Лабораторна робота №1

Тема: Призначення й основні можливості антивірусної програми Doctor Web

Мета роботи: вивчення основних можливостей роботи антивірусної програми Doctor Web.

Стислі теоретичні відомості

Антивірусні програми сімейства DrWeb І. Данилова і Санкт-Петербурзької антивірусної лабораторії містять захист від усіх відомих типів і видів вірусів – звичайних, скрипкових, троянських, поштових, макровірусів, у тому числі і від нових різновидів. Виконують пошук і видалення відомих програмі вірусів з пам'яті і з дисків комп'ютера, а так само здійснюють евристичний аналіз файлів і системних областей дисків комп'ютера. Евристичний аналіз дозволяє з високим ступенем імовірності виявляти нові, раніше невідомі комп'ютерні віруси.

У комплект програм для Windows 9x/NT/2000 входить поліфаг (сканер) Dr.Web, монітор SpIDer Guard, утиліта оновлення антивірусної бази через мережу DrWeb Update та утиліта Планувальник.

Програма-поліфаг (сканер) виявляє і видаляє фіксований набір відомих вірусів у пам'яті, файлах і системних областях дисків комп'ютера.

SpIDer Guard перехоплює звертання до файлів і системних областей дисків, здійснюючи перевірку на наявність у них комп'ютерних вірусів "з лету". При виявленні вірусу SpIDer Guard починає дії по знешкодженню (лікуванню, видаленню, переміщенню в заздалегідь задану область) чи блокуванню інфікованого файлу (заборона доступу до інфікованого файлу). Дії можуть починатися в автоматичному (без утручання користувача) чи напівавтоматичному режимах. У напівавтоматичному режимі користувач самостійно визначає тип конкретної дії з інфікованим файлом. Таким чином, при активізованому сторожі, доступ до файлів і/чи системних областей дозволяється тільки у випадку, якщо віруси не виявлені, або їх удалося знешкодити.

Крім того, у SpIDer Guard передбачений спеціальний режим роботи - виявлення і блокування вірусної активності. При активізації цього режиму SpIDer Guard здатний знайти і заблокувати спроби невідомих і невизначуваних евристичним аналізатором комп'ютерних вірусів робити повторне інфікування об'єктів на дисках комп'ютера.

Для аналізу об'єктів на наявність комп'ютерних вірусів сторож SpIDer Guard і поліфаг Dr.Web використовують єдину вірусну базу й одне ядро.

Починаючи з версії 4.20 у комплект програм входить Планувальник Dr.Web (Scheduler), що дозволяє робити запуск антивірусних програм і оновлення бази за розкладом, що задається користувачем.

Основи роботи з антивірусною програмою DrWeb

Активізація SpIDer Guard виконується автоматично при завантаженні операційної системи. При цьому здійснюється перевірка оперативної пам'яті комп'ютера на наявність активного резидентного вірусу. Після завантаження SpIDer Guard його іконка міститься в праву частину панелі задач Windows. Натисканням правої кнопки миші на цій іконці викликається меню SpIDer Guard, а подвійним натисканням лівої кнопки - його панель настроювань.

Рис. 1.1 Фрагмент панелі задач

Запуск антивірусної програми DrWeb здійснюється подвійним кліком лівою кнопкою миші по іконці, розташованій на **Робочому столі** Windows чи послідовністю **Пуск⇨ Програми↴ DrWeb↴ DrWeb**.

В основному вікні програми задаються об'єкти тестування і дії, які необхідно здійснювати над ними. Після завершення перевірки в головному вікні відображаються результати роботи програми чи статистика всіх проведених перевірок за даний сеанс роботи. Крім цього, з головного вікна доступні всі додаткові функції і настроювання програми через систему меню і кнопки швидкого доступу.

Рис. 1.2. Вікно антивірусної програми DrWeb

Елементи вікна антивірусної програми DrWeb:

1- рядок меню: **Файл**, **Вид**, **Настроювання**, **Малюнок**, **Мова** і **Допомога**;

2 – панель інструментів;

3 – область дисків;

4 – опції перевірки;

5 – панель **Дерево об'єктів**;

6 – кнопка запуску і стану перевірки.

Більшість елементів основного вікна мають спливаючі короткі підказки, що з'являються при сполученні покажчика мишки з відповідним елементом вікна. При цьому натискання правої кнопки мишки здійснює доступ до розширеного контекстного файлу допомоги.

Виконання перевірки

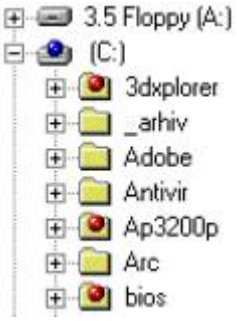
Для перевірки об'єктів на наявність вірусів необхідно вибрати пристрої чи їх частину (каталоги, файли), що буде перевіряти Dr.Web. Це може бути зроблено декількома способами:

- за допомогою швидкого вибору пристроїв за типом;
- за допомогою ручного вибору об'єктів для перевірки.

Установивши відповідну опцію, ви можете вибрати для перевірки всі дисководи, усі логічні диски, усі приводи CD-ROM і всі мережні диски. Зміни, зроблені в групі **Виділити диски**, відразу відбиваються в панелі **Дерево об'єктів**.

У лівій частині основного вікна розташовані кілька перемикачів, об'єднаних у групу за назвою **Виділити диски** (3)

Панель дерево об'єктів (5) (вибору об'єктів для перевірки), що знаходиться в центральній частині основного вікна, відображає деревоподібну структуру наявних у системі пристроїв збереження інформації.



Ви можете вибрати будь-як пристрій лівою кнопкою миші. Після вибору пристрою його іконка набуде нового виду (диск C: з червоною кулькою).

Для перевірки якої-небудь окремої папки (каталогу) необхідно відкрити структуру папок (каталогів). Для цього потрібно клацнути лівою кнопкою мишки по значку  ліворуч від іконки пристрою. Відкриється дерево папок (каталогів) пристрою і тепер можна вибрати для перевірки одну чи кілька папок (каталогів) за допомогою кліка лівої кнопки мишки.

При включенні опції 

показуються не тільки папки (каталоги), але і файли і стає можливим вибір окремих файлів для перевірки.

Двома перемикачами, що входять у групу **Перевіряти** (4), можна включити перевірку завантажувальних секторів пристроїв збереження інформації і файлів у вкладених підкаталогах.

Запуск перевірки здійснюється за допомогою кнопки (6), розташованої в нижній правій частині основного вікна. Кнопка може знаходитися в одному з трьох станів:


немає обраних об'єктів для чи перевірки йде перевірка пам'яті, кнопка неактивна;


натискання на кнопку приводить до запуску процесу пошуку вірусів;

натискання на кнопку приводить до зупинки процесу пошуку вірусів.

Панель інструментів

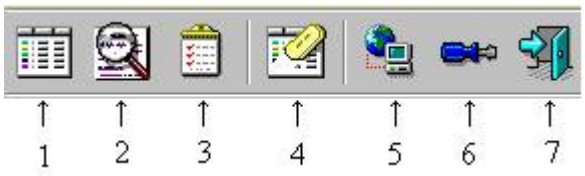


Рис.1.3. Панель інструментів

Призначення кнопок панелі інструментів:

1-переключає головне вікно в режим відображення звіту про результати тестування;

2 - переключає головне вікно в режим відображення дерева дисків;

3 - переключає головне вікно в режим відображення статистики результатів проведених перевірок;

4 - очищає список звіту, сформований у результаті тестування;

5 - робить запуск програми відновлення Dr.Web через Internet,

6 - викликає вікно настроювань програми;

7 - завершує роботу програми і закриває головне вікно.

Звіт про результати тестування

По завершенню перевірки об'єктів на наявність вірусів у головному вікні відображаються результати тестування. У таблиці, що може бути розкрита на весь екран, відображаються **Об'єкт**, про який в програмі є яка-небудь інформація, **Шлях до нього**, **Статус об'єкта** (назва вірусу, "Можливо <клас вірусу>") і **Дія**, зроблена програмою над об'єктом.

Поява в колонці **Статус** повідомлення типу "Можливо <клас вірусу>" означає, що відбулося спрацьовування евристичного аналізатора, що знайшов підозрілі дії аналізованої програми. Це не є ознакою наявності відомого Dr.WEB вірусу, що відображається явним визначенням імені вірусу

в колонку Статус, однак попереджає користувача про можливість наявності невідомого вірусу в об'єкті.

У випадку, якщо в налаштуваннях програми встановлена опція "Інформувати" користувача про наявність чи підозру на наявність вірусу, після закінчення тестування стовпчик **Дія** буде порожній, оскільки Ви не "замовили" інших дій програми, крім видачі інформації. Ви можете прийняти рішення про виконання яких-небудь дій самостійно, виділивши в таблиці рядок з потрібним об'єктом і натиснувши праву кнопку мишки. У меню, що з'явилось можна вибрати необхідні дії над виділеним об'єктом.

ПОРЯДОК ВИКОНАННЯ РОБОТИ

1. Завантажте антивірусну програму Dr.Web. Для цього активізуйте програму Z:\TOOLS\DrWeb for Windows\Drweb32.exe
2. Дослідіть призначення пунктів головного меню програми та занотуйте у звіт зміст пунктів „Файл", „Вид", „Настройки".
3. Дослідіть та занотуйте у звіт призначення кнопок на панелі інструментів.
4. Налаштуйте програму на перевірку усіх файлів диску Z:\. Установіть дію при виявленні вірусу - **Лікувати** і включіть опцію **Запит підтвердження**.
5. Протестуйте диск X:\.
6. Протестуйте будь-яку папку диска X:\.
7. Проаналізуйте інформацію, яка виводиться у звіт про результати тестування.
8. Закрийте антивірусну програму.

Запитання для самоконтролю

1. Що таке комп'ютерний вірус?
2. Які програми входять до антивірусного комплексу DrWeb?
3. В чому полягає робота сканера DrWeb?
4. Які особливості роботи монітора SpIDer Guard?
5. Яка інформація виводиться у звіт про тестування?