Міністерство транспорту та зв'язку України
Державна адміністрація зв'язку

Одеська національна академія зв'язку ім. О.С. Попова

Кафедра інформаційної безпеки та передавання даних

Д. В. Голев, В. Й. Кільдишев, В. Г. Кононович

ІНФОРМАЦІЙНА БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ
Лабораторний практикум
Частина 1 – Комплекси засобів захисту інформації від НСД

Навчальний посібник

Для студентів вищих навчальних закладів, які навчаються за напрямом «Системи технічного захисту інформації»

За редакцією члена-кореспондента МАЗ, к. т. н., доцента В.Г. Кононовича

Одеса 2010

УДК 004.056; 681.336; 621.39

Голев Д.В., Кільдишев В.Й., Кононович В.Г. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум Частина 1 – Комплекси засобів захисту інформації від НСД: Навч. посібник / За ред. чл.-кор. МАЗ **В.Г. Кононовича**.– Одеса: ОНАЗ ім. О.С. Попова, 2010. – С.176.

Рецензенти:

……..

ISBN _____

Представлені тематичні цикли лабораторного практикуму в галузі знань «Інформаційна безпека». Цикли лабораторного практикуму складені з навчально методичних рекомендацій та посібників для виконання лабораторних робіт з напряму підготовки «Системи технічного захисту інформації» і об'єднані задачею створення комплексних систем технічного захисту інформації на об'єктах інформаційної діяльності органів місцевої державної влади.

Навчальний посібник буде корисний студентам бакалаврату, магістрату та слухачам курсів підвищення кваліфікації у галузі знань інформаційної безпеки.

Для студентів старших курсів вищих навчальних закладів.

СХВАЛЕНО
на засіданні кафедри інформаційної
безпеки та передавання даних
і рекомендовано до друку
Протокол № 1 від 28.08.2010 р.

ISBN

ВСТУП

Комплексна система технічного захисту інформації є важливою і невід'ємною системою об'єктів інформаційної діяльності органів державної влади, зокрема їх інформаційно – аналітичних систем, систем електроніки та телекомунікацій. Практична підготовка технічних фахівців для роботи в галузі «Інформаційна безпека» передбачає здобуття компетенцій фахівців, які мають бути здатними та уміти виконувати професійну роботу на посадах:

- фахівець із організації захисту інформації з обмеженим доступом;
- фахівець із експлуатації, модернізації та ремонту засобів технічного захисту інформації;
- фахівець із захисту інформації в комп'ютерних та інших технічних засобах від копіювання та несанкціонованого доступу;
- фахівець із режиму секретності;
- фахівець – консультант з безпеки промислових об'єктів, помешкань і громадських будинків включно з оцінкою їхньої безпеки;
- фахівець з розслідування та дізнання;
- фахівець з нагляду, охорони та інших видів захисту.

Випускники курсів мають набути професійні компетенції щодо вирішення проблем і задач соціальної діяльності та системи умінь, що забезпечують наявність цих компетенцій.

Бакалаври за напрямом підготовки «Системи технічного захисту інформації» мають набути такі загально професійні компетенції:

- здатність оперативно управляти діяльністю підрозділу з захисту інформації;
- здатність і готовність до використання методів аналізу й діагностики стану програмно-апаратних засобів і систем технічного захисту інформації та до забезпечення процесу захисту інформації з використанням необхідних видів, методів, засобів і технологій захисту;
- здатність і готовність до використання вміння:
  - по обліку, обробці, зберіганню, передачі, організації використання різних носіїв конфіденційної інформації;
  - по виявленню й блокуванню каналів і методів несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію;
  - по установці та адаптації систем і засобів забезпечення захисту інформації;
  - по здійсненню контролю якості функціонування устаткування захищених інформаційних систем, аналізу якісних і кількісних показників функціонування устаткування, діагностиці й усунення відмов, настроюванню й ремонту устаткування.

Бакалаври мають набути також спеціалізовано професійні компетенції, які забезпечуються здатністю та готовністю використовувати уміння:

- експериментального визначення наявності загроз інформації в автоматизованих системах;

- розрахунку характеристик і вибору елементів конкретної автоматизованої системи з урахуванням забезпечення необхідного рівня захисту інформації;
- оцінки працездатності елементів захищеної автоматизованої системи;
- використання комплексної системи захисту інформації в організації (підприємстві); засобів захисту програмного забезпечення від несанкціонованого копіювання, впливу комп'ютерних вірусів тощо; криптографічних методів і програмно – апаратних засобів захисту інформації;
- здійснення технічного обслуговування, контролю і діагностики комплексної системи захисту інформації в організації (підприємстві);
- настроювання, регулювання й ремонту устаткування автоматизованої системи й настроювання й апгрейду спеціального програмного забезпечення;
- забезпечення виконання вимог інструкцій з інформаційної безпеки;
- контролю правильності застосування технічних засобів забезпечення інформаційної безпеки;
- забезпечення інформаційної безпеки периметру та протидії атакам;
- організувати моніторинг стану інформаційної безпеки;
- аналізувати порушення інформаційної безпеки та вплив інформаційної безпеки на економіку бізнесу.

Проведення лабораторного практикуму та самостійне вивчення розділів змістовних модулів забезпечується лабораторними класами, оснащеними сучасною комп'ютерною технікою, вимірювальними та індикаторними приладами й комплексами, зразками технічних та програмно – технічних засобів захисту інформації, автоматизованими системами навчання.

Кожному студенту доступні загальні та режимні бібліотечні фонди, бази даних, навчальні пакети на носіях, за змістом відповідним дисциплінам основної освітньої програми:
- «Методи та засоби технічного захисту інформації»;
- «Безпека інформаційно – комунікаційних систем»;
- «Технічні засоби охорони об'єктів»;
- «Комплексні системи захисту інформації»
- «Управління інформаційною безпекою»;
- «Системи технічного захисту інформації»
- «Аудит інформаційної безпеки».

Навчальний посібник підготували: Д.В. Голев (розд. 1, розд. 2), В.Й. Кільдишев (розд. 2), к.т.н., доцент В.Г. Кононович (вступ, розд. 1,).

ГЛАВА 1 КОМПЛЕКСНІ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Організація та технічна експлуатація систем захисту грифованої інформації від несанкціонованого доступу на робочих станціях

1.1.1 Політика безпеки інформації в комп'ютерній системі

Автоматизованим робочим місцем (АРМ) називається робоче місце працівника підприємства, оснащене персональним комп'ютером та відповідним програмно-апаратним забезпеченням. Термін *робоча станція* є синонімом терміну АРМ. Його застосовують, коли слід підкреслити, що в комп'ютерній мережі даний комп'ютер є прикінцевим устаткуванням мережі і на ньому функціонує операційна система кінцевого робочого місця, на відміну від мережної операційної системи серверів, маршрутизаторів тощо.

У цьому розділі посібника розглядаються два типи автоматизованих робочих місць: відокремлених автономно працюючих та робочих місць, приєднаних до інформаційно-обчислювальної мережі.

Відокремлені автоматизовані робочі місця, доступ до яких контролюється з використанням організаційних заходів, належать до класу "1" автоматизованих систем. Клас "1" — це одномашинний однокористувацький комплекс, який опрацьовує інформацію однієї чи кількох категорій конфіденційності. Істотні особливості цього класу:

- в кожний момент часу з комплексом може працювати лише один користувач, хоч у загальному разі осіб, які мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка опрацьовується;
- технічні засоби – носії інформації та засоби введення/виведення – з точки зору захищеності належать до однієї категорії і всі можуть використовуватись для зберігання та/чи введення/виведення всієї інформації.

АРМ, приєднані до інформаційно-обчислювальної мережі, слід відносити до того чи іншого класу за видом інформаційно-обчислювальної мережі, до якої їх долучено: локальної чи глобальної.

Можливі є два протилежні підходи до зрелізовувння систем захисту інформації в комп'ютерних системах:

- перший підхід полягає у дороблянні існуючих систем і доповненні їх додатковими засобами захисту;
- другий, більш надійний, – полягає у створенні захищеної комп'ютерної системи починаючи зі створення базового захищеного ядра й далі – захищених оболонок.

Прикладом другого підходу є операційна система (ОС) Windows NT чи VAX VMS, у яких система захисту є частиною ОС.

Розглянемо практичне зреалізовування системи захисту першого типу у стандартній незахищеній операційній системі MS Windows 95/98.

В Україні започатковано власне виробництво захищених від витікання каналами побічних електромагнітних випромінювань і наведень (ПЕМВН) засобів обчислювальної техніки, програмно-апаратних засобів захисту, активних засобів захисту інформації, пристроїв захисту інформації в телефонних лініях та ін. Є можливості реалізовувати функціональний профіль захищеності, що задовольняє заданим вимогам щодо захищеності інформації.

Комплекс заходів захисту (КЗЗ) системи автоматизації, окрім вимог щодо блокування технічних каналів витікання, має відповідати вимогам, які сформульовано в НД ТЗІ 2.5-005-99 [10], а саме вимогам щодо конфіденційності, доступності та спостережуваності. КЗЗ має забезпечувати конфіденційність опрацьовування інформації на окремому комп'ютері, спостережуваність дій користувача й цілісності інформації. Слід заблоковувати доступ сторонніх та організовувати спільну роботу легальних користувачів.

Загрози інформації на окремо взятому комп'ютері можуть бути природними чи техногенними, випадковими чи зумисними, спричинені хибними налаштовуваннями системи чи помилками у ній тощо.

Основні потенційні загрози на окремо взятому комп'ютерові такі:

- інформацію можна підглянути, порушивши у такий спосіб її конфіденційність;
- інформацію можна підмінити, порушивши її цілісність;
- доступ до інформації може бути заблоковано, отже порушується доступність інформації та послуг, надаваних комп'ютером;
- понад зазначене існує небезпека того, що зреалізовування загрози залишиться таємним, або провину буде покладено на непричетну до цього особу. Це є порушування спостережуваності дій користувача чи поводження системи.

Для захисту від загроз в комп'ютерних системах зреалізовують функції захисту, які у сукупності створюють так звані послуги безпеки. Кожна послуга, яка складається з набору функцій, протистоїть певній множині загроз конфіденційності, цілісності, доступності чи спостережуваності.

За зреалізовуванні засобів захисту враховують такі моменти:

- властивості обчислювальної системи та інформації, яка на ній опрацьовується. Сюди можуть входити опрацьовування конфіденційної інформації, організація спільної роботи декількох користувачів на одному комп'ютері, можливість надання атрибутів одного чи декількох привілейованих користувачів-адміністраторів, які могли б зорганізувати роботу;
- необхідна стійкість та надійність зреалізовування функцій захисту;
- від кого чи від чого є необхідний захист;
- вимоги нормативних документів, критерії оцінювання, накопичений досвід та здоровий глузд;
- вимоги щодо вартості створення системи захисту. Витрати на захист інформації не повинні перевищувати можливих збитків за здійсненні загроз;

- зручність експлуатації системи захисту. Якщо система не є зручна й заважає роботі, якщо вона не є дружня стосовно легального користувача, то користувач шукатиме способи оминання захисту і врешті відзнайде їх;
- розробник системи захисту. Систему захисту має бути атестовано.

У кожній організації існують певні правила роботи з інформацією. Нагадаємо, що *політикою безпеки* інформації називають сукупність правил, законів, інструкцій та інших правових норм, які регламентують порядок опрацьовування інформації, прийнятий в організації. Політика безпеки інформації є складовою частиною загальної політики безпеки підприємства.

Політика безпеки включає в себе перелік вимог, перелік загроз та оцінювання ризиків і описання створеного комплексу заходів протидії.

У загальному разі комплекс заходів протидії, тобто система захисту інформації включає:

- організаційні – інструкції, рекомендації тощо;
- фізичні – охорона, сигналізація тощо;
- технічні заходи безпеки й засоби захисту.

До технічних заходів належить використання:

- засобів захисту від витікання каналами електромагнітного випромінювання, телефонними лініями, сигналізацією тощо;
- програмних засобів захисту від несанкціонованого доступу;
- засобів криптографічного захисту.

Сукупність програмно-апаратних засобів, які функціонують безпосередньо у складі комп'ютерної системи, називають *комплексом засобів захисту*. КЗЗ зреалізовує послуги безпеки, котрі протистоять існуючим загрозам. Зауважимо, що такий КЗЗ обов'язково має бути частиною загальної системи безпеки поряд з організаційними та фізичними заходами.

1.1.2 Принципи впровадження політики безпеки

Розмежовування доступу користувачів до ресурсів здійснюється у відповідності з концепцією диспетчера доступу (reference monitor, див. підрозділ 6.3). У процесі перевірення легальності кожного запиту на доступ до ресурсів беруть участь такі компоненти обчислювальної системи:

- *активний об'єкт,* чи *суб'єкт доступу*, – це користувач чи породжений користувачем процес, який намагається отримати доступ до певної інформації. Процес – це програма, в якій знаходиться керування і яка в даний момент є представником користувача в системі;
- *пасивний об'єкт,* чи *об'єкт доступу*, – це пасивне джерело/приймач інформації, до якого звертаються і який потребує захисту;
- *база даних (БД) авторизації (повноважень)* – це інформація, яка визначає права доступу користувачів і процесів до пасивних об'єктів. Така інформація називається *атрибутами доступу*;
- *база даних реєстрування*, – це записи щодо запитів та надавання доступу суб'єктів до об'єктів;

- *диспетчер доступу*, – це засоби, які зреалізовують встановлені правила розмежовування доступу і сприяють дотриманню політики безпеки інформації, прийнятої на підприємстві. Диспетчер доступу зреалізовує функції захисту і забезпечує безпеку інформації шляхом:

- керування створенням користувачів, процесів та пасивних об'єктів;

- надавання активним об'єктам доступу до пасивних у відповідності з інформацією, котра міститься у базі даних;

- реєструванні подій та дій активних об'єктів у базі даних реєстрування.

Цей комплекс засобів захисту зреалізовує адміністративне (mandatory) розмежовування доступу. Це означає, що керування БД авторизації (атрибутами доступу) та БД реєстрування здійснюють лише адміністратори – тобто користувачі, які мають відповідні повноваження. Звичайні користувачі не можуть змінювати атрибути доступу та виконувати будь-які інші функції керування засобами захисту.

Користувачі. Кожна особа, котра матиме доступ до ПЕОМ, має бути зареєстрована. В перебігу реєстрування кожного користувача для нього створюється структура даних, називана обліковим записом користувача, яка записується до БД користувача. В БД користувача фіксуються також всі атрибути користувача, його привілеї тощо. Реєструє користувачів адміністратор, який має відповідні повноваження.

В обліковому записі користувача містяться такі його атрибути:

- ім'я чи псевдонім;
- встановлений системою захисту ідентифікаційний код;
- реєстровані в журнальному файлі події та режим реагування на спроби несанкціонованого доступу;
- функції адміністратора чи привілеї, доступні даному користувачеві;
- дата дії повноважень користувача та термін чинності паролю;
- дні тижня та години дня, в які користувачеві дозволено вхід до системи;
- додаткова інформація, використовувана за ідентифікування та автентифікування користувача при входженні до системи.

Адміністратори. Політика безпеки окрім правил розмежовування доступу, встановлює правила керування. Функції керування покладаються на довірених осіб, які несуть відповідальність за безпеку опрацьовуваної інформації. Цих осіб називають адміністраторами комп'ютерних систем. Адміністратори – це користувачі, за якими закріплено й записано в облікових даних привілеї на переглядання журнальних файлів, реєстрування програмного забезпечення, реєстрування користувачів, керування доступом до каталогів та файлів.

Користувач, який встановлює систему, автоматично призначається головним адміністратором і має майже всі доступні привілеї. Він має фіксований ідентифікаційний номер – "1" і його обліковий запис не може бути вилучено. Головний адміністратор має право створювати, вилучати та змінювати повноваження будь-яким користувачам, як звичайним, так і

адміністраторам. Але він **не має права** створювати захищені каталоги й призначати права доступу до них.

Адміністратор (не головний) реєструється в системі головним адміністратором і має право створювати, вилучати та змінювати повноваження звичайному користувачеві, але не має права це робити для головного адміністратора.

Процеси. В комплексних засобах захисту (КЗЗ) зреалізовують розмежовування доступу до каталогів КЗЗ з боку процесів. Користувачі можуть отримати доступ за записом до каталогу КЗЗ лише через АРМ адміністратора. АРМ адміністратора дозволяє модифікувати БД КЗЗ лише маючим повноваження користувачам і у відповідності з установленими правилами. В журнали завжди заноситься інформація про те, від якого процесу надійшов запит на доступ до об'єкта та/чи виконання певної операції.

Пасивні об'єкти. Захищуваними об'єктами є каталоги логічних дисків та файли, розміщені в них. Розмежовування доступу користувачів до файлів і каталогів здійснюється у відповідності з принципами адміністративного розмежовування доступу. Для кожного каталогу адміністратор може встановити список доступу, в якому перелічено користувачів, котрі мають права доступу до цього каталогу і файлів та дозволені цим користувачам типи доступу, наприклад лише читання.

1.1.3 Надбудований КЗЗ над стандартними операційними системами

Комплекс засобів захисту від НСД першого типу призначено для захисту опрацьовуваної на ПЭОМ інформації від несанкціонованого ознайомлення, модифікування, вилучання. КЗЗ дозволяє створити безпечне технологічне середовище для систем електронного документообігу, банківських та інших систем, для яких ключовою вимогою є дотримання конфіденційності опрацьовуваної інформації та технології її опрацьовування. КЗЗ слугує спеціалізованою надбудовою над стандартною операційною системою MS Windows 95/98 і доповнює її функціями розмежування доступу. Комплекс дозволяє створити захищене автоматизоване робоче місце з обмеженим колом користувачів, які мають різні повноваження щодо доступу до ресурсів.

Сукупність зреалізованих у комплексі функцій та механізмів захисту інформації забезпечує рівень захищеності інформації, достатній для опрацьовування інформації, яка становить як державну так і комерційну таємницю.

КЗЗ зреалізовує такі функції,як:

- ідентифікування й автентифікування користувачів при завантаженні ПЕОМ до завантаження будь-яких програмних засобів з дисків на підставі пароля, котрий вводиться користувачем, та ідентифікатора, котрий носиться тим самим користувачем. Це дозволяє заблоковувати завантаження операційної системи (ОС) й використання ПЭОМ сторонньою особою, а також розпізнавати конкретного легального користувача й відповідно реагувати на його запити надалі;

- заблокування завантаження ОС з гнучкого диска та CD-ROM. Це дозволяє гарантувати долучення до роботи всіх компонентів КЗЗ;
- розмежовування доступу користувачів до обраних каталогів та файлів, які розміщено в них. Це дозволяє зорганізовувати спільну роботу декількох користувачів, котрі мають різні права й обов'язки, а також захищати інформацію від випадкового вилучання й модифікування;
- керування потоками інформації й заблокування потоків інформації, які призводять до зниження її конфіденційності;
- гарантоване вилучання конфіденційної інформації шляхом затирання вмісту файлів при їхньому вилучанні;
- контроль за виведенням інформації на роздруківку;
- контроль цілісності прикладного програмного забезпечення (ПЗ) та ПЗ КЗЗ, а також блокування завантаження сторонніх (незареєстрованних) програм і програм, цілісність яких порушено. Це дозволяє забезпечувати захист від вірусів і дотримання технології опрацьовування інформації;
- заблокування пристроїв інтерфейсу користувача (гасіння екрана й заблокування клавіатури й миші) за обраною комбінацією клавіш чи після певного періоду бездіяльності користувача;
- реєстрування подій (завантаження ОС користувачем і завершення сеансу роботи, спроби несанкціонованого доступу, запускання програм, доступ до конфіденційної інформації тощо) у спеціальних журнальних файлах (ЖФ). Це забезпечує зворотний зв'язок і дозволяє адміністраторові стежити за тим, як здійснюється доступ до інформації з боку користувачів, і коригувати на підставі цього параметри конфігурації КЗЗ;
- адміністрування (визначення ресурсів, реєстрування користувачів, призначення прав доступу, опрацьовування журнальних файлів тощо).

Для того, аби зробити обґрунтовані висновки про те, що дозволяє система й чи придатна вона для застосовування в конкретних умовах, слід, як мінімум, розглянути політику безпеки системи в цілому і кожної із зреалізовуваних послуг. Розмежовування доступу користувачів до ресурсів здійснюється за двома способами:

- у відповідності з концепцією диспетчера доступу (reference monitor);
- як зреалізовуванням адміністративного (mandatory) розмежовування доступу.

Структуру системи розмежовування доступу користувачів до ресурсів подано на рис. 1.1.

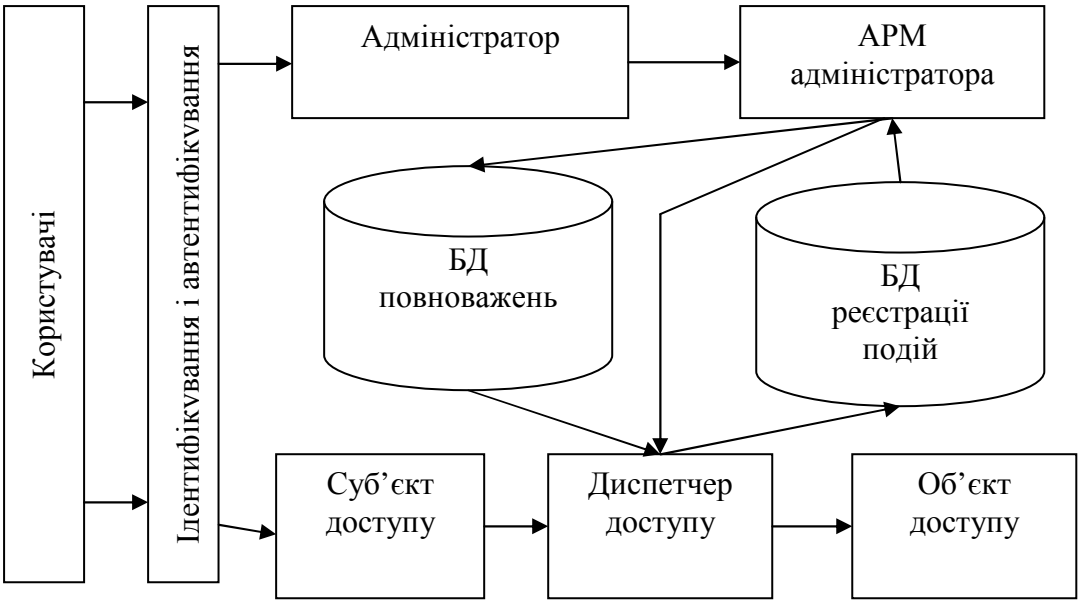

Рисунок 1.1 – Система розмежовування доступу користувачів до ресурсів.

За адміністративного розмежовування доступу керування базою даних повноважень (атрибутами доступу) і базою даних реєстрування здійснюють лише користувачі, котрі мають відповідні повноваження, – адміністратори. Звичайні користувачі не можуть змінювати атрибути доступу, а отже й надавати іншим користувачам доступ до інформації, з яким вони працюють, а також виконувати будь-які функції з керування КЗЗ.

Послуги зреалізовані в КЗЗ

КЗЗ системи автоматизації обраного функціонального профілю захищеності має зреалізовувати такі послуги із захисту інформації:

1) надавати послуги із захисту об'єктів від несанкціонованого ознайомлення з їхнім змістом (компрометації). Конфіденційність забезпечується такими послугами: КА-1 – мінімальна адміністративна конфіденційність, КО-1 – повторне використання об'єктів;

2) надавати послуги із захисту опрацьовуваної інформації від несанкціонованого модифікування. Цілісність може забезпечуватись послугою ЦА-1 – мінімальна адміністративна цілісність;

3) надавати послуги щодо забезпечування можливості використання системи автоматизації в цілому, окремих функцій чи опрацьовуваної інформації на певному проміжку часу і гарантувати здатність системи автоматизації функціонувати у разі відмовляння її компонентів. Доступність може забезпечуватися послугою ДВ-1 – ручне відновлювання після збоїв;

4) надавати послуги із забезпечування відповідальності користувача за свої дії і за підтримування здатності КЗЗ виконувати свої функції. Спостережуваність забезпечується в системі автоматизації такими послугами: НР-2 – реєстрування (аудит), (захищений журнал), НИ-2 – одиночне ідентифікування та автентифікування, НК-1 – односпрямований вірогідний канал, НО-1 – розподіл обов'язків, а саме виокремлення адміністратора, НЦ-1 – КЗЗ з контролем цілісності, НТ-2 – самотестування при стартуванні.

Зреалізовувані системою захисту послуги безпеки можна подати через функціональний профіль. Згідно з НД ТЗИ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”. КЗЗ від НСД може зреалізовувати функціональний профіль:

{КА-2, КО-0, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-1, НТ-2}. Найчастіше розробляння виконують відповідно до вимог щодо рівня гарантій Г-3.

Поданий функціональний профіль є зумовлений призначенням комплексу і сформований на підставі попередньо проведеного аналізування загроз та ризиків з урахуванням таких моментів:

- комплекс призначено для автономної (не підімкненої до локальної мережі і не виступаючої в ролі сервера) ПЕОМ, на якій водночас не можуть працювати кілька користувачів чи виконуватися процеси інших користувачів, що значно скорочує перелік загроз, а отже, й вимоги до набору послуг безпеки;
- комплекс за визначенням є надбудований над програмно-апаратною платформою імпортного виробництва, що накладає низку обмежень на перелік та рівні послуг, які не можна здолати принципово; цим фактом, зокрема, обмежено й рівень гарантій;
- зреалізовування додаткових послуг та/чи їхніх більш високих рівнів, які забезпечують захист від малоймовірних загроз, чи подальше зниження рівня ризику потребує значних витрат.

Зазначений функціональний профіль досягається лише в тому разі, якщо виконується низка умов та обмежень, зокрема обов’язковим є використання апаратного захисту від несанкціонованого завантаження.

Ідентифікування й автентифікування користувача виконуються за допомогою функціональних послуг:

- *НИ-3 – множинне ідентифікування й автентифікування;*
- *НК-1 – односпрямований вірогідний канал.*

Перш ніж здійснювати розмежовування доступу до ресурсів, КЗЗ має розпізнати користувача і блокувати доступ неавторизованих користувачів. Для цього при входженні користувача до системи виконується його ідентифікування (розпізнавання) і автентифікування (перевіряння результатів ідентифікування).

Ідентифікування користувача виконується на підставі введеного ним з клавіатури імені (псевдоніму). Автентифікування користувача виконується на підставі введеного ним з клавіатури пароля й наданого ідентифікатора, що носиться. Отже, зреалізовано автентифікування користувача водночас за двома принципами: “маю щось” – ідентифікатор, що носиться, і “знаю дещо” – пароль.

Носимим ідентифікатором може бути ключова дискета чи ідентифікатор Touch Memory. Touch Memory у базовій конфігурації КЗЗ підмикається до зовнішнього чи внутрішнього розніму спеціальної плати чи може підмикатися до паралельного порту LPT1 (через адаптер DS1410D(E) чи до послідовного порту COM2 (через адаптер DS9097).

У разі, якщо надана користувачем інформація щодо автентифікування не відповідає еталонові, – доступ до системи заблоковується. Окрім того, КЗЗ веде контроль за спливанням терміну чинності повноважень користувача та його пароля, а також за відповідністю дня тижня й часового інтервалу, за який користувач здійснює входження до системи. Всі ці параметри задаються адміністратором.

Вірогідний канал взаємодії користувач–КЗЗ забезпечується шляхом зреалізовування функцій ідентифікування й автентифікування програмами, "прошитими" у мікросхемі ПЗУ розширення BIOS, яка входить до складу КЗЗ. Ці програми отримують керування після ввімкнення електроживлення чи скидання комп'ютера до завантаження будь-яких програм з диска.

У КЗЗ зреалізовано також можливість заблоковування пристроїв інтерфейсу користувача (клавіатури, миші й монітора). Заблоковування здійснюється чи користувачем за допомогою певної комбінації клавіш, чи КЗЗ за бездіяльності користувача в плині певного періоду часу. Для розблокування комп'ютера користувачеві слід пред'явити свій ідентифікатор, що носиться, і ввести пароль.

Контроль цілісності КЗЗ та самотестування виконується за допомогою функціональних послуг:

- *НЦ-1 – КЗЗ з контролем цілісності;*
- *НТ-2 – самотестування при стартуванні.*

Контроль цілісності КЗЗ полягає в перевіренні цілісності ПЗ КЗЗ за кожного завантаження системи. Окрім того, дані операції можуть виконуватися за бажанням адміністратора з використанням програми адміністрування. У разі виявлення порушування цілісності користувачеві надсилається відповідне повідомлення – і подальша робота заблоковується. У такій ситуації необхідне втручання адміністратора для відновлювання цілісності чи переінсталяції КЗЗ.

Однією з додаткових вимог для більш високих рівнів послуги "цілісність КЗЗ" є забезпечування неможливості оминання засобів захисту, що включає забезпечування неперервної роботи цих засобів від моменту ввімкнення електроживлення. Для того аби заблоковувати можливість завантаження ОС за час відсутності засобів захисту, програми, "прошиті" у мікросхемі ПЗУ, зреалізовують:

- заблоковування завантаження ОС з дискети та CD-ROM;
- заблоковування клавіатури до завантаження драйвера реального режиму.

Додатково заблоковується можливість вибору варіанта завантаження ОС у разі аварійного завершення попередньої спроби завантаження.

Окрім того, КЗЗ зреалізовує *контроль цілісності програмного забезпечення*. Дана функця переслідує кілька цілей:

- запобігає поширенню вірусів, а отже, порушенню цілісності ОС, КЗЗ та інформації;
- дозволяє уникнути витікання інформації за рахунок використання прихованих каналів, порушування встановленої технології опрацьовування

інформації, а також інших дій, пов'язаних з упровадженням "троянських коней";

- дозволяє створити умови, коли в системі працює лише перевірене ПЗ, яке, за означенням, не виконує жодних дій, які могли б спричинити вимкнення чи подолання засобів захисту.

Контроль цілісності ПЗ полягає в перевіренні цілісності виконуваних модулів за їхнього завантаження. Завантаження модулів, котрі не відповідають даним про них в еталонному записі БД КЗЗ, заблоковується. БД еталона ПЗ створюється й модифікується уповноваженим адміністратором.

Розмежовування доступу до ресурсів забезпечується виконанням функціональних послуг:

- *КА-2 – базова адміністративна конфіденційність;*
- *ЦА-1 – мінімальна адміністративна цілісність;*
- *КО-0 – мінімальне повторне використання об'єктів.*

Розмежовування доступу користувачів до ресурсів здійснюється на рівні каталогів відповідно до принципів адміністративного розмежовування доступу. Захищувані ресурси, якими є каталоги, ідентифікуються КЗЗ так само, як і операційна система, на підставі повного імені (включаючи ім'я диска та шлях). Кожному каталогові ставиться у відповідність спеціальний атрибут – рівень конфіденційності, який обмежує можливості користувачів з доступу до даного каталогу. Кожному користувачеві ставиться у відповідність рівень допуску.

У КЗЗ може бути введено два чи більше рівнів допуску користувачів та конфіденційності каталогів. Приміром, можна увести два рівні допуску користувачів та конфіденційності: "ДСК" та "ТАЄМНО". Рівень допуску користувача має бути явно заданий адміністратором, у противному разі за вмовчанням згаданий користувач не зможе одержати доступу до захищених каталогів. Рівень конфіденційності каталогу встановлюється при його створенні і його не може бути змінено. Незахищені каталоги вважаються за вмовчанням відкритими (не мають рівня конфіденційності) і доступ до них є дозволений для усіх користувачів.

Приміром, кожен користувач має свій ідентифікаційний код (ІК), який автоматично надається даному користувачеві за його реєстрування. Ідентифікаційний код користувача є унікальним для кожного користувача і надається лише одноразово. Змінити ІК користувача, на відміну від інших атрибутів (імені, пароля, переліку привілеїв, рівня допуску тощо), не можна. Саме на підставі ІК КЗЗ ідентифікує користувача й визначає його повноваження. Кожному користувачеві ставиться у відповідність спеціальний атрибут – рівень допуску, що є аналогічний до форми допуску при роботі з інформацією з обмеженим доступом і визначає його можливості з доступу до цієї інформації.

КЗЗ веде базу даних захищених каталогів, керувати якою можуть адміністратори, котрі мають відповідні повноваження. Для кожного захищеного каталогу адміністратор установлює список доступу, в якому перелічено користувачів, котрі мають права доступу до даного каталогу, підкаталогів та файлів, розміщених в них, і дозволені для цих користувачів

типи доступу (читання чи читання/запис). Для того аби користувач міг одержати доступ до захищеного каталогу, його рівень допуску має бути не менш за рівень конфіденційності каталогу. Користувачі мають лише ті права доступу до захищених каталогів, а отже й до інформації в них, які явно надано адміністратором.

КЗЗ підтримує керування потоками інформації. КЗЗ стежить за тим, аби не відбувалося переміщення інформації (наприклад копіювання файлів) із захищених каталогів у каталоги з меншим рівнем конфіденційності чи відкриті, тобто стежить за тим, аби процеси, в яких є відкриті для читання файли, розміщені в захищених каталогах, не змогли відкривати для запису файли, розміщнеі в незахищених (відкритих чи загальних) каталогах чи каталогах з меншим рівнем конфіденційності. Це, зокрема, дозволяє заблоковувати копіювання файлів із захищених каталогів у незахищені чи з каталогів з більш високим рівнем конфіденційності – в каталоги з меншим рівнем, що запобігає поряд з іншим несанкціонованому експортуванню конфіденційної інформації на змінні носії.

Окрім того, адміністратор має можливість явно визначати спеціальні каталоги імпортування/експортування (наприклад дисковод A:) і користувачів, котрі мають доступ до них, а також здійснювати контроль за виведенням інформації на друкування.

Додатково зреалізовано певні обмеження на доступ (для записування) до каталогу КЗЗ і файлів налаштовування ОС.

Оскільки ідентифікування захищених каталогів здійснюється на підставі повного шляху, то при створюванні захищених каталогів і роботі з ними можливі такі обмеження:

- захист поширюється на всю гілку дерева, розпочинаючи із зазначеного в БД захищеного каталогу, включаючи його підкаталоги. Тому не припускається зазначати як новий захищений каталог, який є підкаталогом уже захищеного каталогу.
- КЗЗ забороняє виконувати перейменування і вилучання захищеного каталогу й тих каталогів, що його містять, аж до диска, розміщеного в корені дерева каталога.

Додатково обмежено доступ до каталогу КЗЗ та файлів налаштовування ОС (CONFIG.SYS, MSDOS.SYS) за записом. Доступ для записування до каталогу КЗЗ користувачі можуть одержати лише через АРМ адміністратора, котрий дозволяє змодифіковувати БД лише користувачам, які мають відповідні повноваження. Право доступу до файлів налаштовування ОС за записом має лише головний адміністратор. Є також можливість заблоковування віддаленого доступу до локальних файлів через ЛВС як до поділюваних ресурсів, навіть якщо таку можливість визначено в налаштовуваннях ОС.

За спроби користувача одержати заборонений вид доступу (наприклад, вилучити файл у каталозі, до якого дозволено доступ лише для читання) у журнальному файлі КЗЗ реєструється спроба НСД і, якщо для користувача не встановлено “м’який” режим реагування на спроби НСД, у якому здійснюється лише реєстрування НСД, – доступ заблоковується.

Додатково до функцій безпосереднього розмежовування доступу в КЗЗ зреалізовано послугу “повторне використання об’єктів”. У разі включення даної можливості за вилучання файлів, розміщуваних в захищених каталогах, здійснюється запис поверх інформації, що є у файлах, псевдовипадкової бінарної послідовності (так званий wiping). Додатково може затиратися інформація в записі каталогу даного файла – ім’я файла та його довжина.

Реєстрування дій користувачів здійснюється за допомогою функціональної послуги *НР-2 – захищений журнал.*

КЗЗ реєструє спроби несанкціонованого доступу в спеціальних журнальних файлах і, якщо для користувача не встановлено “м’який” режим реагування на спроби НСД, – заблоковує виконання несанкціонованих дій. Окрім того, в журнальних файлах реєструються факти входження користувача до системи, а також факти змінення стану бази даних КЗЗ: реєстрування користувачів та ПЗ, змінення прав доступу до файлів тощо. Додатково для кожного користувача може бути встановлено необхідність реєстрування фактів запускання програм, доступу до захищених каталогів і звертань до звичайних файлів та каталогів (відкриття файлів для читання та/чи записування, створення, перейменовування, вилучання файлів та каталогів, переглядання вмісту каталогів).

У кожнім записі журнального файла фіксуються дата й час події, тип та атрибути операції, наприклад відкриття файла для читання/записування, атрибути процесу й користувача, котрі зініціювали подію, ознаки успішності завершення операції й у разі відмовлення – причина, а також інша інформація.

Опрацьовування журнального файла здійснюється адміністратором, котрий має відповідні повноваження, і включає:

- переглядання інформації, наявної в журнальному файлі;
- аналізування статистики;
- добирання певних записів при перегляданні за діапазоном параметрів;
- групування повторюваних подій чи стандартних послідовностей подій, задаваних адміністратором, у групи подій;
- роздруковування журнального файла.

Опрацьовування журнального файла здійснюється адміністратором за допомогою відповідного режиму АРМ адміністратора.

Розмежовування обов’язків виконується за допомогою функціональної послуги *НО-2 – розмежовування обов’язків адміністраторів.*

За кожним адміністратором може бути закріплено привілеї на:

- переглядання журнальних файлів;
- реєстрування ПЗ;
- реєстрування користувачів;
- керування правами доступу до каталогів.

Окрім того, явно виокремлена роль головного адміністратора, який має право призначати адміністративні привілеї і встановлювати інші атрибути для

інших адміністраторів, однак не має і не може мати права на керування доступом до каталогів.

Відновлювання після збоїв виконується функціональною послугою *ДВ-1 – ручне відновлювання.*

У КЗЗ передбачено можливість відновлювання працездатності системи головним адміністратором після збоїв, які призвели до порушування цілісності ПЗ чи БД КЗЗ, і в інших подібних ситуаціях.

Отже, установлення на ПЕОМ КЗЗ дозволяє забезпечувати:

- неможливість неконтрольованого й несанкціонованого ознайомлення, копіювання та відновлювання інформації;
- неможливість неконтрольованої й несанкціонованого модифікування та вилучання інформації;
- надавання доступу до інформації лише за умови вірогідного розпізнавання користувачів та з урахуванням повноважень, надаваних відповідно до службової необхідності;
- облік дій користувачів та реєстрування спроб порушування встановленого порядку доступу до інформації, включаючи заблоковування доступу до інформації у разі виявлення таких спроб, а також можливість здійснення контролю за доступом до інформації з боку уповноважених осіб.

1.1.4 Надбудований мережний комплекс засобів захисту інформації

,

В комп'ютерних мережах зреалізовують КЗЗ із централізованим керуванням. При цьому часто зреалізовують централізоване віддалене адміністрування локальних комплексів, установлених на робочих станціях локальної обчислювальної мережі з протоколом TCP/IP. До складу такого КЗЗ входить автоматизоване робоче місце віддаленого адміністрування (АРМ ВА) та комплекс засобів захисту робочих станцій (РС).

На робочих станціях зреалізовуються такі додаткові функції:

- криптографічний захист файлів в обраних каталогах у прозорому режимі;
- підтримування віддаленого адміністрування.

Криптографічний захист

При установленні захисту на каталог за бажанням адміністратора може здійснюватися шифрування інформації у всіх файлах даного каталогу і його підкаталогів. Шифрування інформації здійснюється відповідно до алгоритму криптографічного захисту, установленого ГОСТ 28147-89. Розшифровування/зашифровування інформації, розміщеної в зашифрованих файлах, здійснюється в прозорому режимі, тобто безпосередньо при читанні/записуванні інформації.

За рахунок зреалізовування даної функції запобігаються загрози порушування конфіденційності захищеної інформації у разі оминання засобів захисту чи відторгнення носіїв інформації НЖМД, наприклад викрадання. Окрім того, використання криптографічних перетворень дозволяє задовольняти

вимоги щодо послуги “повторне використання об’єктів” по відношенню до файлів, розміщених в зашифрованих каталогах, навіть без зреалізовування затирання інформації при вилучанні.

Віддалене адміністрування

Для підтримування можливості віддаленого адміністрування до складу ПЗ КЗЗ на робочій станції уводиться спеціальний компонент – агент АРМ віддаленого адміністрування (рис. 1.2).

Взаємодія компонентів ПЗ КЗЗ на робочий станції відбувається так, як це подано на рис. 1.2. Елементи взаємодіїї становлять запити/відповіді від/до АРМ віддаленого адміністрування: призначення прав доступу і повноважень, керуючих команд до диспетчера доступу, перевірення прав доступу, реєстрування подій, переглядання журналів аудиту.

Агент АРМ віддаленого доступу (агент АРМ ВД) забезпечує виконання таких функцій:

- приймання керувальних команд від АРМ віддаленого доступу;
- модифікування локальних баз даних відповідно до команд АРМ віддаленого адміністрування й видавання керувальних запитів диспетчерові доступу;
- передавання модифікованих баз даних та журнальних файлів на АРМ віддаленого адміністрування;
- протоколювання запитів АРМ віддаленого адміністрування та дій з виконання цих запитів.

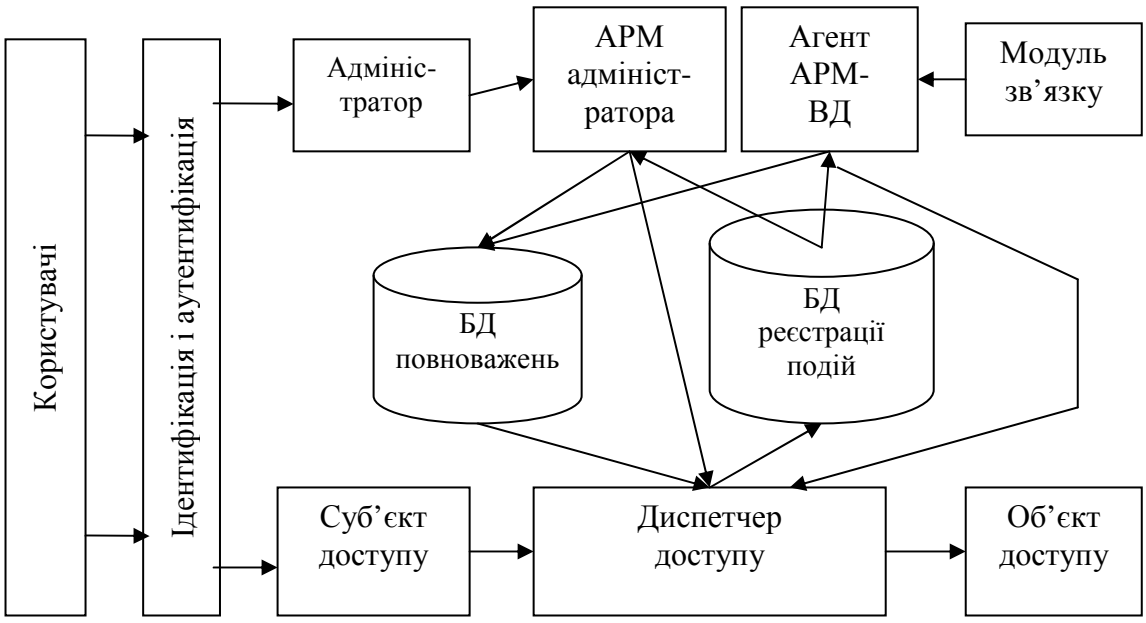

Рисунок 1.2 – Архітектура ПЗ КЗЗ на робочій станції

АРМ віддаленого адміністрування зреалізовує такі функції:

- ведення централізованої бази даних робочої станції (створення, вилучання і модифікування атрибутів робочої станції та груп робочих станцій);
- формування паспорта робочої станції у вигляді файла, необхідного для інсталяції робочої станції;
- приймання баз даних від робочих станцій та їхнє переглядання;
- одержання журнальних файлів від робочих станцій та їхнє аналізування;
- заблоковування доступу користувача до робочої станції й надавання такого доступу;
- передавання на робочу станцію керівних команд, спричинених модифікуванням атрибутів робочої станції чи заблоковуванням/дозволом доступу користувача до робочої станції;
- ідентифікування й автентифікування користувача АРМ віддаленого адміністрування;
- розмежовування обов'язків адміністраторів системи КЗЗ;
- налаштовування АРМ віддаленого адміністрування за допомогою інтерфейсу користувача.

В процесі роботи комп'ютерної мережі здійснюється синхронізація стану локальних баз даних на робочих станціях централізованої бази даних на АРМ віддаленого доступу. З метою захисту передаваної інформації від несанкціонованого модифікування й переглядання при обміні поміж АРМ віддаленого адміністрування та його агентами на робочих станціях забезпечується захищений канал.

1.1.5 Вимоги до середовища експлуатації, системи та персоналу

Вимоги до середовища експлуатації

Вимоги до середовища експлуатації мають враховуватись співробітниками, котрі відповідають за безпеку опрацьовування інформації в ПЕОМ підприємства, а також співробітниками, котрі інсталюватимуть та/чи виконувати роль адміністраторів КЗЗ від НСД.

Засоби захисту ПЕОМ від НСД, які функціонують безпосередньо в складі обчислювальної системи, є однією зі складових загальної системи заходів безпеки, яка, окрім того, включає організаційні, фізичні, а також технічні заходи безпеки.

Система заходів безпеки інформації впроваджується з метою здійснення політики безпеки інформації, ухваленої на підприємстві.

Ефективність використання КЗЗ багато в чому залежить від інших складових системи захисту інформації. Будь-яка складова системи забезпечує захист лише від певної підмножини, а не від всіх загроз, а поза системою, як правило, не може забезпечувати адекватного захисту навіть від цієї підмножини. Жоден КЗЗ не забезпечує стовідсоткового захисту від загроз безпеці інформації. Їхнє завдання – зниження ймовірності здійснення загроз.

Окрім того, для будь-якого КЗЗ існує ціла низка обмежень щодо того, як він має експлуатуватися, для того, аби можна було гарантувати, що КЗЗ дійсно здійснює свої функції й що доступ до інформації здійснюється лише під контролем КЗЗ. Дотримання даних обмежень має забезпечуватись зовнішніми стосовно КЗЗ компонентами системи захисту інформації – організаційно-технічними заходами.

Нижчерозглянуто рекомендовані організаційно-технічні заходи, котрі має бути втілено для створення середовища експлуатації КЗЗ, у якому б ефективність використання КЗЗ була максимальною. Вимоги до середовища експлуатації включають вимоги до фізичного середовища, персоналу й обчислювальної системи.

Вимоги до фізичного середовища й персоналу

Упровадження засобів захисту ПЕОМ від НСД не означає, що після цього можна відмовитися від заходів фізичної безпеки приміщення, в якому розташована захищена ПЕОМ, чи можна допускати сторонніх осіб до ПЕОМ, на якій опрацьовується критична інформація.

Головне призначення КЗЗ від НСД – забезпечувати захист від таких типових загроз:

- доступ сторонніх осіб до інформації;
- доступ сторонніх осіб до ПЕОМ;
- доступ неавторизованих, котрі не мають відповідних повноважень, користувачів до інформації;
- доступ авторизованих користувачів до інформації, в наслідок чого може мати місце витікання конфіденційної інформації чи зниження рівня її конфіденційності;
- неконтрольований доступ авторизованих користувачів до інформації;
- дії адміністраторів, які можуть призвести до встановлення параметрів налаштовування, за яких зростає ймовірність витікання інформації.

На підставі цього виокремлюються такі категорії типових порушників:

- сторонні особи, котрі потенційно можуть одержати доступ до ПЕОМ (наприклад залишеної без догляду) чи інформації (наприклад у перебігу ремонту чи викрадання);
- користувачі, які внаслідок помилок чи зумисно можуть одержати доступ до інформації, до якої вони не повинні мати доступу, чи доступ з порушуванням установлених правил, в наслідок якого може відбутися витікання інформації;
- адміністратори, котрі внаслідок помилок чи зумисно можуть надати доступ до інформації неавторизованим користувачам, чи припуститися інших помилок.

Для захисту від зазначених загроз, КЗЗ, зреалізовує функції, описані в попередніх розділах посібника. При цьому такі заходи, як організація

перепускного режиму, організація навчання користувачів, періодичні семінари для адміністраторів, дозволять ще більш підвищити безпеку інформації.

У разі, якщо на ПЕОМ опрацьовується таємна комерційна інформація, безумовно, має бути виконано всі вимоги відповідних інструкцій з організації пропускного режиму, захисту від ПЕМВН, протипожежної безпеки тощо. Усі користувачі повинні мати відповідну категорію допуску.

Вимоги до обчислювальної системи й організації робіт

Слід розуміти, що:

- якщо інформацію не зашифровао, то вона є захищена від несанкціонованого переглядання й модифікування лише в тому разі, якщо завантажено засоби захисту (драйвери, які зреалізовують розмежовування доступу);
- якщо інформацію зашифровано, то вона захищена від несанкціонованого переглядання в будь-якому разі, навіть, якщо засоби захисту й не завантажені, але від несанкціонованого модифікування вона знову ж є захищена лише в тому разі, якщо задіяно засоби захисту.

Можливість доступу до інформації поза засобами захисту розглядається як відчуження інформації від засобів захисту. Найбільш очевидним прикладом відчуження є викрадання носіїв і наступний доступ до них у середовищі ОС без засобів захисту.

В ОС Windows 95/98 існують такі можливості переривання стандартної послідовності завантаження ОС і оминання засобів захисту:

- завантаження з дискети чи CD-ROM без засобів захисту;
- покрокове завантаження з відмовленням від завантаження засобів захисту;
- часткове завантаження ОС (у режимі MS-DOS чи емуляції MS-DOS).

Для дотримання встановлених правил доступу до інформації слід вжити заходів, які гарантували б безумовне вдолучення засобів захисту до роботу. КЗЗ самостійно (за згоди адміністратора) вживає певних заходів з метою запобігання завантаженню ОС без засобів захисту (резидентну частину засобів захисту становлять драйвери реального й захищеного режимів. При цьому обов’язково має бути завантажено драйвер реального режиму):

- До файла CONFIG.SYS в перебігу інсталяції заноситься опис драйвера реального режиму. На файл встановлюється атрибут ОС “лише для читання”, а в перебігу роботи доступ за записом до файла CONFIG.SYS заблоковується засобами захисту для всіх, окрім головного адміністратора. Це дозволяє гарантувати, що з даного файла не буде вилучено рядок з описом драйвера реального режиму.
- До файла MSDOS.SYS в перебігу інсталяції заноситься рядок BootKeys = YES, що дозволяє запобігти можливості покрокового завантаження ОС та відмовляння від опрацьовування файла CONFIG.SYS шляхом вибору відповідного варіанта завантаження ОС. На файл MSDOS.SYS також

встановлюється атрибут ОС “лише для читання”, а в перебігу роботи доступ за записом до файла MSDOS.SYS заблоковується засобами захисту для всіх, окрім головного адміністратора. Це гарантує, що з файла не буде вилучено рядок BootKeys = 0.

- Додатково, аби запобігти можливості вибору варіанта завантаження, програмами ПЗУ блокується можливість використання клавіатури до завантаження драйвера реального режиму.
- Окрім того, аби запобігти можливості вибору варіанта завантаження в разі аварійного завершення попередньої спроби завантаження ОС, за ініціалізації КС3 (БД) виконується редагування файла IO.SYS. У даному файлі рядок “\WNBOOTNG.STS” замінюється на рядок “\~NBOOT-NG.STS”. Оригінал зберігається в файлі C:\-iFLY-i\ IO.BNS. У разі, якщо було виконано переінсталяцію ОС, дану операцію слід повторити.
- Аби запобігти можливості завантаження ОС з дискети чи CD-ROM, програмами ПЗУ блокується можливість читання/запису дискет до завантаження драйвера реального режиму й завантаження з CD-ROM.
- Перезавантаження в режимі емуляції MS-DOS дозволено лише для головного адміністратора. Для інших користувачів спроба входження в режим емуляції MS-DOS (з використанням пункту “Перезавантаження в режимі MS DOS” меню “Завершення роботи Windows”) завершується примусовим перезавантаженням ОС. Оскільки використання даної можливості заблоковується, то зазначений пункт меню приховується від користувачів шляхом занесення до ключа реєстру HKEY_CURENT_USER\SOFTWARE\ Microsoft\Windows\CurrentVersion\Policies\WinOldApp значення Disabled = 1. Окрім того, до цього самого ключа встановлюється значення NoRealMode = YES, яке полегшує адміністраторові можливість за необхідності заблоковувати в наступний запуск застосувань (*рос. “приложений”*) MS-DOS шляхом установлення значення NoRealMode = 1.
- При роботі в MS-DOS драйвер реального режиму заблоковує доступ до файлів, розміщених в захищених каталогах, якщо користувач не є головний адміністратор чи для нього не встановлено режим "м’якого" реагування на спроби НСД.

Установлення апаратного захисту від несанкціонованого завантаження (ПЗУ) дозволяє заблоковувати завантаження ОС з дискети чи CD-ROM і гарантувати, що в принципі одержати доступ до ПЕОМ може лише авторизований користувач.

Для виключення можливості завантаження ОС з дискети чи CD-ROM у разі виходу ПЗУ з ладу, слід вжити додаткових організаційних та технічних заходів. У якості останніх рекомендується: встановити в SETUP BIOS пароль на доступ до SETUP; установити в SETUP послідовність завантаження C:, A:.

Якщо це визнано недостатнім, то можна залишити в системі лише один НЖМД і шляхом відповідного підімкнення до контролера зробити його дисководом A:.

Обмеження доступу до SETUP BIOS дозволяє також уникнути можливості вилучання програм ПЗУ шляхом установлення певних параметрів SETUP (вікна пам'яті ПЗУ, наданої для плат ISA), що є наявні в багатьох комп'ютерах.

Небезпеку для оминання засобів захисту являє також конфігурація ПЕОМ з можливістю вибору варіанта завантаження (MultiBoot), який існує, якщо на ПЕОМ установлено декілька ОС. У такій ситуації неможливо гарантувати, що ПЕОМ не вдасться завантажити без засобів захисту.

Установлення апаратного захисту від несанкціонованого завантаження не дозволить скористатися з можливості вибору варіанта завантаження, оскільки на час завантаження заблоковується клавіатура ПЕОМ і доступним буде лише перший варіант завантаження.

Робота КСЗ без ПЗУ припускається лише на етапі налаштовування чи при відновлюванні після аварії (наприклад виході ПЗУ з ладу) і розглядається як позаштатна ситуація. Оскільки за відсутності ПЗУ існує ймовірність завантаження ОС без засобів захисту, то опрацювання критичної інформації за відсутності ПЗУ є неприпустиме.

Необхідно розуміти також, що існує можливість створювання програм, котрі дозволятимуть здобувати доступ до інформації оминаючи механізми контролю, зреалізованми засобами захисту.

Найбільш типовий приклад – програми, які безпосередньо читають інформацію з диска з використанням низкорівневих інтерфейсів введення/виведення оминаючи файловоу систему ОС. Такі дії не відстежуються КЗЗ, оскільки захищуваними об'єктами для нього є файли та каталоги.

У зв'язку з цим, рекомендується використовувати для роботи лише перевірене ПЗ, яке для доступу до інформації використовує стандартні інтерфейси ОС і не містить прихованих можливостей і закладок, а також задіювати функції КЗЗ з контролю цілісності прикладного ПЗ.

Окрім того, рекомендується також забезпечувати якамога більшу сталість програмного середовища, оскільки інсталяція нового ПЗ, а тим паче нової версії ОС, майже завжди спричинює необхідність переналаштовування засобів захисту, що зазвичай супроваджується конфліктами й помилками. Не рекомендується вести на захищеній ПЕОМ розробляння нового ПЗ.

Ще одним аспектом, від якого залежить функціонування засобів захисту, а отже й конфіденційність, цілісність та доступність інформації, є цілісність баз даних КЗЗ. КЗЗ (АРМ адміністратора) сам контролює цілісність своїх БД, однак у певних ситуаціях, наприклад за збоїв дискової підсистеми, БД (та й ПЗ) КЗЗ можуть бути попросту загублені. Єдиним способом відновлювання працездатності КЗЗ у подібній ситуації є його переінсталяція й наступне відновлювання БД з резервної копії.

Природно, що попередньо резервна копія має бути створена. АРМ адміністратора здійснює функції, які полегшують створення резервної копії БД. Порядок резервного копіювання БД КЗЗ має бути визначено особою, відповідальною за дотримання політики безпеки інформації.

Запитання для самоперевірки

1 Структура КЗЗ, зреалізованого в стандартній операційній системі (ОС) MS WINDOWS 95/98.

2 Правила розмежування доступу при роботі на спеціалізованому робочому місці з обмеженим колом користувачів, наділених різними повноваженнями з доступу до ресурсів.

3 З чого слід розпочинати входження до системи?

4 Який існує порядок завантаження ОС легальним користувачем?

5 Які засоби й методи використовуються в КЗЗ для запобігання несанкціонованому завантаженню?

6 Що відбувається за спроби несанкціонованого завантаження?

7 Які обмеження накладаються на термін чинності повноважень користувача?

8 Поясніть принципи перевіряння цілісності ПЗ КЗЗ.

9 Як здійснити змінення пароля користувача?

10 Які існують правила вибору і зберігання пароля?

11 Права доступу користувача до захищуваних каталогів.

12 Які існують обмеження при роботі із захищуваними каталогами?

13 Які є правила й обмеження при роботі зі змінними носіями і виведенням на друкування?

14 За яких умов користувачеві заборонено запускати сторонні програми?

15 У який спосіб слід виконувати заблоковування і розблоковування іінтерфейсних пристроїв комп’ютера?

16 Чому забороняється вимикати живлення комп’ютера при заблокованої клавіатури?

17 Який існує порядок коректного завершення роботи?

Завдання для самостійної роботи

Завдання адміністрування системи захисту інформації від несанкціонованого доступу та експлуатаці її користувачами ілюстровані в лабораторних роботах (Додаток А). Запитання для самоперевірки та завдання для самостійної роботи приведені у методичних вказівках до лабораторних робіт.

1.2 Системи антивірусного захисту

1.2.1 Загальні положення та означення

Комп'ютерний "вірус" – це програма, здатна створювати власні копії, необов'язково збіжні з оригіналом, та впроваджувати їх у файли, системні області комп'ютера, комп'ютерних мереж, а також чинити інші деструктивні дії. При цьому копії зберігають здатність подальшого розповсюдження. Такий паразитуючий програмний код зумовлює виконання несанкціонованих команд/програм на ураженому комп'ютері. Вірус розповсюджується у вигляді програм, файлів та макросів. Він впливає на цілісність інформації, програмне забезпечення та/чио режим роботи обчислювальної техніки, що може призвести до відмови комп'ютера, виконання ним дій, прихованих від користувача, й відповідно, до порушування цілісності та доступності інформації чи її витікання.

В області вірусології застосовують наведені нижче терміни.

З а х и с т п р о г р а м н и х з а с о б і в – організаційні, правові, технічні та технологічні засоби, спрямовані на попередження можливих несанкціонованих дій по відношенню до програмних засобів та усунення наслідків цих дій.

"П р о ф і л а к т и к а" – систематичні дії експлуатаційного персоналу, мета яких – виявляти та усувати несприятливі змінення у властивостях та характеристиках використовуваних програмних засобів, зокрема перевіряти експлуатовані, збережувані й нові отримувані програмні засоби на наявність комп'ютерних вірусів.

Р е в і з і я – перевіряння нових отриманих програм спеціальними засобами, яке провадиться шляхом їхнього запускання у контрольованому середовищі.

"В а к ц и н у в а н н я" – опрацьовування файлів, дисків, каталогів, що воно провадиться із застосовуванням спеціальних програм, які створюють умови, подібні до тих, які створюються певним комп'ютерним вірусом, і утруднює повторну його появу.

Н е с а н к ц і о н о в а н и й д о с т у п до програмних засобів – доступ до програм, записаних у пам'яті ПЕОМ чи на машинному носії, а також до відображених даних у документації на ці програми, здійснений з порушуванням встановлених правил.

Найбільш критичним до впливу вірусів чинником є працездатність автоматизованих робочих місць користувачів комп'ютерних мереж та серверного комплексу: серверів електронної пошти, серверів доменів, DNS серверів, WINS серверів, DHCP серверів, а також серверів забезпечування безпеки даних.

Ймовірними вірусними загрозами працездатності автоматизованого робочого місця можуть бути:

- ушкодження комп’ютерним вірусом файлової структури операційної системи та прикладного програмного забезпечення автоматизованого робочого місця, наприклад ушкодження файлів Microsoft Office;
- ушкодження локальної системи роботи з електронною поштою чи несанкціоноване її використання;
- знищення даних в енергонезалежній пам’яті комп’ютера (Flash BIOS, CMOS), що може призвести до відмови роботи комп’ютера.

Загрозами працездатності серверного комплексу мереж можуть бути:

- ушкодження комп’ютерним вірусом файлової структури операційної системи, прикладного та сервісного програмного забезпечення;
- порушування комп’ютерним вірусом цілісності та доступності інформації, яка зберігається та опрацьовується на серверах;
- несанкціоноване витікання інформації з комп’ютерної мережі;
- перенавантаження комп’ютера чи заблокування обчислювальних ресурсів, спричинювані діями комп’ютерного вірусу.

Причиною зараження об’єктів комп’ютерних мереж вірусами можуть бути такі джерела:

- переносні носії інформації: дискети, компакт-диски тощо;
- Інтернет, за допомогою WEB-сторінок, електронної пошти, вільно розповсюджуваного програмного забезпечення;
- суб’єкти комп’ютерної мережі: користувачі, адміністратори, розробники програмного забезпечення.

Практика свідчить, що комп’ютерні віруси наносять значних фінансових збитків. Для протистояння загрозам зараження в галузі телекомунікацій створюють системи антивірусного захисту.

Мета створення системи антивірусного захисту – забезпечування захисту робочих станцій та серверів локальних обчислювальних мереж від деструктивного впливу комп’ютерних вірусів за мінімальних видатків на адміністрування, ресурси обчислювальної техніки та телекомунікаційне устаткування.

Система антивірусного захисту має гарантувати достатній рівень захищеності від комп’ютерних вірусів, необхідний для забезпечування цілісності, доступності та спостережуваності опрацьовуваної в інформаційно-обчислювальній мережі інформації, потрібної для забезпечування життєдіяльності галузі.

Система антивірусного захисту призначена для організації та проведення обстежування, виявляння й усування комп’ютерних вірусів у програмних засобах та їхніх компонентах силами служби захисту інформації на головних етапах життєвого циклу програм: придбавання та здавання до експлуатації, архівування та власне технічної експлуатації обчислювальних мереж. Комплексна система антивірусного захисту використовується службою захисту

інформації для забезпечування інформаційної безпеки в сегментах корпоративної мережі передавання інформації, локальних обчислювальних мережах, автоматизованих робочих місцях (АРМ).

1.2.2 Функції системи антивірусного захисту на стадії здавання програм до експлуатації

На стадії придбавання та здавання до експлуатації нового програмного забезпечення система антивірусного захисту має забезпечувати спеціальне опрацьовування програмного забезпечення з метою виявляння комп'ютерних вірусів, а також усування наслідків, спричинених можливими впливами вірусів на операційні системи, системні файли та файли користувачів з програмами та даними, початкові сектори магнітних дисків, таблиці розміщення файлів тощо.

На цій стадії забезпечується виконання вимог щодо випробувань програмного забезпечення на наявність вірусів, у тому числі до:

- складу заходів з підготовлення та проведення випробувань;
- складу, структури та призначення основних частин програмно-апаратного стенда, який забезпечує проведення випробувань;
- обирання та використання методів проведення випробувань;
- тестових антивірусних програм, які виявляють та знищують віруси;
- складу та змісту документації, котра фіксує порядок проведення випробувань та їхні результати.

Випробування програмного забезпечення на наявність комп'ютерних вірусів провадять на спеціально устаткованому програмно-апаратному випробувальному стенді, в складі якого мають бути необхідні технічні та програмні засоби, у тому числі антивірусні програми.

Служба захисту інформації, яка провадить перевіряння програмного забезпечення на наявність вірусів, визначає мету та обсяг випробувань, підтримує випробувальний стенд у працездатному стані і має не припускати проникнення вірусів до програм та даних до початку проведення випробувань.

Заходи захисту перевірюваного програмного забезпечення від зараження вірусами можуть включати в себе:

- розробляння та виконання комплексу заходів з профілактики, ревізії та вакцинування використовуваних програм;
- підготовку посадових осіб, котрі відповідають за проведення випробувань програмного забезпечення;
- розробляння та вибір способів застосовування програмно-технічних засобів для виявлення вірусів у програмному забезпеченні;
- взаємодію підрозділів, які замовляють випробування, зі службою захисту інформації при проведенні випробувань програмного забезпечення;
- контроль за проведенням випробувань програмного забезпечення;
- оцінювання ефективності застосовуваних антивірусних засобів;

- вдосконалювання системи заходів із захисту програмного забезпечення від вірусів на підставі сучасних досягнень інформаційної технології;
- встановлення адміністративної відповідальності посадових осіб за виконання вимог щодо захисту програмного забезпечення від вірусів;
- призначення відповідальних посадових осіб та визначення їхніх повноважень, стосовних організації та проведення заходів із захисту програмного забезпечення від вірусів.

Служба захисту інформації має забезпечувати весь процес перевіряння необхідними обчислювальними технічними та програмними засобами, а також призначати спеціально навчених співробітників для проведення випробування. Служба захисту інформації призначає постійного представника, який отримує певні повноваження і несе постійну відповідальність за виконання вимог цих рекомендацій.

До складу технічних засобів випробувального стенда мають входити:

- сумісні ПЕОМ;
- необхідні елементи телекомунікаційних мереж;
- канали зв'язку.

Конкретний набір технічних компонентів має бути таким, аби було забезпечено умови відтворення всіх необхідних зовнішніх впливів на програмне забезпечення в перебігу проведення випробувань. До складу випробувального комплексу можуть входити відповідні апаратні антивірусні засоби:

- комп'ютери спеціальної конструкції, завдяки яким несанкціонований доступ до даних та зараження файлів вірусами може бути суттєво утруднено;
- спеціальні плати, які приєднуються до одного з рознімів ПЕОМ і виконують ті чи інші функції захисту інформації;
- електронні багатофункціональні ключі захисту інформації.

Склад та функціональне призначення програмних засобів випробувального центру визначаються системою захисту, яка застосовується при проведенні випробувань програмного забезпечення на наявність вірусів. Програмні засоби, котрі входять до складу випробувального стенду, повинні забезпечувати:

- регулярне ведення архівів змінюваних файлів;
- контрольне перевіряння відповідності довжини та значення контрольних сум, зазначених в сертифікаті та отриманих програмах;
- систематичне обнуління перших трьох байтів сектора початкового завантаження на отриманих несистемних дискетах;
- інші види контролю цілісності програм перед зчитуванням з дискети;
- перевіряння програм на наявність відомих видів комп'ютерних вірусів;

- виявляння спроб несанкціонованого доступу до випробувальних інструментальних та/чи досліджуваних програм та даних;
- вакцинації файлів, дисків, каталогів з використанням резидентних програм-вакцин, які створюють при функціонуванні умови для виявлення вірусу даного виду;
- автоконтроль цілісності програм перед їхнім запусканням;
- вилучання виявленого вірусу із заражених програм чи даних та відновлювання їхнього первинного стану;

Перевірюване програмне забезпечення має бути передане для випробувань на магнітних носіях (дискетах) разом з документацією.

Склад і послідовність робіт з підготовки та проведення випробувань програмного забезпечення на наявність вірусів у загальному разі є такі:

- ознайомлення з документацією на програмне забезпечення;
- вибір методів перевіряння на наявність вірусів;
- визначання конфігурації програмних та апаратних засобів випробувального стенда;
- підготовка програмно-апаратного випробувального стенда до проведення випробувань;
- організація та проведення випробувань;
- оформлення протоколу перевіряння програмного забезпечення;
- передавання до підрозділу-замовника перевірених програм на магнітних носіях (дискетах);
- встановлення правил (порядку) гарантійного супроводження перевірених програмних засобів.

Перевіряння на наявність вірусів у загальному разі включає:

- пошук вірусоподібних фрагментів кодів програмного забезпечення;
- моделювання ситуацій, які за припущенням здатні спричинити активізацію комп'ютерних вірусів;
- аналізування особливостей взаємодії компонентів програмного забезпечення з оточуючим операційним середовищем;
- відбиття результатів перевіряння у відповідній документації.

Документація, котра оформлюється при підготовці та проведенні випробувань програмного забезпечення на наявність вірусів, має містити відомості, які відбивали б мету, обсяг, порядок проведення та результати випробувань. Обов'язковим є документ вигляду "Протокол перевіряння програмних засобів на відсутність комп'ютерних вірусів". Документацію стосовно випробувань на наявність вірусів, може бути подано на магнітних носіях.

1.2.3 Методи проведення випробувань програмних засобів на наявність комп'ютерних вірусів

При дослідженні програмного забезпечення на наявність комп'ютерних вірусів використовують дві основні групи методів виявлення вірусів і захисту програм від них: програмні та апаратно-програмні. *До програмних методів* належать сканування; виявлення змінень; евристичне аналізування; резидентна «сторожа»; вакцинування програмного забезпечення. *Апаратно-програмні методи* базуються на здійсненні будь-яких із зазначених вище програмних методів захисту від вірусів за допомогою спеціальних технічних пристроїв. У конкретних дослідженнях може бути використано способи та засоби виявлення комп'ютерних вірусів, які зреалізовують один із розглянутих методів чи їхні комбінації.

Метод *сканування* полягає в тому, що спеціальна антивірусна програма, яка називається с к а н е р о м, послідовно переглядає перевірювані файли в пошуках так званих "сигнатур" відомих вірусів. Під с и г н а т у р о ю розуміють унікальну послідовність байтів, яка належить конкретному відомому вірусові і не зустрічається в інших програмах. Сканування є найпростішим програмним методом пошуку вірусів. Антивірусні програми-сканери можуть гарантовано виявити лише вже відомі віруси, які було вивчено і для яких було визначено сигнатуру. Антивірусні програми-сканери, які можуть вилучати виявлені віруси, називають п о л і ф а г а м и. Для ефективного використання антивірусних програм, які зреалізовують метод сканування, слід постійно оновлювати їх, отримуючи найостанні версії.

Метод *виявлення змінень* полягає в тому, що антивірусна програма спочатку запам'ятовує характеристики всіх областей диска, які може бути піддано нападові вірусів, а потім періодично перевіряє їх. Якщо змінення цих характеристик буде виявлено, то така програма повідомляє користувачеві, що, можливо до комп'ютера потрапив вірус. Метод виявлення змінень базується на використанні антивірусних програм-ревізорів, які запам'ятовують у спеціальних файлах образи головного завантажувального запису, завантажувальних секторів логічних дисків, параметри усіх контрольованих файлів, інформацію щодо структури каталогів та номери поганих кластерів диска. Може бути перевірено інші характеристики комп'ютера, обсяг встановленої оперативної пам'яті, кількість підімкнених дисків та їхні параметри.

Програми-ревізори потенційно можуть виявляти які-завгодно віруси, навіть раніше невідомі. Але слід враховувати, що не всі змінення спричиняються вторгненням вірусів. Завантажувальний запис може змінюватись при оновлянні операційної системи, певні програми записують змінювані дані всередині свого виконавчого файла. Файл AUTOEXEC.BAT може змінюватись при встановленні нового програмного забезпечення. Програми-ревізори не виявляють випадків, коли користувач записує до

комп'ютера новий файл, заражений вірусом. Але якщо вірус заразить і інші програми, вже враховані ревізором, то він буде виявлений. Є додаткова можливість програм-ревізорів щодо здатності відновлювати змінені (заражені) файли та завантажувальні сектори на підставі раніш запам'ятованої інформації. Антивірусні програми-ревізори неможливо використовувати для виявлення вірусів у файлах документів, тому що ці файли повсякчас змінюються. Для контролю таких файлів слід використовувати програми-сканери чи евристичне аналізування.

Метод *евристичного аналізування з*реалізовується за допомогою антивірусних програм, які перевіряють інші програми та завантажувальні сектори дисків та дискет, намагаючись виявити в них код, притаманний комп'ютерним вірусам.Приміром, евристичний аналізатор може виявити, що у перевірюваній програмі є наявний код, який встановлює резидентний модуль у пам'яті. Евристичне аналізування дозволяє виявляти раніше невідомі віруси. До головних недоліків евристичного методу належать:

- принципово не може бути виявлено всі віруси;
- можливі хибні сигнали щодо виявлення вірусів у програмах, які використовують вірусоподібні технології (приміром антивіруси).

У методі *резидентної сторожі* використовуються антивірусні програми, які постійно перебувають в оперативній пам'яті комп'ютера й відстежують усі підозрілі дії, виконувані іншими програмами. Резидентна сторожа повідомляє користувачеві про те, що певна програма намагається змінити завантажувальний сектор твердого диска чи дискети, а також виконуваний файл. Резидентна сторожа дозволяє автоматично перевіряти всі задіювані програми на зараження відомими вірусами. Процес завантаження програми при цьому уповільнюється. Резидентна сторожа має багато недоліків, які роблять її малопридатною до використання. Резидентна сторожа постійно перериває роботу користувача – і він кожного разу вимушений з'ясовувати, чим це спричинено: комп'ютерним вірусом чи легальною командою чи програмою. Багато програм, не заражених комп'ютерними вірусами, можуть виконувати дії, на які реагує резидентна сторожа. Окрім того, вони зменшують обсяг пам'яті, доступний для інших програм.

Вакцинування встановлює спосіб захисту будь-якої конкретної програми від вірусів, за якого до цієї програми долучається спеціальний модуль контролю, що стежить за її цілісністю. При цьому перевіряються контрольна сума програми чи певні інші її характеристики. Якщо вірус заражає вакцинований файл, модуль контролю виявляє змінення контрольної суми файла і повідомляє про це користувача. Метод вакцинування має той недолік, що є можливість оминання такого захисту за використання віруса так званої "стелс-технології". Певні програми після вакцинації можуть працювати некоректно.

Апаратно-програмні методи захисту програмного забезпечення від комп'ютерних вірусів зреалізовуються за допомогою спеціалізованого пристрою – контролера, котрий вставляється в один із рознімів розширення комп'ютера, і спеціального програмного забезпечення, яке керує роботою цього контролера і здійснює один чи декілька програмних методів, зазначених вище. Апаратно-програмні методи є найбільш надійний спосіб захисту від зараження вірусами. Контролер захисту підімкнено до системної шини комп'ютера й він повністю контролює усі звернення до дискової підсистеми комп'ютера. Програмне забезпечення апаратного захисту дозволяє зазначати області файлової системи, які заборонено змінювати.

Користувач може захистити головний завантажувальний запис, завантажувальні сектори, виконавчі файли, файли конфігурації тощо. Якщо апаратно-програмний комплекс виявить спробу порушування встановленого захисту, то він може повідомити про це і заблокувати роботу комп'ютера.

Апаратний рівень контролю за дисковою підсистемою комп'ютера не дозволяє вірусові замаскувати себе. Щойно вірус проявить себе, – його одразу ж буде виявлено. При цьому цілковито байдуже, як саме працює комп'ютерний вірус і які засоби він використовує для доступу до дисків та дискет.

Апаратно-програмні засоби захисту дозволяють не лише захищати комп'ютер від вірусів, але також вчасно попереджати виконання програм, націлених на руйнування файлової системи комп'ютера. Окрім того, апаратно-програмні засоби дозволяють захищати комп'ютер від некваліфікованого користувача, не дозволяючи йому вилучати важливу інформацію, переформатовувати дистк, змінювати файли конфігурації.

Недоліком апаратно-програмних методів є принципова можливість пропустити комп'ютерний вірус, якщо вони не здійснюють спроби змінити захищені файли та системні області.

1.2.4 Структура та функції системи антивірусного захисту на стадії технічної експлуатації інформаційно-обчислювальних мереж

Розглянемо систему антивірусного захисту, розгорнуту в корпоративній інформаційно-обчислювальній мережі галузі. Система антивірусного захисту виконує функції із захисту серверів та робочих станцій від атак комп'ютерних вірусів та перекриває найбільш імовірні варіанти проникнення вірусів до мережі. Система антивірусного захисту забезпечує:

- можливість невпинного захисту об'єктів інформаційно-обчислювальної мережі відповідно до встановлених вимог та політики безпеки;
- можливість автоматизованого блокування проникнення комп'ютерних вірусів з усіх можливих джерел;
- принципи мінімальної достатності, автоматичного функціонування та централізованого захищеного віддаленого керування антивірусним програмним забезпеченням і має доповнюватися адміністративними заходами.

Також система антивірусного захисту не повинна істотно знижувати продуктивність об’єктів інформаційно-обчислювальної мережі;

- роботу з повним набором існуючих операційних систем для серверів та робочих станцій інформаційно-обчислювальної мережі;
- “лікування” усіх відомих комп’ютерних вірусів із занесенням інформації про це у відповідні протоколи роботи для забезпечування моніторингу роботи. В разі підозри на зараження невідомими комп’ютерними вірусами та неможливості лікування забезпечується блокування доступу користувачів до цієї інформації;
- можливість оперативного повідомлення відповідальних осіб щодо виникнення критичних чи особливих ситуацій у мережі, тобто: виявлення вірусу, збої у системі оновлень, змінення налаштовувань системи антивірусного захисту. Також передбачено генерацію керувальних SNMP-послідовностей з метою візуалізації контрольованих подій у системі мережного керування;
- автоматизоване централізоване оновлення антивірусного програмного забезпечення;
- гнучке масштабування за з’явлення нових об’єктів антивірусного захисту;
- ліцензійність та підтримування постачальниками застосовуваного антивірусного програмного забезпечення.

Структурно систему антивірусного захисту зорганізовано за ієрархічним рівневим принципом. Ефективний захист від комп’ютерних вірусів забезпечується комплексною системою антивірусного захисту, котра складається з чотирьох антивірусних рівнів і передбачає встановлення антивірусного програмного забезпечення на об’єкти, які є найбільш піддавані вірусному зараженню.

На першому рівні антивірусного захисту захищається інформаційно-обчислювальна мережа шляхом встановлення первинного антивірусного шлюзу тйперевіряння усіх операцій взаємодії з глобальними мережами і, зокрема, Інтернетом. Контролюються як вхідний, так і вихідний трафіки протоколів HTTP та FTP. В разі виявлення антивірусним шлюзом комп’ютерного вірусу у трафіка, інфікована інформація блокується й чиняться дії, передбачувані шлюзовим антивірусним засобом.

На другому рівні антивірусного захисту захищаються сервери електронної пошти шляхом встановлення на них антивірусного програмного забезпечення, яке в режимі реального часу перевіряє вхідні та вихідні поштові повідомлення. В разі виявлення зараженого листа можуть надсилатися необхідні повідомлення про вірусну загрозу передбачуваним адресатам: відправникові, одержувачеві та адміністраторові. Якщо поштове повідомлення може бути вилікуване, воно добувається до місця призначення, а противному разі – воно заблоковується до з’ясування обставин. Листи електронної пошти, з

яких антивірусна програма не спрмоглася вилучити комп'ютерного віруса, може бути знищено чи спрямовано до Ізолятору.

На третьому рівні антивірусного захисту захищаються файлові сервери інформаційно-обчислювальної мережі: файлові, баз даних, та за потреби, технологічні сервери й сервери розробників програмного забезпечення. Антивірусне програмне забезпечення, встановлюване на файлові сервери, має виявляти спроби запису заражених та підозрюваних файлів на ці сервери. Інформація перевіряється в режимі реального часу в фоновому режимі чи за запитом адміністратора. Є можливість заблоковувати спроби запису заражених, підозрюваних файлів на сервери.

Кожна така спроба фіксується в протоколах та звітах антивірусної програми із зазначенням імені зараженого файла, шляху до нього. Інформацію стосовно таких спроб також може бути негайно надіслано адміністраторові антивірусної безпеки та на робочу станцію, з якої вчинено спробу запису заражених та/чи підозрюваних файлів. Ведення протоколів антивірусного захисту здійснюється централізовано, завдяки наявності утиліти мережного керування.

На технологічні комп'ютери, які за режимом не мають доступу до джерел зараження комп'ютерними вірусами, антивірусне програмне забезпечення також встановлюється, але обслуговується вручну групою антивірусного захисту.

На четвертому рівні антивірусного захисту захищаються автоматизовані робочі місця (АРМ) користувачів та комп'ютери, яких з певних причин не підімкнено до мережі. АРМ мають у своєму складі антивірусний монітор та антивірусний сканер, який здійснює перевіряння за запитом користувача чи адміністратора антивірусного захисту.

1.2.5 Організація та керування системою антивірусного захисту

Керування системою антивірусного захисту є централізованим і має трирівневу структуру:

- первинний сервер антивірусного захисту;
- сервери антивірусного захисту другого рівня;
- сервери та робочі станції користувачів.

На верхньому рівні керування розгорнуто систему моніторингу, аналізування звітів та загального керування антивірусним захистом інформаційно-обчислювальної мережі. Рівень базується на одному первинному сервері. Є, окрім того, консоль керування та моніторингу антивірусного захисту поштового сервера. Первинний сервер антивірусного захисту призначено для:

- керування антивірусним захистом серверів та робочих станцій всієї інформаційно-обчислювальної мережі;

- надавання можливості отримання файлів оновлення антивірусного програмного забезпечення серверами антивірусного захисту другого рівня;
- ведення загальної бази даних про стан всіх елементів системи антивірусного захисту інформаційно-обчислювальної мережі;
- проведення моніторингу стану антивірусного захисту та аналізування звітів.

На другому рівні керування здійснюється можливість централізованого керування всіма елементами антивірусного захисту на рівні окремих відокремлених частин (будівель) територіально розподіленої інформаційно-обчислювальної мережі. Рівень базується на так званих вторинних серверах, розташованих у відокремлених частинах мережі й пов'язаних з первинним сервером. Вторинним сервером можуть бути постійно ввімкнені робочі станції.

Вторинні сервери антивірусного захисту призначено для:

- автономного керування, в разі потреби, антивірусним захистом відповідної окремої частини інформаційно-обчислювальної мережі;
- збирання інформації в режимі реального часу та ведення бази даних про стан усіх елементів системи антивірусного захисту, розташованих у відокремленій частині інформаційно-обчислювальної мережі та підімкнених до вторинного серверу цієї частини;
- опрацьовування і щоденного передавання отриманої інформації про стан антивірусного захисту відокремленої частини інформаційно-обчислювальної мережі на центральний сервер антивірусного захисту;
- організації роботи системи оновлення вірусних баз та версій антивірусних програм від центрального сервера та надавання можливості користувачам автоматично оновлювати антивірусне програмне забезпечення на власних комп'ютерах.

На третьому рівні здійснюється безпосереднє керування антивірусним захистом окремого робочого місця користувача.

Організаційні засоби роботи системи антивірусного захисту включають розробляння інструкцій, навчання персоналу, організацію та контроль поточної роботи. Для організації роботи створюється група антивірусного захисту, яка відповідає за організаційне забезпечення завдань керування системою антивірусного захисту та здійснення контролю за її функціонуванням. Група антивірусного захисту зобов'язана:

- забезпечувати функціонування системи антивірусного захисту та контроль за виконанням її вимог;
- взаємодіяти з відповідними підрозділами супровадження інформаційно-обчислювальної мережі при визначенні налаштовувань антивірусного програмного забезпечення чи внесення до нього змінень;
- провадити моніторинг роботи антивірусних засобів захисту, та оперативно реагувати на виникнення при цьому критичних ситуацій;

- контролювати вчасне оновлювання антивірусного програмного забезпечення;
- оперативно взаємодіяти з користувачами інформаційно-обчислювальної мережі у разі виникнення ситуацій, пов'язаних з антивірусним захистом;
- погоджувати свої дії з відповідними підрозділами супровадження інформаційно-обчислювальної мережі у разі необхідного внесення змінень у роботу програмно-апаратного забезпечення автоматизованих робочих місць користувачів чи серверного устаткування, що може бути пов'язано з вірусною загрозою.

Користувачі інформаційно-обчислювальної мережі мають відповідати за дотримання вимог до системи антивірусного захисту. Користувачам забороняється вносити змінення до програмного забезпечення свого автоматизованого робочого місця, які можуть порушити вимоги щодо функціонування засобів антивірусного захисту. Користувачі інформаційно-обчислювальної мережі зобов'язані:

- дотримуватися вимог та рекомендацій щодо захисту інформації в інформаційно-обчислювальній мережі від вірусного зараження;
- повідомляти групу антивірусного захисту в разі підозри на зараження автоматизованого робочого місця комп'ютерним вірусом;
- не вносити змінень до програмно-апаратного забезпечення власних автоматизованих робочих місць без відома підрозділів, повинних забезпечувати ці функції.

Начальники підрозділів відповідають за дотримання вимог до системи антивірусного захисту співробітниками свого підрозділу.

Підрозділи супровадження інформаційно-обчислювальної мережі мають брати участь у впровадженні засобів антивірусного захисту та підтримувати відповідність складових інформаційно-обчислювальної мережі вимогам щодо системи антивірусного захисту. Ці підрозділи зобов'язані:

- забезпечувати сприяння щодо функціонування системи антивірусного захисту в інформаційно-обчислювальній мережі;
- брати участь у встановленні та підтримці працездатності антивірусного програмного забезпечення;
- попереджати групу антивірусного захисту щодо встановлення, вилучання чи внесення змінень до програмно-апаратного забезпечення автоматизованих робочих місць користувачів інформаційно-обчислювальної мережі.

1.2.6 Захист серверів та робочих станцій від зараження комп'ютерними вірусами

Захист серверів та робочих станцій можна здійснювати за допомогою Norton AntiVirus Corporate Edition. Окремі робочі станції чи групи станцій, долучених до вторинних серверів, можуть перевірятися на наявність вірусів у такі способи:

- вручну чи за запитом. Перевіряються обрані файли й теки на обраних робочих станціях:
- у реальному часі. Ця функція невпинно перевіряє на наявність відомих вірусів файли, які читаються/записуються на сервер чи робочу станцію;
- планово. Перевіряються обрані файли й теки на обраних робочих станціях запланованого часу.

Зари виявлення вірусів можуть виконуватись такі основні й резервні дії щойно після виявлення вірусу:

- *лікування інфікованого файла.* Якщо обирається даний параметр, система антивірусного захисту намагається вилікувати інфікований файл;
- *ізоляція інфікованого файла.* Якщо обирається даний параметр, система антивірусного захисту намагається перемістити інфікований файл до ізолятора інфікованої робочої станції. Внаслідок цього користувач цього файла не зможе запустити його, поки він не буде вилікуваний та переміщений назад у початкове розташування. Ізолювання небезпечних файлів запобігає подальшому поширенню вірусу. Можна заражені файли автоматично спрямовувати з робочих станцій та серверів на ізоляторний сервер без втручання користувача. Це дозволяє групі антивірусного захисту переспрямовувати заражені файли до ізольованої області на первинний сервер антивірусного захисту для вивчання;
- *вилучання зараженого файла.* Якщо обирається даний параметр, система антивірусного захисту намагається вилучати заражений файл. Даний параметр використовується лише в тому разі, якщо заражений файл можна замінити чистою резервною копією, оскільки файл вилучається назавжди;
- *залишити, як є, й надіслати повідомлення.* Якщо обирається даний параметр, система антивірусного захисту сповіщатиме про виявлення вірусу й записуватиме подію, але не виконуватиме жодних інших дій.

Система антивірусного керування має єдину консоль керування. Засобом адміністрування системи антивірусного захисту є Symantec System Center. Symantec System Center дає можливість регулювання корпоративної антивірусної політики шляхом налаштовування, переглядання та блокування конфігурацій на клієнтах і серверах, що дозволяє уникнути втручання користувачів у політику захисту інформації.

Symantec System Center складається з таких компонентів:

- консоль Symantec System Center;
- система керування сигналами.

Основні функції, виконувані з консолі *Symantec System Center:*

- створення й керування групами вторинних серверів та підімкнених до них робочих станцій та серверів;
- виявлення нових вторинних серверів та робочих станцій;
- переглядання інформації про антивірусній захист серверів та робочих станцій;
- керування подіями з сигналами попереджування;
- запускання дистанційно пошуку вірусів на серверах та робочих станціях;
- керування оновленнями.

Система керування сигналами надає можливості керування позаштатними ситуаціями. Вона дозволяє налаштовувати різні засоби попереджування про виявлені віруси, включаючи пейджер, SMS, SNMP та електронну пошту.

Для переглядання списку всіх сигналів, генерованих мережними комп'ютерами, на яких запущено модулі системи антивірусного захисту, можна використовувати журнал сигналів. Первинні та вторинні сервери зберігають власні локальні копії журналів сигналів.

Журнал вірусів містить перелік усіх виявлених вірусів для обраних робочих станцій чи груп робочих станцій. Можна обрати об'єкт у списку й виконати додаткові дії, такі як "Вилучити" чи "Ізолювати".

Журнал оглядання використовується для переглядання виконаних чи виконуваних сеансів оглядання вірусів на обраних робочих станціях чи групах робочих станцій. Можна призначити часовий діапазон для добирання записів у журналі.

Журнал подій містить решту інформації, яка не потрапила до двох попередніх категорій.

Якщо буде виявлено новий вірус, то електронною поштою одержується оновлений опис вірусів. В інформаційно-обчислювальній системі є кілька методів завантаження вірусних описів і налаштовування захищених серверів та робочих станцій для їхнього одержання:

- *Метод транспортування вірусних описів.* Цей метод можна використовувати для цілковитої автоматизації процесу оновлення вірусних описів для всіх серверів та робочих станцій системи антивірусного захисту.
- LiveUpdate. Головна перевага цього методу – у невеликому розмірі файла, який розгортається. Norton AntiVirus визначає, який вірусний опис уже розміщено на сервері чи робочій станції. Надалі запитується лише частина файла, яка містить нові дані. Для порівняння: метод транспортування вірусних описів використовує набагато більший файл, який потребує більшої смуги пропускання мережі. Первинний сервер завантажує файли описів вірусів. Потім вторинні сервери завантажують оновлення з первинного сервера для своїх робочих станцій.

- *Definition Updater.* Цей метод можна використовувати, аби легко розподілювати оновлення вірусних описів для мобільних користувачів за допомогою корпоративної електронної пошти.
- *Intelligent Updater.* Файли Intelligent Updater – це архіви, які саморозпаковуються. Вони є доступні для завантаження через Інтернет. Цей метод може використовуватися для доставляння спеціальних файлів описів вірусів.

Отже, на підприємстві зв'язку, де використовуються інформаційні технології, слід зреалізовувати *заходи щодо виявлення й запобігання проникненню вірусів* до систем та процедури інформування користувачів про їхню шкоду. Запобігання проникненню вірусам, зрозуміло, є більш раціональне, аніж ліквідація наслідків від їхнього проникнення. В основу захисту від вірусів має бути покладено знання й розуміння правил безпеки, належні засоби керування доступом до систем і наведені нижче рекомендації:

1 Підприємство має визначати формальну політику, котра вимагала б дотримання умов ліцензій на використання програмного забезпечення і забороняє використання несанкціонованих програм.

2 Антитивірусні програмні засоби, розроблені постачальником з доброю репутацією, слід використовувати в такий спосіб:

- програмні засоби виявлення конкретних вірусів мають регулярно оновлюватися й використовуватися відповідно до інструкцій постачальника. Вони застосовуються для перевіряння комп'ютерів та носіїв інформації на наявність відомих вірусів як запобіжний захід чи як повсякденна процедура;
- мають використовуватись програмні засоби виявлення змінень, внесених до даних, для виявлення змінень у виконуваних програмах;
- програмні засоби нейтралізації вірусів слід використовувати з обережністю й лише в тих випадках, коли характеристики вірусів цілковито вивчено, а наслідки від їхньої нейтралізації є передбачувані.

3 Слід провадити регулярне перевіряння програм та даних у системах, які підтримують критично важливі виробничі процеси. Наявність випадкових файлів та несанкціонованих виправлянь має бути розслідуване за допомогою формальных процедур.

4 Дискети невідомого походження перевіряють на наявність вірусів до їхнього використання.

5 Слід визначати керуванські процедури й обов'язки стосовно повідомлення про випадки зараження систем комп'ютерними вірусами і вживання заходів з ліквідації наслідків від їхнього проникнення. Слід складати належні плани забезпечування безперебійної роботи підприємства у разі випадків вірусного зараження, у тому числі плани резервного копіювання всіх необхідних даних і програм та їхнього відновлювання.

Ці заходи є особливо важливі для мережних файлових серверів, які підтримують велику кількість робочих станцій.

1.2.7 Система безпеки використання електронної пошти

Електронна пошта посідає значне місце у виробничій діяльності підприємств зв'язку. Роль електронної пошти зростатиме завдяки чинності законів України щодо цифрового підпису, електронного документообігу та електронної комерції. Електронна пошта є дешева, зручна і нескладна у використанні, має велику кількість користувачів, стала масовим сервісом та засобом спілкування.

Але електронній пошті притаманні різного роду ризики:

- перенесення вірусів, небезпечних вкладень, небезпечних мобільних кодів, команд, виконуваних за спроби читання повідомлення;
- руйнування чи перенавантаження системи;
- небажане витікання інформації й утруднене його виявлення;
- використання електронної пошти з неділовою метою.

Для ефективного використання електронної пошти, як і будь-якого іншого сервісу, потрібна ієрархічна система керування безпекою та ефективністю, яка має включати:

- керування на системотехнічному рівні: локальними мережами, поштовими серверами, серверами каталогів тощо;
- керування користувачами: їхнє реєстрування, створення адресних книг, переліків розсилання тощо;
- протидія зараженню комп'ютерними вірусами;
- забезпечування конфіденційності шляхом аналізування структури та вмісту електронних листів та оперативного реагування на виявлені порушування;
- керування інформаційними потоками: обмеження неділового трафіка, забезпечування доступності інформації, контроль процесів, ініційованих електронним листуванням.

Керування електронною поштою є засобом здійснення політики використання електронної пошти. *Політика використання електронної пошти* – це набір правил, які визначають дії за різних ситуацій. Правила містять умови та дії; умови чи критерії визначають ознаки виникнення критичних ситуацій, дії – реагування за виникнення цих ситуацій.

На підставі використання правил, умов та дій працює система моніторингу електронної пошти. За один з прикладів може слугувати система захисту поштового сервера за допомогою TrendMicro Scan Mail for MS Exchenge. Розгортання даного антивірусного засобу може відбуватися віддалено з єдиної консолі одного з поштових серверів, на якому вже встановлено TrendMicro Scan Mail for MS Exchenge.

Усіма серверами ScanMail можна керувати централізовано. Автоматично забезпечується захист у реальному часі для знову створених поштових скриньок.

Антивірусне сканування поштових повідомлень здійснюється у фоновому режимі чи вручну. У разі виявлення зараженого повідомлення відправникові,

одержувачам та адміністраторові надсилається попередження необхідного змісту електронною поштою. Користувачі не в змозі вимкнути сканування пошти, аби передати неприпустимий файл, оминаючи систему.

При скануванні використовується активний фільтр повідомлень. Адміністратор може задавати типи електронної пошти й даних, які сервер Exchange пропускатиме чи не пропускатиме за допомогою фільтра на підставі інформації в їхніх заголовках – наприклад домена, звідки відправлене повідомлення, чи вмісту полів From (Відправник), To (Кому) і Subject (Тема). Це може використовуватися для боротьби зі спамом.

Спамом називають потік небажаної незапланованої інформації до поштової скриньки. Фільтр можна використовувати для ранньої профілактики епідемій нових вірусів, задаючи ключові слова, рядок теми, розширення й імена файлів вкладень, з яких блокуватиметься проникнення заражених повідомлень на сервер Exchange.

Скануванню підлягають також стиснені й закодовані формати. Галузева система виконує сканування файлів, стиснених за допомогою схем PKZIP, ZIP2EXE, ARJ, ARJ2EXE, LHA, LHA2EXE, TAR, GZIP, LZEXE, PKLITE, DIET, MSCOMPRESS, CABINET, UNIX LZW, COMPRESS та UNIX PACK. Може бути просканово файли з декількома рівнями стиснення на глибину до 20 рівнів.

Результати роботи заносяться до журналів роботи. Журнали роботи антивірусу дозволяють відшукувати й розв’язувати проблеми антивірусного захисту поштового сервера.

Окрім антивірусного захисту, система забезпечує низку функцій моніторингу поштових повідомлень. Коли поштове повідомлення потрапляє до системи, провадиться повне розбирання листа й аналізування структури та змісту, включаючи долучені файли. Система працює й зі стисненими файлами.

Система моніторингу виконує:

- контроль відправників та одержувачів повідомлень електронної пошти;
- фільтрування повідомлень за їхнім розміром, датою, типом долучених файлів;
- визначення реального типу долучених файлів за сигнатурою, тобто за двійковим кодом. Ця функція запобігає спробам оминання системи шляхом підміни розширення файла;
- розпізнавання графічних, відео та звукових файлів. Їхня циркуляція може призвести до втрати мережних ресурсів внаслідок перенавантаження;
- аналізування змісту повідомлень на предмет наявності заборонених слів у поштових повідомленнях.

Підсистема фільтрації повідомлень базується на правилах, які складаються з набору умов та дій, виконуваних системою при задоволенні умов.

При задоволенні чи незадоволенні певних умов система виконує дію чи послідовність дій, встановлену правилами політики. Приклади дій: дозвіл чи

заборона проходження листа; його реєстрування; розміщення в архіві; надсилання повідомлення адміністраторові чи іншому користувачеві у мережі.

Короткотермінове та довготривале архівування поштових повідомлень має суттєве значення для аналізування змісту за різними системними критеріями, які можуть задаватись адміністратором системи.

Запитання для самоперевірки

1 Поясніть термін “комп’ютерний вірус” та інші терміни, застосовувані у вірусології.

2 Перелічіть імовірні вірусні загрози.

3 Призначення системи антивірусного захисту.

4 Функції системи антивірусного захисту на стадії здавання програм до експлуатації.

5 Наведіть склад та функції технічних та програмних засобів випробувального антивірусного стенда.

6 Поясніть послідовність робіт з підготовки та проведення випробувань програмного забезпечення на наявність вірусів.

7 Наведіть перелік методів проведення випробувань програмних засобів на наявність комп’ютерних вірусів.

8 Поясніть принципи дії, переваги й недоліки програмних методів антивірусного захисту: сканування, виявлення змінень, евристичного аналізування, резидентної «сторожі», вакцинування програмного забезпечення.

9 Поясніть принципи антивірусного захисту за допомогою спеціальних технічних пристроїв.

10 Система безпеки використання електронної пошти.

11 Поясніть роль та функції моніторингу поштових повідомлень.

12 Заходи для виявлення й запобігання проникненню вірусів до систем.

Завдання для самостійної роботи

1 Розробити посадові інструкції для відповідальних за антивірусний захист.

2 Скласти план робіт перевіряння програмних засобів на відсутність комп’ютерних вірусів на стадії приймання до експлуатації.

Інші завдання для самостійної роботи дивіться в лабораторній роботі № 4 (додаток А).

1.3 Методичні вказівки до виконання лабораторних робіт

У цьому розділі забезпечується здобуття знань і умінь виявлення та блокування витоку інформації технічними каналами. Професійні компетенції цього циклу передбачають уміння:

- кваліфіковано аналізувати інформацію, надану технічними системами, з метою виявлення типових ознак можливого несанкціонованого доступу;
- уміти зафіксувати інформацію з додержання чи порушення заходів об'єктового контролю у відповідних реєстраційних документах;

розробляти план використання наявних технічних пристроїв (прийомів або процедур) для закриття можливих каналів витоку інформації обмеженого доступу;

- проводити атестацію режимних територій в умовах додержання режиму секретності із за фіксуванням результатів у відповідних документах;
- розробляти узагальнений перелік потрібних технічних засобів;
- використовувати технічні засоби захисту інформації в умовах забезпечення режиму секретності на підприємствах, в організаціях та установах різних форм власності, уміти провести дії щодо організації технічного захисту інформації, зокрема приймати рішення про додержання чи наявність факту порушення конфіденційності інформації обмеженого доступу;
- розробляти номенклатурний перелік технічних засобів захисту інформації від витоку технічними каналами та реалізовувати технічні заходи закриття можливих каналів витоку інформації (за переліком каналів витоку);
- оцінювати ефективність систем захисту.

Лабораторна робота № 1. Структура й функції системи захисту інформації від НСД

1 Мета роботи

Вивчення структури та функцій комплексу засобів захисту (КЗЗ) інформації, опрацьовуваної на ПЕОМ, від несанкціонованого доступу (НСД), зреалізованого в стандартній операційній системі MS WINDOWS 95/98.

2 Ключові положення

Комплекс засобів захисту інформації, опрацьовуваної на ПЕОМ, від НСД є спеціалізованою надбудовою над стандартною операційною системою (ОС) MS Windows 95/98 і доповнює її функціями розмежування доступу. Комплекс дозволяє створювати спеціалізоване робоче місце з обмеженим колом користувачів, які мають різні повноваження з доступу.

Комплекс орієнтовано на використання в організаціях для захисту конфіденційності та цілісності критичної інформації, опрацьовуваної на персональному комп'ютері в середовищі ОС MS Windows 95/98.

Програмні засоби КЗЗ є сумісні із засобами, які входять до комплекту постачання ОС, а також з іншим системним, інструментальним та прикладним ПЗ, яке використовує стандартні інтерфейси ОС.

Програмні засоби КЗЗ **можуть бути несумісні** з іншими засобами захисту від НСД, антивірусним ПЗ та з ПЗ, яке працює з дисками й файлами на низькому рівні поза файловою системою.

Функції, структура й принципи захисту інформації від НСД описано у підрозділах 1.1.3, 1.1.5 даного посібника.

2.1 Структура та вміст каталогів комплексу засобів захисту

Файлова система комплексу засобів захисту (КЗЗ) складається з головного каталогу C:\--FLY--\ та каталогів:

BASE\ – каталог бази даних;

BIN\ – каталог виконуваних файлів;

JRN\ – каталог журнальних файлів;

HELP\ – каталог документації та файлів контекстної допомоги;

TMP – каталог для тимчасових файлів.

У головному каталозі C:\--FLY--\ розміщуються протокол інсталяції Install.log та програма деінсталяції Unwise.exe.

У підкаталозі BIN\ розміщують виконувані файли, динамічні бібліотеки, файли ліцензій та конфігурації. Основні його файли такі:

Fly95.lic – "файл ліцензії" – містить контрольні суми інших файлів КЗЗ;

Flydos.sys – допоміжний системний драйвер реального режиму;

Fly95adm.exe – VxD драйвер захищеного режиму. Це ядро КЗЗ, який виконує всі функції із розмежування доступу;

Fly95adm.exe – автоматизоване робоче місце (АРМ) адміністратора;

Fly95adm.ini – файл конфігурації АРМ адміністратора, який містить надбудови, котрі визначають конкретну політику безпеки. Типовий вміст цього файлу є такий:

[DIRS]

BaseDir=C:\--FLY--\BASE\

[COMON]

System = Grif – назва;

Version = 1.1 – версія;

FlawControl = ON – контроль за вихідними потоками;

Encryption = OFF – шифрування файлів у захищених каталогах;

WipeType = Name – затирання файлів та їхніх типів при вилучанні;

InpExpControl =ON – контроль імпортування/експортування;

ScreenSaver = ON – блокування пристроїв введення/виведення;

SWControl = Dynamic – контроль цілісності програмного забезпечення при запусканні;

Remote Access = ON – контроль за віддаленим доступом;

AdminRestrict = Main – політика обмеження повноважень адміністраторів:

Main – заборона для головного адміністратора на керування БД захищених каталогів та доступу до конфіденційної інформації;

All – заборона для всіх адміністраторів, окрім головного, на редагування атрибутів інших адміністраторів та надавання адміністративних повноважень звичайним користувачам;

Add – накладання всіх заборон.

TmpAdmin = ON – запуск АРМ адміністратора не тим користувачем, який завантажив ОС;

TMType = ICT – тип пристрою зчитування ідентифікаторів Touch Memory:

ICT – плата ІКТ;

LPT – паралельний порт;

COM2 – послідовний порт.

Цей файл конфігурації редагувати забороняється. Редагування призведе до порушування цілісності та заблокування подальшої роботи.

LogView.dll – динамічна бібліотека переглядання журнальних файлів;

Etalon.dll – динамічна бібліотека роботи з еталоном програмного забезпечення.

C4ASCX.DLL, C4PRLIBX.DLL, C4RUNX.DLL,C4TPSX.DLL – стандартні динамічні бібліотеки СУБД Clarion.

Дані файли становлять програмну частину КЗЗ й їхня цілісність контролюється КЗЗ.

У підкаталозі BASE\ розміщуються бази даних КЗЗ. Їхній склад є такий:

PQA.CSP – файл початкових параметрів;

TCB_DB.TRS, TSB_DB – початкова та робоча копії БД робочого місця;

USER_DB.TRS, USER.DB – початкова та робоча копії БД користувачів;

PD_DB.TRS, PD_DB – початкова та робоча копії БД захищених каталогів;

SW_DB.TRS, SW_DB – початкова та робочі копії БД програмного забезпечення;

MESCOD.TRS, MESFUNC.TRS, MESSUBF.TRS – БД кодів повідомлень для переглядання журнальних файлів;

ARMADMDB.IMM – файл контрольних сум TRS файлів.

Всі операції із встановлення, зняття та налаштовування КЗЗ виконуються за допомогою програми Fly95adm.exe адміністраторами, які мають відповідні повноваження.

3 Лабораторне устаткування

Комплекс засобів захисту встановлено на IBM-сумісній ПЕОМ у стандартній операційній системі MS WINDOWS 95/98 і складається з програмної, апаратної та ключової систем.

Програмне забезпечення складається з резидентної й нерезидентної частин. До складу програмних засобів КЗЗ від НСД входять системні драйвери реального (FLYDOS.SYS) й захищеного (BARVXD.VXD) режимів, які виконують функції розмежування доступу, програма автоматизованого

робочого місця (АРМ) адміністратора FLY95ADM.EXE, а також низка додаткових службових утиліт та динамічних бібліотек.

До апаратної частини належить ПЗУ з мікропрограмами рівня розширення BIOS, встановлене на спеціальній чи мережній платі. Частину програмних засобів КЗЗ, який зреалізовує функції ідентифікування й автентифікування користувача, зреалізовано як розширення BIOS і розміщено в мікросхемі ПЗУ. Для встановлення мікросхеми ПЗУ в (E)ISA-слот материнської плати ПЕОМ може використовуватись плата, на якій є місце під мікросхему ПЗУ, інтерфейс з ідентифікаторами Touch Memory та генератор випадкових чисел, а також мережна плата з місцем під ПЗУ віддаленого завантаження.

Ключова система являє собою спеціальний пристрій – ідентифікатор Touch Memory чи дискету, на якій записуються ідентифікаційні дані користувача. У разі використання ідентифікаторів Touch Memory потрібен пристрій зчитування для цих ідентифікаторів.

4 Порядок підготовки й виконання роботи

Підготовка до проведення роботи

1 Визначити призначення та ознайомитись зі структурою й функціями КЗЗ від НСД, зреалізованої в стандартній операційній системі MS WINDOWS 95/98, користуючись даним посібником (підрозд. 1.1.3, 1.1.5).

2 Визначити область застосовування КЗЗ від НСД і ознайомитись з політикою безпеки (підрозд. 1.1.2 даного посібника), зреалізованого за допомогою цього комплексу.

3 З’ясувати, який функціональний профіль захисту й які вимоги рівня гарантій зреалізовано КЗЗ від НСД.

Виконання роботи

4 Виконати завантаження системи, використовуючи ім’я головного адміністратора, пароль і ключову дискету. Простежити процедури ідентифікування/автентифікування користувача.

5 Ознайомитись з порядком контролю цілісності КЗЗ. Запустити програму адміністрування й виконати тестування системи.

6 Ознайомитись з порядком і цілями контролю цілісності використовуваного програмного забезпечення.

7 Вивчити принципи адміністративного розмежування доступу.

8 Вивчити призначення та зміст БД захищуваних каталогів, що, і списків доступу.

9 Створити пробний захищений каталог. Перевірити виконання режиму доступу.

10 Ознайомитись з принципами керування потоками інформації.

11 З’ясувати, як у системі зреалізовано послугу “повторне використання об’єктів”.

12 З’ясувати вимоги до середовища експлуатації, необхідні для ефективного функціонування КЗЗ.

13 З’ясувати вимоги до фізичного середовища й персоналу. Визначити загрози інформації й типових порушників.

14 Сформулювати вимоги до обчислювальної системи й організації робіт.

15 З’ясувати заходи із запобігання завантаженню ОС без засобів захисту:

- переконатись, що до файла CONFIG.SYS в перебігу інсталяції занесено опис драйвера реального режиму, що на файл встановлено атрибут ОС “лише для читання” і що в перебігу роботи доступ із запису до файла CONFIG.SYS блокується засобами захисту для всіх, окрім головного адміністратора;

- переконатись, що до файла MSDOS.SYS в перебігу інсталяції занесено рядок BootKeys = YES, що дозволяє запобігти можливості покрокового завантаження ОС й відмови від опрацьовування файла CONFIG.SYS шляхом вибору відповідного варіанта завантаження ОС. Переконатись, що на файлі MSDOS.SYS встановлено атрибут ОС “лише для читання”, а в перебігу роботи доступ із запису до файла MSDOS.SYS блокується засобами захисту для всіх, окрім головного адміністратора;

- переконатись, що програмами ПЗУ блокується можливість використання клавіатури до завантаження драйвера реального режиму, для запобігання вибору варіанта завантаження;

- переконатись, що за ініціалізації КЗЗ (БД) виконується редагування файла IO.SYS, аби запобігти можливості вибору варіанта завантаження у разі аварійного завершення попередньої спроби завантаження ОС;

- переконатись, що програмами ПЗУ блокується можливість читання/записування дискет до завантаження драйвера реального режиму й завантаження з CD-ROM, аби запобігти можливості завантаження ОС з дискети чи CD-ROM.

16 Скласти список необхідних налаштовувань КЗЗ.

17 Визначити, які існують шляхи оминання засобів захисту і способи їхнього нейтралізування.

18 Визначити, у який спосіб запобігається копіювання конфіденційної інформації у відкриті каталоги й несанкціоноване здобуття конфіденційної інформації шляхом “збирання сміття”.

5 Ключові запитання

1 Структура й функції КЗЗ, зреалізованого в стандартній операційній системі MS WINDOWS 95/98.

2 Правила й принципи ідентифікування й автентифікування користувача. Роль додаткових пристроїв у перебігу автентифікування користувача.

3 Які засоби й методи використовуються в КЗЗ для запобігання несанкціонованому завантаженню?

4 Як здійснюється контроль цілісності КЗЗ та тестування?

5 Як провадиться і в чому полягають цілі контролю цілісності використовуваного програмного забезпечення?

6 Які принципи адміністративного розмежування доступу до ресурсів, що захищаються?

7 Призначення і склад БД захищених каталогів. Зміст списків доступу.

8 Які обмеження накладаються на створення захищених каталогів?

9 Процес створення спробного захищеного каталогу. Як перевіряти дотримання режиму доступу до нього?

10 Права доступу користувача до захищених каталогів.

11 Які існують обмеження при роботі із захищеними каталогами?

12 В чому полягає і як підтримується керування потоками інформації?

13 Хто має право доступу до файлів налаштовування ОС за записом?

14 Як у системі зреалізовано послугу “повторне використання об’єктів”? Який використовується давач випадкових чисел для цього?

15 Які треба виконувати вимоги до середовища експлуатації, необхідні для ефективного функціонування КЗЗ від НСД?

16 Від чого залежить і чим визначається ефективність функціонування КЗЗ від НСД?

17 Які вимоги пред’являються до фізичного середовища й персоналу?

18 Наведіть перелік загроз інформації.

19 Визначте типових порушників.

20 Які існують шляхи оминання засобів захисту і як їх знейтралізовувати?

21 Які заходи дозволяють гарантувати, що з файлів CONFIG.SYS і MSDOS.SYS не буде вилучено рядки налаштовувань? Які це рядки?

22 Чому КЗЗ не повинен працювати без ПЗУ?

23 Чому не можна використовувати на захищеному робочому місці неперевірене ПЗ?

24 Хто визначає порядок резервного копіювання БД КЗЗ?

Лабораторна робота № 2. Адміністрування системи захисту інформації від НСД

1 Мета роботи.

Набуття навичок адміністрування комплексу засобів захисту (КЗЗ) інформації, опрацьовуваної на ПЕОМ, від несанкціонованого доступу (НСД). Вивчення функціонування КЗЗ, зреалізованого в стандартній операційній системі (ОС) MS WINDOWS 95/98. Знайомство з функціями адміністратора безпеки й організацією захисту інформації на спеціалізованому робочому місці з обмеженим колом користувачів, котрим надано різні повноваження з доступу до ресурсів.

2 Ключові положення.

2.1 Початкові дані про систему.

КЗЗ інформації від НСД інстальовано в ОС MS WINDOWS 95/98. В перебігу інсталяції було зроблено реєстрування Головного адміністратора, через дисковод A: на чисту дискету було записано його ідентифікатор та пароль для входження адміністратора в систему. Нагадаємо, що мінімальна довжина пароля – 6 символів. Припускається використання латинських літер, цифр і спеціальних символів. Будь-які три символи пароля, що слідують один за одним, не повинні повторюватися та/чи відрізнятися на одиницю.

За замовчуванням ім'я головного адміністратора ***"admin"*** (без лапок на нижньому регістрі). Після реєстрування Головного адміністратора було прийнято значення налаштовувань КЗЗ, пропоновані за замовчуванням.

У вільний слот материнської плати комп'ютера вставлено плату з мікросхемою ПЗУ, що входить до комплекту постачання.

Робота КЗЗ без ПЗУ припускається лише на етапі налаштовування чи при відновлюванні після аварії (наприклад за виходу ПЗУ з ладу) і розглядається як позаштатна ситуація. Оскільки за відсутності ПЗУ існує ймовірність завантаження ОС без засобів захисту, то опрацювання критичної інформації за відсутності ПЗУ є неприпустиме.

2.2 Порядок завантаження системи

У перебігу завантаження системи адміністратор має переконатись, що в цей час не виникає жодних конфліктів, і що програми ПЗУ включено до роботи.

У відповідь на запити КЗЗ слід увести свої ім'я й пароль. У перебігу введення імені й пароля неодмінне є дотримування регістра при введенні всіх символів. У разі помилки використовуються клавіші <*Esc*> чи <*Backspace*>, що призведе до повторного видавання запиту. Введення імені й пароля завершується натисканням клавіші <*Enter*>. Наприклад:

Username > *admin*

Password > ******

Після повідомлення

Insert ID device and press <*Enter*> *when ready*

вставити в дисковод А: дискету з ідентифікатором і натиснути клавішу *<Enter>*.

Аби переконатися, що програми ПЗУ включено до роботи, слід простежити за з'явленням запиту імені й пароля користувача до видання повідомлення "*Завантаження Windows"* чи "*Starting Windows"*.

2.3 Реєстрування додаткових користувачів

Для реєстрування додаткових користувачів виконуються такі дії:

- завантажується АРМ адміністратора;
- викликається діалог роботи з БД користувачів за допомогою іконки на панелі інструментів чи пункт меню "Користувачі/Облікові записи";
- вводиться ім'я користувача й задаються інші необхідні атрибути;
- зберігається введений запис;
- вставляється новий ідентифікатор у пристрій читання (дискету в дисковод А:), вводиться й отверджується пароль користувача.

При цьому рекомендовано таке:

- *Не можна використовувати один і той самий ідентифікатор для різних користувачів;*
- для роботи із захищеними каталогами потрібен хоча б один адміністратор, окрім головного, котрий мав би повноваження роботи з БД захищених каталогів і допуск "ТАЄМНО";
- на етапі налаштовування КЗЗ для користувачів рекомендується встановлювати "м'який режим" реагування на НСД, що згодом при переході до штатної роботи слід заборонити;
- не слід встановлювати надто докладне реєстрування подій, оскільки тоді журнальні файли КЗЗ займатимуть вельми багато місця на диску;
- допуск інших користувачів слід задавати відповідно до рівня конфіденційності інформації, до якої вони потенційно можуть мати доступ.

2.4 Створення пробного захищеного каталогу.

- Для створення пробного захищеного каталогу слід виконати таке:
- завантажити АРМ адміністратора з повноваженнями користувача, який має повноваження роботи з БД захищених каталогів;
- викликати діалог роботи з БД захищених каталогів, використовуючи іконку на панелі інструментів чи пункт меню "Каталоги". Обрати в дереві каталогів гілку "ДСП" чи "ТАЄМНО" і натиснути кнопку "Створити";
- обрати ім'я каталога й натиснути кнопку "Зберегти". Як защищуваний каталог не можна обирати кореневий каталог диска;
- натиснути кнопку "Користувачі" й задати користувачів, котрі мають права доступу до даного каталогу, і вид доступу (лише читання чи читання/запис).

2.5 Встановлення необхідних налаштовувань КЗЗ.

- Для встановлення налаштовувань КЗЗ виконуються такі дії:
- завантажується АРМ адміністратора з повноваженнями головного адміністратора;
- викликається діалог “Налаштовування системи” за допомогою пункту меню “Система/Налаштовування”. Обирається закладка “Ресурси”;
- для заблоковування можливості копіювання конфіденційної інформації у відкриті каталоги встановлюється прапорець “Контроль вихідних потоків”;
- для заблоковування можливості несанкціонованого здобуття конфіденційної інформації шляхом “збирання сміття” встановлюється прапорець “Затирати вміст файлів при вилучанні” й “Затирати імена файлів при вилучанні”. Використання даної функції сповільнює процес вилучання файлів у захищених каталогах і унеможливлює їхнє відновлювання за випадкового вилучання.

2.6 Встановлення режиму контролю цілісності ПЗ.

Для встановлення режиму контролю цілісності ПЗ виконується таке:

- вилучається з дисків зайве ПЗ;
- завантажується АРМ адміністратора з повноваженнями головного адміністратора;
- викликається діалог роботи з БД захищених каталогів за допомогою іконки на панелі інструментів чи пункт меню “Програми” й натискається кнопка “Реєстрація”;
- у діалозі “Майстер реєстрації” у лівому верхньому списку каталогів обирається кореневий каталог диска С. Натискається кнопка [”], розташована праворуч від дерева каталогів. У правому вікні з’явиться список програмних модулів, знайдених на диску. Встановлюється праворуч угорі перелік контрольованих параметрів і натискається кнопка “Зареєструвати!”. Слід враховувати, що дана операція може виконуватись тривалий час (десятки хвилин), особливо якщо задано необхідність контролю цілісності коду програмних модулів;
- операція повторюється для всіх логічних дисків;
- викликається діалог “Налаштовування системи за допомогою пункту меню “Система/Налаштовування”, обирається закладка “Ресурси” і встановлюється прапорець “Контролювати цілісність ПЗ при запусканні”.

2.7 Моделювання планованої технології роботи

Для моделювання планованої технології роботи контролюють роботу КЗЗ за журналами. Для цього:

- завантажте АРМ адміністратора з повноваженнями головного адміністратора;

- викличте діалог роботи з БД захищених каталогів за допомогою іконки на панелі інструментів чи пункт меню “Журнали”;
- оберіть у списку журнал за потрібну дату й натисніть кнопку “Переглядання”;
- перегляньте журнал. Повідомлення про НСД позначаються червоними іконками зі знаком оклику чи зірочкою (синіми, якщо встановлено “м’який режим”).

У разі виникнення конфліктів та/чи повідомлень про спроби НСД установіть коректні налаштовування КЗЗ, права доступу користувачів, їхні повноваження тощо.

Після того як буде випробувано технологі. роботи й визначено необхідні налаштовування КЗЗ і права доступу користувачів, можете розпочинати працювати з реальною інформацією. Не забудьте вимкнути для користувачів “м’який режим” реагування на НСД.

3 Лабораторне устаткування

КЗЗ встановлено на IBM-сумісній ПЕОМ у стандартній операційній системі MS WINDOWS 95/98 і складається з апаратної, програмної та ключової систем. До апаратної частини належить ПЗУ з мікропрограмами рівня BIOS, встановлене на спеціальній чи мережній платі. Програмне забезпечення складається з резидентної й нерезидентної частин. Ключова система являє собою спеціальний пристрій чи дискету, на якій записуються ідентифікаційні дані користувача.

4 Порядок підготовки й виконання роботи

Підготовка до проведення роботи

1 Повторити структуру й функції КЗЗ від НСД, зреалізованого в стандартній операційній системі MS WINDOWS 95/98.

2 Визначити й спланувати технологію роботи на спеціалізованому робочому місці з обмеженим колом користувачів, яких наділено різними повноваженнями з доступу до ресурсів.

3 З’ясувати, які засоби й методи використовуються в КЗЗ для запобігання несанкціонованому завантаженню.

Виконання роботи

4 Завантажити систему, використовуючи ім’я головного адміністратора, пароль і ключову дискету.

5 Зареєструвати додаткових користувачів. З’ясувати вимоги до реєстрування.

6 Створити спробний захищений каталог. Перевірити виконання режиму доступу до нього.

7 Скласти список необхідних налаштовувань КЗЗ. Установити необхідні налаштовування КЗЗ.

8 Визначити, у який спосіб запобігають копіюванню конфіденційної інформації у відкриті каталоги й несанкціоноване здобуття конфіденційної інформації шляхом “збирання сміття”.

9 Установіть режим контролю цілісності ПЗ.

10 Промоделюйте плановану технологію роботи.

5 Ключові запитання

1 Структура й функції КЗЗ, зреалізованого в стандартній операційній системі MS WINDOWS 95/98.

2 Правила завантажування системи.

3 Як переконатись у правильності завантаження КЗЗ?

4 Які засоби й методи використовуються в КЗЗ для запобігання несанкціонованому завантаженню?

5 Як провадиться і які існують вимоги щодо реєстрування додаткових користувачів?

6 Процес створення спробного захищеного каталогу. Як перевіряти додержання режиму доступу до нього?

7 Права доступу користувача до захищених каталогів.

8 Які існують обмеження при роботі із захищеними каталогами?

9 Як установити необхідні налаштовування КЗЗ?

10 Які налаштовування КЗЗ є необхідні відповідно до політики безпеки?

11 Як запобігти можливості копіювання конфіденційної інформації у відкриті каталоги й можливості несанкціонованого здобуття конфіденційної інформації шляхом “збирання сміття”?

12 Як установити режим контролю цілісності ПЗ?

13 Пояснити принципи контролю цілісності ПЗ КЗЗ.

14 У який спосіб здійснити коректне завершення роботи і перемкнути систему до режиму роботи з реальною інформацією?

15 Чому при роботі з реальною інформацією потрібно вилучати “М’який режим” реагування на НСД?

Лабораторна робота № 3. Експлуатація системи захисту інформації від НСД

1 Мета роботи.

Набуття навичок експлуатації комплексу засобів захисту (КЗЗ) інформації, опрацьовуваної на ПЕОМ, від несанкціонованого доступу (НСД). Вивчення функціонування системи розмежування доступу в КЗЗ, зреалізованого у стандартній операційній системі (ОС) MS WINDOWS 95/98. Знайомство з порядком захисту інформації при роботі на спеціалізованому робочому місці з обмеженим колом користувачів, яких наділено різними повноваженнями з доступу до ресурсів.

2 Ключові положення.

2.1 Загальні відомості

В основному, робота користувача на ПЕОМ у захищеному середовищі провадиться так само, як на звичайній. Проблемами захисту на спеціалізованому робочому місці займається адміністратор. При цьому користувачеві слід чітко слідувати його вказівкам. Адміністратор має проінструктувати користувача про встановлені правила роботи, права користувача, обов'язки й обмеження.

У свою чергу, про всі помічені відхилення від штатної роботи (відсутність чи поява незрозумілих повідомлень, особливо в процесі завантажування, змінення поводження системи при доступі до захищених каталогів тощо) користувач зобов'язаний негайно повідомляти адміністраторові.

2.2 Входження до системи

Процес входження до системи має розпочинатись із ввімкнення живлення чи перезавантаження ОС (гарячого чи холодного). Якщо користувач, підійшовши до ПЕОМ, бачить, що ще не завершено попередній сеанс роботи, його слід завершити неодмінно. Якщо користувач, підійшовши до ПЕОМ, бачить на екрані запит імені й пароля, йому не слід покладатися на те, що це запити засобів захисту, а обов'язково перезавантажити ПЕОМ.

2.3 Завантаження ОС легітимним користувачем

При завантаженні ОС засоби захисту здійснюють ідентифікування й автентифікування користувача. Для цього користувача просять ввести ім'я (псевдонім — username) і пароль (password), а також пред'явити ідентифікатор, що носиться – ідентифікатор Touch Memory або, у нашому разі, ключову дискету. Ідентифікатор, що носиться, а також пароль для першого входження до системи користувачеві надає адміністратор.

Завантаження ОС відбувається в такий спосіб. При ввімкненні живлення, холодному чи гарячому перезавантаженню перед завантаженням ОС надсилається запит "Username >", у відповідь на який слід ввести ім'я користувача. У перебігу введення імені (й пароля) обов'язковє дотримання регістра при введенні всіх символів. У разі помилки користувач має натиснути

клавішу <*Esc*> *чи* <*Backspace*>, що призведе до повторного видання запиту. Введення імені завершується натисканням клавіші <*Enter*>. Після цього надсилається наступний запит – "Password >", у відповідь на який користувач повинен увести свій пароль. Початковий пароль надається адміністратором при реєструванні користувача й має бути змінений користувачем при першому ж входженні до системи. При введенні пароля на екрані замість символів, що вводяться, відбиваються "зірочки". Введення пароля також завершується натисканням клавіші <*Enter*>. Після введення пароля надсилається повідомлення "*Insert ID device and press* <*Enter*> *when ready",* у відповідь на яке слід вввести ідентифікатор до зчитувача. Якщо за носимий ідентифікатор користувач використовує ключову дискету, то він вставляє її в дисковод *A:*, якщо ідентифікатор Touch Memory – то у зчитувач, після чого натискає клавішу <*Enter*>. Після цього здійснюється пошук ідентифікаторів (у такому порядку: Touch Memory, дискета) й читання першого відзнайденого ідентифікатора.

Приклад діалогу при входженні до системи наведено нижче.

Username > *admin*

Password > ******

Insert ID device and press <*Enter*> *when ready*

..... Search for TM .....

У разі введення коректної інформації на короткий час надсилається (користувач його навіть не помічає) повідомлення "Access *granted"* (доступ дозволено) – і процес завантаження системи триває.

У перебігу подальшого завантаження відбувається таке:

- надсилається повідомлення *ОС "Starting Windows";*
- здійснюється опрацювання файла CONFIG.SYS, при цьому надсилаються діагностичні повідомлення "*IKT-ROM Present"* (ПЗУ КЗЗ є присутнім), вітання "<*username*>*, you welcome"* (Користувач такий-то, завжди Вам раді) і "*Device FLYDOS loaded"* (Драйвер КЗЗ завантажено);
- здійснюється опрацювання файла AUTOEXEC.BAT (якщо він є).

Якщо апаратний захист від несанкціонованого завантаження (НЗЗ) не встановлено, то ідентифікування й автентифікування користувача здійснюються драйвером FLYDOS.SYS – після повідомлення "*IKT-ROM absent"* (ПЗУ відсутній) видаються запити імені й пароля. Однак, подальше завантаження відбувається лише в тому разі, якщо користувач має привілей "Завантаження без ПЗУ", а до ЖФ буде внесено відповідний запис про НСД. Про дану ситуацію слід довести до відома адміністратора КЗЗ.

Робота КЗЗ без *ПЗУ розглядається як позаштатна ситуація. Опрацювання критичної інформації за відсутності ПЗУ є неприпустиме. У разі видання системою повідомлень про відсутність ПЗУ – користувач повинен негайно довести це до відома адміністратора.*

2.4 Спроби несанкціонованого завантаження

У разі повторення більш двох разів некоректного введення імені чи пароля користувача, чи пред'явлення підробленого ідентифікатора видається

повідомлення “*Access denied. System halted”* (Доступ заборонено. Зупин системи) – і здійснюється зупин системи (завантаження припиняється).

2.5 Перевіряння терміну чинності повноважень

Коли адміністратор реєструє користувача в системі, він задає термін закінчення чинності його повноважень і пароля. Коли користувач змінює свій пароль, термін закінчення чинності пароля встановлюється автоматично (за замовчуванням — три місяці).

У перебігу завантаження КЗЗ порівнює поточну дату з датами закінчення терміну чинності пароля і повноважень, і за сім днів до закінчення терміну чинності попереджає про це, видаючи відповідно повідомлення “*Your account is about to expirate. Call admin”* (Термін чинності Вашого облікового запису минає. Зверніться до адміністратора) чи “*Your password is about to expirate. Change it”* (Термін чинності Вашого пароля минає. Замініть його). У першому випадку користувачеві слід звернутися до адміністратора, а в другому – замінити пароль.

Якщо термін чинності повноважень чи пароля минув, то буде видане повідомлення “*Your account is expirate. Access denied. System halted”* (Термін чинності Вашого облікового запису минув. Доступ заборонено. Зупин системи) чи “*Your password is expirate. Access denied. System halted”* (Термін чинності Вашого пароля минув. Доступ заборонено. Зупин системи), відповідно, – і користувач не зможе ввійти до системи. У цьому разі користувачеві слід звернутися до адміністратора.

Окрім того, КЗЗ допускає входження користувача в систему лише в ті дні тижня й години дня, в які йому це дозволено адміністратором. Якщо користувач спробує ввійти до системи в той день тижня чи в той час, коли це йому не дозволено, то КЗЗ видасть повідомлення “*Your come at a wrong date/time. Access denied. System halted”* (Ви прийшли не в той день/невчасно. Доступ заборонено. Зупин системи). У цьому разі користувачеві також слід звернутися до адміністратора.

2.6 Перевіряння цілісності КЗЗ

У перебігу завантаження КЗЗ виконує перевіряння цілісності свого ПЗ. У разі виявлення порушування цілісності подальше завантаження ОС припиняється зі стандартним повідомленням про те, що живлення комп’ютера можна вимкнути. У даній ситуації необхідне втручання адміністратора.

2.7 Змінення пароля

Користувач має змінити пароль при першому ж входженні до системи, інакше, зареєструвавши, його адміністратор зможе входити до системи і працювати під його ім’ям.

Пароль має обмежений термін чинності, тому періодично його слід змінювати. Про необхідність змінення пароля свідчить видаване при завантаженні ОС повідомлення “*Your passwordis about to expirate. Change it”* (Термін чинності Вашого пароля минає. Замініть його).

Для змінення пароля слід запустити з каталогу C:\-iFLY-BIN\ програму FLY95ADM.EXE і обрати підпункт “Пароль” пункту “Користувачі” основного меню. Після цього програма попросить користувача пред’явити ідентифікатор, що носиться, (уставити дискету в дисковод чи підімкнути ідентифікатор ТМ до зчитувача), і запросить старий (чинний) пароль для входження до системи. У відповідь на це слід ввести чинний пароль у діалозі введення пароля. При введенні правильної інформації стає активним діалог уведення нового пароля. Слід ввести, а потім потвердити новий пароль, після чого програма знову попросить підімкнути ідентифікатор, що носиться, до якого вона занесе необхідну інформацію.

Мінімальна довжина пароля для входження до системи є 6 символів, максимальна – 16. Окрім того, забороняється використовувати тривіальні паролі. Правила перевіряння пароля на тривіальність є такі:

- будь-які три підряд символи пароля не повинні повторюватися;
- будь-які три підряд символи пароля не повинні відрізнятися від попередніх на одиницю.
- При обиранні пароля можна керуватися такими правилами:
- обирати свій пароль таким, аби його було легко запам’ятати, а іншим складно добрати;
- не використовувати за пароль своє ім’я чи прізвище, імена й прізвища (у т. ч. дівочі) рідних, клички домашніх улюбленців, дні народження й інші знаменні дати;
- уникати використання географічних назв і, взагалі слів, що вони зустрічаються в словниках, у тому числі слів, доповнених певною літерою, іноземних слів, набраних українською мовою, й навпаки, тощо;
- оптимальний вибір – пароль, що він являє собою перші літери слів, котрі складають приказку чи крилатий вираз, “розведений” спеціальними символами (розділовими знаками, символами арифметичних операцій тощо) та/чи цифрами (лише не слід забувати, який саме вираз було обрано і де “повтикано” розділові знаки).

Окрім того, слід пам’ятати, що інформація автентифікування (пароль і вміст ідентифікатора, що носиться,) на відміну від інформації ідентифікування (імені) є “таємною” інформацією і не повинна бути відома та/чи доступна нікому, окрім користувача, якому вона належить. Тому, завжди дотримуйтесь таких правил:

- не залишайте свій ідентифікатор, що носиться, без догляду й ніколи й нікому його не передавайте;
- ніколи й нікому не повідомляйте свого пароля;
- ніколи й ніде не записуйте свого пароля.

Якщо усе зроблено правильно, то новий пароль набирає чинності. Його слід буде вводити у відповідь на запит “Password >” при завантажуванні системи.

2.8 Робота із захищеними каталогами

Адміністратор має поінформувати користувача про те, які каталоги є захищеними і які права доступу до них користувач має. Адміністратор визначає так само можливість використання змінних носіїв (дискет).

Користувач не повинен копіювати файли із захищених каталогів, до яких він має доступ, у незахищені. Вони не для того захищаються, аби потім будь-хто мав змогу їх читати. Такі дії відстежуються й блокуються КЗЗ та контролюються по журналах.

Користувач не повинен виконувати жодних операцій з файлами в каталогах КЗЗ.

Наявність права щодо читання захищеного каталогу дає користувачеві можливість переглядати вміст каталогу і його підкаталогів, читати файли, переглядати атрибути файлів і запускати на виконання програми, які розміщено в даному каталозі та його підкаталогах.

Наявність права щодо записування до захищеного каталогу надає користувачеві можливість редагувати й вилучати в даному каталозі та його підкаталогах файли й їхні атрибути, а також перейменовувати ці файли й підкаталоги.

Окрім того, при роботі із захищеними каталогами діє таке обмеження: КЗЗ забороняє здійснювати перейменування і вилучання захищеного каталогу й тих каталогів, що його містять, аж до диска, що він перебуває в корневому каталозі.

Усі спроби несанкціонованого доступу до захищених каталогів фіксуються в спеціальних журналах і про них повідомляється адміністраторові.

2.9 Робота зі змінними носіями й виведення інформації на друкування

Адміністратор має право обмежити доступ до змінних носіїв інформації, через які може здійснюватися імпортування/експортування інформації, а також виведення на друкування. У цьому разі він має поінформувати користувача про те, які каталоги є каталогами імпортування/експортування й чи має користувач до них доступ, а також чи може користувач роздруковувати інформацію. Користувач має погоджувати з адміністратором порядок використання змінних носіїв (дискет).

2.10 Запускання програм

У КЗЗ зреалізовано функцію контролю цілісності прикладного програмного забезпечення. Якщо її задіяно, то користувач не може запускати на робочому місці сторонні програми, у тому числі й зі змінних носіїв.

Усі подібні дії розглядаються як несанкціоновані, фіксуються в спеціальних журналах і про них повідомляється адміністраторові.

2.11 Заблоковування клавіатури

У КЗЗ зреалізовано можливість заблоковування пристроїв інтерфейсу користувача (клавіатури, миші й монітора). Заблоковування здійснюється чи

користувачем за допомогою певної комбінації клавіш (Ctrl-Alt- F11> чи <Ctrl-Alt-F12>), чи КЗЗ за бездіяльності користувача в плині визначеного адміністратором періоду часу.

У стані заблоковування маніпулятор “миша” вимикається, екран гаситься й на нього виводиться попереджувальне повідомлення й запит пароля (“Password > ”). Будь-яке натискання клавіші на клавіатурі сприймається як уведення символу пароля. Робота фонових програм при цьому може тривати.

Для розблоковування комп’ютера користувачеві треба пред’явити свій ідентифікатор, що носиться, і увести свого пароля. Розблоковувати пристрій інтерфейсу користувача може лише той користувач, що він завантажив ОС у даному сеансі.

Забороняється вимикати живлення ПЕОМ у стані заблоковування, – це може призвести до втрати інформації.

2.12 Завершення роботи

Після того, як користувач завершив роботу на ПЕОМ і планує вийти, йому слід неодмінно завершити свій сеанс роботи, у противному разі будь-яка людина, що підійшла, зможе здійснювати доступ до інформації з правами користувача, який не завершив свого сеансу роботи. Завершення сеансу роботи здійснюється штатними засобами Windows, наприклад за допомогою вибору кнопки “Пуск” і пункту “Завершення роботи.../Вимкнути комп’ютер”. Про нормальне завершення сеансу роботи свідчить поява напису “*Тепер живлення комп’ютера можна вимкнути”*.

Перезавантаження в режимі емуляції MS-DOS (з використанням пункту “Перезавантажування в режимі MS DOS” меню “Завершення роботи Windows”) для користувачів заборонено. Спроба виходу до режиму емуляції MS-DOS завершується примусовим перезавантаженням ОС.

3 Лабораторне устаткування

КЗЗ зреалізовано в стандартній операційній системі MS WINDOWS 95/98 і складається з апаратної, програмної та ключової систем. До апаратної частини належить ПЗУ з мікропрограмами рівня BIOS, установлене на спеціальній чи мережній платі. Програмне забезпечення складається з резидентної й нерезидентної частин. Ключова система являє собою спеціальний пристрій чи дискету, на якій записуються ідентифікаційні дані користувача.

4 Порядок підготовки й виконання роботи

Підготовка до проведення роботи

1 Повторити структуру КЗЗ, зреалізованого в стандартній операційній системі MS WINDOWS 95/98.

2 Визначити і сформулювати правила розмежування доступу при роботі на спеціалізованому робочому місці з обмеженим колом користувачів, наділених різними повноваженнями з доступу до ресурсів.

3 З’ясувати, які засоби й методи використовуються в КЗЗ для запобігання несанкціонованому завантаженню.

Виконання роботи

4 Здійснити входження до системи використовуючи надані адміністратором ім’я, пароль і ключову дискету.

5 Випробуйте дію системи перевіряння терміну чинності повноважень користувача.

6 Змініть пароль користувача.

7 Дослідіть можливості роботи користувача в захищених каталогах. Перевірте, у який спосіб документується робота користувача в системних журналах.

8 Розгляньте правила роботи зі змінними носіями і виведенням на друкування.

9 Перевірте, чи може користувач запускати сторонні програми.

10 Виконайте заблоковування й розблоковування інтерфейсних пристроїв комп’ютера.

11 Здісніть коректне завершення роботи.

5 Ключові запитання

1 Структура КЗЗ, зреалізованого в стандартній операційній системі (ОС) MS WINDOWS 95/98.

2 Правила розмежування доступу при роботі на спеціалізованому робочому місці з обмеженим колом користувачів, наділених різними повноваженнями з доступу до ресурсів.

3 З чого слід розпочинати входження до системи?

4 Який існує порядок завантаження ОС легальним користувачем?

5 Які засоби й методи використовуються в КЗЗ для запобігання несанкціонованому завантаженню?

6 Що відбувається за спроби несанкціонованого завантаження?

7 Які обмеження накладаються на термін чинності повноважень користувача?

8 Поясніть принципи перевіряння цілісності ПЗ КЗЗ.

9 Як здійснити змінення пароля користувача?

10 Які існують правила вибору і зберігання пароля?

11 Права доступу користувача до захищуваних каталогів.

12 Які існують обмеження при роботі із захищуваними каталогами?

13 Які є правила й обмеження при роботі зі змінними носіями і виведенням на друкування?

14 За яких умов користувачеві заборонено запускати сторонні програми?

15 У який спосіб слід виконувати заблоковування і розблоковування іінтерфейсних пристроїв комп’ютера?

16 Чому забороняється вимикати живлення комп’ютера при заблокованої клавіатури?

17 Який існує порядок коректного завершення роботи?

Лабораторна робота № 4.
Експлуатація системи антивірусного захисту
1 Мета роботи

Набуття навичок експлуатації комплексу антивірусного захисту. Вивчення функціонування системи антивірусного захисту на серверах та робочих станціях. Знайомство з порядком антивірусного захисту інформації при роботі на автоматизованому робочому місці, поштовому сервері та інших серверах.

2 Ключові положення

Система антивірусного захисту в галузі створена й базується на підставі принципів, викладених у підрозділах 1.2.3 … 1.2.7 цього посібника. Система антивірусного захисту побудована на антивірусних продуктах:

- TrendMicro Inc. Scan mail for MS Exchenge виробництва компанії TrendMicro Inc.;
- Антивірус Symantec Inc. Norton AntiVirus Corporate Edition 7.6 for Desktops & File Servers виробництва Symantec Inc.

Антивірусні продукти забезпечують лікування усіх відомих комп'ютерних вірусів із занесенням інформації про це у відповідні протоколи роботи для забезпечування централізованого моніторингу роботи. В разі підозри на зараження невідомими комп'ютерними вірусами система антивірусного захисту має можливість заблоковування доступу користувачів до цієї інформації.

3 Лабораторне устаткування

Систему антивірусного захисту зреалізовано в стандартних операційних системах MS Windows NT/ 2000MS, Windows 95/98/NT(SP4)/2000(SP2)/XP/ME, Windows 3.1 та DOS і складається вона з апаратної й програмної частин серверів та клієнтів. Сервери побудовано на Pentium Pro чи вище, твердому дискові на 75 MB та ОЗУ 64 MB чи більше. Для Norton AntiVirus client/server disk image потрібно 24 MB обсягу на твердому дискові та 3 MB ОЗУ. Клієнти DOS мають процесор 33 MHz Intel 386, 640 KB системної пам'яті, 2 MB розширеної пам'яті і 6 MB обсягу на твердому дискові. Клієнти Windows 3.1 мають процесор Intel 486, не менш 16 MB ОЗУ, 640 KB системної пам'яті, 17 MB обсягу на твердому дискові. Клієнти Windows 95/98/NT(SP4)/2000(SP2)/XP/ME мають процесор не менш за Intel 486 (рекомендується процесор Pentium), не менш за 16 MB ОЗУ, 17 MB обсягу на твердому дискові. При виконанні роботи використовується дискета з файлами, інфікованими комп'ютерними вірусами.

4 Порядок підготовки й виконання роботи

Підготовка до проведення роботи

1 Вивчити структуру та функції системи антивірусного захисту на стадії технічної експлуатації інформаційно-обчислювальної системи.

2 Визначити завдання трирівневого керування системою антивірусного захисту.

3 З’ясувати організаційні засоби роботи системи антивірусного захисту. Ознайомитись з відповідальністю та обов’язками групи антивірусного захисту, користувачів та групи супровадження.

4 Вивчити способи перевіряння на зараження комп’ютерними вірусами робочих станцій та серверів.

Виконання роботи

5 Ознайомитись із параметрами налаштовування системи антивірусного захисту.

6 Випробувати роботу системи антивірусного захисту з параметрами налаштовування: лікування інфікованого файла, вилучання зараженого файла. Проаналізувати результати роботи системи антивірусного захисту. Перевірити, у який спосіб документовано роботу системи в журналах.

7 Випробувати роботу системи антивірусного захисту з параметром налаштування: ізоляція інфікованого файла. Проаналізувати результати роботи системи антивірусного захисту в каталозі IZOLATOR. Зробити висновок щодо подальших можливих дій із зараженим файлом.

8 Ознайомитись із засобами адміністрування використаними в системі антивірусного захисту.

9 Ознайомитись з основними функціями виконуваними з консолі *Symantec System Center*.

10 Дослідити вміст журналів вірусів, огляду та подій. Зробити висновки.

11 Проаналізувати методи оновлення системи антивірусного захисту.

5 Ключові запитання

1 Структура та призначення системи антивірусного захисту на стадії технічної експлуатації інформаційно-обчислювальної системи.

2 Функції системи антивірусного захисту на стадії технічної експлуатації інформаційно-обчислювальної системи.

3 Принцип ієрархічнї рівневої побудови системи антивірусного захисту.

4 Рівнева система керування системою антивірусного захисту.

5 Призначення первинних серверів антивірусного захисту та серверів антивірусного захисту другого рівня.

6 Організація роботи системи антивірусного захисту.

7 Які є сфери відповідальності й обов’язки групи антивірусного захисту, користувачів та групи супровадження?

8 Загрози безпеці інформації при використанні електронної пошти.

9 Які функції виконує система моніторингу електронної пошти?

10 Поясніть параметри налаштовування системи антивірусного захисту. Які дії виконує система при цих налаштовуваннях?

11 Призначення ізолятора на робочій станції.

12 Які засоби адміністрування використовуються в системі антивірусного захисту?

13 Основні функції виконувані з консолі *Symantec System Center.*

14 Призначення журналів вірусів, оглядів та подій.

15 Методи оновлювання системи антивірусного захисту.

Лабораторна робота № 5. Розробка моделі загроз інформаційним ресурсам ЦАТС та ТЗ на КЗСІ на ЦАТС

1. Мета роботи

Вивчення методики розробки моделі загроз інформаційним ресурсам ЦАТС на основі типової моделі загроз. Вивчення методики розробки технічного завдання на комплексну систему захисту інформації (КЗСІ)

2. Література

1. КНД 45-164-2001 Типова модель загроз для інформаційних ресурсів цифрових АТС, що використовуються в мережах електрозв'язку загального користування України.
2. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення;
3. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
4. НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту;
5. НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту;
6. НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації ;довірчих оцінок реалізації захисту;
7. НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт;
8. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).

3. Основні положення

Розроблення моделі загроз є складовою частиною робіт з ТЗІ на ЦАТС, що здійснюються згідно з НД ТЗІ 2.7-001, ДСТУ 3396.0 та ДСТУ 3396.1. Відповідно до принципу мінімальної достатності система захисту повинна бути спроектована таким чином, щоб здійснювалася протидія тільки тим загрозам, що мають суттєве значення для держави, операторів електрозв’язку та абонентів, і тільки в тій мірі, у котрій необхідно нейтралізувати (послабити, зменшити) наслідки прояву таких суттєвих загроз, для того щоб втрати від їхніх можливих реалізацій не перевищили гранично допустимих рівнів.

Типова модель загроз для інформаційних ресурсів ЦАТС – це модель загроз, розроблена з урахуванням типових (притаманних усім або більшості ЦАТС) характеристик середовищ функціонування (інформаційного, технологічного, користувачів).

У типовій моделі загроз враховані найбільш вірогідні та (або) такі загрози, що призводять до найбільшої шкоди для операторів електрозв'язку та користувачів послуг електрозв'язку.

Порядок використання типової моделі загроз наведено у КНД 45-164-2001 (додаток А) .

Методи аналізу, рекомендовані для застосування під час розроблення моделі загроз наведені у КНД 45-164-2001 (додаток Б).

Загальні вимоги до побудови моделі захисту з урахуванням моделі загроз наведені у КНД 45-164-2001 (додаток В).

4. Домашнє завдання

4.1. З'ясувати призначення загальних термінів, таких як
- типова структура інформаційних ресурсів ЦАТС,
- структура інформаційних ресурсів
- загроза для інформаційних ресурсів ЦАТС
- аналіз середовища функціонування ЦАТС
- уразливість інформаційних ресурсів порушник (стосовно ТЗІ у ЦАТС)
- профіль середовища

4.2. Сформулювати види загроз інформаційним ресурсам ЦАТС

4.3. Сформулювати причини реалізації загроз для інформаційних ресурсів ЦАТС

4.4. Ознайомитись з порядком використання типової моделі загроз

4.5. Ознайомитись з загальними вимогами до побудови моделі захисту з урахуванням моделі загроз

5. Контрольні запитання

1 Розкрити види загроз інформаційним ресурсам ЦАТС

2. Розкрити причини реалізації загроз для інформаційних ресурсів ЦАТС

3. Привести порядок використання типової моделі загроз

4. Визначити загальні вимоги до побудови моделі захисту з урахуванням моделі загроз

5. Розкрити визначення „Модель порушника"

6. Лабораторне завдання

6.1. Перевірка працездатності підсистеми захисту від несанкціонованого доступу (НСД), що реалізована на ЦКС EWSD.

6.2. Перевірка працездатності системи розподілу прав доступу на ЦКС EWSD.

6.3. Перевірка сталості підсистеми керування доступом та її реакції на некоректні дії користувачів.

6.4. Перевірка працездатності ЦКС EWSD щодо виконання функцій аудиту (контролю) стану ресурсів ЦКС.

6.5. Перевірка працездатності ЦКС EWSD щодо виконання функцій контролю трафіку (ступеню навантажень на пропускну спроможність) через основні компоненти ЦКС та через усю ЦКС у цілому.

6.6. Перевірка працездатності ЦКС EWSD щодо виконання послуг архівування (створення “history file”) та контролю дій персоналу ЦКС.

6.7. Перевірка існування обмежень у доступі до архівних файлів для користувачів ЦКС, що не мають необхідних для цього прав доступу

6.8. Перевірка існування обмежень у доступі до технологічних баз даних (у т. ч., із абонентською інформацією), які розміщені на ЦКС EWSD.

6.9. Перевірка коректності функціонування на ЦКС EWSD інформаційно-уразливих режимів та послуг, що надаються.

6.10. Перевірка функції ідентифікації абонентів.

6.11. Перевірка функції аудиту абонентів в підсистеми комутації.

6.12. Перевірка функції аудиту абонентів в підсистеми керування.

6.13. Перевірка функції адміністративного обмеження трафіку абонентів.

6.14. Перевірка функції індівідуальної протидії несанкціонованому користуванню абонентською лінією (паролі).

6.15. Перевірка функції вимірювання параметрів абонентських ліній.

6.16. Перевірка функції ізоляції системних файлів.

7. Опис лабораторного макета

7.1. Типова модель загроз виконується для інформаційних ресурсів реальних цифрових АТС на прикладі ЦКС EWSD, що використовуються в мережах електрозв'язку загального користування України

8. Порядок виконання роботи

8.1. Переконатися, що підсистема захисту від НСД, що реалізована на випробуваному зразку ЦКС EWSD, виявиться працездатною: всі спроби виконати припустимі послідовності команд для всіх припустимих категорій доступу мають виявитись успішними.

8.2. Перевірити, чи система розподілу прав доступу до підсистеми керування випробуваним зразком ЦКС EWSD виявиться працездатною: всі спроби порушити права доступу з боку зареєстрованих у системі суб’єктів, що мали різні визначені системою права доступу, мають виявитись безуспішними

8.3. Перевірити, чи підсистема керування доступом оцінюваного зразка ЦКС EWSD задокументованим чином буде реагувати на усі некоректні дії

8.4. Перевірити, чи результати виконання усіх відображених у технічній документації на ЦКС EWSD команд, що здійснюють виконання функцій аудиту (контролю) стану ресурсів ЦКС виявляться позитивними.

8.5. Перевірити, чи усі команди контролю трафіку через основні компоненти ЦКС EWSD та через усю ЦКС EWSD у цілому, що відображені у технічній документації, на момент випробувань будуть позитивними. При перевірці керуватися – „Инструкцией по эксплуатации и техническому обслуживанию ЦКС EWSD (приложение)”

8.6. Перевірити, що усі команди щодо виконання послуг архівування та контролю дій персоналу ЦКС EWSD, що відображені у технічній документації, на момент випробувань будуть працездатними

8.7. Перевірити, чи всі спроби випробувальної групи здійснити доступ до архівних файлів у ЦКС EWSD з боку суб'єктів, які не мали для цього відповідних прав доступу виявляться безуспішними.

8.8. Перевірити, чи всі спроби випробувальної групи здійснити доступ до технологічних баз даних ЦКС EWSD з боку суб'єктів, які не мали для цього відповідних прав доступу виявляться безуспішними.

8.9. Перевірити коректність дії тимчасової заборони викликів на зв'язок, обмеження можливості зв'язку з міжміськими та міжнародними абонентами, надання зв'язку по паролю згідно з інструкцією по експлуатації.

8.10. Перевірити, чи дійсно при задані відповідних сервісних послуг ідентифікуються усі визиваючи абоненти

8.11. Перевірити, чи дійсно при введені відповідних команд висвітлюються усі дзвінки даного абонента за певний період часу.

8.12. Перевірити, чи дійсно при введені відповідних команд висвітлюються усі дії абонентів в підсистеми керування за певний період часу.

8.13. Перевірити, чи дійсно при введені відповідних команд обмежується трафік даного абонента ЦКС EWSD.

8.14. Перевірити коректність функціонування системи вводу, заміни та просмотру паролів.

8.15. Перевірити неможливість будь яких дій з системними файлами з боку користувачів системи.

9. Зміст протоколу

9.1. Блок-схема побудови моделі загроз для інформаційних ресурсів ЦАТС

9.2. Схема ЦАТС з позиції ТЗІ.

9.3. Протоколи перевірок

Лабораторна робота № 6 Налаштування та адміністрування між мережних екранів

1 Мета роботи

Вивчення структури, функцій та набуття навиків налагодження та технічної експлуатації міжмережних екранів (брандмауерів), реалізованих у локальних обчислювальних мережах (ЛОМ) та автоматизованих робочих місцях (АРМ). Крім того, вивчаються типи політик мережного доступу, технічна реалізація цих політик, вибір типів міжмережних екранів для забезпечення безпеки ЛОМ, порядок їх реалізації і технічної експлуатації.

2 Література

2.1 Єфремов В.П., Кононович В.Г., Тардаскін М.Ф. Технічна експлуатація систем захисту інформації. Частина 2 Експлуатація систем захисту інформації. Навч. посібник/ За редакцією М.В. Захарченка. – Одеса: ОНАЗ, 2003. – С. 248.

2.2 Домарев В. В. Захист інформації і безпека комп'ютерних систем. К.: Видавництво "Диасофт", 1999. – 480 с.

3 Основні положення

3.1 Призначення міжмережних екранів та причини їх використання

Розвиток сучасних інформаційних технологій привел до появи нового механізму безпеки - межмережевого екранування. Даний механізм вирішує завдання аналізу інформаційних потоків, що проходять між виділеними сегментами інформаційної системи з розмежуванням доступу й приховання топології й функціональності кожного із сегментів. Найбільше повно дана функція реалізована в міжмережевих екранах (firewall).

Сучасні міжмережеві екрани являють собою програмно-апаратні комплекси, реалізовані на сучасних ОС, що відповідають високим вимогам у частині безпеки й надійності функціонування, аналізують і розділяють інформаційні потоки на всіх рівнях моделі ISO/OSI, містять засоби моніторингу й автоматичного реагування на спроби НСД.

Крім класичних варіантів міжмережеве екранування перспективно використати в Internet-додатках. Internet-рішення засновані на використанні засобів, застосовуваних в інформаційній структурі Internet, тому на ці рішення часто поширюють недоліки, типові для роботи в Internet. Ця точка зору заснована на недооцінці специфіки Internet-систем.

Архітектурно Internet-системи являють собою трьох рівневі системи "клієнт-сервер" з використанням WWW-сервера в якості ПО як проміжного шару. Оскільки саме трьох рівневі системи звичайно використаються для найбільш ефективної роботи механізмів безпеки, немає підстав сумніватися в можливості настільки ж успішного впровадження механізмів безпеки в Internet-системи. Додатковою перевагою такого підходу буде можливість атестації таких систем відповідно до діючого законодавства. У цьому випадку WWW-

сервер використає механізм екранування сервисів для створення незалежного засобу доступу й блокування дії програмних закладок у ПО сервера баз даних.

3.2 Компоненти брандмауера

Основними компонентами брандмауера є:

- політика мережного доступу;
- механізми посиленої автентифікації;
- фільтрація пакетів;
- прикладні шлюзи.

3.3 Можливі різні конфігурації брандмауерів

- брандмауер з пакетною фільтрацією;
- брандмауер зі шлюзом із двома адресами;
- брандмауер з екранованим хостом;
- брандмауер з екранованою мережею;
- інші.

3.4 Основні етапи настроювання міжмережевого екрана

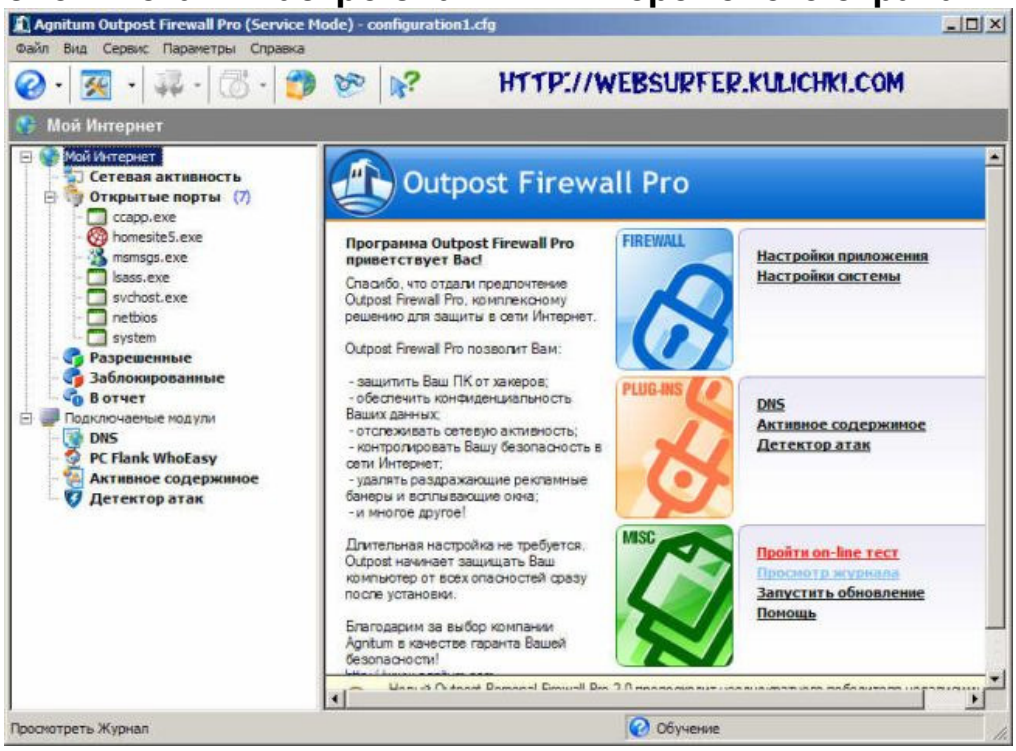

Рис. 1

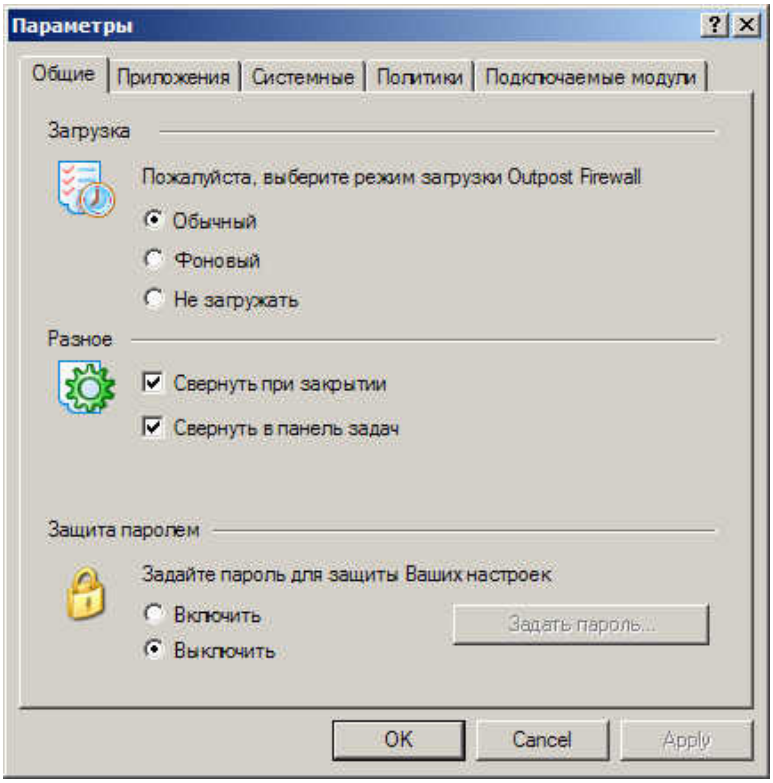

Рис. 2

Закладка - загальні, рисунок 2. У самому верху вікна опція - завантаження й три варіанти на вибір - звичайний, фоновий і не завантажувати. За замовчуванням встановлено перший варіант.

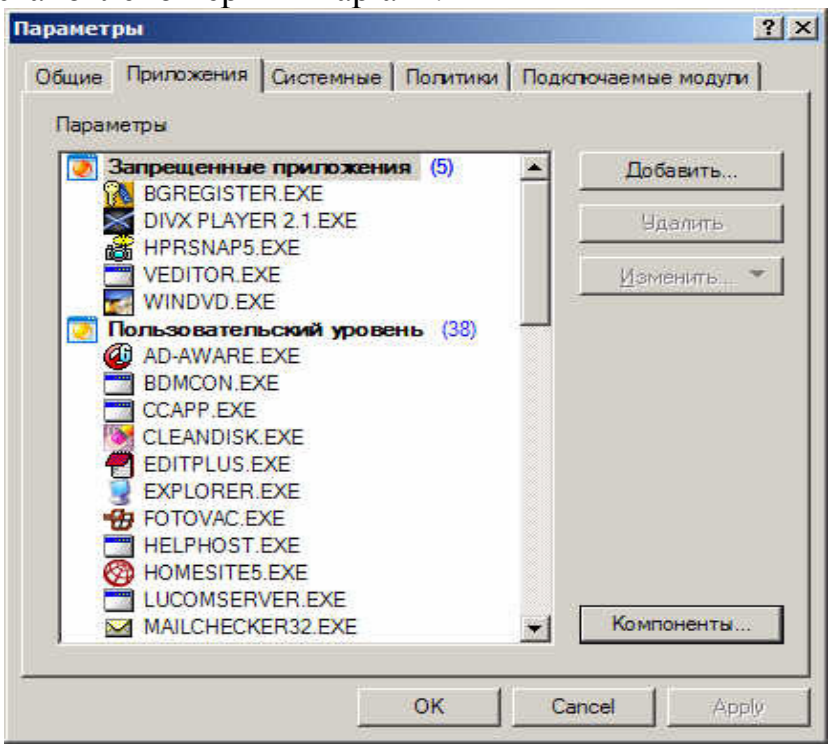

Рис. 3

Закладка - додатки, рисунок 3. У цьому вікні будуть з'являтися програми в міру їхнього першого запуску й виходу в мережу. Діляться додатки (мається на увазі програми) на три категорії - заборонені, користувальницький рівень і дозволені. Заборонені - це ті програми, яким адміністратор заблокував доступ до інтернету, до користувальницького рівня ставляться ті програми, для яких

адміністратор склав певні правила використання мережі (тобто не все можна, а тільки певні дії) і нарешті останній варіант - це дозволені програми, тобто ті, котрим дозволено все (мається на увазі, що використати мережу вони можуть як завгодно). Кнопка - компоненти відображає всі складові програм із цього вікна - динамічні бібліотеки, запущені файли, тобто всі ті компоненти програм, які власне кажучи й використають мережу (Рис. 4).

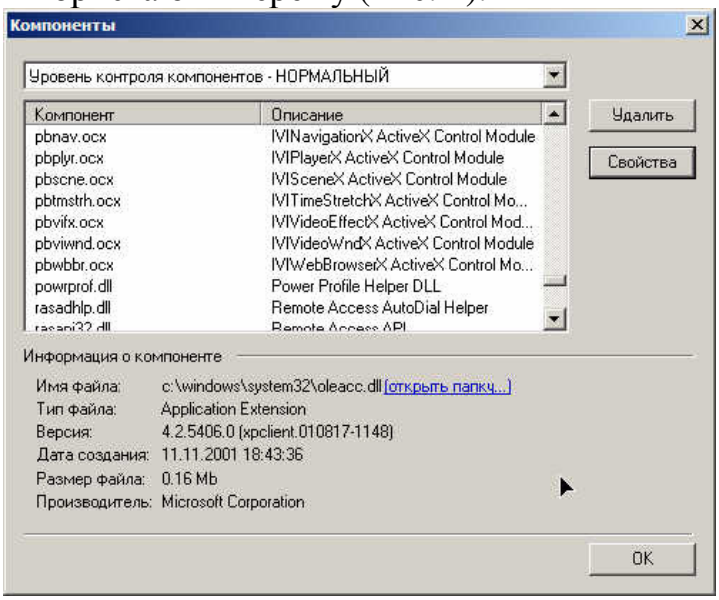

Рис. 4

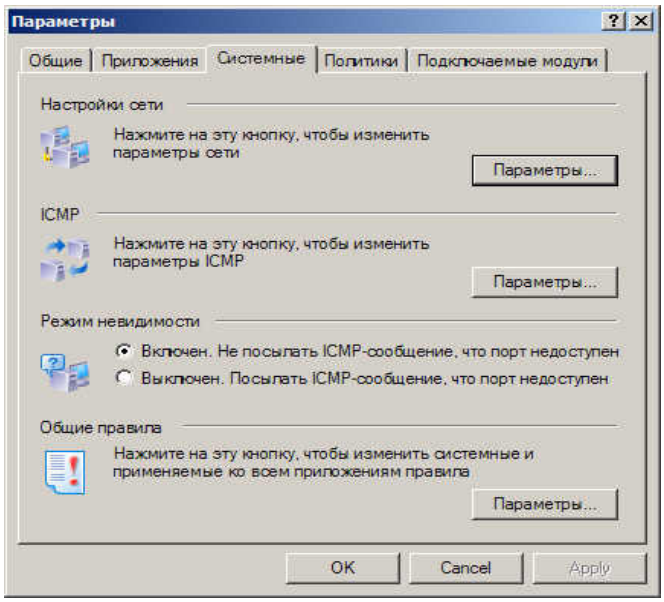

Рис. 5

Закладка - системні. Сюди входять - настроювання мережі (Рис. 6), ICMP (Internet Control Message Protocol) - використовується, щоб посилати повідомлення про помилки керування між комп'ютерами, зв'язаними по мережі (Рис. 7). Ці параметри встановлені за замовчуванням. Далі секція - режим невидимості. Тут два варіанти - включений/виключений, за замовчуванням цей режим включений.

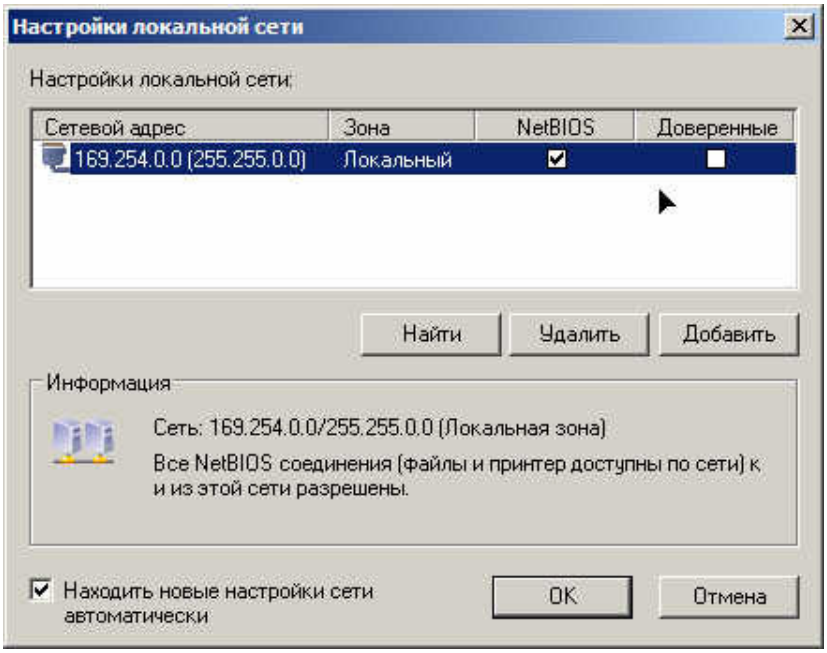

Рис. 6

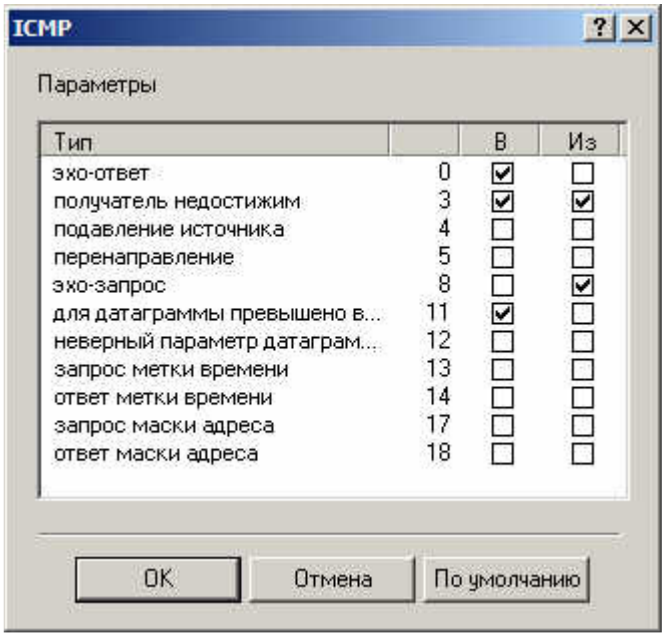

Рис. 7

Секція загальні правила показана на Рис. 8. У цьому вікні можна побачити встановлені правила використання мережі, сюди ж можна додавати й свої правила й це буде відноситись до варіанта програм користувальницького рівня.

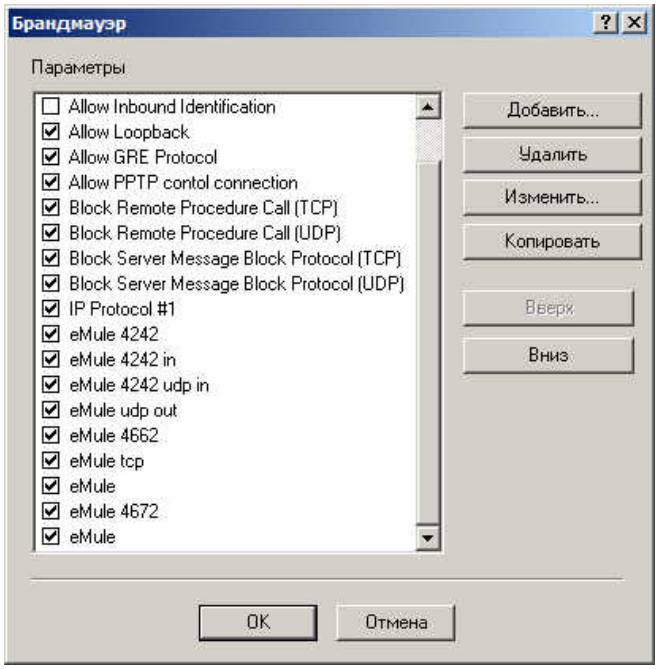

Рис. 8

Закладка - політики (Рис. 9). Тут є досить багатий вибір, що залежить від цілей, які переслідуєте адміністратор. Такі як - дозволяти (будуть дозволені всі з'єднання, крім заблокованих), режим навчання. При цьому режимі все, що взаємодіє з мережею й запускається в перший раз буде піддано питанню програми - як взаімодіяти із цим? І залежно від відповіді адміністратора буде створене правило. Режим блокування (при ньому в протилежність режиму дозволу все, що не дозволено буде заблоковано для виходу в мережу), далі, режим заборони (при ньому абсолютно все буде заблоковано, у не залежності від правил дозволу), нарешті, режим відключити (відключає активність програми, тобто не закриваючи її можливе користування Інтернетом начебто ніякого файервола не встановлено).

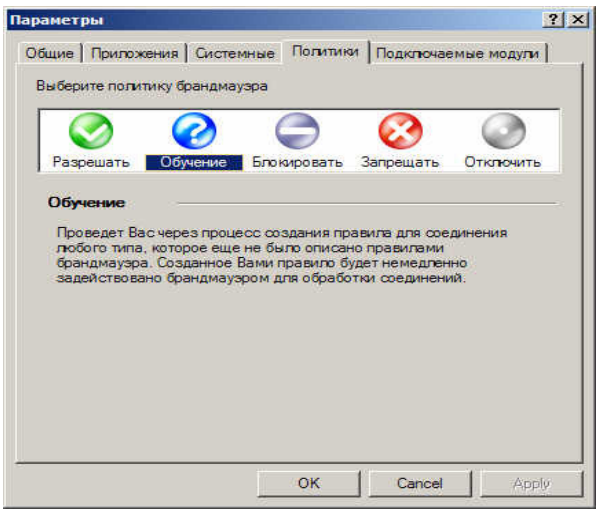

Рис. 9

Переходимо до останньої закладки настроювань – на якій підключаються модулі (Рис. 10), простіше говорячи плагіни. Із програмою йдуть шість плагінів, хоча окремо можна встановлювати більше. Перелічемо ті, що йдуть у комплекті.

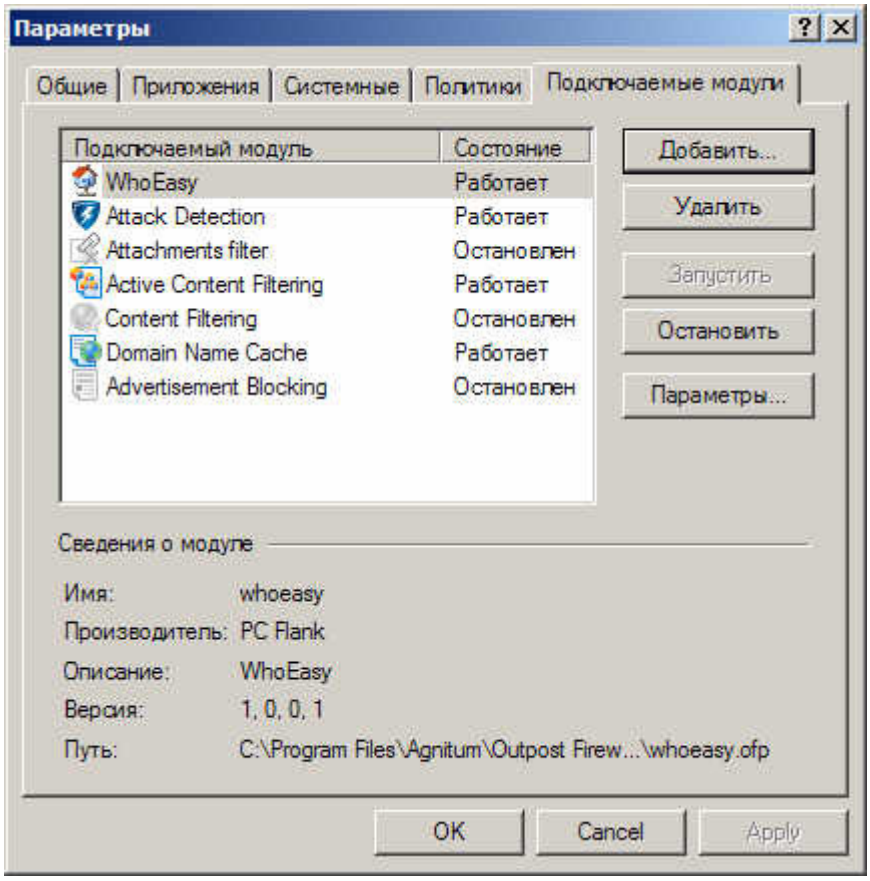

Рис. 10

Atack Detection (Рис. 11) - подивившись на рисунок 11, Ви побачите настроювання за замовчуванням, хоча рівень можна встановити на один із трьох - байдужий (програма при ньому буде видавати попередження тільки у випадку 100% атаки на комп'ютер), далі йде режим за замовчуванням - звичайний (при ньому будуть видаватися попередження при скануванні портів комп'ютера), нарешті, третій, максимальний режим (при ньому, навіть при скануванні одного порту на комп'ютері буде видаватися попередження).

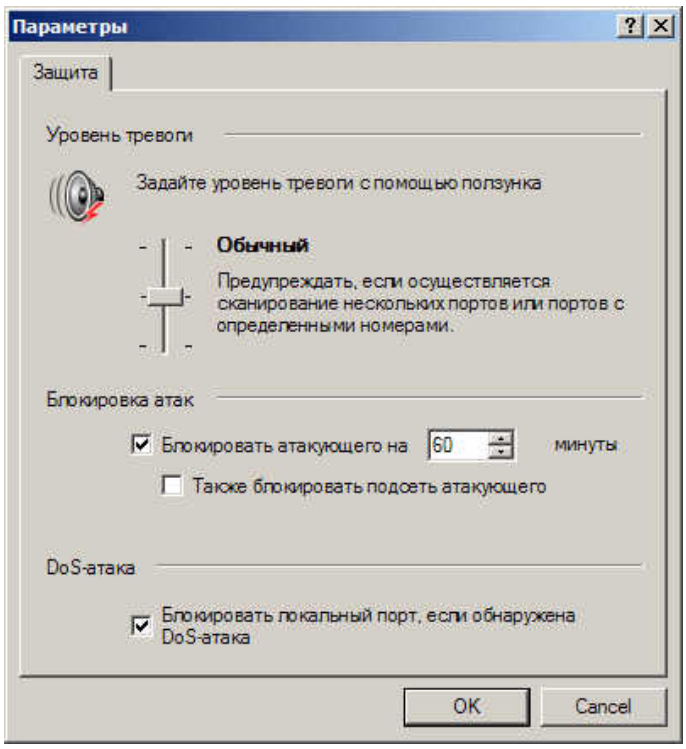

Рис. 11

Attachments Filter (Рис. 12) - цей плагін дозволяє настроїти роботу із вкладеннями в листи. Залежно від типу файлу, вкладеного в лист можна або перейменувати його, або повідомити про вкладення.

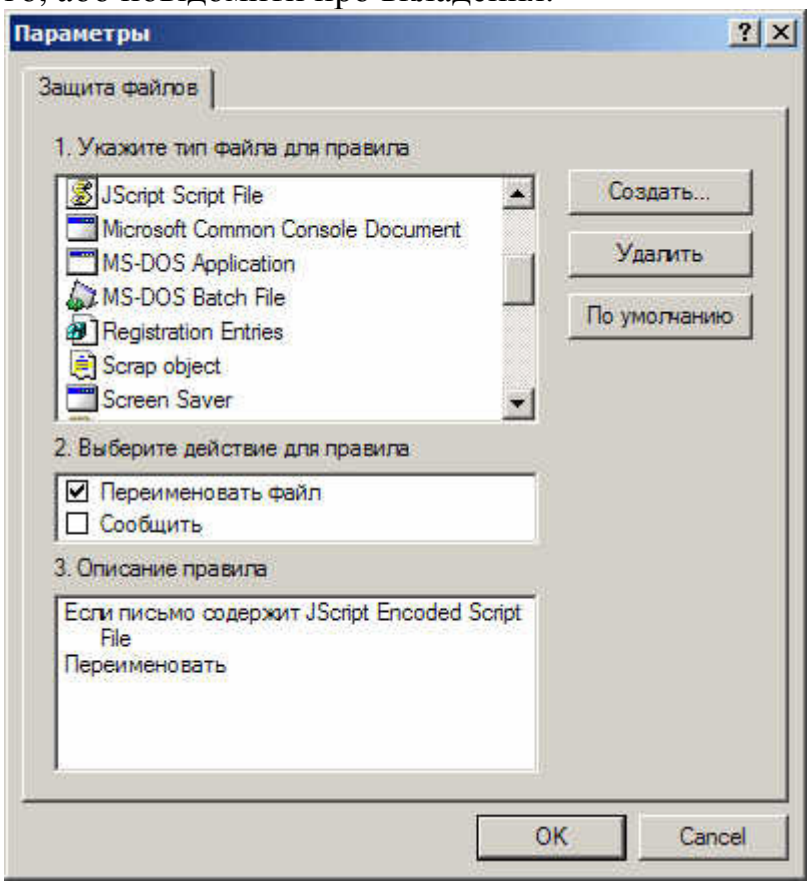

Рис. 12

Active Content Filtering (Рис. 13) - це своєрідний аналог настроювань безпеки в браузері. Плагін цей за замовчуванням працює.

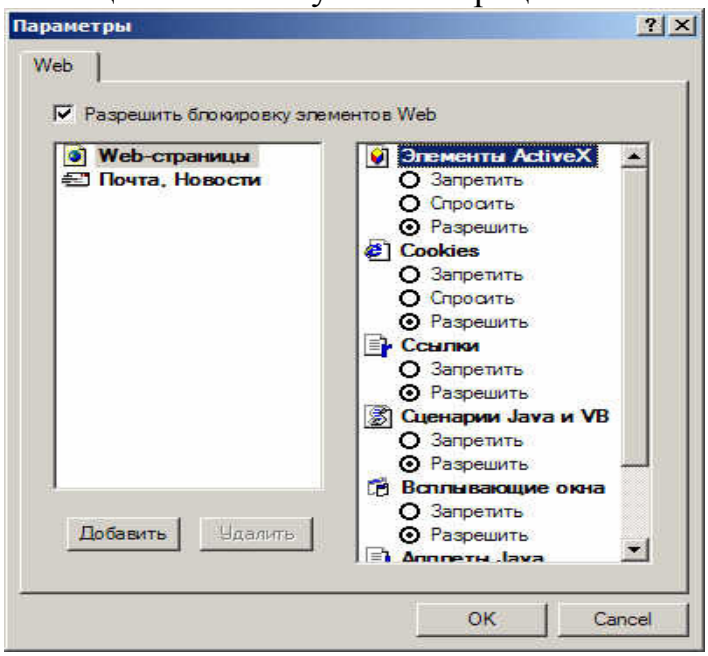

Рис. 13

Content Filtering (Рис. 14). З допомогою цієї опції можливо ввести адреси сайтів або просто окремі слова, виявивши які програма буде блокувати доступ до них. За замовчуванням плагин активний, але список у нього порожній.

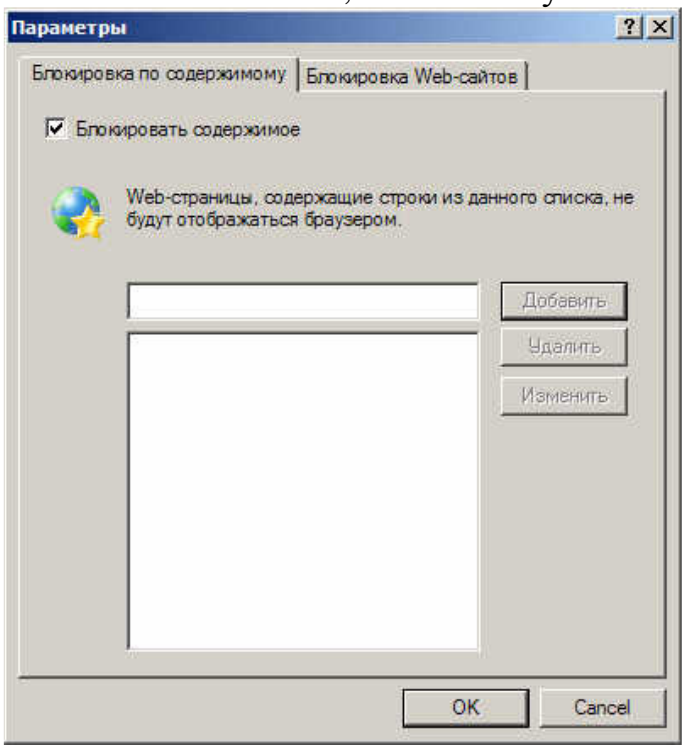

Рис. 14

Domain Name Cache (Рис. 15) - плагін частково виконуючої функції проксі. Ця опція дозволяє настроїти фіксовану кількість DNS адрес яку необхідно запам'ятовувати й скільки їх пам'ятати. Це даси можливість швидше

завантажувати сторінки, оскільки не потрібно буде щораз шукати відповідність DNS адрес та імен сайту.

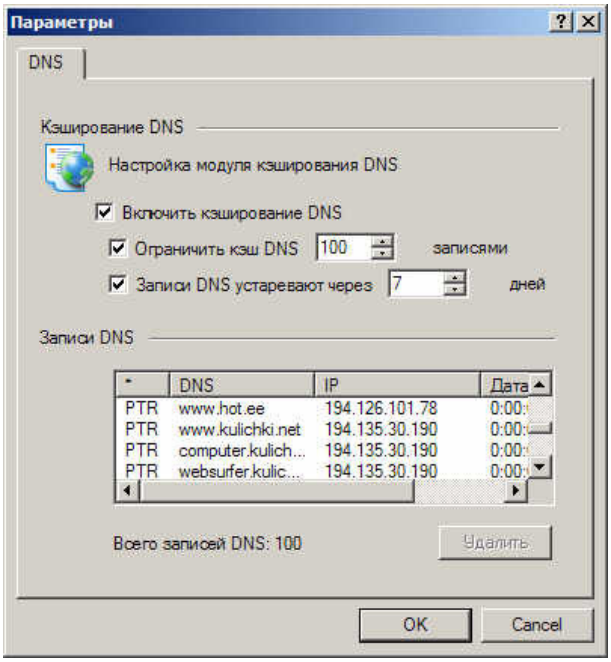

Рис. 15

Advertisement Blocking (Рис. 16) - блокування рекламного змісту web-сторінки. Тут можна блокувати не тільки рекламні зображення по розміру (баннери), але й рядки рекламного характеру.

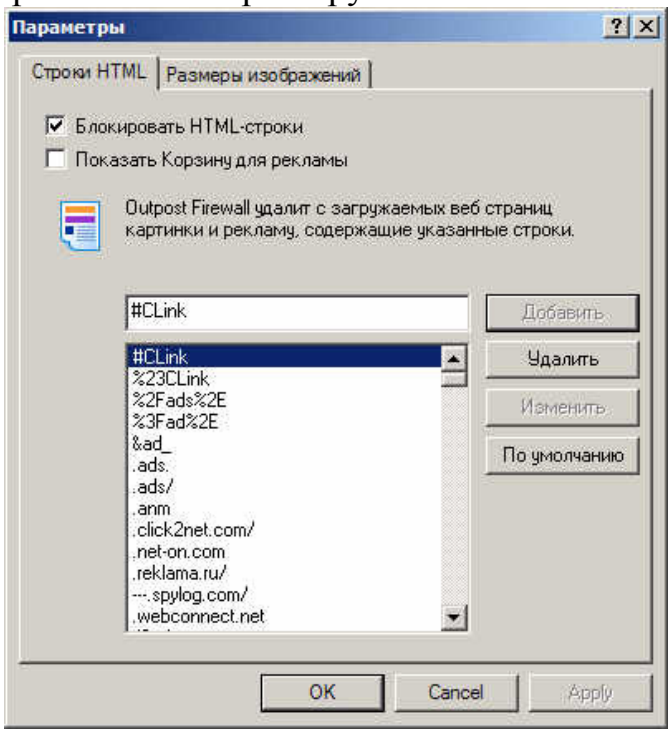

Рис. 16

Журнал подій програми (Рис. 17). Всю статистику програми можливо подивитись в цьому журналі.

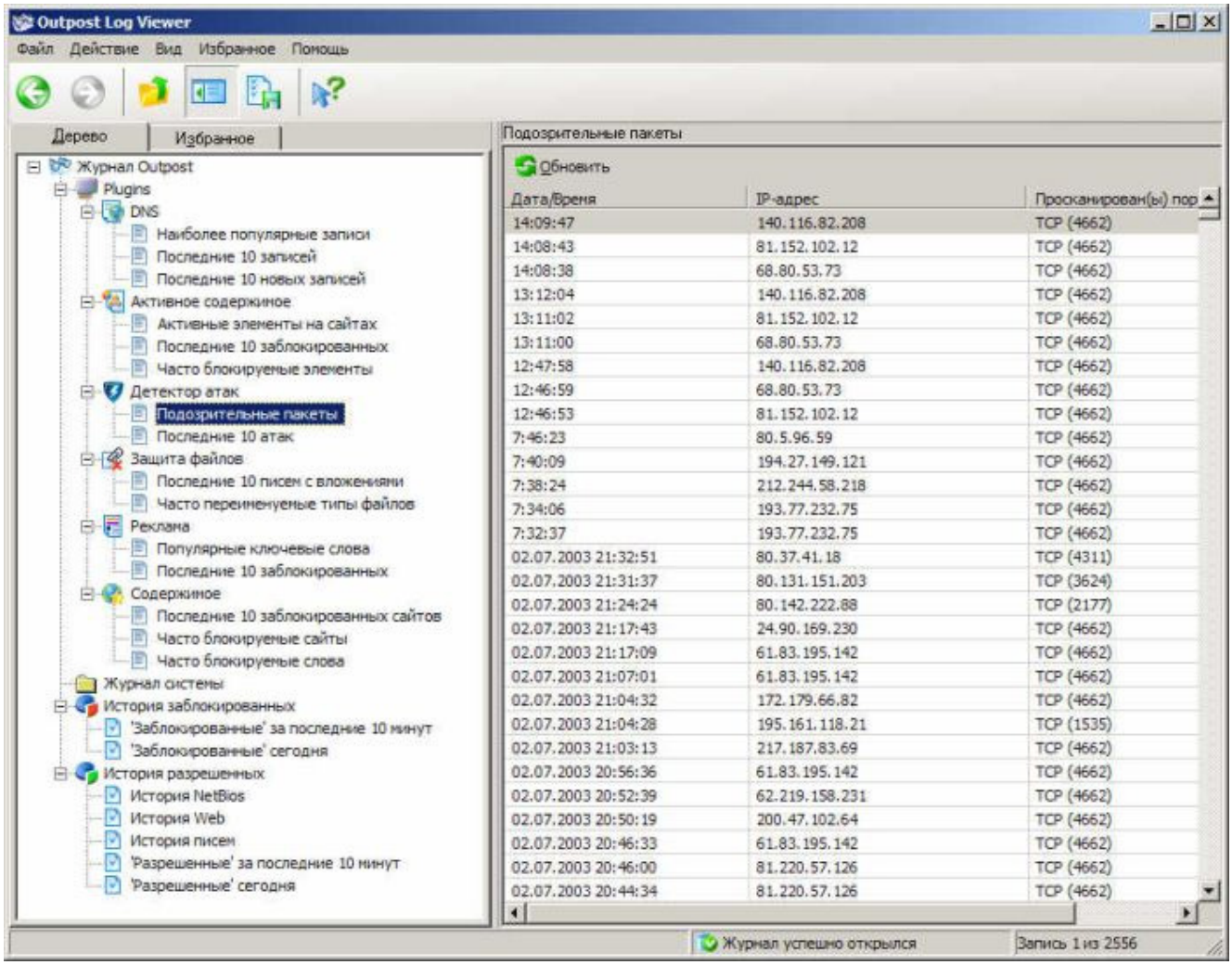

Рис. 17

Створення правил слід розглянути докладніше. Основне навантаження в створенні правил лягають на адміністратора у навчальному режимі (Рис. 9), тому й будемо розглядати роботу із програмою саме в цьому режимі. Правила можна розділити на дві категорії - правила для програм і системні правила. Почнемо зі складання правил для програм. Правила програм у свою чергу можна також розділити на дві категорії – встановленні по замовчуванню файерволом і створені адміністратором. На рисунку 18 показаний перший тип - встановленні по замовчуванню файерволом. До них віднесені - ftp менеджери, менеджери завантажень, браузери, програми для інтернет спілкування (наприклад ICQ) і т.д., тобто програми зі стандартним використанням інтернету (постійні номери портів, використовувані протоколи й т.д.). Коли якась програма в перший раз запитує інтернет, файервол відразу пропонує створити правило для цієї програми. Якщо програма відноситься до перерахованих вище, то серед опцій можна побачити тип даної програми й відповідне йому правило. На малюнку 18 один з варіантів - ftp клієнт. Також на Рис. 18 можна бачите ще два варіанти - дозволити однократно або блокувати однократно. Вони не так часто потрібні і як правило їх треба запускати у випадку, якщо програму

встановлено вперше і треба її протестувати. Тоді слід вибрати варіант - дозволити однократно (щоб потім не видаляти у ручному режимі зі списку (Рис. 3).

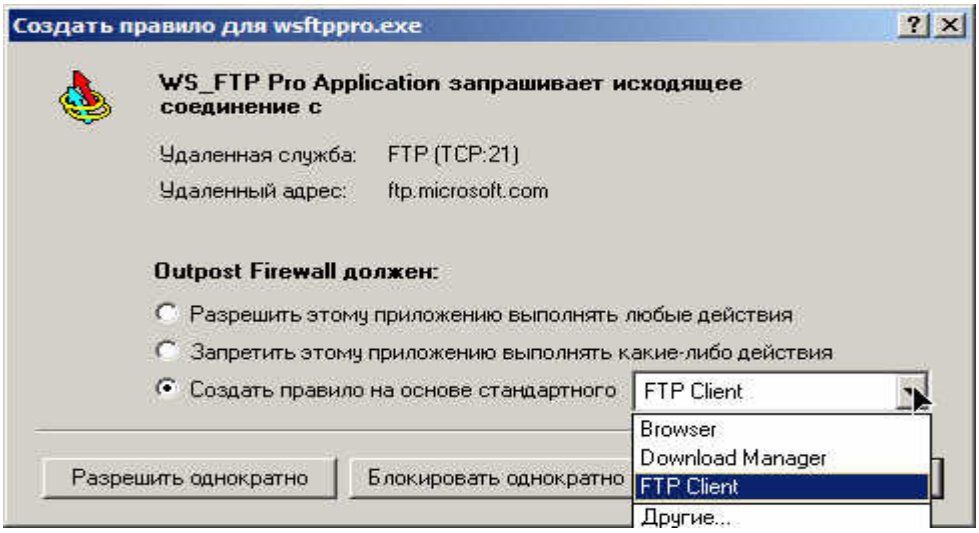

Рис. 18

Перейдемо до другого типу правил - правила створювані користувачем. Розглянемо той же самий варіант (із програмою WS FTP Pro - ftp клієнтом), але в ситуації, коли створюється правило у ручному режимі. Отже, перший запуск ftp клієнта, файервол "викидає" те ж саме вікно для створення правил, але ми не вибираємо пункт - ftp клієнт, а вибираємо нижній варіант - інші (Рис. 19).

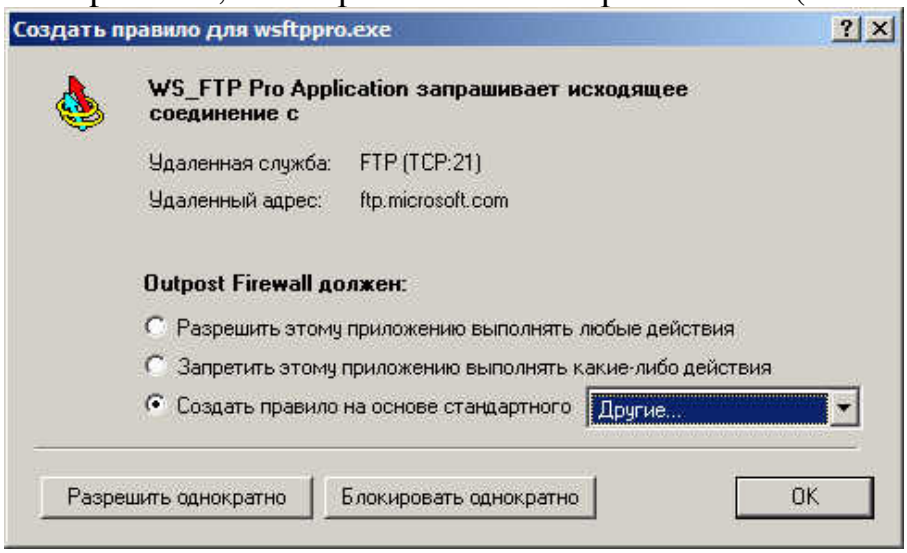

Рис. 19

Натискаємо ОК і бачимо вікно, зображене на рисунку 20. Можна вибирати тип протоколу, що буде використати програма, напрямок (вхідне/вихідне), порти, якими можна користуватися або навпаки - не можна, адреси в інтернеті (мережі) до яких програма може або не може звертатися й т.д. Все це дуже схоже на створення правил для повідомлень у поштових програмах (наприклад Microsoft Outlook).

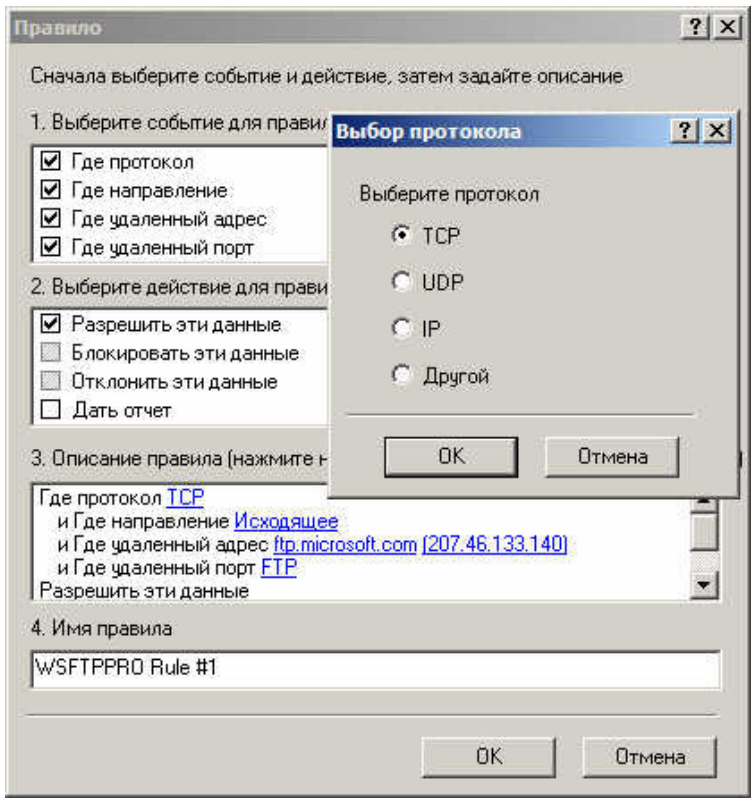

Рис. 20

4 Домашне завдання

4.1 Визначити призначення та ознайомитись з причинами застосування міжмережних екранів в локальних і корпоративних мережах передачі даних.

4.2 Визначити переваги, недоліки і проблеми застосовування міжмережних екранів.

4.3 З'ясувати, з яких основних компонентів складаються міжмережні екрани.

4.4 З'ясувати види та зміст політики мережного доступу, що впливають на проектування, установку і експлуатацію системи міжмережних екранів в локальних і корпоративних мережах передачі даних.

4.5 Підготувати приклад правил фільтрації пакетів відповідно до політики міжмережного екрану.

5 Контрольні запитання

5.1 Складові міжмережних екранів: політика, зміни в структурі мережі, технічні засоби, організаційні заходи.

5.2 Причини проблем з інформаційною безпекою ЛОМ.

5.3 Інциденти, викликані використанням слабких паролів та спостереження за каналами передачі даних.

5.4 Загрози від неправильного використання електронної пошти.

5.5 Способи маскування під іншого користувача.

5.6 Які принципи побудови між мережних екранів.

5.7 Система міжмережних екранів як засіб захисту підмереж від неправильного використання протоколів і служб.

5.8 Які переваги використання міжмережних екранів для забезпечення інформаційної безпеки ЛОМ та корпоративних мереж.

5.9 Які недоліки використання міжмережних екранів для забезпечення інформаційної безпеки ЛОМ та корпоративних мереж.

5.11 Проблеми, які не вирішуються за допомогою міжмережних екранів.

5.12 Перелічити компоненти міжмережних екранів.

5.13 Пояснити політику мережного доступу та доступу до сервісів.

5.14 Пояснити політику проектування між мережних екранів.

5.15 Пояснити необхідність та способи посиленої автентифікації.

5.16 Способи та особливості фільтрації пакетів.

5.17 Які пакети потрібно фільтрувати.

5.18 Наведіть, які проблеми є з маршрутизаторами з фільтрацією пакетів.

5.19 Пояснити використання прикладних шлюзів (хостів з проксі-службою).

5.20 Пояснити особливості шлюзів транспортного рівня.

5.21 Схема та використання міжмережних екранів з фільтрацією пакетів.

5.22 Схема та використання міжмережних екранів на основі ПЕОМ, підключеної до двох мереж.

5.23 Схема та використання міжмережних екранів з ізольованим хостом.

5.24 Схема та використання міжмережних екранів з ізольованою під мережею.

5.25 Способи інтеграції модемних пулів з міжмережними екранами.

6 Лабораторне завдання

6.1 Виконати завантаження програм міжмережного екрану Agnitum Outpost Firewall 2 на хості. Простежити процедури ініціалізації.

6.2 Ознайомитись з порядком настроювання міжмережного екрану. Запустити програму брандмауера й ознайомитись з її інтерфейсом.

6.3 Ознайомитись з порядком настроювання і цілями політики міжмережного екрану.

6.4 Вивчити принципи реалізації політики міжмережного екрану з фільтрацією пакетів.

6.5 Вивчити призначення та зміст правил фільтрації пакетів.

6.6 Створити пробну сукупність правил фільтрації пакетів. Провести настроювання і перевірити виконання режимів доступу до мережі.

6.7 Ознайомитись з принципами фільтрування потоків інформації, служб, протоколів та портів на робочій станції.

6.8 З’ясувати, які засоби та протоколи необхідно фільтрувати.

6.9 З’ясувати вимоги до експлуатації прикладних шлюзів, необхідні для ефективного функціонування ЛОМ.

6.10 З’ясувати форму та принципи протоколювання роботи міжмережного екрану. Визначити способи виявлення типових порушень інформаційної безпеки.

6.11 Проаналізувати поточний протокол роботи міжмережного екрану. Сформулювати заходи, які необхідно реалізувати для ліквідації інцидентів.

6.13 Скласти список необхідних налаштовувань міжмережного екрану.

6.14 Визначити, які існують шляхи обходу засобів захисту і способи їх нейтралізації.

7 Опис лабораторного макета

7.1 Комплекс засобів міжмережного екрану Agnitum Outpost Firewall 2 встановлено на IBM-сумісній ПЕОМ у стандартній операційній системі MS WINDOWS XP (2000) і складається з програмної та апаратної частин.

7.2 Програмне забезпечення складається з системних драйверів та бібліотечних модулів (DLL), які виконують функції розмежування доступу, програм інтерфейсу автоматизованого робочого місця (АРМ) адміністратора, а також низка додаткових службових утиліт та динамічних бібліотек.

7.3 До апаратної частини належать спеціальні чи мережні плати, які забезпечують фізичне та логічне з'єднання ПЕОМ з апаратними засобами захищаємої мережі.

7.4 Інтерфейсна частина міжмережного екрану забезпечує організацію робочого місця адміністратора для настроювання і технічної експлуатації міжмережного екрану та керування інформаційною безпекою захищеної підмережі.

8 Порядок виконання роботи

8.1 Виконати завантаження системи Agnitum Outpost Firewall 2.

8.2 Простежити процедури ідентифікування/автентифікування користувача.

8.3 Викликати підсистему взаємодії з адміністратором, виконавши такі дії:

- завантажити АРМ адміністратора з повноваженнями головного адміністратора;
- викликати діалог "Налаштовування системи" за допомогою пункту меню "Система/Налаштовування".

8.4 Вивчити призначення пунктів меню.

8.5 Провести настроювання по прикладу правил фільтрації пакетів відповідно до політики міжмережного екрану.

8.6 Перевірити виконання режимів доступу до мережі.

8.7 Скласти план настроювань міжмережного екрану.

8.8 Прочитати та проаналізувати протокол роботи міжмережного екрану.

8.9 Скласти план реагування на інциденти з інформаційною безпекою.

9 Зміст протоколу

9.1 Структурна та функціональна схеми міжмережного екрану.

9.2 Приклад правил фільтрації пакетів.

9.3 Список необхідних настроювань та порядок настроювань міжмережного екрану.

9.4 Вибірка з протоколу роботи міжмережного екрану та результати його аналізу.

9.5 План реагування на інциденти з інформаційною безпекою.

ГЛАВА 2

МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

2.1 Дослідження політики облікових записів ОС WINDOWS XP

Настроювання безпеки авторизації користувачів.

Існує три типи політик для керування обліковими записами користувачів:

– політики паролів;

– політики блокування облікових записів;

– політики «*Kerberos*».

Налаштування політик паролів.

Політики паролів контролюють безпеку паролів і вони включають:

– вимагання неповторності паролів;

– максимальний термін дії паролів;

– мінімальний термін дії паролів;

– мінімальна довжина пароля;

– пароль повинен відповідати вимогам складності;

– зберігати паролі всіх користувачів у домені, використовуючи оборотне шифрування.

Настроювання політик блокування облікових записів користувачів.

Політики блокування облікових записів користувачів контролюють, як і коли блокуються системою домені або локальні облікові записи, а саме:

– граничне значення блокування;

– блокування облікового запису користувача та тривалість блокування;

– скидання лічильника блокування.

Настроювання політик *Kerberos*.

Kerberos, є основним механізмом перевірки дійсності, якій використовується у домені *Active Directory*. Механізм *Kerberos* використовує квитки служби й квитки користувача для ідентифікації користувачів і мережних служб. Квитки служби використовуються службовими процесами Windows, а квитки користувача користувальницькими процесами. Квитки містять зашифровані дані, що підтверджують дійсність користувача або служби.

Можливо контролювати тривалість квитка, його поновлення й застосування, використовуючи наступні політики:

– примусові обмеження входу користувачів;

– максимальний строк життя квитка служби;

– максимальний строк життя квитка користувача;

– максимальний строк життя для поновлення квитка користувача;

– максимальну погрішність синхронізації годин комп'ютера.

Настроювання безпеки доступу користувачів і груп до файлів.

Для керування доступом користувачів до папок і файлів використовується деталізована система дозволів. Для файлів і папок існує не

менш 14 дозволів NTFS, які можуть бути включені або блоковані й перевірені. Ці дозволи можна призначати файлам, директоріям, користувачам, групам. Крім того, можна призначати порядок спадкування дозволів для файлів, директорій, користувачів, груп.

Користувач не входить у безпосереднє зіткнення з яким-небудь об'єктом Windows, весь доступ до об'єктів здійснюється через програми або процеси. Програма, що звертається до ресурсів від імені користувача, виконує процедуру, що називається імперсоналізацією (*impersonation*). Програма, що звертається до вилученого ресурсу, виконує процедуру, що називається делегуванням (*delegation*).

Після реєстрації користувача його системний ідентифікатор (*System Identifier - SID*) і ідентифікатор (*Group Identifier - GID*) групи обробляються процесом lsass.exe, що генерує маркер безпечного доступу користувача. У маркер безпечного доступу вводиться й інша інформація, у тому числі про призначені користувачеві права, дозволи, ідентифікатор сеансу користувача, маску дозволів з детальним описом типу запитаного доступу. Права, призначені користувачеві, можливо побачити за допомогою команди:

WHOAMI /all

Якщо програма звертається від імені користувача до захищеного ресурсу, то монітор захисту (*security reference monitor*) Windows запитує у програми маркер безпечного доступу користувача. Потім монітор захисту аналізує маркер, щоб визначити ефективні дозволи користувача, і дозволяє або забороняє виконання запитаної користувачем операції.

Кожний із захищених об'єктів Windows, у тому числі файли, директорії, загальні ресурси, принтери, розділи реєстру, підтримують дозвіл безпеки. Будь-яку директорію Windows можна зробити загальнодоступною, щоб дозволити дистанційний доступ. Дозвіл загальнодоступності (*Share)* можна призначати будь-якому об'єкту директорії (*folder)* і прінтерів (*printer)*. Дозволи застосовуються, тільки якщо звертання до об'єкта відбувається через мережний ресурс. До дозволів директорії (*Folder Share)* ставиться повний дозвіл (*Full Control),*дозвіл на зміну *(Change),* дозвіл на перегляд *(Read).*

Якщо в Windows використовується файлова система *NTFS*, а не *FAT*, то всі файли, директорії, розділи реєстру й багато інших об'єктів мають дозвіл *NTFS*. Дозвіл *NTFS* застосовуються як при локальному, так і при дистанційному доступі до об'єкта. Для перегляду й зміни дозволів *NTFS* файлу або директорії, використовується вкладка «*Властивості*» (*Properties)* пункту «*Безпеки*» (*Security)*.

Настроювання безпеки прав доступу користувачів і груп до операційної системи Windows.

Локальна політика безпеки застосовується за допомогою розширення параметрів безпеки для групової політики. Локальна політика безпеки містить у собі дві області: політики облікових записів і локальних політиків. Політика облікових записів містить інформацію про політику паролів і політику блокування облікових записів. Область локальної політики містить інформацію про політику аудита, призначення прав користувачів і параметри безпеки.

2.2 Настроювання захисту даних комп'ютерної мережі, при використанні ОС Windows XP

Настроювання безпеки стека протоколів TCP/IP.

Щоб настроїти безпеку протоколу TCP/IP, необхідно скористатися меню «*Пуск*», у пунктах «*Настроювання*», «*Панель керування*», вибрати «*Мережа й вилучений доступ до мережі*». Вибрати інтерфейс, для якого буде настроюватися контроль вхідного доступу, вибрати команду «*Властивості*», у списку «*Відзначені компоненти використовуються цим підключенням*», вибрати елемент «*Протокол Інтернету (TCP/IP)*», «*Властивості*». У вікні «*Властивості протоколу Інтернету (TCP/IP)*» нажати кнопку «*Додатково*». Відкрити вкладку «*Параметри*». Вибрати параметр «*Фільтрація TCP/IP*» і нажати кнопку «*Властивості*». Установити прапор «*Задіяти фільтрацію TCP/IP (всі адаптери)*». Установка цього параметру, приводить до включення фільтрації для всіх адаптерів, настроювати фільтри необхідно окремо для кожного адаптера. Одні й ті ж самі фільтри не застосовуються до всіх адаптерів.

Настроювання безпеки ресурсів мережі.

Права доступу визначають повноваження окремих користувачів або груп користувачів, які перебувають в одній мережі.

Існує два способи керування доступом:

– на рівні ресурсів, коли надається доступ всім користувачам, які знають пароль;

– на рівні користувачів, коли визначаються користувачі, яким дозволений доступ до загальних ресурсів комп'ютера й надаються права.

При керуванні доступом на рівні ресурсів пароль установлюється для кожного загального ресурсу. Різним користувачам можна надати різні типи доступу: повний доступ, доступ тільки для читання або обидва типи доступу.

При другому способі керування доступом, список користувачів мережі зберігається на сервері й може бути змінений тільки адміністратором мережі. Для керування доступом на рівні користувачів комп'ютер повинен бути підключений до сервера ОС Windows або ОС NetWare. У мережах з рівноправними вузлами не можна управляти доступом на рівні користувача.

Для доступу до диска на іншому комп'ютері мережі потрібно відкрити директорію «*Мережне оточення*» (*My network places*). У цій директорії поміщені значки всіх комп'ютерів та всіх мережних принтерів, які входять в один домен і доступні в мережі на даний момент. Ця директорія, дозволяє одержати доступ, при наданні прав, до цих ресурсів мережі.

Настроювання безпеки за допомогою групової політики.

Редактор об'єктів групової політики являє собою засіб керування настроюванням користувача й комп'ютера, що входить до складу «*Каталога домену*» (*Active Directory*). До групової політики входять параметри безпеки, задані в редакторі об'єктів групової політики. Параметри безпеки постійно

зберігаються в реєстрі, у той час як параметри адміністративних шаблонів групової політики перезаписуються при кожному відновленні політики.

Редактор об'єктів групової політики використовується для редагування всіх об'єктів групової політики, у тому числі перетворених з формату майстра настроювання безпеки.

Крім створення й поширення політик безпеки за допомогою майстра настроювання безпеки, можна застосувати параметри безпеки, скориставшись шаблонами. Шаблони безпеки являють собою файли з розширенням *INF*, наприклад, *securedc.inf*, які за замовчуванням розташовані в каталозі *%systemroot%\security\templates*. Параметри шаблона безпеки в редакторі об'єктів групової політики й консолі керування груповою політикою розташовані в наступному місці: *ім'я_об'єкта_груповий_політики\ComputerConfiguration\WindowsSettings\ SecuritySettings*

Існує три способи застосування шаблонів безпеки:

– для підключення шаблона безпеки до об'єкта групової політики необхідно вибрати елемент «*Параметри безпеки*», вибрати «*Імпортувати політикиі*» і вказати місцезнаходження файлу з розширенням *INT;*

– підключити шаблон безпеки до політики майстра настроювання безпеки у вікні «*Ім'я файлу політики безпеки*» «*Включити шаблони безпеки*», нажати «*Додати*»;

– підключити шаблон до файлу політики з розширенням *XML* і виконати з командного рядка команду *scwcmd transform/p:файл_політики.xm /g:відображуване_ім'я_об'єкта_групової політики*, щоб створити об'єкт групової політики, якій можна потім зв'язати за допомогою консолі керування груповою політикою.

У середовищі, де застосовується групова політика, майстер настроювання безпеки й кілька шаблонів безпеки варто використовувати наступні рекомендації, щоб спрогнозувати пріоритетність тих або інших параметрів безпеки:

Політика безпеки, застосовувана за допомогою об'єктів групової політики *Active Directory*, має більш високий пріоритет, чим політика безпеки, застосована за допомогою файлів політики майстра настроювання безпеки (*файли XML*).

Пріоритет об'єктів групової політики по відношенню друг до друга не залежить від того, застосовувався для їхнього створення засіб scwcmd.exe чи ні. Використовуються стандартні правила спадкування Active Directory, згідно яким послідовно застосовуються об'єкти групової політики локального рівня, рівня сайту, домену й підрозділу, а також порядок прив'язки об'єктів.

Політика безпеки, задана за допомогою засобів інтерфейсу користувача майстра настроювання безпеки, має більше високий пріоритет, чим конфліктуюча політика шаблона безпеки INF-*Файлу*, підключеного до XML-*Файлу* політики.

Якщо до XML-*Файлу* підключено кілька шаблонів безпеки, шаблон, розташований вище в списку діалогового вікна «*Включення шаблонів безпеки*», має більше високий пріоритет, чим розташовані нижче.

Забезпечення безпеки за допомогою моніторингу системи.

Програма «*Перегляд подій*» використовується для перегляду подій, записаних у журналах додатків, безпеки й системи. У журналах подій засобу перегляду подій відображають відомості про неполадки встаткування, додатків і системи. Можна вести спостереження за подіями системи безпеки.

Спостереження за продуктивністю системи є важливою складовою частиною системи обслуговування й адміністрування операційною системою. Дані про продуктивність використовуються для:

– визначення завантаження системи й ефективності використання ресурсів системи;

– виявлення змін і тенденцій у робочому навантаженні й використанні ресурсів для планування майбутньої модернізації;

– перевірки змін конфігурації й інших способів настроювання;

– діагностики неполадок і кінцевих компонентів або процесів з метою оптимізації.

Компоненти «*Системний монітор*» і «*Журнали й оповіщення продуктивності*» надають докладні відомості про ресурси, використовуваних конкретними об'єктами операційної системи й програмами, призначеними для збору даних. Дані про продуктивність відображаються у вигляді діаграм. Крім того, дані записуються в журнали. Компонент «*Оповіщення*» дозволяє відправити користувачам повідомлення, коли значення лічильника досягне, перевищить або впаде нижче заданого граничного значення.

Консоль «*Продуктивність*» включає наступні засоби:

– системний монітор;

– журнали й оповіщення продуктивності;

– диспетчер завдань.

2.3 Дослідження та захист реєстру операційної системи Windows XP

У редактора реєстру є ключ */e*, що дозволяє автоматично зберігати в reg-*файлі* певний розділ реєстру. Це може знадобитися, коли потрібно зберегти настроювання певної програми, наприклад, при щоденному резервному копіюванні. Експорт може бути здійснений як з командного рядка, так і з пакетного файлу. Наступна команда зберігає ключ реєстру *HKEY_CURRENT_USER\Software\Far у файл far.reg*

regedit /e c:\far.reg HKEY_CURRENT_USER\Software\Far

У результаті роботи цієї команди з кореня диска C:\\ буде створений файл *far.reg*, що містить всі підрозділи й параметри зі значеннями зазначеного розділу реєстру. Для того, щоб відновити всі настроювання, буде досить запустити цей файл.

Для автоматизації збереження ключів реєстру можна написати пакетний файл, що буде запускатися «*Планувальником*» у певний час.

У реєстрі можуть зберігатися дані семи типів:

REG_BINARY зберігає довільні двійкові дані, без переформатування й синтаксичного розбору. Ці дані можна переглядати у двійковому або шестнадцатеричному виді за допомогою редактора реєстру.

REG_DWORD зберігає параметри, представлені восьмибайтними цілими числами. Цей тип даних звичайно застосовується, коли параметр позначає лічильник або інтервал. Ще одне його застосування як флаг (0 - флаг знят, 1 - встановлений).

REG_SZ являє собою звичайний рядок у кодуванні Unicode будь-якої довжини. В цьому типі даних зберігається інформація, яка буде читатися користувачем, шляхи доступу, назви пристроїв.

REG_EXPAND_SZ - вид REG_SZ, використовується додатками для зберігання конструкцій виду %SystemRoot%\System32, наприклад. При читанні цього рядка Windows заміняє *%SystemRoot%* на ім'я папки, куди вона встановлена.

REG_MULTI_SZ являє собою набір довільної кількості параметрів типу REG_SZ. У цьому типі даних зберігається, наприклад, список IP адрес, призначених мережному інтерфейсу.

REG_FULL_RESOURCE_DESCRIPTOR застосовується для кодування інформації про системні ресурси, необхідні для якого-небудь із пристроїв.

REG_NONE служить як семафор, тобто параметр існує, але не містить ніякого значення. Деякі додатки перевіряють наявність цього параметра й, виходячи з результату перевірки, виконують або не виконують дію.

Кореневі розділи реєстру.

HKEY_LOCAL_MACHINE (HKLM) зберігає всі настроювання, що ставляться до локального комп'ютера. У підрозділі HARDWARE зберігаються записи операційної системи й драйверів. А також спільно використовувана, поділювана інформація про фізичні пристрої, що виявляються операційною системою під час завантаження інших пристроїв *Plug-and-Play*, які можуть бути додані після завантаження операційної системи. Додатки повинні зберігати тут дані тільки в тому випадку, коли вони призначені для всіх, хто користується комп'ютером. Наприклад, драйвер принтера може зберігати набір настроювань принтера, застосовуваних за замовчуванням, і копіювати ці дані для кожного профілю користувача при вході користувача в систему.

HKEY_USERS (HKU) містить записи для кожного з користувачів, які коли-небудь входили в систему. Власником кожної із цих записів є відповідний користувальницький обліковий запис, там утримуються настроювання профілю цього користувача. Якщо використовується групова політика, то настроювання, що задаються в ній, застосовуються тут до профілів окремих користувачів.

HKEY_CURRENT_CONFIG (HKCC) зберігає інформацію про поточну завантажувальну конфігурацію комп'ютера. Зокрема, тут зберігається інформація про поточний набір системних служб і про пристрої, що були під

час завантаження. Цей кореневий розділ є покажчиком на розділ усередині *HKLM*.

HKEY_CURRENT_USER (HKCU) указує на профіль поточного користувача, що ввійшов у цей момент у систему. Microsoft вимагає, щоб додатки зберігали всі переваги користувачів у підрозділах під *HKCU*. Наприклад, *HKCU\Software\Microsoft\Windows\Current Version\Applets\Paint* містить особисті настроювання користувачів програми *Paint*.

HKEY_CLASSES_ROOT (HKCR) сопоставляє розширення файлів і ідентифікатори класів *OLE.* Фактично він указує на *HKLM\Software\Classes*. Система використовує ці відповідності щоб визначити, які додатки або компоненти потрібно використовувати при відкритті або створенні тих або інших типів файлів або об'єктів даних.

Синтаксис REG-Файлу.

Перший рядок може бути двох типів:

– *REGEDIT4* - формат reg-файлу, якій співпадає з операційними системами Windows 98/NT.

– *Windows Registry Editor Version 5.00* - указує на те, що даний файл співпадає з операційними системами Windows 2000 і вище.

Другий рядок повинен бути порожній.

Далі, необхідно вказати розділ реєстру. який являє собою шлях до параметру, який змінюється. У форматі REG-*Файлів* розділи завжди вказують у квадратних дужках.

Далі, необхідно вказати параметр реєстру і його значення. Залежно від значення параметра, змінюється поводження операційної системи або об'єкта. Багато параметрів можна настроїти в графічному інтерфейсі операційної системи, але не всі. У таких випадках для зміни параметра використовують редактори реєстру, «твікери» або REG-*файли*.

Якщо необхідно провести зміни в декількох розділах, один рядок між останнім параметром попереднього розділу й назвою наступного розділу залишається порожнім.

Всі рядки, що починаються з крапки з комою, являються коментаріями.

Значення параметрів REG-*Файлу*.

Кожному типу параметрів відповідають свої значення.

Для видалення розділу з реєстру треба перед його ім'ям у квадратних дужках поставити символ «-».

Запуск reg-файлів з командних файлів.

Якщо reg-*файли*, необхідно періодично застосовувати, можна використовувати командний bat-*файл* із рядками виду *REGEDIT /S "D:\path\filename.reg"*

Ключ */S*, (*silent)*, не виводить запит на підтвердження внесення змін до реєстру й появу повідомлення про внесення змін.

Можна скористатися командним файлом для швидкого збереження розділів реєстру в *reg-файли*. Такий командний файл повинен складатися з рядків виду:

REGEDIT /EA «D:\path\filename.reg» «HKEY_CURRENT_USER\name»

Ключ */EA, export ANSI*, означає експорт у форматі *REGEDIT4*, що має кодування *ANSI*. Якщо вказати ключ */E*, то Windows 2000/XP експортує розділи реєстру в кодуванні *UNICODE*, що створює проблеми при редагуванні reg-*файлів* редакторами, що не підтримують *UNICODE*, наприклад, стандартним блокнотом і його аналогами. Windows 95/98/Me/NT у кожному разі експортує в кодуванні *ANSI*.

2.4 Організація безпеки за допомогою утиліт, що виявляють уразливості локальної мережі

Утиліта TCPView.

TCPView – це утиліта, призначена для ОС Windows, яка виводить на екран списки кінцевих вузлів всіх установлених у системі з'єднань по протоколах *TCP* і *UDP* з докладними даними, у тому числі із вказівкою локальних і вилучених адрес і стану TCP-з*'єднань*, повідомляє ім'я процесу, якому належить кінцевий вузол. При запуску утиліта *TCPView* перераховує всі з'єднання *TCP* і *UDP*, конвертує всі IP-адреси в доменні назви.

Утиліта *TCPView* є доповненням утиліти *Netstat*, що поставляється разом з ОС Windows. Вона надає розширений набір відомостей у більш зручній формі. У комплект завантаження утиліти *TCPView* входить програма *Tcpvcon* з тими ж функціональними можливостями, але призначена для роботи в режимі командного рядка.

Сканер безпеки Xspider.

XSpider – це засіб мережного аудита, призначений для пошуку уразливостей на серверах і робочих станціях. *XSpider* дозволяє виявляти уразливості на комп'ютерах, що працюють під керуванням різних операційних систем: AIX, Solaris, Unix-Системи, Windows і інші. Програма працює під керуванням MS Windows 95/98/Millenium/NT/2000/XP/.NET.

XSpider може в автоматичному режимі перевіряти комп'ютери й сервіси в мережі на виявлення уразливості. База уразливостей постійно поповнюється фахівцями Positive Technologies. *XSpider* може виконувати перевірки за розкладом. *XSpider* виводить у звіт про результати перевірки не тільки інформацію про знайдену уразливість, але й посилання, які описують виявлену *XSpider* уразливість і дають рекомендації з її усунення. В *XSpider* версії 7, використовуються евристичні алгоритми, які не просто перебирають уразливості з бази, але й виконують додатковий аналіз по ходу роботи, виходячи з особливостей поточної ситуації. Завдяки цьому, *Xspider 7* може іноді виявити специфічну уразливість, інформація про яку ще не була опублікована.

2.5 Організація безпеки даних, при використанні засобів виявлення мережних атак

Основним призначенням утиліти *APS*, є виявлення мережних атак. Утиліта *APS* проводить обмін з атакуючим і дозволяє однозначно

ідентифікувати факт атаки, тому що після сканування портів багато сканерів роблять визначення типу сервісу шляхом передачі тестових запитів і аналізу відповіді сервера. Утиліта *APS* призначена:

– для виявлення атак сканування портів, ідентифікації сервісів, появи в мережі троянських програм, мережних хробаків. У базі *APS* більше сотні портів, використовуваних хробаками й Backdoor – компонентами;

– для тестування сканерів портів і мережної безпеки. Для перевірки роботи сканера необхідно запустити на тестовому комп'ютері *APS* і провести сканування портів, по протоколах *APS* можна встановити, які перевірки проводить сканер і в якій послідовності;

– для тестування й контролю за роботою *Firewall*. У цьому випадку утиліта *APS* запускається на комп'ютері із установленим *Firewall* і проводиться сканування портів або інших атак. Якщо *APS* видає сигнал тривоги, то це є сигналом про непрацездатність *Firewall* або про його невірне настроювання. *APS* може бути постійно запущений за захищеному за допомогою *Firewall* комп'ютері для контролю за справним функціонуванням *Firewall* у реальному часі;

– блокування роботи мережних хробаків і *Backdoor* модулів. Принцип виявлення й блокування заснований на тому, що той самий порт може бути відкритий на прослуховування тільки один раз, тому, відкриття портів, використовуваних троянськими й Backdoor програмами до їхнього запуску перешкодить їхній роботі, а після запуску приведе до виявлення факту використання порту іншою програмою;

– тестування антитроянських і антивірусних програм, систем *IDS*. У базі *APS* закладено більше сотні портів найпоширеніших троянських програм. Деякі антитроянські засоби мають здатність проводити сканування портів вузла, що перевіряється, або будувати список портів, що прослуховуються, без сканування за *допомогою* API Windows. Такі засоби повинні повідомляти про підозру на наявність троянські програми з виводом списку портів.

У переданому банері можливі макроси, які будуть замінені в момент відправлення на їхні значення. У даний момент підтримуються наступні макроси:

– *#DATE#* - заміняється на поточну дату, відформатовану відповідно до настроювань системи, формат DD.MM.YYYY;

– *#TIME#* - заміняється на поточний час, відформатоване відповідно до настроювань системи, формат HH24.MI.SS;

– *#DATETIME#* - заміняється на поточну дату й час, відформатоване відповідно до настроювань системи, формат DD.MM.YYYY HH24.MI.SS;

– *#UNIXDATE#* - дата у форматі, прийнятому в Інтернет;

– *#UNIXDATETIME#* - дату і час у форматі, прийнятому в Інтернет;

– *#RAND_BIN#* - випадкові бінарні дані випадкової довжини, мінімальна довжина блоку даних становить 50 байт, максимальна – 250;

– *#RAND_TXT#* - випадкові текстові дані випадкової довжини, мінімальна довжина блоку даних становить 50 байт, максимальна - 250. Відрізняється від *#RAND_BIN#* тим, що складається з байтів з кодами 32 – 127, текст, цифри й пробіли;

– *$xx* - байт, *xx* - значення в шеснадцатирічному форматі, для символів з кодами 0 - 9 обов'язковий попередній нуль, тобто *$00, $01* .... Застосовується для уведення в переданий текст бінарних даних, застосовується в першу чергу для передачі символів перекладу рядка й перекладу каретки ($0D і $0A).

Параметри, *#TIME#, #DATETIME#, #UNIXDATE#, #UNIXDATETIME#* застосовуються для додання відповідям *APS* реалістичності, сучфасні сканери мають інтелект і розуміють, що замість сервісу встановлена *APS*, це досягається порівнянням банерів, отриманих у результаті декількох підключень до порту. Параметри *#RAND_BIN# і #RAND_TXT#* утрудняють роботу інтелектуального сканера, тому що він намагається аналізувати отримані дані.

2.6 Організація безпеки локальної мережі при використанні утиліт, що реалізують моніторинг трафіку

Network Monitor поставляється у двох версіях: спрощеної, котра включена в ОС *Windows* і повної, що ввійшла до складу окремого продукту *Systems Management Server*. Спрощена версія може контролювати тільки локальний трафік, тобто тільки ті кадри які приймаються мережним адаптером робочої станції, що відслідковується.

Повна версія програми фіксує повністю весь трафік у мережі, при підключенні до іншого сервера або робочої станції, на яких установлений *Network Monitor* і дозволяє контролювати вилучену систему.

В утиліту *Network Monitor* входять фільтри, що дозволяють виділити спеціальну інформацію при більших мережних потоках; фільтри захвата, що вибирають із всієї захопленої інформації ту, котра необхідна; і тригери, що дозволяють системі виконувати певні дії з даними, що втримуються в пакетах.

Після запуску програми, вибирається мережа, трафік якої буде контролюватися.

Вибір мережі робиться за допомогою меню *Capture* і пункту *Networks*. У панелі, що з'явилася, відображаються всі мережні інтерфейси, які є в даному комп'ютері, мережні адаптери, COM-порти служби RAS, якщо вона встановлена на комп'ютері.

Утиліта *Iris The Network Traffic Analyzer*, крім стандартних функцій збору, фільтрації й пошуку пакетів, побудови звітів, має можливість реконструювання даних. *Iris The Network Traffic Analyzer* допомагає відтворити сеанси роботи користувачів з різними ресурсами.

Технологія реконструювання даних, реалізована в модулі дешифрування (*decode module*), яка перетворює зібрані двійкові мережні пакети у вихідний вид, розширюючи можливості наявних засобів моніторингу й аудита.

Аналізатор пакетів, дозволяє зафіксувати різні деталі атаки, такі як дата й час, IP-адреси й DNS-імена комп'ютерів зловмисника, а також використані порти.

Аналізатор пакетів, може відтворити точну, аж до натискання клавіш і рухів миші, картину вторгнення, що необхідна для усунення наслідків атаки й

посилення мер безпеки. Аналізатор пакетів дозволить підсилити захист корпоративної мережі.

2.7 Організація безпеки механізму аутентифікації, при перехопленні парольних хешей і їхньої розшифровки

Основне завдання утиліти *Cain&Abel* це відновлення паролів. Відновити можна паролі входу в систему, загальні паролі, паролі екранної заставки, паролі доступу до мережі й будь-які інші, кэшируемі в системі, у зовнішньому PWL-Файлі або в системному реєстрі. *Cain&Abel* не використовує системних уразливостей, однак має досить потужні засоби дешифрування.

Програма *Cain&Abel* за принципом дії не ставиться до мережних сканерів, але демонструє одну з методик зловмисників, використовувану для збору інформації про атакуєму систему. У результаті успішно проведеної операції, названої розроблювачами *Arp Poison Routing* (*APR*), на обрані комп'ютери впроваджують сфальсифіковані зв'язки мережних і апаратних адрес комп'ютерних систем. У результаті весь трафік між атакованими комп'ютерами починає пересилатися через систему зловмисника. Утиліта *Cain&Abel* дозволяє виступати одночасно в якості *ARP spoofer* і перехоплювача *RDP* трафіку між обраними вузлами.

2.8 Організація шифрування трафіку при використанні утиліти IPSec

Існує два режими роботи *IPSec*: транспортний і тунельний режим.

У транспортному режимі шифрується або підписується тільки інформативна частина *IP-пакета*. Маршрутизація не зачіпається, тому що заголовок *IP-пакета* не змінюється, не шифрується. Транспортний режим, як правило, використовується для встановлення з'єднання між вузлами. Він може також використовуватися між шлюзами, для захисту тунелів, організованих яким-небудь іншим способом, IP tunnel, GRE.

У тунельному режимі *IP-пакет* шифрується цілком. Для того, щоб його можна було передати по мережі він міститься в інший *IP-пакет,* це захищений *IP-тунель*. Тунельний режим може використовуватися для підключення вилучених комп'ютерів до віртуальної приватної мережі або для організації безпечної передачі даних через відкриті канали зв'язку, наприклад, Інтернет, між шлюзами для об'єднання різних частин віртуальної приватної мережі.

Режими *IPSec* не є взаємовиключними. На тому самому вузлі, можливе використання транспортного й тунельного режиму.

Шифрування даних для будь-якого додатка відбувається перед передачею їх по мережі. При пересиланні шифрованих даних клієнтським додатком з комп'ютера 1 на серверний додаток на комп'ютері 2, додатки на обох сторонах з'єднання ніяк не беруть участь у процесі шифрування. Клієнтський додаток посилає дані нижче по стеку протоколів, де вони перехоплюються протоколом *IPSec*, шифруються й потім посилаються на сервер. На сервері дані рухаються

нагору по стеку протоколів і розшифровуються *IPSec* перед їхньою передачею серверному додатку.

IPSec може виступати в якості, як служби шифрування, так і аутентифікації.

Функція забезпечення безпеки мережного трафіку за допомогою шифрування здійснюється за допомогою протоколу, називаного *ESP* (*Encapsulating Security Payload*).

Іншою функцією *IPSec* є здатність перевірки дійсності й цілісності пакетів за допомогою протоколу *AH* (*Authentication Header*). Цей протокол позначає пакети спеціальним підписом так, що одержувач може бути впевнений, що дані прийшли від справжнього відправника. Протокол забезпечує захист даних від змін при передачі, так що ніхто не міг підмінити пакети. Протокол *AH* забезпечує цілісність даних, але не робить нічого для безпеки потоку даних, якщо не використовується разом з *ESP*.

Трафік *ESP* використовує *IP-порт* 50, протокол *AH* використовує *IP-порт* 51.

Якщо два комп'ютери хочуть використовувати *IPSec* для цілей безпечної взаємодії, вони повинні бути настроєні на використання політики *IPSec*. Ці політики настроюються за допомогою локальних або групових політик ОС Windows. Політики *IPSec* повинні визначати протоколи, які потрібно захищати, визначати використання ключів, визначати механізми аутентифікації.

За замовчуванням існує три політики *IPSec*. Розташовані в директорії *\Windows Settings\Security Settings\IPSec Policies*, ці політики є відповідно політиками для *Client (Respond Only) (Клієнта – тільки відповідь), Secure Server (Require Security) (Безпечного сервера – вимагати безпека) і Server (Request Security) (Сервера – запит безпеки)*. Тільки одна політика може бути застосована до системи в даний момент часу.

2.9 Організація безпеки АРМ на базі ОС Windows XP за допомогою міжмережевого екрана Outpost Firewall

Функціональні можливості *Outpost Firewall Pro:*

– можливість настроїти обмеження мережного доступу на рівні системи й додатків;

– використання схованого режиму;

– структура програми дозволяє додавати нові захисні модулі, у вигляді фільтрів;

– програма сумісна з усіма сучасними версіями Windows;

– мінімальні вимоги до системи, на якій встановлено програму;

– можливість задавати список додатків, що мають мережний доступ, указувати діючі протоколи, порти й напрямки трафіку для кожного додатка;

– можливість блокувати або обмежувати надходження різної інформації, у тому числі рекламних банерів, спливаючих вікон на web-сторінках, зайвих даних у складі деяких web-сторінок;

– можливість обмежувати або забороняти дії активних елементів у складі web-сторінок, таких як *Java-апплеты*, *ActiveX* і *Java-скрипти;*

– повне й часткове блокування *cookies*;

– створення зони «дружніх» *IP-Адрес*, у якій, *Outpost* не буде здійснювати контроль мережної активності;

– передбачено блокування поштових вкладень із метою захисту системи від Інтернет-хробаків.

Вікно програми *Outpost Firewall* складається з наступних елементів:

– меню *Outpost Firewall;*

– панель інструментів;

– рядок подань;

– панель подань;

– інформаційна панель;

– рядок стану.

Панель інструментів складається з наступних пунктів меню:

– «*параметри*» - відкриває вікно параметрів, призначене для настроювання роботи програми;

– «*параметри*», «*політики*» - змінює політику роботи програми;

– «*вид*», «*групувати по*» - міняє порядок угруповання;

– «*вид*», «*вибрати за часом*» - обмежує відображення подій за часом;

– «*сервіс*», «*відновлення*» - перевіряє наявність відновлень модулів і компонентів *Outpost Firewall;*

– «*сервіс*», «*перегляд журналу*» - відкриває журнал і відображає фільтри.

– «*довідка*», «*контекстна довідка*» - відкриває контекстну довідку *Outpost Firewall.*

Панель представлення відображає перелік компонентів, Outpost Firewall, які призначені для охорони і містить у собі директорії «*Мій Інтернет*» і «*Підключені модулі*». Директорія «*Мій Інтернет*» містить наступні елементи:

– «*мережна активність*» - показує всі додатки й протоколи, які використовують у даний момент мережну активність;

– «*відкриті порти*» - показує відкриті порти системи;

– «*дозволені*» - показує статистику подій для всіх додатків і з'єднань, дозволених Outpost Firewall. Можна переглядати статистику фільтрації поточного сеансу роботи, дня, або всіх сеансів;

– «*заблоковані*» - показує статистику подій для всіх додатків і з'єднань, заблокованих Outpost Firewall;

– «*звіт*» - журнал подій, де зареєстровані всі спроби зазначених додатків і з'єднань до Інтернет або до локальної мережі.

Вибір політики.

Політика - це базова установка, відповідно до якої Outpost Firewall контролює мережну взаємодію комп'ютера.

Таблиця 2.1 – Опис політик

Режим	Опис
Забороняти	Всі вилучені з'єднання блокуються
Блокувати	Всі вилучені з'єднання блокуються, крім спеціально дозволеного.
Навчання	Допомагає користувачеві визначити, як додаток взаємодіє з мережею під час першого запуску
Дозволяти	Всі вилучені з'єднання дозволені, крім спеціально блокованого.
Відключити	Всі вилучені з'єднання дозволені

Фільтрація додатків.

Outpost Firewall ділить всі додатки на 3 категорії:

– «*Заборонені*» - всі робочі процеси даної групи блоковані. Рекомендується відносити до цієї групи додатки, яким не потрібне з'єднання з Інтернет.

– «*Користувальницький рівень*» - з'єднання для даної групи додатків, дозволено на основі правил, створених користувачами або за замовчуванням.

– «*Довірені*» - дозволені всі робочі процеси цих додатків.

Фільтрація системи.

Для настроювання фільтрації системи, використовується контекстне меню «*Параметри*/*Системні*». У даному меню, можна змінити:

– «*Настроювання локальної мережі*» - зміна параметрів локальної мережі, протоколу NetBIOS, діапазон довірених *IP-адрес*.

– «*ICMP*» - дозволяє призначати типи й напрямки дозволених повідомлень *ICMP*.

– «*Режими видимості*».

– «*Загальні правила*».

У програму Outpost Firewall входять наступні фільтри:

– «*Активний зміст*» - контролює діяльність наступних активних web-елементів:

– *ActiveX.*

– *Аплети Java.*

– Програми, засновані на мовах сценаріїв *Java Script* і *VBScript*.

– *Cookies*.

– Спливаючі вікна.

– *Referrers*.

– «*DNS*» - контролює взаємодію з різними сайтами.

– «*Захист файлів*» - контролює листи й поштові вкладення.

– «*Детектор атак*» - контролює спроби атак і має наступні можливості:

– «*Блокувати атакуючого на*» - блокує всі мережні запити атакуючого комп'ютера протягом зазначеного часу (за замовчуванням - 60 хвилин).

– «*Також блокувати підмережу атакуючого*» - блокує всі мережні запити підмережі, до якої належить атакуючий комп'ютер.

– *«Блокувати локальний порт, якщо виявлено DoS-Атаку»* – блокує локальний порт у випадку *DOS-атаки*.

– «*Реклама*» - блокує рекламні оголошення.

Журнал подій.

Журнал *Outpost Firewall* предоставляє історію всіх операцій, виконаних брандмауером, а саме:

– Кожний додаток або з'єднання, дозволене або блоковане *Outpost Firewall.*

– Спеціальні дії фільтрів *Outpost Firewall.*

– Початок роботи кожної програми й всі зміни політик, настроювань конфігурації й паролів.

Основними функціями журналу, є:

– Інтерфейс фільтрів, що набудовується, вибір стовпців, з обмеженням їхніх параметрів, сортування по певним параметрам.

– Настроювання відображення груп подій.

– Передбачено настроювання SQL-*Запитів* з метою моніторингу.

– Фільтри можуть переглядатися через убудовану «*Консоль керування Microsoft*» (*MMC*).

2.10 Організація безпеки мережі, при використанні ОС Unix за допомогою міжмережевого екрану IPFW

Коли пакет відповідає правилу із ключовим словом *log*, повідомлення буде зафіксовано згідно *syslogd*. Пакет, що попадає під правило, буде фіксуватися тільки за умови, що системна змінна *net.inet.ip.fw.verbose* дорівнює 1. Вона встановлена в 1 за замовчуванням, якщо ядро скомпільоване із включеною опцією *IPFIREWALL_VERBOSE.*

Правило повинно бути пов'язане з дією, що буде виконана, коли пакет збіжиться з тілом правила. Дії можуть бути:

– дозволити;

– заборонити;

– перенаправляти на зовнішній додаток;

– порахувати кількість пакетів.

Тіло правила містить нуль або більше критеріїв фільтрації, яким пакет повинен відповідати.

Критерії фільтрації – це адреса джерела й адреса призначення, порти, параметри протоколу, інтерфейс і інше. Пакет може проходити фільтр від 0 до 4 разів залежно від джерела пакета, приймача пакета й настроювань системи. Пакети можуть попадати у фільтр із декількох положень у стеку протоколів, залежно від значень системних змінних.

Після того, як пакети попадуть у фільтр, кожний з пакетів послідовно проходить за всіма правилами. Якщо критерії пакета задовольняють якому-небудь із правил, то виконується задана правилом дія й пакет залишає фільтр. Однак, залежно від настроювань системи і дій над пакетом, він може після обробки по правилу, залишається у фільтрі і продовжуватиме оброблятися.

Наприклад, після дії count, пакет продовжує оброблятися фільтром. Фільтр ipfw завжди містить правило, яке не може бути модифіковано, і яке визначає політику за замовчуванням. Це правило має номер 65535 і може бути allow або deny залежно від конфігурації ядра.

Якщо правило містить опції *keep-state* або *limit*, то для цих правил створюються тимчасові динамічні правила із вказівкою мережних адрес і портів, на яких потрібно очікувати відповідь. Таке поводження фільтра називається «*поводження зі збереженням стану*». Динамічні правила мають фіксований час життя й відкривають фільтр тільки для відповідей на вихідні запити.

Всі правила фільтра мають кілька лічильників: лічильник пакетів, лічильник байт і часу останнього проходження пакета через дане правило. Переглянути значення лічильників пакетів і час проходження останнього пакета можна командою *ipfw -at list*. Обнулити значення лічильників можна командою *ipfw zero*.

2.11 Методичні вказівки до виконання лабораторних робіт

У цьому розділі забезпечується здобуття знань і умінь виявлення та блокування витоку інформації технічними каналами. Професійні компетенції цього циклу передбачають уміння:

- кваліфіковано аналізувати інформацію, надану технічними системами, з метою виявлення типових ознак можливого несанкціонованого доступу;
- уміти зафіксувати інформацію з додержання чи порушення заходів об’єктового контролю у відповідних реєстраційних документах;

розробляти план використання наявних технічних пристроїв (прийомів або процедур) для закриття можливих каналів витоку інформації обмеженого доступу;

- проводити атестацію режимних територій в умовах додержання режиму секретності із за фіксуванням результатів у відповідних документах;
- розробляти узагальнений перелік потрібних технічних засобів;
- використовувати технічні засоби захисту інформації в умовах забезпечення режиму секретності на підприємствах, в організаціях та установах різних форм власності, уміти провести дії щодо організації технічного захисту інформації, зокрема приймати рішення про додержання чи наявність факту порушення конфіденційності інформації обмеженого доступу;
- розробляти номенклатурний перелік технічних засобів захисту інформації від витоку технічними каналами та реалізовувати технічні заходи закриття можливих каналів витоку інформації (за переліком каналів витоку);
- оцінювати ефективність систем захисту.

Лабораторна робота № 1 Дослідження політики облікових записів ОС WINDOWS XP

Ціль роботи

Вивчити методи забезпечення безпеки робочої станції під керуванням ОС Windows. Ознайомиться з основними засобами забезпечення безпеки, вбудовані в операційну систему та доступні при її налаштуванні. Навчитися налаштовувати рівні безпеки локального комп'ютера.

Ключові положення

Облікові записи користувачів дозволяють Microsoft Windows відслідковувати інформацію про користувачів і управляти їх правами доступу й привілеями. При створенні облікових записів користувача, основними засобами керування обліковими записами, є:

– Оснаска «*Користувачі й Комп'ютери Каталогу Домена»* (*Active Directory Users And Computers), яка* використовується для керування обліковими записами користувачів у межі домену.

– Оснаска «*Локальні Користувачі й Групи»* (*Local User and Groups), яка* використовується для керування обліковими записами користувачів на локальному комп'ютері.

Облікові записи Windows використовують паролі й відкриті сертифікати, щоб засвідчувати доступ до ресурсів мережі. Пароль – це чутливій до регістра рядок, якій містить до 104 символів у «*Службі каталогу Active Directory»* і до 14 символів у «*Диспетчері безпеки Windows*». Щоб уникнути неавторизованого доступу до ресурсів мережі, потрібно використовувати безпечні паролі. Різниця між звичайним і безпечним паролем полягає у тому, що безпечний пароль важко вгадати й взламати. Важким, для взлому, пароль робить комбінація всіх можливих типів символів, включаючи рядкові й заголовні букви, цифри й спеціальні символи.

Завдання до лабораторної роботи

1. Вивчити засіб настроювання аутентифікації, реалізованої при вході в операційну систему Windows. Для цього необхідно запустити утиліту «*Облікові записи користувачів*», набравши в командному рядку ім'я утиліти control userpasswords2 або з меню «*Мій комп'ютер/керування/локальні користувачі й групи*». Зробити зміни, залежно від варіанта.

2. Настроїти доступ користувачів і груп до файлів і директорій операційної системи Windows, для цього відкрити властивості директорії й вибрати вкладку «*Безпеки*» «*Security*». Зробити зміни, залежно від варіанта.

3. Настроїти розмежування прав доступу користувачів і груп до ОС Windows, за допомогою настроювання локальної політики, для цього запустити з командного рядка утиліту *secpol.msc*. Зробити зміни, залежно від варіанта.

4. Настроїти необхідні служби для роботи локального комп'ютера, відповідно до варіанта, для цього запустити утиліту *services.msc*. Перевірити

список запущених служб, за допомогою виклику з командного рядка утиліти *cmd.exe* і команди *net start*.

5. Ознайомитися з настроюванням забезпечення безпеки ОС Windows, за допомогою оснащення «*Настроювання системи*», для цього запустити з командного рядка утиліту *msconfig*. Зробити зміни, залежно від варіанта.

6. Настроїти файл завантаження системи. Для цього необхідно, залежно від варіанта, зробити зміни параметрів завантаження у файлі *C:\boot.ini*.

7. Настроїти рівні доступу в Інтернет, стандартними способами ОС Windows *Internet Explorer* (низький, середній, високий). Зробити зміни, залежно від варіанта.

8. Настроїти засоби автоматичного відновлення ОС Windows. Зробити зміни, залежно від варіанта.

9. Настроїти стандартний брандмауер ОС Windows. (низький, середній, високий). Зробити зміни, залежно від варіанта.

10. Забезпечити захист даних локальної робочої станції, за допомогою реєстру, для цього запустити утиліту *RegEdit*, і зробити зміни, залежно від варіанта.

Таблиця 1.1 – Варіанти завдань для виконання лабораторної роботи

№ вар.	**Завдання**
1	*1)* Скасувати автоматичний вхід користувача в систему.
	2) Створіть директорію *temp* і настроїти права доступу до даної директорії, таким чином, щоб користувачі, групи «*Гості*» мали права читання даних, огляду директорій, але не могли переглядати атрибути.
	3) За допомогою однієї з доступних утиліт, зупинити службу факсів, призначивши їй тип запуску: «*Вручну*».
	4) У вікні «*Автозавантаження (startup)*», утиліти *msconfig*, відключити автоматичний запуск всіх програм, крім антивірусу.
	5) За допомогою *параметра /SOS, включити* виведення на екран, список системних драйверів, які завантажуються, під час початкового завантаження системи,
2	*1)* Задати автоматичний вхід у систему, залишивши одного користувача.
	2) Створіть директорію *temp* і настройте права доступу до даної директорії, таким чином, щоб користувачі, групи «*Оператори архіву*» не мали прав читання атрибутів, запису атрибутів, читання дозволів, зміну дозволів.
	3) У вікні «*Служби (Services)*», утиліти *msconfig*, відключити служби DHCP-*Клієнта*, координатора розподілених транзакцій, службу факсів.
	4) Закрити доступ до запуску реєстру для всіх користувачів

	5) Скасуєте дію ключів */DEBUG*, для цього заборонити налагодження привілейованого режиму (ядра) під час ініціалізації, за допомогою параметра */NODEBUG.*
3	*1)* Скасуєте вимогу натискання *Ctrl+Alt+Del*, перед входом у систему.
	2) Створіть директорію *temp* і настройте права доступу до даної директорії, таким чином, щоб користувачі, групи «*Досвідчені користувачі*» мали права читання, запису, видалення файлів, але не мали право змінити дозволи і власника директорії.
	3) Задайте функцію вимоги неповторності пароля, пароль повинен відповідати вимогам складності.
	4) За допомогою однієї з доступних утиліт, зупинити *службу завантаження зображень (WIA)*, призначивши тип запуску: «*Відключене*».
	5) У вікні «*Файлу завантаження (BOOT.INI)*», утиліти *msconfig*, змінити час очікування входу в систему.
4	*1)* Задайте обмеження терміну дії пароля користувача.
	2) Створіть директорію *temp* і настройте права доступу до даної директорії, таким чином, щоб користувачі, групи «*Адміністратори*» мали повні права доступу.
	3) Задайте максимальний термін дії пароля 14 днів, мінімальну довжину пароля 8 символів.
	4) За допомогою однієї з доступних утиліт, зупинити службу *COM запису компакт-дисків IMAPI*, призначивши їй тип запуску: «*Вручну*».
	5). У вікні «*Автозавантаження (startup)*», утиліти msconfig, відключити автоматичний запуск мультимедійних програм, таких як *Winamp, RealPlayer*.
5	*1)* Дозвольте зміну пароля користувачем, додайте користувача в групу операторів настроювання мережі.
	2) Створіть директорію *temp* і настройте права доступу до даної директорії, таким чином, щоб користувачі, групи «*Оператори настроювання мережі*» не мали прав видалення інформації і її редагування.
	3) За допомогою параметра */PCILOCK,* скасуйте динамічний розподіл *IO/IRQ* для *PCI* пристроїв.
	4) У вікні «*Служби (Services)*», утиліти *msconfig*, відключіть служби диспетчера черги печатки, старт-карт, *Telnet*.
	5) Скасуйте використовувану за замовчуванням функцію ОС, що показує ім'я користувача, якій останнім входив у систему, для цього у вітці реєстру *HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System* необхідно задати наступне значення параметру *DontDisplayLastUserName:DWORD = 1*

6	*1)* Перейменуйте обліковий запис адміністратора, задайте нестандартний шлях до профілю адміністратора.
	2) Створіть директорію *temp* і настройте права доступу до даної директорії, таким чином, щоб користувачі, групи «*Користувачі вилученого робочого стола*» мали права переглядати, видаляти, створювати файли й директорії, але не могли змінити права доступу на них.
	3) За допомогою однієї з доступних утиліт, зупиніть службу доступу до HID-*Пристроїв*, призначивши їй тип запуску: «Відключене».
	4) За допомогою параметра */DEBUG*, включіть налагодження.
	5). У вікні «*Файлу завантаження* (*BOOT.INI*)», утиліти *msconfig*, змінити завантаження ОС у захищеному режимі з підтримкою мережі, за допомогою параметра *SAFEBOOT* і додаткового ключа *NETWORK*.
7	*1)* Настройте вимогу до зміни пароля користувача, при наступному вході в систему, підключіть користувача до мережного профілю.
	2) Створіть директорію «*temp*» і змініть власника даної директорії.
	3) За допомогою параметра */NUMPROC=*, визначте число процесорів, які будуть використовуватися в мультипроцесорної системі.
	4) За допомогою однієї з доступних утиліт, зупиніть службу диспетчера сеансу довідки для вилученого робочого столу, призначивши їй тип запуску: «*Вручну*».
	5) У вікні «*Автозавантаження (startup)*», утиліти *msconfig*, відключити автоматичний запуск офісних програм, наприклад *Microsoft Office TSR*.
8	*1)* Перейменуйте обліковий запис гостя. Створіть нового користувача, додайте його в групу операторів архіву.
	2) Створіть директорію «*temp*», закрийте директорію від всіх користувачів, крім групи адміністраторів.
	3) Настройте аудит відстеження процесів.
	4) У вікні «*Служби (Services)*», утиліти *msconfig*, відключити служби джерела безперебійного живлення, службу підтримки *TCP/IP NetBIOS*.
	5) За допомогою параметра */BASEVIDEO*, настройте використання стандартного *VGA* драйвера в графічному режимі.
9	*1)* Обмежте використовуваний ОС Windows обсяг пам'яті, указавши параметр *MAXMEM=16*.
	2) Настройте права доступу до локального диска *D:*\\ і застосуєте спадкування даних прав до піддиректорій.
	3) Настройте аудит успішного й невдалого доступу до служби каталогів.
	4) За допомогою однієї з доступних утиліт, запустіть службу журналів і оповіщення продуктивності, призначивши їй тип запуску: «*Авто*».

	5) У вікні «*файлу завантаження (BOOT.INI)*», утиліти *msconfig*, вкажіть, за допомогою параметра *ALTERNATESHELL*, яку графічну оболонку використовувати за замовчуванням, замість *Explorer'a.*
10	*1)* Включіть налагодження й установіть швидкість передачі даних, замість передбаченої за замовчуванням (19200), за допомогою параметра */BAUDRATE=115200*.
	2) Перегляньте діючі дозволи користувачів, що входять у групу *«Users»* на диск *D:*\\.
	*3)*Настройте аудит успішних і невдалих входів користувачів у систему.
	4) За допомогою однієї з доступних утиліт, запустіть службу тіньового копіювання тома, призначивши їй тип запуску: «*Авто*».
	5) У вікні «*Автозавантаження (startup)*», утиліти *msconfig*, відключити автоматичний запуск систем керування базами даних, таких як *Microsoft SQL Server*.
11	*1)* Настройте доступ до вилученого редагування реєстру, для групи адміністраторів домену.
	2) Створіть директорію «*temp*», настройте права доступу до даної директорії групі «*Users*», задавши право читання, перегляду й запуску файлів, тільки в даній директорії.
	*3)*Настройте заборону входу в систему, через службу терміналів.
	4) У вікні «*Служби (Services)*», утиліти *msconfig*, відключити служби планувальника завдань.
	5) За допомогою параметра */ONECPU,* укажіть використання одного процесора.
12	*1)* Настройте щомісячну зміну паролів.
	2) За допомогою параметра *SAFEBOOT* і додаткового ключа *MINIMAL* задайте завантаження ОС Windows у захищеному режимі без підтримки мережі.
	*3)*Настройте право на завершення роботи системи, тільки для групи «*Адміністратори*».
	4) За допомогою однієї з доступних утиліт, запустіть службу центра забезпечення безпеки, призначивши їй тип запуску: «*Авто*».
	5) У вікні «*Файлу завантаження (BOOT.INI)*», утиліти *msconfig*, змінити час очікування входу в систему.

Зміст протоколу

Звіти до всіх лабораторних робіт, повинні містити:
– назву теми лабораторної роботи;
– ціль лабораторної роботи;
– завдання для вашого варіанта;
– хід роботи;
– висновки.

У ході виконання лабораторної роботи, необхідно включити змінені параметри, інструмент (утиліти, команди), за допомогою яких вироблялися зміни, опис призначення кожного зміненого параметра й зроблених вами настроювань.

Контрольні питання

1. За допомогою, яких інструментів, можливе настроювання служб ОС Windows?
2. Поясніть, для чого служать відключені вами служби?
3. Поясніть призначення утиліти *msconfig*.
4. Для чого служить файл *boot.ini*?
5. Які настроювання безпеки ви можете зробити, за допомогою утиліти «*Локальні політики*»?
6. За допомогою якого інструмента можливий доступ до редагування реєстру системи? Яким чином можливо уникнути несанкціоновану або випадкову зміну реєстру, користувачами системи?
7. За допомогою якого інструмента можливо розмежувати права доступу до системного диска?
8. Яким чином можливе керування настроюванням користувачів і груп? Які вимоги безпеки існують для настроювання користувачів і груп?

Лабораторна робота № 2 Настроювання захисту даних комп'ютерної мережі, при використанні ОС Windows XP

Ціль роботи

Визначення прав доступу до ресурсів операційної системи. Настроювання правил авторизації й прав доступу до мережних об'єктів і файлової системи сімейства операційних систем Windows, для забезпечення захисту інформації. Ідентифікація комп'ютерів у мережі. Настроювання протоколів безпеки. Використання протоколів безпеки для віртуальних приватних мереж. Створення політики вилученого доступу.

Ключові положення

ОС Windows, починаючи з версії 2000, підтримує кілька методів контролю вхідного доступу. Одним з найбільш простих і одночасно самих потужних є фільтрація TCP/IP. Фільтрація TCP/IP корисна з погляду безпеки, оскільки працює в режимі ядра, у відмінності від протилежних методів контролю вхідного доступу на комп'ютери, наприклад, фільтри політики IPSec або сервер маршрутизації й вилученого доступу, які залежать від процесів режиму користувача або служби робочих станцій і серверів.

Для контролю вхідного доступу по протоколу TCP/IP може бути використана комбінована схема із застосуванням фільтрації TCP/IP, фільтрів IPSec і фільтрації пакетів маршрутизації й вилученого доступу. Такий метод особливо ефективний, якщо потрібно контролювати як вхідні, так і вихідні пакети протоколу TCP/IP. Фільтрація TCP/IP дозволяє стежити тільки за вхідним доступом.

Завдання до лабораторної роботи

1. Настроїти забезпечення безпеки стека протоколів TCP/IP, а також настроїти мережну ідентифікацію робочих станцій. Для цього в утиліті «*Властивості комп'ютера*» (*Computer Properties*), необхідно надати відомості про комп'ютер, настроївши мережне ім'я, робочу групу, опис, а також задати логічну адресу мережі, настроїти протоколи в утиліті «*Мережне оточення*» (*My network places*).

2. Настроїти *безпеку*, за допомогою додаткових вкладок в утиліті «*Мережне оточення*» (*My network places*).

3. Після виконання завдання з табл.2.1, визначте фізичну адресу мережного адаптера вашого комп'ютера і його доменне ім'я, за допомогою утиліти *cmd* і команди *ipconfig* з параметром *all*.

4. Ознайомтеся з призначенням утиліт *ping*, *tracert*, *nbtstat nslookup* і їх ключами. Перевірте мережні з'єднання, за допомогою даних утиліт.

5. Надайте користувачам мережі, доступ до ресурсів комп'ютера, забезпечивши, залежно від варіанта, необхідні політики безпеки прав доступу. Для надання прав користування файлом або принтером необхідно скористатися вкладкою «*Конфігурація*» (*Configuration*), утиліти «*Мережа*» (*Network*), де вибрати пункт «*Доступ до файлів і принтерів*» (*File And Print Sharing*). Для

надання доступу до ресурсів і настроювання керування доступом, необхідно для початку визначити, хто має право працювати з ресурсами даного комп'ютера і який рівень доступу має кожний користувач. Щоб настроїти доступ на рівні ресурсів, необхідно у вікні утиліти «*Мережа*» (*Network*) відкрити вкладку «*Керування доступом*» (*Access Control*) і включити опцію «*На рівні ресурсів*» (*Share-Level Access control)*. Щоб установити пароль і рівень доступу до певної директорії, необхідно з контекстного меню вибрати опцію «*Доступ*» (*Sharing*) і у вікні, що відкрилося, зробити необхідні настроювання. Для надання загального доступу до принтера, необхідно відкрити вікно утиліти «*Мережа*» (*Network*), вибрати вкладку «*Конфігурація*» (*Configuration*), «*Доступ до файлів і принтерів*» (*File And Print Sharing*). Щоб установити доступ до мережного принтера, необхідно відкрити папку «*Принтери*» (*Printers*), і додати мережний принтер. Для надання загального доступу до директорій, необхідно скористатися вікном «*Властивості*» (*Properties*) даної директорії, та вкладкою «*Доступ*» (*Sharing*).

Підключіть мережний ресурс, у вигляді логічного диска, для цього необхідно скористатися контекстним меню «*Властивості*» (*Properties*) у вікні «*Провідника*» (*Explorer*), вибравши команду «*Підключити мережний диск*» (*Map Network Driver*). У діалоговому вікні, що з'явиться після виконання цих команд, необхідно призначити букву логічного диска, указати шлях до підключаємого диску, і встановити опцію «*Автоматично підключати при вході в систему*», для підключення ресурсу при завантаженні ОС Windows.

6. Ознайомтесь з забезпеченням безпеки й захисту даних у мережі, за допомогою утиліти «*Групова політика*» (*Group Policy*). Ознайомтесь з організацією і призначенням функції «*Групової політики*» (*Group Policy*). Розглянете реалізацію «*Об'єктів Групової політики*» *(Group Policy objects (GPOs)*) і керування об'єктами *GPOs*, Зробіть необхідні настроювання групової політики, залежно від завдання, зазначеного у вашому варіанті. Вивчіть настроювання параметрів безпеки за допомогою даної утиліти.

7. Ознайомтеся з утилітами, що забезпечують моніторинг безпеки, за допомогою, відстеження змін локальних і мережних даних і процесів системи. Запустіть і ознайомтесь з моніторингом процесів, що працюють за допомогою утиліти «*Диспетчер завдань Windows*». Запустіть і ознайомтеся з утилітою «*Перегляд подій*» (*Event Viewer*). Запустіть і ознайомтеся з утилітою «*Продуктивність*» (*Performance*). Залежно від варіанта докладно опишіть роботу однієї з утиліт.

Таблиця 2.1 – Варіанти завдань для виконання лабораторної роботи

№ вар.	Завдання
1	*1)* Відкрийте загальний доступ до підключення Інтернет, дозволивши іншим користувачам використовувати підключення до Інтернет через мережний адаптер вашого комп'ютера, за допомогою вкладки «Властивості», «Підключення по локальній мережі».
	2) Видаліть існуючі підключення мережних дисків, за допомогою команди *net use*.
	3) У параметрах безпеки утиліти «*Групова політика*» настройте політику користувальницьких паролів, задавши максимально можливі вимоги для забезпечення безпечної аутентифікації.
	4) Опишіть призначення вкладки «*Моніторингу продуктивності системи*» утиліти «*Диспетчер завдань Windows*», з поясненням представлених у ній значень.
2	*1)* Настройте Ір-ідресу вашої робочої станції, укажіть маску підмережі класу В, а також вкажіть шлюз сервера, за допомогою якого ви підключаєтеся до Інтернет.
	2) Задайте підключення мережних дисків, за допомогою команди *net use*.
	3) У параметрах безпеки утиліти «*Групова політика*» настройте політику аудита, відповідно до вимог забезпечення безпеки в мережі.
	4) Змініть пріоритет запущених процесів у вкладці «*Процеси*», утиліти «*Диспетчер завдань Windows*». Приведіть приклад необхідності такої зміни.
3	*1)* Задайте адреси DNS і WINS сервера в домен вашої мережі.
	2) Відкрийте права доступу на принтер, підключений до вашого комп'ютера, для загального користування певними групами домену, у який входить ваш комп'ютер.
	3) У параметрах безпеки утиліти «*Групова політика*» настройте політику прав користувачів, вказавши обмеження на локальний вхід у систему, для груп, що не використовують дану робочу станцію. А також забороніть всім групам, крім адміністраторів входити через службу терміналів.
	4) Запустіть оснащення «*Перегляд подій*» із групи «*Адміністрування*», «*Панель керування*». Опишіть призначення значень вікна оснащення вкладок «*Загальні*» і «*Фільтр*».
4	*1)* Настройте статичну мережну IP-адресу вашого комп'ютера, настройте використання фільтрації TCP/IP, указавши порт ftp, як дозволений трафік.
	2) Додайте мережний принтер, щоб надалі користуватися даним ресурсом.

	3) У параметрах безпеки утиліти «*Групова політика*» настройте політику прав користувачів, вказавши групи для доступу до комп'ютера з мережі й права для груп, що можуть здійснювати завершення роботи системи.
	4). Запустіть оснащення «*Перегляд подій*» із групи «*Адміністрування*», «*Панель керування*». Створіть новий вид журналу, задавши потрібний вид стовпців, фільтра, спосіб сортування.
5	*1)* Використовуючи правила фільтрації стека протоколів TCP/IP, заблокуйте весь вхідний трафік, за винятком порту TCP 80 для http і для протоколу захищених сокетів (SSL), указавши порт 443.
	2) Задайте загальний доступ до диска на вашій робочій станції, тільки для груп домену, у якому перебуває ваш комп'ютер.
	3) У параметрах безпеки утиліти «*Групова політика*» настройте політику прав користувачів, вказавши групу, що має право здійснювати
	4) Приведіть опис дій, необхідний для перегляду подій на іншому комп'ютері.
6	*1)* Настройте стек протоколів TCP/IP на динамічну адресацію, за допомогою вкладки «Загальні», для підключення по локальній мережі, «Властивостей TCP/IP», вибравши опцію «Одержати IP-Адресу автоматично».
	2) На одному з комп'ютерів мережі перебуває директорія, з якої ви працюєте досить часто. Підключіть цю директорію до свого комп'ютера як логічний диск.
	3) У параметрах безпеки утиліти «*Групова політика*» настройте локальну політику безпеки, визначивши необхідні параметри для інтерактивного входу в систему.
	4) Приведіть перелік опцій, доступних для фільтрації журналів подій.
7	*1)* Перегляньте таблицю IP маршрутизації, за допомогою команди *route print.* Опишіть результат роботи утиліти в протоколі.
	2) Настройте управління доступом до ресурсів для персоналу відділу виробництва.
	3) У параметрах безпеки утиліти «*Групова політика*» настройте локальну політику безпеки, визначивши необхідні параметри для цифрового підпису.
	4) Опишіть, що являє собою оснащення *«Продуктивність (Performance)».* Опишіть призначення «*Системного монітора (System monitor)*» і «*Журналу продуктивності (Performance Logs and Alerts)*».
8	*1)* За допомогою вкладки «Перевірка дійсності» установіть настроювання, щоб виконати перевірку дійсності в мережі, якщо відомості про користувача й комп'ютер недоступні. Також настройте перевірку дійсності у гостя при неприступності відомостей про комп'ютер.

	2) Настройте управління доступу до ресурсів мережі для персоналу відділу маркетингу.
	3) У параметрах безпеки утиліти «*Групова політика*» настройте локальну політику безпеки, визначивши необхідні параметри для мережної безпеки.
	4) Приведіть список параметрів, які дає можливість переглядати утиліта «*Системного монітора» (System monitor)*.
9	*1)* Додайте статичний IP-маршрут, за допомогою наступного командного рядка: *route_add_призначення_mask_маска_підмережі_шлюз_metric_вартість _if_інтерфейс*. Де шлюз – це IP-Адреса або ім'я вузла шлюзу або маршрутизатора, використовуваного для перенапрямку. (Наприклад, *route add 10.0.0.0 mask 255.0.0.0 192.168.0.1 metric 2*)
	2) Настройте управління доступом до ресурсів для персоналу відділу закупівель.
	3) У параметрах безпеки утиліти «*Групова політика*» настройте локальну політику безпеки, визначивши необхідні параметри безпеки пристроїв.
	4) Перелічте об'єкти, які найбільше часто використовуються для відстеження роботи системних компонентів, утилітою «*Системного монітора» (System monitor)*.
10	*1)* Використовуйте правила фільтрації стека протоколів TCP/IP, для блокування всього вхідного трафіку, за винятком telnet .
	2) Визначте результуючі дозволи на права доступу до директорії. Перегляньте всі мережні диски, підключені до вашої робочої станції, за допомогою команди *net use*.
	3) У параметрах безпеки утиліти «*Групова політика*» настройте локальну політику безпеки, визначивши необхідні параметри безпеки для .облікових записів і членів домену.
	4) Опишіть процес вибору частоти реєстрації, методу моніторингу та процес вибору комп'ютера, якій буде використаний для моніторингу, за допомогою утиліти «*Системного монітора» (System monitor)*.
11	*1)* Настройте параметри служби NetBIOS, за допомогою вкладки «*Додаткові параметри TCP/IP*», включивши NetBIOS через порт TCP/IP за замовчуванням.
	2) Підключіть мережний диск D:\\, що перебуває на робочій станції вашого сусіда.
	3). У параметрах безпеки утиліти «*Групова політика*» настройте політику безпечної конфігурації операційної системи Windows.
	4) Перелічите можливості оснащення «Оповіщення журналу продуктивності» (Performance Logs and Alerts) .

12	*1)* За допомогою вкладки «*Підключення по локальній мережі*», настройте параметри брандмауера Windows, заборонивши дистанційне керування робочим столом.
	*2)*Змініть права доступу до будь-якої директорії. Сформуйте на своєму комп'ютері каталог з декількома файлами. Надайте ці файли для загального використання з різним рівнем доступу.
	3) У параметрах безпеки утиліти «*Групова політика*» настройте профілі користувачів, сценарії входу в систему, можливості Ctrl+Alt+Del.
	4) Використовуйте оснащення «Оповіщення журналу продуктивності» (Performance Logs and Alerts), для створення нових журналів лічильника, трасування, оповіщення.

Зміст протоколу

У звіт необхідно включити опис зроблених вами настроювань безпеки протоколу TCP/IP, з поясненням призначення даних настроювань. Включіть опис настроювань безпеки локальних і мережних ресурсів робочих станцій.

Залежно від завдання у вашому варіанті, включіть докладний опис реалізованих вами політик безпеки, заданих в утиліті «*Групові політики» (Group policy)*, з поясненням необхідності пророблених вами настроювань.

Залежно від завдання у вашому варіанті, опишіть одну з утиліт моніторингу.

Контрольні питання

1. Як надати іншим користувачам доступ до ресурсів вашого комп'ютера?
2. Як настроїти керування доступом на рівні ресурсів?
3. Як знайти потрібний ресурс у мережі?
4. Як створити логічний диск?
5. Як підключити мережний принтер?
6. Вам необхідно подивитися файл презентації, над яким ви працювали на іншому комп'ютері. Яким чином, можливо знайти цей файл? Опишіть способи знаходження мережного ресурсу.
7. Для чого потрібні утиліти *ping*, *tracert*, *nslookup*? У яких випадках, пов'язаних з безпекою мережі, можливе використання цих утиліт?
8. Які рівні безпеки, дозволяє настроїти утиліта «*Групові політики» (Group Policy)?*
9. Опишіть призначення й функціональні можливості вкладок меню «*Панель керування» (Control Panel*), «*Мережа» (Network)*, «*Протоколи TCP/IP*».
10. Опишіть призначення служб Wins, DHCP, DNS.
11. Опишіть які зміни в систем ви можете спостерігати, з використанням утиліт моніторингу.

Лабораторна робота № 3 Дослідження та захист реєстру операційної системи Windows XP

Ціль роботи

Вивчити на практиці автоматизоване створення реєстрових програм - скриптів формату .reg, для створення механізмів, забезпечення безпеки робочої станції й серверів комп'ютерної мережі. Вивчити роботу утиліти RegSnap. Вивчити параметри командного рядка редактора реєстру RegEdit.

Ключові положення

Reg-файл це текстовий файл певної структури з розширенням reg, що містить ключі реєстру й служить для швидкого керування ключами реєстру. За допомогою reg-файлу можна видаляти, створювати ключі реєстру й параметри з певними значеннями.

Reg-файли можливо створювати вручну або скористатися експортом з реєстру. Щоб експортувати ключ, необхідно відкрити редактор реєстру, виділити ключ, що буде експортуватися й вибрати «*Реєстр - Експорт файлу реєстру*». У зазначеному місці буде створений файл, що має розширення *reg*. Завдяки тому, що розширення, асоційовано з редактором реєстру, запуск цього файлу приведе до того, що він буде оброблений редактором. Буде виданий запит на підтвердження додавання інформації з файлу до реєстру й після підтвердження інформація буде додана.

Завдання до лабораторної роботи

1. Створіть текстовий файл, у який внесіть, задані у вашому варіанті настроювання реєстру. Збережіть файл, з розширенням *REG*.

2. Запустіть файл настроювання реєстру, перевірте роботу внесених вами змін.

3. Внесіть до протоколу текст файлу.

Таблиця 3.1 – Варіанти завдань для виконання лабораторної роботи

№ вар.	Завдання, для створення REG-Файлу
1	Обмежте запуск програм, змінивши розділ *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows \CurrentVerson\Policies\Explorer* реєстру, і створивши ключ *RestrictRun* типу *DWORD* зі значенням 0x00000001, перелічивши список дозволених до запуску програм.
2	Забезпечте блокування системи від стороннього втручання, заборонивши запуск користувачам редактора реєстру. Для цього в розділі реєстру *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows \CurrentVerson\Policies\System* змініть значення ключа *DisableRegistryTools* на одиницю.
3	Установіть мінімальну кількість символів у паролях більше 8. Для цього, призначте параметру *MinPwdLen*, значення *hex*:8, у розділі реєстру *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion \Policies\Network.*

4	Забороніть користувачам можливість перезавантаження системи, не виконуючи вхід у систему. Для цього, призначте параметру *ShutdownWithoutLogon* значення рівне нулю, у розділі реєстру *HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion \Winlogon.*
5	Забороніть користувачам можливість запуску «Диспетчера завдань Windows» (*Task Manager*). Для цього, призначте параметру *DisableTaskMgr* типу *DWORD*, значення рівне одиниці, у розділі *HKEY_CURRENT_USER\Software\Microsoft\Windows \CurrentVersion\Policies\System.*
6	Забороніть користувачам режим командного рядка (*cmd.exe*) і обробку bat-*файлів*. Для цього, призначте параметру *DisableCMD*, типу *DWORD*, значення 2., у розділі реєстру *HKEY_CURRENT_USER\Software\Policies\Microsoft \Windows\System.*
7	Відключте на вашім комп'ютері, загальні ресурси, задані за замовчуванням, такі як *admin$, c$*. Для цього призначте параметру *AutoShareWks*, типу - *REG_DWORD*, значення нуль, у розділі реєстру *HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer \Parameters.*
8	Задайте опцію вимоги від користувачів комбінувати при складанні пароля букви й цифри. Для цього, призначте параметру *AlphanumPwds*, значення рівне одиниці, у розділі реєстру *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows \CurrentVersion\Policies\Network*.
9	Забороніть можливість видалення й перейменування контекстного меню, кнопки «*Пуск*» (*Start*), а також переміщення пунктів меню методом *drag-n-drop.* Для цього, призначте параметру *NoChangeStartMenu*, типу *DWORD* значення рівне одиниці, у розділі *HKEY_CURRENT_USER\Software\Microsoft\Windows \CurrentVersion\Policies\Explorer.*
10	Забороніть анонімний доступ на ваш комп'ютер користувачам з мережі, при цьому забороніть перегляд облікових записів і загальних ресурсів. Для цього, у розділі реєстру *HKLM\System\CurrentControlSet\ Control\Lsa* призначте параметру *Restrictanonymous*, типу *REG_DWORD*, значення рівне одиниці.
11	Очистіть файл *PageFile - HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Control\ Session Manager\ Memory Management* - привласнивши значення 1 параметру *ClearPageFileAtShutdown*, активуючи можливість видаляти при завершенні роботи всі дані, які могли зберегтися в системному файлі, а також автоматичне видалення трешевих файлів після роботи в мережі Інтернет, за допомогою *HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Internet Settings\ Cache* - привласнивши 0 значенню *Persistent*.
12	Видаліть пункт «*Завершення роботи»* (*Shutdown*) з меню «*Пуск*» (*Start*), а також забороніть можливість завершення роботи системи, за допомогою кнопок *Ctrl+Alt+Del.* Для цього, призначте параметру *NoClose* типу *DWORD* значення, рівне одиниці, у розділі *HKEY_CURRENT_USER\Software\Microsoft\Windows \CurrentVersion\Policies\Explorer.*

Зміст протоколу

У звіт необхідно внести текст reg-файлу, з докладним описом інструкцій.

Контрольні питання

1. Опишіть призначення основних розділів реєстру.
2. Перелічте й поясніть призначення типів даних реєстру.
3. Яким чином, здійснюється запуск reg-файлів з командних файлів.
4. Опишіть структуру й синтаксис reg-файлів.
5. Опишіть призначення й функціональні можливості reg-файлів.

Лабораторна робота № 4 Організація безпеки за допомогою утиліт, що виявляють уразливості локальної мережі

Ціль роботи

Вивчити методи захисту мережі. Навчиться здійснювати моніторинг існуючих мережних з'єднань і відкритих портів у комп'ютерній мережі за допомогою утиліт *TCPView* і *XSpider*, під керуванням операційної системи сімейства Windows.

Ключові положення

TCPView - це утиліта, призначена для ОС Windows, яка виводить на екран списки кінцевих вузлів всіх установлених у системі з'єднань по протоколах *TCP* і *UDP* з докладними даними, у тому числі із вказівкою локальних і вилучених адрес і стану TCP-з*'єднань*, повідомляє ім'я процесу, якому належить кінцевий вузол. При запуску утиліта *TCPView* перераховує всі з'єднання *TCP* і *UDP*, конвертує всі IP-адреси в доменні назви.

XSpider – це засіб мережного аудита, призначений для пошуку уразливостей на серверах і робочих станціях. *XSpider* дозволяє виявляти уразливості на комп'ютерах, що працюють під керуванням різних операційних систем: AIX, Solaris, Unix-Системи, Windows і інші. Програма працює під керуванням MS Windows 95/98/Millenium/NT/2000/XP/.NET.

Завдання до лабораторної роботи

1. Відкрийте утиліту *TCPView*. При запуску, ви побачите список всіх активних кінцевих вузлів з'єднань по протоколах *TCP* і *UDP*. Ознайомтеся з основними пунктами меню. Змініть період відновлення інформації, за допомогою пункту «*Період відновлення» (Refresh Rate»* у меню «*Параметри» (Options)*. Якщо в період між відновленнями стан кінцевих вузлів мережі змінився, вони виділяються жовтим кольором, якщо вузол не знайден, то червоним кольором, нові вузли мережі, відображаються зеленим кольором.

2. Занесіть до протоколу результати сканування відкритих з'єднань.

3. Закрийте встановлені підключення по протоколах *TCP/IP,* з станом «*Установлене» (ESTABLISHED)*, за допомогою пункту «*Закрити підключення» (Close Connections)* у меню «*Файл» (File).* Закрийте утиліту *TCPView*.

4. Відкрийте утиліту *XSpider*. Вивчіть основні пункти меню, скориставшись документацією з меню «*Довідка*».

5. Сформуйте завдання для сканування, для цього створіть нове робоче вікно *XSpider* і додайте список робочих станцій. Для цього виберіть команду меню «*Виправлення/Додати*». У з'явившомуся вікні, *задайте IP-адресу*, імена або діапазон комп'ютерів, заданих у табл. 4.1. Обмежте одночасне сканування, тільки для 2 робочих станцій.

6. Створіть свій профіль сканування, для цього виберіть пункти «*Профіль*», «*Створення нового профілю*». Визначте набір настроювань для сканування, виходячи з даних табл.4.1. Для цього в діалозі, що з'явився, у

дереві настроювань виберіть пункт *«Сканер уразивостей/Визначення уразливостей»*. Збережіть створені вами завдання.

7. Запустіть сканування. Для цього виберіть відповідну команду з меню «*Сканування*».

8. Перескануйте окремі сервіси. Це може знадобитися в деяких особливих ситуаціях, наприклад, для підтвердження наявності DoS-уразливості. Іноді, при поганій якості зв'язку з перевіряється можливе помилкове визначення DoS-уразливості, коли зв'язок з вузлом перервався випадково, а *XSpider* зробив вивід, що пройшла DoS-атака. У цьому випадку можна провести повторне сканування відповідного сервісу й при повторному виявленні уразливості більш упевнено зробити вивід про її наявність.

9. Заплануйте запуск вашого завдання, за допомогою планувальника. Для цього, викличте з меню «*Розклад/Створити*» майстер створення розкладу. Виберіть ваше завдання для автоматизації зі списку, збережених завдань у директорії *Tasks*. або натисніть «*Огляд*», якщо потрібне завдання перебуває не в директорії *Tasks*. Виберіть інтервал періодичності перевірок, інтервал, протягом якого створюваний розклад буде активним. Задайте автоматичну генерацію й параметри звіту після кожного автоматичного виконання завдання.

10. По результатам кожного сканування, згенеруйте звіт про поточне сканування. Для цього виберіть команду з меню «*Сервіс/Створити звіт*», у вікні «*Майстер створення звіту*». Виберіть формат звіту. *RTF*, потім виберіть варіант звіту.

11. Проаналізуйте результати сканування вашого завдання. Занесіть до протоколу результат сканування.

12. Занесіть до протоколу порівняльну характеристику, отриманих вами результатів за допомогою утиліт *TCPView* і *XSpider.*

Таблиця 4.1 – Варіанти завдань для виконання лабораторної роботи

№ вар.	**Завдання для сканування**	**Параметри профілю**
1	172.16.1.11, Inet-2, Inet-5	Вам необхідно перевірити мережу на уразливість в «*безпечному*» режимі, без DoS-атак, у мережі немає сервера баз даних.
2	172.16.1.66, Inet-3, Inet-4	Вам необхідно перевірити мережу на уразливість нових DoS-атак, за допомогою евристичного методу.
3	З 172.16.1.8 по 172.16.1.10	Вам необхідно перевірити мережу на уразливість, за допомогою аналізатора скриптів, включивши складну перевірку всіх скриптів.
4	172.16.1.33, Inet-7, Inet-10	Вам необхідно перевірити мережу на уразливість протоколів, для передачі/прийому пошти, використовуючи розширені словники логинів і паролів.
5	172.16.1.77, Inet-1, Inet-6	Вам необхідно перевірити мережу на уразливість, збільшивши час пошуку одного вузла до 5 секунд.
6	172.16.1.44, Inet-5, Inet-8	Вам необхідно перевірити мережу на уразливість, використовуючи весь діапазон портів, з 1 по 65535.

7	172.16.1.55, Inet-2, Inet-9	Вам необхідно перевірити мережу на уразливість, визначаючи операційну систему вузлів, за допомогою *Nmap*.
8	З 172.16.1.5 по 172.16.1.8	Вам необхідно перевірити мережу на уразливість у полях запиту Cookie.
9	172.16.1.99, Inet-1, Inet-4	Вам необхідно перевірити мережу на уразливість, збільшивши кількість директорій, що перевіряються, на підбір пароля, до 10.
10	172.16.1.88, Inet-7, Inet-6	Вам необхідно перевірити мережу на уразливість, якщо у вашій мережі немає поштового й ftp сервера, немає СУБД. Для прискорення роботи утиліти, відключіть невикористовувані параметри.
11	З 172.16.1.1 по 172.16.1.5	Вам необхідно перевірити мережу на уразливість, збільшивши кількість потоків для пошуку до 100.
12	172.16.1.22, Inet- 3, Inet-9	Вам необхідно перевірити мережу на уразливість, збільшивши час очікування сканування портів.

Зміст протоколу

До протоколу внести звіт, докладно інформацію про всі робочі станції, сервіси, уразливості, які було скановано. Також потрібен звіт про статистику і перелік виявлених уразливостей, звіт про перелік виявлених портів і сервісів для кожного вузла, звіт про угруповання вузлів, із сортуванням по убуванню небезпек, звіт про угруповання по уразливостям, із сортуванням по убуванню небезпеки. Діаграму по історії скануванні завдання.

Зробіть вивід про продуктивність розглянутих вами утиліт, з погляду забезпечення безпеки в локальних комп'ютерних мережах.

Контрольні питання

1. Поясните призначення утиліт *TCPView* і *XSpider.* У чому полягає принципова відмінність даних утиліт?
2. При яких факторах можливе перевантаження каналу утиліти *XSpider*? Яким чином можна боротися з даним перевантаженням?
3. Призначивши для кожного завдання певний розклад роботи, які переваги ви одержуєте?
4. Для чого бажано задати інтервал, протягом якого створюваний автоматичний розклад буде активним?
5. Які типи уразливостей можливо виявити, за допомогою утиліти *XSpider*?
6. За портами яких мережних служб, ведеться спостереження, за допомогою, сканера безпеки *XSpider*?
7. Поясните призначення сервісу «*Перевизначення уразливості*».
8. Де зберігається, за замовчуванням файл портів утиліти *XSpider* і яким чином ви можете настроїти сканування тільки по певних портів?
9. Поясніть поняття евристичних методів пошуку уразливостей. У чому перевага даного методу?
10. Яким чином, можливо автоматизувати роботу утиліти *XSpider?*

Лабораторна робота № 5 Організація безпеки даних, при використанні засобів виявлення мережних атак

Ціль роботи

Вивчити принцип роботи засобу виявлення мережних атак і сканерів портів (сніфферів) у комп'ютерній мережі, на прикладі утиліти *APS*.

Ключові положення

Програма відкриває описані в базі дані порти й працює в режимі, що чекає, виходячи з нього тільки в моменти звертання до порту, що прослухується. Це відрізняє *APS від* Firewall, якій аналізує кожний пакет, якій приходить з мережі. У такий спосіб *APS*, споживає малу кількість ресурсів, не навантажує процесор, та практично не використовує системні ресурси.

Принцип роботи програми заснований на прослуховуванні портів, описаних у базі даних. Якщо адміністраторові відомий порт, використовуваний троянської або *Backdoor* програмою, існує можливість створити користувальницьку базу даних. При виявленні спроби підключення до порту, що прослуховується, програма фіксує факт підключення в протоколі, аналізує отримані після підключення дані й для деяких сервісів передає так званий банер, деякий набір текстових або бінарних даних, переданих реальним сервісом після підключення.

Завдання до лабораторної роботи

1. Запустіть сканер портів *XSpider* на сканування сусідніх робочих станцій з виявленням можливості *DoS* атак.

2. Запустіть утиліту *APS*, для виявлення факту сканування портів по протоколах *TCP, UDP* і розсилання *UDP broadcast* пакетів для заданих портів.

3. Настройте утиліту *APS.* Для цього з пункту меню «*Сервіс/Настроювання*» викличте діалогове вікно «*Настроювання*».

4. Відкрийте вкладку «*Загальні настроювання*», категорію «*Інтерфейс*». Ознайомтесь з можливостями даного меню. Відключіть перемикач звукового сигналу при виявленні атаки й задайте опцію розкриття вікна, при виявлені атаки. Включіть перемикач «*Сортування списку портів після їхнього завантаження*», для автоматичного сортування бази портів по номеру порту. Задайте автоматичне стартування програми, при старті системи.

5. Відкрийте вкладки «*Оповіщення*», «*Звіти*», «*Протоколювання*», призначені, відповідно, для настроювання оповіщення адміністраторів по мережі, що ведеться за допомогою відправлення повідомлень на *mailslot* з ім'ям «*messngr*» і є аналогом виконання команди *NET SEND*, для настроювання передачі інформації службі *SysLog* серверів, для передачі звітів по електронній пошті, для настроювання системи протоколювання утиліти. Ознайомтесь з можливостями даного меню. Зробіть настроювання, відповідно до завдання, наведеному у табл.5.1.

6. Для зміни состава інформації повідомлень і листів, що відправляються утилітою *APS,* створіть шаблон, що формує звіт у форматі *XML,* з необхідними для вас даними; шаблон, що формує мінімальний по обсязі звіт для відправлення по *SMS,* з необхідними для вас даними; шаблон, що формує таблицю *CSV* формату для аналізу в *Excel,* з необхідними для вас даними. Шаблони зберігається в текстовому файлі з розширенням *etf* у директорії *template*. Формат шаблона:

[Info]
Name=назва шаблона
[Header]
...
[Footer]
...
[HackerInfo]
...
[HackerPortInfo]
...

Додаткові відомості про параметри секцій шаблона:

Секція *Info* містить обов'язковий параметр *Name=<назва шаблона>* і параметр *MaxRecCount*, що задає максимальну кількість записів, виведених у лист. Секції *Header* і *Footer* містять дані, однократно виведені на початку й наприкінці листа. У цих секціях крім довільного тексту припустимі макроси, замінні в момент генерації листи значеннями, ці макроси припустимі в будь-якій секції: *#VERSION#,* версія програми; *#DB_VERSION#,* дата відновлення й версія бази портів; *#TIME#,* час формування листа; *#LOCAL_IP#, IP адреса* комп'ютера, на якому спрацював *APS; #LOCAL_HOST#,* ім'я комп'ютера, на якому спрацював *APS*. Секція *HackerInfo* містить шаблон, по якому формуються дані по кожному з атакуючих вузлів. У цій секції припустимі макроси, замінні в момент генерації листи значеннями: *#HACKER_IP#, IP адреса* атакуючого комп'ютера; *#HACKER_HOST#,* ім'я вузла для атакуючого *IP; #ATTACK_START_DATE#,* дата початку атаки; *#ATTACK_START_TIME#,* час початку атаки; *#ATTACK_END_DATE#,* дата завершення атаки; *#ATTACK_END_TIME#,* час завершення атаки; *#ATTACK_COUNT#,* кількість атак; *#ATTACK_DOS_COUNT#,* кількість підозр *DoS*; *#ATTACK_PORT_COUNT#,* кількість атакованих портів; *#ATTACK_PORT_COUNT#,* кількість атакованих портів; *#ATTACK_PORT_DETAIL#,* деталізовані дані про порти; *#ATTACK_EXPRESS_TEST#,* результати експрес-оцінки, чи є *DoS, Flood*, сканування, виводиться в текстовому виді в три рядки. Секція *HackerInfo* містить шаблон, по якому формуються дані по кожному з атакованих портів. У цій секції припустимі макроси, замінні в момент генерації листи значеннями: *#HACKER_IP#, IP адреса* атакуючого комп'ютера; *#HACKER_HOST#,* ім'я вузла для атакуючого *IP; #PORT_NUM#,* номер порту; *#PORT_PROTO#,* протокол *TCP* або *UDP*; *#PORT_ATTACK_COUNT#,* кількість атак по даному порту; *#PORT_DOS_COUNT#,* кількість підозр *DoS* по даному порту;

#PORT_DATA_SIZE#, обсяг даних, отриманих по даному порту від атакуючих; *#PORT_FLOOD_INFO#,* ознака флуда в текстовому виді.

7. Натисніть кнопку «*Тестувати настроювання*», для тестування вірного настроювання відправлення оповіщень по мережі. При натисканні на цю кнопку програма відправить тестове повідомлення відповідно до поточних настроювань.

8. Відкрийте вкладку «*Імітація сервісів*», для настроювання системи імітації сервісів *TCP*. Ознайомтесь з можливостями даного меню. Зробіть настроювання, відповідно до завдання, наведеним у табл.5.1. Зробіть настроювання імітації сервісів *UDP*, настроївши передачу випадкових даних замість відгуку з бази даних.

9. Відкрийте вкладку «*Редагування користувальницької бази портів*». Ознайомтесь з можливостями функцій, представлених у вікні редактора бази портів. У стовпці «*Переданий текст*» утримується текст банера. Задана в цьому полі інформація передається атакуючому вузлу після підключення до порту. Ознайомтесь з призначенням динамічних елементів, що втримуються, у даному стовпці.

10. Після настроювання утиліти *APS*, запустіть її знову й переконаєтеся, що настроювання утиліти працюють.

Таблиця 5.1 – **Варіанти завдань для виконання лабораторної роботи**

№ вар.	**Настроювання параметрів звітів, оповіщень, протоколювання системи *APS***	**Настроювання параметрів імітації сервісів**
1	Включіть перемикач «*Використовувати оповіщення по мережі NET SEND*», для активування режиму оповіщення по мережі. Заповніть поле «*ПК адміністраторів*», включивши імена *NetBios* комп'ютерів адміністраторів	Задайте, дії утиліти *APS* при з'єднанні з атакуючим портом, для передачі відгуку з бази даних *APS* атакуючому.
2	Дозвольте доступ до убудованого *Web* серверу формувача звітів з IP-*Адрес* сусідніх комп'ютерів	Виключіть систему імітації, для того, щоб не проводити активної взаємодії з атакуючим і негайно розривати з'єднання з ним.
3	Включіть перемикач «*Використовувати запис в Syslog на зазначених серверах*», для керування режимом відправлення інформації служби *Syslog*. Занесіть у поле «*Адреси серверів*», список *IP адрес* серверів мережі	Задайте, дії утиліти *APS* при з'єднанні з атакуючим портом, для передачі відгуку атакуючому з бази даних *APS*, плюс блок даних змінної довжини, від 100 до 500 байт, заповненого випадковими даними.
4	Настройте режим відправлення звіту по електронній пошті.	Настройте дії програми після обміну з атакуючим, утримуючи з'єднання відкритим при відсут-

		ності *Flood* і розриваючи, при його наявності, поріг становить більше 60 підключень у хвилину.
5	Настройте оповіщення «*тривоги*» по електронній пошті.	Настройте передачу відгуку, із заданої, за допомогою регулятора ймовірністю, щоб внести додатковий фактор випадковості й спотворити результати сканування.
6	Задайте відправлення повідомлення для кожної події.	Настройте дії програми після обміну з атакуючим, розриваючи з'єднання, після обміну з атакуючим з ініціативи утиліти *APS*.
7	Настройте пункт меню «*Оповіщення*», таким чином, щоб адміністратор, одержував повідомлення від програми, тільки на локальному комп'ютері.	Включите режим утримання з'єднання, для втримання з'єднання з атакуючим, що сповільнить роботу деяких сканерів мережної безпеки.
8	Включіть перемикач «*Розкривати вікно програми при виявленні атаки*», для автоматичного відображення головного вікна програми, при виявленні спроби сканування портів.	Настройте дії *APS* при з'єднанні з атакуючим портом, таким чином, щоб атакуючому передавався буфер, заповнений випадковими байтами.
9	Настройте деталізацію листів, указавши відправлення списку атакуючих і даних про порти.	Настройте дії *APS* при з'єднанні з атакуючим портом, для передачі текстового рядка, заповненого випадковими символами.
10	Задайте правила іменування й ротації протоколів.	Настройте дії програми після обміну з атакуючим, утримуючи з'єднання відкритим, тривалий час.
11	Настройте відправлення повідомлень для кожної події сканування портів, що містять не статистику про атакуючих, а дані про кожне конкретне сканування.	За допомогою перемикача «*Включити емуляцію сервісів TCP*», виключіть систему імітації сервісів *TCP*, для негайно розриву з'єднання з атакуючим вузлом без передачі атакуючому будь-якої інформації.
12	Задайте інтервал між повідомленнями з інформацією про атаку в числове поле «*Відправляти повідомлення не частіше, ніж один раз в XXX хвилин*».	Настройте режим передачі випадкових даних, тому що наявність у відповіді *APS* випадкової інформації вводить в обман сканери мережної безпеки, утрудняє й сповільнює їхню роботу.

Зміст протоколу

Опишіть необхідність використання утиліти APS і результат її роботи, на прикладі завдань, виконаних у лабораторній роботі. У звіт необхідно включити опис призначення пунктів меню «*Сервіс/Настроювання*» і «*Редагування користувальницької бази портів*». Опишіть, у яких випадках, корисні опції, зазначені й застосовані вами, у вашім варіанті. Занесіть до протоколу формат створених вами шаблонів. Опишіть призначення використовуваних у шаблоні параметрів.

Контрольні питання

1. Для чого призначена утиліта *APS*?
2. Якими достоїнствами володіє утиліта *APS*?
3. Для чого служить фільтр утиліти *APS*?
4. Що містить закладка настроювання системи імітації сервісів *UDP*? Для організації яких атак, може застосовуватися відгук по *UDP* портах, при включенні імітації сервісів *UDP*.
5. Поясніть, призначення користувальницької бази портів.
6. Які варіанти можливі, при виборі протоколу у вікні редактора користувальницької бази портів?
7. Які динамічні елементи може містити текст «банера»?

Лабораторна робота № 6 Організація безпеки локальної мережі при використанні утиліт, що реалізують моніторинг трафіку

Ціль роботи

Виявлення вторгнень у мережі Windows, виявлення сканування портів, повідомлення про спроби вторгнень. Вивчити на практиці механізм захисту локальних мереж, за допомогою моніторингу. Для цього вивчити основи роботи, з утилітами моніторингу мережного трафіку в локальній мережі, на прикладі *Network Monitor*.

Вміти набудовувати фільтри даної утиліти. Навчиться реконструювати сеанси, вести статистики по протоколах, комп'ютерам, завантаженню мережі, розміру пакетів, за допомогою аналізатора трафіку *EEYE IRIS*.

Ключові положення

Утиліта *Network Monitor* використовується для аналізу й виявлення проблем у мережі. *Network Monitor* записує данні, переданні й отримані комп'ютерами мережі, для наступного перегляду й аналізу цих даних. Кадри й пакети канального рівня записуються через прикладний рівень і представляються в графічному виді. Кадри й пакети містять інформацію:

– адресу відправника й адресата;

– порядкові номери;

– контрольні суми.

Утиліта *Network Monitor* розшифровує цю інформацію, дозволяючи аналізувати мережний трафік і вести журнал мережної активності. Крім даних канального рівня, *Network Monitor* відображає деякі дані прикладного рівня, наприклад протоколи *http* або *FTP*.

Завдання до лабораторної роботи

1. Запустіть утиліту *Network Monitor*. Ознайомтеся з основними механізмами моніторингу мережного трафіку, а також з настроюваннями, представленими в пунктах меню *Вид (View)*, *Фрейми* (*Frames*), (*Capture*), *Фільтр* (*Filter*), *Властивості* (*Tools*).

2. Настройте й запустіть перехоплення трафіку, залежно від вашого варіанта, зазначеного в табл.6.1. Для цього скористайтеся вікном редактора фільтра запису (*Capture Filter*) або фільтра перегляду (*Display Filter*), що відкривається з вікном *Capture*. Через якийсь час зупиніть перехоплення заданого трафіку. Для цього, у меню *Capture*, виберіть меню зупинки перехоплення.

3. Проаналізуйте отриманий мережний трафік. Занесіть до протоколу правило фільтра, що ви використовували.

4. Запустіть утиліту *eEye Iris*. Ознайомтеся з основними механізмами моніторингу трафіку, а також з настроюваннями, представленими в основних пунктах меню.

5. Запустіть сканування трафіку. Через деякій час зупиніть утиліту. Виберіть фільтри перегляду, залежно від завдання, зазначеного в табл.6.1.

7. Зрівняйте роботу двох, вивчених вами в даній лабораторній роботі, утиліт. Опишіть у протоколі розходження, достоїнства й недоліки кожної з них.

Таблиця 6.1 – **Варіанти завдань для виконання лабораторної роботи**

№ вар.	Настроювання параметрів фільтрів
1	Настройте перехоплення трафіку між двома сусідніми робочими станціями.
2	Настройте перехоплення трафіку між локальною робочою станцією й сусідньою.
3	Настройте перехоплення по протоколу *ARP*.
4	Настройте запис кадрів, що містять певний тип даних.
5	Настройте перехоплення всього мережного трафіку.
6	Настройте перехоплення тільки зовнішнього трафіку.
7	Отфільтруйте кадри, для відображення широкомовних пакетів у мережі.
8	Отфільтруйте кадри, для відображення адреси відправника й приймача кадру для канального й мережного рівнів.
9	Отфільтруйте кадри, щоб відобразити кадри, для відправлення яких використовувався протокол ftp.
10	Отфільтруйте кадри, щоб відобразити кадри, передані по протоколу TCP
11	Отфільтруйте кадри, щоб відобразити кадри, передані по протоколу IP
12	Отфільтруйте кадри, щоб відобразити весь мережний трафік, крім широкомовних повідомлень.

Зміст протоколу

Розберіть рядок записаних даних і структуру кадрів, у кожній з утиліт.

До протоколу внесіть відомості по обраному сегменті мережі, залежно від вашого завдання. Відомості повинні містити інформацію:

– про використання мережі;

– про кількість отриманих байт у секунду;

– про кількість отриманих кадрів у секунду.

Відомості повинні включати наступну інформацію:

– статистику сеансу;

– статистику робочої станції;

– загальну статистику.

Ознайомтеся з типами фільтра відображення й занесіть до протоколу таблицю різних способів фільтрування.

Контрольні питання

1. На якому рівні семірівневої моделі *OSI*, виробляється збір даних в утиліті *Network Monitor*?
2. Для чого потрібна утиліта *Microsoft Network Monitor*?
3. Яку інформацію про передані й отримані дані по мережі, бачить адміністратор, за допомогою утиліти *Network Monitor*?
4. Для чого служить і яким чином настроюється фільтр запису утиліти *Network Monitor*?
5. Для чого служить і яким чином настроюється фільтр відображення утиліти *Network Monitor*?
6. Яким чином можливе виявлення утиліти *Network Monitor* і яка інформація видається, при виявленні даної утиліти?
7. Для чого потрібна утиліта *eEye Iris?*
8. Які настроювання й фільтри можливо застосовувати в утиліті *eEye Iris?*
9. Дайте порівняльну характеристику *Network Monitor* і *eEye Iris?*
10. Поясніть, яким чином можливо одержати інформацію про зловмисника, за допомогою утиліт *Network Monitor* і *eEye Iris?*

Лабораторна робота №7 Організація безпеки механізму аутентифікації, при перехопленні парольних хешей і їхньої розшифровки

Ціль роботи

Вивчення на практиці, основ роботи, з утилітами перехоплення й розшифровки парольних хешей програмою *Cain&Abel*, при аутентифікації по мережі, для перевірки коректної роботи механізму аутентифікації.

Ключові положення

Основне завдання утиліти *Cain&Abel* це відновлення паролів. Відновити можна паролі входу в систему, загальні паролі, паролі екранної заставки, паролі доступу до мережі й будь-які інші, кэшируемі в системі, у зовнішньому PWL-Файлі або в системному реєстрі. *Cain&Abel* не використовує системних уразливостей, однак має досить потужні засоби дешифрування.

Завдання до лабораторної роботи

1. Запустіть програму. Ознайомтесь з можливостями основних пунктів меню: *Конфігурації* (*Configure*), *Сервіс* (*Tools*).

2. Створіть на вашій робочій станції, кілька локальних користувачів з паролями різної довжини й складності. При створенні користувачів, не встановлюйте флаг «*User must change password at next logon*». Також створіть загальний каталог, з ім'ям «*Test*» і надайте, створеним вами користувачам права на нього.

3. Відкрийте пункт меню *Конфігурації (Configure), на* вкладці «*Sniffer*», виберіть ваш мережний адаптер і натисніть *OK*. Потім натисніть на кнопку *Start Sniffer* і перейдіть на вкладку *Sniffer*, у ній на вкладку *Passwords,* для того щоб переглянути інформацію про перехоплені паролі.

4. Попросіть сусіда підключитися до вашого комп'ютера по мережі від імені створених вами користувачів, для цього можна скористатися меню директорії «*Сервіс*» (*Service*), «*Підключити мережний диск*» (*Map Network Drive*), с параметром «*Підключити, використовуючи ім'я*» (*Connect using a different user name*). Переконаєтеся, що в контейнері SMB є перехоплені парольні хеші.

5. Переглянете кількість завантажених хеш. Для цього в контекстному меню *Send all to Cracker* виберіть перехоплені парольні хеші, із вкладки *Cracker*, потім виберіть меню (*Dictionary Attack NTLM + Challenge*) для перегляду інформації про кількість завантажених хеш.

6. Здійсніть перебір паролів, методом, залежно від вашого варіанта, зазначеного в табл.7.1.

7. Протестуйте пароль, за допомогою команди «*Тестувати пароль*» (*Test Password*), контекстного меню.

8. Після закінчення лабораторної роботи, видаліть створених вами користувачів і мережних дисків.

Таблиця 7.1 – **Варіанти завдань для виконання лабораторної роботи**

№ вар.	Метод перебору
1	Здійсните перебір паролів, по словнику. Для цього у вікні «*Словник*» (*Dictionary Crack*) виберіть пункт «*Додати*» (*Add*) і виберіть файл *Wordlists.txt* у директорії *Wordlists*, верніться до меню «*Словник*» (*Dictionary Crack*) і виберіть пункт «*Почати*» (*Start*), для перегляду, як відбувається перебір паролів по словнику.
2	Здійсните перебір паролів «грубою силою». Для цього, скористайтеся пунктом контекстного меню «Атака» (*Brute-Force Attack NTLM + Challenge*). Подивитеся, як оцінить необхідний час для перебору утиліта Cain. При великих часових витратах, виберіть пароль, з меншої довжиною. На основі проробленої роботи, занесіть до протоколу вимоги, які, на вашу думку, необхідно пред'являти до пароля.
3	Проскануйте *MAC*-адреси робочих станцій, у вашій локальній мережі. Для цього відкрийте вкладку «*Sniffer*», перейдіть у режим сніфінгу й виберіть «S*tar/Stop Sniffer*», і додайте «*SCAN MAC addresses*». Після виявлення робочих станцій у локальній мережі, на вкладці «*Sniffer*», перейдіть на вкладку «*ARP*». Додайте правила *ARP* Poison routing, для того, щоб ваша робоча станція виступала в ролі сніфера між обраними сусідніми робочими станціями з лівих і правих полів. Не виключаючи режим сніфера, виберіть меню «Start/Stop *ARP*», для того щоб відслідковувати обмін пакетами й поступово наповнювати рядки Passwords, поки не зміниться поле *ARP-RDP* на (1).
4	Використовуйте для перехоплення пароля меню *Конфігурації (Configure),* «Фільтр і перемикання портів» (*Filters and Ports Tab*), щоб захоплювати тільки аутентифікаційну інформацію. Здійсніть відновлення пароля, за допомогою перегляду схованих паролів.
5	Використовуйте для перехоплення пароля меню *HTTP Fields Tab*, що містить список імені і поля пароля.
6	Здійсніть перебір паролів за допомогою методу *Cryptanalysis*.
7	Здійсніть перебір паролів за допомогою методу *Brute-Force.*
8	Здійсніть перебір паролів за допомогою виявлення пароля шляхом перехоплення інформаційних пакетів і їх наступний аналіз кеш.
9	Здійсніть перебір паролів за допомогою виявлення пароля шляхом перехоплення інформаційних пакетів і їх наступний аналіз запису переговорів по мережі.
10	Здійсніть перебір паролів за допомогою «атаки по масці».
11	Здійсніть перебір паролів за допомогою «гібридної атаки».
12	Здійсніть перебір паролів за допомогою «атаки розподіленим перебором».

Зміст протоколу

На основі виконаної лабораторної роботи, опишіть у протоколі, методи, які застосовуються для відновлення пароля в утиліті *Cain&Abel,* а також опишіть, яким чином реалізуються ці можливості. Докладно опишіть метод, яким ви скористалися. На закінчення, розробіть план використання механізмів запобігання взлому пароля схожими утилітами. Опишіть всі існуючі можливості запобігання взлому пароля із внутрішньої мережі й із глобальної мережі Інтернет.

Контрольні питання

1. Опишіть призначення, можливості й принцип роботи утиліти *Cain&Abel?*

2. Поясніть, для чого потрібний протокол ARP і опишіть принцип здійснення атаки з його використанням.

3. Для чого необхідне виконання ARP-spoofing в утиліті *Cain&Abel?*

4. Які вимоги до пароля, як адміністратор безпеки, ви б пред'являли у вашій локальній мережі?

5. Якими методами, можливо, відновити пароль за допомогою утиліти *Cain&Abel?*

6. Опишіть, як відбувається відновлення пароля по словнику.

Лабораторна робота № 8 Організація шифрування трафіку при використанні утиліти IPSec

Ціль роботи

Вивчити методи захисту й безпеки даних у мережі, використовуючи шифрування даних, за допомогою утиліти *IPSec*. Навчиться створювати й активувати політики утиліти *IPSec*. Уміти перевіряти шифрування даних.

Ключові положення

Internet Protocol Security (IPSec) – це набір протоколів шифрування, аутентифікації й забезпечення захисту при транспортуванні IP-пакетів. IP Security надає можливість шифрування всього мережного трафіку на 3 рівні, що дає можливість використання небезпечних протоколів, таких, наприклад, як *telnet*, оскільки всі дані будуть інкапсульовані утилітою *IPSec* і зашифровані при передачі по мережі.

Використання шифрування, за допомогою протоколу *IPSec*, дозволяє адміністраторові безпеки, спростити процедуру виявлення програм прослуховування портів, тому що, такі програми стають безглуздими.

Завдання до лабораторної роботи

1. Запустіть консоль керування *IPSec* на вашому комп'ютері. Виберіть одну з політик *IPSec, використовувану за замовчуванням,* для цього відкрийте меню «*Локальна політика безпеки*» (*Local Security Policy*) у директорії «*Адміністрування*» (*Administrative Tools*) і виберіть розділ «*Політики безпеки IP на локальному комп'ютері*» (*IP Security Policies on Local Computer*). Ознайомтесь з принципами даної політики безпеки.

2. Створіть свій список фільтрів, зазначений, залежно від варіанта, у табл.8.1. Для цього виберіть у вікні «*Локальні настроювання безпеки*» *(Local Security Settings*) і виберіть у контекстному меню «*Дія*» пункт «*Керування списками IP-Фільтра й діями фільтра*» (*Manage IP filter lists and filter actions*). На закладці «*Керування списками фільтрів IP*» (*Manage IP Filter Lists*) натисніть кнопку «*Додати*» (*Add*). Уведіть у поле ім'я назву списку. У стартовому вікні майстра *фільтрів* IP, натисніть кнопку «Додати», а потім кнопку «Далі» (Next). Виберіть один із пропонованих варіантів, в якості джерела призначення і протокол, що задовольняє вимогам вашого завдання. Виберіть пункт «*Пакети на цей порт*» (*To this port*) і введіть у поле значення, що задовольняє вимогам вашого завдання. Для завершення роботи майстра натисніть кнопку «*Готове*» (*Finish*).

Як джерело ви можете вибрати:

– «*Мій IP-Адреса*» (*My IP Address*);

– «*Любою IP-Адреса*» (*Any IP Address*);

– «*Певне DNS-Ім'я*» (*DNS name*);

– «*Певний IP-Адреса*» (*IP Address*);

– «*Певна* підмережа *IP*» (*IP network*).

Як призначення ви можете вибрати:

– «*Мій IP-Адреса*» (*My IP Address*);
– «*Любою IP-Адреса*» (*Any IP Address*);
– «*Певне DNS-Ім'я*» (*DNS name*)4
– «*Певний IP-Адреса*» (*IP Address*);
– «*Певна* підмережа *IP*» (*IP network*).

Як протокол ви можете вибрати:
– *EGP;*
– *HMP;*
– *ICMP;*
– *RAW;*
– *RDP;*
– *RVD;*
– *TCP;*
– *UDP;*
– *XNS-IDP;*
– *Іншій, із вказівкою номера порту;*
– *Кожний*.

3. Створіть власну дію фільтра, зазначену, залежно від варіанта, у табл.8.1. Для цього в діалоговому вікні «*Керування списками IP-Фільтра й діями фільтра*» (*Manage IP filter lists and filter actions*) перейдіть на закладку «*Керування діями фільтра*» (*Manage Filter Actions*) і натисніть кнопку «*Додати*». У стартовому вікні майстра настроювання дій *фільтрів* IPSec натисніть кнопку «Далі». У вікні настроювання загальних параметрів дії фільтра виберіть один із пропонованих варіантів, що задовольняє вимогам вашого завдання. Для завершення роботи майстра натисніть кнопку «*Готово*». Для завершення настроювання списку і дій фільтрів, натисніть кнопку «*Закрити*» (*Close*).

У вікні настроювання загальних параметрів дії фільтра, ви можете вибрати одну з наступних дій:
– «*погодити*» (*Negotiate*);
– «б*локувати*» (*Block*);
– «д*озволити*» (*Permit*).

4. Створіть свою політику *IPSec*. Для цього у вікні «*Локальні настроювання безпеки*», виберіть із контекстного меню пункт «*Створити політикові безпеки IP*» (*Create IP Security Policy*) і у вікні майстра *політики IP*-Безпеки натисніть кнопку «Далі». Уведіть у поле ім'я, назву вашої політики. Відмовтеся від використання пункту «*Використовувати правило за замовчуванням*» (*Activate the default response rule*) і натисніть «*Далі*». Залишіть пункт «*Змінити властивості*» (*Edit properties*) і натисніть кнопку «*Готово*» для завершення роботи майстра.

5. Додайте до створеної вами політики, правило за зазначеними критеріями, залежно від варіанта, даного в табл.8.1. Для цього в діалоговому вікні властивостей політики натисніть кнопку «*Додати*», потім кнопку «*Далі*». З переліку списків фільтрів виберіть назву вашої політики. Зі списку дій

фільтрів виберіть одну з дій. Для завершення роботи майстра натисніть кнопку «*Готове*».

6. Призначте обрану політику, для цього виберіть пункт «*Призначити*» (*Assign*) політики «*Назва вашої політики*».

Таблиця 8.1 – **Варіанти завдань для виконання лабораторної роботи**

№ вар.	Настроювання параметрів фільтра й політики *IPSec*
1	Установлюючи політики на сервері вашої організації, створіть для комп'ютерів, які повинні використовувати безпечні з'єднання, політику, яка допускає небезпечні з'єднання з комп'ютерами не підтримуючими *IPSec*. Передбачте, щоб комп'ютер приймав незахищений трафік, але завжди виконував спробу захистити додаткові зв'язки, посилаючи відправникові запит безпеки. Включіть в політику, правило запиту безпеки для всього *IP-трафіку*, метод перевірки дійсності *Kerberos*, без параметрів тунелюваня, для типу підключення - всіх мережних підключень.
2	Установлюючи політики на сервері вашої організації, створіть для комп'ютерів, політику, яка дозволяє пересилати весь *ICMP-трафік*, не перевіряючи дійсність, без параметрів тунелюваня, для типу підключення – всіх мережних підключень.
3	Установлюючи політики на сервері вашої організації, створіть для комп'ютерів політики відгуку за замовчуванням для відповіді на запити безпеки від інших комп'ютерів. Включіть в політику динамічний список фільтрів, для дії фільтра – відгук за замовчуванням, з методом перевірки *Kerberos*, без тунелюваня, для типу підключення – всіх мережних підключень.
4	Сервер, вашої організації передає секретні дані. Установіть політики на сервері, для комп'ютерів, таким чином, щоб вони завжди вимагали захист усього вихідного трафіку, допускаючи відсутність захисту тільки для початкового вхідного запиту на з'єднання. Для цього включіть правило запиту безпеки для всього *IP-трафіку*, не перевіряючи дійсність, без тунелюваня, для типу підключення – всіх мережних підключень.
5	Установіть політики на сервері вашої організації, для комп'ютерів, таким чином, щоб дозволити пересилати весь *ICMP-трафік*, перевіряючи дійсність методом *Kerberos*, без тунелюваня, для типу підключення – всіх мережних підключень.
6	Установіть політики на сервері вашої організації, для комп'ютерів, забезпечивши правило відгуку за замовчуванням для відповіді на запити безпеки від інших комп'ютерів. Для цього включіть в правило динамічний список фільтрів *IP*, з дією фільтра за замовчуванням, методом перевірки дійсності *Kerberos*, без тунелюваня, для типу підключення – всіх мережних підключень.
7	Створіть політики для комп'ютерів, які захищають дані по запиту, для рішення задачі, коли клієнти інтрамережі можуть не вимагати

	використання *IPSec*, крім випадків, коли запит виходить із іншого комп'ютера, щоб забезпечити комп'ютеру, на якому активізована політика, відповідати на запити безпечного зв'язку. Включіть в політику правило відгуку за замовчуванням, що створює динамічні фільтри *IP* для вхідного і вихідного трафіку на основі методу перевірки дійсності *Kerberos*, без тунелюваня, для типу підключення – всіх мережних підключень.
8	Дозвольте дію, задавши, у фільтрі *IP*, політику для взаємодії з *DNS* сервером, таким чином, щоб дані передавалися з адреси вашого комп'ютера, на будь-яку адресу й з будь-якої адреси на адресу вашого комп'ютера, по 53 порту *tcp* і *udp* протоколів. Включіть в політику правило зв'язку списка з дією; для всіх мережних інтерфейсів; на основі методу перевірки дійсності *Kerberos*, без тунелюваня, для типу підключення – всіх мережних підключень.
9	Дозвольте дію, задавши, у фільтрі *IP*, політики для взаємодії з *SQL* сервером, таким чином, щоб дані передавалися з адреси вашого комп'ютера, на будь-яку адресу й з будь-якої адреси на адресу вашого комп'ютера, по портах *1433* порту *tcp* і *udp* протоколів. Включіть в політику правило зв'язку списока з дією; для всіх мережних інтерфейсів; на основі методу перевірки дійсності кожної з них, без тунелюваня, для типу підключення – всіх мережних підключень.
10	Дозволите дію, задавши, у фільтрі *IP*, політики для Web-*Сервера*, таким чином, щоб з будь-якої адреси й будь-якого порту, передавалися дані на адресу вашого комп'ютера, по *80*/*tcp* порту й з будь-якої адреси, будь-якого порту, передавалися дані на адресу вашого комп'ютера по порту *443*/*tcp*.
11	Створіть політики для комп'ютерів, створивши правило для фільтрації вихідного трафіку, тобто від адреси комп'ютера, на будь-яку адресу, по :порту *1434*/*udp*. За допомогою даного правила, заблокуйте будь-який вихідний трафік через порти *UDP 1434* інших комп'ютерів мережі.
12	Настройте, політики ізолювання доменів, використовуючи наступні правила. Використовуйте настроювання для всього трафіку *IP*, дія фільтра: тільки *Encapsulating Security Payload* (*ESP*), нульове шифрування (null encryption), перевірка цілісності *SHA-1* (*SHA-1 integrity*), обов'язковий захист (*require security*), заборона взаємодії між комп'ютерами без використання протоколу *IPSec*. При цьому дозволивши дії фільтрів, що містять адреси або діапазон адрес контролерів домену.

Зміст протоколу

Опишіть у протоколі настроювання, які ви зробили, для рішення поставленого перед вами завдання, аргументуючи кожний пункт настроювання. Опишіть, яким образом, можливо, створити з'єднання між двома вузлами, з передачею зашифрованого трафіку, переданого по протоколіу *IPSec*.

Контрольні питання

1. Поясніть, у чому полягає метод захищеної передачі даних, з використанням *IPSec*?
2. Яким чином, реалізован метод захищеної передачі даних, з використанням *IPSec*?
3. Поясніть призначення протоколу *ESP.*
4. Поясніть призначення й принцип роботи транспортного й тунельного режиму роботи *IPSec*:
5. Опишіть функції *IPSec.*
6. Опишіть функціональне призначення політик, які *IPSec,* використовує за замовчуванням.
7. Які порти, використовуються, при передачі по протоколу *ESP*?
8. Опишіть можливості фільтра *IPSec.*

Лабораторна робота № 9 Організація безпеки АРМ на базі ОС Windows XP за допомогою міжмережевого екрана Outpost Firewall

Ціль роботи

Настроювання програми *Outpost Firewall*, для реалізації додаткового засобу забезпечення безпеки операційних систем сімейства Windows, що входять у комп'ютерну мережу. Настроювання правил і квот користувачів програми *Outpost Firewall*.

Ключові положення

Можливості Outpost Firewall

Персональний брандмауер *Outpost*, забезпечує захист комп'ютера від погроз, пов'язаних із втратою конфіденційності, витоком даних, несанкціонованим доступом до системи.

Перевагою *Outpost Firewall* є можливість підключення модулів, які представлені як фільтри й мають розширення *.ofp*.

Завдання до лабораторної роботи

1. Відкрийте програму *Outpost Firewall*. Вивчите функціональні можливості вкладок контекстного меню «*Параметри*».

2. Настройте функції програми *Outpost Firewall*, залежно від вимог, зазначених у вашому варіанті й описаних у табл.9.1.

3. Настройте журнал програми *Outpost Firewall,* для відображення тільки необхідної інформації, обумовленої вашим завданням.

Таблиця 9.1 – **Варіанти завдань для виконання лабораторної роботи**

№ вар.	Настроювання параметрів Outpost Firewall
1	На робочих комп'ютерах користувачів, необхідно блокувати відображення в браузерах рекламних банерів. А також повідомляти користувачів про сканування їхнього комп'ютера, навіть якщо, було зафіксовано однократне сканування.
2	Робочі комп'ютери користувачів, необхідно настроїти, заборонивши відображення на Web-Сторінках, елементів *ActiveX*. А також реалізувати блокування атакуючого вузла, при виявленні підозри на здійснення атаки.
3	На робочих комп'ютерах користувачів, необхідно блокувати доступ до Web-Сайтів, що містять слова з певного списку. А також, реалізувати автоматичне блокування підмережі, з якої вироблялися спроби атак.
4	На робочих комп'ютерах користувачів, необхідно дозволити виконання *Java і VB сценаріїв*. А також, реалізувати запобігання підміни *ARP-адрес*, приймаючи тільки ті відповіді, для яких була відправлена адреса.
5	На робочих комп'ютерах користувачів, необхідно блокувати показ інтерактивних рекламних оголошень, що відображаються в браузері. А також, реалізувати виявлення підміни *IP-адреси* й блокувати атаку.

6	На робочих комп'ютерах користувачів, необхідно заблокувати можливість відкривати деякі Web-Сторінки. А також, реалізувати запобігання помилкових повідомлень « *IP-адреса* вже зайнята».
7	На робочих комп'ютерах користувачів, необхідно заборонити показ браузерами *Java-апплетов*. А також, настроїти час після якого, необхідно блокувати *DoS* атаки.
8	На робочих комп'ютерах користувачів, необхідно настроїти фільтрацію .exe-*файлів*, що надходять по електронній пошті. А також, настроїти список системних портів, за яких програма повинна спостерігати, з підвищеною увагою, для виявлення атак.
9	На робочих комп'ютерах користувачів, необхідно настроїти функцію, при якій робота з *cookies*, буде здійснена, тільки за згодою користувача. А також, указати вилучені вузли й порти, довірчих комп'ютерів, які не будуть розглядатися як шкідливі.
10	На робочих комп'ютерах користувачів, необхідно настроїти фільтрацію .bat-*файлів*, що надходять по електронній пошті. А також, настроїти список «троянських» портів, за яких програма повинна спостерігати, з підвищеною увагою, для виявлення атак.
11	На робочих комп'ютерах користувачів, необхідно заборонити відображення в браузерах спливаючих вікон. А також, реалізувати перевірку й блокування невірних *DNS* запитів, а також блокування наддовгих *DNS* запитів.
12	На робочих комп'ютерах користувачів, необхідно блокувати відображення в браузерах рекламних оголошень стандартних розмірів. А також, реалізувати виявлення підміни *MAC-адреси* й блокувати атаку.

Зміст протоколу

Внесіть до протоколу докладний опис функцій, які ви набудовували, для рішення поставленого завдання. Обґрунтуйте вибір настроювань, які ви використовували для рішення завдання.

Внесіть до протоколу результат роботи програми й пророблені вами настроювання журналу.

Контрольні питання

1. Опишіть призначення міжмережевих екранів. Які функції виконує програма *Outpost Firewall*?
2. Поясніть функціональне призначення вкладок вікна «*Параметри*».
3. Для чого служать «*Політики*» *Outpost Firewall*? Опишіть призначення існуючих у програмі *Outpost Firewall* політик.
4. На які групи й для яких цілей, розділяються додатки системи в програмі *Outpost Firewall*?
5. Які дії необхідно зробити, для переносу додатка з однієї групи в іншу?
6. Опишіть функції визначених правил у програмі *Outpost Firewall.*

7. Які дії необхідно зробити, для формування користувальницьких правил?

8. Які умови, можливо сформувати для протоколів. Опишіть призначення цих умов і протоколів.

9. Опишіть процес настроювання системних протоколів. Які параметри настроювання, можливо вибрати, яке функціональне призначення даних параметрів?

10. Для чого служать модули, що підключаються. Опишіть роботу з ними.

Лабораторна робота № 10 Організація безпеки мережі, при використанні ОС Unix за допомогою міжмережевого екрану IPFW

Ціль роботи

Вивчити методи захисту мережі, за допомогою настроювання міжмережевого екрана *IPFW* ОС Unix. Настроювання *IPFW*, настроювання фільтрів, вивчення параметрів *IPFW*.

Ключові положення

В ОС Unix, базовим фільтром є ipfw, що працює, за допомогою правил. Загальний вид правила *ipfw*, представлений нижче:

ipfw [номер_правила] [set номер_набору_правила] дія [log] тіло

Кожне правило пов'язане з полем *номер_правила* в діапазоні від 1 до 65535, останній номер зарезервований для правила, виконуваного за замовчуванням. Правила перевіряються послідовно, відповідно до номера правила. Якщо правила мають один номер, вони виконуються в порядку додавання у фільтр. Якщо номер правила не зазначений, ядро привласнить номер автоматично. Вибір номера правила залежить від системної змінної *inet.ip.fw.automatic_step,* значення за замовчуванням якої дорівнює 100. Якщо наступний номер правила перевищує максимально можливе значення, то використовується номер останнього заданого правила.

Кожне правило пов'язане з полем *номер_набору_правил* у діапазоні від 0 до 31, або з останнім 31-м, зарезервованим для заданого за замовчуванням правила. Набори правил можна дозволяти й забороняти. Якщо правило додається без вказівки номера набору правила, то правило належить нульовому набору правил.

Таблиця 10.1 – Ключі команди IPFW

Ключ	Пояснення
-a	Показує значення лічильників правил. Еквівалентна команді show
-d	При перегляді списку правил показує статичні й динамічні правила
-e	При перегляді списку правил показує минулі динамічні правила
-f	Виконує критичні команди без підтвердження, наприклад flash
-N	Визначає по адресах і портам імена комп'ютерів і сервісів і виводить правила в символьних іменах
-q	Не виводить на термінал повідомлення під час додавання, обнуління лічильників, очищення фільтра. Ця опція корисна для виконання великої кількості команд у скриптів. Так само корисна при запуску файлів скриптів із правилами при вилученому адмініструванні.
-s[field]	Під час перегляду списку правил по каналах (pipes) сортує правила відповідно до одного зі значень лічильника.
-t	Показує час останнього проходження пакета через правило.

Таблиця 10.2 – Дії над пакетам у фільтрі IPFW

Дія	**Пояснення**
allow | accept | pass | permit	Пакет припиняє рух по фільтрі і уважається прийнятим.
check-state	Перевіряє пакет на відповідність динамічному набору правил. Якщо відповідність установлена, виконує дію пов'язану з динамічним правилом, у противному випадку проглядається наступне правило. Якщо правило check-state не вказувати, то динамічний набір правил буде перевірятися, коли зустрітися правило з (keep-state) або limit
Count	Інкрементує лічильники правила при відповідному правилу. Пакет продовжує рух по фільтрі.
deny | drop	Пакет припиняє рух по фільтрі і знищується.
divert port	Перенаправляє пакет у сокет, відповідно до зазначеному порту або демонові, наприклад, natd.
fwd | forward ipaddr[,port]	Змінює наступний пункт проходження на зазначену *IP-адресу*. Пошук по фільтрі не продовжується. Якщо *IP-адреса* - локальна адреса, то пакет буде перенаправлятися в зазначений порт, у противному випадку порт ігнорується.
pipe pipe_nr	Використовується для завдання обмежень по трафіку.
queue queue_nr	Використовується для завдання обмежень по трафіку.
Reset	Знищує пакет, і якщо це tcp пакет, то посилає TCP RST оповіщення.
skipto number	Пропускає всі наступні правила, до зазначеного номера правила, далі пошук відповідності триває.
tee port	Відправляє копію пакета в сокет, відповідно до зазначеного порту.
Unreach code	Відкидає пакет і посилає ICMP повідомлення про неприступність пункту призначення. Код вказує який саме тип ICMP повідомлення потрібно послати, діапазон значень від 0 до 255. Підтримуються наступні символьні позначення: net, host, protocol, port, needfrag, srcfail, net-unknown, host-unknown, isolated, net-prohib, host-prohib, tosnet, toshost, filter-prohib, host-precedence or precedence-cutoff.

Таблиця 10.3 – Основні критерії пакетів у фільтрі IPFW

Критерії	**Пояснення**
dst-ip	IP-адреса приймача пакета.
src-ip	IP-адреса джерела пакета
src-port	Порт джерела пакета. Даний критерій справедливий для протоколів у якому вказуються порти: udp, tcp.
dst-port	Порт приймача пакета. Даний критерій справедливий для протоколів у яких вказуються порти: udp, tcp.

established	Еквівалентно TCP пакетам із установленими бітами ACK або RST.
Frag	Правило поширюється на всі фрагменти пакета, крім першого. Зроблене це тому, що немає можливості визначити вихідний/вхідний порт для фрагмента пакета, а для ICMP-пакетів визначити їхній тип.
In | out	Вхідні або вихідні пакети.
keep-state	При відповідності критеріям створює динамічне правило для інших пакетів даного з'єднання. Динамічні правила мають обмежений час життя.
Proto	Використовується для вказівки типу протоколу. Прикладами протоколів можуть бути TCP, UDP і ICMP. Список протоколів можна подивитися у файлі /etc/protocols.
recv interface	Відповідає пакетам отриманим з мережного інтерфейсу.
xmit interface	Відповідає вихідним пакетам з мережного інтерфейсу.
via interface	Відповідає пакетам минаючим через мережний інтерфейс.
Tcpflags	Застосовується тільки для TCP пакетів. Пакет відповідає критерію, якщо в пакеті виставлені прапори, які перераховуються списком розділеним комами. Підтримуються такі значення прапорів: fin, syn, rst, psh, ack, urg.
In | out	Вхідні або вихідні пакети.

Завдання до лабораторної роботи

1. Ознайомтеся з теоретичними відомостями лабораторної роботи і перевірте, чи включена підтримка фільтра на вашім комп'ютері.

2. Залежно від варіанта, зазначеного в табл. 10.4, виконаєте настроювання міжмережевого екрана. Для додавання правила, що дозволяє проходження пакетів, використовується наступний загальний вид команди:

ipfw add <номер_правила>

Для видалення правила з фільтра *ipfw*, використовується наступний загальний вид команди:

ipfw del <номер_правила>

3. Перевірте роботу фільтра.

4. Зробіть, за допомогою фільтра *ipfw*, підрахунок трафіку на вашому комп'ютері, використовуючи для цього наступні правила:

ipfw add номер_правила count ip from ім'я_вашої_робочої_станції to any

ipfw add номер_правила count ip from any to ім'я_вашої_робочої_станції

5. Виведіть статистику підрахованого трафіку, за допомогою команди:

ipfw show номер_правила

Таблиця 10.4 – Варіанти завдань для виконання лабораторної роботи

№ вар.	Завдання для настроювання правил міжмережевого екрана
1	Забороніть правило, що дозволяє пропускати весь трафік з будь-якого вузла мережі до будь-якого вузла мережі. Для цього видалите правило *allow ip from any to any.*
2	Дозвольте робочим станціям вашої підмережі, звертатися до серверів *DNS*. Для цього додайте у фільтр *ipfw* правило, що дозволяє протоколу *udp* від будь-якої робочої станції звертатися до будь-якого вузла по *53* порту. І правило, що дозволяє протоколу *udp* від вузла по *53* порту, дозволити звертатися до будь-якої робочої станції.
3	Дозвольте всі вихідні пакети з даного комп'ютера. Для цього додайте у фільтр *ipfw* правило, що дозволяє протоколу *ip* вашої робочої станції звертатися до всіх вузлів мережі.
4	Дозвольте виконання команди тестування мережі: *ping* Для цього додайте у фільтр *ipfw* правило, що дозволяє протоколу *icmp* з будь-якого вузла мережі до вашої робочої станції виконувати *icmptypes* для номерів вище заданих правил, наприклад *0,3,5,8,11.* Перевірте дію цього правила, за допомогою команди *ping*.
5	Дозвольте вхідні *ssh* і *web* з'єднання. Для цього додайте у фільтр *ipfw* правило, що дозволяє протоколу *tcp* з будь-якого вузла мережі, звертатися по портах *22* і *80*. Перевірте це правило, запустивши на вашій робочій станції *sshd*, *httpd* і зайдіть по *ssh*. Для перевірки роботи web сервера, виконаєте наступну команду, с іншого комп'ютера: *telnet <ip_Web> 80* Сервер повинен вам надіслати тестову web сторінку.
6	Дозвольте вашій робочій станції роботу по протоколу *ftp*. Для цього додайте у фільтр *ipfw* правило, що дозволяє вхідному і вихідному трафіку проходити по протоколу *tcp 20* і *21* портів.
7	Дозвольте вашій робочій станції роботу по протоколу *http*. Для цього додайте у фільтр *ipfw* правило, що дозволяє вхідному і вихідному трафіку проходити по протоколу *tcp 80* порту.
8	Обмежте швидкість для вашої робочої станції до 64 Кбіт/с. Для цього використовуйте правило виду: *ipfw add pipe 31 ip from any to ім'я_вашої_робочої_станції out назва_мережного_адаптера* *ipfw pipe 31 config 31 bw 64Kbit/s*
9	Дозвольте вашій робочій станції роботу по протоколу *ssh*. Для цього додайте у фільтр *ipfw* правило, що дозволяє вхідному і вихідному трафіку проходити по протоколу *tcp 22 порту* .
10	Створіть правило, що запобігає атаки типу *DoS* (відмова в обслуговуванні), які відкривають велику кількість динамічних

	правил. Для цього обмежте число з'єднань, що може бути відкрито користувачем, дозволивши кожному вузлу в мережі 172.16.0.0 відкрити максимум 10 з'єднань, причому один клієнтський комп'ютер повинен створювати не більше чотирьох одночасних з'єднань. Для цього використовуйте команди виду: *ipfw add allow tcp from підмережа to any назва_мережного_адаптера setup limit src-addr 10* *ipfw add allow tcp from any to ім'я_вашої_робочої_станції limit src-addr 4*
11	Забороніть вашій робочій станції роботу по протоколу *telnet*. Для цього додайте у фільтр *ipfw* правило, що забороняє вхідний і вихідний трафік по протоколу *tcp 23* порту .
12	Дозвольте вашої робочої станції підключення по протоколу *SMTP*. Для цього використовуйте правило, що дозволяє вхідний трафік по *25* порту, протоколу *tcp* від всіх вузлів мережі.

Зміст протоколу

Внесіть у звіт створені вами правила, у фільтрі *ipfw*, результат перевірки роботи даних правил. А також результат статистики підрахованого трафіку.

Контрольні питання

1. Як включати фільтр *IPFW* в ОС Unix?
2. Як можна переглянути які правила завантажені в *IPFW*?
3. Як в *IPFW* дозволити встановлювати з'єднання зі збереженням стану?
4. Як реалізоване перетворення мережних адрес у фільтрі *IPFW*.
5. Які функції демона *natd*.
6. Які ключі й параметри потрібно задати демонові *natd* для динамічного перетворення мережних адрес.
7. Як можна організувати підрахунок вхідного *tcp* трафіку у фільтрі *iptables*. Приведіть приклад.
8. Як можна організувати підрахунок вихідного трафіку *icmp* у фільтрі *IPFW*.

Глава 3

КОМПЛЕКТ ЗАВДАНЬ КОМПЛЕКСНОЇ КОНТРОЛЬНОЇ РОБОТИ

Критерії оцінювання контрольних тестових завдань підсумкових знань студентів навчального напрямку 6.170102 – Системи технічного захисту інформації з навчальної дисципліни «Основи захищених інформаційних технологій»

Тестові завдання з навчальної дисципліни «Основи захищених інформаційних технологій» спрямовано на контроль пізнавальних здібностей студентів до творчого вирішення проблемних питань щодо механізмів та практичних методів захисту інформації в комп'ютерних системах.

Тестові завдання складаються з трьох частин.

Перша частина відповідає початковому і середньому рівням. Вона складається з десяти питань, кожне з яких передбачає три варіанти відповіді. Студент має відібрати вірне одностайне рішення та відобразити його в рядку відповідей. Вірна відповідь на одне питання цього рівня оцінюється в 1 бал.

Друга частина відповідає достатньому рівню. Вона складається з двох питань, кожне з яких передбачає п’ять варіантів відповіді. Студент має відібрати декілька вірних рішень (принаймні два) та відобразити їх у рядку відповідей. Вірна відповідь на 1 питання цього рівня оцінюється в 3 бали.

Третя частина відповідає високому рівню. Вона складається з однієї задачі. Студент має знайти її рішення та зробити відповідні висновки щодо отриманих результатів. Вірна відповідь цього рівня оцінюється в 6 балів.

Питання всіх трьох рівнів охоплюють теми змістовних модулів щодо навчального курсу «Основи захищених інформаційних технологій» – «Програмно-апаратний захист інформації», «Безпека операційних систем».

Співвідношення суми балів за виконання тестового завдання, оцінкою за 100-бальною шкалою та оцінкою за національною шкалою наведено в табл.3.1.

Таблиця 3.1

№ п/п	Бали за виконання тестового завдання	Оцінка за 100-бальною шкалою	Оцінка за національною шкалою	Зміст оцінки
1.	17 – 22	95-100	Відмінно	Відмінні знання навчально-методичного матеріалу, безпомилкове виконання усіх завдань з додатковими прикладами
2.	11 – 16	80-94	Добре	Повні знання та вміння з даного навчально-методичного матеріалу, виконання конкретного завдання з деякими помилками, які не носять принципового характеру

3.	8 – 10	60-79	Задовільно	Знання та вміння в обсязі, який необхідно мати для роботи за фахом, але під час виконання конкретного завдання допустив суттєві помилки
4.	1 – 7	До 60	Незадовільно	Недосконалі знання та вміння з начального матеріалу та під час виконання студент допустив принципові помилки

ВАРІАНТ 1

ПЕРША ЧАСТИНА

Запишіть номер правильної на Ваш погляд, відповіді:

1. УРАЗЛИВІСТЬ ІНФОРМАЦІЇ – ЦЕ:

1) можливість виникнення на якому-небудь етапі життєвого циклу КС такого її стану, при якому створюються умови для реалізації загроз безпеки інформації;
2) подія або дія, що може викликати зміну функціонування КС, пов'язану з порушенням захищеності оброблюваної в ній інформації;
3) дія порушника, яка полягає в пошуку й використанні тієї або іншої уразливості.

2. ДО НАВМИСНИХ ЗАГРОЗ ВІДНОСЯТЬСЯ:

1) несанкціоновані дії обслуговуючого персоналу КС (наприклад, ослаблення політики безпеки адміністратором, відповідальним за безпеку КС);
2) вплив на апаратні засоби КС фізичних полів інших електронних пристроїв (при недотриманні умов їхньої електромагнітної сумісності) та ін.;
3) помилки користувачів КС.

3. ДО БЕЗПОСЕРЕДНІХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ ВІДНОСЯТЬСЯ:

1) обхід засобів розмежування доступу до інформаційних ресурсів внаслідок недоліків у їхньому програмному забезпеченні та ін.;
2) перехоплення побічних електромагнітних випромінювань і наведень (ПЕМВіН);
3) дистанційне відеоспостереження.

4. ДОСТОВІРНА ОБЧИСЛЮВАЛЬНА БАЗА – ЦЕ:

1) абстрактне поняття, що означає повністю захищений механізм обчислювальної системи (включаючи апаратні й програмні засоби), відповідаючий за підтримку реалізації політики безпеки;
2) активний компонент системи, що може стати причиною витоку інформації від об'єкта до об'єкта або зміни стану системи;
3) пасивний компонент системи, що зберігає прийняту або передану інформацію.

5. АВТОРИЗАЦІЯ – ЦЕ:

1) надання повноважень;

2) підтвердження дійсності;
3) порівняння ідентифікатора.

6. БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ КОРИСТУВАЧА ЦЕ:

1) автентифікація потенційного користувача шляхом виміру фізіологічних параметрів і характеристик людини, а також, особливостей її поводження;
2) автентифікація потенційного користувача шляхом вводу пароля;
3) автентифікація потенційного користувача з використанням фізичних носіїв інформації.

7. АПАРАТНО-ПРОГРАМНІ ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ВИКОНУЮТЬ ФУНКЦІЇ:

1) автентифікації користувача, розмежування доступу до інформації, забезпечення цілісності інформації і її захисту від знищення, шифрування;
2) організовують реалізацію політики безпеки інформації на етапі експлуатації КС;
3) перевірки на відсутність закладок приладів, пристроїв.

8. ДИНАМІЧНИЙ РЕЖИМ ВИВЧЕННЯ АЛГОРИТМУ ПРОГРАМИ ПРИПУСКАЄ:

1) виконання трасування програми;
2) вивчення вихідного тексту програми;
3) використання кодів, що самогенерують.

9. СУТНІСТЬ МЕТОДУ, ЗАСНОВАНОГО НА ВИКОРИСТАННІ САМОГЕНЕРУЄМИХ КОДІВ, ПОЛЯГАЄ В ТОМУ, ЩО:

1) коди програми, яку виконують, отримуються самою програмою в процесі її виконання;
2) коди програми, яку виконують, отримуються самою програмою після процесу її виконання;
3) коди програми, яку виконують, отримуються самою програмою до процесу її виконання.

10. ТРАНЗИТНІ ВІРУСИ ЦЕ:

1) віруси, які виконуються тільки в момент запуску зараженої програми;
2) віруси, які після активізації постійно перебувають в оперативній пам'яті комп'ютера й контролюють доступ до його ресурсів;
3) віруси, що заражають програми, які зберігаються в системних областях дисків.

ДРУГА ЧАСТИНА

Запишіть номери правильних на Ваш погляд, відповідей:

1. ДО МЕХАНІЗМІВ ПРОТИДІЇ ТРАСУВАННЮ ПРОГРАМИ ВІДНОСЯТЬСЯ:

1) зміна середовища функціонування;
2) архівація;
3) «випадкові» переходи;
4) використання самогенеруємих кодів;
5) шифрування.

2. ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ЗАХИСТУ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ НЕ ВИКОНУЮТЬ НАСТУПНИХ ФУНКЦІЙ:

1) ідентифікація та автентифікація;
2) пошук прихованих відеокамер;
3) криптографічний захист;
4) захист від просторового високочастотного опромінення;
5) реєстрація подій.

ТРЕТЯ ЧАСТИНА

Задача

Розрахувати ймовірність несправності комп'ютера оператора Р, якщо відомі інтенсивності відмов його комплектуючих:

- інтенсивність відмови жорсткого диска $\lambda 1=30.6*10^{-6}$ (відм/г);
- інтенсивність відмови мережевої карти $\lambda 2=11.2*10^{-6}$ (відм/г);
- інтенсивність відмови модему $\lambda 3=14.3*10^{-6}$ (відм/г);
- інтенсивність відмови мережевого екрану $\lambda 4=4.16*10^{-6}$(відм/г);
- інтенсивність відмови клавіатури $\lambda 5=5.3*10^{-6}$(відм/г);
- інтенсивність відмови миші $\lambda 6=6.3*10^{-6}$(відм/г);

а також відомо, що інтесивність відновлення $\beta=1$.

ВАРІАНТ 2

ПЕРША ЧАСТИНА

Запишіть номер правильної на Ваш погляд, відповіді:

1. АТАКОЮ НА КОМП'ЮТЕРНУ СИСТЕМУ (КС) НАЗИВАЮТЬ:

1) можливість виникнення на якому-небудь етапі життєвого циклу КС такого її стану, при якому створюються умови для реалізації загроз безпеки інформації;
2) подію або дію, що може викликати зміну функціонування КС, пов'язану з порушенням захищеності оброблюваної в ній інформації;
3) дію порушника, яка полягає в пошуку й використанні тієї або іншої уразливості.

2. ДО НЕНАВМИСНИХ ЗАГРОЗ ВІДНОСЯТЬСЯ:

1) помилки в розробці програмних засобів КС;
2) несанкціонований доступ до ресурсів КС з боку користувачів КС і сторонніх осіб, збиток від якого визначається отриманими порушником повноваженнями;
3) загроза порушення конфіденційності, тобто витоку інформації обмеженого доступу, що зберігається в КС або переданій від однієї КС до іншої.

3. ДО НЕПРЯМИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ ВІДНОСЯТЬСЯ:

1) використання підслуховуючих (радіозакладки) пристроїв;
2) маскування під інших користувачів шляхом викрадення їхньої ідентифікуючої інформації (паролів, карт і т.д.);
3) злочинна зміна програм для виконання несанкціонованого копіювання інформації при її обробці.

4. ЗГІДНО З НД ТЗІ 2.5-005-99 «КЛАСИФІКАЦІЯ АВТОМАТИЗОВАНИХ СИСТЕМ І СТАНДАРТНІ ФУНКЦІОНАЛЬНІ ПРОФІЛІ ЗАХИЩЕНОСТІ ОБРОБЛЮВАНОЇ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ» ДО КЛАСУ «1» АВТОМАТИЗОВАНИХ СИСТЕМ ВІДНОСЯТЬ:

1) а) розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності;
2) одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності;

3) локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

5. ПРОЦЕДУРУ УСТАНОВЛЕННЯ СФЕРИ ДІЙ КОРИСТУВАЧА Й ДОСТУПНІ ЙОМУ РЕСУРСИ КС НАЗИВАЮТЬ:

1) авторизацією;
2) автентифікацією;
3) ідентифікацією.

6. ПРОЦЕДУРА «РУКОСТИСКАННЯ» ВИКОРИСТОВУЄТЬСЯ ДЛЯ:

1) взаємної перевірки дійсності;
2) розподілу ключів між справжніми партнерами;
3) безпечного використання інтелектуальних карт.

7. БЕЗПЕКА В ЧАСТКОВО КОНТРОЛЬОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ МОЖЕ БУТИ ЗАБЕЗПЕЧЕНА:

1) ізоляцією від зловмисника ненадійного комп'ютерного середовища, окремого її компонента або окремого процесу за допомогою повністю контрольованих засобів;
2) схемою ідентифікації, що дозволяє збільшити число акредитацій, виконуваних за один цикл, і тим самим зменшити тривалість процесу ідентифікації;
3) зовнішньою автентифікацією об'єкта, що не належить системі.

8. СУТНІСТЬ СТАТИЧНОГО РЕЖИМУ ПОЛЯГАЄ:

1) у вивченні вихідного тексту програми;
2) у виконанні трасування програми;
3) у використанні кодів, що самогенерують.

9. ПРАВИЛЬНІСТЬ ФУНКЦІОНУВАННЯ ЯДРА БЕЗПЕКИ ДОВОДИТЬСЯ ШЛЯХОМ:

1) повної формальної верифікації його програм і покроковим доказом їхньої відповідності обраній математичній моделі захисту;
2) використання додаткових програмних або апаратно-програмних засобів;
3) використання строго певної безлічі програм.

10. STEALTH-ВІРУСИ ЦЕ:

1) віруси, що намагаються бути невидимими на основі контролю доступу до заражених елементів даних;

2) віруси, що містять у собі алгоритми шифрування, які забезпечують розходження різних копій вірусу;
3) віруси, які після активізації постійно перебувають в оперативній пам'яті комп'ютера й контролюють доступ до його ресурсів.

ДРУГА ЧАСТИНА

Запишіть номери правильних на Ваш погляд, відповідей:

1. ДО МЕХАНІЗМІВ ПРОТИДІЇ ДИЗАСЕМБЛЮВАННЮ ПРОГРАМИ ВІДНОСЯТЬСЯ:

1) архівація;
2) зміна середовища функціонування;
3) «випадкові» переходи;
4) модифікація кодів програми;
5) шифрування.

2. ЯКІ З НАВЕДЕНИХ НИЖЧЕ КОМПОНЕНТИ ВХОДЯТЬ ДО СИСТЕМИ РОЗМЕЖУВАННЯ ДОСТУПУ:

1) засоби контролю цілісності;
2) засоби автентифікації суб'єкта доступу;
3) засоби захисту від технічної розвідки;
4) засоби знищення залишкової інформації;
5) засоби реєстрації подій.

ТРЕТЯ ЧАСТИНА

Задача

Розрахувати ймовірність безвідмовної роботи комп’ютерної системи P(t) за проміжок часу t рівний 8 годинам, якщо інтенсивність відмов системи $\lambda = 30.6*10^{-6}$ (відм/г).

Додаток А

Міністерство транспорту та зв'язку України

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ З ПИТАНЬ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ

ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ЗВ'ЯЗКУ ІМ. О.С. ПОПОВА

Кафедра Інформаційної безпеки та передачі даних

ЗАТВЕРДЖУЮ
Ректор ОНАЗ ім. О.С. Попова
_____ П.П. Воробієнко
«___»_____2009 р.

НАВЧАЛЬНА ПРОГРАММА

Безпека інформаційно-комунікаційних систем

Нормативна дисципліна

освітньо-професійної програми
підготовки бакалаврів за напрямом вищої освіти
6.170102 Системи технічного захисту інформації

Спеціальність: Інформаційна безпека

Одеса-2009

Навчальна програма дисципліни: **Безпека інформаційно-комунікаційних систем**

Програму розроблено на кафедрі **Інформаційної безпеки та передачі даних**

Автори: Кільдішев В.Й., Кононович В.Г.

Програму розглянуто і схвалено на засіданні кафедри

Протокол № ___ від «____» _____ 2009 р.

Зав. каф._____ М.В. Захарченко

Програму погоджено з кафедрами:

Безпеки виробничих процесів та електроживлення систем зв'язку

_____ Зав. каф. проф. А.Ф. Кадацький

Інформатизації та управління

_____ Зав. каф. проф. В.І. Загребнюк

Комутаційних систем

_____ Зав. каф. доц. А.Г. Ложковський

Програму розглянуто і схвалено методичною радою ННІ Радіо, телебачення, електроніки

Протокол № __ від «____» _____ 2009 р.

Директор ННІ РТЕ _____ /проф. С.А. Михайлов/

Програму розглянуто і схвалено методичною радою Одеської національної академії зв'язку ім. О.С. Попова

Протокол № __ від «____» _____ 2009 р.

Голова ради, проф. М.В. Захарченко

І. Передмова

Загальна характеристика дисципліни:
кількість кредитів ECTS 3;5
модулів 2;
загальна кількість годин 126;
у тому числі:
лекції 32 год.; лабораторних занять 18 годин; практичні заняття не передбачені;
самостійна робота 75 год.; аудиторної роботи 51 години;
семестри 4.1 та 4.2,
вид контролю залік.

ІІ. Мета навчання з дисципліни

Формування основ знань щодо механізмів та практичних методів захисту інформації в комп'ютерних та інформаційно-комунікаційних системах. Ознайомлення студентів із сучасними засобами захисту інформації в комп'ютерних та інформаційно-комунікаційних системах, оволодіння методами рішення професійних завдань.

ІІІ. Зміст дисципліни

Модуль 1: *Апаратні засоби захисту інформації і захист програм та даних* (кредитів ECTS – 1,8)

Вхідні вимоги до вивчення модуля

№	Зміст знань	Шифр
1	Властивості інформації як предмета захисту	ЗН.1
2	Характеристики інформаційних систем як об'єктів безпеки	ЗН.2
3	Основні напрями забезпечення безпеки інформації та інформаційних ресурсів	ЗН.3
	Зміст умінь	
1	Визначати інформацію, що підлягає захисту	УМ.1
2	Аналізувати загрози та джерела загроз інформаційної безпеці	УМ.2
3	Застосовувати апаратні засоби захисту	УМ.3

Структура залікового модуля 1

Змістовий модуль	лекції (годин)	Заняття		самостійна робота	індивідуальна робота
		практичні	лабораторні		
Модуль 1: Програмно-апаратний захист інформації (1,5 кредити; 54 год.)					
1. *Основні поняття захисту інформаційно-комунікаційних систем*	2			5	
2. *Основні апаратні засоби захисту інформаційно-комунікаційних систем*	2		2	4	
3. *Засоби фізичної безпеки та політика безпеки в комп'ютерних системах*	2			5	
4. *Засоби захисту від витоку інформації технічними каналами: заземлення, електроживлення, ПЕВМН, тощо*	2		2	5	

5. *Засоби й методи обмеження доступу до файлів*	2			4	
6. *Програмно-апаратні засоби шифрування*	2		2	5	
7. *Захист програм від несанкціонованого копіювання*	2			4	
8. *Захист програм від вивчення*	2		2	5	
Разом 1 модуль, год.	**16**	**-**	**8**	**37**	

Зміст змістових модулів (лекційних годин):

1.1. *Основні поняття захисту інформаційних технологій* (2 год.)

Електронний документ (ЕД). Види інформації в КС. Інформаційні потоки в КС. Поняття ЕД. Типи ЕД. Поняття зловмисника.

1.2. *Основні апаратні засоби захисту інформаційно-комунікаційних систем* (2 год.)

Поняття доступу, суб'єкт і об'єкт доступу. Фізичні, організаційно-технічні, технічні, та програмні засоби захисту.

1.3. *Засоби фізичної безпеки та політика безпеки в комп'ютерних системах* (2 год.)

Засоби фізичної безпеки контрольованої території, приміщень і виробничих та ресурсів захисту Оцінка захищеності. Способи захисту конфіденційності, цілісності та доступності в КС.

1.4. *Засоби захисту від витоку інформації технічними каналами: заземлення, електроживлення, ПЕВМН Ідентифікація користувачів КС - суб'єктів доступу до даних* (2 год.)

Засоби захисту від витоку інформації технічними каналами: заземлення, електроживлення, ПЕВМН тощо.

1.5. *Засоби й методи обмеження доступу до файлів* (2 год.)

Поняття несанкціонованого доступу (НСД). Класи й види НСД. Завдання ідентифікації користувача. Поняття протоколу ідентифікації. Локальна й вилучена ідентифікація. Ідентифікуюча інформація. Способи зберігання ідентифікуючої інформації. Основні підходи до захисту даних від НСД. Організація доступу до файлів. Фіксація доступу до файлів. Доступ до даних з боку процесу. Особливості захисту даних від зміни. Несанкціоноване копіювання програм як особливий вид НСД.

1.6. *Програмно-апаратні засоби шифрування* (2 год.)

Апаратні та програмно-апаратні засоби криптозахисту даних. Побудова апаратних компонентів криптозахисту даних. Захист алгоритму шифрування. Необхідні та достатні функції апаратного засобу криптозахисту.

1.7. *Захист програм від несанкціонованого копіювання* (2 год.)

Несанкціоноване копіювання програм як тип НСД. Загальне поняття захисту від копіювання. Прив'язка програмного забезпечення (ПЗ) до апаратного оточення й фізичних носіїв. Способи створення міток, що не копіюються.

1.8. *Захист програм від вивчення* (2 год.)

Вивчення й зворотне проектування ПЗ. Завдання захисту від вивчення й способи їхнього рішення. Аспекти проблеми захисту від дослідження.

Теми практичних занять модуля 1

Практичні заняття не передбачені

Теми лабораторних занять модуля 1

№	Тема	годин
1	Апаратні рішення для виявлення й запобігання витоків конфіденційної інформації	2
2	Засоби фізичного захисту	2
3	Структура, функції захисту інформації від НСД	2
4	Адміністрування системи захисту інформації від НСД	2
5	Експлуатація системи захисту інформації від НСД	2
6	Експлуатація системи антивірусного захисту	2
7	Ідентифікація користувачів КМ – суб'єктів доступу до даних	2
8	Організація доступу до файлів. Особливості захисту даних від зміни	2
	Усього:	**8**

Вихідні знання та уміння з модуля 1

№	Зміст знань	Шифр
1	Можливі дії супротивника, спрямовані на порушення політики безпеки інформації	ЗН.1
2	Механізми рішення типових завдань захисту інформації	ЗН.2
	Зміст умінь	
1	Кваліфіковано оцінювати область застосування конкретних механізмів захисту	УМ.1
2	Грамотно використовувати апаратні засоби захисту при рішенні практичних завдань	УМ.2

Модуль 2: *Захист в операційних системах та в мережах* (кредитів ECTS – 1,7)

Вхідні вимоги до вивчення модуля

№	Зміст знань	Шифр
1	Можливі дії супротивника, спрямовані на порушення політики безпеки інформації	ЗН.1
2	Механізми рішення типових завдань захисту інформації	ЗН.2
	Зміст умінь	
1	Кваліфіковано оцінювати область застосування конкретних механізмів захисту	УМ.1
2	Грамотно використовувати апаратні засоби захисту при рішенні практичних завдань	УМ.2

Структура залікового модуля 2

Змістовий модуль	лекції (годин)	Заняття		самостійна робота	індивідуальна робота
		практичні	лабораторні		
Модуль 2: Безпека операційних систем (1,5 кредити; 54 год.)					
1. *Захист інформації в операційних систем*	2		2	5	
2. *Підсистема захисту інформації в ОС Windows*	2			4	
3. *Підсистеми захисту інформації в ОС UNIX*	2		2	5	
4. *Атаки на мережні служби*	2			4	
5. *Адаптивна безпека*	2		2	5	
6. *Міжмережні екрани*	2			4	
7. *Віддалений доступ до мережі*	2		2	5	
8. *Віртуальні приватні мережі*	2			5	
Разом 2 модуль, год.	**16**		**8**	**37**	

Зміст змістових модулів (лекційних годин):

2.1. *Захист інформації в операційних систем* (2 год.)

Модель безпеки операційних систем (ОС). Механізми захисту ОС. Аналіз захищеності ОС.

2.2. *Підсистема захисту інформації в ОС Windows* (2 год.)

Основні компоненти підсистеми захисту Windows NT і Windows 2000. Політики. Поняття домена. Особливості встановлення довірчих відносин.

2.3. *Підсистеми захисту інформації в ОС UNIX* (2 год.)

Файлова система – як основа підсистеми захисту. Права доступу до елементів файлової системи. Керування процесами. Основні проблеми з безпекою й можливі рішення в Unix-подібних системах.

2.4. *Атаки на мережні* служби (2 год.)

Поняття атаки. Типи погроз. Класифікація атак по основним механізмам реалізації погроз. Мережні сканери.

2.5. *Адаптивна безпека* (2 год.)

Поняття адаптивності безпеки й системи виявлення атак. Класифікація по використовуваних механізмах виявлення атак, і по принципам їхньої практичної реалізації. Особливості застосування різних типів систем.

2.6. *Міжмережні екрани* (2 год.)

Поняття міжмережених екранів (МЕ). Їхня класифікація. Основні приклади конфігурації захищених мереж з використанням МЕ.

2.7. *Віддалений доступ до мережі* (2 год.)

Проблеми забезпечення безпеки при вилученому доступі. Протоколи автентифікації вилученого доступу у програмних засобах Microsoft.

2.8. *Віртуальні приватні мережі* (2 год.)

Поняття віртуальної приватної мережі, її призначення. Стандартні можливості каналоутворюючого устаткування різних виробників.

Теми практичних занять модуля 2

Практичні заняття не передбачені

Теми лабораторних занять модуля 2

№	Тема	годин
1	Функціональні профілі ОС Windows XP SP2	2
2	Файлова система	2
3	Адміністративні шаблони	2
4	Політика облікових записів ОС Windows XP SP2	2
5	Параметри локальної політики	2
6	Системні служби	2
7	Журнал подій	2
8	Настроювання реєстру	2
	Усього:	16

Вихідні знання та уміння з модуля 2

№	Зміст знань	Шифр
1	Етапи розробки політики інформаційної безпеки організації	ЗН.1
2	Особливості підсистем захисту ОС Windows та Unix	ЗН.2
3	Особливості застосування мережа-орієнтованих систем виявлення вторгнень	ЗН.3
	Зміст умінь	
1	Оцінювати ефективність і надійність захисту ОС	УМ.1
2	Виявляти слабості захисту ОС та використовувати їх для розкриття захисту	УМ.2
3	Планувати політику безпеки організації	УМ.3
4	Організовувати захист сегмента, що підключається до відкритих телекомунікаційних мереж	УМ.4

Курсове проектування не передбачено

IV. Методи навчання

Лекції, практичні заняття з використанням опитування, обговорення проблем і дискусій, лабораторні роботи з використанням ЕОМ, самостійна робота.

V. Методи оцінювання

Поточний контроль знань: *залік*.

Оцінювання проводиться за шкалою , національною та за шкалою ОНАЗ (100 бал.)

VI. Література

1. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник – К.: «МК-Прес», - 2005. – 432 с.

2. Вильям Столлингс Криптографическая защита сетей. – М.: Издательсткий дом “Вильямс”, 2001.

3. Домарев В.В./ Защита информации и безопасность компьютерных систем / Киев: диа-софт 1999.

4. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р — КиївіООО "Д.В.К.", 2004 . — 508 с.

5. Єфремов В.П., Кононович В.Г., Тардаскін М.Ф. Технічна експлуатація систем захисту інформації. Частина 2. Експлуатація безпечних інформаційних технологій: Навч. посібник / за ред. М.В. Захарченка. – Одеса: ОНАЗ, 2003. – С 248

Тримовний тезаурус навчальної дисципліни

№ з/п	Терміни, категорії, поняття українською, російською та англійською мовами	Умовні позначення	Визначення терміна (категорії, поняття)	Джерело визначення
1	2	3	4	5
1	Автентифікація Аутентификация Authentication		Перевірка належності суб'єктові доступу пред'явленого ним ідентифікатора.	Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – КиївіООО "Д.В.К.", 2004
2	Адміністратор Администратор Administrator, manager		Користувач, роль якого включає функції керування системою комп'ютерною і (або) комплексом засобів захисту.	[4] – 24 с.
3	Аналіз Анализ Analysis		Метод дослідження, що полягас в мисленому або практичному розчленуванні питого на складові частини.	[4] –33 с.

1	2	3	4	5
4	Антивірус Антивирус Antivirus		В обчислювальній техніці – програма, що виявляє або виявляє та знищує віруси комп'ютерні.	[4] – 38 с.
5	Атака Атака Attack		Дії порушника, спрямовані на порушення однієї з функцій захисту інформації (причетності, автентифікації, цілісності, доступності, конфіденційності); зловмисна дія.	[4] – 44 с.
6	Безпека комп'ютерних систем Безопасность компьютерных систем Computer security		Такий стан комп'ютерних систем, при якому забезпечується без пека даних, які обробляються ними.	[4] – 60 с.
7	Витік інформації Утечка информации Information leakage		Несанкціонований процес перенесения інформації від джерела до зловмисника.	[4] – 76 с.
8	Вірус комп'ютерний Вирус компьютерный Computer virus		Специальна програма, що здатна самочинно розмножуватися, створюючи свої копії, і поширюватися, модифікуючи (заражаючи) інші програми шляхом приеднання до них для наступного одержання управління та відтворення нових копій.	[4] – 94 с.
9	Дискета ключова Дискета ключевая Key diskette		Дискета, що містить ключі системи захисту інформації.	[4] – 130 с.
10	Доступ несанкціонований до інформації Доступ несанкционированный к информации Unauthorized access to information	НСД НСД	Доступ до інформації під час якого порушуютвся встановлені правові норми і порядок його здійснення (правила розмежування доступу).	[4] – 149 с.
11	ЕОМ ЭВМ Computer	ЕОМ ЭВМ	Комплекс технічних засобів, призначений для автоматичного оброблення ін-формації в процесі вирішення задач обчислювальних і завдань інформаційних.	[4] – 158 с.

1	2	3	4	5
12	Журнал контрольний Журнал контрольный Audit journal		Журнал, в якому реєструються події, що мають відношення до забезпечення безпеки обчислювальної системи, зокрема, звернення до захищених даних.	[4] – 163 с.
13	Загроза безпеці обчислювальної системи Угроза безопасности вычислительной системы Threat		Впливи на систему обчислювальну, які прямо або побічно можуть нанести шкоду її безпеці.	[4] – 178 с.
14	Зашифровування Зашифровывание Encryption		Процес перетворення тексту відкритого до виду, незрозумілого несанкціонованому користувачеві (в шифротекст).	[4] – 222 с.
15	Ідентифікатор Идентификатор Identification		Лексична одиниця, що використо-вується як ім'я для елементів мови; ім'я, що присвоюється даним і являє собою послідовність латинських літер і цифр, яка починається з літери.	[4] – 233 с.
16	Ідентифікація Идентификация Identification		Надання суб'єктам і об'єктам доступу ідентифікатора і (або) порівняння пред'явленого ідентифікатора з переліком наданих ідентифікаторів.	[4] – 234 с.
17	Конфіденціиність інформації Конфиденциальность информации Information confidentiality		Властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом.	[4] – 304 с.
18	Розмежування доступу до інформації Разграничение доступа к информации Differentiation		Сукупність заходів, які здійснюють розділення інформації на частини і організацію доступу до неї посадових осіб у відповідності до їхніх функціональних обов'язків і повноважень.	[4] – 574 с.

1	2	3	4	5
19	Розшифровування Расшифрование Decryption		Процес перетворення ши-фротексту у текст відкритий при відомому ключі; процес, зворотний процесу зашифровування.	[4] – 576 с.
20	Шифрування Шифрование Encryption		Процес зашифровування або розшифровування. Процес перетворення криптографічного даних, за допомогою якого текст відкритий перетворюється в шифртекст з метою захисту від несанкціонованого доступу.	[4] – 744 с.

Перелік використаних скорочень та позначень

У цьому навчальному посібнику використовуються такі позначення й скорочення:

АРМ – автоматизоване робоче місце
АС – автоматизована система
БД – база даних
В/В – введення/виведення
ЖФ – журнальний файл
ЕОД – електронне опрацьовування даних
ЕОМ – електронна обчислювальна машина, комп'ютер
ІБ – інформаційна безпека
ІзОД – інформація з обмеженим доступом
ІК – ідентифікаційний код
ІТ-безпека – безпека інформаційної технології
ІТ-система – системи інформаційної технології
ІТ-продукт – продукт інформаційної технології
КЗЗ – комплекс засобів захисту
КСЗІ – комплексна система захисту інформації
ЛОМ – локальна обчислювальна мережа
НГМД – нагромаджувач на гнучких магнітних дисках
НД ТЗІ – нормативний документ системи технічного захисту інформації
НСД – несанкціонований доступ
НСЗ – несанкціоноване завантаження
ОС – операційна система
ПБ – політика безпеки
ПЗУ (ПЗП) – постійний запам'ятовувальний пристрій
ПЗ – програмне забезпечення
ПЕОМ – персональна електронна обчислювальна машина, персональний комп'ютер
ПЕМВН – побічні електромагнітні випромінювання і наведення
ПК – персональний комп'ютер
СЗІ – система захисту інформації
СУБД – система управління базами даних
ТЗІ – технічний захист інформації
OSI (ВВС) – взаємодія відкритих систем
SDU – блок сервісних даних
SMIB – бази керування безпекою інформації
MIB – інформаційна база керування
ISO/SEC – міжнародні організації стандартів

Позначення послуг безпеки згідно з НД ТЗІ 2.5-004:
ДВ-1 – ручне відновлювання
ДЗ-1 – модернізація
ДР-1 – квоти

ДС-1 – стійкість за обмежених відмовлянь
КА-2 – базова адміністративна конфіденційність
КВ-1 – мінімальна конфіденційність при обміні
КД-2 – базова довірча конфіденційність
КО-1 – повторне використання об’єктів
НВ-1 – автентифікування вузла
НИ-2 – поодиночна ідентифікування та автентифікування
НК-1 – однонаправлений вірогідний канал
НО-1 – розподіл обов’язків
НО-2 – розподіл обов’язків адміністраторів
НТ-1 – самотестування за запитом
НТ-2 – самотестування при старті
НР-2 – захищений журнал
НЦ-1 – КЗЗ з контролем цілісності
НЦ-2 – КЗЗ з гарантованою цілісністю
ЦА-1 – мінімальна адміністративна цілісність
ЦА-2 – базова адміністративна цілісність
ЦВ-1 – мінімальна цілісність при обміні
ЦД-1 – мінімальна довірча цілісність
ЦО-1 – обмежений відкот

Тезаурус

Автентифікування (authentification) – процедура перевіряння відповідності пред’явленого ідентифікатора об’єкта комп’ютерної системи на предмет приналежності його до цього об’єкта; встановлення чи потвердження автентичності.

Автентифікаційна інформація – інформація, використовувана для встановлення законності потрібної особи.

Автентифікування однорівневих об’єктів – потвердження, що однорівневий у спілкуванні об’єкт є саме той, який потрібен.

Обмін автентифікаційною інформацією – механізм, призначений для завірення особистості об’єкта шляхом обміну інформацією.

Пароль (password) – конфіденційна автентифікаційна інформація, яка складається здебільшого з послідовності символів і яку слід ввести для отримання доступу.

Ідентифікування (identification) – процедура надавання ідентифікатора об’єктові комп’ютерної системи чи встановлення відповідності поміж об’єктом та його ідентифікатором; розпізнавання.

Ідентифікування походження даних – потвердження, що джерело даних визначено у належний спосіб.

Персональний ідентифікаційний номер; ПІН (personal identification number, PIN) – вид паролю, який здебільшого складається лише з цифр, і який, як правило, має бути пред’явлено нарівні з носимим ідентифікатором.

Авторизація – надавання прав, які включають надавання доступу на підставі права доступу.

Аудит захисту – незалежний огляд й експертиза системних записів та дій, щоби випробувати на адекватність системний контроль, гарантувати відповідність встановленої політики й операційних процедур, аби виявляти порушування у захисті й рекомендувати відповідні змінення в керуванні, політиці й процедурах.

Журнал аудиту захисту – зібрані й потенційно корисні дані для полегшування аудиту захисту.

Аналізування трафіка – виведення інформації від спостерігання потоків трафіка (наявність, відсутність, кількість, напрямок та частота).

Виявлення маніпуляції – механізм, використовуваний для виявлення того, чи було блок даних змінено випадково чи зумисно.

Відповідальність – властивість, яка гарантує, що дії об'єкта може бути відстежено винятково щодо об'єкта.

Вибірковий польовий захист – захист певних полів у межах повідомлення, яке має бути передане.

Довірче функціонування – функціональні можливості, сприймані, як правильні стосовно певних критеріїв, наприклад, як встановлено політикою захисту.

Загроза – потенційне порушування захисту.

Активная загроза – загроза зумисного неправочинного змінення стану системи. За прикладом активних загроз, які порушують безпеку, можуть слугувати: модифікування повідомлень, повторне використання повідомлень, вставлення фальшивих повідомлень, маскарад під авторизований об'єкт та відмова в обслуговуванні.

Пасивна загроза – загроза протиправного розкривання інформації без змінення стану системи.

Відмова – спростування одним із об'єктів, включених у зв'язок, того, що взято участь у всьому чи в частині сеансу зв'язку.

Маскарад – намагання певного об'єкта подати себе за інший об'єкт.

Відмовлення в обслуговуванні – перешкодження авторизованого доступу до ресурсів чи затримування операцій, які критичні у часі.

Заповнення трафіка зайвою інформацією – генерація фальшивих випадків зв'язку, фальшивих блоків даних та/чи фальшивих даних у межах блоків даних.

Контроль доступу – попередження неавторизованого використання ресурсу, включаючи попередження використання ресурсу в неавторизований спосіб.

Список контролю доступу – список об'єктів разом з їхніми правами доступу, уповноважених мати доступ до ресурсу.

Повноваження – дані, передані, аби встановити потрібну особистість об'єкта.

Можливості – символ, використовуваний як ідентифікатор ресурсу у таий спосіб, що володіння символом надає права доступу до ресурсу.

Позначка (мітка) захисту – має позначати ресурс (котрий може бути й блоком даних), який називає чи визначає атрибути захисту цього ресурсу. Маркування та/чи зв'язки можуть бути явні чи неявні.

Ступінь важливості – характеристика ресурсу, яка схарактеризовує його значення чи важливість, і може включати його вразливість.

Канал – шлях для передавання інформації.

Конфіденційність – властивість, завдяки якій інформація не стає доступною чи відкритою неправочинним особам, об'єктам чи процесам.

Цілісність інформації – властивість, що дані не було змінено чи знищено у противочинний спосіб.

Доступність – властивість доступності й придатності до використання після запиту авторизованим об'єктом.

Таємність – право особистостей управляти чи впливати на те, яку інформацію, пов'язану з ними, може бути зібрано й збережено; а також на те, кому й ким цю інформацію може бути розкрито.

Політика захисту – набір критеріїв для забезпечування сервісів безпеки. Завершена політика захисту неодмінно включає функції та механізми поза можливостямс відкритої системи, котрі визначаються організаційними, організаційно-технічними заходами тощо.

Політика захисту на підставі ідентифікаційної інформації – політика захисту, яка грунтується на ідентифікаційній інформації та/чи атрибутах окремих користувачів, груп користувачів, чи об'єктів, котрі діють від імені користувачів і отримують доступ до ресурсів/об'єктів.

Політика захисту на підставі правил – політика захисту, яка грунтується на глобальних правилах, наданих для всіх користувачів. Ці правила здебільшого базуються на порівнянні ступеня важливості ресурсів, які отримують доступ й право володіння відповідними атрибутами окремих користувачів, груп користувачів, чи об'єктів, котрі діють від імені користувачів.

Сервіс безпеки – сервіс, забезпечуваний рівнем зв'язку відкритих систем, котрий гарантує адекватний захист систем чи передаваних даних.

Конфіденційність трафіка – сервіс конфіденційності для захисту проти аналізування трафіка.

Шифрування – галузь техніки, яка зреалізовує принципи, засоби й методи перетворення даних для приховування змісту інформації, аби попереджувати її невиявлене модифікування та/чи попереджувати її неправочинне використання. Ці методи використовуються у шифруванні й дешифруванні. Внаслідок криптографічного перетворення даних здобувається шифротекст. Вплив на криптографічні принципи, засоби чи методи називається криптоаналізом.

Криптоаналіз – аналізування криптографічної системи та/чи її вводів та виводів, що використовується, аби здобути конфіденційні змінні та/чи таємні дані, включаючи чистий текст.

Чистий текст – зрозумілі дані, семантичний зміст яких є доступний.

Шифротекст – дані, випродуковані за допомогою шифрування. Внаслідок шифрування семантичний зміст даних стає не доступний.

Дешифрування – перетворення, протилежне до шифрування.

Ключ – послідовність символів, яка управляє операціями шифрування й дешифрування.

Керування ключами – генерування, зберігання, розподіл, знищування, архівування й застосовування ключів у відповідності з політикою безпеки.

Криптографічна контрольна величина – інформація, здобута при виконанні криптографічного перетворення блока даних.

Цифровий підпис – дані, які додано наприкінці, чи криптографічне перетворення блока даних, яке дозволяє довести джерело і цілісність блока даних отримувачеві повідомлення й захищає блок даних від підробляння, приміром отримувачем повідомлення.

Нотаризація – реєстрування даних довіреною третьою особою, яка дозволяє з часом потвердити точність його характеристик: змісту, походження, часу й доставляння.

Фізична безпека – заходи, які забезпечують фізичний захист ресурсів проти зувмисних та випадкових загроз.

Керування маршрутизацією – застосовування правил протягом процесу маршрутизації, щоби обрати чи відхилити певні мережі, канали зв’язку чи передавання.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1 Закон України "Про інформацію" від 02.10.92 р.

2 Закон України "Про державну таємницю" від 21.12.94 р.

3 Закон України "Про науково-технічну інформацію".

4 Закон України “Про захист інформації в автоматизованих системах” від 05.07.1994.

5 Закон України “Про зв’язок”. Від 16.11.2003 р.

6 Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. № 1229.

7 Концепція технічного захисту інформації в Україні. – 1997.

8 Концепція технічного захисту інформації в галузі зв’язку України. – 1999.

9 ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

10 ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

11 ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

12 НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

13 НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.

14 НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу (Критерії базуються на аналізі Федеральних критеріїв США і критеріїв оцінки безпеки Канади).

15 НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

16 НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

17 НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

18 НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

19 НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

20 НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супровадження і модернізації засобів технічного захисту інформації від несанкціонованого доступу.

21 НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

22 НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення.

23 НД ТЗІ 2.5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту.

24 НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.

25 НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту.

26 НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.

27 НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінювання захищеності інформації (базова).

28 Recomendation CCITT X.800. Security architecture for open systems interconnection for CCITT applications. Geneva.1991; Стандарт ISO 7498-2:1989. Архітектура безпеки ВВС.

29 Recomendation CCITT X.200. Reference Model of open systems interconnection for CCITT applications. Geneva.1991; Стандарт ISO 7498-1:1984. Базова модель ВВС.

30 ISO/IEC 17799:2000 (BS 7799). Практичні рекомендації з керування інформаційною безпекою.

31 Стандарт ISO/IEC 15408:2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 1: Introduction and general model.

32 Стандарт ISO/IEC 15408:2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 2: Security functional requirements.

33 Стандарт ISO/IEC 15408:2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 3: Security assurance requirements.

34 Домарев В. В. Защита информации и безопасность компьютерных систем. К.: Диасофт, 1999. – 480 с.

35 Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.

36 Герасименко В.А. Размахин М. К. Защита информации в вычислительных информационных и управляющих системах и сетях // Зарубежная радиоэлектроника. –1984. –№ 8.

37 Тардаскін М.Ф., Кононович В.Г. Технічний захист комерційної таємниці підприємства зв'язку: Навч. посібник/ За ред. М.В. Захарченка. – Одеса: ОНАЗ, 2002. – 76 с.

38 Банкет В. Л., Захарченко Н. В., Дырда А. В., Гулак Г. Н., Владишевский Б. С. Защита информации в системах телекоммуникации. Одесса-1997.

ЗМІСТ С.

Навчальне видання

Голев Денис Володимирович,
Кільдишев Віталій Йосипович,
Кононович Володимир Григорович

ІНФОРМАЦІЙНА БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ
Лабораторний практикум
Частина 1 – Комплекси засобів захисту інформації від НСД

Навчальний посібник

Редактор *Л.А. Кодрул*
Комп'ютерне верстання *Ж.А. Гардиман*

Здано до набору
Підписано до друку Обсяг ум. -друк. арк.
Формат Зам. № Наклад прим.
Видруковано на видавничому устаткуванні фірми RISO
в друкарні редакційно-видавничого центру ОНАЗ ім. О.С. Попова
Одеса, 65021, вул. Старопортофранківська, 61
Тел. (0482) 207-894