Міністерство освіти і науки України
Національний авіаційний університет
Навчально-науковий інститут комп'ютерних інформаційних технологій
Кафедра комп'ютеризованих систем управління

Лабораторна робота №5
з дисципліни «Діагностика та експлуатація комп'ютера»
на тему «Лікування комп'ютера від вірусів»

Виконав:
студент ННІКІТ
групи СП-325
Клокун В. Д.
Перевірив:
Масловський Б. Г.

Київ 2018

1 Ціль роботи

Ознайомлення з процесом використання антивірусного програмного забезпечення для очищення комп'ютера від вірусних загроз.

2 Короткі теоретичні відомості

При постійному контакті комп'ютера з файлами та носіями, які були створені або знаходились у інших комп'ютерах виникає ризик занесення на свій комп'ютер програми, яка може погіршити роботу комп'ютера та пошкодити дані на жорсткому диску. Такі програми прийнято називати «комп'ютерними вірусами». Про комп'ютерний вірус можна сказати, що це комп'ютерна програма, яка має здатність до прихованого саморозмноження, одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера.

Розрізняють файлові, завантажувальні та макро-віруси. Можливі також комбінації цих типів.

Файлові віруси — поширюється шляхом впровадження свого коду в тіло виконуваних файлів. При кожному запуску такого зараженого файлу спочатку виконується код вірусу, і тільки потім — код самої програми. Об'єктом вірусного ураження можуть виступати виконувані двійкові файли (EXE, COM), файли динамічних бібліотек (DLL), драйвери (SYS), командні файли (BAT, CMD) та інші. Заражаючи файл, вірус може потрапити до його початку, кінця або в середину. Найбільш поширеним способом є впровадження в кінець файлу, коли його основний код дописується в кінець файлу, а в початок записується команда переходу до тіла вірусу. Щоб приховати свою присутність в системі, файловий вірус може попередньо зберегти дату і час останньої модифікації і значення атрибутів файлу.

Завантажувальні віруси — записуються в завантажувальний сектор дискети, твердого диска чи флеш-накопичувача й активізується при завантаженні комп'ютера або відкриття цього диску. При звертанні до нового диска, вірус копіює себе в його завантажувальний сектор і таким чином заражає його та передається далі. Через специфіку роботи комп'ютерів майже будь-який носій, містить завантажувальний сектор, що дозволяє автоматично завантажувати розташовані на ньому програмні коди.

Макро-вірус — вірус, який написано на мові макросів. Технічно, головною відміною макро-вірусу від інших видів комп'ютерних вірусів є лише середовище виконання. Для макро-вірусу таким середовищем є не операційна система, а те середовище, що забезпечує виконання макро-програм (наприклад, мова Visual Basic, що забезпечує автоматизацію дій у середовищі офісного пакету MS Office). Зазвичай, макровірус вбудовується в файли певних типів, для яких передбачені можливості автоматичного виконання

вбудованих в них макросів.

Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу. Необізнані користувачі ПК помилково відносять до комп'ютерних вірусів також інші види зловмисного ПЗ — програм-шпигунів чи навіть спам. Такі віруси можна віднести до типу веб-вірусів, які проникають на інтернет-ресурси, розсилають спам та блокують роботу серверів.

Для боротьби з вірусами використовуються антивірусні програми або фаерволи (мережеві екрани).

Антивірусна програма (антивірус) — програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом.

Фаервол (firewall) — тип антивірусного програмного забезпечення, що встановлюється на комп'ютер, сервер або інший мережевий пристрій. Головним чином служить для запобігання мережевих атак та автоматичного проникнення вірусних програм на комп'ютер. Також існують фаерволи у вигляді фізичного пристрою, що працюють на прикладному рівні та відбивають атаки, пов'язані з фізичною природною роботи мережі.

Сучасні антивірусні програми можуть поставлятися у вигляді комплексних рішень, поєднуючи у собі властивості звичайного файлового антивірусу з можливостями програмного фаерволу.

Також антивірусне програмне забезпечення може поділятися на платне та безкоштовне. Платні антивіруси, як і інше програмне забезпечення, потребує від користувача оплачувати ліцензію на використання, на термін дії якої антивірус буде повністю захищати комп'ютер. Безкоштовні антивіруси не вимагають витрачати гроші на їх використання, але в деяких випадках можуть містити значно менше функціональних можливостей, що негативно відображається на захищеності комп'ютера.

До найбільш відомих платних антивірусних програм можна віднести:

— Norton Antivirus/Norton Internet Security;
— Антивірус Касперського/Kaspersky Internet Security;
— ESET NOD32 Antivirus/ESET NOD32 Smart Security.

Серед антивірусів з безкоштовним використанням є:

— avast! Free Antivirus;
— AVG AntiVirus;

— Panda Antivirus;

— Avira Free Antivirus.

У антивірусів існує два основних режими роботи: перевірка в режимі реального часу та перевірка за вимогою.

Перевірка в режимі реального часу, або постійна перевірка, забезпечує безперервність роботи антивірусного захисту. Полягає в обов'язковій перевірці всіх дій скоєних іншими програмами і самим користувачем. Перевірка відбувається на предмет небезпечності, незалежно від їх вихідного виконання — будь це свій жорсткий диск, зовнішні носії інформації, чи інші мережеві ресурси або власна оперативна пам'ять.

В деяких випадках наявності постійно працюючої перевірки в режимі реального часу може бути недостатньо або неможливим з точки зору ресурсоємності. Для такого режиму зазвичай передбачається, що користувач особисто вкаже які файли, каталоги або області диска необхідно перевірити, а також час, коли потрібно виконати таку перевірку — у вигляді розкладу або разового запуску вручну.

Зазвичай, після активізації, віруси копіюють свої файли у системні теки операційної системи, через те, що їх вміст невидимий для користувача та у деяких випадках захищений від втручання. До таких тек можна віднести теки Windows, System32, Program Files, User та Application Data.

Деякі віруси створюють свої копії з різними іменами у різних теках створених при роботі комп'ютера, через що недосвідчені користувачі вважають їх важливими системними файлами.

Основними методами зараження вірусів є завантаження програм та файлів з джерел невідомого походження, тобто використання носіїв інформації без їх перевірки або завантаження маловідомих програм з Інтернету. Останнім часом набули поширення програми, які маскуються під завантажувальники файлів або інші програми, запаковані у архіви. Запуск таких програм призводить до зараження системи і може бути не сприйнятий антивірусом як небезпечна дія. У таких випадках зловмисники підроблюють електронні підписи програм та антивірус вважає їх безпечними.

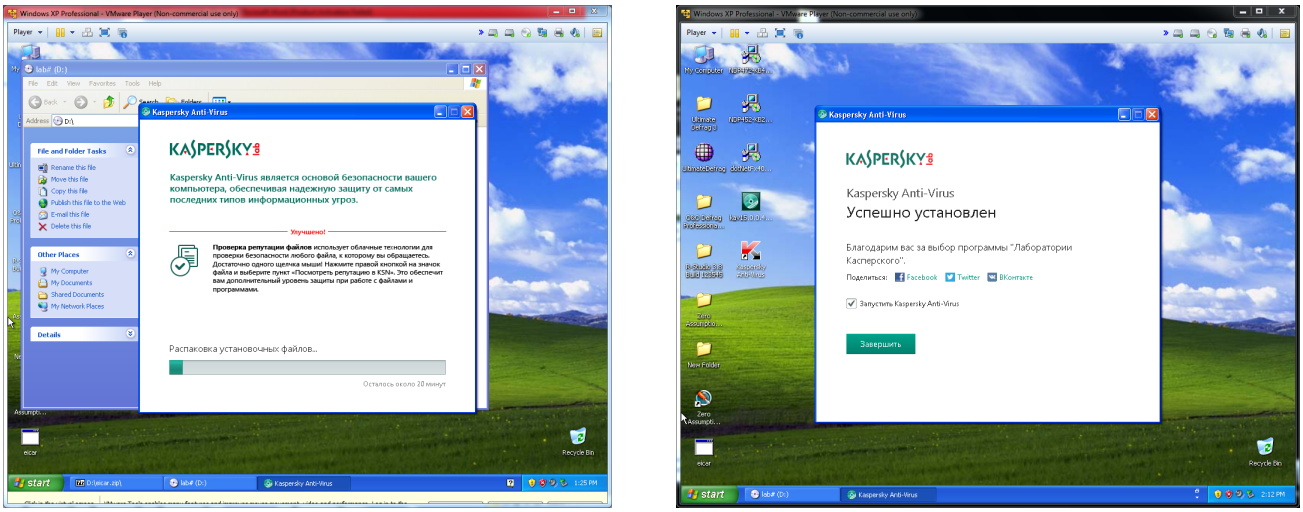
Також можливе зараження комп'ютера через інтернет-браузер. Недосвідчений користувач може випадково прийняти сертифікат безпеки, який дозволить спеціально створеному інтернет-сайту завантажити на комп'ютер вірус та запустити його.

3 Хід роботи

Запускаємо віртуальну машину та копіюємо пакет встановлення антивірусного програмного забезпечення та тестовий вірусний файл на жорсткий диск віртуальної машини. Після завершення копіювання файлів копіюємо файл з архіву `eicar.zip` на Ро-

бочий стіл, у папку `C:\Windows\` та у корінь диску `C:\`.

Скопіювавши тестовий псевдовірусний файл, встановлюємо антивірусне програмне забезпечення. Для цього запускаємо надану програму-інсталятор «Антивірусу Касперського» та встановлюємо антивірус відповідно до наданих інструкцій (рис. 1).



а) б)

Рис. 1: Встановлення «Антивірусу Касперського»

Після завершення встановлення операційна система не запитує про мережеву активність антивірусу, тому переходимо до пункту оновлення баз антивірусних сигнатур. Для цього натискаємо на кнопку «Оновлення» та бачимо повідомлення, що антивірусні бази неактуальні (рис. 2). На тестовій віртуальній машини відсутній доступ до мережі Інтернет, тому оновити бази неможливо — переходимо до наступного пункту.

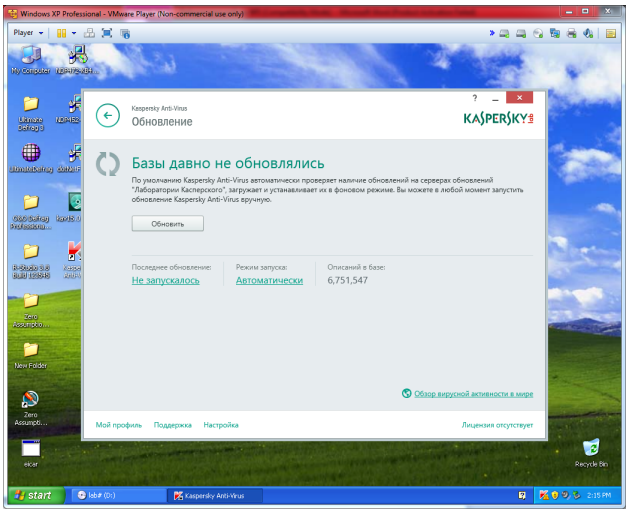
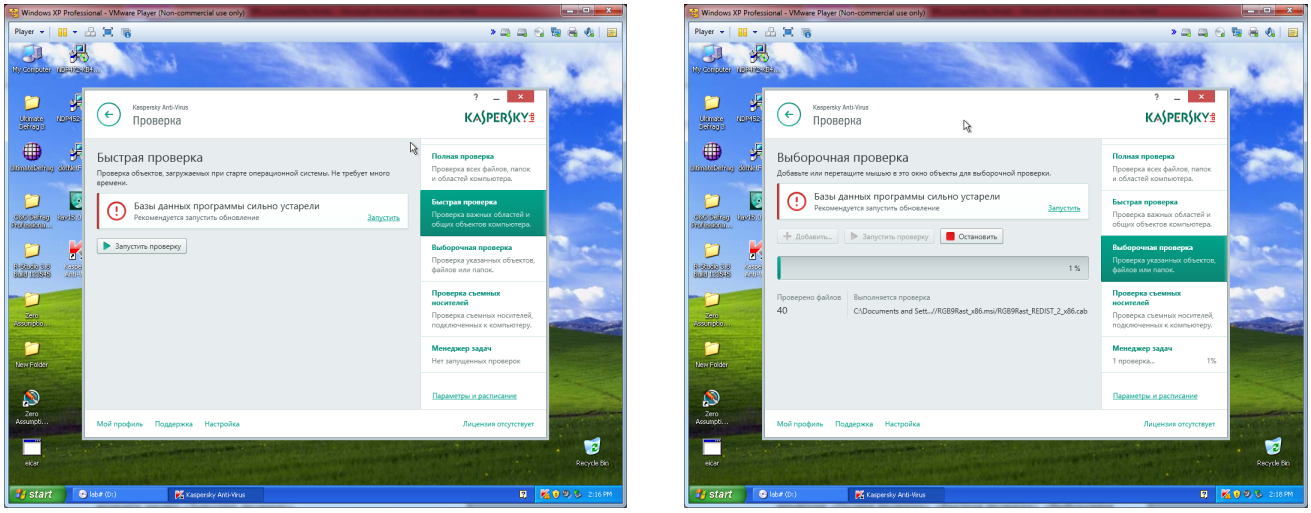


Рис. 2: Вікно оновлення баз антивірусних сигнатур «Антивірусу Касперського»

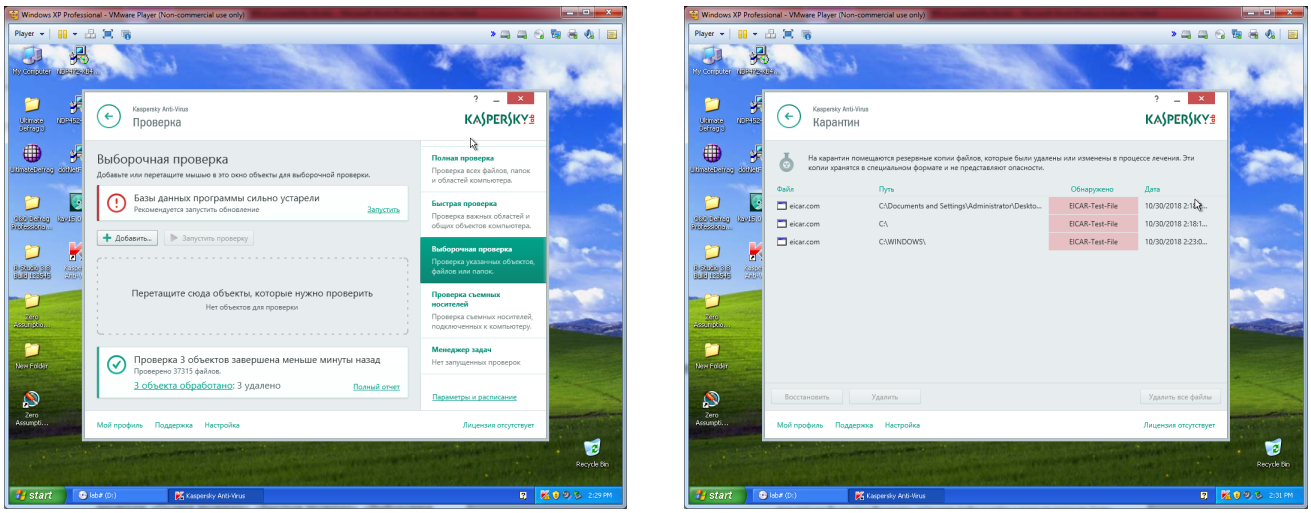
Виконуємо перевірку комп'ютера на наявність шкідливого програмного забезпечення. Для цього відкриваємо головне меню, натискаємо кнопку «Перевірка» та переходимо у меню Швидкої перевірки. Однак для економії часу на перевірку оберемо та запустимо Вибіркову перевірку, оскільки місцезнаходження тестового файлу нам вже відоме (рис. 3).



а) б)

Рис. 3: Вікно запуску Швидкої та Вибіркової перевірок

Після завершення перевірки отримали результат: було знайдено 3 файли, які антивірус вважає шкідливими (рис. 4). Антивірус не пропонує жодних подальших дій зі знайденими файлами, тому переглядаємо деталізацію.

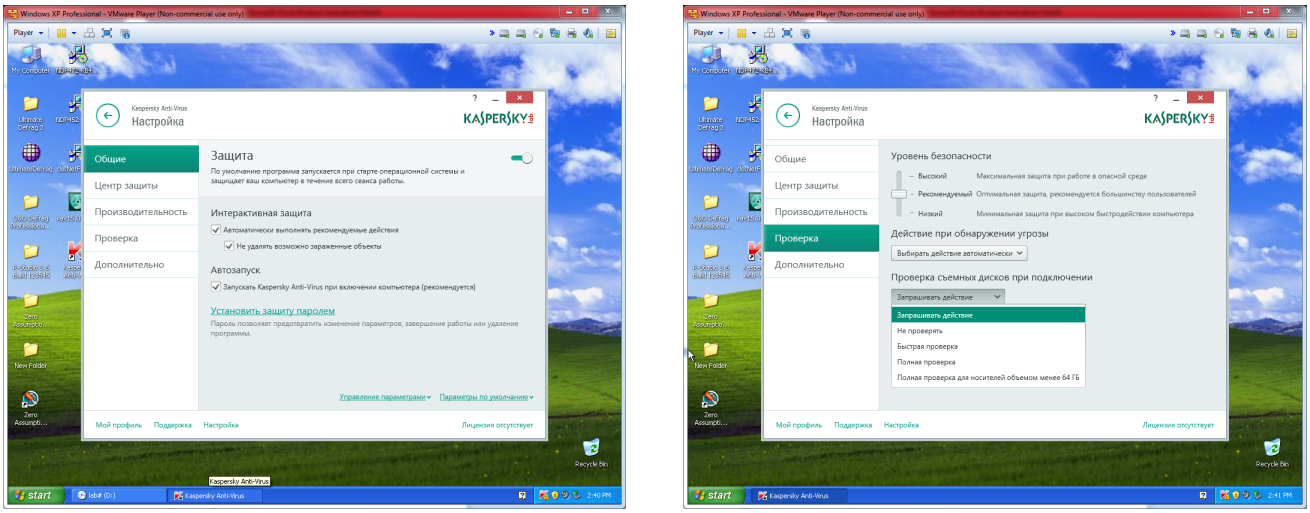


а) б)

Рис. 4: Результати перевірки комп'ютера на віруси

Налаштовуємо параметри перевірки. Для цього повертаємось у головне меню, на-

тискаємо кнопку «Налаштування» та переходимо у підпункт «Перевірка». В обраному підпункті встановлюємо рівень безпеки «Рекомендований» та дію при знаходженні загрози — «Лікувати, невиліковну — видаляти» (рис. 5).



а) б)

Рис. 5: Результати перевірки комп’ютера на віруси

4 Висновки

Виконуючи дану лабораторну роботу, ми ознайомились з процесом використання антивірусного програмного забезпечення для очищення комп’ютера від вірусних загроз.