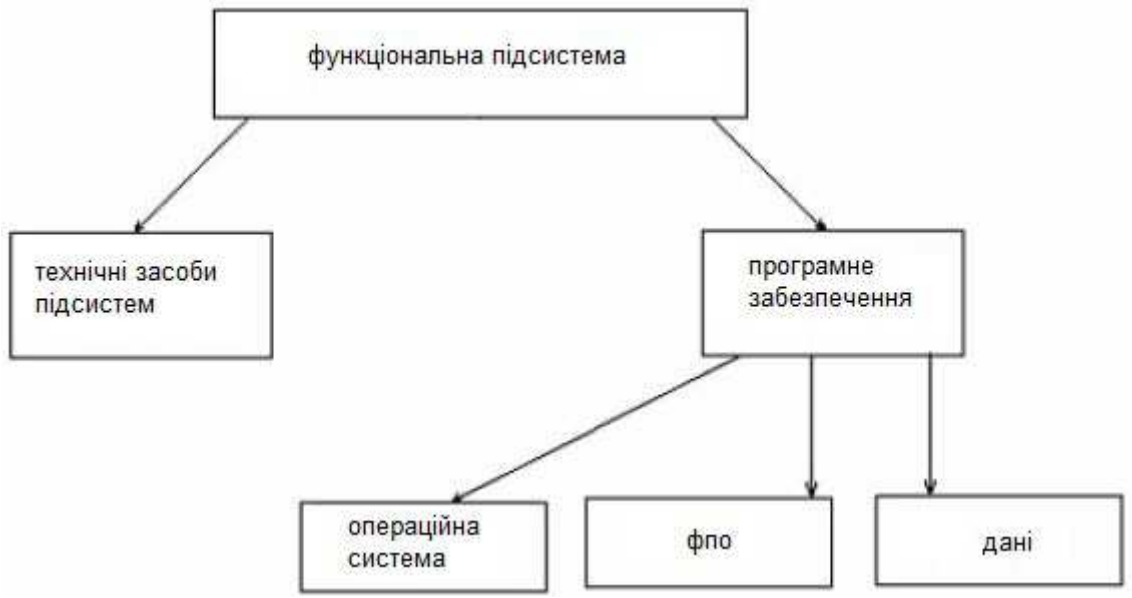

Рис. 1.4. Елементи функціональної підсистеми

1.4 Узагальнена структура корпоративної мережі. Загальні вимоги до адміністрування мережі

З урахуванням введених класифікаційних ознак можна отримати деяку узагальнену структуру корпоративної мережі, яка наведена на рисунку 1.5. Практично будь-яка корпоративна мережа буде містити фрагменти наведеної узагальненої структури. У рамках даної мережі повинна бути реалізована вторинна мережа зв'язку - система управління, представлена на рисунку 1.6. Тут також можуть використовуватися виділені канали (пунктир на рисунку 1.5 позначає функціональний зв'язок - фізичний канал проходить через засоби маршрутизації, захисту тощо (рис. 1.6)). В основі системи управління корпоративної мережі повинні лежати такі принципи:

- суміщення адміністрування окремих функціональних підсистем (питання ефективності не може вирішуватися поза розгляду питання живучості мережі, а питання безпеки без обліку ефективності та живучості (іншими словами, при зміні рівня безпеки, наприклад, змінюється і ефективність, що має бути враховано);
- централізоване/розподілене адміністрування, припускає, що основні завдання адміністрування повинні вирішуватися з центру (основний фрагмент

мережі); вторинні завдання (наприклад, в рамках віддалених фрагментів) засобами управління окремих підсистем;

- в рамках керуючої системи повинні бути реалізовані функції системи автоматичного управління. З метою підвищення оперативності реакції системи управління на особливо важливі події, в системі повинна реалізуватися автоматична обробка особливо важливих впливів;
- в рамках системи безпеки повинен бути реалізоване адаптивне управління безпекою адекватною зміною відповідних подій (наприклад, система виявлення атак може блокувати локальний порт в разі атаки типу «відмова в обслуговуванні»).
- для підвищення ефективності і надійності системи управління необхідно передбачити експертну систему – систему «підказок» для вироблення управляючих впливів на різні події.

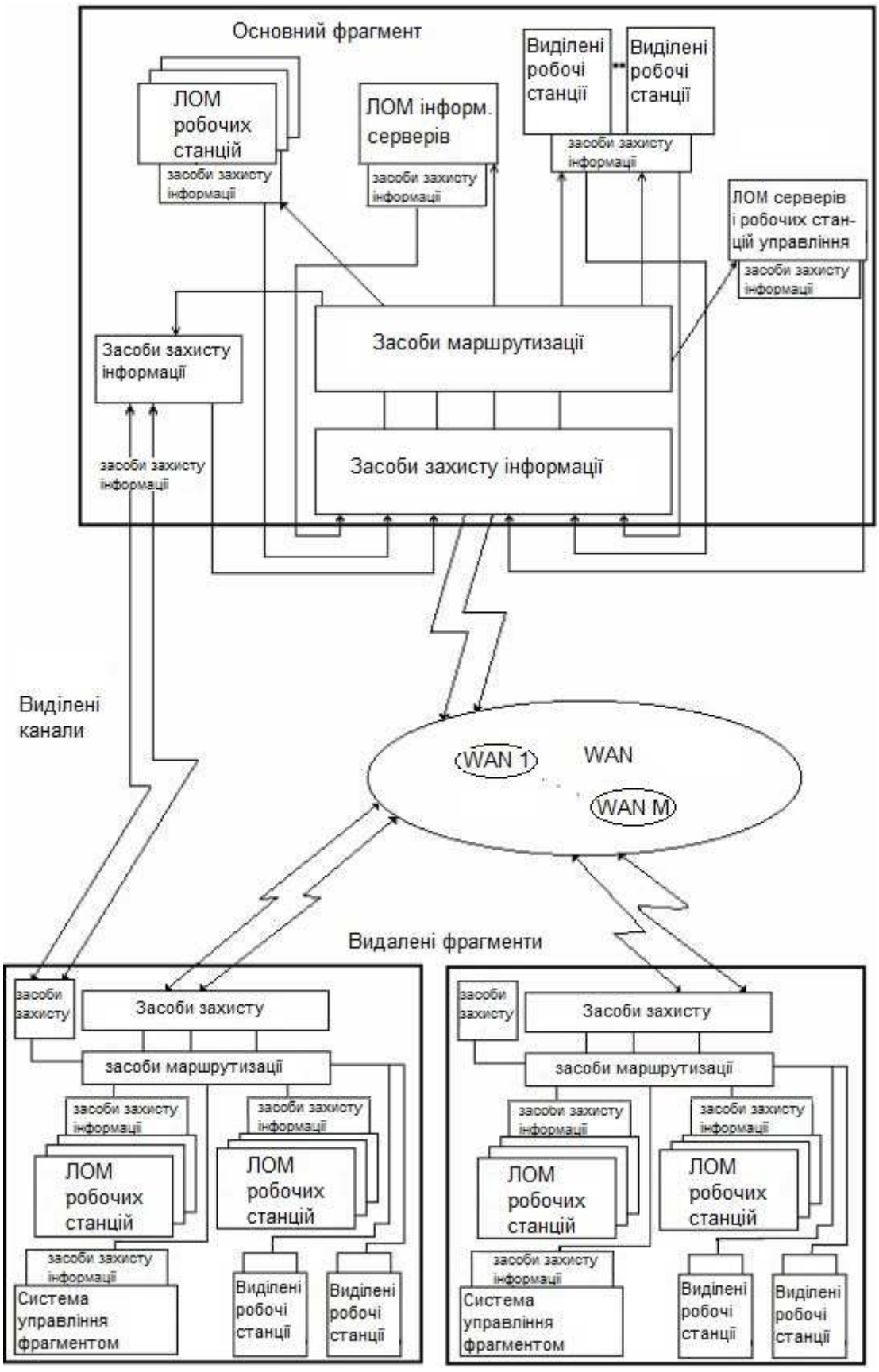

Рис. 1.5. Узагальнена структура корпоративної мережі

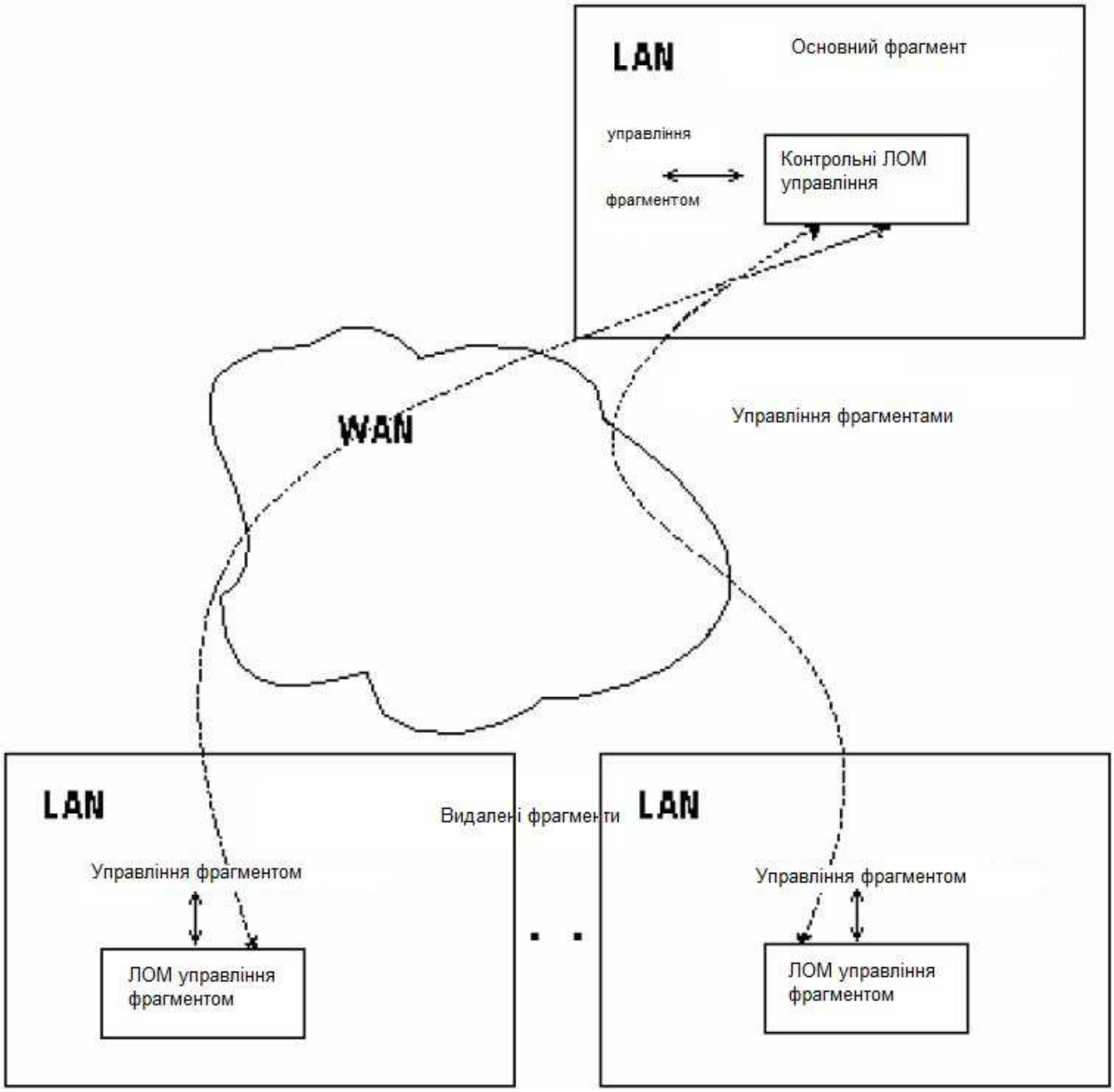

Рис. 1.6. Система управління корпоративною мережею

На рисунку 1.5 проілюстрований загальний випадок, який відрізняється тим, що структури основного та віддаленого фрагментів збігаються (по функціям вони різні - в основному фрагменті реалізується централізоване управління мережею зв'язку). Як правило, дані фрагменти мають різну складність. При цьому слід зазначити, що спрощення структури мережі полягає в частині зменшення складності віддалених фрагментів, з перенесенням відповідних функцій на елементи основного фрагмента, (відповідно з його ускладненням), що, перш за все, має місце для наступних елементів:

- інформаційні сервери (з точки зору забезпечення безпеки мережі має сенс сконцентрувати всі інформаційні сервери, забезпечуючи для них необхідний захист організаційними і технічними заходами);

- адміністрування всіма функціональними підсистемами для корпоративних мереж, що використовують обмежену кількість додаткових засобів реалізації функціональних підсистем (наприклад, маршрутизаторів) може бути сконцентровано в основному фрагменті;

- підключення до загальнодоступних сервісів (мережа Інтернет) здійснюється з виділених робочих місць основного фрагмента (тут використовуються відповідні засоби захисту, підключення до глобальних мереж у загальному випадку відмінні від інших).

1.5 Структура управління безпекою мережі. Основні вимоги

Система забезпечення безпеки інформації повинна мати багаторівневу структуру і включати наступні рівні:

- рівень захисту автоматизованих робочих місць (АРМ);
- рівень захисту локальних мереж та інформаційних серверів;
- рівень захисту корпоративної АС.

На рівні захисту автоматизованих робочих місць повинна здійснюватися ідентифікація та аутентифікація користувачів операційної системи. Повинно здійснюватися управління доступом: надання доступу суб'єктів до об'єктів відповідно до матрицею доступу, виконання реєстрації та обліку всіх дій суб'єкта доступу в журналах реєстрації. Повинна бути забезпечена цілісність програмного середовища, періодичне тестування засобів захисту інформації. Такі засоби захисту повинні володіти гнучкими засобами налаштування і можливістю віддаленого адміністрування.

Рівень захисту локальних мереж і мережевих серверів повинен забезпечувати:

- ідентифікацію користувачів і встановлення автентичності доступу в систему, до компонентів;

- захист аутентифікаційних даних;
- встановлення аутентичності при доступі до серверів;
- пропуск аутентификаційної інформації від одного компонента до іншого без перевстановлення аутентичності доступу.

Механізми захисту повинні бути здатні створювати, обслуговувати (підтримувати) і захищати від модифікації або неправомірного доступу або руйнування аутентифікаційні інформацію і матрицю доступу до об'єктів.

Повинна здійснюватися реєстрація наступних подій:

- використання ідентифікаційних і аутентифікаційних механізмів;
- дії користувачів з критичними об'єктами;
- знищення об'єктів;
- дії, вжиті операторами та адміністраторами системи та/або офіцерами безпеки;
- інші випадки безпеки.

Параметри реєстрації:

- дата і час події;
- користувач;
- тип випадку;
- успішна або неуспішна спроба для ідентифікації/аутентифікації додатково;
- походження запиту (наприклад, локальна або мережева аутентифікації);

для випадків знищення об'єктів і доставки інформації в місце адреси користувача назва об'єкта.

Адміністратор системи повинен бути здатний вибірково контролювати дії будь-якого користувача або групи користувачів на підставі індивідуальної ідентичності.

Засоби захисту інформації повинні мати модульну структуру, кожен модуль повинен підтримувати область пам'яті для власного виконання. Для кожного модуля системи захисту інформації, кожного компонента системи захисту інформації, розділеного в автоматизовану систему, повинна

забезпечуватися ізоляція ресурсів, що потребують захисту так, щоб вони підкорялися контролю доступу і вимогам ревізії.

Періодичне тестування правильності функціонування апаратних засобів, мікропрограмних елементів і програмного забезпечення систем захисту інформації.

При поділі систем захисту інформації повинна забезпечуватися здатність повідомлення адміністративному персоналу про відмови, помилки, спробах несанкціонованого доступу, виявлених в розділених компонентах систем захисту інформації. Протоколи, здійснені в межах систем захисту інформації, повинні бути розроблені так, що повинно забезпечуватися правильне функціонування у випадку відмов (збоїв) комунікаційної мережі або її індивідуальних компонентів.

Механізми безпеки повинні бути перевірені і функціонувати відповідно до вимог документації. Рівень захисту корпоративної автоматизованої системи повинен гарантувати:

1. Цілісність передачі інформації від її джерел до адресата:

- аутентифікацію;
- цілісність комунікаційного поля;
- неможливість відмови партнерів по зв'язку від факту передачі або прийому повідомлень.

2. Безвідмовність у наданні послуг:

- безперервність функціонування;
- стійкість до атак типу «відмова в обслуговуванні»;
- захищений протокол передачі даних.

3. Захист від несанкціонованого розкриття інформації:

- збереження конфіденційності даних за допомогою механізмів шифрування;
- вибір маршруту передачі.

Засоби захисту повинні забезпечувати:

- конфіденційність змісту (відправник повинен бути упевнений, що ніхто не прочитає повідомлення, крім певного одержувача);

- цілісність змісту (одержувач повинен бути впевнений, що зміст повідомлення не модифіковано);
- цілісність послідовності повідомлень (одержувач повинен бути впевнений, що послідовність повідомлень не змінена);
- аутентифікацію джерела повідомлень (відправник повинен мати можливість аутентифицироваться у одержувача як джерело повідомлення, а також у будь-якого пристрою передачі повідомлень, через який вони проходять);
- доказ доставки (відправник може переконатися в тому, що повідомлення доставлено неспотвореним потрібного одержувачу);
- доказ подачі (відправник може переконатися в ідентичності пристрою передачі повідомлення, на яке воно передано);
- безвідмовність джерела (дозволяє відправникові довести одержувачу, що передане повідомлення належить йому);
- безвідмовність надходження (дозволяє відправникові повідомлення отримати від пристрою передачі повідомлення, на яке воно надійшло, доказ того, що повідомлення надійшло на це пристрій для доставки визначеному одержувачу);
- безвідмовність доставки (дозволяє відправникові отримати від одержувача доказ отримання ним повідомлення);
- управління контролем доступу (дозволяє двом компонентам системи обробки повідомлень встановити безпечне з'єднання);
- захист від спроб розширення своїх законних повноважень (на доступ, формування, розподіл і т.п.), а також зміни (без санкції на те) повноважень інших користувачів;
- захист від модифікації програмного забезпечення шляхом додавання нових функцій.

1.6 Аналіз рівня захищеності корпоративної інформаційної системи. Поняття захищеності АС

При створенні інформаційної інфраструктури корпоративної автоматизованої системи (АС) на базі сучасних комп'ютерних мереж неминуче виникає питання про захищеність цієї інфраструктури від загроз безпеки інформації. А саме: наскільки адекватні реалізовані в АС механізми безпеки існуючим ризикам; чи можна довіряти цій АС обробку (зберігання, передачу) конфіденційної інформації; чи є в поточній конфігурації АС помилки, що дозволяють потенційним зловмисникам обійти механізми контролю доступу; чи містить встановлене в АС програмне забезпечення (ПЗ) уразливості, які можуть бути використані для злому захисту; як оцінити рівень захищеності АС і як визначити чи є він достатнім в даному середовищі функціонування; які контрзаходи дозволять реально підвищити рівень захищеності АС; на які критерії оцінки захищеності слід орієнтуватися і які показники захищеності використовувати. Такими питаннями рано чи пізно задаються всі фахівці IT-відділів, відділів захисту інформації та інших підрозділів, відповідають за експлуатацію та супровід АС. Відповіді на ці питання далеко неочевидні. Аналіз захищеності АС від загроз безпеки інформації є не простою задачею. Уміння оцінювати і управляти ризиками, знання типових загроз і вразливостей, критеріїв і підходів до аналізу захищеності, володіння методами аналізу та спеціалізувати інструментарієм, знання різних програмно-апаратних платформ, що використовуються в сучасних комп'ютерних мережах - ось далеко не повний перелік професійних якостей, якими повинні володіти фахівці, провідні роботи з аналізу захищеності АС. Аналіз захищеності є основним елементом таких взаємно пересічних видів робіт як атестація, аудит та обстеження безпеки АС.

Захищеність є одним з найважливіших показників ефективності функціонування АС, поряд з такими показниками як надійність, відмовостійкість, продуктивність і т. п. Під захищеністю АС будемо розуміти ступінь адекватності реалізованих в ній механізмів захисту інформації

існуючим в даному середовищі функціонування ризикам, пов'язаним з здійсненням погроз безпеки інформації [1]. Під погрозами безпеки інформації традиційно розуміється можливість порушення таких властивостей інформації, як конфіденційність, цілісність і доступність.

На практиці завжди існує велика кількість непіддатних точній оцінці можливих шляхів здійснення загроз безпеки в відносно ресурсів АС. В ідеалі кожен шлях здійснення загрози повинен бути перекритий відповідним механізмом захисту. Дане умова є першим фактором, що визначає захищеність АС. Другим чинником є міцність існуючих механізмів захисту, що характеризується ступенем опірності цих механізмів спробам їх обходу або подолання. Третім фактором є величина збитку, що наноситься власникові АС у разі успішного здійснення загроз безпеки.

На практиці отримання точних значень наведених характеристик утруднено, так як поняття загрози, збитку і опірності механізму захисту тяжко формулюючі. Наприклад, оцінку збитку в результаті несанкціонованого доступу до інформації політичного та військового характеру точно визначити взагалі неможливо, а визначення вірогідності здійснення загрози не може базуватися на статистичному аналізі. Оцінка ступеня опірності механізмів захисту завжди є суб'єктивною.

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:

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.

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

Положення про технічний захист інформації в Україні

1. Це Положення визначає правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства.

Технічний захист інформації здійснюється щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ, організацій (далі - органи, щодо яких здійснюється ТЗІ).

2. Ужиті в цьому Положенні терміни мають таке значення:

- конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення;
- цілісність - властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;
- доступність - властивість інформації бути захищеною від несанкціонованого блокування;
- технічний захист інформації (ТЗІ) - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;
- інформаційна система - автоматизована система, комп'ютерна мережа або система зв'язку;
- дозвіл - документ, що надає право на виконання робіт з технічного захисту інформації для власних потреб;
- комплекс технічного захисту інформації - сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті.

3. Правову основу технічного захисту інформації в Україні становлять Конституція України (254к/96-ВР), закони України, акти Президента України та

Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України, з питань технічного захисту інформації, а також це Положення. {Пункт 3 із змінами, внесеними згідно з Указом Президента N333/2008 (333/2008) від 11.04.2008}

4. Державна політика технічного захисту інформації формується згідно із законодавством і реалізується Державною службою спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку України) у взаємодії з органами, щодо яких здійснюється ТЗІ. {Пункт 4 із змінами, внесеними згідно з Указом Президента N333/2008 (333/2008) від 11.04.2008}

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

6. Організаційно-технічні принципи, порядок здійснення заходів з технічного захисту інформації, порядок контролю у цій сфері, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації, порядок атестації та експертизи комплексів технічного захисту інформації визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами.

Нормативно-правові акти з технічного захисту інформації є обов'язковими для виконання всіма суб'єктами системи технічного захисту інформації.

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-дослідні та науково-виробничі установи Держспецзв'язку України, державні підприємства, що перебувають в управлінні Держспецзв'язку України та виконують завдання з питань технічного захисту інформації; {Абзац четвертий пункту 8 в редакції Указу Президента N333/2008 (333/2008) від 11.04.2008}

- військові частини, підприємства, установи та організації всіх форм власності й громадяни-підприємці, які провадять діяльність з технічного захисту інформації за відповідними дозволами або ліцензіями;

- навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців з технічного захисту інформації.

{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 органів, щодо яких здійснюється ТЗІ, є:

- забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів з питань технічного захисту інформації;

- видання у межах своїх повноважень нормативно-правових актів із зазначених питань;

- здійснення контролю за станом технічного захисту інформації.

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

- створюють або визначають підрозділи, на які покладається забезпечення технічного захисту інформації та контроль за його станом, узгоджують 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;
- забезпечують підготовку, перепідготовку та підвищення кваліфікації кадрів з технічного захисту інформації;
- 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}

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}

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 будь-яких стандартизованих методик аналізу захищеності АС, тому в конкретних ситуаціях алгоритми дій аудиторів можуть істотно різнитися. Однак типову методику аналізу захищеності корпоративної мережі запропонувати таки можливо. І хоча дана методика не претендує на загальність, її ефективність багаторазово перевірена на практиці.

Типова методика включає використання наступних методів:

- вивчення вихідних даних по АС;
- оцінка ризиків, пов'язаних із здійсненням погроз безпеки в відносно ресурсів АС;
- аналіз механізмів безпеки організаційного рівня, політики безпеки організації і організаційно-розпорядчої документації щодо забезпечення режиму інформаційної безпеки та оцінка їх відповідності вимогам існуючих нормативних документів, а також їх адекватності існуючим ризикам;
- ручний аналіз конфігураційних файлів маршрутизаторів, МЕ і проксі - серверів, які здійснюють управління міжмережевими взаємодіями, поштових і DNS серверів, а також інших критичних елементів мережевої інфраструктури;
- сканування зовнішніх мережевих адрес ЛОМ з мережі Інтернет;
- сканування ресурсів ЛОМ зсередини;
- аналіз конфігурації серверів і робочих станцій ЛОМ за допомогою спеціалізованих програмних засобів.

Перераховані методи дослідження припускають використання як активного, так і пасивного тестування системи захисту. Активне тестування системи захисту полягає в емуляції дій потенційного зловмисника з подолання механізмів захисту. Пасивне тестування передбачає аналіз конфігурації ОС і додатків за шаблонами з використанням списків перевірки. Тестування може проводитися вручну або з використанням спеціалізованих програмних засобів.

1.9 Вихідні дані обстежуваної АС

Відповідно до вимог про технічний захист інформації в Україні при проведенні робіт з атестації безпеки АС, що включають в себе попереднє обстеження та аналіз захищеності об'єкта інформатизації, замовником робіт повинні бути надані наступні вихідні дані:

1. Повне і точне найменування об'єкта інформатизації та його призначення.

2. Характер (науково-технічна, економічна, виробнича, фінансова, військова, політична) інформації і рівень секретності (конфіденційності) оброблюваної інформації визначено в відповідності до деяких переліків (державним, галузевим, відомчим, підприємства).

3. Організаційна структура об'єкта інформатизації.

4. Перелік приміщень, складу комплексу технічних засобів (основних і допоміжних), що входять в об'єкт інформатизації, у яких (на яких) обробляється зазначена інформація.

5. Особливості та схема розташування об'єкта інформатизації з зазначенням меж контрольованої зони.

6. Структура програмного забезпечення (загальносистемного і прикладного), використовуваного на атестуються об'єкті інформатизації і призначеного для обробки інформації, що захищається, використовувані протоколи обміну інформацією.

7. Загальна функціональна схема об'єкта інформатизації, включаючи схему інформаційних потоків та режими обробки захищається інформації.

8. Наявність і характер взаємодії з іншими об'єктами інформатизації.

9. Склад і структура системи захисту інформації на атестуючому об'єкті інформатизації.

10. Перелік технічних і програмних засобів в захищеному виконанні, засобів захисту та контролю, що використовуються на атестуючому об'єкті інформатизації та мають відповідний сертифікат, припис на експлуатацію.

11. Відомості про розробників системи захисту інформації, наявність у сторонніх розробників (стосовно підприємства, на якому розташований атестуючий об'єкт інформатизації) ліцензій на проведення подібних робіт.

12. Наявність на об'єкті інформатизації (на підприємстві, на якому розташований об'єкт інформатизації) служби безпеки інформації, служби адміністратора (автоматизованої системи, мережі, баз даних).

13. Наявність і основні характеристики фізичного захисту об'єкта інформатизації приміщень, де обробляється захищена інформація і зберігаються інформаційні носії).

14. Наявність і готовність проектної та експлуатаційної документації на об'єкт інформатизації та інші вихідні дані по аттестуючому об'єкту інформатизації, що впливають на безпеку інформації.

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

При аналізі конфігурації засобів захисту зовнішнього периметра ЛОМ та управління міжмережевими взаємодіями особливу увагу звертається на наступні аспекти, які визначаються їх конфігурацією:

- налаштування правил розмежування доступу (правил фільтрації мережевих пакетів) на МЕ і маршрутизаторах;
- використовувані схеми та налаштування параметрів аутентифікації;
- налаштування параметрів системи реєстрації подій;
- використання механізмів, що забезпечують приховування топології мережі, що захищається, включають у себе трансляцію мережевих адрес (NAT);
- налагодження механізмів оповіщення про атаки та реагування;
- наявність і працездатність засобів контролю цілісності;
- версії використовуваного ПЗ та наявність встановлених пакетів програмних корекцій.

Тестування системи захисту АС проводиться з метою перевірки ефективності використовуваних в ній механізмів захисту, їх стійкості щодо

можливих атак, а також з метою пошуку вразливостей в захисті. Традиційно використовуються два основні методи тестування:

- тестування за методом «чорного ящика»;
- тестування за методом «білого ящика».

Тестування за методом «чорного ящика» передбачає відсутність у тестуючої сторони будь-яких спеціальних знань про конфігурацію і внутрішню структуру об'єкта випробувань. При цьому проти об'єкта випробувань реалізуються всі відомі типи атак і перевіряється стійкість системи захисту щодо цих атак. Використовувані методи тестування емулюють дії потенційних зловмисників, що намагаються зламати систему захисту. Основним засобом тестування в даному випадку є мережні сканери, розташовують базами даних відомих вразливостей.

Метод «білого ящика» передбачає складання програми тестування на підставі знань про структуру та конфігурації об'єкта випробувань. У ході тестування перевіряються наявність і працездатність механізмів безпеки, відповідність складу і конфігурації системи захисту вимогам безпеки і існуючим ризикам. Висновки про наявність вразливостей робляться на підставі аналізу конфігурації використовуваних засобів захисту та системного ПЗ, а потім перевіряються на практиці. Основним інструментом аналізу в даному випадку є програмні агенти засобів аналізу захищеності системного рівня.

РОЗДІЛ 2
СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

2.1 Міжмережеві екрани та їх класифікація

Міжмережевий екран (МЕ) називають локальний або функціонально розподілений програмний (програмно-апаратний) засіб (комплекс), який реалізує контроль за інформацією, що надходить в автоматизовану систему і/або виходить з автоматизованої системи. Також зустрічаються загальноприйняті назви брандмауер і firewall (англ. вогняна стіна). У будівельній сфері брандмауером (нім. brand - пожежа, mauer - стіна) називається вогнетривкий бар'єр, що розділяє окремі блоки в багатоквартирному будинку і перешкоджає поширенню пожежі. МЕ виконує подібну функцію для комп'ютерних мереж.

За визначенням МЕ служить контрольним пунктом на кордоні двох мереж. У найпоширенішому випадку ця межа лежить між внутрішньою мережею організації та зовнішньою мережею, зазвичай мережею Інтернет (рис. 2.1). Проте в загальному випадку, МЕ можуть застосовуватися для розмежування внутрішніх підмереж корпоративної мережі організації.

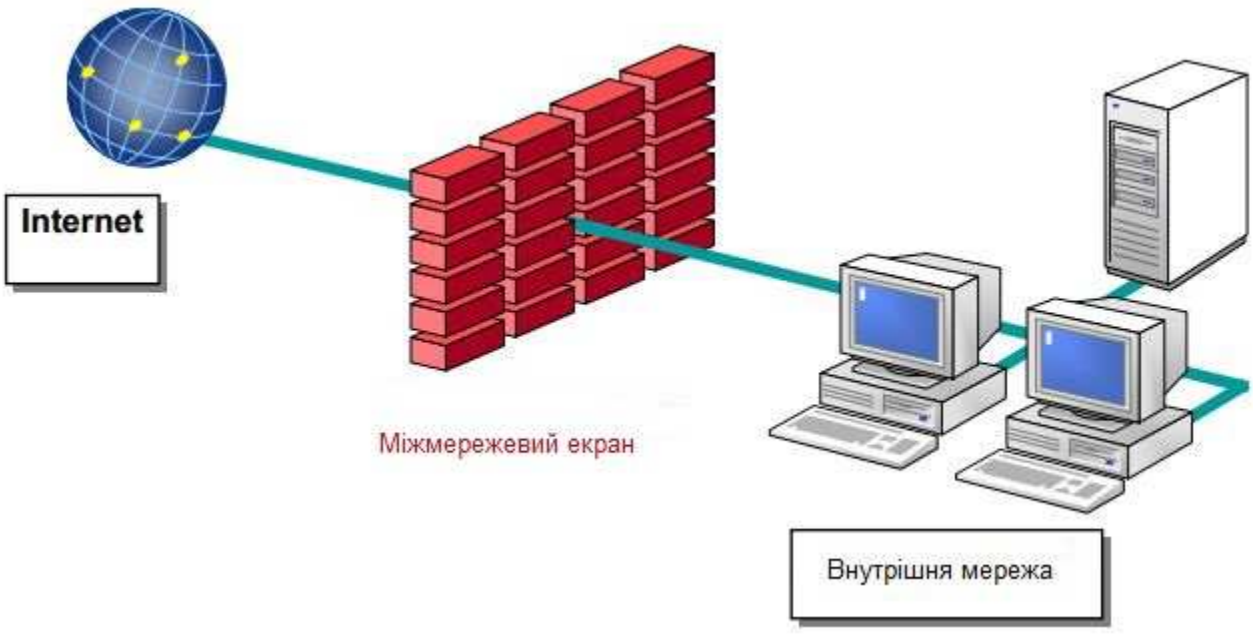

Рис. 2.1. Типове розміщення МЕ в корпоративній мереж

Завданнями МЕ, як контрольного пункту, є:

- контроль всього трафіку, що входять у внутрішню корпоративну мережу;
- контроль всього трафіку, що виходить з внутрішньої корпоративної мережі.

Контроль інформаційних потоків складається в їхній фільтрації і перетворенні у відповідність із заданим набором правил. Оскільки в сучасних МЕ фільтрація може здійснюватися на різних рівнях еталонної моделі взаємодії відкритих систем (EMBOC, OSI), МЕ зручно представити у вигляді системи фільтрів. Кожен фільтр на основі аналізу проходять через нього даних, приймає рішення - пропустити далі, перекинути за екран, блокувати або перетворити дані (рис. 2.2).

Невід'ємною функцією МЕ є протоколювання інформаційного обміну. Ведення журналів реєстрації дозволяє адміністратору виявити підозрілі дії, помилки в конфігурації МЕ і прийняти рішення про зміну правил МЕ.

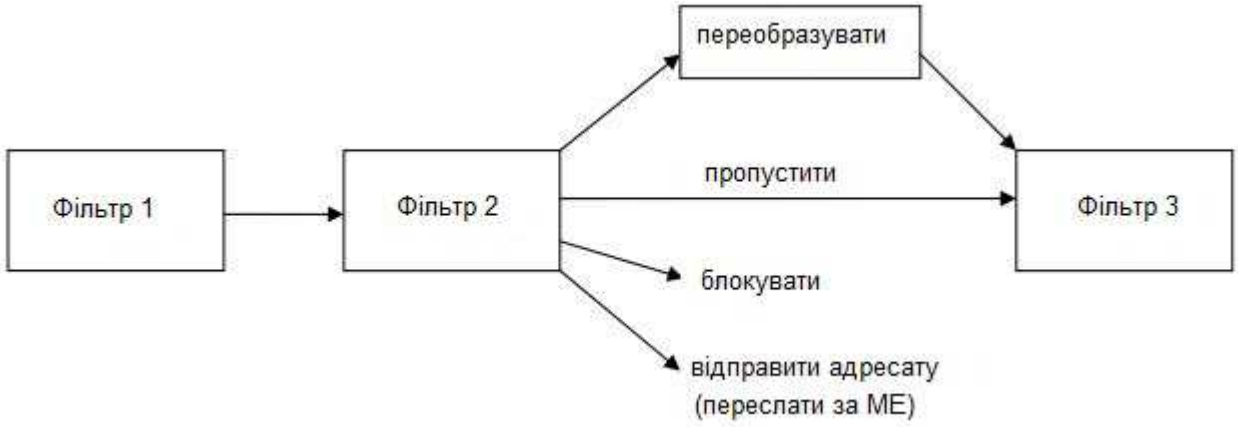

Рис. 2.2. Схема фільтрації в МЕ

Виділяють таку класифікацію МЕ, у відповідність з функціонуванням на різних рівнях МВОС (OSI):

- Мостові екрани (2 рівень OSI);
- Фільтруючі маршрутизатори (3 і 4 рівні OSI);
- Шлюзи сеансового рівня (5 рівень OSI);
- Шлюзи прикладного рівня (7 рівень OSI);
- Комплексні екрани (3-7 рівні OSI).

Мостові МЕ. Даний клас МЕ, що функціонує на 2-му рівні моделі OSI, відомий також як прозорий (stealth), прихований, тіньовий МЕ. Мостові МЕ з'явилися порівняно недавно і представляють перспективний напрям розвитку технологій міжмережевого екранування. Фільтрація трафіку ними здійснюється на канальномурівні, тобто МЕ працюють з фреймами (frame, кадр). До достоїнств подібних МЕ можна віднести:

- Немає необхідності в зміні налаштувань корпоративної мережі, не потрібно додаткового конфігурування мережевих інтерфейсів МЕ.

- Висока продуктивність. Оскільки це простіпристрою, вони не вимагають великих витрат ресурсів. Ресурси потрібні або для підвищення можливостей машин, або для більш глибокого аналізу даних.

- Прозорість. Ключовим для цього пристрою є його функціонування на 2 рівні моделі OSI. Це означає, що мережевий інтерфейс не має IP - адреси. Ця особливість більш важлива, ніж легкість в налаштуванні. Без IP-адреси цей пристрій не доступно в мережі і є невидимим для навколишнього світу. Якщо такий МЕ недоступний, то як його атакувати? Атакуючі навіть не будуть знати, що існує МЕ, перевіряючий кожен їхній пакет. Схема фільтрації трафіку МЕ забражена на рисунку 2.3.

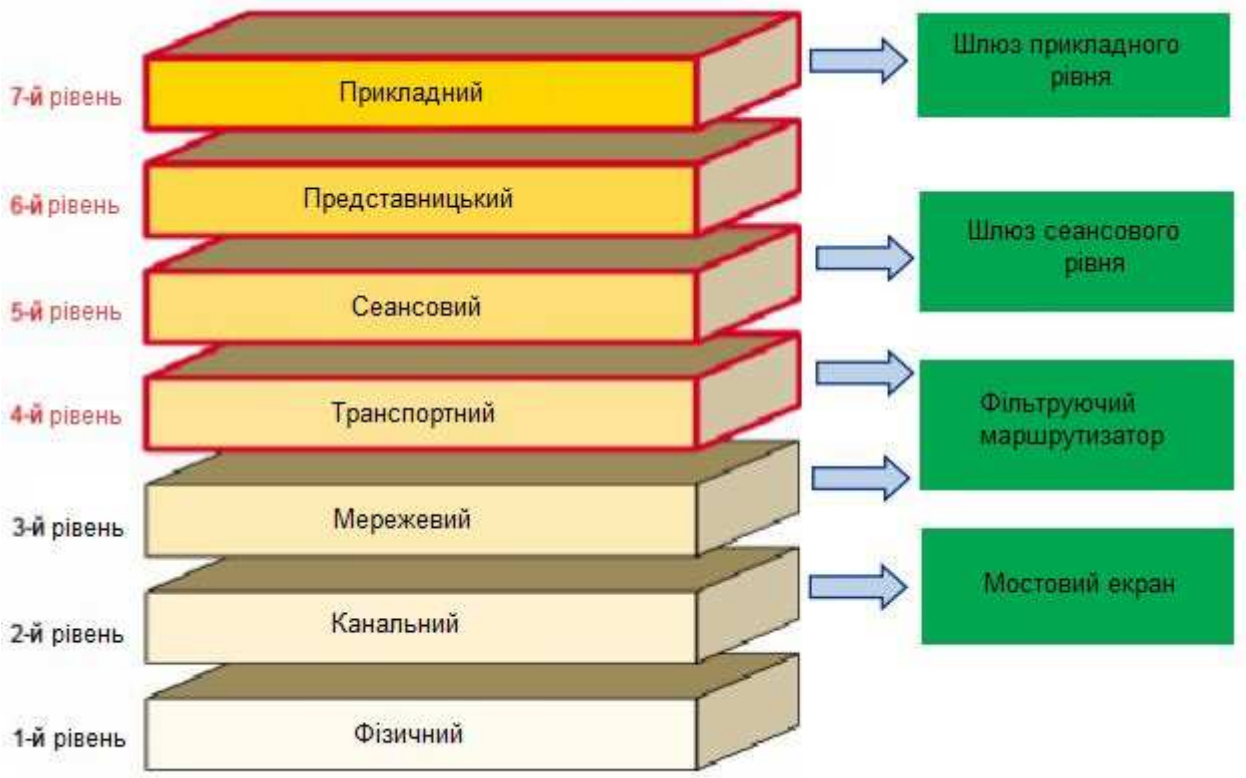

Рис. 2.3. Фільтрація трафіку МЕ на різних рівнях MBOS

Фільтруючі маршрутизатори. Packet-filtering firewall (Брандмауер з фільтрацією пакетів) - Міжмережевий екран, який є маршрутизатором або комп'ютером, на якому працює програмне забезпечення, сконфігуроване таким чином, щоб фільтрувати певні види вхідних і вихідних пакетів. Фільтрація пакетів здійснюється на основі інформації, що міститься в TCP- і IP- заголовках пакетів (адреси відправника і одержувача, їх номери портів та ін.)

- Працюють на 3 рівні;
- Також відомі, як МЕ на основі порту;
- Кожен пакет порівнюється зі списками правил (адреса джерела/одержувача, порт джерела/одержувача);
- Недорогий, швидкий (продуктивний в силу простоту), але найменш безпечний;
- Технологія 20-річної давності;
- Приклад: список контролю доступу (ACL, access control lists) маршрутизатора.

Шлюз сеансового рівня. Circuit-level gateway (Шлюз сеансового рівня) - міжмережевий екран, який виключає пряму взаємодію між авторизованим клієнтом і зовнішнім хостом. Спочатку він приймає запит довіреної клієнта на певні послуги і, після перевірки допустимості запитаного сеансу, встановлює з'єднання із зовнішнім хостом. Після цього шлюз просто копіює пакети в обох напрямках, не здійснюючи їх фільтрації. На цьому рівні з'являється можливість використання функції мережевий трансляції адрес (NAT, network address translation). Трансляція внутрішніх адрес виконується за відношенню до всіх пакетам, наступним з внутрішньої мережі в зовнішню. Для цих пакетів IP-адреси комп'ютерів – відправників внутрішньої мережі автоматично перетворюються в один IP-адрес, асоційований з екрануючим МЕ. В результаті всі пакети, виходять з внутрішньої мережі, виявляються відправленими МЕ, що виключає прямий контакт між внутрішньою і зовнішньою мережею. IP-адреса шлюзу сеансового рівня стає єдиною активною IP-адресою, яка потрапляє в зовнішню мережу.

- Працює на 4 рівні;
- Передає TCP підключення, грунтуючись на порту;
- Недорогий, але більш безпечний, ніж фільтр пакетів;
- Взагалі потребує роботи користувача або програми конфігурації для повноцінної роботи;
- Приклад: SOCKS файрвол.

Шлюз прикладного рівня. Application-level gateways (Шлюз прикладного рівня) – міжмережевий екран, який виключає пряму взаємодію між авторизованим клієнтом і зовнішнім хостом, фільтруючи всі вхідні і вихідні пакети на прикладному рівні моделі OSI. Пов'язані з додатком програми-посередники перенаправляють через шлюз інформацію, що генерується конкретними сервісами TCP/IP.

Можливості:

- Ідентифікація та аутентифікація користувачів при спробі встановлення з'єднання через МЕ;

- Фільтрація потоку повідомлень, наприклад, динамічний пошук вірусів і прозоре шифрування інформації;
- Реєстрація подій та реагування на події;
- Кешування даних, запитуваних із зовнішньої мережі.

На цьому рівні з'являється можливість використання функцій посередництва (Proxy).

Для кожного обсуговуваного протоколу прикладного рівня можна вводити програмних посередників - HTTP-посередник , FTP-посередник і т.д. Посередник кожної служби TCP/IP орієнтований орієнтований на обробку повідомлень і виконання функцій захисту, що відносяться саме до цієї служби. Також, як і шлюз сеансового рівня, прикладний шлюз перехоплює за допомогою відповідних екрануючих агентів вхідні і вихідні пакети копіює і перенаправляє інформацію через шлюз, і функціонує як сервера-посередника, виключаючи прямі з'єднання між внутрішньою ізовнішньою мережею . Однак, посередники, використовувані прикладним шлюзом, мають важливі відмінності від канальних посередників шлюзів сеансового рівня. По-перше, посередники прикладного шлюзу пов'язані з конкретними додатками програмними серверами, а по-друге, вони можуть фільтрувати потік повідомлень на прикладному рівні моделі MBOS.

Особливості:

- Працює на 7 рівні;
- Специфічний для додатків;
- Помірно дорогий і повільний, але більш безпечний і допускає реєстрацію діяльності користувачів;
- Вимагає роботи користувача або програми конфігурації для повноцінної роботи;
- Приклад: Web (http) proxy.

МЕ експертного рівня. Stateful inspection firewall - міжмережевий екран експертного рівня, який перевіряє вміст прийнятих пакетів на трьох рівнях моделі OSI: мережевому, сеансовому і прикладному. При виконанні цього завдання використовуються спеціальні алгоритми фільтрації пакетів, з

допомогою яких кожен пакет порівнюється з відомим шаблоном авторизованих пакетів.

- Фільтрація 3 рівня;
- Перевірка правильності на 4 рівні;
- Огляд 5 рівня;
- Високі рівні вартості, захисту і складності;
- Приклад: CheckPoint Firewall.

Деякі сучасні МЕ використовують комбінацію перерахованих вище методів і забезпечують додаткові способи захисту, як мереж, так і систем.

«Персональні» МЕ. Цей клас МЕ дозволяє далі розширювати захист, допускаючи управління по тому, які типи системних функцій або процесів мають доступ до ресурсів мережі. Ці МЕ можуть використовувати різні типи сигнатур і умов, для того, щоб дозволяти або відкидати трафік.

Ось деякі із загальних функцій персональних МЕ:

- Блокування на рівні додатків - дозволяти лише деяким додаткам або бібліотекам виконувати мережеві дії або приймати вхідні підключення;
- Блокування на основі сигнатури - постійно контролювати мережевий трафік і блокувати всі відомі атаки.

Додатковий контроль збільшує складність управління безпекою через потенційно великі кількості систем, які можуть бути захищені персональним файрволом. Це також збільшує рівень ризику пошкодження і вразливості через погане налаштування.

Динамічні МЕ Динамічні МЕ об'єднують в собі стандартні МЕ (перераховані вище) і методи виявлення вторгнень, щоб забезпечити блокування «на льоту» мережевих підключень, які відповідають певній сигнатурі, дозволяючи при цьому підключення від інших джерел до того ж самого порту. Наприклад, можна блокувати діяльність мережевих черв'яків, не порушуючи роботу нормального трафіку.

2.2 Схеми підключення МЕ

- Схема єдиного захисту локальної мережі;
- Схема захищена закритою і не захищена відкритою підмережами;
- Схема з роздільним захистом закритою і відкритою підмережею.

Схема єдиного захисту локальної мережі

Найбільш простим є рішення, при якому міжмережевий екран просто екранує локальну мережу від глобальної. При цьому WWW-сервер, FTP-сервер, поштовий сервер та інші сервера, виявляються також захищені фаєрволом. При цьому потрібно виділити багато уваги на запобігання проникнення на захищені станції локальної мережі за допомогою засобів легкодоступних WWW-серверів. Схема єдиного захисту локальної мережі зображено на рисунку 2.4.

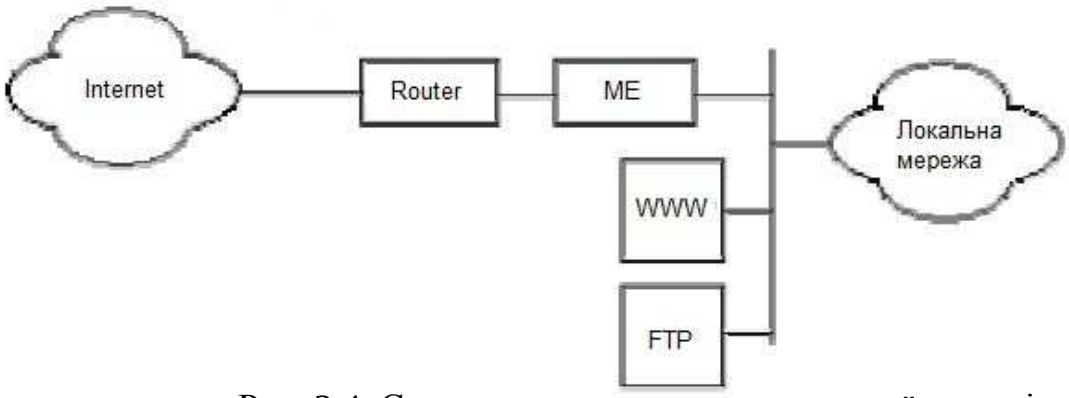

Рис. 2.4. Схема єдиного захисту локальної мережі

Схема захищена закритою і не захищена відкритою підмережами.

Для запобігання доступу в локальну мережу, використовуючи ресурси WWW-сервера, рекомендується загально доступні сервери підключати перед міжмережевим екраном. Даний спосіб має більш високу захищеність локальної мережі, але низьким рівнем захищеності WWW-і FTP-серверів. Схема захищена закритою і не захищена відкритою підмережами зображено на рисунку 2.5.

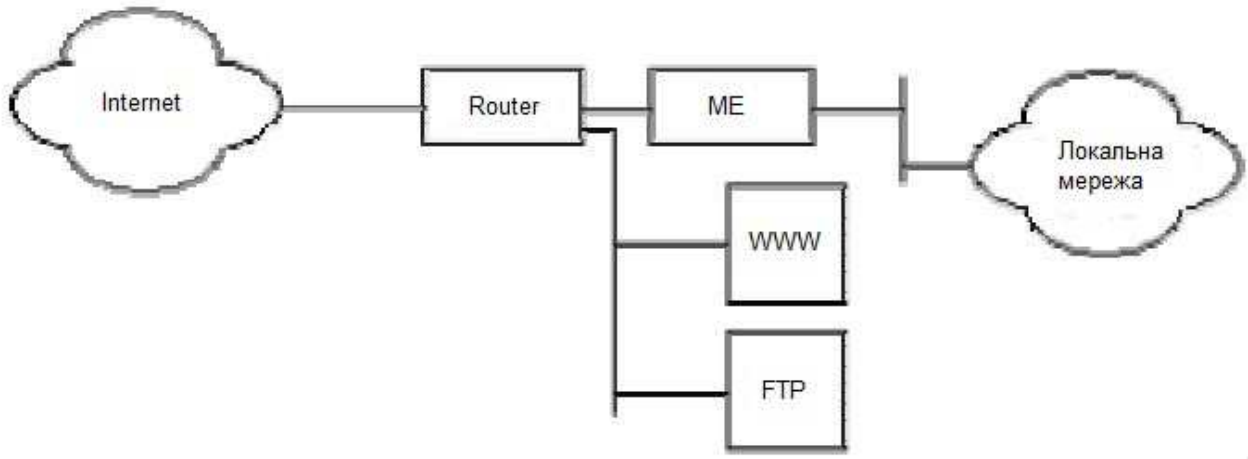

Рис. 2.5. Схема захищена закритою і не захищена відкритою підмережами

Схема з роздільним захистом закритою і відкритою підмережею.

Дана схема підключення має найвищу захищеність в порівнянні з розглянутими вище. Схема заснована на застосуванні двох МЕ, що захищають окремо закриту і відкриту підмережі (рис 2.6). Ділянка мережі між МЕ також називається екранованої підмережею або демілітаризованою зоною (DMZ, demilitarized zone).

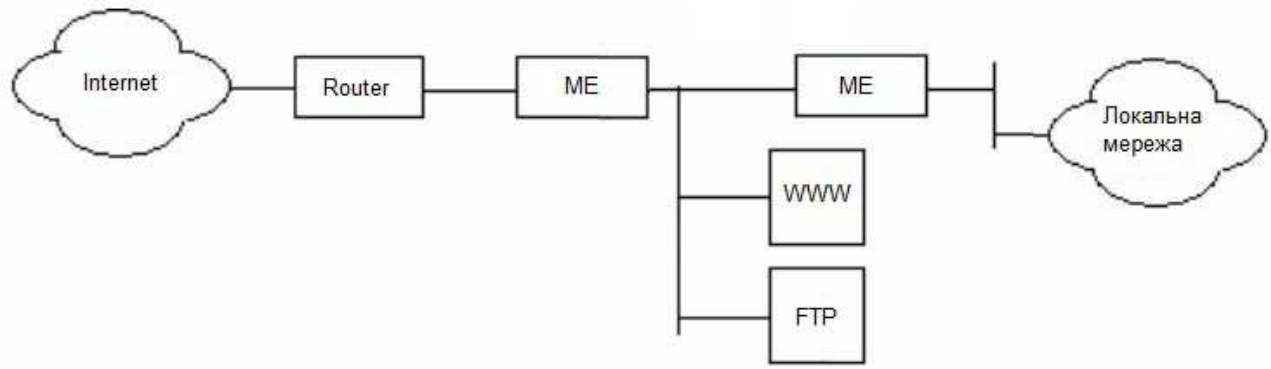

Рис. 2.6. Схема з роздільним захистом закритою і відкритою підмережею

2.3 Системи виявлення атак

Поряд зі стандартними засобами захисту, без яких немислимо нормальне функціонування АС (таких як МЕ, системи резервного копіювання та антивірусні засоби), існує необхідність використання СВА (IDS, систем

виявлення атак або вторгнень), які є основним засобом боротьби з мережевими атаками [3].

В даний час СВА починають все ширше впроваджуватися в практику забезпечення безпеки корпоративних мереж. Однак існує ряд проблем, з якими неминуче стикаються організації, розгортають у себе систему виявлення атак. Ці проблеми істотно ускладнюють, а часом і зупиняють процес впровадження IDS. Ось деякі з них:

- висока вартість комерційних СВА;
- невисока ефективність сучасних СВА, характеризується великим числом помилкових спрацьовувань і неспрацьовуванні (false positives and false negatives);
- вимогливість до ресурсів і часом незадовільна продуктивність СВА вже на 100 Мбіт/с мережах;
- недооцінка ризиків, пов'язаних із здійсненням мережевих атак;
- відсутність в організації методики аналізу та управління ризиками, що дозволяє адекватно оцінювати величину ризику і обгрунтовувати вартість реалізації контрзаходів для керівництва;
- висока кваліфікація експертів з виявлення атак, вимагається для впровадження і розгортання СВА.

Типова архітектура системи виявлення атак, як правило, включає в себе наступні компоненти:

1 . Сенсор (засіб збору інформації);

2 . Аналізатор (засіб аналізу інформації);

3 . Засоби реагування;

4 . Засоби управління.

Звичайно, всі ці компоненти можуть функціонувати і на одному комп'ютері і навіть у рамках однієї програми, однак найчастіше вони територіально і функціонально розподілені. Такі компоненти СВА, як аналізатори та засоби управління, небезпечно розміщувати за МЕ у зовнішній мережі, оскільки якщо вони будуть скомпрометовані, то зловмисник може

отримати доступ до інформації про структуру внутрішньої мережі, що захищається на основі аналізу бази правил, використовуваної СВА.

Типова архітектура системи виявлення атак зображена на рисунку 2.7. Мережеві сенсори здійснюють перехоплення мережевого трафіку, хостової сенсори використовують в якості джерел інформації журнали реєстрації подій ОС, СУБД і додатків. Інформація про події також може бути отримана хостовим сенсором безпосередньо від ядра ОС, МЕ або програми. Аналізатор, розміщується на сервері безпеки, здійснює централізований збір і аналіз інформації, отриманої від сенсорів.

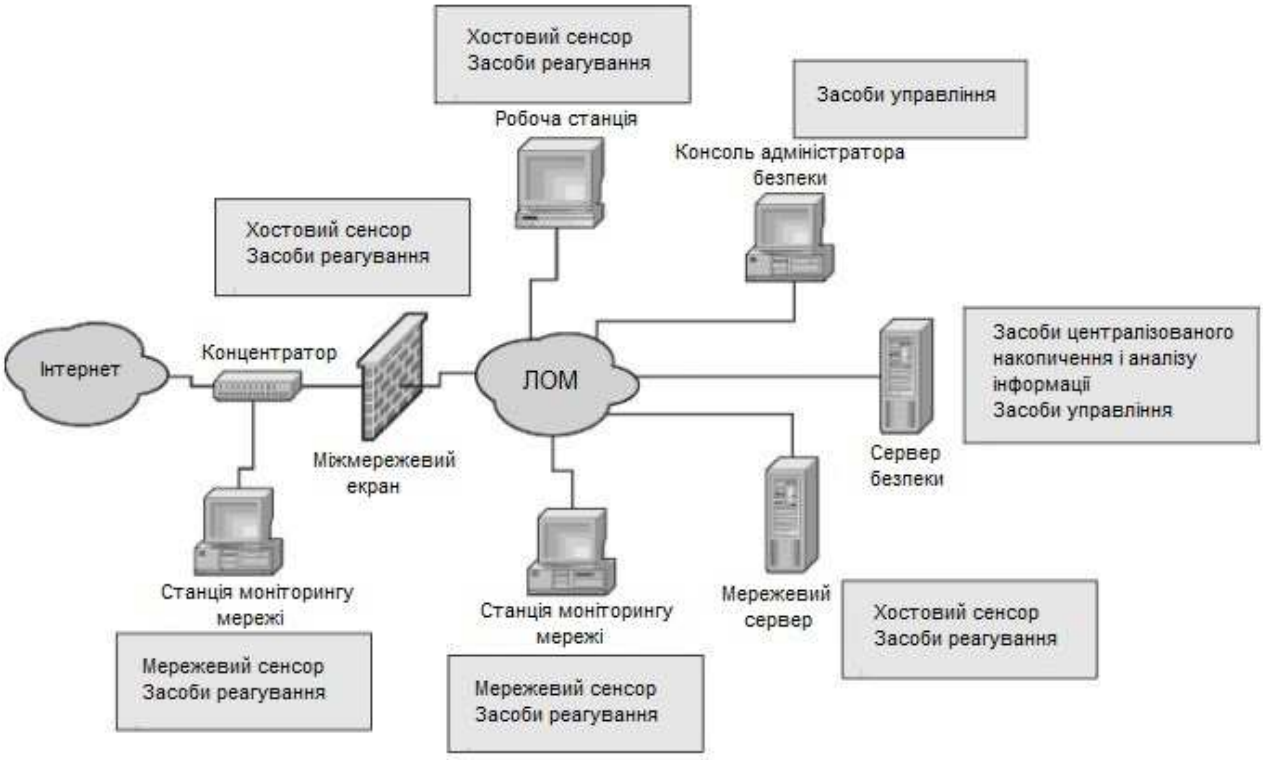

Рис. 2.7. Типова архітектура СВА

Засоби реагування можуть розміщуватися на станціях моніторингу мережі, МЕ, серверах і робочих станціях ЛОМ. Типовий набір дій з реагування на атаки містить у собі оповіщення адміністратора безпеки (засобами електронної пошти, виведення повідомлення на консоль або відправки на пейджер), блокування мережевих сесій і користувальницьких реєстраційних записів з метою негайного припинення атак, а також протоколювання дій атакуючої сторони.

Засоби управління призначені для адміністрування всіх компонентів системи виявлення атак, розробки алгоритмів виявлення та реагування на порушення безпеки (політик безпеки), а також для перегляду інформації про порушення і генерації звітів.

2.4 Віртуальні приватні мережі. Функції та компоненти мережі VPN

У зв'язку з широким розповсюдженням Internet, intranet, extranet при розробці та застосуванні розподілених інформаційних мереж і систем одним з найактуальніших завдань є вирішення проблем інформаційної безпеки [4].

В останнє десятиліття у зв'язку з бурхливим розвитком Internet і мереж колективного доступу в світі стався якісний стрибок у поширенні і доступності інформації. Користувачі отримали дешеві й доступні канали зв'язку. Прагнучи до економії коштів, підприємства використовують такі канали для передачі критичною комерційної інформації. Однак принципи побудови Internet відкривають зловмисникам можливості крадіжки або навмисного спотворення інформації. Не забезпечений достатньо надійний захист від проникнення порушників у корпоративні та відомчі мережі.

Для ефективної протидії мережевим атакам і забезпечення можливості активного і безпечного використання в бізнесі відкритих мереж на початку 90-х років народилася і активно розвивається концепція побудови захищених віртуальних приватних мереж – VPN (Virtual Private Networks).

Захищеною віртуальною мережею VPN називають об'єднання локальних мереж і окремих комп'ютерів через відкриту зовнішню середу передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку циркулюючих даних.

При підключенні корпоративної локальної мережі до відкритої мережі виникають загрози безпеки двох основних типів:

- несанкціонований доступ до корпоративних даних у процесі їх передачі по відкритій мережі;

- несанкціонований доступ до внутрішніх ресурсів корпоративної локальної мережі, одержуваний зловмисником в внаслідок несанкціонованого входу в цю мережу.

Захист інформації в процесі передачі по відкритих каналах зв'язку заснована на виконанні таких основних функцій:

- аутентифікації взаємодіючих сторін;
- криптографическом закритті (шифруванні) переданих даних;
- перевірці автентичності та цілісності доставленої інформації.

Для цих функцій характерний взаємозв'язок один з одним. Їх реалізація заснована на використанні криптографічних методів захисту інформації.

Для захисту локальних мереж і окремих комп'ютерів від несанкціонованих дій з боку зовнішнього середовища зазвичай використовують міжмережеві екрани, що підтримують безпеку інформаційної взаємодії шляхом фільтрації двостороннього потоку повідомлень, а також виконання функцій посередництва при обміні інформацією. Міжмережевий екран розташовують на стику між локальної та відкритою мережею. Для захисту окремого віддаленого комп'ютера, підключеного до відкритої мережі, програмне забезпечення мережевого доступу встановлюють на цьому ж комп'ютері, і такий міжмережевий екран називається персональним.

2.4.1 Тунелювання

Захист інформації в процесі її передачі по відкритих каналах заснована на побудові захищених віртуальних каналів зв'язку, званих криптозахищені тунелями. Кожен такий тунель являє собою з'єднання, проведене через відкриту мережу, по якому передаються криптографічно захищені пакети повідомлень.

Створення захищеного тунелю виконують компоненти віртуальної мережі, що функціонують на вузлах, між якими формується тунель. Ці компоненти прийнято називати ініціатором і термінатором тунелю. Ініціатор тунелю інкапсулює (вбудовує) пакети в новий пакет, що містить поряд з вихідними даними новий заголовок з інформацією про відправника та

одержувача. Хоча всі передаються по тунелю пакети є пакетами IP, інкапсулюючі пакети можуть належати до протоколу будь-якого типу, включаючи пакети немаршрутизуючих протоколів, таких, як NetBEUI. Маршрут між ініціатором і термінатором тунелю визначає звичайна маршрутизована мережа IP, яка може бути і мережею відмінною від Інтернет. Термінатор тунелю виконує процес зворотний інкапсуляції - він видаляє нові заголовки і направляє кожен вихідний пакет в локальний стек протоколів або адресату в локальній мережі.

Сама по собі інкапсуляція ніяк не впливає на захищеність пакетів повідомлень, переданих по тунелю. Але завдяки інкапсуляції з'являється можливість повного криптографічного захисту інкапсулюючих пакетів. Конфіденційність інкапсулюючих пакетів забезпечується шляхом їх криптографічного закриття, тобто зашифровування, а цілісність і справжність - шляхом формування цифрового підпису. Оскільки існує велика безліч методів криптозахисту даних, дуже важливо, щоб ініціатор і термінатор тунелю використовували одні й ті ж методи і могли погоджувати один з одним цю інформацію.

Крім того, для можливості розшифровки даних та перевірки цифрового підпису при прийомі ініціатор і термінатор тунелю повинні підтримувати функції безпечного обміну ключами. Ну і нарешті, щоб тунелі створювалися тільки між уповноваженими користувачами, кінцеві сторони взаємодії потрібно аутентифікувати.

2.4.2 Класифікація VPN по робочому рівню EMBBC

Для технологій безпечної передачі даних по загальнодоступній (незахищеній) мережі застосовують узагальнену назву – захищений канал (secure channel). Захищений канал можна побудувати за допомогою системних коштів, реалізованих на різних рівнях еталонної моделі взаємодії відкритих систем (EMBOC, OSI) (табл. 2.1).

Таблиця 2.1

Рівні протоколів захищеного канала

Протоколи захищеного доступу	Прикладний	Впливають на додатки
	Представницький	
	Сеансовий	
	Транспортний	
	Мережевий	Невидимі для додатків
	Канальний	
	Фізичний	

Від вибраного рівня OSI багато в чому залежить функціональність реалізованої VPN і її сумісність з додатками ІС, а також з іншими засобами захисту. За ознакою робочого рівня моделі OSI розрізняють 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.

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. Протокол захищає тільки цілком певну мережеву службу-файлову, гіпертекстову або поштову. Наприклад, протокол

S/MIME захищає виключно повідомлення електронної пошти. Тому для кожної служби необхідно розробляти відповідну захищену версію протоколу.

На верхніх рівнях моделі OSI існує жорсткий зв'язок між використовуваним стеком протоколів та програмою.

VPN канального рівня

Засоби VPN, використовувані на канальному рівні моделі OSI, дозволяють забезпечити інкапсуляцію різних видів трафіку третього рівня (і більш високих рівнів) і побудову віртуальних тунелів типу «крапка-крапка» (від маршрутизатора до маршрутизатора або від персонального комп'ютера до шлюзу ЛОМ). До цієї групи відносятся VPN-продукти, які використовують протоколи L2F (Layer 2 Forwarding) і PPTP (Point-to-Point Tunneling Protocol), а також порівняно недавно затверджений стандарт L2TP (Layer 2 Tunneling Protocol), розроблений спільно фірмами Cisco Systems і Microsoft.

Протокол захищеного каналу PPTP заснований на протоколі PPP і забезпечує прозорість засобів захисту для додатків і служб прикладного рівня. Протокол PPTP може переносити пакети як в мережах IP, так і в мережах, що працюють на основі протоколів IPX, DECnet або NetBEUI.

Протокол L2TP використовується при організації віддаленого доступу до ЛОМ (оскільки базується в основному на ОС Windows). Тим часом рішення другого рівня не придбають, ймовірно, таке ж значення для взаємодії ЛОМ, з причини недостатньої масштабованості при необхідності мати декілька тунелів із загальними кінцевими точками.

VPN мережевого рівня

VPN-продукти мережевого рівня виконують інкапсуляцію IP в IP. Одним з широко відомих протоколів на цьому рівні є SKIP, який поступово витісняється новим протоколом IPSec, призначеним для аутентифікації, тунелювання і шифрування IP -пакетів.

Працюючий на мережевому рівні протокол IPSec являє компромісний варіант. З одного боку, він прозорий для додатків, а з іншого, може працювати практично у всіх мережах, так як заснований на широко поширеному протоколі IP.

Протокол IPSec передбачає стандартні методи ідентифікації користувачів або комп'ютерів при ініціації тунелю, стандартні способи використання шифрування кінцевими точками тунелю, а також стандартні методи обміну і управління ключами шифрування між кінцевими точками.

Протокол IPSec може працювати спільно з L2TP; в результаті ці два протоколи забезпечують більш надійну ідентифікацію, стандартизоване шифрування і цілісність даних. Тунель IPSec між двома локальними мережами може підтримувати безліч індивідуальних каналів передачі даних, в результаті чого додатки даного типу отримують переваги з точки зору масштабування.

Говорячи про IPSec, необхідно згадати протокол (IKE) дозволяє захистити передану інформацію від стороннього втручання. Він вирішує завдання безпечного управління та обміну криптографічними ключами між віддаленими пристроями.

VPN сеансового рівня

Деякі VPN використовують інший підхід під назвою «Посередники каналів» (circuit proxy). Цей метод функціонує над транспортним рівнем і ретранслює трафік із захищеної мережі в загальнодоступну мережу Internet для кожного сокета окремо. (Протокол IP не має п'ятого-сеансового-рівня, однак орієнтовані на сокети операції часто називають операціями сеансового рівня.)

Шифрування інформації, переданої між ініціатором і термінатором тунелю часто здійснюється за допомогою захисту транспортного рівня TLS.

Для стандартизації аутентифікованого проходу через міжмережеві екрани консорціум IETF визначив протокол під назвою SOCKS, і в даний час протокол SOCKS v.5 застосовується для стандартизованої реалізації посередників каналів.

У протоколі SOCKS v.5 клієнтський комп'ютер встановлює аутентіфікований сокет (або сеанс) з сервером, виконуючим роль посередника (proxy). Цей посередник - єдиний спосіб зв'язку через міжмережевий екран. Посередник, у свою чергу, проводить будь-які операції, запитувані клієнтом. Оскільки посереднику відомо про трафіку на рівні сокета, він може

здійснювати ретельний контроль, наприклад блокувати конкретні програми користувачів, якщо вони не мають необхідних повноважень.

2.4.3 Класифікація VPN з архітектури технічного рішення

За архітектурою технічного рішення прийнято виділяти три основних види віртуальних приватних мереж:

- VPN з віддаленим доступом;
- внутрішньокорпоративні VPN;
- міжкорпоративні VPN.

Віртуальні приватні мережі VPN з віддаленим доступом (Remote Access) призначені для забезпечення захищеного віддаленого доступу до корпоративних інформаційних ресурсів мобільним і/або віддаленим (home-office) співробітникам компанії.

Внутрішньокорпоративні мережі VPN (intranet-VPN) призначені для забезпечення захищеної взаємодії між підрозділами всередині підприємства або між групою підприємств, об'єднаних корпоративними мережами зв'язку, включаючи виділені лінії.

Міжкорпоративні мережі VPN (extranet-VPN) забезпечують співробітникам підприємства захищений обмін інформацією зі стратегічними партнерами по бізнесу, постачальниками, великими замовниками, користувачами, клієнтами і т.д.

Extranet - VPN забезпечує прямий доступ з мережі однієї компанії до мережі іншої, тим самим сприяючи підвищенню надійності зв'язку, підтримуваної в ході ділового співробітництва. У міжкорпоративних мережах велике значення надається контролю доступу за допомогою міжмережевих екранів і аутентифікації користувачів.

2.4.4 Класифікація VPN за способом технічної реалізації

За способом технічної реалізації розрізняють такі групиVPN:

- VPN на основі мережевої операційної системи;
- VPN на основі міжмережевих екранів;
- VPN на основі маршрутизаторів;
- VPN на основі програмних рішень;
- VPN на основі спеціалізованих апаратних засобів із вбудованими шифропроцесорами.

VPN на основі мережевої ОС

Реалізацію VPN на основі мережевої ОС можна розглянути на прикладі операційної системи Windows NT. Для створення VPN компанія Microsoft пропонує протокол PPTP, інтегрований в мережеву операційну систему Windows NT. Таке рішення виглядає привабливо для організацій, що використовують Windows як корпоративну ОС. У мережах VPN, заснованих на Windows NT, використовується база даних клієнтів, що зберігається в контролері PDC (Primary Domain Controller). При підключенні до PPTP – сервера користувач авторизується по протоколах PAP, CHAP або MS CHAP. Для шифрування застосовується нестандартний фірмовий протокол Point-to-Point Encryption з 40-бітовим ключем, одержуваним при встановленні з'єднання.

В якості гідності наведеної схеми слід зазначити, що вартість рішення на основі мережевої ОС значно нижче вартості інших рішень.

Недосконаліть такої системи - недостатня захищеність протоколу PPTP.

VPN на основі маршрутизаторів

Даний спосіб побудови VPN передбачає застосування маршрутизаторів для створення захищених каналів. Оскільки вся інформація, що виходить з локальної мережі, проходить через маршрутизатор, то цілком природно покласти на нього і завдання шифрування.

VPN на основі міжмережевих екранів

Міжмережеві екрани більшості виробників містять функції тунелювання і шифрування даних. До програмного забезпеченню власне брандмаузера додається модуль шифрування.

До недоліків цього методу відносяться висока вартість рішення в перерахунку на одне робоче місце і залежність продуктивності від апаратного забезпечення, на якому працює міжмережевий екран. При використанні міжмережевих екранів на базі ПК треба пам'ятати, що подібний варіант підходить тільки для невеликих мереж з обмеженим обсягом переданої інформації.

VPN на основі програмного забезпечення

Для побудови мереж VPN також застосовуються програмні рішення. При реалізації подібних схем використовується спеціалізоване ПЗ, яке працює на виділеному комп'ютері і в більшості випадків виконує функції proxy-сервера. Комп'ютер з таким програмним забезпеченням може бути розташований за міжмережевим екраном.

VPN на основі спеціалізованих апаратних засобів із вбудованими шифропроцесорами

Варіант побудови VPN на спеціалізованих апаратних засобах може бути використаний в мережах, що вимагають високої продуктивності. Недолік подібного рішення його висока вартість.

2.4.5 Технічні та економічні переваги впровадження технологій VPN в корпоративні мережі

Технологія віртуальних приватних мереж VPN дозволяє ефективно вирішувати завдання, пов'язані з циркуляцією конфіденційної інформації з каналів зв'язку. Вона забезпечує зв'язок між мережами, а також між віддаленим користувачем і корпоративною мережею за допомогою захищеного каналу (тунелю), «Прокладеного» в загальнодоступній мережі Internet.

Таким чином, на сучасному етапі розвитку, в умовах, коли філії одного і того ж підприємства знаходяться на значній видаленні один від одного, потреба в оперативному і надійному обміні інформацією стала найбільш гострою. Використання дорогих високопропускних каналів зв'язку не завжди виявляється доцільним і економічно вигідним. Розвиток же засобів зв'язку, особливо недорогих і найбільш доступних (наприклад, Internet), призводить до того, що їх практичне використання, особливо корпораціями, стає все більш масовим. У цих умовах стає принадним їх використання для передачі цінної корпоративної інформації, збитки від втрати або спотворення якої можуть згубно позначитися на діяльності компанії. Тому використання захищених віртуальних приватних мереж VPN з урахуванням всіх їх переваг стає все більш актуальним і життєво необхідним. Концепція таких мереж дозволяє організовувати такий необхідний обмін інформацією усередині компанії і з клієнтами при найкращому поєднанні продуктивності, оперативності, захищеності і вартості. Треба припустити, що такі технології, як VPN, будуть активно розвиватися, вдосконалюватися і набувати все більш масовий характер.

РОЗДІЛ 3
ВНУТРІШНІ ЗЛОВМИСНИКИ В КОРПОРАТИВНИХ МЕРЕЖАХ ТА ДОСЛІДЖЕННЯ МЕТОДІВ ПРОТИДІЇ ЇМ

3.1 Внутрішні зловмисники в корпоративних мережах. Методи впливу

Всупереч поширеній думці про те, що основну небезпеку для компанії представляють зовнішні порушники, діючі з мережі Інтернет, так звані хакери, реальна загроза сучасній компанії виходить від внутрішніх порушників. За численним дослідженням близько 70-80% всіх порушень у корпоративному середовищі припадає на частку внутрішніх порушників (рис. 3.1).

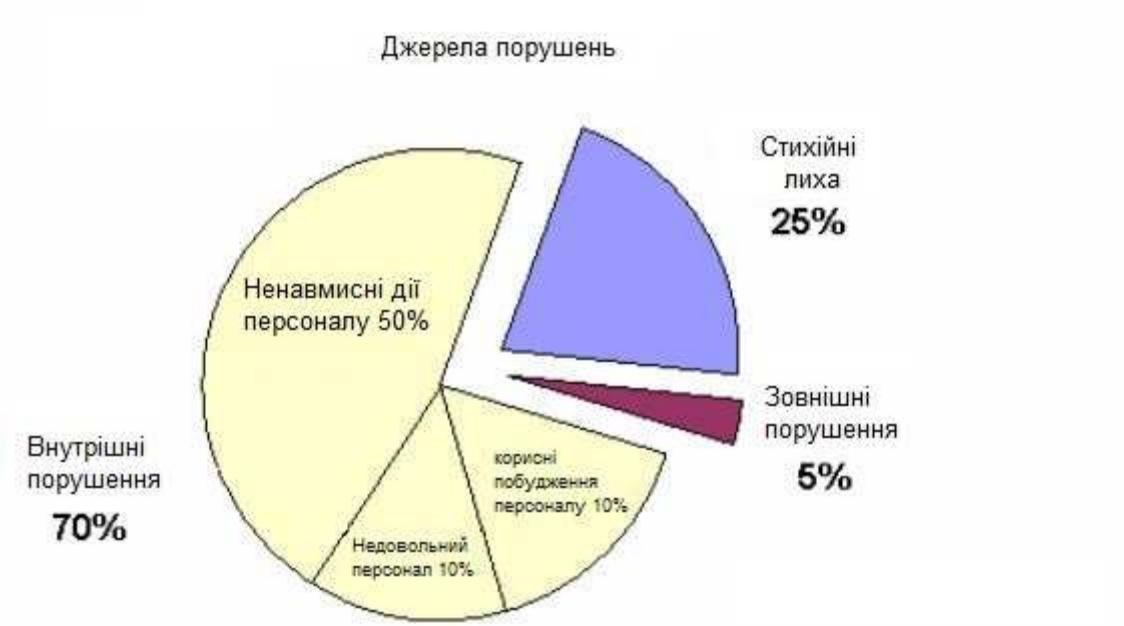

Рис. 3.1. Джерела порушень в сучасній компанії

Порушником в загальному сенсі є особа, помилково, незнання або усвідомлено зробив спробу виконання заборонених операцій і використовує для цього різні можливості, методи і кошти. Внутрішній порушник являє собою легітимного співробітника організації, що має певний доступ до її інформаційних ресурсів. Причому, причинами порушень всередині організації можуть бути як помилки персоналу, так і навмисні дії з їхнього боку. Таким чином, згідно загальносвітової статистики на частку внутрішніх порушників,

навмисне вчиняють протиправні дії, припадає близько 20% всіх інцидентів в компанії, в той час як зовнішні порушники винні лише в 5% подібних випадків. У цьому розділі розглянуто можливі дії внутрішніх зловмисників усередині корпоративної мережі і запропоновано заходи протидії.

У вітчизняній і зарубіжній комп'ютерній літературі застосовується різна термінологія щодо комп'ютерних злочинців. Відсутність єдиної класифікації часто призводить до плутанини. Так, «хакером» (hacker) найчастіше називають саме комп'ютерних зловмисників, а іноді - висококваліфікованих комп'ютерних фахівців. Останніх ще іноді називають «білими капелюхами» (white-hats), на відміну від «Чорних капелюхів», мета яких завдати шкоди системі. Також часто використовуються поняття кракер (cracker), kid-hacker, spy і т.д [5]. Щоб уникнути плутанини тут і далі застосовуються терміни «порушник» і «зловмисник» (intruder), для узагальненого позначення тих, хто навмисне робить порушення в корпоративну мережу [6]. Порушники можуть бути розбиті на дві категорії:

Outsiders (англ. чужий , сторонній) - це порушники з мережі Інтернет, які атакують внутрішні ресурси корпоративної мережі (видалення інформації на корпоративному веб - сервері, пересилання спаму через поштовий сервер і т.д.) і які обходять МЕ і СВА для того, щоб проникнути у внутрішню корпоративну мережу. Зловмисники можуть атакувати з Інтернет, через модемні лінії, через фізичне підключення до каналів зв'язку або з мережі партнерів (постачальників, замовників, дилерів і т.д.).

Insiders (англ. свій, добре обізнана людина) - це ті, хто знаходиться усередині корпоративної мережі, і мають певний доступ до корпоративних серверів і робочих станцій. Вони включають користувачів, неправильно використовують свої привілеї, або виконуючих роль привілейованого користувача (наприклад, з привілейованого терміналу). Ці люди спочатку знаходяться в переважному положенні, ніж Outsiders. Оскільки вони вже володіють конфіденційною інформацією про фірму, недоступною для зовнішніх порушників. На відміну від зовнішніх порушників, для яких у загальному випадку атакується корпоративна мережа спочатку представляє

«чорний ящик», внутрішні порушники - це люди, які знають, як працює фірма, і розуміють її слабкості. Знають, що пароль у шефа записаний на папірці, який лежить у нього на столі, що пароль секретарки - ім'я її собачки, знають, коли адміністратор йде пити чай і т.д.

Так за статистикою найбільша частина злочинів проти банків скоюється з використанням так званої «інсайдерської» інформації [7].

Ще кілька прикладів. У лютому 2001 року двоє колишніх Співробітників компанії Commerce One, скориставшись вкраденим паролем адміністратора, видалили з сервера файли, що складали великий (на декілька мільйонів доларів) проект для іноземного замовника. На щастя, малася резервна копія проекту, так що реальні втрати обмежилися витратами на слідство і засоби захисту від подібних інцидентів у майбутньому. У серпні 2002 року злочинці постали перед судом.

Крадіжка 3 мільйонів доларів була здійснена з банку Стокгольма, з використанням привілейованого становища декількох службовців в інформаційній системі банку і також виявилася успішною [8].

Таким чином, проблема захисту від внутрішніх порушників знаходиться в центрі уваги. Саме ця проблема є зараз найбільш актуальною і менш дослідженою. Якщо в забезпеченні захисту від зовнішніх порушників давно вже вироблені усталені підходи (хоча розвиток відбувається і тут), то методи протидії внутрішнім порушникам в даний час мають багато нерозглянутих питань. Зокрема, немає ясного уявлення про методи роботи внутрішніх порушників.

3.2 Модель внутрішнього порушника

Дослідження проблем захисту корпоративних мереж доцільно почати з розгляду моделі потенційного порушника.

За оцінками фахівців в даний час близько 70-90 % інтелектуального капіталу компанії зберігається в цифровому вигляді - текстових файлах, таблицях, базах даних. Використання інформаційних технологій надає значні

переваги для бізнесу, проте призводить і до появи нових загроз. Унаслідок недостатнього серйозного ставлення керівництва до інформаційної безпеки, недобросовісним співробітникам надаються широкі можливості несанкціонованого доступудо інформації компанії, що становить комерційну таємницю і що має реальну або потенційну економічну цінність.

Розглянемо, за яких умов легального співробітника організації можна назвати внутрішнім порушником. Для ефективного функціонування організації необхідно, щоб у ній була загальна стратегія діяльності та чіткі посадові інструкції кожному співробітнику. Наступним організаційним документом має бути політика безпеки організації, в якій викладені принципи організації та конкретні заходи з забезпечення інформаційної безпеки підприємства. Класифікаційний розділ політики безпеки описує наявні в організації матеріальні та інформаційні ресурси і необхідний рівень їх захисту. У штатному розділі наводяться описи посад з точки зору інформаційної безпеки. Нарешті, розділ, що описує правила розмежування доступу до корпоративної інформації, є ключовим для визначення внутрішнього порушника [9].

Будь-яке порушення легальним співробітником політики безпеки організації автоматично робить його внутрішнім порушником. Подібні дії можна розділити на умисні і ненавмисні. Ненавмисні дії викликані недоліком кваліфікації користувачів і в даній роботі не розглядаються. Умисні дії розрізняються по цілях: спрямовані на отримання конфіденційної інформації поза рамками основної діяльності та пов'язані з порушенням розпорядку роботи.

Однак дослідження, проведене компанією Gartner Group показало, що 85% сучасних компаній не мають ні концепції, ні політики безпеки [10]. І хоча ситуація повинна змінитися – за прогнозами Gartner до 2005 року таких компаній буде тільки 50%, слід внести корективи у формулювання внутрішнього порушника. Таким чином, для більшості компаній внутрішнього порушника не можна визначити, як особу, що порушує політику безпеки, так як остання просто відсутня. Тому в подібному випадку внутрішнім порушником, чинним навмисне, будемо вважати співробітника компанії, робилися

спрямовані спроби отримання, зміни або знищення конфіденційних даних організації поза рамками основної діяльності співробітника.

Прикладами таких дій можуть бути:

- Несанкціонований доступ до даних про клієнтів і співробітниках організації поза рамками основної діяльності;
- Спроби зміни статусу користувача;
- Спроби підбору паролів в захищені програми, області дискового простору;
- Умисні дії, пов'язані зі спробами зміни інформаційного наповнення системи;
- Умисні дії, спрямовані на деструкцію системи;
- Впровадження апаратних і програмних "закладок" і "вірусів", дозволяють долати систему захисту, потай і незаконно здійснювати доступ до системних ресурсів мережі;

Керуючись положенням «про технічний захист інформації в Україні», визначимо кваліфікацію передбачуваного внутрішнього порушника. Будемо припускати, що порушник за рівнем можливостей в системі відноситься до 3-го рівня. Третій рівень визначається можливістю управління функціонуванням автоматизованих систем, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування. 4-му, і самому високому, рівню відповідає системний адміністратор або адміністратор безпеки, чиї можливості в системі максимальні по визначенням. За образним висловом одного з експертів по інформаційної безпеки компанії ISS, мережевий адміністратор - це «сірий кардинал» компанії, якому доступна практично вся інформація в організації. Тому ми обмежуємося розглядом 3-го рівня, коли порушник у межах своєї робочої станції має широкі можливості по модифікації програмного забезпечення та апаратної частини.

Відзначимо що, згідно розглянутого положення, в своєму рівні порушник є спеціалістом вищої кваліфікації, знає все про АС і, зокрема, про систему і засоби її захисту. Дане припущення дозволяє більш адекватно оцінювати можливі погрози. Наприклад, у компаніях, що займаються наданням послуг

інформаційної безпеки, більшість співробітників є кваліфікованими технічними фахівцями.

При створенні моделі порушника й оцінці ризику втрат від дій персоналу необхідно диференціювати всіх співробітників по їх можливостях доступу до системи і, отже, по потенційному збитку від кожної категорії користувачів. Наприклад, оператор чи програміст може завдати незрівнянно більший збиток, ніж звичайний користувач, тим більше непрофесіонал.

Нижче наводиться приблизний список персоналу типовою корпоративної мережі і відповідне ступінь ризику від кожного з них [11]:

1. Найбільший ризик:
- Мережевий адміністратор;
- Адміністратор безпеки.

2. Підвищений ризик:
- Оператор системи;
- Оператор введення і підготовки даних;
- Менеджер обробки;
- Системний програміст.

3. Середній ризик:
- Інженер системи;
- Менеджер програмного забезпечення.

4. Обмежений ризик:
- Прикладний програміст;
- Інженер або оператор з зв'язку;
- Адміністратор баз даних;
- Інженер з обладнання;
- Оператор периферійного обладнання;
- Бібліотекар системних магнітних носіїв;
- Користувач - програміст;
- Користувач - операціоніст.

5. Низький ризик:
- Інженер по периферійному обладнанню;

- Бібліотекар магнітних носіїв користувачів;
- Користувач мережі.

Кожен з перерахованих вище користувачів у відповідності зі своєї категорією ризику може завдати більший або менший збиток системі.

Ми не розглядаємо тут питання мотивації співробітників, спонукають їх здійснювати протиправні дії. Однак відзначимо, що найчастіше причинами є: робота на компанію- конкурента, цікавість, помста керівництву компанії.

3.3 Модель типової корпоративної мережі

Розгляд можливих дій зловмисників необхідно вести в умовах, які існують в сучасних вітчизняних компаніях. Розглянемо типову корпоративну мережу, побудовану на апаратних і програмних засобах, які широко використовуються в корпоративних мережах приватних і державних організацій.

Апаратні засоби корпоративних мереж включають фізичну середовище і обладнання передачі даних. Внаслідок обмеженого застосування в даний час бездротових мереж, типова корпоративна мережа побудована на основі кабельної системи, що представляє собою виту пару 5-ї категорії. Сучасні корпоративні мережі розробляються з застосуванням комутаторів (switch) і концентраторів (hub). Обидва цих мережевих пристрої служать для об'єднання комп'ютерів в локальні мережі. Хоча концентратори в даний час витісняються комутаторами, тим не менш, у багатьох мережах організацій концентратори широко використовуються в силу своєї дешевизни. Комутатор представляє собою більш складне мережеве пристрій. І як наслідок розрізняються за набору підтримуваних функцій. Найбільш складні (і дорогі) моделі називаються керованими інтелектуальними комутаторами і володіють власним IP-адресою, підтримкою віддаленого адміністрування, засобами організації віртуальних мереж (VLAN) і розвиненим набором засобів захисту. Вартість інтелектуальних комутаторів може досягати 2000 доларів, що ускладнює їх купівлю невеликими організаціям. програмні засоби, що використовуються у типовій мережі, також

є стандартними для більшості організацій. Робочі станції на базі операційних систем (ОС) Windows 95, 98, NT4 Workstation, 2000, XP (за статистикою в 90 % всіх організацій у світі використовуються робочі станції на базі Windows різних версій). Сервера на базі ОС Windows NT4 Server/Terminal Server Edition, 2000 Server, 2003 Server. Пакети популярного програмного забезпечення (ПО) для офісної роботи: 1С, MS Outlook, MS Office 97/2000/XP Серверне ПЗ: 1С, MS SQL Server, MS Exchange.

В якості засобів захисту використовуються міжмережеві екрани: Agnitum Outpost Firewall, Kerio Personal Firewall, Kaspersky Anti-Hacker, Norton Personal Firewall; системи виявлення атак Black ICE, Snort, RealSecure.

3.4 Дослідження Методів впливу порушника на корпоративну мережу

Порушник вивчає об'єкт нападу як теоретично, так і практично. Практичне дослідження об'єкта та його системи безпеки може бути пасивним і активним. Пасивним впливом називають вплив, яке безпосередньо не впливає на роботу корпоративної мережі, але яке може порушувати її політику безпеки. Зважаючи на відсутність безпосереднього впливу на роботу мережі, такий вплив дуже важко виявити. Прикладом пасивного впливу є прослуховування каналу зв'язку.

Активні дії припускають безпосередній вплив на роботу корпоративної мережі і порушують діючу в ній політику безпеки. У результаті активних дій у системі відбуваються певні зміни. Тому активні впливу легше виявити, ніж пасивні. Методи впливу внутрішнього порушника на корпоративну мережу зображені на рисунку 3.2.

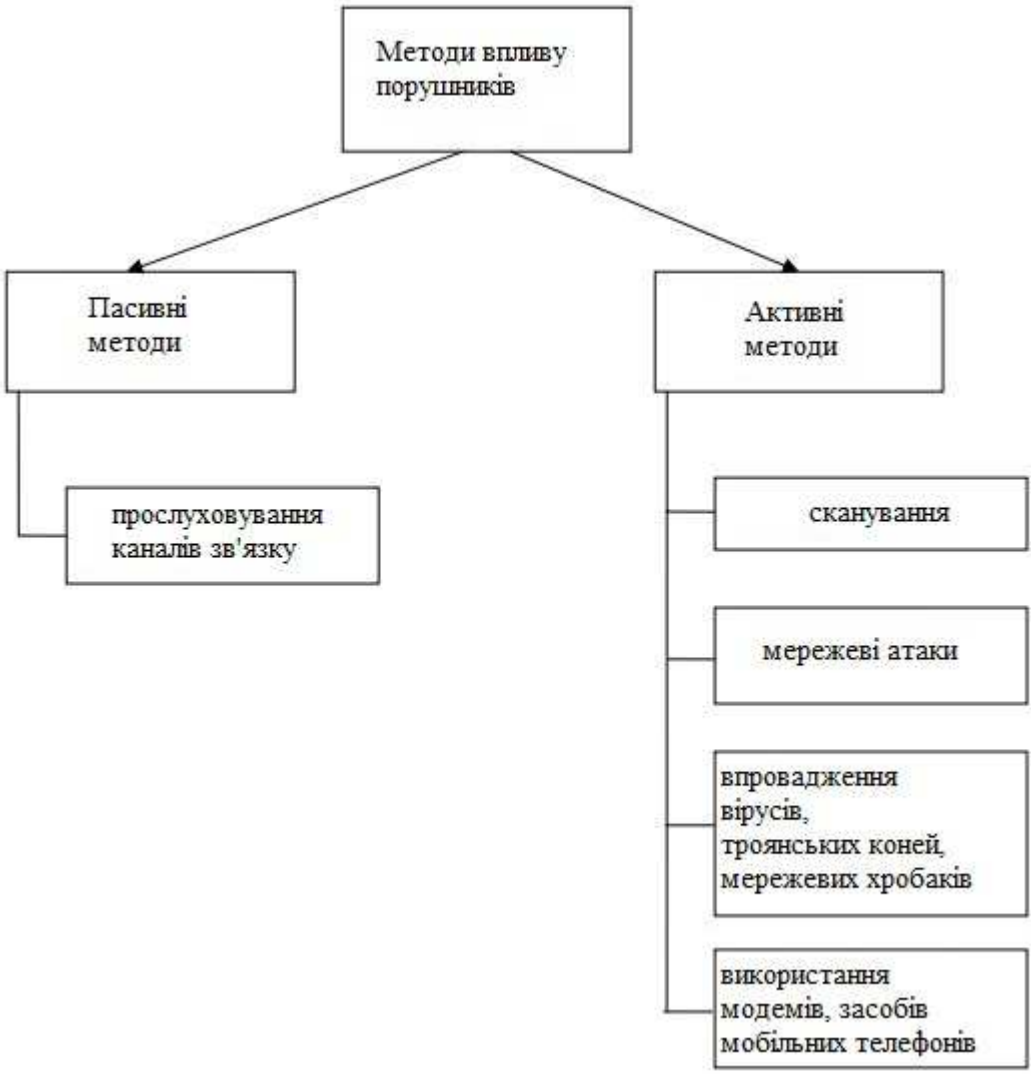

Рис. 3.2. Методи впливу внутрішнього порушника на корпоративну мережу

3.4.1 Пасивні методи впливу

Прослуховування мережевого трафіку

Розглянемо можливість прослуховування каналу зв'язку (sniffing) у локальної мережі організації. Для прослуховування трафіку необхідно перевести мережевий адаптер в «безладний» (promiscuous) режим. Уданому режимі адаптер перехоплює всі мережеві пакети, що проходять через нього, а не тільки призначені даному адресою, як у нормальному режимі функціонування. Якщо локальна мережа побудована на концентраторах, то для зловмисника виявляється доступним весь мережевий трафік в межах сегмента локальної мережі. У мережі побудованої на комутаторах, трафік прямує тільки

до того комп'ютера, якому він призначений. Тобто якщо комп'ютер "А" обмінюється пакетами з комп'ютером "В", то комп'ютер "З" не здатний перехоплювати цей трафік. Однак, існує ряд технологій дозволяють обійти обмеження, що накладаються комутаторами. Ці технології - ARP Spoofing (ARP – poisoning), MAC Flooding і MAC Duplicating [12].

Метод ARP-Spoofing заснований на атаці «людина посередині» (man-in-the-middle).

Дана атака можлива через уразливість в реалізації протоколу ARP. Протокол дозволу адрес ARP (Address Resolution Protocol) призначено для з'ясування MAC-адреси хоста по його IP - адресою. для обміну інформацією двом хостам в мережі Ethernet, кожному з них необхідно отримати MAC-адресу іншого. Ця процедура здійснюється з використанням протоколу ARP. Хост «А», бажаючий встановити з'єднання з хостом «В», спочатку перевіряє наявність MAC-адреси хоста «В» у своєму ARP-кеші. У разі його відсутності в кеші, здійснюється розсилка широкомовного запиту з метою виявити MAC-адресу, відповідний IP-адресою хоста «В». Хост «В», порівнявши IP-адреса в запиті зі своєю IP-адресою, посилає відповідь (ARP-reply), в який поміщає свою MAC-адресу. Обидва хоста «А» і «В» поміщають отримані MAC-адреси в свої ARP-кеші, щоб мінімізувати кількість широкомовних запитів. Тепер хости можуть обмінюватися даними використовуючи MAC-адреси.

Атаку на даний інформаційний обмін можливо зробити, тому що протокол ARP не вимагає аутентифікації. Для реалізації атаки зловмисникові з хоста «С» необхідно надіслати обом хостам згенеровані ARP-reply пакети:

- для хоста «А», в якому прописано, що IP-адрес хоста «В» відповідає MAC-адресу хоста «С»;
- для хоста «В», в якому прописано, що IP-адрес хоста «А» відповідає MAC-адресу хоста «С».

Хости «А» і «В» у відповідності зі специфікацією протоколу ARP, отримавши подібні reply-пакети, оновлять свої ARP - кеші. Тепер, пакети, що відправляються хостом «А» хосту «В» будуть фактично надсилатися хосту «С», оскільки в ARP-кеші хоста «А» IP-адресою хоста «У» відповідає MAC-адресу

хоста «С». Тому дана атака отримала також назву ARP-poisoning (отруєння ARP-кешу). Для нормальної передачі пакетів між хостами «А» і «В» хосту «С» необхідно виконувати функції роутера для даних хостів, тобто організувати їх передачу по маршрутах A-C-B і B-C-A.

Відзначимо деякі особливості реалізації даної атаки:

- так як протокол ARP функціонує тільки рамках однієї широкомовної підмережі, атаку ARP-spoofing не можна провести для хостів у різних підмережах або віртуальних локальних обчислювальних мережах (VLAN);
- оскільки операційна система хостів періодично оновлює ARP-кеш, хосту «С» необхідно періодично виконувати процедуру «отруєння кешу» для хостів «А» і «В»;
- у разі прослуховування трафіку між деяким хостом і роутером мережі, в результаті виходить, що зловмисник зможе прослуховувати трафік між даними хостом і будь-яким хостом в Інтернет.

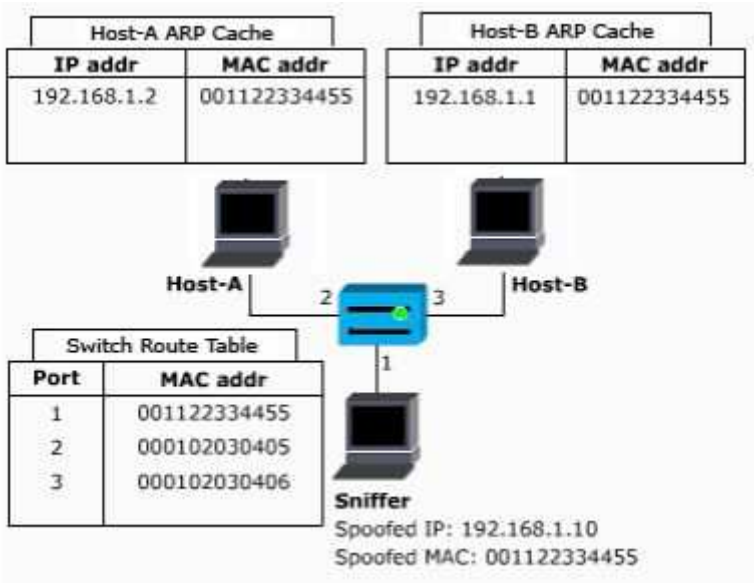

Рис. 3.3. Демонстрація атаки ARP-spoofing

Слід зазначити, що якщо на комутаторі не включена функція Port-Security (дана функція буде розглянута пізніше), то можна в якості MAC-адреси сніфферу використовувати будь яку другу MAC-адресу.

Атака MAC-duplicating полягає в установці на хості зловмисника «С» MAC-адреси, що збігається з MAC-адресою іншого хоста в мережі, наприклад «В». Тепер всі пакети, що направляються хосту «В» будуть також надіслані і хосту «С». Завдання зловмисника не відповідати на ці пакети, а тільки приймати їх.

Атака MAC-flooding заснована на особливості роботи комутаторів. Посилка на комутатор величезного числа ARP-запитів на неіснуючі IP-адреси, викличе переповнення пам'яті комутатора і його перехід в режим функціонування концентратора. Для зворотного переходу в нормальний режим функціонування необхідно перевантажити комутатор.

Таким чином, реалізуючи атаки ARP-Spoofing і MAC-duplicating, можна прослуховувати трафік між будь-якими хостами в локальній мережі корпорації, побудованої на концентраторах і комутаторах без використання шифрування.

Перехоплення мережевого трафіку здійснюється з використанням спеціального ПЗ-мережевих моніторів. Треба відзначити, що не всі мережеві монітори можуть перехоплювати весь мережевий трафік що проходить через них. Наприклад, Microsoft Network Monitor в стандартній комплектації Windows, відображає пакети адресовані тільки даному комп'ютеру. У той же час, існує безліч альтернативних мережевих моніторів, з яких самими багатими по набору функцій є Sniffer Pro від компанії NAI, IRIS Network Traffic Analyzer від компанії eEYE і TCP Dump. Цікавою програмою також є утиліта Cain&Abel 2.5 італійського фахівця з мережевої безпеки Massimiliano Montoro, що включає в себе багато корисних для адміністраторів функцій. Зазначимо, що переважній більшості снифферів для перехоплення всього мережевого трафіку потрібно встановити спеціальні драйвера, для чого потрібні адміністраторські права в ОС. Однак існують сніффери, що не вимагають ніяких спеціалізованих драйверів, наприклад, NGSSniff від компанії NGSS Inc., який може здійснювати захоплення, використовуючи Windows Sockets.

Досліджуємо, до яких наслідків може призвести прослуховування мережевого трафіку. Сучасні мережеві протоколи локальних і глобальних мереж розроблялися, коли проблеми інформаційної безпеки не були

першочерговими. Відповідно, в даних протоколах практично відсутні механізми захисту. Це справедливо для багатьох широко-використовуваних протоколів -TCP/IP, ARP, HTTP, FTP, SMTP, POP3 і т.д. Тому в останні 5-10 років були розроблені вдосконалені версії протоколів передачі даних, здатних протистояти загрозам безпеки. Однак за ряду причин перехід на більш захищені протоколи затягнувся. Так вже кілька років ведуться дискусії про перехід від використання в Інтернет протоколу IPv4 до IPv6, що включає специфікацію IPSec для захисту переданих даних. А в корпоративних мережах як раніше використовуються незахищені протоколи. Розглянемо уразливості цих протоколів важливі стосовно до корпоративних мереж.

Основними слабкостями мережевих протоколів є відсутність засобів забезпечення конфіденційності даних. Так, за наявності у корпоративній мережі поштового сервера з доступом за протоколах POP3, SMTP і IMAP, зловмисник, що перехоплює трафік між поштовим сервером і будь-яким вузлом мережі (наприклад, комп'ютером директора) , може заволодіти аутентификационного даними користувача. Це можливо, оскільки згідно специфікації протоколу POP3 [13] аутентифікаційні дані передаються в відкритому вигляді. Використання даної уразливості ілюструє наступний рисунок (рис. 3.4).

Таким чином, внутрішній порушник, використовуючи спеціальне ПЗ, може отримати паролі всіх користувачів до корпоративного поштового сервера. У результаті зловмисник зможе читати будь-яку корпоративну переписку, а також писати листи від імені інших користувачів. Так само можна використовувати скомпрометований поштовий обліковий запис для виносу з корпоративної мережі конфіденційної інформації. Наприклад, використовуючи обліковий запис-якого службовця переслати внутрішні конфіденційні матеріали на тимчасовий безкоштовний електронний ящик в Інтернеті.

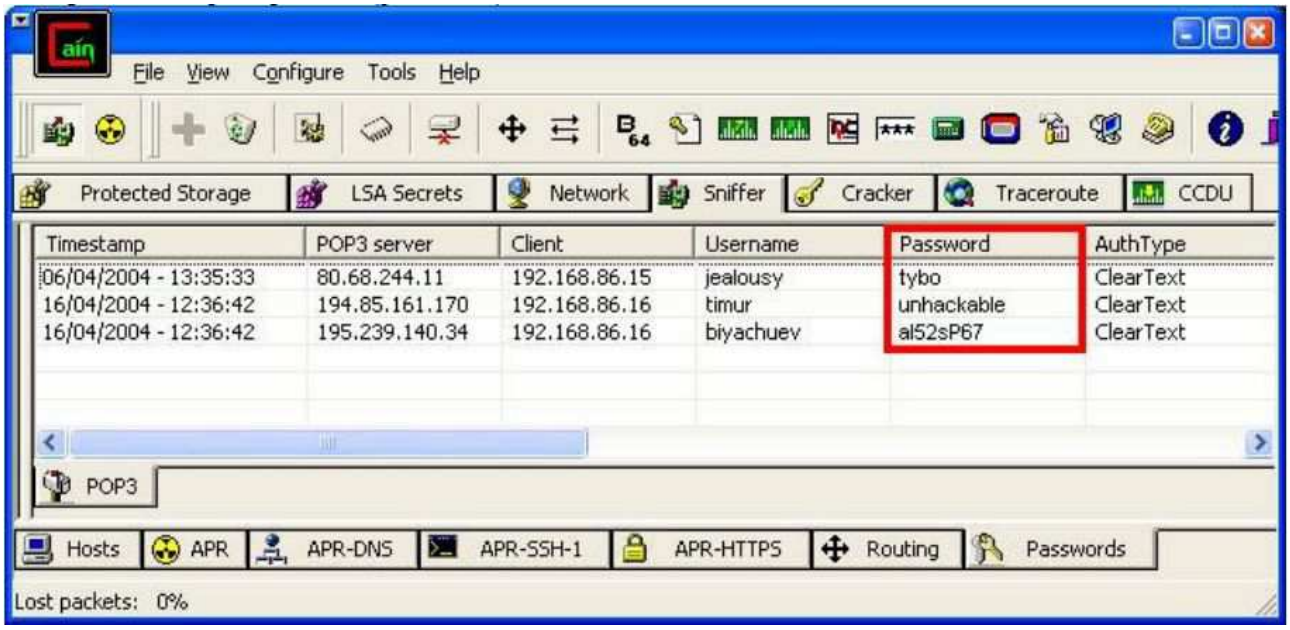

Рис. 3.4. Екранний знімок програми Cain & Abel, перехоплюючий поштові паролі.

Проте існують більш серйозні наслідки перехоплення поштових облікових записів. При використанні поштових серверів на базі Microsoft Exchange в мережах побудованих на базі домену Windows NT/2000, при створенні користувача, відразу ж створюється поштовий ящик з тими ж ім'ям користувача і паролем, що і для доступу до домену Windows NT. В результаті, перехоплення аутентифікаційних даних поштового сервера дозволяє зловмисникові отримати доступ до домену від імені іншої особи, наприклад, свого безпосереднього начальника. А, скомпрометувавши комп'ютер адміністратора мережі, можна отримати практично необмежений доступ до її інформаційних ресурсів.

Знаючи доменні аутентифікаційні дані користувача або адміністратора домену, зловмисник може отримати практично повний доступ до даних, що зберігаються на локальних машинах. В ОС Windows 2000/XP/Server при запущеній службі доступу до файлів і принтерів (file and printer sharing), функціонуючої за протоколом NetBIOS, в налаштуваннях за замовчуванням для доступу з мережі відкриті всі диски комп'ютера (під адміністраторським паролем). Дана функція реалізована для адміністративних потреб, однак вона надає значну небезпеку. Знаючи аутентифікаційні дані користувача комп'ютера,

якщо комп'ютер не входить у домен, або адміністратора домену, якщо комп'ютер включений в домен, можна отримати необмежений доступ до файлових ресурсів комп'ютера.

Так само скомпрометованим виявиться і файловий сервер - основне сховище конфіденційної інформації компанії. Оскільки доступ до файлового сервера Windows, функціонуючому найчастіше по протоколу NetBIOS, також здійснюється за аутентифікаційними даними домену.

У разі використання в корпоративній мережі файлового FTP-сервера, можливе перехоплення аутентифікаційних даних і в цьому випадку. У специфікації протоколу FTP також не передбачено приховання параметрів аутентифікації [14].

Використання внутрішнього Web-сервера в корпорації з розмежуванням доступу поки не поширене. Однак і в цьому випадку без прийняття спеціальних заходів (наприклад, підтримки SSL), в режимі «базової аутентифікації» по протоколу HTTP ім'я користувача і його пароль передаються у відкритому вигляді. Також не шифрують передані дані протоколи Telnet і SNMPv1.

Багато користувачів мають безкоштовні поштові скриньки в Інтернеті, такі як mail.ru, hotbox.com і т.д. Доступ до цих скриньках здійснюється з використанням web-інтерфейсу або за допомогою поштових програм, таких як Microsoft Outlook або The Bat. У більшості випадків користувачі, не бажаючи запам'ятовувати безліч паролів, вибирають один і той же пароль для безлічі служб - безкоштовного поштового сервера, сервера додатків, комп'ютера на роботі або домену. Таким чином, перехоплений зловмисником пароль до поштової серверу до Інтернету, може надати йому доступ до ресурсів корпоративної мережі. На підтвердження актуальності даної загрози, наведемо результати дослідження InfoSecurity 2003. Серед 152 учасників дослідження слово «password» у вигляді пароля використовують 12%. Популярнішою тільки власне ім'я користувача-16%. Далі йдуть назви футбольної команди (11%) і дата народження (8%). Упорядники InfoSecurity 2003 також встановили, що дві третини громадяни використовують скрізь один той же пароль: і на роботі, і для банківського рахунку, і для електронної пошти.

Слід зазначити, що в даний час набули широкого поширення служби миттєвого обміну повідомленнями (IM-служби) - ICQ, Windows Messenger, AOL та інші. Миттєві повідомлення (IM, instant messaging) - зручне доповнення, а в ряді випадків, і непогана заміна листуванні по електронній пошті. На відміну від електронної пошти, миттєва передача повідомлень дозволяє користувачеві бачити чи доступний вибраний один або співробітник в мережі. Як правило, IM-служба дає користувачеві інформацію, якщо доступний хтось із кореспондентів особистого списку користувача. Служба миттєвого обміну повідомленнями також вигідно відрізняє від електронної пошти можливість двостороннього обміну повідомленнями практично в реальному масштабі часу. Існує величезне число користувачів такого зв'язку, у неї маса прихильників і навіть своїх ідеологів, які доводять, що використання миттєвої передачі повідомлень на робочому місці замість традиційної електронної пошти веде до більш ефективної і надійної зв'язку робочого місця і, тому, до більш високої продуктивності праці співробітників. В результаті, IM швидко розвивається і в професійних і в особистих додатках. За інформацією Ferris Research, до 70 % офісних працівників користуються «ICQ» або іншими IM-інструментами в ділових цілях, цілком покладаючись на їх надійність. Однак використання такої служби в компанії призводить до появи серйозних загроз. У Зокрема, дані, передані по мережі служби миттєвої передачі повідомлень, не шифруються. Так що в більшості IM-мереж перехоплення повідомлень можна знову таки використовувати звичайний сніффер. Це особливо небезпечно у великих корпораціях, так як часто особиста, секретна та інша конфіденційна інформація передається по ICQ або інший IM-мережі (так як існує поширена помилкова думка про більшу надійність саме такого способу передачі самої секретної інформації). Перехват IM-повідомлень за допомогою програми-сніффера ICQ-повідомлень ICQ sniff зображено на рисунку (рис. 3.5)

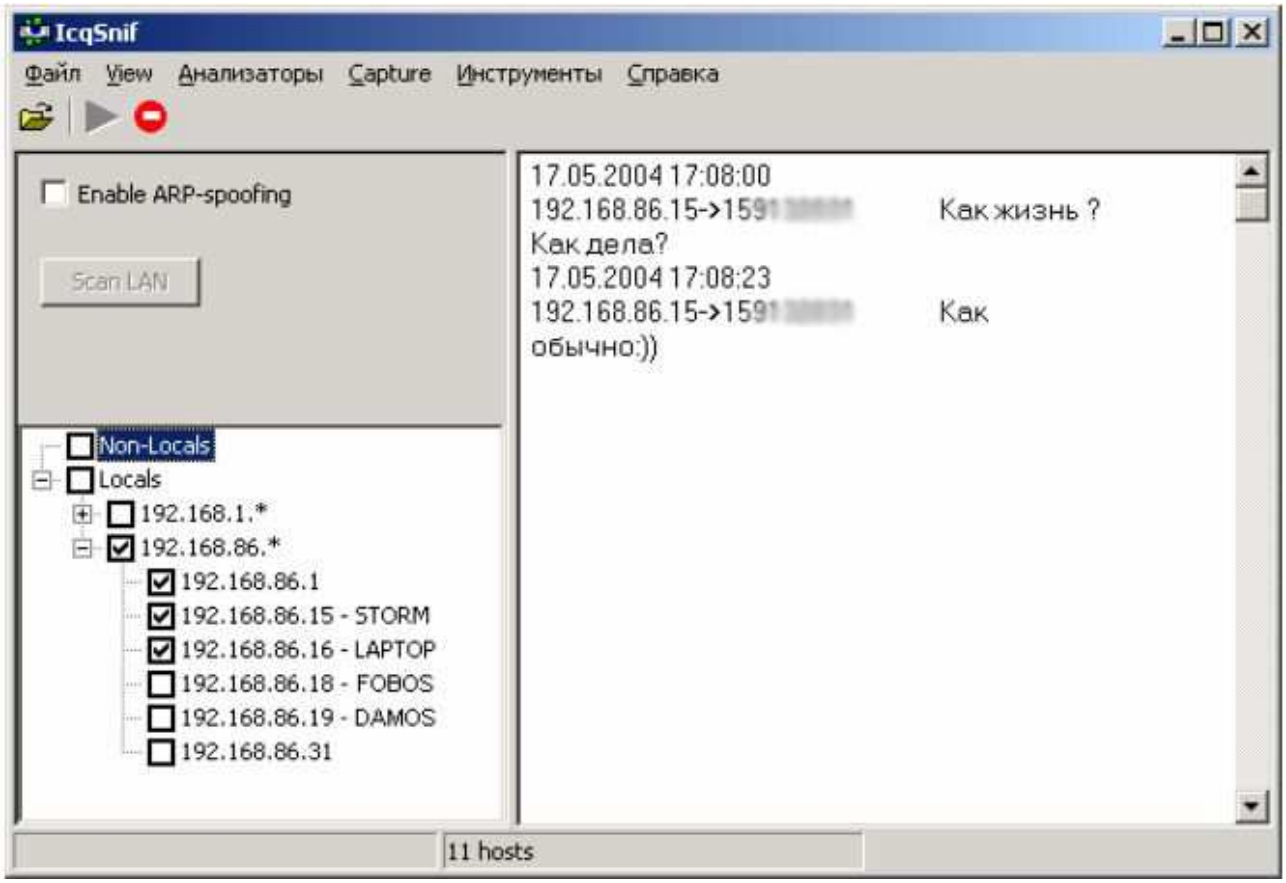

Рис. 3.5. Перехоплення ІМ-повідомлень за допомогою програми - сніфферу ICQ-повідомлень ICQ Sniff

Ми розглянули уразливості протоколів передачі даних без механізмів аутентифікації і з вбудованими механізмами аутентифікації, а тепер досліджуємо захищеність протоколів мережевої аутентифікації.

Аутентифікація є процес перевірки автентичності користувача, тобто підтвердження того, що користувач дійсно має обліковий запис і може її використовувати при зверненні до служб і ресурсів як локальним, так і мережевим. В даний час в мережах, побудованих на базі MS Windows, застосовуються такі протоколи аутентифікації: LAN Manager, NTLM v.1, NTLM v.2, Kerberos. З розвитком Windows компанія Microsoft прагнула посилити безпека застосовуваних протоколів аутентифікації. Так протокол LAN Manager, що володіє дуже низькою криптостійкістю був замінений протоколом NTLM v.1, який після знайдених в ньому вразливостей був модифікований до версії NTLM v.2. Проте в результаті були знайдені вразливості методу аутентифікації і для цього протоколу [15]. Тому в Windows 2000 Microsoft перейшла на новий

протокол перевірки достовірності в мережах - Kerberos v.5, що є відкритим промисловим стандартом. Тим не менш, були знайдені вразливості і у цього механізму аутентифікації в Windows [16], [17]. Зазначимо, що для сумісності з попередніми версіями Windows, в старших версіях здійснюється підтримка всіх менш надійних протоколів аутентифікації.

В результаті, прослуховуючи трафік можна отримати аутентифікаційні дані, що представляють собою права доступу до мережевих ресурсів, наприклад, доменні облікові записи користувачів. Паролі посилаються по мережі не у відкритому вигляді, а у вигляді хешей (рис 3.6). Таким чином, перехопивши аутентифікаційні дані, можна спробувати відновити по них вихідні паролі.

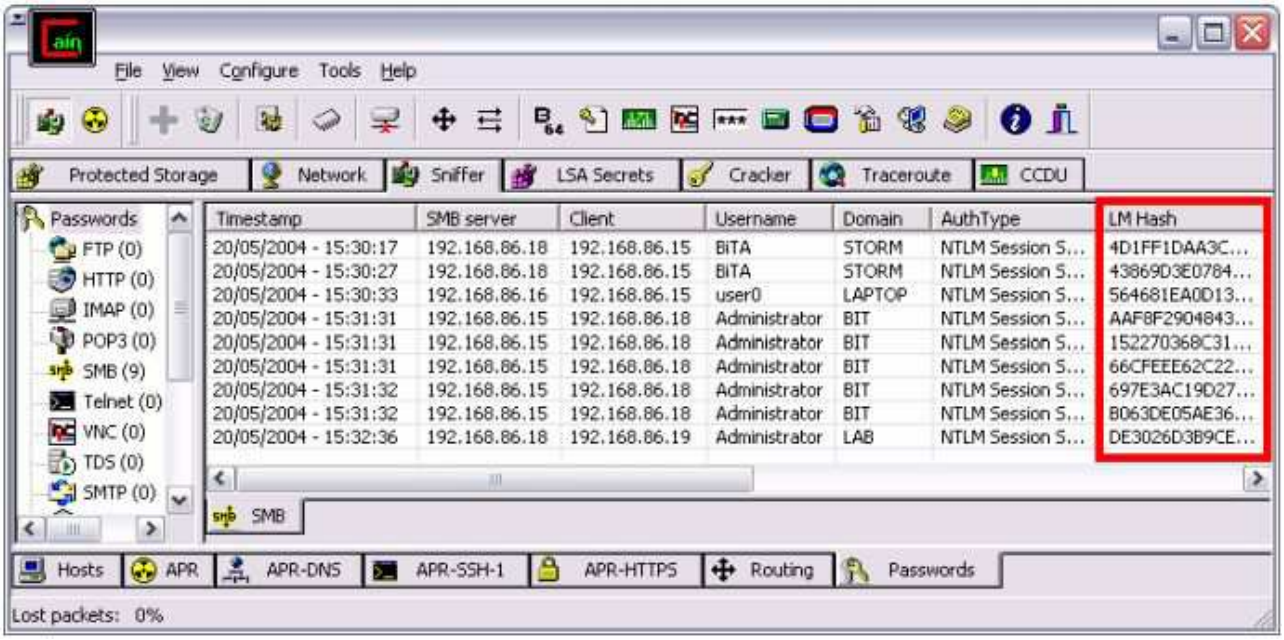

Рис. 3.6. Захват даних аутентифікації

Досліджуємо, наскільки небезпечна можливість перехоплення паролів з точки зору їх подальшого злому. Розглянемо два основних підходи до криптоаналізу: перебір (прямий або за словником) і з використанням таблиць попередніх обчислень (table precomputation).

При методі прямого перебору атакуючий пробує всі можливі ключі для дешифрування тексту. Перебір за словником передбачає, що пароль наймовірніше є осмисленим словом або простий комбінацією слів, букв, цифр.

Існують спеціалізовані словники, що містять комбінації, найбільш часто вживаних паролів. Застосування атаки по словнику дозволяє значно скоротити час, необхідний для підбору паролів (рис. 3.7).

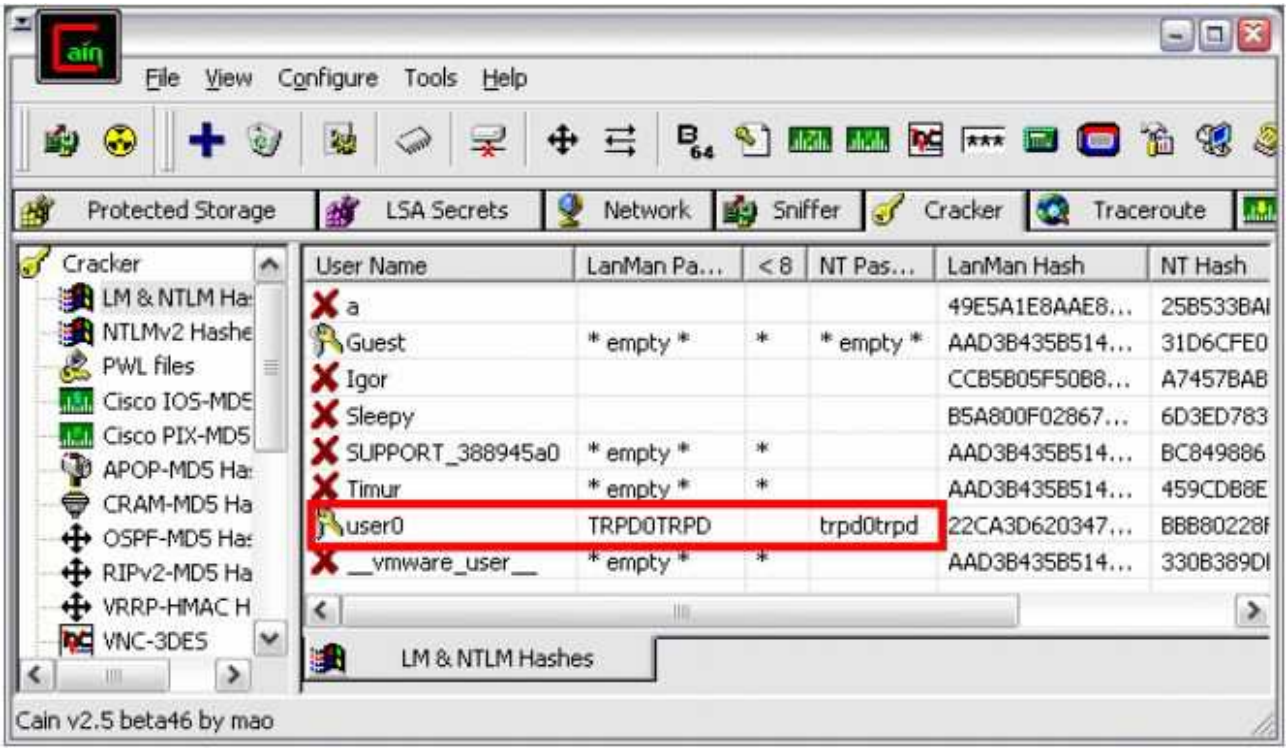

Рис. 3.7. Підбір паролів користувача User0 методом прямого перебору

Ідея таблиць попередніх обчислень полягає в тому, щоб попередньо обчислити і зберегти в таблиці вибірковий вихідний текст і відповідні ключі для всіх можливих ключів. Вперше подібний метод запропонував в 1980 році Matrin Hellman. Модифікований швейцарським вченим-дослідником Philippe Oechslin метод отримав назву «Time-Memory Trade-Off» (компроміс між часом і пам'яттю) [18]. Для перевірки теоретичних положень була розроблена програма RainbowCrack [19].

Програма дозволяє побудувати попередні хеш - таблиці для заданого набору символів і далі по готовим таблицями підбирати паролі. Наприклад, для підбору паролів складаються лише із символів латинського алфавіту і довжиною не більше 7 символів, зашифрованих за допомогою алгоритму, застосовуваного в LAN Manager, буде потрібно не більше 3-х діб обчислень на комп'ютері Celeron 666 MHz. Об'єм таблиць складе порядку 610 Мбайт. Далі, з наявною таблицею підбір будь-якого пароля, задовольняє заданим умовам,

складе не більше 10 секунд. Існують і онлайнові підбирачі паролів, однак вони обмежені по довжині підбираючих паролів.

Наводжу й інші розрахунки. Наприклад, створення таблиці для підбору паролів, що складаються з усіх символів латинського алфавіту, цифр і спеціальних символів і довжиною не більше 7 символів, зажадає близько 7, 5 років обчислень на Celeron 666 MHz при загальному обсязі бази 119 Gb. Звичайно, використання паралельних обчислень і більше потужних обчислювальних станцій може значно скоротити час створення подібних таблиць.

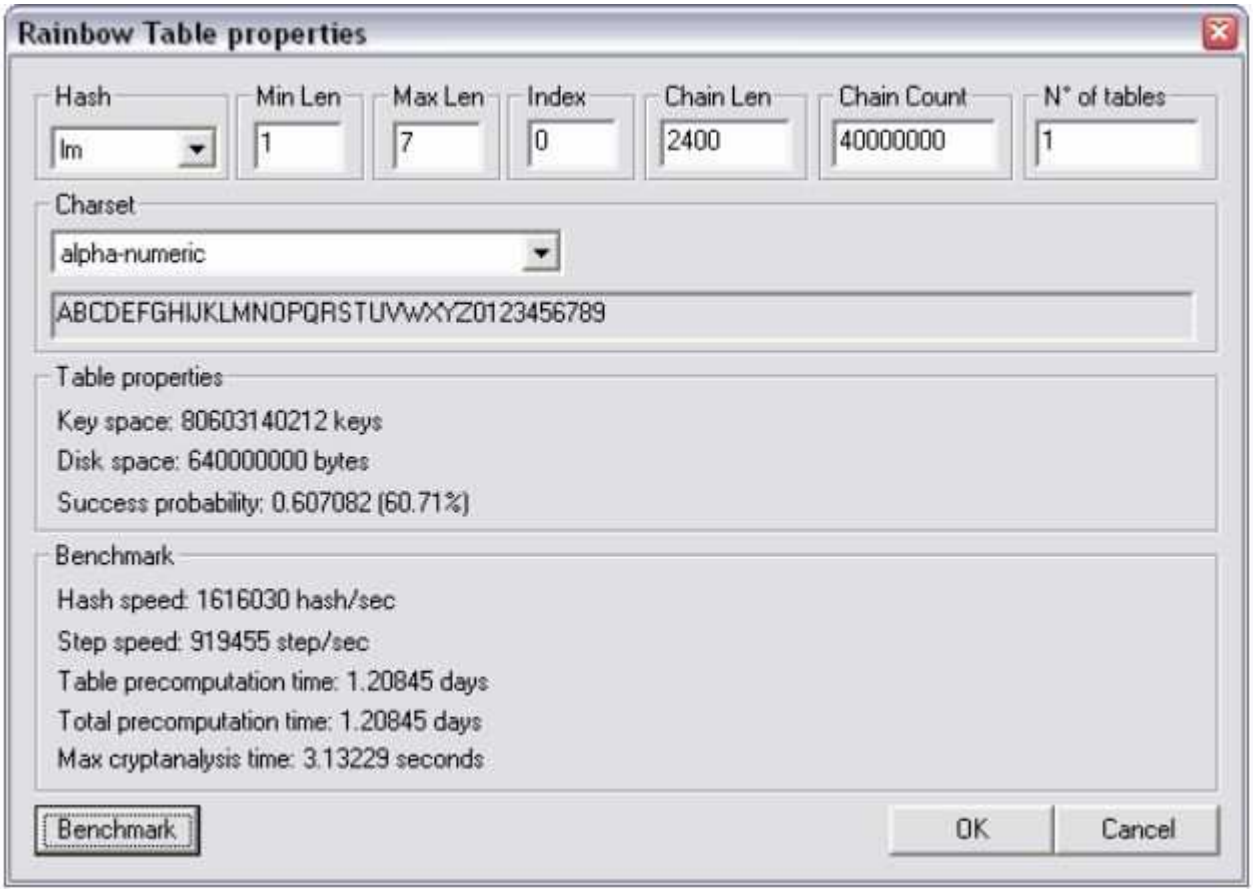

Рис. 3.8. Вікно програми Winrtgen 1.1 для генерації кеш-таблиць

3.4.2 Активні методи впливу

Сканери вразливостей

Сканування вразливостей - це автоматизований процес, спрямований на виявлення відомих вразливостей в мережевих і програмних платформах. Адміністратори використовують сканери вразливостей для оцінки ефективності захисту компонентів їх корпоративної мережі. В результаті аналізу визначаються вразливі місця системи, які можуть бути використані зловмисниками для здійснення несанкціонованого доступу, і адміністратор вживає заходів щодо їх усунення. Таким чином, результатом роботи сканера є досить докладна інформація про корпоративну мережу, яка включає список мережевого обладнання, комп'ютерів, з запущеними на них службами, версіями мережевого програмного забезпечення, вразливостей властивих даному ПО, облікові записи користувачів системи.

Таким чином, сканування зловмисником вразливостей є етапом, предвісником атаки. На практиці, внутрішній порушник може зібрати дуже важливу інформацію, яка є недоступною для нього в рамках службових повноважень. Наприклад, визначити ролі комп'ютерів в корпоративній мережі, виділити файлові сервера і сервера баз даних, маршрутизатори і інтелектуальні комутатори. І що особливо важливо, саме результати сканування дозволяють точно підібрати експлойти для здійснення безпосередньо несанкціонованого доступу до вузлам корпоративної мережі. Розглянемо результати використання сканера вразливостей Internet Security Scanner (ISS) в моделюється корпоративної мережі (рис. 3.9). Слід зазначити, що зловмисник для цих цілей, наймовірніше, скористається одним з безкоштовних сканерів. Однак застосування в даному прикладі комерційного сканера ISS обумовлено тим, що це один із кращих інструментів для аналізу захищеності мереж.

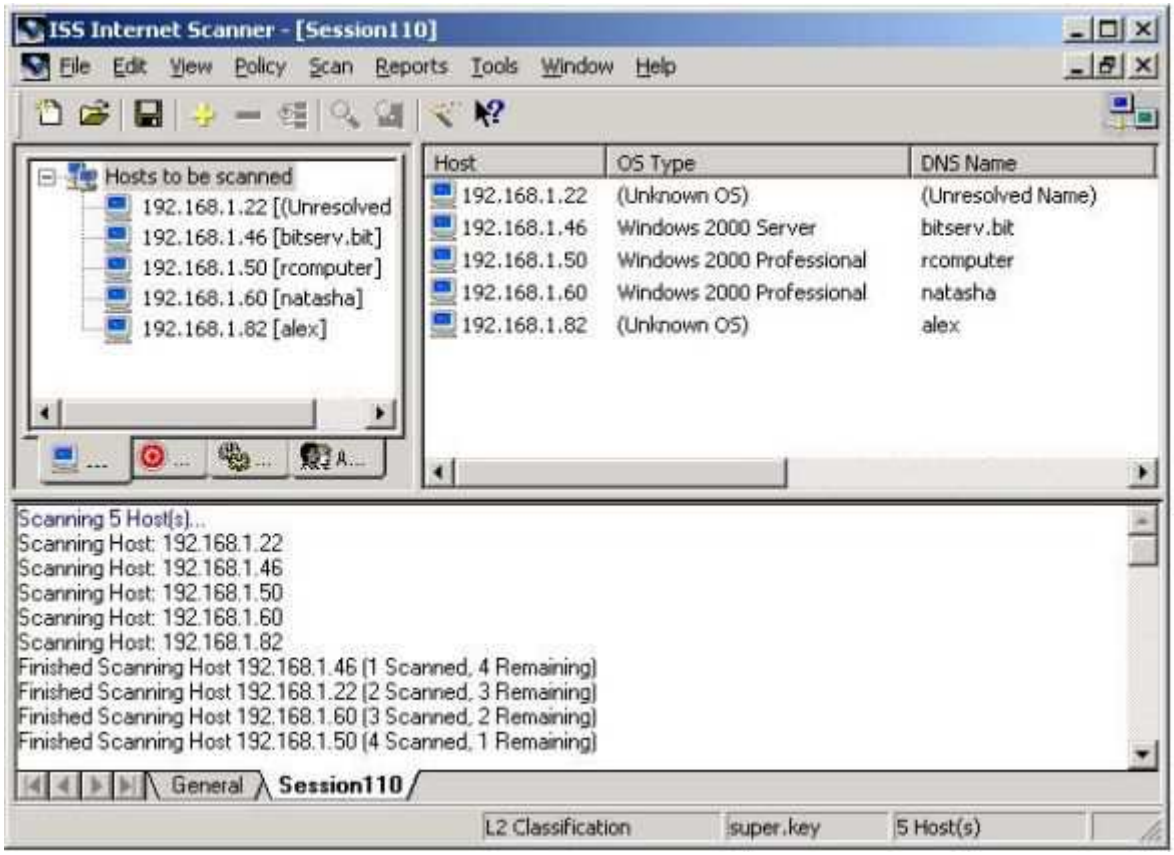

Рис. 3.9. Результати сканування типової мережі

Зловмисник, проаналізувавши служби, запущені на хостах, може розділити їх за функціональною ознакою – доменні контролери, файлов , термінальні, принт-сервера, робочі станції. За результатами сканування можна з'ясувати, яким відомим вразливостям схильні досліджувані хости, і підібрати для подальшої атаки відповідні експлойти.

Мережеві атаки

Всі мережеві атаки за способом маніпуляції з даними можна розділити на три групи:

- атаки, засновані на переповненні буфера (overflow based attacks);
- атаки, спрямовані на відмову-в-обслуговуванні (Denial-Of-Service attacks);
- інші атаки.

Атаки, засновані на переповненні буфера, використовують вразливість системи, яка полягає в некоректній програмної обробці даних. При цьому з'являється можливість виконання шкідливого коду з підвищеними привілеями.

Розглянемо реалізацію атаки подібного типу на прикладі уразливості, знайденої в Microsoft Internet Information Services (IIS) 4.0 і 5.0. Уразливість дозволяє зловмисникові виконати віддалене переповнення буферу. Некоректну перевірку кордонів змінних виробляє ISAPI фільтр при обробці параметрів .IDA файлів. Мережевий черв'як Code Red використовує дану уразливість для проникнення на веб -сервер, використовуючи наступний запит:http://www.example.com/default.ida?NNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%u
cbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u90
90%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a

У даному прикладі, 224 символа N в якості аргументу передаються файлу default.ida і використовуються для переповнення буфера. Наступний далі машинний код впроваджується (inject) в стек і виконується на сервері який атакують.

Атаки типу відмова-в-обслуговуванні не обов'язково використовують уразливості в програмному забезпеченні системи, що атакується. Порушення працездатності системи відбувається через те, що посилають їй дані наводять до значної витрати ресурсів системи.

Найпростішим прикладом атаки цього типу є атака «Ping Of Death». Сутність його в наступному: на машину жертви надсилається сильно фрагментований ICMP пакет великого розміру (64KB). Реакцією систем Windows 95/98 на отримання такого пакету є повне зависання.

Інші види атак використовують помилки в конфігурації мережевих сервісів, що дозволяють зловмисникам виконувати системні команди і отримувати несанкціонований доступ до даних. Прикладом тут можуть бути атаки, що використовують розміщені на веб-сервері вразливі CGI-скрипти. Задаючи спеціальні параметри цим скриптам, зловмисник може отримати, наприклад, доступ до файлової системи веб-сервера.

Розглянемо більш докладно мережеві атаки, засновані на використанні вразливостей в програмному забезпеченні мережних додатків.

Переклад терміну "exploit" у вітчизняних публікаціях не зустрічається, і еквівалента цього слова в українській мові також немає. Тому надалі буде використовуватися транслітерація з англійської - "експлойт". Даний клас атак заснований на експлуатації різних дефектів у програмному забезпеченні (тому й отримав таку назву - від англ. експлуатувати, використовувати). Слід відзначити, що останнім часом поряд з терміном «exploit», став застосовуватися термін «PoC» (від англ. Proof of Concept – дослівно доказ ідеї, рішення або демонстраційний приклад). Даний термін більш точно відображає дослідний сенс експлойта - демонстрація, що підтверджує можливість реалізації знайденої уразливості. Тому на сайтах, присвячених інформаційної безпеки, частіше використовується саме термін PoC.

Експлойти являють собою шкідливі програми, реалізують відому уразливість в ОС або прикладному ПЗ, для отримання несанкціонованого доступу до уразливому хосту або порушення його працездатності. Сучасні програмні продукти через конкуренцію потрапляють у продаж з помилками і недоробками. Розробники, включаючи в свої вироби всілякі функції, не встигають виконати якісну налагодження створюваних програмних систем . Помилки і недоробки, що залишилися в цих системах, призводять до випадкових і навмисним порушень інформаційної безпеки. Наприклад, причинами більшості випадкових втрат інформації є відмови в роботі програмно-апаратних засобів, а більшість атак на комп'ютерні системи засновані на знайдених помилках і недоробки в програмному забезпеченні. Так, наприклад, за перші півроку після випуску серверної операційної системи компанії Microsoft Windows Server 2003 було виявлено 14 вразливостей, 6 з яких є критично важливими [20]. Незважаючи на те, що з часом Microsoft розробляє пакети оновлень, що усувають виявлені недоробки, користувачі вже встигають постраждати від порушень інформаційної безпеки, що трапилися з причини помилок які залишились. Така ж ситуація має місце і з програмними продуктами інших фірм.

Таким чином, перед адміністраторами стоїть проблема стеження за періодичним встановленням оновлень і латочок ПО, усуваючі відомі вразливості. Однак, як показує практика, оновлення встановлюються вкрай нерегулярно. Більше того, після установки деяких латочок, що вносять зміни в ОС, деяке прикладне ПЗ перестає нормально функціонувати. Адміністратори бувають змушені відмовитися від установки оновлень, щоб зберегти працездатність корпоративного ПЗ. Така ситуація створює додаткові загрози.

Розглянемо дію експлойтів на прикладі експлойта KaHt2, реалізує одну з найсерйозніших вразливостей, знайдену в MS Windows. Даний експлойт організовує атаку типу «відмова-в-обслуговуванні» (Denial-Of-Service, DoS) на службу «Віддаленого виклику процедур» (Remote Procedure Call, RPC). Атаці уразливі системи MS Windows NT/2000/XP/2003 [13]. Експлойт KaHt2, реалізує атаку на службу RPC, в результаті якої здійснюється помилка переповнення буфера, що дозволяє зловмисникові виконати будь-який код на віддаленій системі (рис. 3.10).

У процесі атаки протягом короткого проміжку часу (порядку 0,1 сек.) на 135-й порт, що відповідає за службу RPC, з хоста зловмисника BLACK надсилається шторм TCP -пакетів на хост HOST1. У силу уразливості служби RPC на вузлі HOST1 виникає помилка переповнення буфера і виконується код експлойта, відкриває командну оболонку на порту 33815.

Дія всіх експлойтів зводиться або до отримання віддаленого доступу до атакується системі у вигляді командної оболонки, т.зв. шелла (shell або rootshell), або в віддаленому виконанні якої-небудь системної команди (наприклад, додавання нового користувача командою net user add), або до вимушеної перезавантаженні видаленої системи (рис. 3.11).

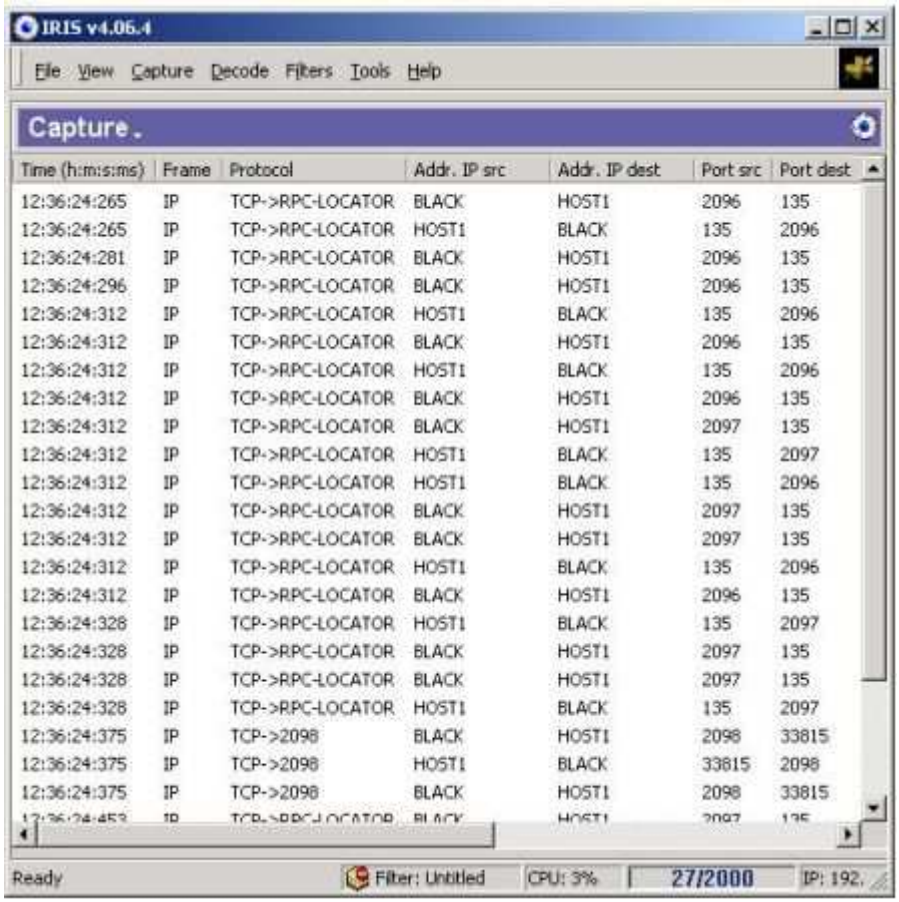

Рис. 3.10. Атака на службу RPC (135-й порт) з хоста BLACK на хост HOST1

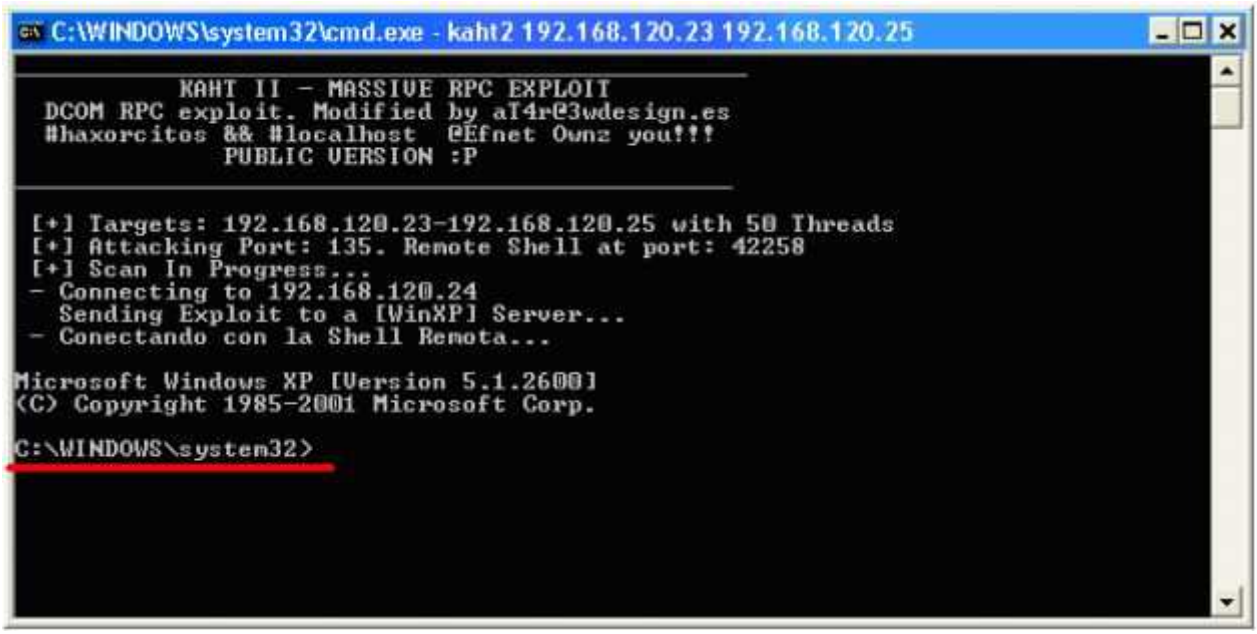

Рис. 3.11. В результаті реалізації уразливості Windows XP SP1експлойтів kaHt2 отримана командна оболонка видаленої системи.

Для даного та багатьох інших експлойтів характерна наявність функцій придушення антивірусних програм і міжмережевих екранів.

Наслідки застосування експлойтів можуть бути самими критичними. У разі отримання зловмисником віддаленого доступу до системи, він має практично повний (системний) доступ до комп'ютера. Наступні дії зловмисника і збиток від них можуть бути наступними:

- впровадження троянської програми. Блокуючи роботу антивіруса, можна встановити на скомпрометованій системі програму віддаленого адміністрування – так званого троянського коня;
- впровадження набору утиліт для приховування факту компрометації системи, так званих Rootkits;
- несанкціоноване копіювання зловмисником даних з жорстких і знімних носіїв інформації скомпрометованої системи;
- заклад на віддаленому комп'ютері нових облікових записів з будь-якими правами в системі для подальшого доступу як віддалено, так і локально;
- крадіжка файла з хешами паролів користувачів комп'ютера для їх подальшого підбору. У разі якщо скомпрометованою системою є доменний контролер, то під загрозою опиняються всі користувачі даного домену;
- знищення або модифікація інформації на віддаленому хості. Може призвести до значних фінансових або матеріальних втрат;
- здійснення дій від імені користувача скомпрометованої системи.

3.5 Троянські програми

Троянські програми (Trojans) - шкідливі програми, основне призначення яких непомітно проникнути на комп'ютер під виглядом законної програми і виконати шкідливі дії. Троянські програми (також звані троянцями або троянськими кіньми) складаються з двох частин: серверної (server) і клієнтської (client). Коли користувач, не підозрюючи, запускає серверну частину троянської програми, зловмисник використовує клієнтську частину для з'єднання з сервером по мережі. З'єднання зазвичай встановлюється за протоколами TCP і

UDP. Будучи запущеною, серверна частина робить дії, спрямовані на приховування своєї присутності в систем, маскуючись під інші процеси (рис. 3.12), чекає з'єднання клієнтської частини на певному порту, намагаються зупинити роботу антивірусів і міжмережевих екранів, перешкоджають його функціонуванню . Також, сервер троянської програми забезпечує свій запуск при наступному завантаженні системи в Windows для цього є кілька способів. Для використання серверної частини троянської програми, зловмисникові необхідно знати IP-адресу скомпрометованої системи. Оскільки навіть усередині корпоративної мережі можливе застосування динамічної адресації (DHCP), коли при кожному завантаженні хост одержує нову IP-адресу, троянські програми мають засоби оповіщення зловмисника про IP-адресу зараженої системи. Так можлива відправка серверної частиною адреси комп'ютера-жертви на електронну адресу, по ICQ або IRC.

Зазвичай троянські програми виконують одну або кілька завдань:

- надання віддаленого доступу зловмисникові (remote access). Найбільш поширена функція троянських програм, що дозволяє зловмисникові одержати повний доступ до комп'ютера-жертві.
- перехоплення і пересилання паролів. Троянські програми часто крадуть паролі для популярних програм, таких як Outlook , ICQ і т.д. з кеша або конфігураційних файлів, а також шляхом відстеження натискань клавіш. Зібрані паролі відсилаються на електронну адресу.
- запис всіх натискань клавіатурних клавіш (keyloggers). У даному випадку у файл записуються всі підряд натискання клавіш, для подальшого аналізу потрібної інформації. Файл з даними також пересилається електронною поштою.
- знищення файлів. Троянські програми з такою деструктивною функцією також відомі як логічні бомби. Найчастіше вони видаляють певні файли на комп'ютері-жертви в заданий час.
- створення платформи для розподіленої DoS-атаки. Використання троянських програм дозволяє підготувати платформу - агентів для проведення розподілених DoS-атак. Зловмисник, керуючи агентами, в певний період часу з

безлічі комп'ютерів-жертв одночасно здійснюється атаки на певний вузол мережі.

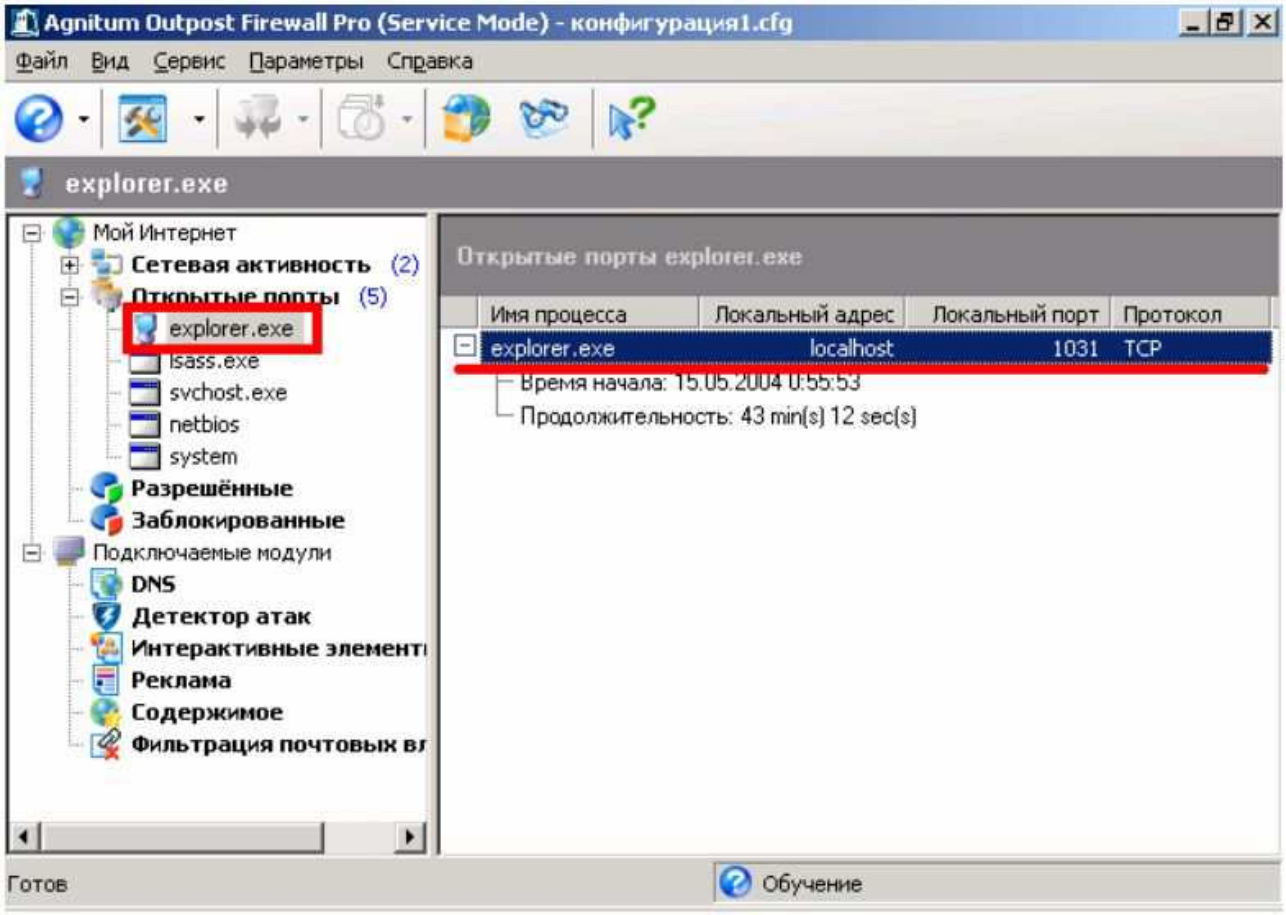

Рис. 3.12. Троянська програма Back Orifice 2000 чекає з'єднання на 1031 порту і маскується в списку процесів під додаток Windows Explorer.

Збиток, що наноситься троянськими програмами, може бути дуже великий - крадіжка паролів, конфіденційної інформації, видалення, блокування або модифікація інформації на скомпрометованих комп'ютерах за допомогою віддаленого управління.

Основними способами проникнення троянських програм в даний час є:

- Запуск вкладень в листах електронної пошти;
- Запуск активного вмісту web-сторінок неблагонадійних web-сайтів;
- Запуск неперевірених антивірусним ПЗ програм з зовнішніх джерел.

3.6 Утиліти для приховування факту компрометації системи (Rootkits)

Існують спеціально розроблені утиліти для приховування факту компрометації системи, шляхом приховування всіх фактів діяльності зловмисника. Такі утиліти є для різних систем і Windows, і Linux, і називаються Rootkits, що можна перекласти як набір адміністративних утиліт.

Зокрема, утиліта AFX Windows Rootkit 2003 з даного класу програм дозволяє конфігурувати спеціальний патч (латочку), встановлення якого в ОС Windows 9x/NT/2000/XP/2003 приховує зазначені процеси, файли, каталоги, ключі реєстру, а також мережеву активність. Таким чином, адміністратор скомпрометованої системи не побачить у списку процесів ніяких підозрілих програм, і ніяких підозрілих мережевих з'єднань, що видаються, наприклад, командою netstat.

Демонстраційне використання даної утиліти для приховування певного процесу представлено на рисунках 3.13 – 3.14.

Рис. 3.13. Генерація патча з використанням AFX Windows Rootkit 2003 для приховування всіх процесів, в назві яких є слово notepad.

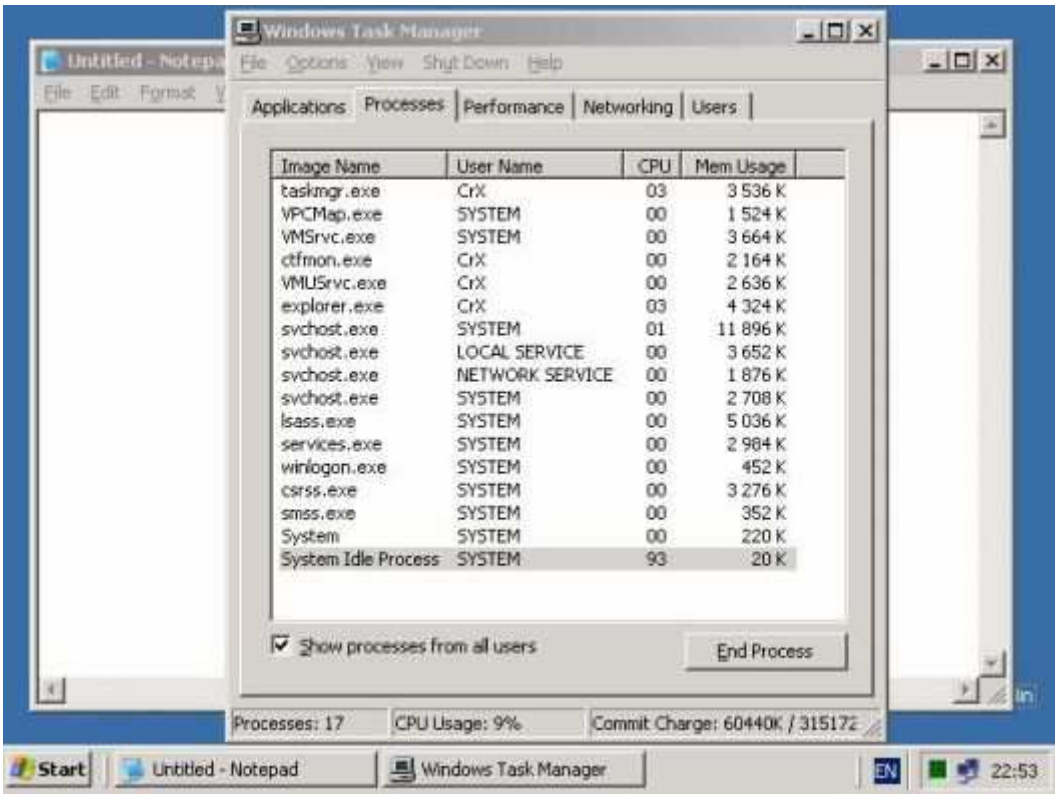

Рис. 3.14. Запущений текстовий редактор Notepad, однак у вікні процесів Task Manager, відповідний процес не відображається.

Віруси і мережеві хробаки

Віруси можуть бути серйозним знаряддям у руках внутрішнього порушника. Застосування вірусів і мережевих хробаків дозволяє досягти наступних цілей:

- Знищення або непоправне зміна текстових документів, виконуваних файлів, баз даних;
- Порушення працездатності всієї корпоративної мережі та окремих елементів: серверів, робочих станцій.

Втрати від вірусної епідемії для компанії можуть бути непоправними. Так, існують спеціалізовані версії вірусів - хробаків, наприклад, хробака MyDoom, що знищує тільки всі офісні документи - форматів Word, Excel, Access і т.д. Враховуючи, що 70-90% інтелектуального капіталу сучасної компанії зберігається в електронному вигляді, серйозна вірусна атака може завдати значної шкоди . Фінансові втрати від простоювання і витрати на відновлення також можуть бути вагомими. (Табл 3.1).

Таблиця 3.1

Фінансові витрати від простоювання

Наслідки	Відсоток (%)
Втрата продуктивності	75
Комп’ютери були недоступні	69
Пошкодження файлів	62
Втрата доступу до файлів	49
Втрата даних	47
Втрата довіри користувачів	33
Закриття доступу	18
Ненадійність прикладного ПЗ	13
Труднощі з читанням файлів	12
Труднощі з зберіганням файлів	9
Падіння системи	9
Труднощі з виводом на друк	7
Небезпека втрати роботи	2

Способи проникнення вірусів у корпоративну мережу аналогічні описаним вище для троянських програм. В останні роки з'явилося нове джерело проникнення мережевих черв'яків - через IM-клієнтів. Тільки в 2002 році з'явилося 5 відомих IM-хробаків, а вже на початку 2004 року по даними Лабораторії Касперського в світі пройшла перша глобальна епідемія нового мережного хробака «Bizex» серед користувачів інтернет-пейджера ICQ. Механізм розповсюдження IM-черв'яків розглянемо на прикладі хробака «Bizex». На комп'ютер жертви доставляється ICQ-повідомлення, де, зокрема, пропонується відвідати якийсь веб-сайт. Для маскування користувачеві показуються мультфільми з популярного серіалу "Joecartoon". Тим часом у систему непомітно проникає Java-вірус, який, використовуючи пролом в ICQ, непомітно розсилає від імені власника комп'ютера посилання на вище вказаний

веб-сайт по всім одержувачам з контактного аркуша. Уникнути зараження можна, негайно видаливши дане повідомлення і не відвідуючи зазначений сайт. Зазначимо, що жоден з видів сучасних ІМ-хробаків поки ще не здатний автоматично виконуватися після отримання. Тому, якщо користувачі ІМ-систем в компанії краще дізнаються про всі наявні загрози та методи їх запобігання, здатність хробаків до розмноження буде істотно знижена.

3.7 Несанкціонована установка додаткових технічних засобів

Загроза несанкціонованого встановлення додаткових технічних засобів полягає в установці порушником спеціалізованих технічних засобів, що полегшують здійснення несанкціонованого доступу до інформації. Наприклад, інсталяція модему на робочому місці користувача та підключення його до телефонного проводу дозволить останньому здійснювати неконтрольований доступ до корпоративної мережі з зовні. Дана загроза дуже небезпечна так, як з'являється «чорний хід» в корпоративну мережу в обхід засобів захисту встановлених для перешкоджання зовнішнім порушників. У той час, як установка модему зовнішнього або внутрішнього все таки операція, яку важко справити приховано, тим більше в процесі передачі інформації необхідно зайняти офісну телефонну лінію, широке поширення мобільних телефонів призводить до нової розстановки пріоритетів загроз. У більшості сучасних мобільних телефонів є вбудований модем, який можна використовувати для підключення до Інтернет. Швидкість з'єднання варіюється від 1 Кб/с до декількох десятків Кб/с (наприклад, для технології GPRS), що дозволяє передавати по ньому досить великі обсяги інформації. Щоб використовувати модем, вбудований в мобільний телефон, останній підключається до комп'ютера або в паралельний порт за допомогою спеціалізованого кабелю, або по інфрачервоного зв'язку. Таким чином, якщо не прийнято спеціальних заходів, будь співробітник може принести сучасний мобільний телефон і підключивши його до своєї робочої станції, потай передати з організації доступні йому матеріали, практично будь-якого обсягу. Можливо також, через

залишений на ніч у режимі модему телефон, здійснити віддалену атаку на корпоративну мережу. Причому в цьому випадку роботу по проникненню може провести вже не внутрішній співробітник, а висококваліфікований зловмисник, так званий «хакер».

3.8 Протидія пасивних методів впливу. Протидія загрозі прослуховування мережевого трафіку

Для прослуховування мережевого трафіку в мережі, побудованої на концентраторах зловмисникові досить запустити на своєму комп'ютері програму-сніффер і аналізувати прохідні пакети. Розглянемо деякі існуючі методи визначення наявності запущеного сніфферу в локальної мережі - це метод пінгу, метод ARP, метод DNS і метод пастки [14].

Метод пінгу (Ping method) використовує виверт, який полягає в відсиланні «ICMP Echo request» (Ping запиту) не на MAC-адресу машини, а на її IP-адресу. Проілюструємо використання даного методу на прикладі.

1. Припустимо, хост, який ми підозрюємо на використання сніфферу, має IP-адресу 10.1.1.1 і MAC-адрес 00-40-05-A4-79-32.

2. Ваш комп'ютер повинен знаходитися в тому ж сегменті ЛОМ, що і підозрюваний комп'ютер.

3. Ви посилаєте «ICMP Echo request», вказавши у запиті IP-адресу підозрюваного хоста і його злегка змінену MAC-адресу, наприклад, 00-40-05-A4-79-33.

4. Кожен хост, отримавши даний запит, порівнює зазначений у запиті MAC-адрес зі своїм MAC-адресом. У разі збігу MAC-адреса, хост відповідає джерелу запита за допомогою «ICMP Echo Reply», інакше пакет ігнорується. У даному випадку, жоден з хостів в ЛОМ не повинен побачити даний пакет.

5. Якщо ж отримана відповідь від будь-якого хоста, це означає що у нього не використовується фільтр MAC-адреси, тобто його мережевий адаптер знаходиться в «Безладному режимі

Метод пінгу може бути перенесений на інші протоколи, які генерують відповіді на запити, наприклад, запит на встановлення TCP-з'єднання або запит за протоколом UDP на порт 7 (exo).

Метод ARP (ARP method) використовує схожу техніку, а також особливості реалізації протоколу ARP в Windows і Linux. Розглянемо дію даного методу на прикладі визначення хоста під управлінням Windows із запущеним сніффером.

1. Ви підозрюєте, що на хості (A) с IP-адресою 192.168.86.19 запущений сніффер. Якщо ви розішлете широкомовний ARP-запит, якому відповідає Ethernet-адрес «FF:FF:FF:FF:FF:FF», з метою з'ясування MAC-адреси хоста (A), всі хости повинні отримати ваш запит, але відповість тільки той, чия IP-адреса вказана в ARP-запиті. У таблиці 3.2 наведені поля пакета розсилаючого ARP-запиту.

Таблиця 3.2

Поля пакета розсилаючого ARP-запиту

Ethernet-адреса хоста-одержувача	FF:FF:FF:FF:FF:FF
Ethernet-адреса хоста-відправника	Власна MAC-адреса
Тип протоколу (ARP=0806)	08 06
Адресний простір (Ethernet = 01)	00 01
…	
Апаратний адреса хоста-відправника	Власна MAC-адреса
IP-адреса хоста-відправника	Власний IP-адрес
Апаратний адреса хоста-одержувача	00 00 00 00 00 00
IP-адреса хоста-одержувача	IP-адреса хоста(A)

А на рисунку 3.15 наведено сам ARP-запит у вікні деталізації аналізатора протоколів Sniffer Pro.

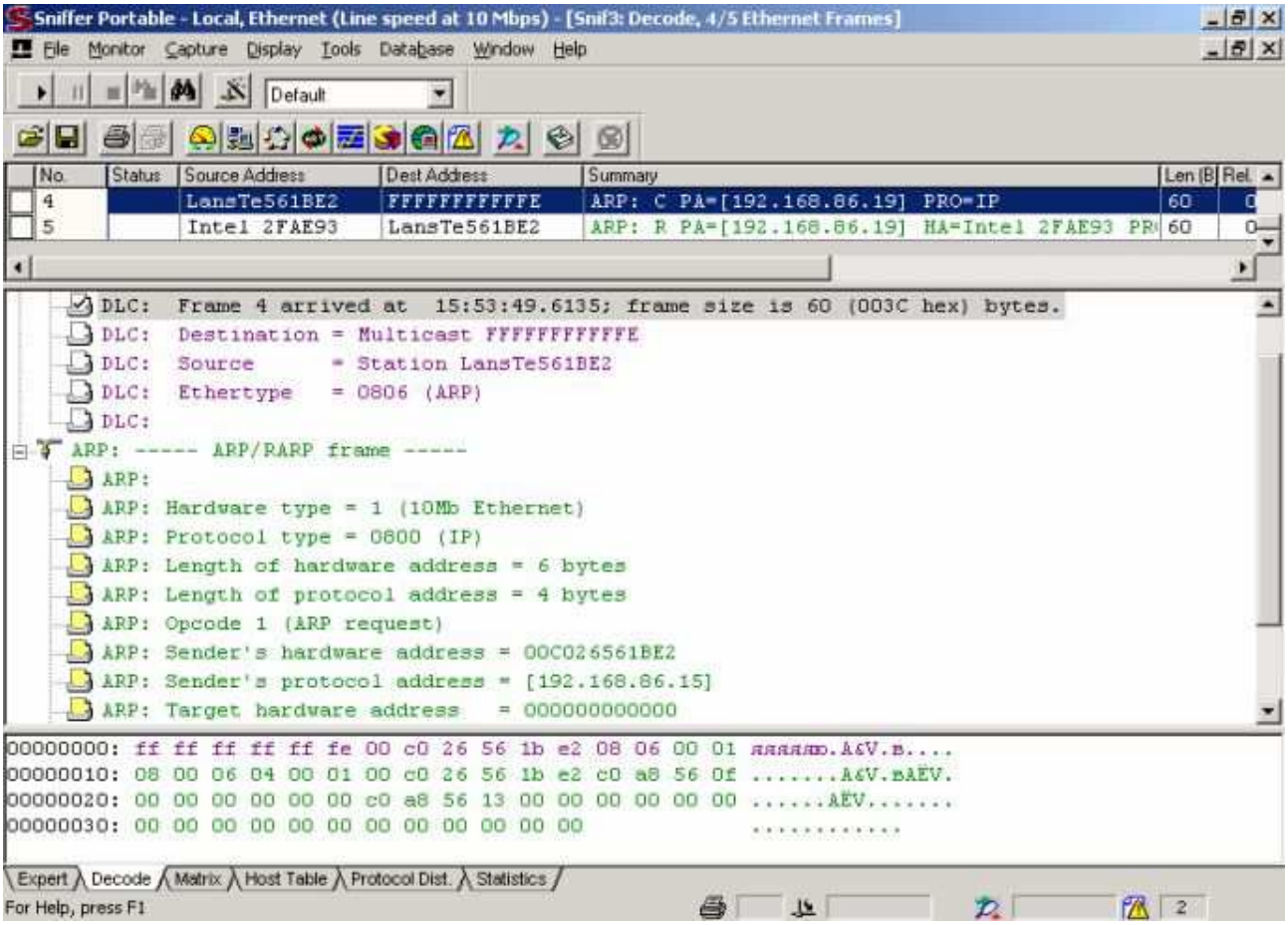

Рис.3.15. Циркулярний ARP-запит у вікні аналізатора протоколів Sniffer Pro для з'ясування MAC-адреси хоста з IP-адресою 192.168.86.19

Однак було виявлено, що якщо на хості запущений сніффер, то в деяких випадках він неправильно обробляє ARP-запити.

2. Використовуючи запропонований метод, ви посилаєте точно такий же ARP-запит, але де замість широкомовної адреси «FF:FF:FF:FF:FF:FF» вказано адресу «FF:FF:FF:FF:FF:FE» (помилковий широкомовний адрес, з якого відняли один біт). Оскільки адреса не є широкомовною, теоретично жоден з хостів не повинен відповісти на такий запит. Однак практичні експерименти, що Windows 2000/XP/2003 за умови, що мережевий адаптер, працює в безладному режимі, вважатиме такий запит широкомовним. Відповідно хост (А), на якому запущений сніффер, порівнявши IP-адреса в запиті зі своїм IP-адресом, пошле відповідь ARP-reply. Таким чином, хост (А) видасть, що він прослуховує весь мережевий трафік. Ситуацію ілюструють рисунки 3.16 і 3.17, зроблені з аналізатора протоколів Sniffer Pro:

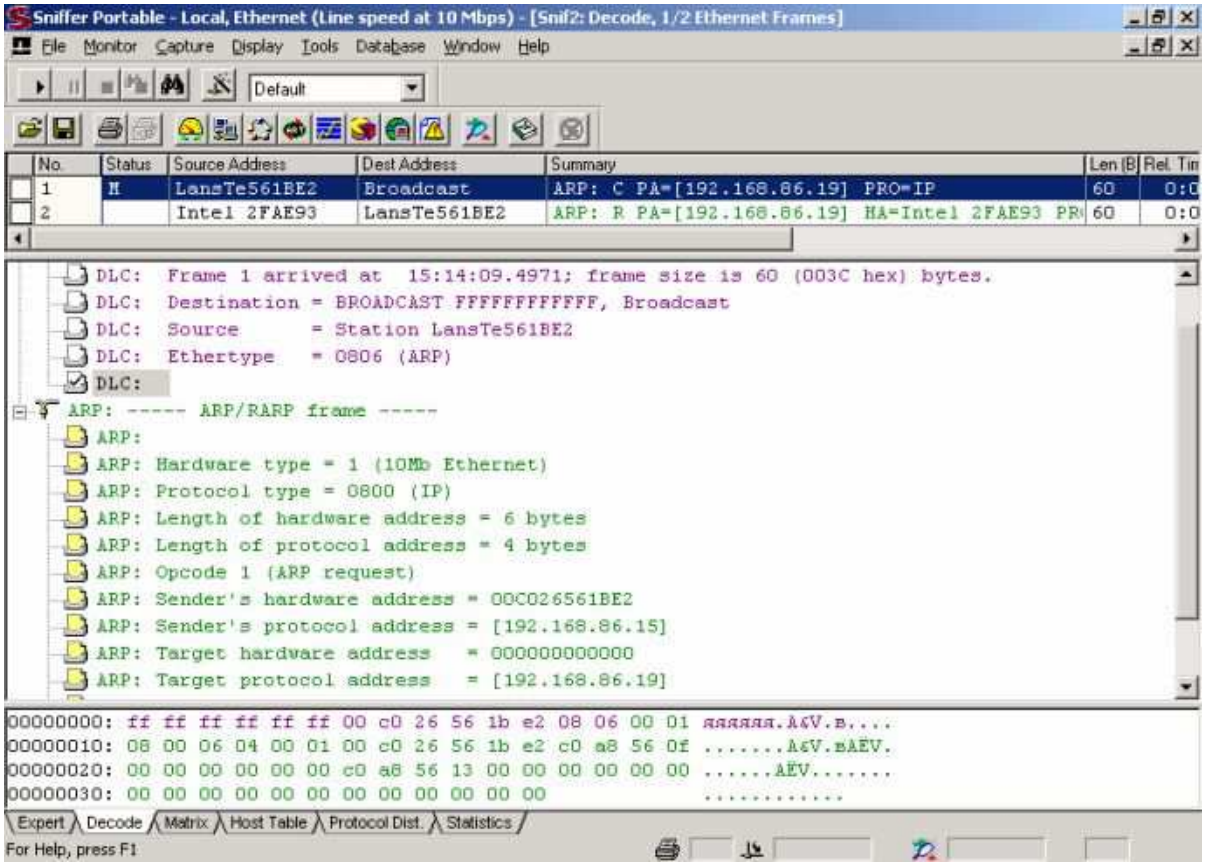

Рис. 3.16. Розсилка ARP-запиту на помилковий широкомовний адрес «FF:FF:FF:FF:FF:FE».

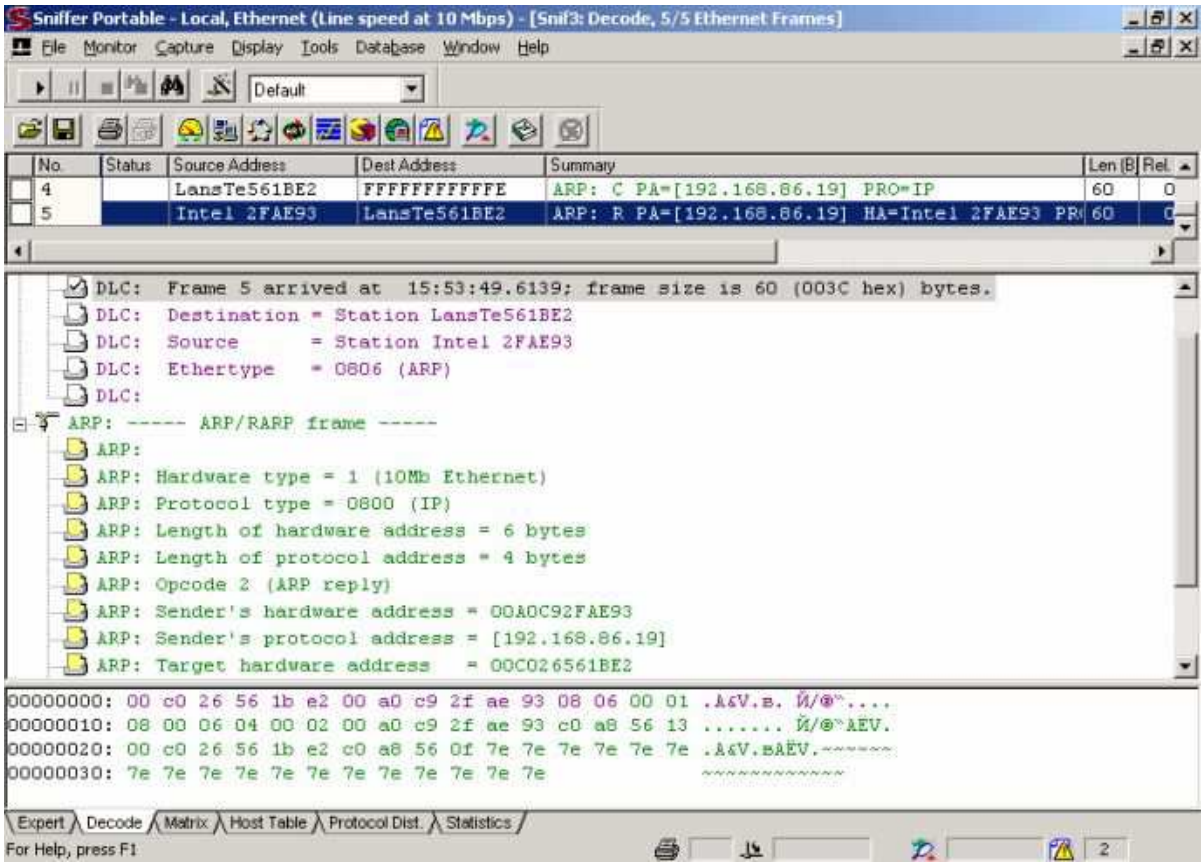

Рис. 3.17. Хост (А) відповідає ARP-відповіддю на помилковий широкомовний ARP-запит, видаючи тим самим, що на ньому запущений сніффер.

Експериментальним шляхом були створені таблиці аномальних відповідей на різні ARP-запити для сучасних ОС – Windows і Linux, в яких запущені сніффери.

Зазначимо тільки, що дані методи в більшості випадків дозволяють лише з деякою вірогідністю визначити наявність сніфферу. В даний час існує безліч безкоштовних і комерційних снифферів, які можна знайти в Інтернет. А програм, віддалено визначають їх наявність, не так багато. Розглянемо найбільш популярні з таких програм L0pth Antisniff, Cain & Abel і PMD:

- L0pht Antisniff реалізує більшість відомих методів виявлення снифферів, проте дана програма написана в 1998 році, фінальна версія так і не вийшла (доступна тільки beta), і в даний виробником не підтримується. Програма функціонує тільки під ОС Windows 9x/NT і не працює під Windows 2000/XP, що накладає серйозні обмеження на її використання.

- Cain & Abel, вже згадувана утиліта, має реалізацію засобів визначення сниферів на основі ARP-методу (рис. 3.18).

- PMD (Promiscuous Mode Detector) з комплекту Anti Sniff Toolbox, розробленого Roberto Larcher. У програмі використовується метод ARP. Експеримент в тестовій корпоративної мережі з запущеними Сніффер - IRIS Network Analyzer, Sniffer Pro, TCP Dump, показав, що в цілому всі три програми успішно визначають сніфферів, однак для правильного налаштування програм необхідно мати теоретичні відомості про роботу методів виявлення снифферів.

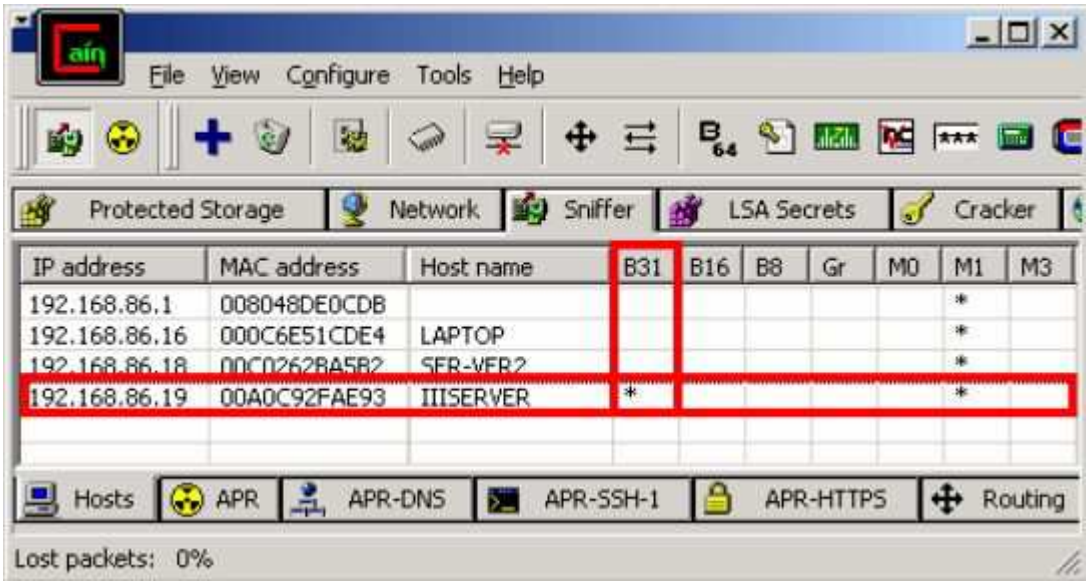

Рис. 3.18. Визначення сніфера на хості з IP-адресою 192.168.86.19 з використанням розсилки помилкового широкомовного ARP-запиту типу B31 («FF:FF:FF:FF:FF:FE»).

Для прослуховування мережевого трафіку в мережі, побудованої на комутаторах зловмисникові необхідно реалізувати одну з атак ARP-spoofing, MAC-duplicating або MAC-flooding. Оскільки всі три атаки мають активний характер, їх теоретично можна виявити.

Реалізацію атаки MAC-flooding виявити порівняно легко - досить запустити на будь-якому хості сніффер і побачити пакети, що не призначені даному хосту. Існують і методи захисту від цієї атаки. Багато сучасних комутаторів підтримують функцію «Port Security», призначення якої в жорсткій фіксації MAC–адреси за портами комутатора. Оскільки MAC-адреси унікальні,

то підключення іншого комп'ютера до порту комутатора не дозволить йому отримати доступ до мережевих ресурсів. Дана міра ефективна проти атак MAC-Flooding і MAC-Duplicating, проте не перешкоджає атаці ARP-Spoofing.

Сучасні міжмережеві екрани і системи виявлення вторгнень в більшості випадків не виявляють атаку ARP-Spoofing. Звичайно, це можна пояснити, тим, що уразливість закладена в сам протокол ARP. Однак методи виявлення атаки ARP-spoofing існують і реалізовані в деяких спеціалізованих програмних засобах. Утиліта ACiD (ARP Change Intrusion Detector) з комплекту Anti Sniff Toolbox, розробленого Roberto Larcher, виконує моніторинг мережевого трафіку з метою виявлення аномалій, властивих атаці «отруєння ARP-кешу» (рис. 3.19).

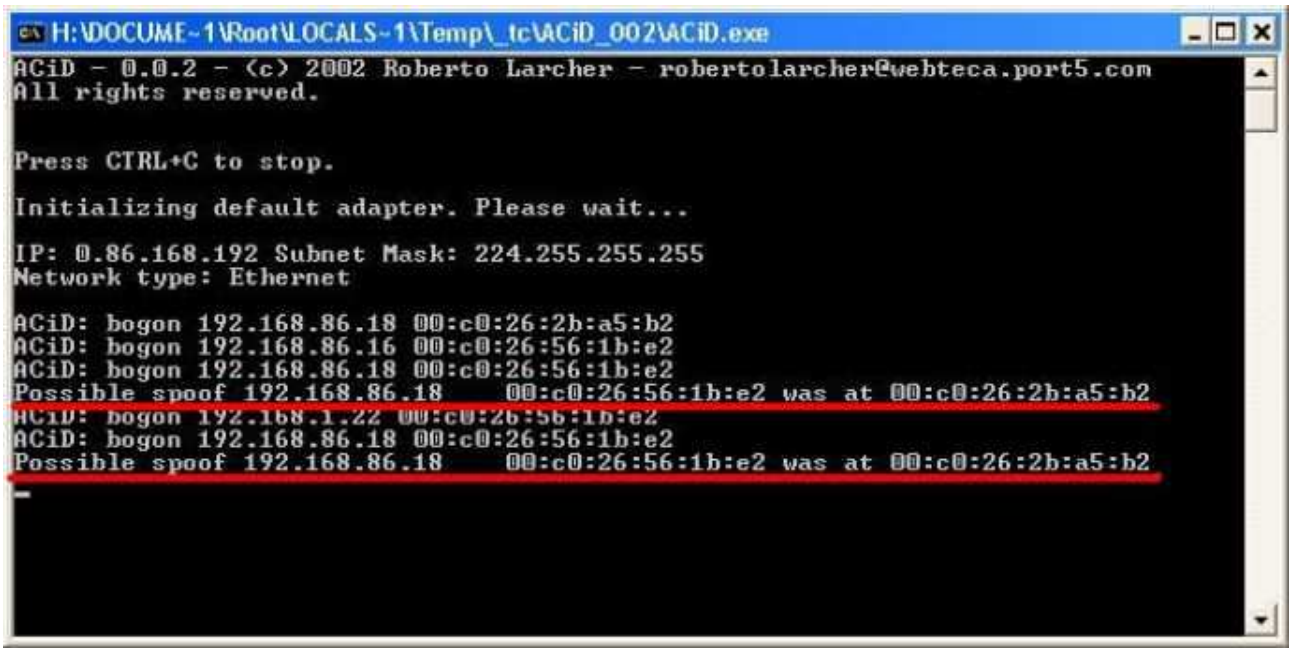

Рис. 3.19. Визначення атаки ARP-Spoofing програмою AciD

Оскільки механізм атаки ARP-Spoofing заснований на уразливості в протоколі ARP, має сенс доопрацювати даний протокол. Для ОС Linux є утиліта Arp_antidote, що змінює реалізацію протоколу ARP в ОС таким чином, щоб зробити дану атаку безглуздою. Механізм оновленого протоколу працює таким чином. При прийомі ARP-reply пакету проводиться порівняння старого і нового MAC-адресу, і при виявленні його зміни запускається процедура верифікації. Посилається ARP-запит, що вимагає всім господарям IP-адреси

повідомити свої MAC-адреси. У разі атаки ARP-Spoofing "справжня" система, що має цей IP-адрес, відповість на запит, і , таким чином, атака буде розпізнано. Якщо ж зміна MAC-адреси було пов'язано не з атакою, а зі стандартними ситуаціями, відповіді, що містить "старий" MAC-адрес, не буде, і по закінченні певного таймаута система оновить запис у кеші. При виявленні підозрілої ситуації ("двійника") ядро виводить повідомлення: "ARP_ANTIDOTE: Possible MITM attempt!" і не оновлює запис ARP-кешу, а навпаки, прописує старий запис як статичний. Про подібний утілітах або оновленнях для Windows невідомо.

Використання статичних ARP-записів не завжди є вирішенням проблеми. Згідно з дослідженням на системах Windows 9x/NT/2000/XP/2003 статичний ARP запис може завжди бути перезаписаний, використовуючи фальшиве ARP повідомлення.

Використання мережевих систем виявлення вторгнень, наприклад ISS RealSecure, дозволяє виявити ARP-атаку шляхом виявлення в мережі двох однакових IP-адрес.

Ну і, нарешті, самим радикальним рішенням є зробити перехоплення мережевого трафіку безглуздим. Для цього необхідно застосувати механізми шифрування. Заміна всіх небезпечних протоколів не завжди можлива. Більш практичним є шифрування всього трафіку на 3-му рівні моделі OSI, використовуючи протокол IPSec. При цьому виявляться захищеними і всі протоколи прикладного рівня - POP3, SMTP, FTP і т.д. підтримка цього протоколу в ОС сімейства Windows реалізована починаючи з версії Windows 2000. Таким чином, клієнти з Windows NT4/9x/ME використовувати даний протокол не можуть.

Якщо застосування протоколу IPSec неможливо з якихось причин, а оскільки як показано вище, розкриття паролів корпоративної електронної пошти може мати серйозні наслідки, необхідно вжити заходів щодо захисту аутентифікаційних даних при доступі до поштових серверів. Існують спеціалізовані протоколи захисту певних протоколів прикладного рівня. Наприклад, протоколи POP3S і SMTPS (POP3, SMTP over SSL) дозволяє

надійно зашифрувати повідомлення електронної пошти. Подібні модифікації є і для протоколів HTTP - HTTPS, FTP -FTPS, IMAP - IMAPS та ін, а їх підтримка реалізована в багатьох сучасних серверах і клієнтах.

У разі застосування захисту даних на мережевому рівні, захищеними також опиняться і аутентифікаційні дані користувачів до безкоштовних електронних поштових скриньок в Інтернет. В іншому випадку, рекомендується обмежити доступ користувачів корпоративної мережі до безкоштовних поштових служб в Інтернет.

Використання адміністратором спеціалізованого сніфферу, наприклад вже згадуваного Cain, дозволить побачити мережу очима потенційного порушника. А зручний інтерфейс програми Cain дозволить відразу ж виявити слабкі місця в корпоративній мережі. Наприклад, працівнику, що скористався безкоштовним поштовим ящиком в Інтернет, можна продемонструвати його пароль, перехоплений за допомогою сніффер, і пояснити, що таке може зробити і внутрішній порушник. Якщо ж пароль до ящика збігається з одним з корпоративних паролів, то це може скомпрометувати всю корпоративну мережу і позначитися на службовому положенні працівника. Така організаційні заходи дозволять знизити ймовірність загроз, пов'язаних з паролями. Слід зазначити, що дії служби безпеки, спрямовані на приховане спостереження, можуть трактуватися як втручання у приватне життя. Однак для уникнення подібній ситуації достатньо повідомити співробітників з письмовим підтвердженням про прослуховування всіх служб комунікації встановлених на робочих місцях.

3.9 Протидія активним методам впливу

Протидіяти активним впливам зловмисників, як внутрішніх, так і зовнішніх, покликані міжмережеві екрани і системи виявлення атак. Оскільки застосування МЕ і СВА в даному розділі розглядається в контексті протидії внутрішнім порушникам, розглянуті персональні МЕ і СВА рівня мережі та хоста.

Виявлення сканування

Саме по собі сканування не є чимось незаконним [26]. Однак, якщо сканування з боку зовнішньої, стосовно корпоративної, мережі як показує практика звичайне явище, то сканування комп'ютерів з внутрішньої мережі - безумовно, інцидент безпеки, що вимагає негайної реакції з боку мережевого адміністратора або адміністратора безпеки.

Виявити сліди сканування можна, вивчаючи журнали реєстрації МЕ. Однак такий підхід не дозволяє своєчасно реагувати на подібні інциденти. Тому сучасні МЕ мають модулі (plug-in) дозволяють виявити атаки і сканування в режимі реального часу, також як це зроблено в СВА. Деякі сканери вразливостей використовують оригінальні методи, що дозволяють виробляти сканування максимально приховано. Наприклад, в одному з кращих мережевих сканерів Nmap існують можливості, дозволяють значно ускладнити виявлення сканування для СВА:

- можливість задавати часові параметри сканування - інтервали між пакетами. Для виявлення такого сканування необхідно проаналізувати пакети за значний проміжок часу;
- можливість задавати групу помилкових хостів, з яких нібито виробляється сканування, для приховування реальної IP-адреси зловмисника. Дана функція особливо небезпечна, тому що в якості помилкових хостів можуть бути вказані хости легальних співробітників, що значно ускладнить виявлення справжнього порушника.

Рішенням проти подібних методів сканування може бути використання мережевих СВА, або періодичне вивчення журналів реєстрації МЕ.

3.9.1 Протидія експлойтам

Як показали експерименти, міжмережеві екрани і системи виявлення вторгнень, встановлені на атакується системі, в ряді випадків не в змозі відобразити дію експлойтів. Для успішного відбиття атак експлойтів засоби захисту необхідно оновлювати, оскільки механізм виявлення вторгнень

заснований на розпізнаванні сигнатур вже відомих атак. Хоча існують розробки, здатні за запевненнями розробників відображати невідомі атаки, практика показує, що вони все ще не ефективні. На рисунку 3.20 проілюстровано як система виявлення атак Black ICE 3.5 без встановлених оновлень сигнатур атак не в змозі відобразити дію експлойта KaHt2.

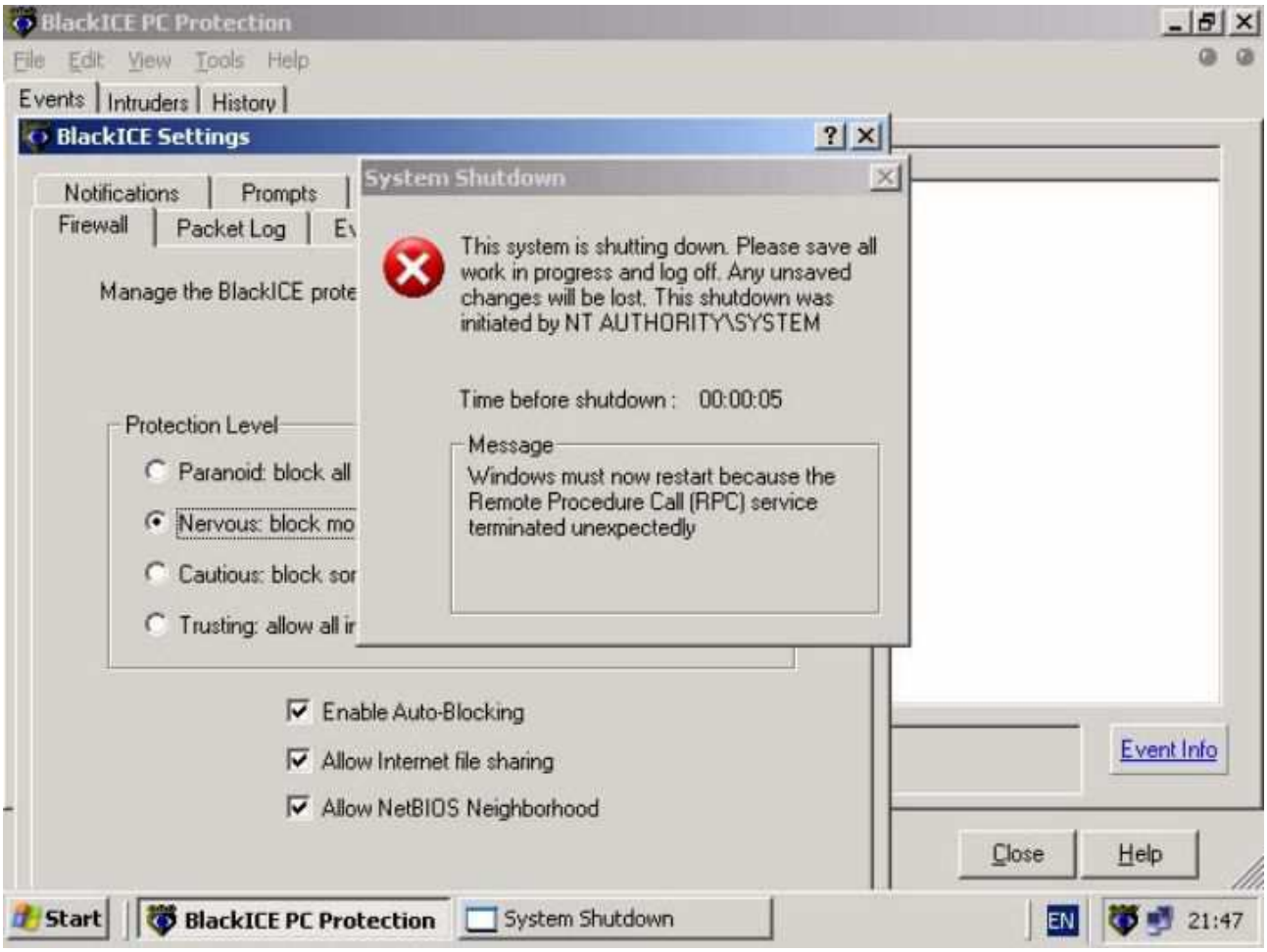

Рис. 3.20. СВА Black ICE пропускає DoS-атаку, викликану експлойтом, що використовує уразливість DCOM RPC Buffer Overflow, що призводить до перезавантаження ОС.

Після оновлення баз даних сигнатур, системи захисту успішно відображають експлойти (рис. 3.21).

Рис. 3.21. ME Agnitum Outpost PRO повідомляє про виявлення і відбитті атаки, викликаної експлойтом, що використовує уразливість MS04-007-dos в бібліотеці Microsoft Windows ASN.1

Якщо виконати оновлення сигнатур ME або СВА неможливо, то тимчасово нейтралізувати атаки можна лише повним блокуванням трафіку на уразливі служби, наприклад RPC, що очевидно не завжди здійсненно без втрат функціональності ОС.

3.9.2 Протидія троянським програмам, мережевим черв'якам і вірусам

Ефективним методом протидії трьом даних видів загроз є використання антивірусних засобів, що працюють в режимі реального часу (моніторів). Для виявлення троянських програм існує спеціалізоване ПЗ (наприклад Tauscan від Agnitum), однак, як показує практика, сучасні антивіруси успішно виявляють і всіляких троянських програм, і експлойти (рис. 3.22).

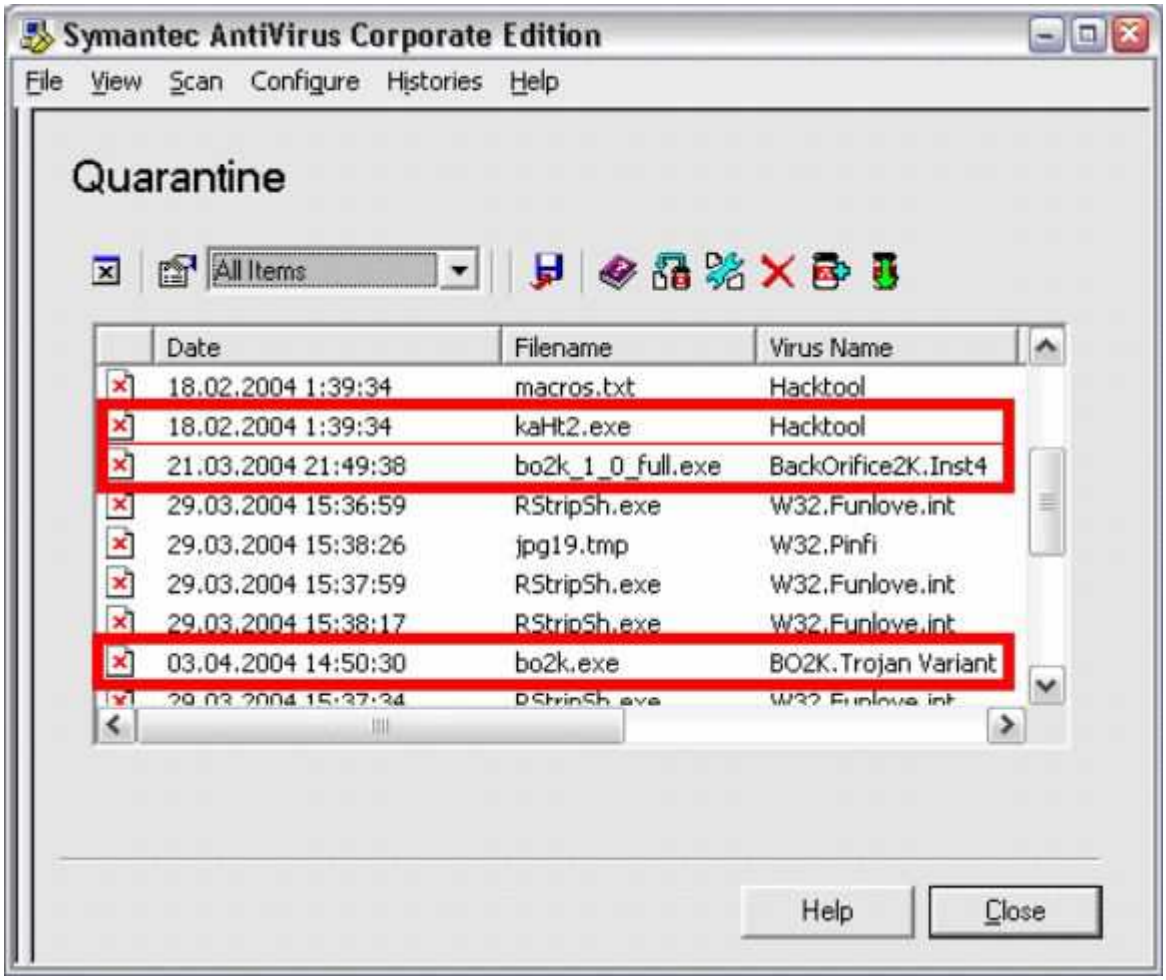

Рис. 3.22. Антивірус Symantec Antivirus Server 8.1 виявив і помістив в карантин експлойт kaHt2 і троянську програму Back Orifice 2000

Додатковою перешкодою для троянських програм є персональний ME. При спробі програми - троянського коня здійснити вихід в мережу, ME відповідно до налаштованими правилами його роботи, або блокує дане звернення, або виведе сповіщення для поточного користувача (рис. 3.23).

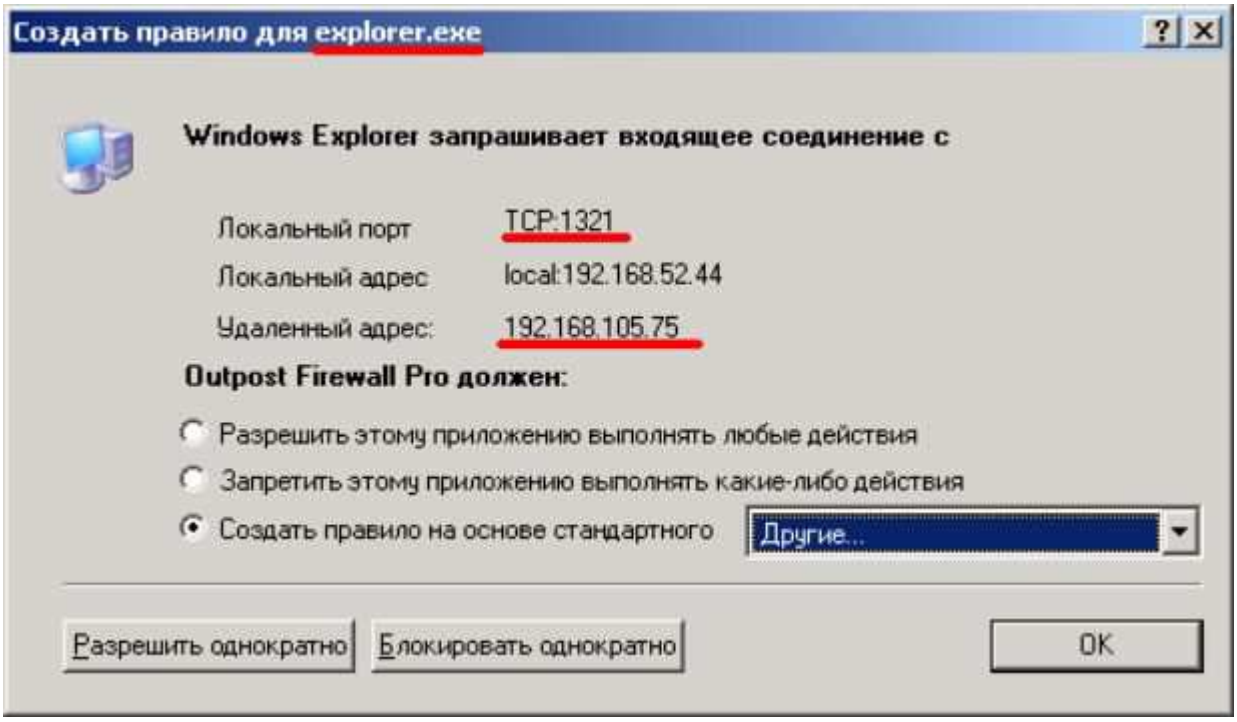

Рис. 3.23. ME Agnitum Outpost попереджає про те, що з додатком explorer.exe (під яке замаскувалася троянська програма Back Orifice) намагається встановити з'єднання з віддаленим хостом 192.168.105.75

На закінчення опису методів захисту від активних впливів, наведемо ряд рекомендацій з того, як визначити, що хтось віддалено підключився до вашої системи, використовуючи троянську програму або експлойти:

1. Троянські програми і експлойти для віддаленого управління системою відкривають певний порт і встановлюють з ним з'єднання. Найчастіше це порт має номер більше 1024, тобто лежить в діапазоні портів, які не закріплених жорстко за певною службою. Переглянути відкриті порти і помітити аномалію в Windows можна командою netstat-an (рис. 3.24).

2. Як було зазначено вище, якщо експлойт спрямований на отримання несанкціонованого доступу до віддаленої системи, то він найчастіше організовує віддалений доступ за допомогою командної оболонки (також відомої як shell або консоль), відкритої на віддаленій системі з правами облікового запису SYSTEM. Оскільки в нормальному режимі функціонування консоль з правами SYSTEM не може бути запущена, то подібну аномалію в разі застосування експлойта помітити легко (рис. 3.25). Слід зазначити, що

примусове завершення процесу CMD.EXE з вікна Windows Task Manager може в ряді випадків привести до вимушеної перезавантаженні Windows (це залежить від того, в якій службі Windows була використана вразливість).

Як наслідок того, що командна оболонка, викликана дією експлойта, запускається з правами облікового запису SYSTEM, відповідної самої ОС, виявити віддалено підключився допомогою експлойта користувача з вікна «Активні користувачі» неможливо (рис. 3.26).

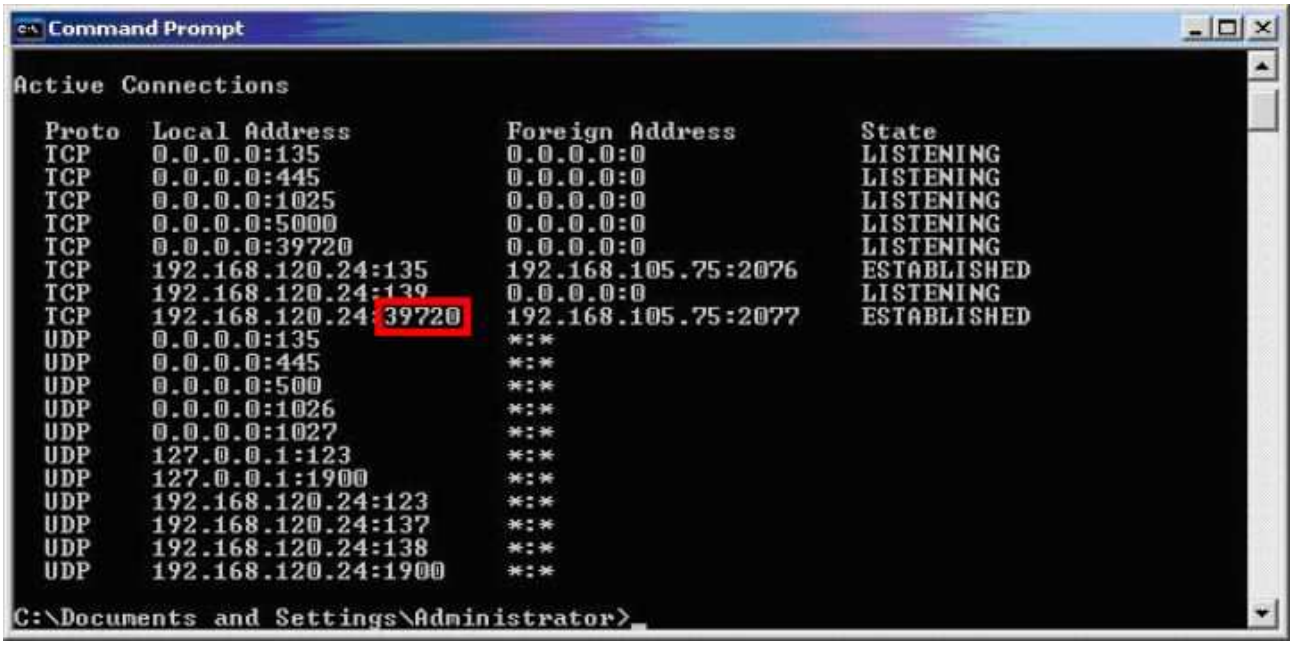

Рис. 3.24. Зловмисник, використовуючи експлойт kaHT2 відкрив на віддаленій системі порт 39720 для віддаленого управління нею і встановив з цим портом з'єднання (стан established).

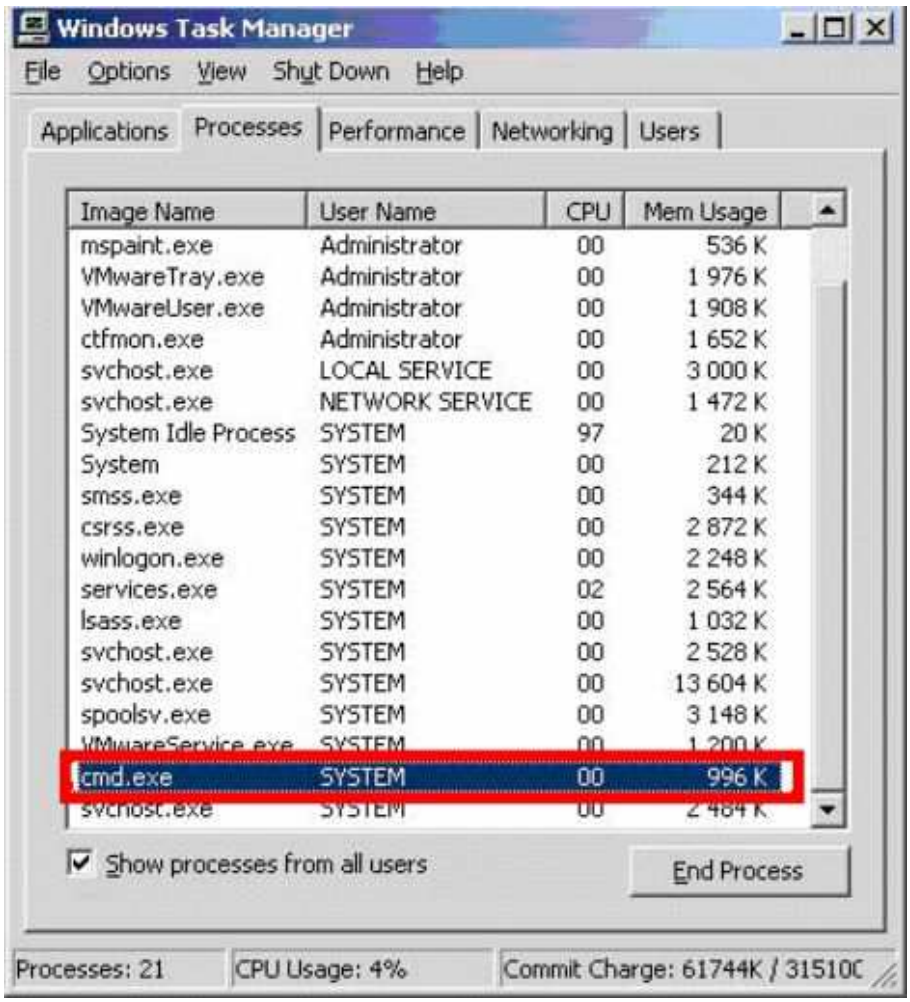

Рис. 3.25. На системі, до якої був застосований експлойт, в списку запущених процесів присутня консоль, запущена від імені облікового запису SYSTEM, що в MS Windows є аномальним.

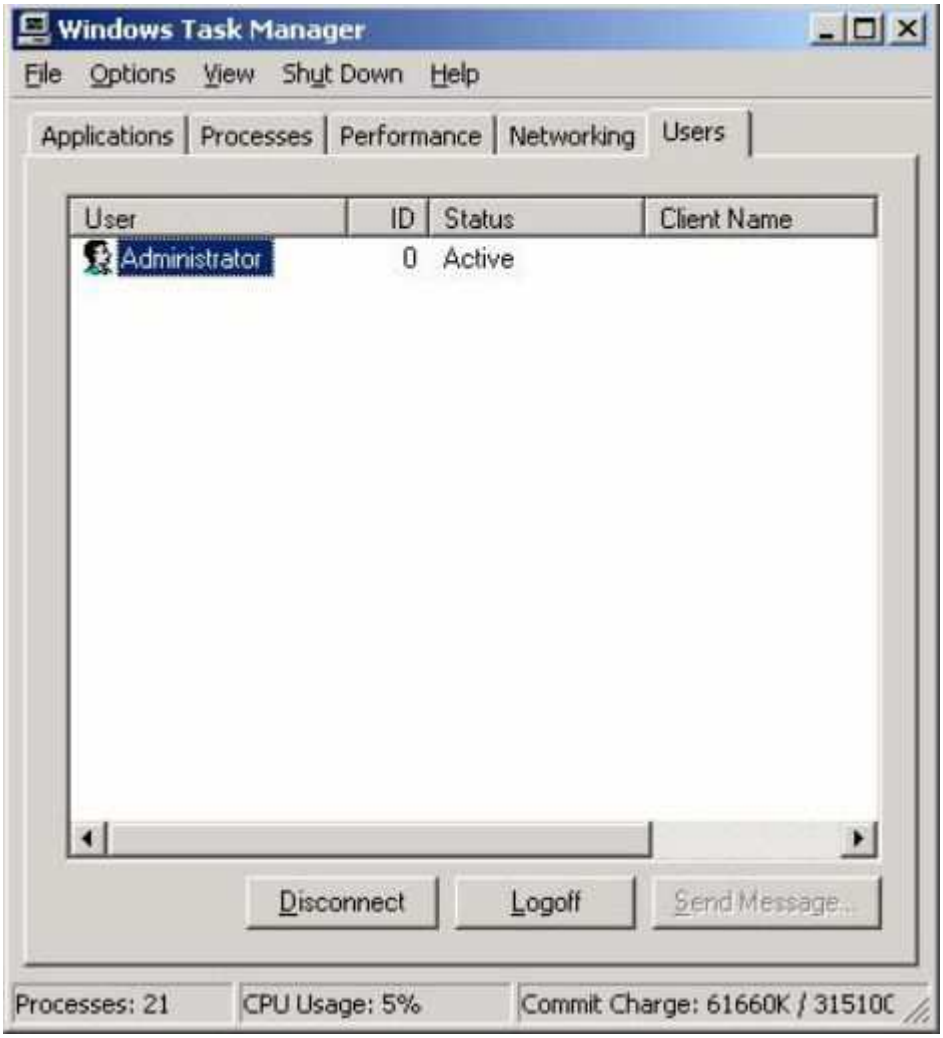

Рис. 3.26. Незважаючи на те, що до системи підключився віддалений користувач, у вкладці «Users» відображається лише адміністратор скомпрометованої системи.

3.9.3 Виявлення утиліт для приховування факту компрометації системи

Як показано вище, подібні утиліти не дозволяють стандартними засобами ОС визначити їх наявність. Для їх виявлення розроблені спеціальні програми, наприклад, Rootkit Hunter (Linux/Unix) або Patchfinder (Windows) (рис. 3.27).

Також додатковою перешкодою є антивірусні програми. Антивірусні монітори часто визначають відомі (тобто занесені до бази) програми для генерації таких патчів, як троянські. Наприклад, антивірус Касперського визначає розглянутий AFX Windows Rootkit 2003, як троянську програму Troyan.Win32.Madtol.a і пропонує видалити цей об'єкт (Рис. 3.28). Однак якщо

патч вже був встановлений, то антивірусна програма виявляє його в пам'яті, але спроба видалення/лікування призводить до нескінченного перезавантаження системи, так як патч дуже глибоко інтегрується в ОС.

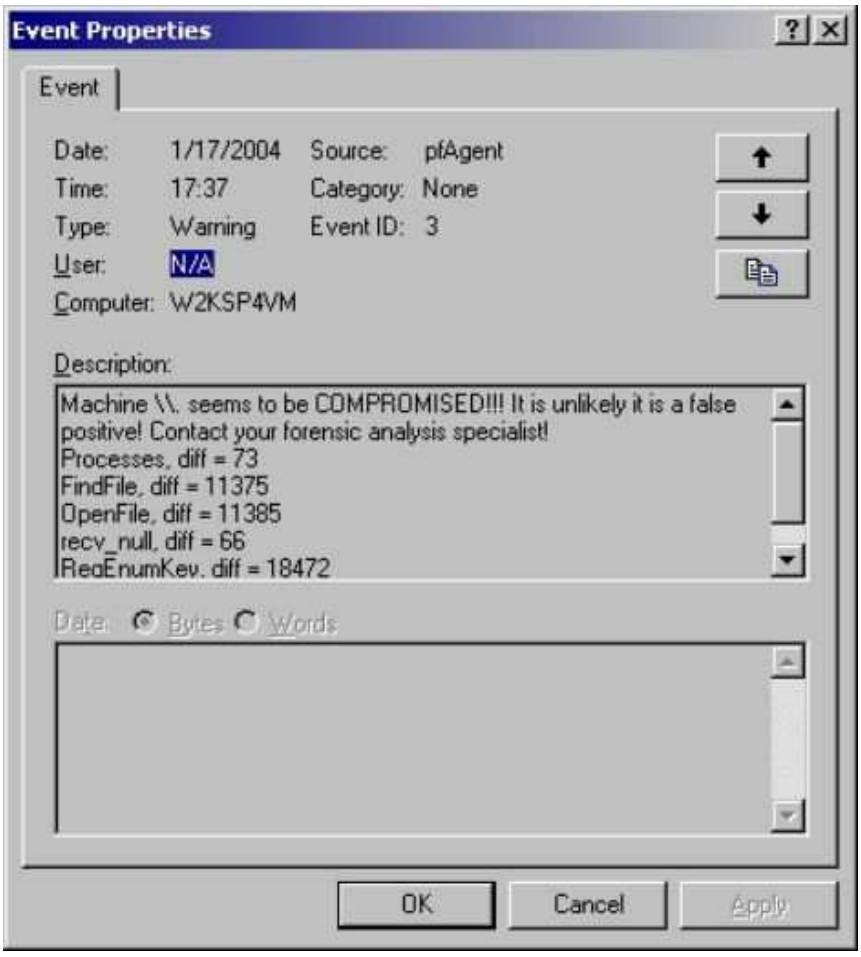

Рис.3.27. Програма Patchfinder виявила популярний rootkit

HackerDefender для Windows, запущений на локальній системі.

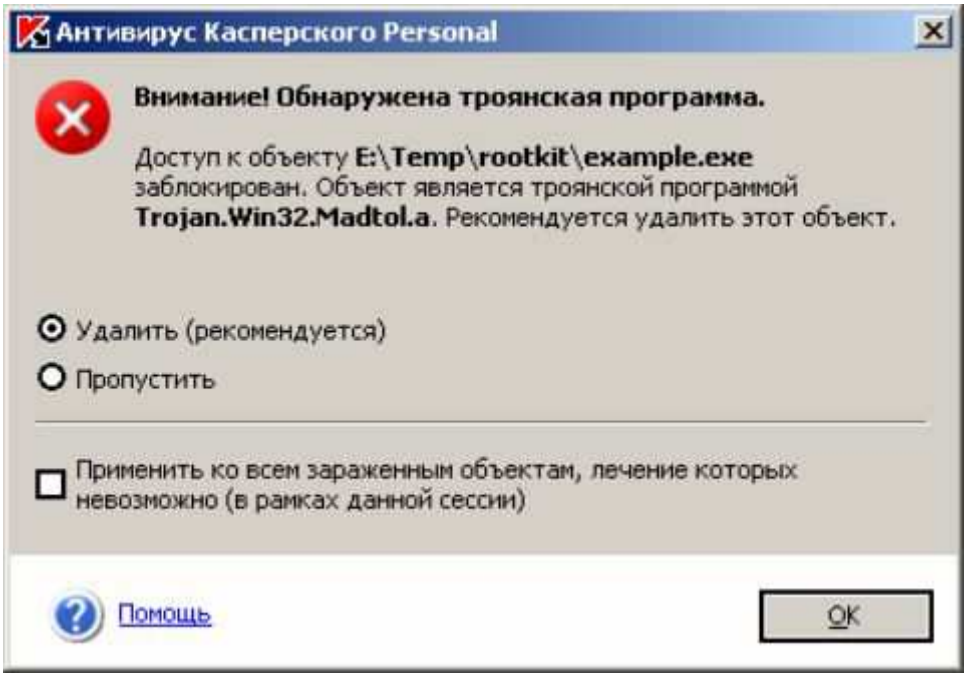

Рис. 3.28. Антивірус Касперського виявив AFX Windows Rootkit 2003

3.9.4 Протидія несанкціонованої установці модемів

Для запобігання установки користувачами будь-якого технічного обладнання необхідно передбачити заходи трьох рівнів - організаційного, фізичного і програмно-паратного. На організаційному рівні необхідно в політиці безпеки заборонити співробітникам подібні дії, встановивши заходи відповідальності. На фізичному рівні заходи захисту повинні включати опечатування всіх вільних роз'ємів, портів комп'ютера. Апаратні заходи передбачають відключення всіх невикористовуваних модулів, роз'ємів. Можлива установка спеціалізованих засобів захисту, що сигналізують про спробу розкриття корпуса комп'ютера. Програмні заходи включають використання коштів функціонують на трьох рівнях - рівні базової системи введення-виводу (BIOS), рівні ОС, рівні спеціалізованих СЗІ. Оскільки стійкість засобів захисту рівня BIOS і ОС залишається низькою - існують засоби подолання такого захисту, рекомендується використання спеціалізованих і особливо сертифікованих СЗІ, таких як Secret Net, Spectr-M. Розглянемо механізми захисту від загроз зміни апаратної конфігурації, реалізовані в СЗІ Secret Net 2000. Функція системи «Контроль апаратної

конфігурації комп'ютера» призначена для своєчасного виявлення змін конфігурації і вибору найбільш доцільного способу реагування на ці зміни.

Зміни апаратної конфігурації комп'ютера можуть бути викликані: виходом з ладу, чи заміною окремих пристроїв або всього комп'ютера. Для ефективного контролю конфігурації використовується широкий набір контрольованих параметрів, з кожним з яких пов'язані правила виявлення змін і дії, що виконуються у відповідь на ці зміни. Відомості про апаратної конфігурації комп'ютера зберігаються в БД системи захисту. Початкові (еталонні) дані про конфігурацію надходять від програми установки. Кожного разу при завантаженні комп'ютера, а також при повторному вході користувача система отримує відомості про актуальну апаратну конфігурацію і порівнює її з еталонною. При виявленні невідповідності аналізується серйозність виникаючої помилки і її подальше вплив на безпеку інформації. Контроль конфігурації програмних і апаратних засобів проводиться ядром системи Secret Net. За результатами контролю ядро приймає рішення про необхідності блокування комп'ютера. Рішення приймається після входу користувача і залежить від налаштувань користувача. Значення налаштувань користувача визначає адміністратор безпеки. Якщо було виконано запланована зміна конфігурації комп'ютера, то користувач, що володіє адміністративними привілеями, може за допомогою підсистеми управління оновити еталонні відомості про конфігурації.

3.10 Дослідження систем централізованого моніторингу безпеки

Одним з методів автоматизації процесів аналізу і контролю захищеності розподілених комп'ютерних систем є використання технології інтелектуальних програмних агентів. Система захисту будується на архітектурі консоль-менеджер-агент. На кожну з контрольованих систем встановлюється програмний агент, який і виконує відповідні налаштування ПЗ і перевіряє їх правильність, контролює цілісність файлів, своєчасність установки пакетів програмних корекцій, а також виконує інші корисні завдання з контролю

захищеності АС. (Управління агентами здійснюється по мережі програмою менеджером.) Менеджери є центральними компонентами подібних систем. Вони посилають керуючі команди всім агентам контрольованого ними домену та зберігають всі дані, отримані від агентів в центральній базі даних. Адміністратор управляє менеджерами за допомогою графічної консолі, що дозволяє вибирати, налаштовувати і створювати політики безпеки, аналізувати зміни стану системи, здійснювати ранжування вразливостей і т. п. Всі взаємодії між агентами, менеджерами і керуючою консоллю здійснюються за захищеного клієнт-серверного протоколу. Такий підхід був використаний при побудові комплексної системи управління безпекою організації Symantec Enterprise Security Manager, Tivoli IT Director.

Застосування таких систем дозволяє значно підвищити рівень захищеності в мережі, однак висока вартість даних програмних продуктів є стримуючим фактором для їх більш широкого розповсюдження.

Цікавим підходом до виявлення внутрішніх порушників є використання «віртуальних пасток». «Віртуальні пастки» - honeypots (горщик меду), з'явилися порівняно недавно. Основна мета таких пасток - стати приманкою для зловмисника, прийняти атаку, сканування і бути зламаною їм.

Популярні віртуальні пастки KFSensor і NFR Back Officer Friendly (BOF) здатні емулювати роботу різних сервісів (рис. 3.29). Наприклад, можлива емуляція FTP-сервера, POP3-сервера, SMTP-сервера, TELNET-сервера, HTTP-сервера, SQL-сервера і багатьох інших, у тому числі серверної частини троянської програми BackOrifice. При будь-якій спробі доступу до даної службі видається оповіщення для адміністратора і протоколювання всієї активності. Мається можливість сповіщення адміністратора через електронну пошту. KFSensor також пропонує різну ступінь емуляції служб – від простої до максимально правдоподібної.

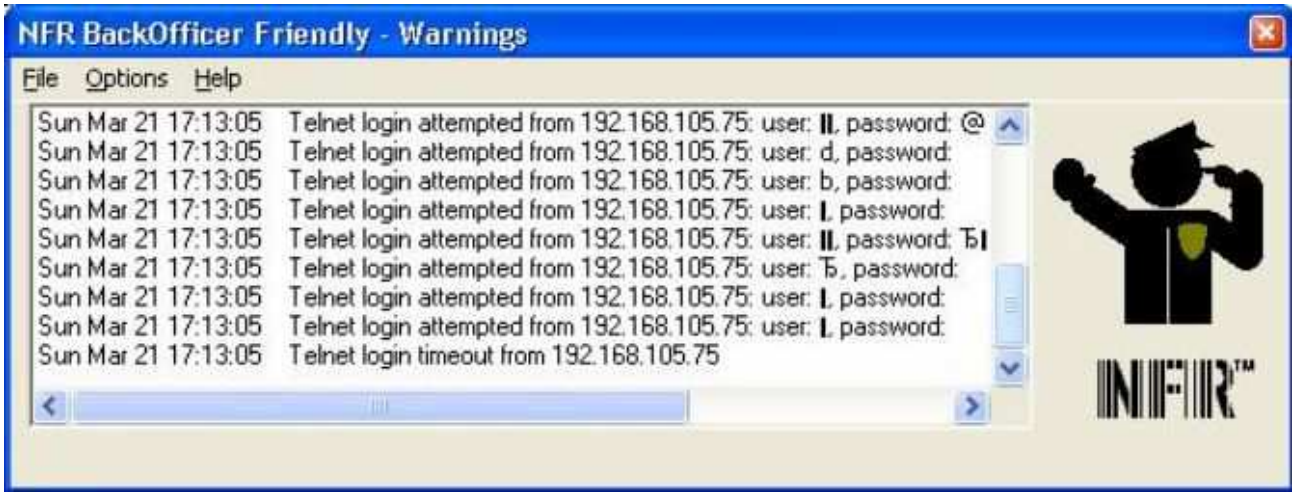

Рис. 3.29 NFR BackOfficer Friendly, емулює роботу TELNET-сервера, оповіщає про процес підбору зловмисником (IP-адресу 192.168.105.75) паролів до помилкового сервера

В цьому розділі було досліджено вплив внутрішніх зловмисників на корпоративну мережу та методи протидії їм. Досліджено пасивні та активні методи впливу, протидію експлойтам та систему централізованого моніторингу безпеки.

РОЗДІЛ 4
ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНА ЧАСТИНА

Метою дипломного проекту є визначення сучасних інформаційних загроз захищених корпоративних мереж, а також визначення методів протидії їм. Головною метою розділу є встановлення економічної доцільності проведення даної розробки.

4.1 Розрахунок норм часу на виконання науково-дослідної роботи

Ефективне використання часу має велике значення тому, що коефіцієнт корисної дії залежить від оптимального використання часу.

Розробку поділяють на декілька етапів, що дозволить полегшити і структуризувати виконання роботи.

Основні етапи при виконанні дослідження наступні:

1. Підготовка опису задачі.
2. Збір необхідної інформації по послідженню.
3. Вибір програмного забезпечення для проведення дослідження.
4. Розробка структури дослідження.
5. Розробка основних та додаткових розділів дослідження.
6. Перевірка результатів дослідження.

Для оцінки тривалості виконання окремих робіт використовують нормативи часу або попередній досвід.

Виконавцем усіх операцій по дослідженню являється інженер.

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 4.1.

Таблиця 4.1

Операції технологічного процесу та час їх виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Підготовка опису задачі.	Інженер	7
2.	Збір необхідної інформації по послідженню	Інженер	22
3.	Вибір програмного забезпечення для проведення дослідження	Інженер	5
4.	Розробка структури дослідження.	Інженер	14
5.	Розробка основних та додаткових розділів дослідження.	Інженер	50
6.	перевірка результатів дослідження.	Інженер	17
Разом			**115**

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично

відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Рекомендовані тарифні ставки: керівник проекту – 4,5...8,0 грн./год., інженер – 3,0...5,0 грн./год., консультант – 3,5...5,5 грн./год., технік – 3,0...4,5 грн./год., лаборант – 2,0...3,5 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г \,, \qquad (4.1)$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в даному випадку виконує інженер, то основна заробітна плата буде розраховуватись тільки за однією формулою

$$З_{осн.} = 5 \cdot 115 = 575 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \qquad (4.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод} = 575 \cdot 0{,}15 = 86{,}25 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.} \quad (4.3)$$

$$В_{о.п.} = 575 + 86,25 = 661,25 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи:

1. фонд страхування на випадок безробіття – 1,3 %;
2. фонд по тимчасовій втраті працездатності – 2,9 %;
3. пенсійний фонд – 32,3 %.

У сумі зазначені відрахування становлять 37,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = Ф_{оп} \cdot 0,375 , \quad (4.4)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$$В_{с.з.} = 661,25 \cdot 0,375 = 236,07 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2

Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівни–ків	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на плату праці, грн. 6=3+4+5
		Тарифна ставка, грн.	К–сть відпра–цьов. год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1.	інженер	5	115	575	86,25	236,07	897,32

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених

матеріалів та їх ціни:

$$M_{ві} = q_i \cdot p_i \,, \tag{4.5}$$

Де: q_i – кількість витраченого матеріалу і–го виду;

p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{ві} \,. \tag{4.6}$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3

Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Один. виміру	Норма витрат	Ціна за один., грн.	Затрати матер., грн.	Транс-портно-заготівель-ні витрати, грн.	Загальна сума витрат на матер., грн.
1	2	3	4	5	6	7
1. Допоміжні витрати						
Використання мережі Internet	години	–	100	100	–	100
Разом:						**100**

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

$$З_в = W \cdot T \cdot S \,, \tag{4.7}$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів (0,203 грн. + 20% ПДВ за 1 кВт). Отже, 1 кВт з ПДВ коштує 0,2436 грн.

Потужність комп'ютера для створення проекту – 550 Вт, кількість годин роботи обладнання згідно таблиці 3.1 –115 годин.

Тоді,

$$З_в = 0{,}55 \cdot 115 \cdot 0{,}2436 = 15{,}41 \text{ грн.}$$

4.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \qquad (4.8)$$

де A – амортизаційні відрахування за звітний період, грн.;

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Для даного проекту засобом розробки є комп'ютер. Його сума становить 7900 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 7900 \cdot 5\% / 100\% = 395 \text{ грн.}$$

Оскільки робота виконувалась 115 години, то амортизаційні

відрахування будуть становити:

$$A = 395 \cdot 115 / 115 = 395 \text{ грн.}$$

4.6 Обчислення накладних витрат

Накладні витрати пов’язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб’єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2\ldots0{,}6\ , \qquad (4.9)$$

де $H_в$ – накладні витрати.

Отже, накладні витрати:

$$H_в = 661{,}25 \cdot 0{,}2 = 132{,}25 \text{ грн.}$$

4.7 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4.

Таблиця 4.4

Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
1	2	
Витрати на оплату праці (основну і додаткову заробітну плату)	575	39,6
Відрахування на соціальні заходи	236,07	16,2
Матеріальні витрати	100	6,8
Витрати на електроенергію	15,41	1,1
Амортизаційні відрахування	395	27,2

Продовження таблиці 4.4

Накладні витрати	132,25	9,1
Собівартість	1453,73	100

Собівартість ($С_в$) програмного продукту розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.з.} + З_{м.в.} + З_в + А + Н_в \, . \qquad (4.10)$$

Отже, собівартість програмного продукту дорівнює:

$С_в$ = 575 + 236,07 + 100 + 15,41 + 395 + 32,25 = 1453,73 грн.

4.8 Розрахунок ціни програмного продукту

Ціну НДР можна визначити за формулою:

$$Ц = \frac{С_В \cdot (1 + Р_{рен}) + К \cdot В_{н.і.}}{К} \cdot (1 + ПДВ) \, , \qquad (4.11)$$

де $Р_{рен.}$ – рівень рентабельності, 30 %;

$К$ – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем);

$В_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту);

ПДВ – ставка податку на додану вартість, (20 %).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти К та Ві.н , оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = С_В \cdot (1 + Р_{рен}) \cdot (1 + ПДВ) \, . \qquad (4.12)$$

Звідси ціна на проект складе:

$$Ц = 1453{,}73 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 2267{,}82 \text{ грн.}$$

4.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність ($E_р$) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_р = \frac{П}{C_В}, \tag{4.13}$$

де $П$ – прибуток;

$C_В$ – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_в . \tag{4.14}$$

Розраховуємо плановий прибуток:

$$П_{пл} = 2267{,}82 - 1453{,}73 = 814{,}09 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П_{пл}}{C_в}. \tag{4.15}$$

Тоді,

$$E_р = 814{,}09 / 1453{,}73 = 0{,}56 .$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень ($T_р$):

$$T_p = \frac{1}{E_p}\ , \qquad (4.16)$$

Термін окупності дорівнює:

$$T_p = 1 / 0{,}56 = 1{,}8 \text{ роки}$$

Висновок:

В організаційно-економічній частині дипломного проекту було розраховано основні техніко-економічні показники дослідження (таблиця 4.5).

Розраховане значення економічної ефективності, яке становить 0,56, що є високим значенням.

Так само нормальним є термін окупності, який повинен коливатися від 1 до 3 років, тоді розробка вважається доцільною і економічно вигідною. Для даного продукту він становить 1,8 років.

Таблиця 4.5

Техніко–економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	1453,73
2.	Плановий прибуток, грн..	814,09
3.	Ціна, грн.	2267,82
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Отже, даний проект може бути впроваджений та мати подальший розвиток, оскільки він є економічно вигідним за всіма основними техніко-економічними показниками.

5 РОЗДІЛ
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Охорона праці

Темою моєї дипломної роботи є дослідження методів і засобів захисту інформації в корпоративних мережах. В моєму дослідженні охорона праці грає велику роль, адже необхідно створити безпечне і нешкідливе робоче місце. Робоче місце для аналізу умов праці було обрано науково-дослідну лабораторію "Інформаційних технологій та інтелектуальних систем", яка знаходиться за адресою м.Тернопіль, вул.Руська, 56.

Основними вимогами охорони праці та техніки безпеки при використанні комп’ютерної техніки є: параметри освітлення, оптимальні умови мікроклімату, ергономічні характеристики основних елементів робочого місця, рівні шуму, вібрації, електромагнітні, ультрафіолетові та інфрачервоні випромінювання та електростатичні поля. Зокрема:

- площа на одне робоче місце становить не менше ніж 6,0 кв. м, а об'єм не менше ніж 20,0 куб. м;
- приміщення має природне та штучне освітлення відповідно до СНиП II-4-79 та ДСанПіН 3.3.2-007-98;
- природне освітлення здійснюється через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечує коефіцієнт природної освітленості (КПО) не нижче ніж 1,5%;
- віконні прорізи лабораторії обладнані регульованими жалюзями;
- лабораторія не межує з приміщеннями, в яких рівні шуму і вібрації перевищують допустимі значення за СН 3223-85, СН 3044-84, ГР 2411-81, ГОСТ 12.1.003-83;
- лабораторія обладнана системами опалення, кондиціонування повітря відповідно до СНиП 2.04.05-91. Нормовані параметри мікроклімату, іонного складу повітря, вмісту шкідливих речовин відповідають вимогам СН 4088-86, СН 2152-80, ГОСТ 12.1.005-88, ГОСТ 12.1.007-76;

- для внутрішнього оздоблення лабораторії використано дифузно-відбивні матеріали з коефіцієнтами відбиття для стелі 0,7 - 0,8, для стін 0,5 - 0,6;
- покриття підлоги є матовим з коефіцієнтом відбиття 0,3 - 0,5. Поверхня підлоги є рівною, неслизькою, з антистатичними властивостями;
- в лабораторії не використано полімерних матеріалів для оздоблення приміщення;
- ЕОМ з ВДТ і ПП, електропроводи та кабелі за виконанням і ступенем захисту відповідають класу зони за НПАОП 40.1-1.01-97, мають апаратуру захисту від струму короткого замикання та інших аварійних режимів;
- оскільки в приміщенні одночасно експлуатуються понад п'ять ЕОМ з ВДТ і ПП, на помітному та доступному місці встановлений аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення;
- ЕОМ з ВДТ і ПП підключаються до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення;
- електромережі штепсельних з'єднань та електророзеток для живлення ЕОМ з ВДТ і ПП виконані за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі;
- в лабораторії щоденно проводиться вологе прибирання.

Ці вимоги поширюються також на умови й організацію праці при роботі з візуальними дисплейними терміналами (ВДТ) усіх типів вітчизняного та зарубіжного виробництва на основі електронно-променевих трубок (ЕПТ), що використовуються в електронно-обчислювальних машинах (ЕОМ) колективного використання та персональних ЕОМ (ПЕОМ).

Відповідальність за виконання цих вимог покладається на інженера лабораторії.

Порушення санітарно-гігієнічних і санітарно-протиепідемічних правил і норм тягне дисциплінарну, адміністративну, кримінальну відповідальність

відповідно до Закону України "Про забезпечення санітарного та епідемічного благополуччя населення" (ст. 45, 46, 49).

В даному розділі було висвітлено роль охорони праці для науково-дослідницької лабораторії та було доведено необхідність розробки заходів з охорони праці у дипломній роботі. Було досліджено і висвітлено питання вимог безпеки до лабораторних приміщень та обладнань для наукових досліджень. Також було проаналізовано законодавчу та нормативну базу з охорони праці, яка використовувалась при написанні даного розділу.

5.2 Безпека в надзвичайних ситуаціях

Темою моєї дипломної роботи є дослідження методів і засобів захисту інформації в корпоративних мережах. Безпека в надзвичайних ситуаціях є актуальною оскільки багато корпорацій працює з небезпечними матеріалами, речовинами тощо, що можут спричинити надзвичайну ситуацію.

В цьому розділі розглянуто питання впливу СДОР на працездатність населення а саме особливості і захист населення при аварії на хіміко небезпечних об’єктах.

При аварії відбувається викид або вилив сильнодіючої отруйної речовини (СДОР) в навколишнє середовище – це хімічні сполуки, які застосовуються в народному господарстві але при аварії і потраплянні їх в атмосферу у великих концентраціях можуть призводити до зараження повітря і стати причиною ураження населення.

В Україні біля 12 млн. людей мешкають в зонах можливого хімічного зараження від потенційно небезпечних об’єктів. На території нашої держави функціонує 1711 об’єктів промисловості на яких зберігається або використовується в виробничої діяльності більше 805 тисяч тон СДОР, у тому числі більше 6 тис. тон хлору, 176 тис. тон аміаку та більше 623 тис. тон інших небезпечних хімічних речовин.

Головним вражаючим чинником під час аварій на ХНО є зараження повітря у вигляді пару або аерозолі, що призводить до ураження людей, які знаходяться в зоні дії СДОР.

За розрахунками спеціалістів під час потрапляння людей в зону зараження на відкритій місцевості без протигазів, практично майже 100% населення можуть отримати ураження. У разі повного забезпечення населення засобами індивідуального захисту втрати будуть, але вони не перевищують10-12%. В останньому випадку втрати можливі через несвоєчасне використання засобів захисту або їх зіпсованість. Розглянемо небезпеку дії деяких СДОР на людину.

Хлор,(Cl_2) речовина з переважно задушливою дією.Запаси хлору на деяких об'єктах особливо великі. Наприклад, на водоочисній станції великого міста зберігається до кількох десятків тон цієї речовини.

Хлор - це газ жовто-зеленого кольору з різким запахом, важчий за повітря в 2,5 рази. Тому при аварії він буде накопичуватися в підвалах, низинах. Конденсується в рідину при температурі32^{o}С. Добре розчинний у воді та деяких органічних розчинниках. В організм хлор потрапляє через органи дихання, слизові оболонки, проявляючи в місцях проникнення подразнюючe-припікаючу дію. При легкому ступені отруєння настає почервоніння і свербіння шкіри, подразнення слизових оболонок очей, сльозотеча, ураження верхніх дихальних шляхів: сухий кашель, різкий біль за грудиною. При великих отруєннях спостерігається: різке подразнення слизових оболонок; сильні приступи кашлю; печіння і біль у носоглотці; різь в очах; некоординовані рухи; втрата свідомості; набряк легень; зупинка дихання.

Перша допомога при ураженні. На потерпілого необхідно надіти протигаз ЦП-5, ЦП-6 з коробкою марки В або ізолюючий протигаз. Винести з небезпечної зони, за необхідності зробити штучне дихання. Зігріти тіло промити слизові оболонки і шкіру 2%-м розчином питної соди, змити уражену поверхню чистою водою з милом. У пошкоджені очі закапати 1%-й розчин новокаїну. При отруєнні середнього ступеня дати випити теплого молока із

содою або лужної мінеральної води типу “Поляна Квасова”. Терміново госпіталізувати.

Сірководень (H_2S) речовина, яка має задушливу та загальноотруйну дію. Сірководень - безбарвний газ із характерним запахом зіпсованих яєць. Важчий за повітря. Використовується для отримання сірки, сірчаної кислоти, різних сульфідів для боротьби з сільськогосподарськими шкідниками.

Основний шлях поступання в організм – інгаляційний, але можливе проникнення і через шкіру. При більш високих концентраціях – виражене подразнення слизової очей, носоглотки, металевий присмак в роті, головний біль, відчуття стиснення в грудях, нудота. Подальше вдихання призводить до розвитку токсичного набряку легень.

При появі таких симптомів потерпілого необхідно винести на повітря, очі і слизові оболонки не менше15 хвилин промивати водою або 2%-м розчином борної кислоти.

Є три способи захисту населення від наслідків надзвичайних ситуацій мирного і воєнного часів це: укриття населення в захисних спорудах; проведення евакуаційних заходів; використання населенням засобів індивідуального і медичного захисту.

Дуже велику роль грає своєчасне оповіщення та інформування населення про загрозу та виникнення надзвичайної ситуації. Це завдання покладено на центральні та місцеві органи виконавчої влади, керівників ПНО об’єктів, які зобов'язані надавати населенню оперативну і достовірну інформацію про обстановку, що склалося під час аварії та необхідні дії населення. Особливо це відноситься до керівників ХНО в зону зараження яких потрапляє населення,що мешкає поблизу цих об’єктів.

Укриття населення в захисних спорудах - найбільш надійний спосіб захисту, так як ці типові інженерні конструкції підземного типу забезпечують надійний захист людей практично від усіх вражаючих факторів мирного і воєнного часу. Укриттю в захисних спорудах підлягає населення відповідно до його належності до групп: працююча зміна категорійованих об’єктів, населення, яке проживає в небезпечних зонах та інше населення. Для укриття

населення в надзвичайних ситуаціях використовують сховища та протирадіаційні укриття, які будуються завчасно в містах та інших населених, пунктах. Крім того, можна використовувати в великих містах метрополітени, підвали, напівпідвали шляхом їх дообладнання, а в сільській місцевості погреби, овочесховища.

Евакуація населення здійснюється шляхом вивозу населення всіма видами громадського транспорту і індивідуальним транспортом; виводом населення пішки (при цьому формуються колони по підприємствам) і комбінованим способом, коли масовий вивід населення пішки поєднується з вивозом його всіма видами транспорту. Аналіз показує що більшість великих транспортних підприємств в містах знаходиться вчасної власності і питання вивозу населення в разі небезпеки, яка потребує евакуації населення не вирішена на місцевому і державному рівні. Нормативні документи, які визначають час для організації і проведення евакуації не виконуються.

Захист населення шляхом використання населенням засобів індивідуального і медичного захисту досить надійний і дозволяє значно зменшити ураження людей при аваріях на підприємствах з викидом хімічних речовин. Держава приділяє увагу цьому питанню. Останнім часом розроблені ефективні препарати (вакцини, виворотки, щеплення) проти небезпечних інфекційних хвороб, розроблені і використовуються антидоти від отруєння (ураження) різними СДОР, використовуються радіопротектори, які зменшують радіаційне ураження людини.

В даному розділі було висвітлено роль охорони праці та безпеки в надзвичайних ситуаціях для сучасного виробництва, та було доведено необхідність розробки заходів безпеки у дипломній роботі. Було досліджено і висвітлено питання впливу СДОР на працездатність населення.

РОЗДІЛ 6
ЕКОЛОГІЯ

6.1 Основні положення в екології

Охорона довкілля та раціональне використання природних ресурсів є невід'ємною частиною процесу суспільного розвитку української держави, адже природні ресурси є основою життєдіяльності населення та економіки держави, тому забезпечення їх збереження, відтворення та невиснажливого використання є однією з основних передумов сталого соціально-економічного розвитку країни.

Сучасне екологічне становище України не може розглядатись без минулого нашої країни, без історії природокористування, без врахування важливої моделі: людина - виробництво - природа. Зміни, які відбуваються внаслідок людської діяльності, негативно впливають на довкілля, тому в сучасному світі надзвичайно важливого значення набула справа охорони навколишнього природного середовища.

Як свідчить досвід, проводити ефективну політику невиснажливого розвитку в державі досить важко, навіть за умов процвітаючої економіки. Тим складнішою виглядає ця проблема в Україні — молодій державі, яка переживає успадковану кризу і змушена одночасно вирішувати безліч проблем: політичних, економічних, соціальних, екологічних.

Забруднення довкілля зв'язане з моєю роботою полягає в шкідливих впливах ПК який використовується в результаті реалізації моєї дипломної роботи. Об'єктом забруднення виступає джерело електромагнітних випромінювань блок живлення.

Електромагнітні хвилі радіочастот, часто звані струмами високої частоти (ТВЧ) - область випромінювань, що характеризується великим діапазоном довжин хвиль: від кількох кілометрів до десятків і одиниць міліметрів.

Поширення електромагнітних хвиль радіочастот пов'язано з появою електричних і магнітних полів (ЕМП). Електромагнітні поля знайшли широке

застосування в різних галузях діяльності людини, наприклад, у машинобудуванні ЕМП застосовують для нагрівання металів при плавці, куванню, загартуванню, пайку, а також неметалів при склеюванні, сушіння та інших технологічних процесах.

Застосування електромагнітних випромінювань в діапазоні радіочастот в електротермічних установках дає значні переваги. Разом з тим, вплив зазначених полів на організм людини протягом робочого дня в дозах, що перевищують допустимі значення, може призвести до тяжких професійним захворюванням.

Зростання напруженості ЕМП і його вплив на людину і природне середовище поки дуже мало вивчені і часто розглядаються як негативне, небезпечне явище з неясними поки біологічними наслідками. Рівні ЕМП поблизу ЛЕП вважаються безпечними. Багато фахівців беруть за безпечні для постійно проживають поблизу ЛЕП людей рівні електричного поля менше 5 кВ / м і магнітного поля менше 0,1 мкТл. Обробляючи грядки під лінією електропередачі 400 - 735 кВ, ви перебуваєте в зоні дії електромагнітного поля з напруженістю електричної компоненти більше 10 кВ / м. Гігієнічні нормативи дозволяють працівнику знаходиться в зоні дії електричного поля з частотою 50 Гц і напруженістю 10 кВ / м не більше 3 годин, а для поля 100 кВ / м і вище - не більше 10 хв в день.

6.2 Метод екологічної статистики.

Екологічна статистика - галузь статистики природних ресурсів і навколишнього середовища. Включає дані про стан забруднення природних об'єктів - атмосферного повітря, природних водних об'єктів, грунтів, одержувані на підставі моніторингу. Якість природних об'єктів оцінюється показниками: кількість вимірів, середня концентрація, максимальна концентрація, повторюваність концентрації шкідливих домішок вище гранично припустимої концентрації. Дані екологічної статистики використовуються в соціально-економічному аналізі для оцінки результатів заходів щодо зниження

шкідливих викидів в атмосферу, забруднених стоків у природні водні об'єкти, визначення взаємозв'язку якості навколишнього середовища і станів здоров'я населення, а також визначення економічного збитку від забруднення навколишнього середовища в зв'язку зі зниженням врожайності сільськогосподарських культур, погіршенням продуктивності у тваринництві, підвищеним зносом будинків, споруджень і т. д..

Статистика стану і забруднення атмосферного повітря — підрозділ статистики природних ресурсів і навколишнього середовища, основним завданням якого є збір і узагальнення інформації про виконання заходів щодо охорони атмосферного повітря, про шкідливі викиди в атмосферу. В аналітичній роботі використовуються також дані про якісний стан атмосфери. Виробничі об'єднання (комбінати), підприємства й організації, що мають шкідливі викиди в атмосферу, представляють у статистичні органи звіт про охорону атмосферного повітря, що характеризує виконання ними заходів щодо охорони атмосферного повітря від забруднень, а також викиди шкідливих речовин в атмосферу (без очищення і після очищення), їхнє уловлювання (знешкодження) і утилізацію, оснащення джерел викидів газоочисними і пиловловлюючими спорудженнями. Для підвищення вірогідності статистичної інформації на підприємствах уведені форми первинної звітної документації, що заповнюються регулярно протягом року. Допоміжним джерелом статистичної інформації є одноразові обстеження, інвентаризація викидів шкідливих речовин в атмосферу, вибіркове обстеження причин простоїв і неефективної роботи газоочисних споруджень. Кількісну оцінку шкідливих викидів автотранспорту здійснюють природоохоронні органи на основі даних про пробіг транспортних засобів і нормативів питомих викидів.

Статистика стану, використання й охорони водних ресурсів — підрозділ статистики природних ресурсів і навколишнього середовища, що вивчає запаси водних ресурсів, їхній склад і якість, забезпеченість народного господарства водними ресурсами, водозабір і водоспоживання, утрати води, економію свіжої води за рахунок повторного й оборотного використання води, водовідведення,

скидання стічних вод у природні водойми й ін. водоприймачі (по видах вод, що скидаються).

Статистика землекористування і земельних угідь - підрозділ статистики сільського господарства. Вивчає склад і структуру землекористувачів і земельних угідь, розмір, стан і динаміку земельного фонду, його трансформацію, ступінь використання, якість ґрунтів, ступінь деградації грунтів та ін.

Статистика охорони і захисту лісу розділ статистики лісового господарства, що характеризує охорону лісу від пожеж, порушення встановленого порядку лісокористування й інші дії, що заподіюють шкоду лісові, а також захист лісу від шкідників і хвороб. Показники охорони і захисту лісу знаходять висвітлення в планах і статистичній звітності.

Статистика знешкодження відходів - підрозділ статистики природних ресурсів і навколишнього середовища, що характеризує утворення, використання, видалення відходів і охорону навколишнього середовища від забруднення ними. У натуральному вираженні враховуються (відповідно до затвердженої номенклатури) маса відходів, що утворяться, (т), їхня утилізація у власному підприємстві і передача для використання ін. підприємствам, вивіз відходів на смітники і сміттєпереробні заводи. У статистиці визначаються розміри земельних площ (га) для складування і знешкодження відходів; витрати на заходи щодо охорони навколишнього середовища від забруднення відходами, включаючи капітальні вкладення на будівництво сміттєпереробних заводів, що забезпечують утилізацію відходів, а також поточні витрати по вивозі і похованню відходів.

6.3 Статичний аналіз тенденцій і закономірностей динаміки в екології.

Екологічніні процеси - явище не статичне, а динамічне. Тобто протягом певного часу - місяць за місяцем, рік за роком змінюється стан забруднень

природних сфер, рівень викидів забруднюючих речовин в навколишнє середовище, об'єм промислових і побутових відходів на звалищах тощо. Дослідження процесів зміни і розвитку явищ у часі відбувається на основі побудови і аналізу рядів динаміки.

В даному розділі було розглянуто основні положення екології, метод екологічної статистики і статичний аналіз тенденцій і закономірностей динаміки в екології.

ВИСНОВКИ

Згідно з результатами дослідження компанії «Ibas», проведеного в січні 2012 року, 70% співробітників крадуть конфіденційну інформацію з робочих місць. Найбільше з роботи забирають такі речі, як книги електронних адрес, бази даних клієнтів, а також комерційні пропозиції і презентації. І, більше того, 72% опитаних не страждають етичними проблемами, вважаючи, що мають законні права на нематеріальне майно компанії. З іншого боку, згідно з існуючою статистикою, в колективах людей, зайнятих тією чи іншою діяльністю, як правило, тільки близько 85% є цілком лояльними (чесними), а інші 15% діляться приблизно так: 5% - можуть зробити що-небудь протиправне, якщо, за їх уявленнями, ймовірність заслуженого покарання мала; 5% - готові ризикнути на протиправні дії, навіть якщо шанси бути викритим і покараним складаються 50% на 50%; 5% - готові піти на протизаконний вчинок, навіть якщо вони майже впевнені в тому, що будуть викриті і покарані. Така статистика в тій чи іншій мірі може бути застосовна до колективів, які беруть участь у розробці та експлуатації інформаційно-технічних складових комп'ютерних систем. Таким чином, можна припустити, що не менше 5% персоналу, що бере участь у розробці та експлуатації програмних комплексів, здатні здійснити дії кримінального характеру з корисливих мотивів або під впливом інших обставин. Отже, порушена в роботі проблема цілком актуальна. І тільки останнім часом компанії, що спеціалізуються на розробці засобів захисту, усвідомили необхідність у розробці засобів захисту від внутрішніх порушників.

В результаті роботи було отримано такі результати:

- виконано огляд сучасних технологій захисту корпоративнх мереж та методів впливу на них зловмисників;
- досліджено доцільність використання кожного із розглянутих методів за конкретних умов;
- представлено результати дослідження у вигляді зручному для кінцевого користувача.

АНОТАЦІЯ

Поліщук А.В. Дослідження методів та засобів захисту інформації в корпоративних мережах.

Метою роботи є дослідження сучасних інформаційних загроз захищених корпоративних мереж.

Предметом дослідження є методи та засоби захисту корпоративних мереж.

Об’єкт дослідження - безпека захищених корпоративних мереж.

Дана робота може бути застосована в вигляді системи підтримки прийняття рішень для захисту інформації в мережах.

Рік виконання дипломної роботи 2013

Рік захисту роботи 2013

Ключові слова: захист мереж, корпоративні мережі, sniffer, захист корпоративних мереж.

Дипломна містить с.141 , рис. - 45 , табл.. - 8 , плакати. – 9, використаних джерел – 28 найменувань.

ANNOTATION

A. Polishchuk Research methods and tools for information security in corporate networks.

The aim is to study threats to modern information secure corporate networks.

The object of study is the methods and means of protection of corporate networks.

The object of study - safety secure corporate networks.

This work can be applied to a decision support system for information security in networks.

Thesis release year 2013

Defense of the thesis year 2013

Key words: network security, corporate network, sniffer, protection of corporate networks.

Explanatory note consists of pages - 141, figures - 45 , tables - 8, placards. – 9.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. А. Астахов. Анализ защищенности корпоративных автоматизированных систем / А. Астахов. – Москва, 2010.

2. Лукацкий А.В. Как работает сканер безопасности / Лукацкий А.В. - Hackzone, 2009.

3. А. Астахов. IDS как средство управления рисками / А. Астахов : [Електронный ресурс]. – Режим доступу : URL : http://www.globaltrust.ru/security/Pubs/Pub2_part5. - Назва з екрану.

4. А. В. Соколов. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. - ДМК Пресс., 2012. – 656с.

5. Hacker Dictionary [Electronic Resource]. – Mode of access : URL : http://www.robergraham.com/hacker-dictionary. - Назва з екрану.

6. Deborah Russell. Computer Security Basics, O'Reilly & Associates / Deborah Russell, G. T. Gangemi. – CA, 2011.

7. Крысин В.А. Безопасность предпринимательской деятельности / Крысин В.А. - М:Финансы и статистика, 2010.

8. Аджиев В. Мифы о безопасности программного обеспечения / Аджиев В. – К: Уроки знаменитых катастроф, 2005. – (Открытые системы).

9. Структура руководства по обеспечению информационной безопасности [Електронный ресурс]. – Режим доступу : URL : http://www.globaltrust.ru/security/knowbase/Policies/Guide_Struct. - Назва з екрану.

10. Как обосновать затраты на информационную безопасность? [Електронный ресурс]. – Режим доступу : URL : http://www.iitrust.ru/articles/zat_ibezop. - Назва з екрану.

11. Демин В.С. Автоматизированные банковские системы / Демин В.С. - М: Менатеп-Информ, 2003.

12. Whalen, Sean. An Introduction to ARP Spoofing / Whalen, Sean. – 2001.

13. RFC 1734 POP3 Authentication command [Electronic Resource]. – Mode of access : URL : http://www.faqs.org/rfcs/rfc1734. - Назва з екрану.

14. RFC 959 File Transfer Protocol [Electronic Resource]. – Mode of access : URL : http://www.faqs.org/rfcs/rfc959. - Назва з екрану.

15. Cracking NTLMv2 Authentication [Electronic Resource]. – Mode of access : URL : http://www.securityfriday.com. - Назва з екрану.

16. Kimmo Kasslin Antti Tikkanen Attacks on Kerberos V in a Windows 2000 Environment [Electronic Resource]. – Mode of access : URL : www.hut.fi/~autikkan/kerberos/docs/phase1/pdf/LATEST_final_report. - Назва з екрану.

17. Frank O'Dwyer Feasibility of attacking Windows 2000 Kerberos Passwords [Electronic Resource]. – Mode of access : URL : http://www.brd.ie. - Назва з екрану.

18. [Electronic Resource]. – Mode of access : URL : http://lasecwww.epfl.ch/php_code/publications/search.php?ref=Oech03. - Назва з екрану.

19. [Electronic Resource]. – Mode of access : URL : http://www.antsight.com/zsl/rainbowcrack. - Назва з екрану.

20. Цифры на стороне Microsoft [Електронный ресурс]. – Mode of access : URL : Internet URL http://www.izone.kiev.ua . - Назва з екрану.

21. [Electronic Resource]. – Mode of access : URL : http://www.microsoft.com/technet/security/bulletin/ms03-026.mspx. - Назва з екрану.

22. Daiji Sanai Detection of Promiscuous Nodes Using ARP Packets [Electronic Resource]. – Mode of access : URL : http://securityfriday.com. - Назва з екрану.

23. SANS Bulletin Why your switched network isn't secure [Electronic Resource]. – Mode of access : URL : http://www.sans.org. - Назва з екрану.

24. Tom King Packet Sniffing In a Switched Environment [Electronic Resource]. – Mode of access : URL : http://www.sans.org. - Назва з екрану.

25. arp_antidote - средство для активной борьбы с атаками типа arpoison [Електронный ресурс]. – Режим доступу : URL : http://www.securitylab.ru/33493. - Назва з екрану.

26. IP Smart Spoofing -новый метод отравления ARP кэша [Електронный ресурс]. – Режим доступу : URL : http://www.securitylab.ru/34607 - Назва з екрану.

27. Михаил Разумов. Десять мифов о паролях в Window / Михаил Разумов: [Електронный ресурс]. – Режим доступу : URL : http://www.securitylab.ru/29827 - Назва з екрану.

28. Сканирование. За и Против. / [Електронный ресурс]. – Режим доступу : URL : http://www.securitylab.ru/40572.html - Назва з екрану.