Міністерство освіти і науки України
Національний університет водного господарства та природокористування

Кафедра водопостачання, водовідведення та бурової справи

01-04-09

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни:
«ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ ТЕХНОЛОГІЯХ»

для студентів спеціальності
7.06010108 "Водопостачання та водовідведення".

Рекомендовано методичною комісією за спеціальністю 7.06010108 "Водопостачання та водовідведення".
Протокол № 3 від 12 листопада 2013р.

Рівне, 2014

Методичні вказівки до виконання лабораторних робіт з дисципліни «Захист інформації в комп'ютерних технологіях» для студентів спеціальності 7.06010108 "Водопостачання, водовідведення". / Мартинов С.Ю., Косінов В.П. – Рівне: НУВГП, 2014 – 24с.

Упорядники: С.Ю. Мартинов, канд. техн. наук, доц.;
В.П. Косінов, канд. техн. наук, доц.

Відповідальний за випуск – В.О. Орлов, д-р техн. наук, професор, завідувач кафедри водопостачання, водовідведення та бурової справи.

ЗМІСТ

ВСТУП

На даний час інформація стає головним ресурсом науково-технічного розвитку світового суспільства. Будь-яка діяльність людини, пов'язана з отриманням, накопиченням, обробкою та використанням різноманітних інформаційних потоків. Одними із найпоширеніших джерел отримання інформації є комп'ютерні мережі, глобальні мережі та розповсюдження інформації на електронних носіях. Розвиток сучасних інформаційних технологій супроводжується зростанням числа комп'ютерних злочинів і пов'язаних з ними розкрадань інформації, а також матеріальних втрат. За даними досліджень біля третини атак спрямовано на промислові секрети або документи, що є цікавим, перш за все, для конкурентів. Тому захист інформації в комп'ютерних технологіях набуває першочергового значення. Метою лабораторних робіт є вивчення та закріплення найпоширеніших способів захисту комп'ютерної інформації та проведення аналізу надійності деяких з них.

Лабораторна робота № 1

ВІРУСИ. АНТИВІРУСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Мета роботи:

1. З'ясувати класифікацію комп'ютерних вірусів, способи поширення та засоби захисту комп'ютерної інформації.
2. Отримати практичні навички роботи з антивірусним програмним забезпеченням **Dr.Web**.

Загальні відомості

Віруси. Комп'ютерні віруси - вид шкідливого програмного забезпечення. Це програми, що володіють здатністю до самовідтворення (розмноження) у середовищі стандартної операційної системи шляхом включення в програми своєї копії або модифікованої копії, здатної до подальшого розмноження. Зазначена властивість характерна всім типам комп'ютерних вірусів.

Термін «комп'ютерний вірус» вперше вжив співробітник Лехайского університету (США) Ф. Коен на конференції по безпеці інформації в 1984 році.

Умовно комп'ютерні віруси можна підрозділити на класи (рис. 1.1). Життєвий цикл комп'ютерного вірусі може включати наступні етапи:

- впровадження (інфікування);
- інкубаційний період;
- саморозмноження (репродукування);
- виконання спеціальних функцій;
- прояв.

Комп'ютерні віруси можуть необмежений час зберігатися на картах пам'яті і жорстких дисках, а потім випадково або навмисно інфікувати комп'ютер при використанні заражених файлів.

Вірус проникає в комп'ютер тільки при виконанні зараженої програми. Але, якщо комп'ютер уже заражений, то практично будь-яка операція на ньому може призвести до зараження програм і файлів, що знаходяться в пам'яті або підключених змінних носіях пам'яті.

При наявності в пам'яті комп'ютера програм їз тілом вірусу можуть заражатися як програми, що виконуються, так і, ті що зберігаються на жорсткому диску.

Копія вірусу вставляється в заражену програму таким чином, щоб при запуску зараженої програми вірус одержав керування в першу чергу. Першою і обов'язковою дією вірусу при виконанні інфікованої програми є саморозмноження. Цей етап може тривати аж до знищення вірусоносія. Одночасно з впровадженням або після деякого проміжку часу, визначеного числом впроваджених копій, вірус приступає до виконання спеціальних функцій, іменованих ще логічними бомбами, що вводяться в програмне забезпечення і спрацьовують тільки при виконанні визначених умов,

наприклад, по сукупності дати і часу, і частково або цілком виводять з ладу комп'ютерну систему.

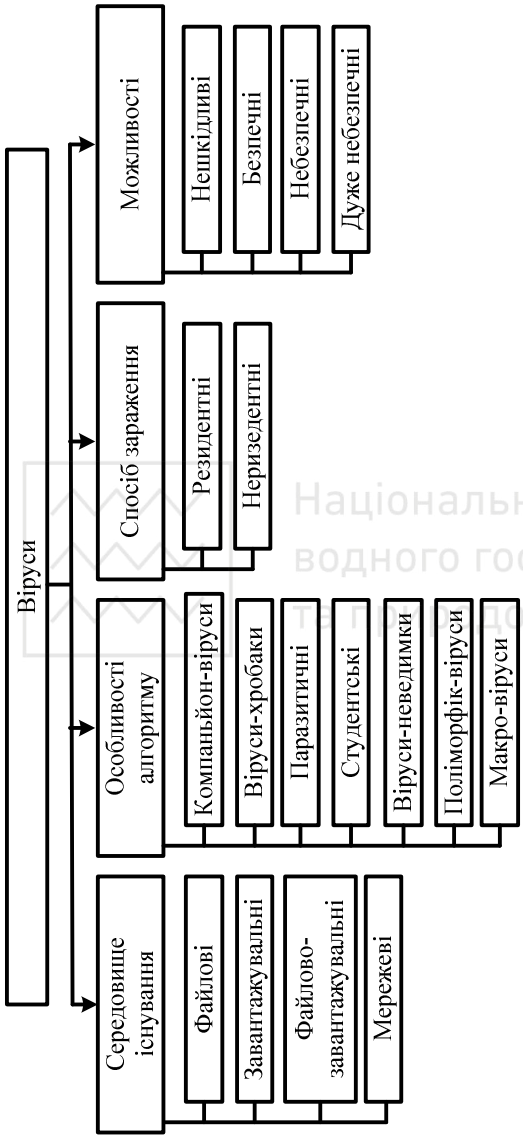

Рис. 1.1 Класифікація комп'ютерних вірусів

Крім того, частина комп'ютерних вірусів має фазу прояву, що супроводжується візуальними або звуковими ефектами. Окремі віруси повідомляють користувачеві про зараження комп'ютера.

Усі відомі віруси можна розділити на класи за наступними ознаками:

- середовище існування;
- спосіб зараження середовища існування;
- деструктивна можливість;
- особливості алгоритму вірусу.

За середовищем існування комп'ютерні віруси можна розділити на завантажувальні, файлові, файлово-завантажувальні і мережеві.

Завантажувальні (бітові) віруси впроваджуються в завантажувальний сектор диска (boot-сектор) або в сектор, що містить системний завантажник жорсткого диску (Master Boot Record).

Файлові віруси - у найпростішому випадку такі віруси заражають файли, що виконуються. До файлових відносяться так звані macro-віруси.

Файлово-завантажувальні віруси заражають файли і завантажувальні сектори дисків. Такі віруси, як правило, працюють по досить складних алгоритмах і

часто застосовують оригінальні методи проникнення в систему.

Мережеві віруси поширюються по комп'ютерній мережі. Варіанти зараження вірусами наведені на рис. 1.2.

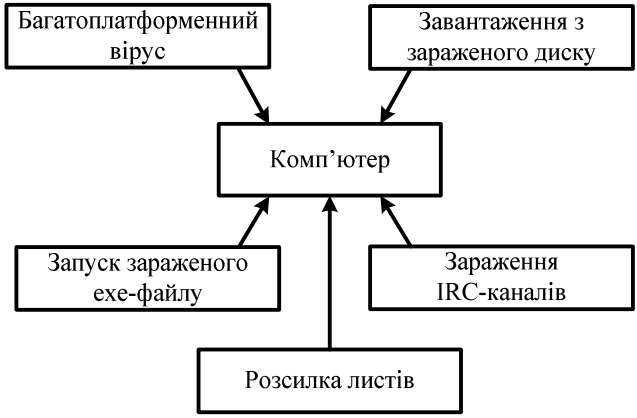

Рис. 1.2 Варіанти зараження вірусами

Віруси, можуть розмішуватися в наступних системах і структурах:

- операційній системі, де вони «зливаються» із програмами, розташованими в системній частині дискети або жорсткого диска;
- бібліотеках компіляторів для впровадження в програми, що складаються компіляторами;
- мережевих драйверах;
- «поганих» або спеціальних секторах жорсткого диска;
- ПЗП (постійна пам'ять) як програмно-технічна закладка;
- структурах програм, що виконуються, або файлових програм.

Способи зараження середовища існування поділяються на резидентний і нерезидентний.

Резидентний вірус при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, що потім перехоплює звертання операційної системи до об'єктів зараження і впроваджується в них. Відбувається це в такий спосіб: резидентний вірус запитує в системи ділянки пам'яті і копіює себе в нього. Він перехоплює переривання, аналізує їх і забезпечує тим самим керування процесором комп'ютера. Якщо наступним етапом життєвого циклу вірусу є інкубаційний період, то вірус ніяк не виявляє себе упродовж визначеного проміжку часу або до досягнення визначеного числа підходящих об'єктів зараження. Після цього настає етап розмноження. Знайшовши звертання до компонентів системи, придатних для зараження, вірус активізує процедуру копіювання. Звичайно ця процедура передбачає перевірку, чи не є вже присутньою в об'єкті копія вірусу (якщо копія присутня, то об'єкт уже заражений); окремі віруси перевіряють номер

версії і заражають об'єкт, якщо їх версія більш нова. Якщо копії вірусу немає, то він копіюється з пам'яті в об'єкт, що заражається, з модифікацією його першої команди. Об'єктами зараження в цьому випадку можуть бути програми, що виконуються, на жорсткому диску і дискетах. Резидентні віруси знаходяться в пам'яті і активні аж до вимикання або перезавантаження комп'ютера.

Нерезидентні (транзитні) віруси не залишаються в пам'яті після виконання зараженої програми. У цьому випадку, вірус перед передачею керування вихідній програмі, шукає ще не заражений файл, придатний для впровадження. Тоді, виконання спеціальних функцій не завжди іде за етапом саморозмноження, щоб встигнути створити достатню кількість своїх копій, перш ніж факт зараження буде виявлений. Тому, механізм виконання спеціальних функцій включається досить рідко і шкідливі наслідки вірусу спочатку можуть бути непомітні. Коли ж користувач помітить зміни в роботі комп'ютера, може виявитися, що вірусом уражені практично всі файли системи.

Відомі на даний час віруси можуть здійснювати наступні руйнівні функції:

- зміна даних у файлах;
- зміна даних, переданих через паралельні і послідовні порти;
- зміна призначеного диска (запис інформації виконується не на диск, зазначений користувачем, а на диск, зазначений вірусом);
- перейменування файлів (не повідомляючи про це користувачеві);
- форматування окремих частин жорсткого диска або навіть усього диска;
- знищення каталогу диска;
- порушення працездатності операційної системи, в результаті чого вона не сприймає зовнішніх дій користувача і вимагає перезавантаження;
- зниження продуктивності через постійне виконання паразитних програм;
- відмова у виконанні визначеної функції (наприклад, блокування клавіатури, блокування завантаження програми із захищеної від запису дискети і т.д.);
- стирання інформації, виведеної на екран дисплея і т.п.;
- «дрібні» ушкодження даних (наприклад, заміна перших байтів кожного блоку при записі, заміна окремих символів і т.д.), які користувач довго не може знайти.

За особливостями алгоритму функціонування віруси поділяють на:

- компаньйони-віруси (companion);
- віруси-хробаки (worm);
- паразитичні;
- студентські;
- stealth-віруси (віруси-невидимки);
- поліморфік-віруси (polymorphic);

- макро-віруси.

Компаньйони-віруси (companion) представлені програмами, що не змінюють файли. Ці віруси створюють для Exe-файлів, що знаходяться в пам'яті комп'ютера, файли-супутники, що мають те ж саме ім'я, але з розширенням COM, наприклад, для файла XCOPY.EXE створюється файл XCOPY.COM. Вірус записується в Com-файл і ніяк не змінює Exe-файл. При запуску такого файлу DOS першим знайде і виконає COM -файл, тобто вірус, що потім запуститься, і EXE -файл.

Віруси-хробаки поширюються в комп'ютерних мережах. Вони, як і компаньйони-віруси, не змінюють файли або сектори на дисках. Вони проникають у пам'ять комп'ютера з комп'ютерної мережі, обчислюють мережеві адреси інших комп'ютерів і розсилають по цих адресах свої копії. Такі віруси іноді створюють робочі файли на дисках системи, але можуть узагалі не звертатися до ресурсів комп'ютера (за винятком оперативної пам'яті).

Паразитичні віруси при поширенні своїх копій обов'язково змінюють вміст дискових секторів або файлів. До цієї групи відносяться усі віруси, що не є вірусами-хробаками або компаньйонами-вірусами.

Студентські віруси - це вкрай примітивні віруси, часто нерезидентні та мають багато помилок.

Stealth-віруси, або віруси-невидимки, являють собою досить досконалі програми, що перехоплюють звертання DOS до уражених файлів або секторів дисків і «підставляють» замість себе незаражені ділянки інформації. Крім цього, такі віруси при звертанні до файлів використовують досить оригінальні алгоритми, що дозволяють обманювати резидентні антивірусні програми.

Поліморфік-віруси - це віруси, що важко виявляються, не мають сигнатур, тобто не мають жодної постійної ділянки коду. У більшості випадків два зразки того самого поліморфік-вірусa не будуть мати жодної схожості. Це досягається шифруванням основного тіла вірусу і модифікаціями програми-розшифровувача.

Формально macro-віруси є файловими вірусами, що заражають файли деяких систем обробки документів (наприклад, Word, Excel). Зазначені системи мають вбудовані макро-мови (VBA). Ці мови мають достатні можливості, щоб робити практично всі операції, необхідні вірусові. Є навіть шифровані і поліморфні macro-віруси.

В даний момент більш 90% macro-вірусів написані для Word. Це тому, що файли даного текстового процесора фактично стали стандартом для текстових документів.

Більшість макро-вірусів мають типову структуру. Вони починаються з макросу, що автоматично виконується, і заражають шаблон Normal.dot. Макрос - це програма, написана на деякій мові, і використовується для автоматизації визначених процесів усередині додатків.

Стратегія антивірусного захисту. Для організації ефективного антивірусного захисту необхідна наявність відповідного антивірусного засобу. Незважаючи на всю різноманітність сучасних антивірусних програмних продуктів, принципи їх роботи однакові. До основних функцій сучасних антивірусів відносяться:

- сканування пам'яті і вмісту дисків за розкладом;
- сканування пам'яті комп'ютера, а також файлів, що записуються і читаються, у реальному режимі часу за допомогою резидентного модуля;
- вибіркове сканування файлів зі зміненими атрибутами (розміром, датою модифікації, контрольною сумою і т.д.);
- сканування архівних файлів;
- розпізнавання поводження, характерного для комп'ютерних вірусів;
- віддалена установка, настроювання та адміністрування антивірусних програм з консолі системного адміністратора; оповіщення системного адміністратора про події, пов'язані з вірусними атаками, по електронній пошті;
- примусова перевірка підключених до корпоративної мережі комп'ютерів, яка ініціюється системним адміністратором;
- віддалене відновлення антивірусного програмного забезпечення і баз даних з інформацією про віруси, у тому числі автоматичне відновлення баз даних по вірусах за допомогою Internet;
- фільтрація трафіка Internet на предмет виявлення вірусів у програмах і документах, переданих за допомогою протоколів SMTP, FTP, HTTP;
- виявлення потенційно небезпечних Java-аплетів і модулів Active;
- функціонування на різних серверних і клієнтських платформах, а також у гетерогенних корпоративних мережах;
- ведення протоколів, що містять інформацію про події, які стосуються антивірусного захисту.

Наявність антивірусного програмного забезпечення - це обов'язкова, але недостатня умова для відбиття вірусної атаки. Мало мати у своєму розпорядженні засіб, варто продумати і методи його правильного використання. Захист від вірусів повинен бути елементом політики безпеки, яку розуміють і дотримуються усі користувачі системи.

Стратегія антивірусного захисту повинна блокувати всі можливі точки проникнення вірусів, такі як:

- проникнення вірусів на робочі станції при використанні на робочій станції інфікованих файлів з переносних джерел (флоппі-диски, компакт-диски і т.д.);
- зараження вірусами за допомогою безкоштовного інфікованого програмного забезпечення, отриманого з Internet через Web або FTP і збереженого на локальній робочій станції;
- проникнення вірусів при підключенні до корпоративної мережі

інфікованих робочих станцій віддалених користувачів;

- зараження вірусами з віддаленого сервера, приєднаного до корпоративної мережі, що обмінюється інфікованими даними з корпоративними серверами;
- поширення електронної пошти, яка містить у додатках файли Excel і Word, інфіковані макровірусами.

Для вирішення задач боротьби з вірусними атаками необхідно:

- відповідним чином сконфігурувати антивірусне програмне забезпечення;
- використовувати тільки ліцензійне програмне забезпечення;
- обмежити набір програм, які користувач здатний встановити в системі;
- усунути відомі вразливості у програмному забезпеченні;
- контролювати використання нагромаджувачів гнучких дисків і дисків CD, DVD;
- розробити політику обробки електронної пошти;
- розробити політику безпеки додатків, що обробляють документи.

Щоб відповідним чином сконфігурувати антивірусне програмне забезпечення, необхідно зробити наступні установки антивірусу:

- повинно бути дозволено сканування в режимі реального часу, у фоновому або аналогічному режимі;
- при старті системи потрібно сканувати пам'ять, завантажувальний сектор і системні файли;
- вчасно обновляти вірусні бази даних;
- бажано сканувати файли всіх типів або, як мінімум, COM-, Exe-файли, а також файли типу VBS, SHS, OCX;
- встановити аудит усіх дій антивірусних програм.

В зв'язку з тим, що повідомлення електронної пошти - один із самих популярних і швидких способів поширення вірусів, то для захисту від проникнення вірусів через повідомлення електронної пошти кожен користувач системи повинен:

- ніколи не відкривати відразу поштове вкладення в повідомленні, що прийшло йому, а зберігати його у визначеному «карантинному» каталозі;
- ніколи не відкривати поштових вкладень, що не були запитані або про які не було повідомлення від відправника (навіть коли відправник відомий, повідомлення може містити вірус, якщо відправник невідомий, повідомлення з вкладенням найкраще видалити);
- перед відкриттям вкладення обов'язково перевірити його за допомогою антивірусного програмного забезпечення;
- якщо після виконання всіх цих процедур залишилися сумніви, варто зв'язатися з відправником і з'ясувати в нього інформацію про послане вкладення;
- усунути можливі вразливості в клієнтському поштовому програмному забезпеченні.

Для виявлення та знищення вірусів розроблена велика кількість

антивірусних програм. Найбільшого поширення набули **DrWeb** та **AVP**.

Таблиця 1.1

Порівняльна характеристика антивірусних програм

Найменування	Boot	Standart	Polymorphic	Macro
UNA	100%	99,7%	100%	100%
Dr Solomon's AVTK	100%	100%	98,4%	98,9%
DrWeb	94,4%	97,8%	100%	99,5%
IBM AntiVirus	100%	99,7%	92,3%	96,2%
McAfee VirusScan	100%	98,0%	90,1%	99,5%
AVP	100%	94,4%	95,2%	90,3%
Symantec Norton AntiVirus	100%	84,4%	83,6%	94,3%

Вибір одного "найкращого" антивірусу є вкрай помилковим рішенням. Рекомендується використовувати декілька різних антивірусних пакетів одночасно. Вибираючи антивірусну програму потрібно звернути увагу на такий параметр, як кількість сигнатур, що розпізнаються (послідовність символів, які гарантовано розпізнають вірус). Другий параметр - наявність евристичного аналізатора невідомих вірусів, його присутність дуже корисна, але суттєво уповільнює час роботи програми.

Практична частина

DrWeb - антивірус з сильним алгоритмом знаходження вірусів. Він є поліфагом, тобто може знаходити і знищувати відомі йому віруси. DrWeb може «читати» упаковані файли і архіви, файли даних в форматах Word і Excel, роззброює поліморфні віруси. Евристичний аналізатор DrWeb, що досліджує програми в пошуку ділянок коду, характерних для вірусів, дозволяє знайти біля 90% невідомих вірусів. При завантаженні програми, спочатку DrWeb перевіряє самого себе на цілісність, після чого тестує ОЗП. Алгоритм роботи цього антивірусу заключається в тому, що він емулює роботу процесора (створює програмну модель комп'ютера). Нові версії з'являються нечасто. Програма може працювати у діалоговому режимі, має дуже зручний інтерфейс, який можна настроювати.

Dr.Web для Windows містить у собі наступні компоненти:

1. **Dr.Web Сканер для Windows** – антивірусний сканер із графічним інтерфейсом. Програма запускається по запиту користувача або за розкладом і проводить антивірусну перевірку комп'ютера. Існує також версія програми з інтерфейсом командного рядка (**Dr.Web Консольный сканер для Windows**).
2. **SpIDer Guard для Windows** – антивірусний сторож (називається також монітором). Програма постійно знаходиться в оперативній пам'яті, здійснюючи перевірку файлів «на льоту», а також виявляє прояви вірусної активності.
3. **SpIDer Mail** для робочих станцій Windows – поштовий антивірусний

сторож. Програма перехоплює звернення будь-яких поштових клієнтів комп'ютера до поштових серверів по протоколах POP3/SMTP, виявляє і знешкоджує поштові віруси до одержання листів поштовим клієнтом із сервера або до відправлення листа на поштовий сервер.

4. **Модуль автоматического обновления для Windows** – дозволяє зареєстрованим користувачам одержувати оновлення вірусних баз і інших файлів комплексу, а також проводить їх автоматичне встановлення.

5. До складу програмного комплексу входить також **Планировщик заданий для Windows**, сканер для середовища DOS і ряд допоміжних програм.

Використовуючи вбудовану довідку Dr.Web необхідно:

1. Дослідити інтерфейс та поточні настроювання **Dr.Web Сканер** для Windows;
2. Провести антивірусну перевірку одного з логічних дисків комп'ютера.
3. Дослідити інтерфейс та поточні настроювання **SpIDer Mail** для робочих станцій Windows.
4. Дослідити інтерфейс та поточні настроювання **SpIDer Guard** для Windows.
5. Переглянути статистику роботи **SpIDer Guard** упродовж поточного сеансу.

Лабораторна робота №2

ЗАХИСТ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ПАРОЛІВ ТА ПАРОЛЬНІ ЗЛОМЩИКИ

Мета роботи:

1. З’ясувати можливості парольного захисту інформації. Правила складання та зберігання паролів.
2. Отримати практичні навички захисту інформації з допомогою паролів в MS Office та програмах-архіваторах і проаналізувати їх стійкість.

Загальні відомості

Основною захисною межею проти зловмисних атак у комп'ютерній мережі є система парольного захисту, що є у всіх сучасних програмних продуктах. Відповідно до сталої практики, перед початком сеансу роботи з операційною системою користувач зобов'язаний зареєструватися, повідомивши їй своє ім'я й пароль. Ім'я потрібно для ідентифікації користувача, а пароль служить підтвердженням правильності зробленої ідентифікації. Інформація, введена користувачем у діалоговому режимі, порівнюється з тією, що є у розпорядженні операційної системи. Якщо перевірка дає позитивний результат, то користувачеві стають доступні всі ресурси операційної системи, пов'язані з його ім'ям.

Найбільш ефективним є метод зламу парольного захисту операційної системи (надалі - ОС), при якому атаці піддається системний файл, що

містить інформацію про легальних користувачів й їх паролі. Однак будь-яка сучасна ОС надійно захищає паролі користувачів, які зберігаються в цьому файлі, за допомогою шифрування. Крім того, доступ до таких файлів, як правило, за замовчуванням заборонений навіть для системних адміністраторів, не говорячи вже про рядових користувачів операційної системи. Проте, у ряді випадків зловмисникові вдається шляхом різних маніпуляцій одержати у своє розпорядження файл із іменами користувачів й їх зашифровані паролі. І тоді йому допомагають так звані парольні зламщики - спеціалізовані програми, які служать для злому паролів операційних систем.

Криптографічні алгоритми, що застосовуються для шифрування паролів користувачів у сучасних ОС, є занадто стійкими, щоб можна було сподіватися відшукати методи їх дешифрування, які виявляться більш ефективними, чим тривіальний перебір можливих варіантів. Тому парольні зламщики іноді просто шифрують всі паролі з використанням того ж самого криптографічного алгоритму, що застосовується для їхнього засекречування в ОС. Потім вони порівнюють результати шифрування з тим, що записано в системному файлі, де перебувають шифровані паролі користувачів цієї системи. При цьому, як варіанти паролів, парольні зломщики використовують символьні послідовності, які автоматично генеруються з деякого набору символів. Даний спосіб дозволяє зламати всі паролі, якщо відомо їх представлення в зашифрованому вигляді, і вони містять тільки символи з даного набору.

За рахунок дуже великої кількості комбінацій, що перебираються, яка росте експоненціально зі збільшенням числа символів у вихідному наборі, такі атаки парольного захисту ОС можуть забирати занадто багато часу. Однак, добре відомо, що більшість користувачів операційних систем особливо не затрудняють себе вибором стійких паролів, тобто таких, які важко зламати. Тому, для більш ефективного підбору паролів, зломщики звичайно використовують спеціальні словники, що є заздалегідь сформованими списками слів, які найчастіше використовуються на практиці як паролі.

До кожного слова зі словника парольний зломщик застосовує одне або кілька правил, відповідно до яких воно видозмінюється й породжує додаткову множину паролів:

- виконується поперемінна зміна буквеного регістру, в якому набране слово;
- порядок проходження букв у слові міняється на зворотний;
- на початок й в кінець кожного слова приписується цифра 1;
- деякі букви змінюються на близькі по написанню цифри. У результаті, наприклад, зі слова password виходить pa55w0rd.

Це підвищує ймовірність знаходження пароля, оскільки в сучасних ОС, як правило, розрізняються паролі, набрані заголовними й малими літерами, а користувачам цих систем переконливо рекомендується вибирати такі, у яких

букви чергуються із цифрами.

Одні парольні зламщики по черзі перевіряють кожне слово зі спеціального словника, застосовуючи до нього певний набір правил для генерації додаткової безлічі паролів. Інші - попередньо обробляють весь словник за допомогою цих же правил, одержуючи новий словник більшого розміру, з якого потім черпають паролі для перевірки. З огляду на те, що звичайні словники природних людських мов складаються всього з декількох сотень тисяч слів, а швидкість шифрування паролів досить висока, парольні зламщики, що здійснюють пошук по словнику, працюють досить швидко (до однієї хвилини).

Відповідно до досліджень психологів, більшість чоловіків беруть за пароль короткі слова з ненормативної лексики, а жінки - імена улюблених чоловіків чи дітей.

Для відновлення паролів користувачів ОС Windows у символьному виді існують спеціальні парольні зломщики. Вони виконують як прямий підбір паролів, так і пошук по словнику, а також використають комбінований метод злому парольного захисту, коли як словник задіюється файл із заздалегідь обчисленими паролями, що відповідають символьним послідовностям, які часто застосовуються як паролі користувачів операційних систем. Однією з найвідоміших програм злому паролів Windows являється **LOphtCrack**. Однак варто розуміти, що програмою зламу можна скористатися так само й для перевірки надійності ваших паролів.

Однією з головних задач системного адміністратора Windows є захист інформації, що зберігається в базі даних облікових записів користувачів (Security Account Management Database, скорочено SAM), від несанкціонованого доступу. Ця база обов'язково є на кожному комп'ютері з Windows. У ній зберігається вся інформація, яка використовується для аутентифікації користувачів Windows при інтерактивному вході в систему й при віддаленому доступі до неї по комп'ютерній мережі. Із цією метою системному адміністратору необхідно:

- обмежити фізичний доступ до комп'ютерів мережі й, насамперед, до контролерів доменів;
- встановити паролі BIOS на включення комп'ютерів і на зміну їх настроювань BIOS;
- рекомендується відключити завантаження комп'ютерів із гнучких і компакт-дисків;
- для забезпечення контролю доступу до файлів і папок Windows системний розділ жорсткого диску повинен мати формат NTFS;
- каталог \winnt_root\repair засобами ОС необхідно закрити для доступу всіх користувачів, включаючи адміністраторів, і дозволяти до нього доступ тільки під час роботи утиліти RDISK, що створює в цьому каталозі архівні копії системного реєстру Windows;

- стежити за тим, де і як зберігаються дискети аварійного відновлення (Emergency Repair Disks) і архівні копії на магнітних стрічках, якщо на останніх є присутній дублікат системного реєстру Windows.

Багато користувачів архівують свої дані за допомогою популярних архіваторів ARJ, ZIP, RAR. Потім цим архівам задається пароль, а їх вміст шифрується. Цей спосіб захисту кращий, ніж у MS Word. У нього є одна серйозна перевага - вам не знадобляться додаткові криптографічні програми, оскільки шифрування здійснюється прямо в архіваторі.

Хоча захист файлів в архівах досить надійний, проте далеко не досконалий. В алгоритмах шифрування, які використовують PkZip та ін. архіватори, виявлені "діри", що дозволяють зламати архів, не тільки підібравши пароль, але й іншими способами.

Архиватор **WinRAR** займає провідне місце серед утиліт свого класу по надійності шифрування вмісту архівів. Він працює як з архівами *.zip (усіх версій), так і *.rar. При захисті архіву програми бажано використовувати формат *.rar і пароль довжиною не менш восьми символів.

Але підбір паролів до архівів ARJ, ZIP, RAR не складає особливих зусиль. Досить скористатися програмами **Advanced ARJ Password Recovery, Advanced ZIP Password Recovery, Advanced RAR Password Recovery**.

Практична частина

Для закріплення практичних навичок захисту інформації з допомогою паролів необхідно:

1. Дослідити меню захисту документів MS Word.
2. Самостійно здійснити захист будь-якого файлу MS Word.
3. Користуючись програмою Advanced Office XP Password Recovery визначити пароль для відкриття файлу **Список студентів,** встановивши наступні параметри: мінімальна довжина паролю – 1, максимальна – 4, в паролі можуть бути символи: цифри, букви англійського алфавіту верхнього та нижнього регістрів, пробіли. Відкрити та прочитати файл **Список студентів.**
4. Дослідити меню захисту документів MS Excel. Визначити відмінності захисту інформації, в порівнянні з MS Word. Здійснити захист діапазону клітинок A1:C5, заборонивши їх форматування.
5. Самостійно здійснити захист будь-якого файлу за допомогою архіватора WinRar.

Захист документів MS Word і MS Excel паролем. У Microsoft Word і Excel є спосіб захистити документи за допомогою пароля. Цього цілком достатньо, якщо інформація в даних файлах не представляє великої цінності, але розголошення її небажане. Обидві програми використовують два рівні захисту - від відкриття і запису.

Щоб установити паролі в Word, розкрийте меню **Файл** і виберіть з нього команду **Сохранить как**. Далі в Word, у вікні, що з'явилося, натисніть

кнопку **Сервис** (рис. 2.1) і виберіть опцію **Параметры безопасности** (рис. 2.2).

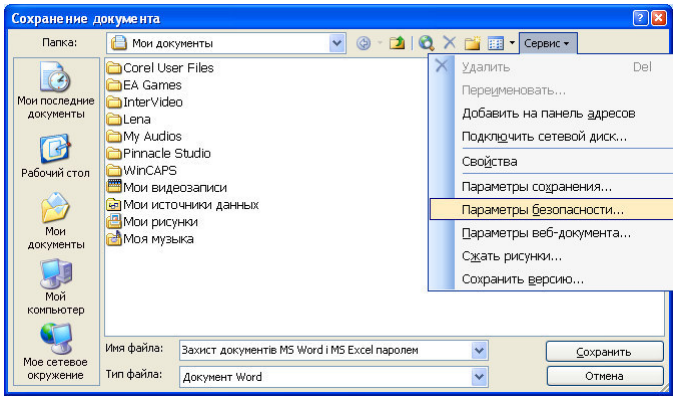

Рис. 2.1 Вікно «Сохранение документа»

Більш детально охарактеризуємо папку **Безопасность.**

1 **Параметры шифрования для данного документа**

1.1 **Пароль для открытия файла**. Задання пароля для активного документа. Документ може бути відкритий потім, тільки при введенні правильного пароля. Пароль може містити будь-яку комбінацію букв, цифр, пропусків і символів (до 15 знаків). Якщо потрібно вказати довший пароль або змінити тип шифрування за замовчуванням - натисніть кнопку **Дополнительно**. Якщо ви забули або втратили пароль - відкрити документ буде неможливо.

2 **Параметры совместного использования для данного документа**

2.1 **Пароль разрешения записи.** При заданні пароля в цьому полі відкрити документ для зміни можна буде тільки після вказівки правильного пароля. Пароль може містити будь-яку комбінацію букв, цифр, пропусків і символів (до 15 знаків). Під час вибору параметрів поліпшеного шифрування, при заданні пароля на відкриття документа, можна створити пароль збільшеної довжини. Якщо ви забули або втратили пароль, відкрити документ для зміни буде неможливо.

2.2 **Рекомендовать доступ только для чтения.** При відкритті файла виводиться повідомлення про те, що документ рекомендується відкривати тільки для читання. Якщо документ відкритий тільки для читання, внесені в нього зміни можуть бути збережені тільки під іншим ім'ям. Цей прапорець може бути встановлений без вказівки паролів.

2.3 **Цифровые подписи.** Натисніть кнопку, щоб відкрити діалогове вікно **Цифровая подпись.**

2.4 **Установить защиту**. Натисніть кнопку, щоб відкрити область задач **Установить защиту**. Використовуйте цю область задач, щоб обмежити зміну форматування і вмісту активного документа.

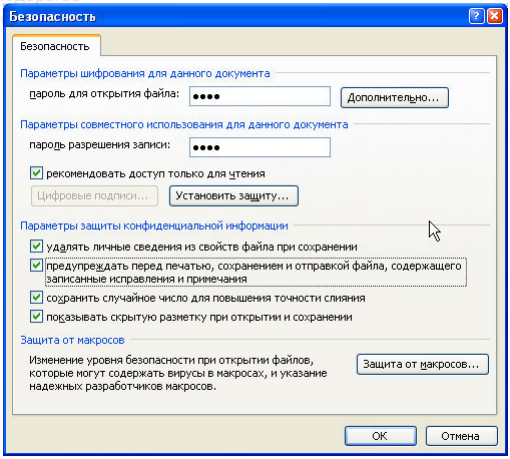

Рис.2.2 Вікно «Безопасность»

3 **Параметры защиты конфиденциальной информации**

3.1 **Удалять личные сведения из свойств файла при сохранении.** Запобігання ненавмисному розповсюдженню прихованих відомостей, таких як відомості про автора документа або про його рецензентів.

3.2 **Предупреждать перед печатью, сохранением и отправкой файла, содержащего записанные исправления и примечания.** Виведення запрошення на перегляд документа на предмет наявності в ньому виділених виправлень і приміток перед збереженням або розповсюдженням документа. Це понизить ризик випадкового розповсюдження конфіденційних відомостей.

3.3 **Сохранить случайное число для повышения точности слияния.** Використання випадкових чисел при порівнянні або об'єднанні виправлень в документах для відстежування зв'язаних документів. Не дивлячись на те, що ці числа є прихованими, вони можуть використовуватися для визначення зв'язку між двома документами. При відключенні збереження цих чисел результат при об'єднанні документів не буде оптимальним.

3.4 **Показывать скрытую разметку при открытии и сохранении.** Відображення всіх приміток, видалених елементів і інших типів виправлень. При використанні меню **Показать** на панелі інструментів **Рецензирование** для приховування всіх або тільки частини виправлень і після установки цього прапорця виправлення з'являтимуться в той момент, коли користувач відкриває файл. Вибір цього параметра не впливає на прихований текст.

4 **Защита от макросов.** Натисніть кнопку, щоб відкрити діалогове вікно **Безопасность.** Використовуйте це діалогове вікно для задання або зміни параметрів захисту від макросів.

У Excel команда захисту книги або листа знаходиться в меню →**Сервис** → **Защита**.

Злам паролів в документах MS Word і MS Excel. Існують десятки програм, за допомогою яких можна розкрити "запаролений" документ за лічені секунди. Прикладом такої програми є **Advanced Office XP Password Recovery.** Інтерфейс даної програми зображений на рис. 2.3.

Для завантаження файлу з невідомим паролем необхідно запустити програму, зайти в **→file →open file**. В діалоговому вікні вибрати файл

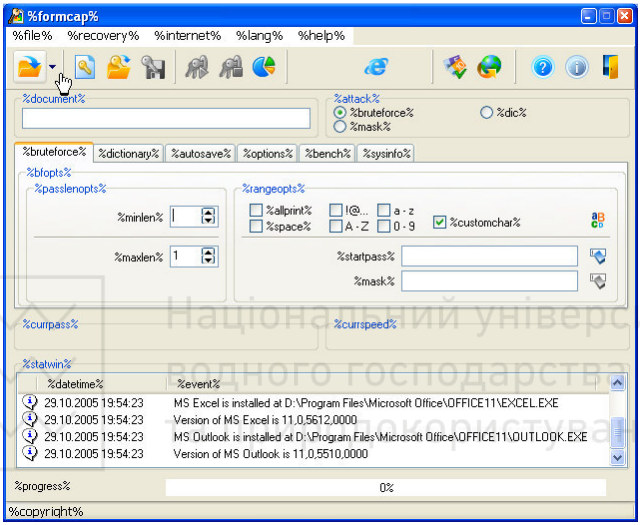

Рис. 2.3 Вікно програми

текстового редактора WORD. Вибати в **minlen** мінімальну довжину пароля, в **maxlen** - максимальну. В розділі **rangeopts** вибрати шляхом встановлення галочок з яких символів може складатися пароль. Зайти в **recovery** і натиснути **start**. Далі ви побачите процес визначення паролю шляхом перебору всіх можливих паролів. При успішному виконанні операції ви побачите діалогове вікно з визначеним паролем та деяку статистику пошуку паролю (рис. 2.4).

Рис. 2.4 Вікно статистики пошуку пароля

Захист файлів за допомогою архіватора WinRar. Для здійснення шифрування вмісту архівів необхідно загрузити архіватор **WinRAR.** Далі в головному вікні вибрати файл для архівації і натиснути кнопку **Добавить**. У вікні **Имя и параметры архива** вибрати закладку **Дополнительно**, в якій натиснути на кнопку **Установить пароль**.

Лабораторна робота № 3

КОМП'ЮТЕРНА СТЕГАНОГРАФІЯ

Мета роботи:

1. Ознайомитися з основами комп'ютерної стеганографії та з'ясувати її місце в захисті комп'ютерної інформації.
2. Отримати практичні навички захисту інформації з використанням комп'ютерної стеганографії.

Загальні відомості

Як відомо, метою криптографії (шифрування) є приховання змісту секретних повідомлень. Задача стеганографії - сховати від сторонніх сам факт існування повідомлень.

Стеганографія має багатовікову історію і за віком істотно старша криптографії. Саме слово «стеганографія» у перекладі з грецького буквально означає «таємнописання» (steganos - секрет, таємниця; graphy - запис). Місцем зародження стеганографії багато хто називає Єгипет.

Стеганографія займає свою нішу в забезпеченні безпеки: вона не замінює, а доповнює криптографію, захищаючи інформацію від зловмисників.

Комп'ютерна стеганографія (стеганографічні програмні продукти) базуються на двох основних принципах:

- файли, що містять оцифроване зображення або звук, можуть бути певним чином видозмінені без втрати своєї функціональності, на відміну від інших типів даних, що вимагають абсолютної точності;
- органи почуттів людини нездатні розрізнити незначні зміни в кольорі зображення або якості звуку.

Стеганографічна система або стегосистема - це сукупність засобів і методів, що використовуються для формування схованого каналу передачі інформації. Модель узагальненої стегосистеми представлена на рис. 3.1.

При побудові будь-якої стегосистеми повинні враховуватися наступні положення:

- супротивник має повне уявлення про стеганографічну систему, деталі її реалізації, і єдиною інформацією, що залишається невідомою потенційному супротивникові, є ключ, за допомогою якого тільки його власник може встановити факт присутності і зміст прихованого повідомлення;

- якщо супротивник якимось чином довідається про факт існування прихованого повідомлення - це не повинно дозволити йому витягти подібні повідомлення з інших даних доти, поки ключ зберігається в таємниці;
- потенційний супротивник повинен бути позбавлений яких-небудь технічних і інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

Рис. 3.1 Узагальнена стегосистема

У сучасної комп'ютерної стеганографії існує два основних типи файлів: повідомлення - файл, що призначений для приховування, і контейнер - файл, що може бути використаний для приховування в ньому повідомлення.

По довжині контейнери можна підрозділити на два типи:

- безперервні (потокові);
- обмеженої (фіксованої) довжини.

Контейнер без вбудованого повідомлення - це порожній контейнер, а контейнер, що містить вбудовану інформацію, - це заповнений або стегоконтейнер.

Вбудоване (сховане) повідомлення, що знаходиться в стегоконтейнері, передається від відправника до одержувача по каналу передачі, що називається стеганографічним каналом або просто стегоканалом.

Вбудовування повідомлень у контейнер відбувається з використанням спеціального стегоключа. Під ключем розуміється секретний елемент, що визначає порядок занесення повідомлення в контейнер.

За аналогією з криптографією, по типу стегоключа всі стегосистеми можна підрозділити на два типи:

- із секретним ключем;
- із відкритим ключем.

Будь-яка стегосистема повинна відповідати наступним вимогам:

- властивості контейнера повинні бути модифіковані так, щоб зміну неможливо було виявити при візуальному контролі;
- стегоповідомлення повинно бути стійке до перекручувань, у тому числі і зловмисних;
- для збереження цілісності повідомлення, що вбудовується, необхідне використання коду з виправленням помилок;
- для підвищення надійності повідомлення, що вбудовується, повинно бути продубльоване.

Нині можна виділити три, тісно зв'язаних між собою, напрямки додатків стеганографії:

- приховування даних (повідомлень);
- цифрові водяні знаки;
- заголовки.

Приховування даних, які у більшості випадків мають великий обсяг, висуває серйозні вимоги до контейнера. Розмір контейнера в кілька разів повинен перевищувати розмір даних, що вбудовуються.

Цифрові водяні знаки використовуються для захисту авторських або майнових прав на цифрові зображення, фотографії або інші оцифровані твори мистецтва. Основними вимогами, що висуваються до таких вбудованих даних, є надійність і стійкість до перекручувань.

Заголовки використовуються, в основному, для маркування зображень у великих електронних сховищах (бібліотеках) цифрових зображень, аудіо- і відеофайлів. У даному випадку, стеганографічні методи використовуються не тільки для впровадження ідентифікуючого заголовка, але й інших індивідуальних ознак файлу.

В даний час існує досить багато різних комп'ютерних методів (і їх варіантів) вбудовування повідомлень. Сьогодні методи комп'ютерної стеганографії (рис. 3.2) розвиваються двома основними напрямами:

- методи, засновані на використанні спеціальних властивостей комп'ютерних форматів;
- методи, засновані на надмірності аудіо- і відео інформації.

Як видно з рис. 3.2, перший напрямок заснований на використанні спеціальних властивостей комп'ютерних форматів представлення даних, а не на надмірності самих даних. Спеціальні властивості форматів вибираються з урахуванням захисту приховуваного повідомлення від безпосереднього прослуховування, перегляду або прочитання.

Другий напрямок використання стеганографії в комп'ютерних системах засновано на використанні надмірності аудіо і візуальної інформації. Цифрові фотографії, цифрова музика, цифрове відео - представляються матрицями чисел, що кодують інтенсивність сигналів у дискретні моменти в просторі і в часі. Цифрова фотографія - це матриця чисел, що представляють

інтенсивність світла у визначений момент часу. Цифровий звук - це матриця чисел, що представляє інтенсивність звукового сигналу в певні моменти часу.

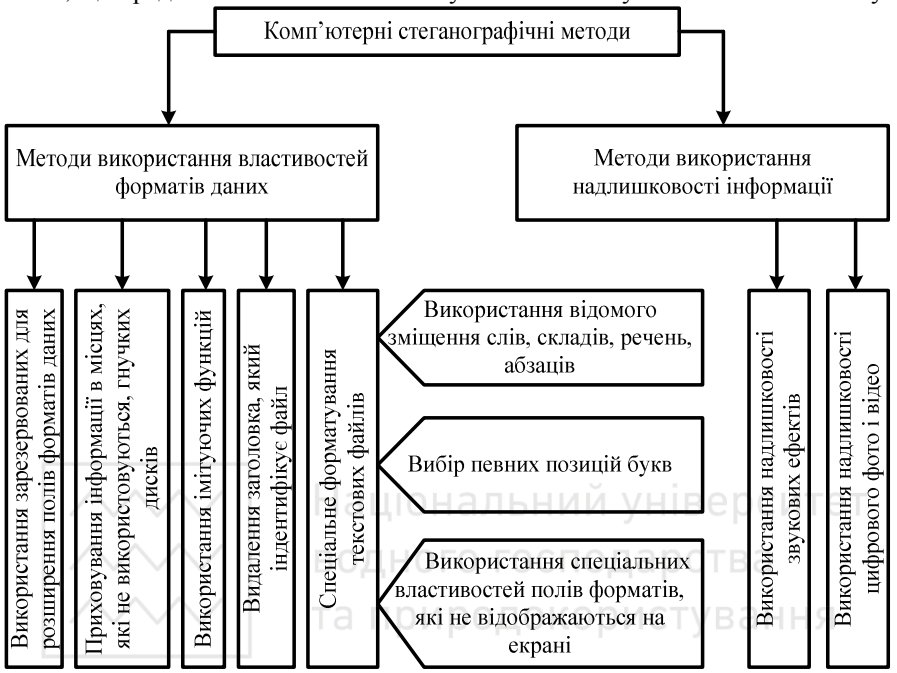

Рис. 3.2 Комп'ютерні стеганографічні методи

Усі ці числа неточні, тому що неточні пристрої оцифровки аналогових сигналів. Погрішність вимірів останніх залежить від суми погрішностей блоку перетворень і датчика, що перетворює фізичну характеристику сигналу в електричний сигнал. Ці погрішності вимірів звичайно виражаються у відсотках або в кількості молодших значущих розрядів і називаються шумами квантування. Молодші розряди цифрових відліків містять дуже мало корисної інформації про поточні параметри звуку і візуального образу, що дозволяє використовувати їх для приховування додаткової інформації.

При використанні комп'ютерної стеганографії дотримують наступних принципів:

- як носій схованої інформації повинен виступати об'єкт (файл), що допускає перекручування власної інформації, яка не порушує його функціональність і суть;
- внесені перекручування повинні бути нижче рівня чутливості засобів розпізнавання.

Перший полягає в тому, що файли, які містять оцифроване зображення або звук, можуть бути до певної межі видозмінені без утрати

функціональності, на відміну від інших типів даних, що вимагають абсолютної точності.

Другий фактор складається в нездатності органів почуттів людини розрізнити незначні зміни в кольорі зображення або якості звуку, що особливо легко використовувати стосовно об'єкта, що несе надлишкову інформацію, будь це 16-бітний звук, 8-бітне або ще краще 24-бітне зображення.

Стеганографічні алгоритми обробки звуку будуються з таким розрахунком, щоб максимально використовувати вікно чутності та інші властивості мовних сигналів (тембр, швидкість і т.д.), незначні зміни яких не відчутні людиною.

Практична частина

З метою практичного засвоєння способів захисту інформації з використанням комп'ютерної стеганографії виконати:

1. Дослідити інтерфейс програми **S-Tools**.
2. Здійснити приховування файлу «**план термінових дій»**;
3. Прочитати приховане повідомлення в файлі «**PA160125.bmp»;**
4. Самостійно встановити, який максимальний об'єм інформації можна приховати у файлі «**P5130016.bmp»**, без явного порушення зображення цього файлу.

Для практичного ознайомлення зі стеганографією скористаємося програмою **S-Tools**. Спочатку здійснимо приховування файлу **«план термінових дій.doc» (**повідомлення**)** в файл **«P5130016.bmp»** (контейнер). Для цього необхідно:

1. Із папки **S-Tools4** запустити файл **S-Tools.exe.**
2. З допомогою миші перетягнути файл **«P5130016.bmp»** (контейнер) у вікно **Actions.** Перетягування за допомогою миші здійснюється наступним чином. Підвести курсор миші до обраного файлу і натиснути ліву кнопку миші (і «не відпускати» кнопку). Не відпускаючи кнопку миші перетягнути файл у вікно **Actions** і відпустити ліву кнопку миші. В результаті, на екрані буде вікно, яке зображено на рис. 3.3.

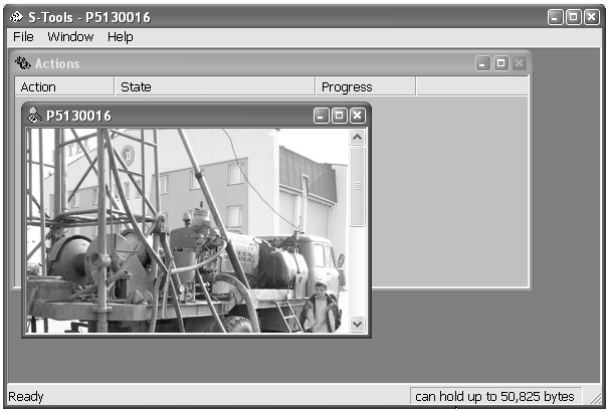

Рис. 3.3

3. З допомогою миші перетягнути файл **«план термінових дій.doc»** (повідом-

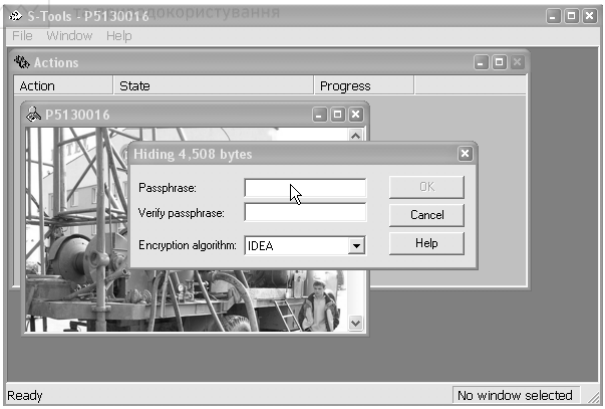

Рис. 3.4

лення) у вікно **«P5130016.bmp»**. В результаті, на екрані буде вікно, яке зображено на рис. 3.4.

4. У вікні **Hiding 4.508 bytes** ввести в полі

a. **Passphrase:** - пароль;

b. **Verify Passphrase:** - підтвердити раніше введений в полі **Passphrase:** пароль;

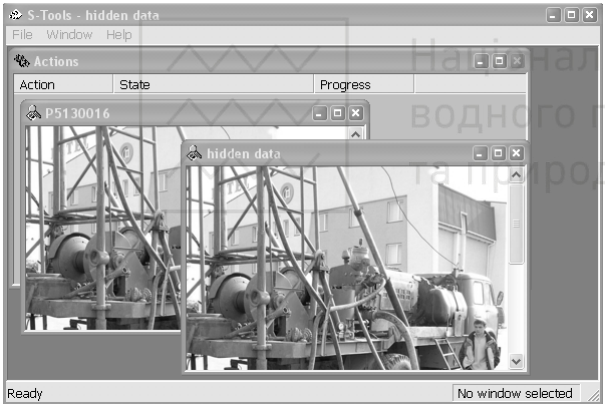

Рис. 3.5

c. **Encryption aigorithm**: - вибрати метод шифрування.

d. Натиснути кнопку **Ок**. В результаті на екрані з'явиться вікно **hidden data** (стегоконтейнер), яке зображено на рис. 3.5.

5. На вікні **hidden data** (в області зображення) натиснути праву кнопку миші і у вікні, що з'явилося вибрати команду «**Save**». В результаті на екрані буде вікно, яке зображено на рис. 3.6.

6. В полі Имя файла ввести **«P5130016.bmp»** і натиснути **Ок.** В результаті, отримаєте контейнер **«P5130016.bmp»** з вбудованим в нього повідомленням **«план термінових дій.doc».** Якщо порівняти інформацію про розмір файлу контейнера до і після вбудовування повідомлення, то з'ясується, що вона однакова. Проте, якщо здійснити їх архівування, то з'ясується, що розмір архіву контейнера менший за розмір архіву стегоконтейнера.

7. Закрити вікно **S-Tools.**

Тепер необхідно прочитати приховане повідомлення в файлі **«PA160125.bmp»** (стегоконтейнер)**.** Для цього необхідно:

1. Із папки **S-Tools4** запустити файл **S-Tools.exe.**

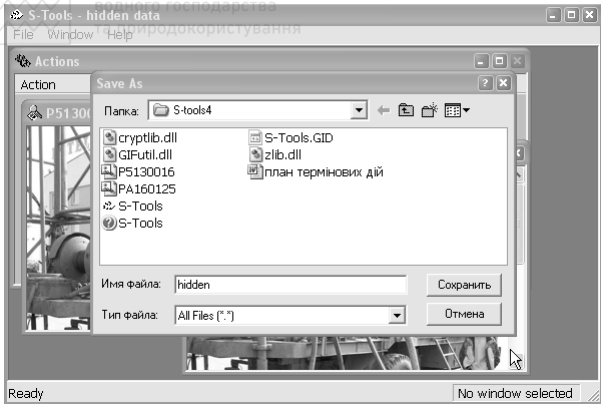

Рис. 3.6

2. З допомогою миші перетягнути файл **«PA160125.bmp»** (стего-контейнер) у вікно **Actions.** В результаті цих дій з'явиться вікно **PA160125.**
3. На вікні **PA160125** натиснути праву кнопку миші і у вікні, що з'явилося вибрати команду «**Reveal…**». В результаті на екрані буде вікно **Revealing from PA160125.**
4. У вікні **Revealing from PA160125** ввести в полі
   a. **Passphrase:** - 1;
   b. **Verify Passphrase:** - 1;
   c. **Encryption aigorithm**: - IDEA.
   d. Натиснути кнопку **Ок**. В результаті на екрані з'явиться вікно **Revealed Arhive**, яке зображено на рис. 3.7.

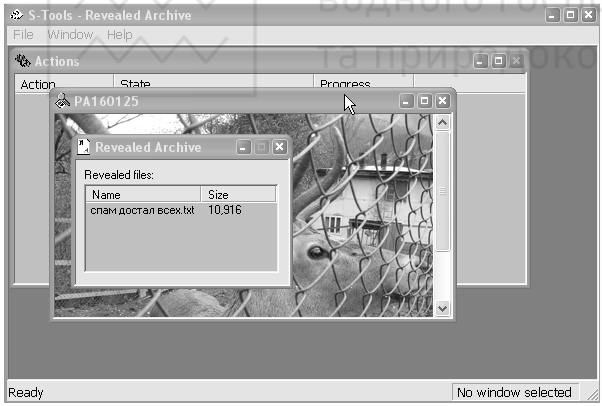

Рис. 3.7

5. У вікні **Revealed Arhive** з'явилося ім'я та розмір прихованого файлу: **«спам достал всех.txt»**. Для збереження цього файлу до нього необхідно підвести курсор миші і натиснути праву кнопку миші. В меню, яке з'явиться, вибрати **Save as...** Далі з'явиться вікно **Сохранить как.** В цьому вікні необхідно вказати місце, куди буде збережено повідомлення **«спам достал всех.txt».**
6. Закрити вікно **S-Tools.**
7. Прочитати приховане повідомлення **«спам достал всех.txt».**

ЛІТЕРАТУРА

1. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие. – СПб.: БХВ – Петербург; Арлит 2002. – 496 с.;
2. Баранов В М. и др. Защита информации в системах и средствах информатизации и связи. Учебное пособие. – СПб.: 1996. – 111 с.
3. Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика. – 1997. – 364 с.