Лабораторна робота №5

Лікування комп’ютера від вірусів

Ціль роботи: Ознайомлення з процесом використання антивірусного програмного забезпечення для очищення комп’ютера від вірусних загроз.

1. 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 само розмноження, 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 (*укр. 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 NOD*32 *Antivirus* / *ESET NOD*32 *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*, *System*32, *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.

2. Виконання роботи

2.1.Вимоги до обладнання та програмного забезпечення

Лабораторна робота виконується на ПК з використанням программ *VMware player*, Антивірус Касперського 15.0.

2.2. Порядок виконання роботи

2.2.1. Запустити віртуальну машину *VMware player* (рис. 1):

Рис. 1 Основне вікно програми *VMware Player*

2.2.2. Скопіювати пакет встановлення антивірусного ПО для виконання встановлення та тестовий вірус на жорсткий диск.

Для цього потрібно виконати монтування образу диску, який знаходиться в папці з лабораторною роботою. Виконання цієї операції потребує у вікні віртуальної машини перейти до налаштування пристрою *CD\DVD* (*Player-Removable Devices-CD\DVD* (*IDE*)-*Settings*…) (рис. 2):

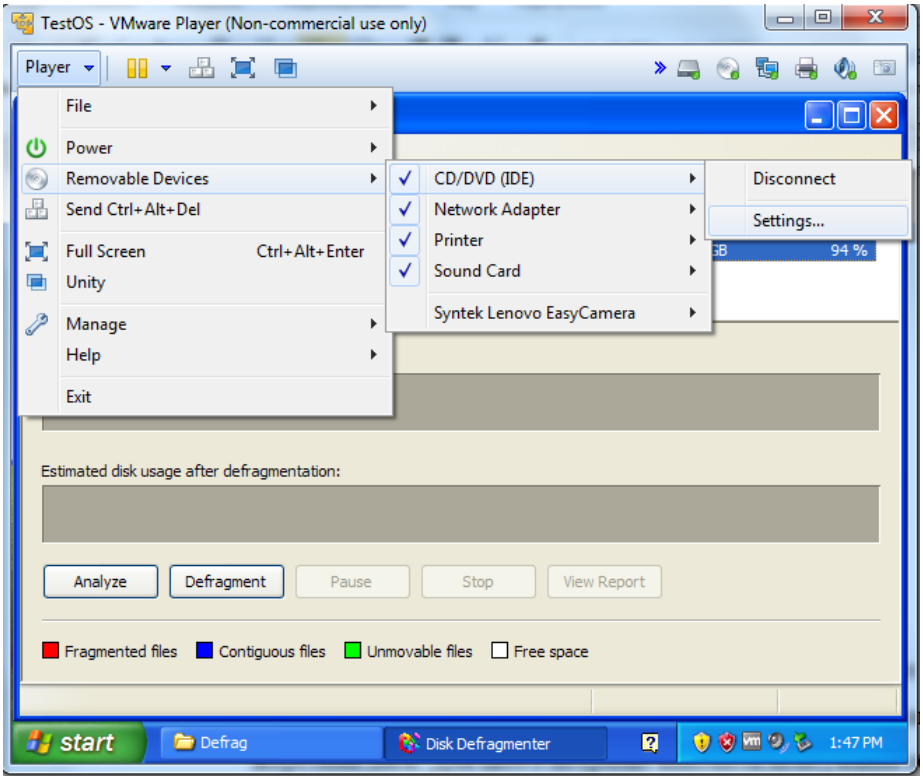

Рис. 2 Налаштування пристрою *CD\DVD Vmware*

У вікні, що з'явилось на екрані, потрібно вибрати пункт *Use ISO image file*: (рис. 3) та вказати шлях до *iso*-файлу, що знаходиться в папці з лабораторною роботою.

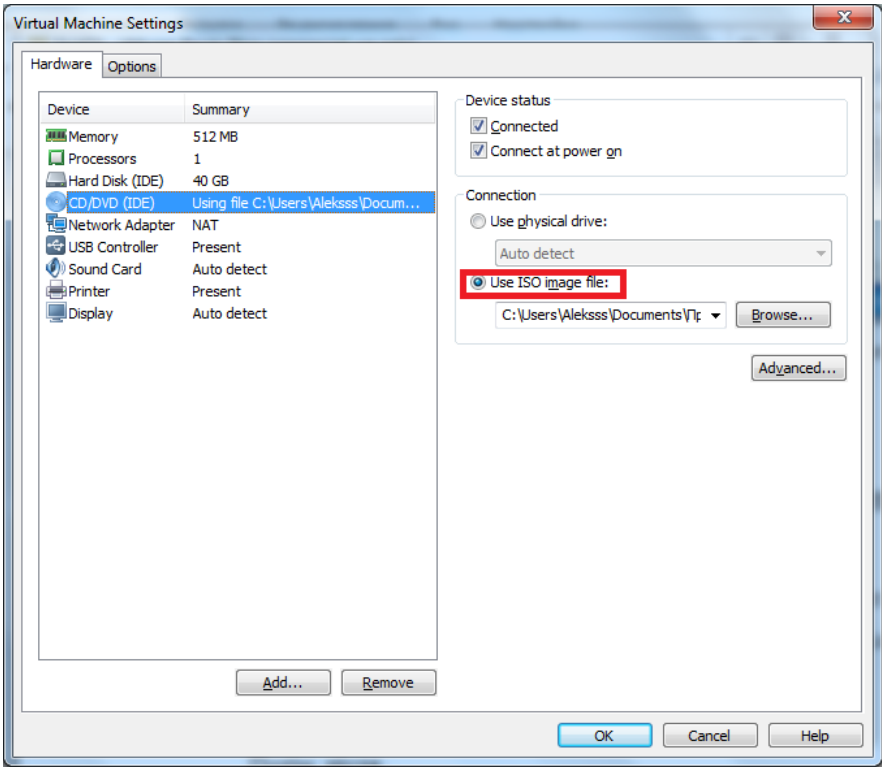

Рис. 3 Налаштування пристрою *CD\DVD VMware*

Потім потрібно натиснути кнопку *OK*. Тепер образ змонтований і ви можете отримати доступ до нього зі своєї віртуальної машини. Після відкриття диску потрібно скопіювати вміст образу на жорсткий диск віртуальної машини.

2.2.3. Після завершення копіювання необхідно з архіву *eiacr.zip* скопіювати файл *eicar.com* на «Робочий стіл», у папку «*Windows*» та у корінь системного диску. Це файл-симулятор вірусу. Оскільки свіжо встановлена система може не містити вірусів, для перевірки роботи антивірусного програмного забезпечення буде використано симуляцію.

2.2.4. Після копіювання файлів потрібно встановити антивірусне програмне забезпечення. Для цього відкрийте файл *kav15.0.0.463 aru_6553.exe* та виконайте встановлення (рис. 4):

Рис. 4 Вікно програми встановлення «Антивірус Касперського»

Встановлення програми проходить у автоматичному режимі. Вам необхідно на першому екрані натиснути кнопку «Установить». На наступному екрані буде виведено текст ліцензійної угоди, для продовження потрібно натиснути кнопку «Принять» (рис. 5).

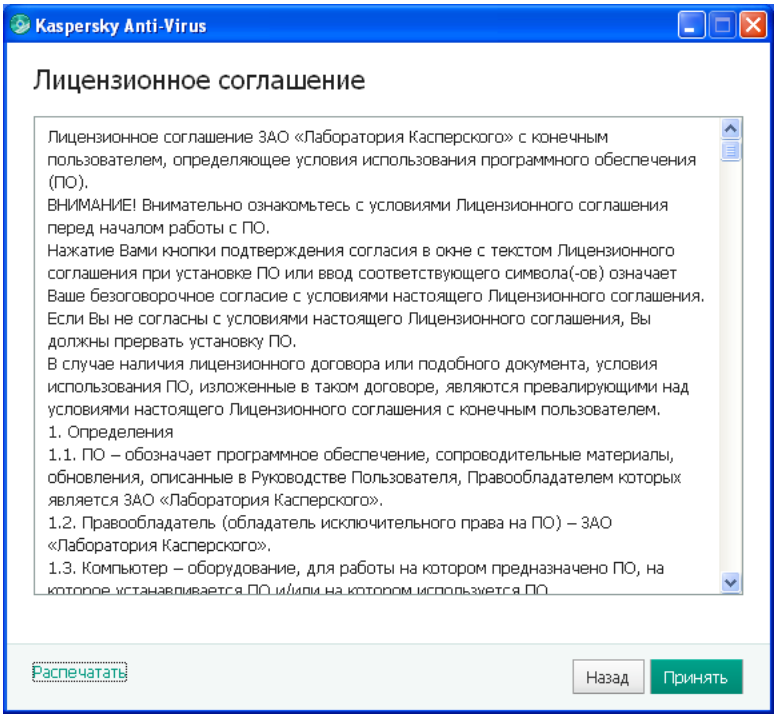

Рис. 5. Вікно ліцензійної угоди

Після тексту угоди буде запропоновано прийняти участь у програмі покращення роботи антивірусу, якщо Ви згодні, можете натиснути кнопку «Принять» або кнопку «Отказаться», якщо це непотрібно. На процес пошуку загроз це не впливає (рис. 6).

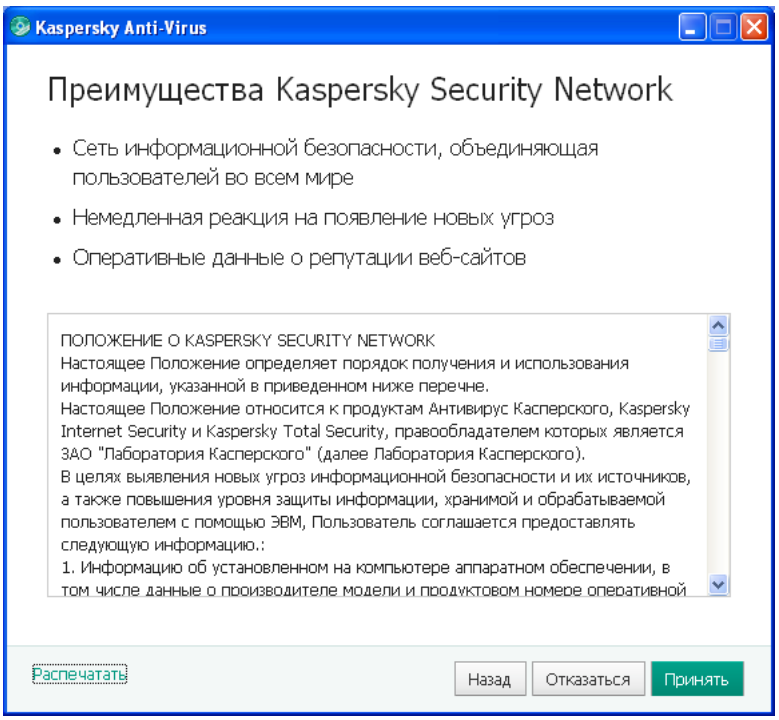

Рис. 6. Вікно угоди участі в покращенні ПЗ

2.2.5. По завершенню встановлення на екрані з’явиться відповідне вікно з кнопкою «Завершить», яку необхідно натиснути. Опціями на вікні буде відмічено пункт про автоматичний запуск. Якщо прибрати відмітку, антивірус не буде завантажено автоматично після закриття. (рис. 7).

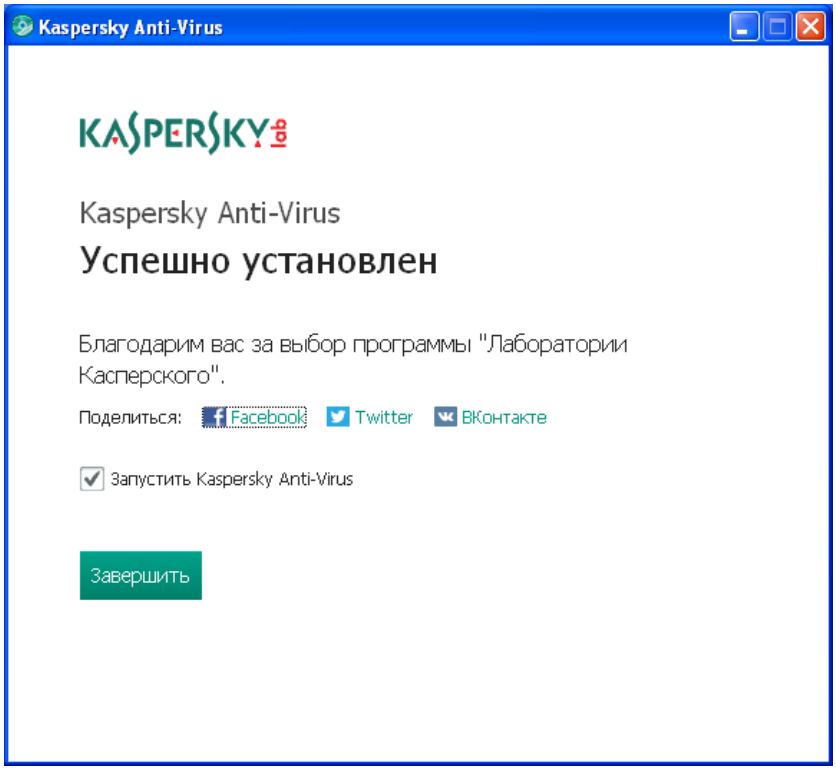

Рис. 7. Вікно результату встановлення

2.2.6. Перед завантаженням, антивірус перевірить систему на цілісність та спробує внести свої зміни у системи. Якщо на комп’ютері увімкнено «Брандмауер *Windows*», він автоматично заблокує мережеву активність антивірусу та сповістить про це (рис. 8).

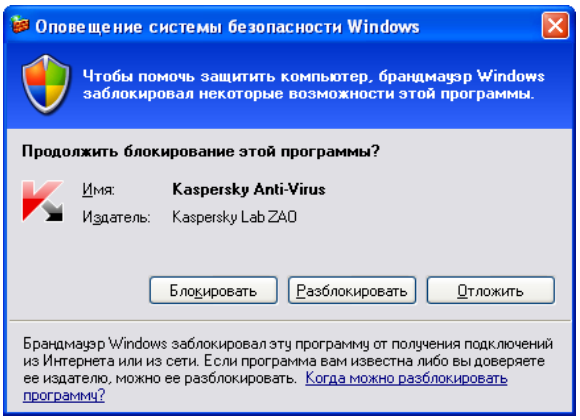

Рис. 8. Попередження про несанкціоноване підключення

У разі виникнення такої ситуації потрібно натиснути кнопку «Разблокировать». Якщо такого на екрані не відбувалося, то можна перейти до наступного пункту.

2.2.7. Оновлення антивірусних баз. Необхідно відкрити «Антивірус Касперського», після першого завантаження програми, на головному вікні потрібно натиснути кнопку «Обновления», яка перемкне програму на екран оновлення. В ньому буде відображено поточну встановлену версію антивірусних баз.

У більшості випадків вірусного зараження комп'ютерів, достатньо тієї версії антивірусних баз, якою комплектуються пакети встановлення. Але зловмисники кожен день розробляють нові види шкідливих програм і не буде зайвим оновити антивірусні бази.

Для оновлення антивірусних баз потрібно натиснути на кнопку «Обновить» та дочекатися завершення процесу оновлення (рис. 9).

(Для оновлення, на комп'ютері повинно бути активне підключення до мережі Інтернет).

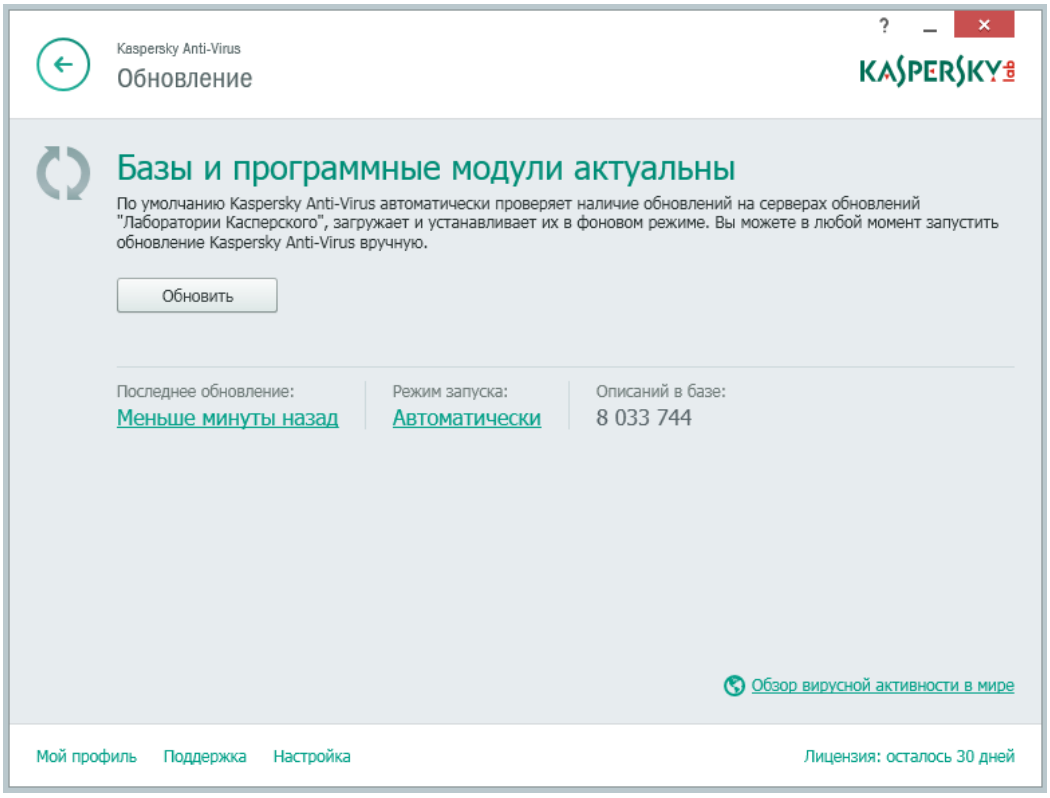

Рис. 9. Запуск оновлення антивірусних баз

2.2.8. Перевірка комп’ютера на наявність шкідливого програмного забезпечення. Для перевірки потрібно відкрити відкрити «Антивірус Касперського» та натиснути кнопку «Проверка».

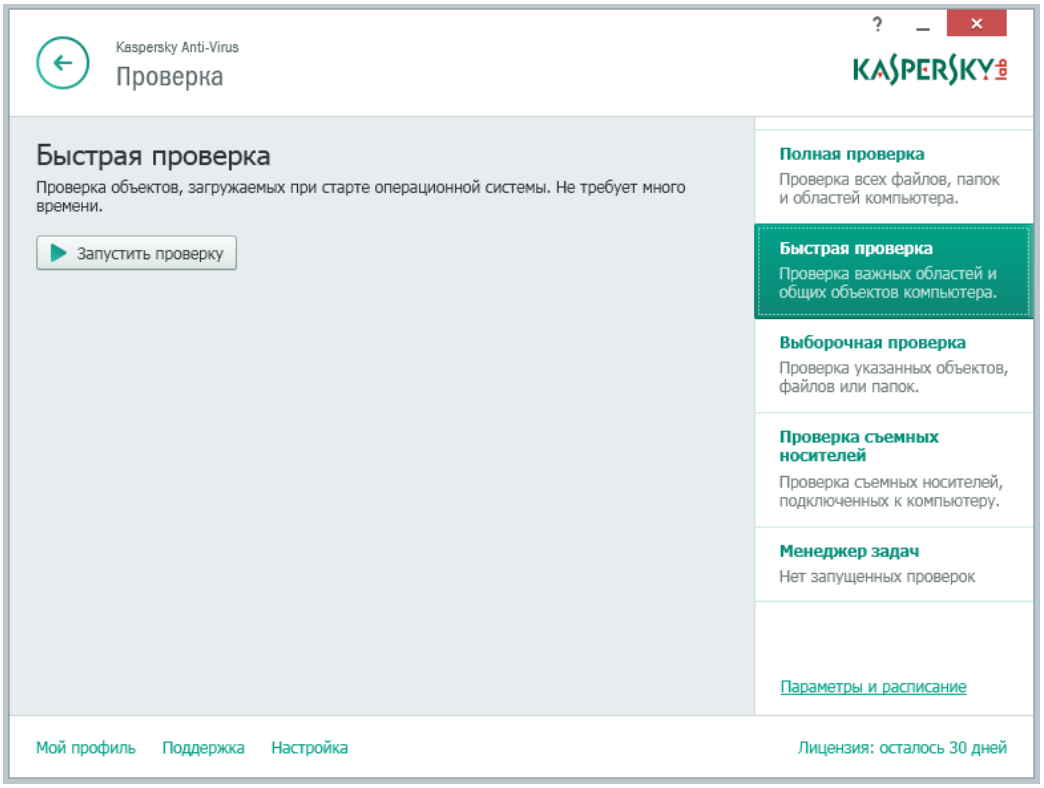

Рис. 10. Запуск швидкої перевірки комп’ютера

На екрані перевірки буде доступно чотири варінати проведення перевірки: «Полная проверка», «Быстрая проверка», «Выборочная проверка», «Проверка съемных носителей» (рис. 10).

Для виконання перевірки оберіть варіант «Швидка перевірка» та натисніть кнопку «Запустить проверку».

При запуску швидкої перевірки буде перевірено основні системні теки та об’єкти автозавантаження (рис. 11).

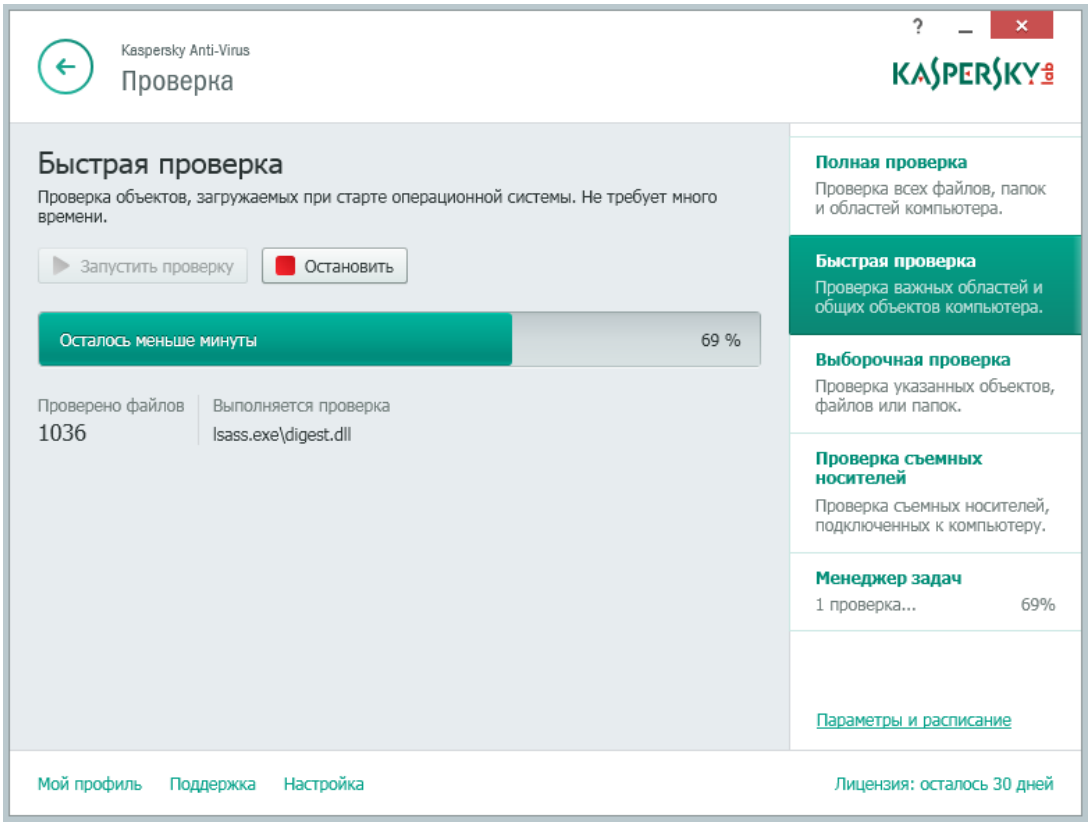

Рис. 11. Процес швидкої перевірки

Оскільки більшість загроз розташовуються саме у критичних зонах, то ця перевірка є добрим прикладом роботи антивірусу і не потребує багато часу. У разі знаходження небезпечної програми на екрані з’явиться спливаюче вікно у якому потрібно обрати подальші інструкції для антивірусу (рис. 12).

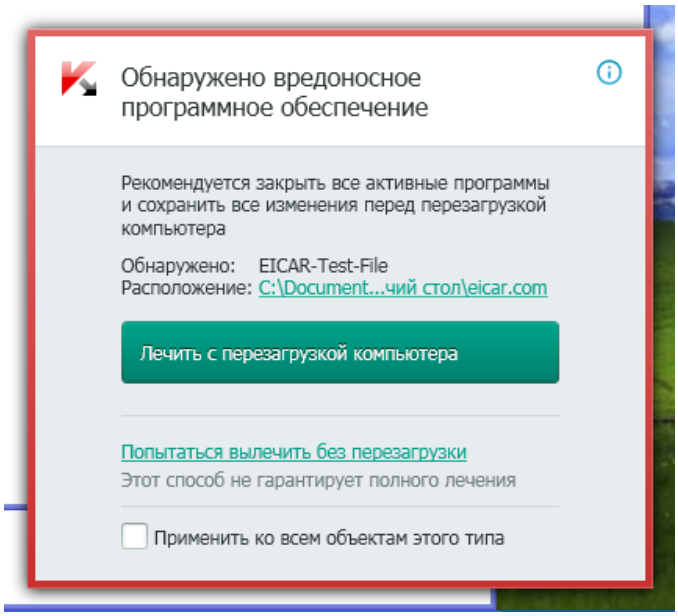

Рис. 12. Спливаюче вікно виконання дій

У більшості випадків достатньо лише вилікувати файл без перезавантаження комп’ютера, тому обираємо пункт «Попытаться вылечить без перезагрузки». В залежності від характеру загрози кількість та перелік пунктів у такому вікні може відрізнятися.

Після завершення перевірки на екрані, у нижній частині вікна перевірки буде відображено звітовну інфрамцію з результатами (рис. 13).

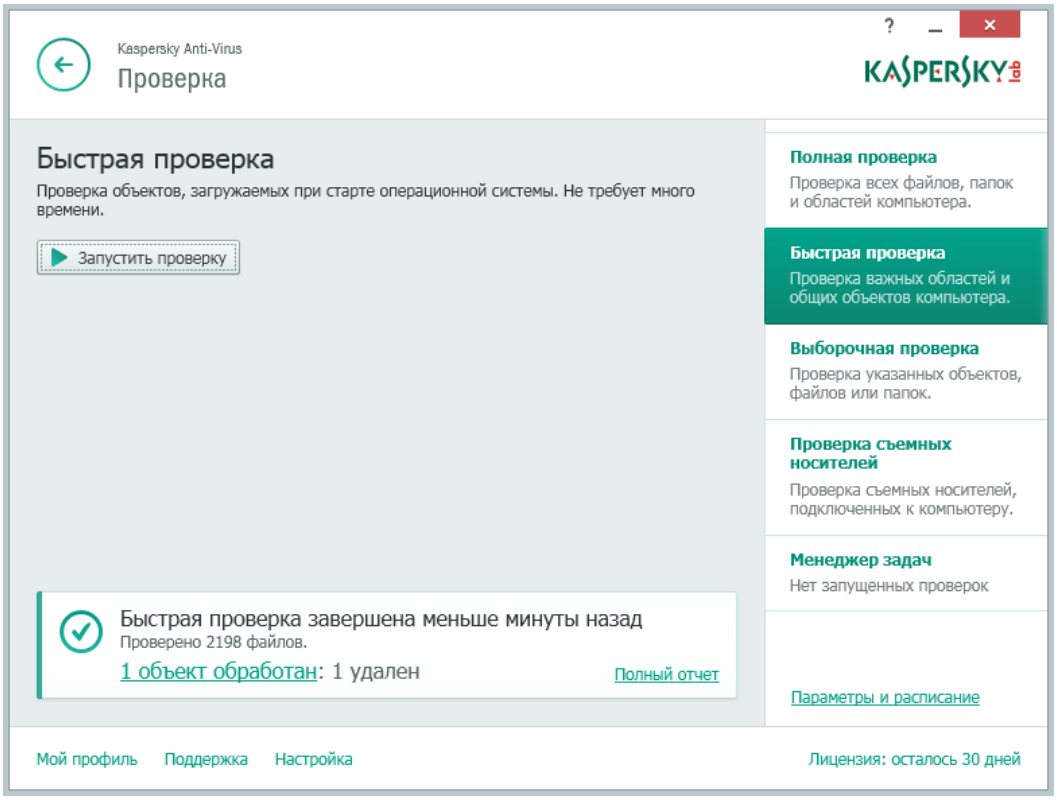

Рис. 13. Результат перевірки

Для перегляду більш детального звіту потрібно натиснути кнопку «Полный отчет» в якому можна передивитися які саме викликали підозру.

2.2.9. Налаштування перевірки. За замовчуванням перевірка комп'ютера виконуються з заздалегіть встановлених параметрів, які передбачають автоматичне виконання дій при наявності загрози.

Для налаштування автматичного виконання дій при перевірці, потрібно натиснути строку «Настройка» у нижній частині будь-якого вікна антивірусу. У відкритому вікні налаштувань натисніть на пункт «Проверка» (рис. 14).

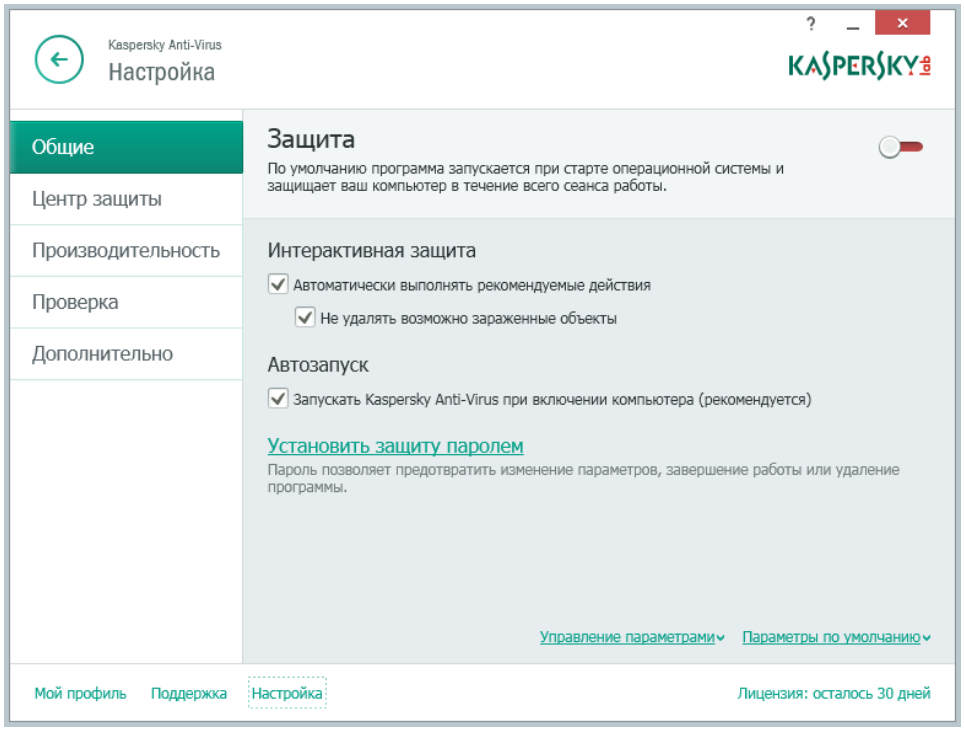

Рис. 14. Вікно загальних налаштувань

Для параметру «Уровень безопасности» потрібно встановити повзунок у положення «Рекомендуемый». Для параметру «Действие при обнаружении угрозы» з випадаючого списку обрати пункт «Лечит, неизлечимую - удалять» (рис. 15). Повторити пункт 2.2.8 з використанням повної перевірки.

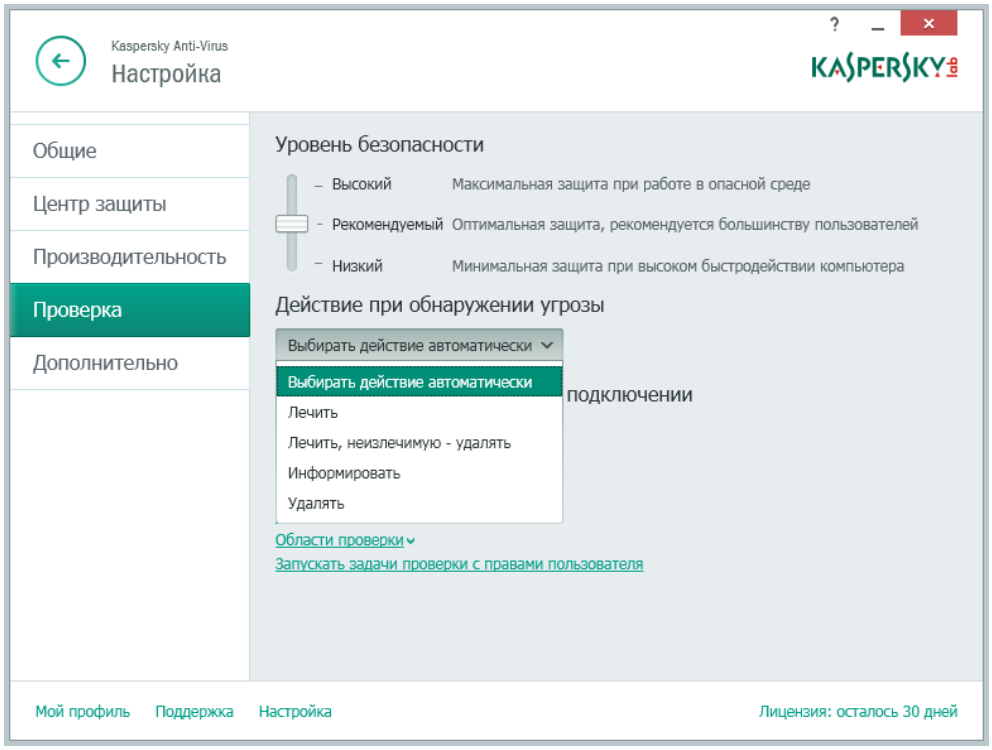

Рис. 15. Вікно налаштувань перевірки

3. **Домашнє завдання**. Провести перевірку домашнього комп'ютера на наявність вірусних програм. Для перевірки використати будь-яке доступне антивірусне програмне забезпечення окрім описаного у лабораторній роботі. Для достовірності роботи антивірусу скопіювати 10 файлів вірус-симуляторів у різні теки на різних дисках комп'ютера. Порядок виконання дій аналогічний пунктам 2.2.3 – 2.2.9. Процес виконання відобразити у звіті.
4. **Вимоги до вмісту і оформлення звіту**

Звіт з лабораторної роботи повинен містити:

— титульний лист;

— короткі теоретичні відомості;

— опис ходу роботи;

— отримані в ході виконання роботи знімки вікон програм;

— результати виконання домашнього завдання;

— висновки.

5. **Вимоги до оформлення звіту:**

— сторінки А4, відступ зліва – 20, зправа – 10, зверху – 15, знизу – 15;

— шрифт *Times New Roman* 14, відступ першого рядку – 1,25, інтервал – полуторний, вирівнювання – по ширині, вирівнювання малюнків – по центру;

— сторінки нумеровані.

6. **Контрольні питання**

1. Що таке комп'ютерний вірус?
2. Які бувають типи вірусів?
3. Що таке антивірус?
4. Що таке програма *firewall*.?
5. Яке антивірусне ПЗ Вам відомо, типи, назви?
6. У яких режимах працює антивірусне ПЗ?
7. Назвіть методи зараження вірусами та шляхи їх отримання?
8. Назвіть основні місця розташування вірусів в структурі ОС?

9. Чи безпечно працювати в Інтернеті за комп’ютером без антивірусу? Обґрунтуйте відповідь.
10. Як позбавитися вірусів якщо вони блокують встановлення антивірусу?
11. Чому жодна з існуючих програм не забезпечує 100% захищення від вірусів?