Київський національний торговельно-економічний університет
Кафедра інженерії програмного забезпечення та кібербезпеки

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Розробка програмного забезпечення антивірусного захисту робочої станції

Студента 4 курсу, 6 групи,
спеціальності 121 «Інженерія програмного забезпечення» _____ підпис студента — Купрієнко Андрія Сергійовича

Науковий керівник
кандидат технічних наук,
доцент _____ підпис керівника — Рассамакін Володимир Якович

Гарант освітньої програми
кандидат технічних наук,
доцент _____ підпис керівника — Цензура Микола Олександрович

КИЇВ – 2021

Київський національний торговельно-економічний університет

Факультет інформаційних технологій
Кафедра інженерії програмного забезпечення та кібербезпеки
Освітній ступінь бакалавр
Спеціальність 121 Інженерія програмного забезпечення

Затверджую
Зав. кафедри інженерії
програмного забезпеченнята
кібербезпеки
Криворучко О. В.
"20" жовтня 2020 р.

Завдання
на випускну кваліфікаційну роботу студентові

Купрієнко Андрію Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної роботи Розробка програмного забезпечення антивірусного захисту робочої станції
   Затверджена наказом ректора від "30" жовтня 2020 р. № 3225
2. Строк здачі студентом закінченої роботи
3. Цільова установка та вихідні дані до роботи
   Мета роботи аналіз існуючих програмно-апаратних засобів захисту робочих станцій. Та розробка програмного антивірусного захисту ПК.
   Об'єкт дослідження антивірусний захист
   Предмет дослідження розробка програми захисту робочої станції

4. Консультанти роботи із зазначенням розділів, які консультують:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видав	Завдання прийняв

5. Зміст випускної кваліфікаційної роботи (перелік питань за кожним розділом)

Вступ

Розділ 1. Комп'ютерні віруси

Загальні поняття та визначення

Класифікація вірусів

Антивірусна гігієна

Висновки до розділу 1

Розділ 2. Антивірусні програми

Сутність, класифікація та види антивірусних програм

Технологія використання антивірусних програм

Порівняльна характеристика існуючих програмних засобів антивірусного захисту

Висновки до розділу 2

Розділ 3. Створення програмного додатку антивірусного захисту

Розробка технічного завдання

Визначення алгоритму створення програми

Створення програми та її апробація

Висновки до розділу 3

Висновки

Список використаних джерел

Додатки

6. Календарний план виконання роботи

№ пор.	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів роботи	
		за планом	фактично
1	2	3	4
1.	*Вибір теми випускної кваліфікаційної роботи*	*21.09.2020*	*21.09.2020*
2.	*Вступ та перелік літературних джерел*	*14.12.2020*	*14.12.2020*
3.	*Розділ 1. «Комп'ютерні віруси»*	*19.02.2021*	*19.02.2021*
4.	*Розділ 2. «Антивірусні програми»*	*05.03.2021*	*05.03.2021*
5.	*Розділ 3. «Створення програмного додатку антивірусного захисту»*	*10.04.2021*	*10.04.2021*
6.	*Висновки*	*24.04.2021*	*24.04.2021*
7.	*Здача випускної кваліфікаційної роботи на кафедру (перша перевірка)*	*14.05.2021*	*14.05.2021*
8.	*Підготовка автореферату та презентації доповіді*	*17.05.2021*	*17.05.2021*
9.	*Попередній захист випускної кваліфікаційної роботи*	*18.05.2021 – 21.05.2021*	*21.05.2021*
10.	*Зовнішнє рецензування випускної кваліфікаційної роботи*	*01.06.2020*	*01.06.2020*
11.	*Здача прошитої випускної кваліфікаційної роботи на кафедру*	*02.06.2020*	*02.06.2020*
12.	*Публічний захист випускної кваліфікаційної роботи*		

7. Дата видачі завдання «20» жовтня 2020р.

8. Науковий керівник випускної кваліфікаційної роботи
Рассамакін В. Я.
(прізвище, ініціали, підпис)

9. Гарант освітньої програми Цензура М. О.
(прізвище, ініціали, підпис)

10. Завдання прийняв до виконання студент Купрієнко А.С.
(прізвище, ініціали, підпис)

11. **Відгук керівника випускної кваліфікаційної роботи**

Науковий керівник випускної кваліфікаційної роботи _____
(підпис, дата)

Відмітка про попередній захист Рассамакін В. Я.
(ПІБ, підпис, дата)

12.Висновок про випускну кваліфікаційну роботу

Випускна кваліфікаційна робота студента Купрієнко А. С.
(прізвище, ініціали)

може бути допущена до захисту екзаменаційній комісії.

Гарант освітньої програми Цензура М. О.
(прізвище, ініціали, підпис)

Завідувач кафедри Криворучко О. В.
(підпис, прізвище, ініціали)

«_____»____2021 р.

АНОТАЦІЯ

Дипломна робота на тему «Розробка програмного забезпечення антивірусного захисту робочої станції» містить 50 сторінок, 18 рисунків, 2 таблиці та 2 додатки. Перелік посилань налічує 19 найменувань.

Мета дослідження: аналіз існуючих програмно-апаратних засобів захисту робочих станцій. Та розробка програмного антивірусного захисту ПК.

Об'єкт дослідження: антивірусний захист.

Предметом дослідження є розробка програми захисту робочої станції.

У першому розділі було проведено аналіз предметної області і розглянуто різновиди вірусів і визначено, що для забезпечення антивірусного захисту необхідно застосовувати антивірусні програми.

У другому розділі було розглянуто різновиди антивірусів, їх класифікації та принципи роботи; також була проведена порівняльна характеристика.

У третьому розділі складено технічне завдання, де визначено мету, призначення та передумови створення додатку; описано вимоги до додатку; було описано процес реалізації додатку із використанням програмного комплексу Microsoft Visual Studio та мови C#, що відповідає всім встановленим вимогам.

ANNOTATION

Thesis on "Development of workstation antivirus protection software" contains 50 pages, 18 figures, 2 tables and 2 appendices. The list of links includes 19 items.

The purpose of the study: analysis of existing software and hardware protection of workstations and the development of software antivirus protection for PC.

Research subject: antivirus protection.

The subject of the study is the development of a workstation protection program.

In the first section, the subject area was analyzed and the types of viruses were considered, and it was determined that antivirus programs should be used to provide antivirus protection.

The second section considered the types of antiviruses, their classifications and principles of operation; a comparative characterization was also performed.

The third section contains a technical task, which defines the purpose, purpose and prerequisites for creating an application; the requirements for the application are described; described the process of implementing the application using Microsoft Visual Studio software and C# language, which meets all the established requirements.

ЗМІСТ

ВСТУП

Персональний комп’ютер відіграє важливу роль у житті сучасної людини, оскільки допомагає їй майже у всіх сферах його діяльності. Сучасне суспільство все більше інтегрується у віртуальний світ Інтернету. Однак при активному розвитку глобальних мереж питання інформаційної безпеки є важливим, оскільки віруси, які проникають в їх мережі, можуть порушити цілісність та збереження нашої інформації. Захист комп’ютера від вірусів - завдання, яке повинні виконувати всі користувачі, особливо ті, хто активно користується Всесвітньою павутиною або працює в локальній мережі.

Вперше термін «комп’ютерний вірус» з’явився в 1984 році.

У листопаді 1983 р. Американський студент Університету Південної Каліфорнії Фред Коен написав програму, яка продемонструвала можливість зараження комп'ютера швидкістю розмноження вірусу від 5 до 60 хвилин. Потім він використав цей термін у своєму звіті на конференції з питань інформаційної безпеки в Університеті Лечай у Сполучених Штатах і того ж року написав книгу під назвою Комп’ютерні віруси, теорія та експерименти.

Перший нелабораторний вірус під назвою "Мозок", який міг заражати лише дискети, з'явився в січні 1986 року і мав пакистанське походження. Перша «епідемія» цього комп’ютерного вірусу коштувала людству 300 000 доларів.

Перша антивірусна програма була розроблена в 1988 році. На даний момент відомо, що понад 150 000 комп’ютерних вірусів заражають комп’ютери та поширюються через комп’ютерні мережі.

Сьогодні Україна наздоганяє світових лідерів за поширенням комп'ютерних вірусів, тому ця тема є досить *актуальною*. Аналітики PC Tools - американського виробника засобів захисту від небажаного ПЗ - запевняють, що

за масштабами поширення комп'ютерних вірусів, шкідливого і шпигунського програмного забезпечення Україна може наздогнати таких "гігантів" в цій галузі, як Китай і США.

За оцінками аналітиків PC Tools на частку України припадає = 5,45 % шкідливих програм в світі (5 місце). Лідери це РФ = 27,89% (1), Китай = 26,52% (2), США = 9,98% (3), Бразилія = 6,77% (4).

Мета: аналіз існуючих програмно-апаратних засобів захисту робочих станцій. Та розробка програмного антивірусного захисту ПК.

Об'єктом випускної кваліфікаційної роботи є антивірусний захист.

Предметом ВКР є розробка програми захисту робочої станції.

Завдання дослідження:

. Аналіз предметної області антивірусного захисту робочої станції.

. Дослідження існуючих програмних засобів антивірусного захисту, їх порівняльна характеристика.

. Створення технічного завдання на розробку антивірусної програми для робочої станції.

. Визначення програмних засобів та середовищ програмування для розробки додатку.

. Визначення алгоритму використання засобів створення програми.

. Складання звіту та інструкцій по роботі з програмою.

Методики дослідження: програмування.

РОЗДІЛ 1
КОМП'ЮТЕРНІ ВІРУСИ

1.1. Загальні поняття та визначення

Поняття комп'ютерного вірусу

Комп'ютерний вірус - це спеціально написана невелика програма, яка може записувати свої копії в комп'ютерні програми, розташовані у виконуваних файлах, системних областях жорсткого диска, драйверах, документах тощо. Ці копії ще можна «відтворити». Процес, за допомогою якого вірус вставляє свою копію в іншу програму, називається зараженням, а програма або інший об'єкт, що містить вірус, - зараженою програмою.

Ознаки вірусної інфекції

Якщо ви підозрюєте, що ваш комп'ютер заражений вірусом, ось декілька основних ознак зараження комп'ютером:

. Комп'ютер працює повільніше, ніж зазвичай.

. Комп'ютер перестає реагувати або продовжує збій.

. Комп'ютер виходить з ладу та перезавантажується кожні кілька хвилин.

. Комп'ютер перезапуститься мимовільно. Крім того, комп'ютер працює не так, як зазвичай.

. Додаткові компоненти, встановлені на вашому комп'ютері, не працюватимуть належним чином.

. Не вдається отримати доступ до носія даних.

. Не вдається правильно надрукувати документи.

. З’являються незвичні повідомлення про помилки.

. Меню та діалоги спотворені.

. Нещодавно відкрите вкладення має подвійне розширення (JPG, VBS, GIF або EXE).

. Чомусь виявилося, що антивірус відключений. Його також не можна перезапустити.

. Антивірусну програму неможливо встановити або запустити.

. На робочому столі з’являються нові піктограми, які там ніхто не розміщував, або значки, які не стосуються останніх встановлених програм.

. Колонки раптом відтворюють дивні звуки або музику.

. Програми випадково видаляються з комп'ютера.

Принцип дії вірусів полягає у наступному. Коли заражена програма починає роботу, то спочатку управління отримує вірус. Вірус знаходить і "заражає" інші програми або інші об'єкти, а також може виконати якісь шкідливі дії. Потім вірус передає управління тій програмі, в якій він знаходиться, і вона працює так само, як зазвичай. Тим самим зовні робота зараженої програми виглядає так само, як і незаражених.

1.2. Класифікація вірусів

Таблиця 1.1

Типи вірусів

Вид	Принцип роботи
нешкідливі віруси	Зменшує вільний простір на жорсткому диску завдяки його "тиражуванню".
безпечні віруси	Скорочує вільний простір. Призводить до появи графіки, звуку та інших зовнішніх ефектів.
небезпечні віруси	Може призвести до збоїв у роботі комп'ютера та збоїв.
Дуже небезпечні віруси	Втрата програм та даних (зміна, видалення файлів та каталогів), форматування жорсткого диска тощо.

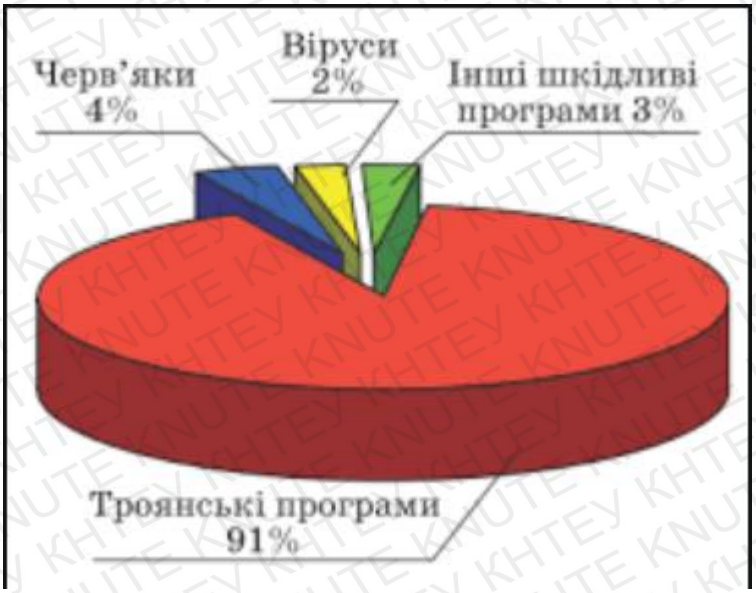

Рис. 1.1. Відсоткова діаграма типів вірусів

Детально розберемо саме 2% які вказані на малюнку 2

Небезпечні та безпечні віруси

Хоча віруси - це всього лише програми, але найчастіше вони зроблені з досить великою винахідливістю і підступністю. Так, деякі віруси можуть:

Обманювати резидентні програми-сторожів, наприклад, виконуючи зараження і псування інформації не за допомогою виклику функцій операційної системи, а за допомогою прямого звернення до програм введення-виведення BIOS або навіть портів контролера жорстких дисків або дискет.

Виживати при перезавантаженні - як при натисканні Ctrl Alt Del, так і при завантаженні з чистого системного диску після натискання кнопки "Reset" або виключення і включення комп'ютера.

Заражати файли в архівах (для витягання файлів з архіву і розміщення їх в архів викликається програма-архіватор, а висновок на екран при цьому блокується).

Заражати файли тільки при приміщенні їх на диски або в архіви (маскуючись тим самим від виявлення програмами-ревізорами).

Боротися з антивірусними програмами, наприклад, знищуючи їх файли або псуючи таблиці з відомостями про файли програми-ревізора.

Довгий час ніяк не проявляти своєї присутності, активізуючись через кілька тижнів або навіть місяців після зараження комп'ютера.

Шифрувати системні області дисків або дані на диску, так що доступ до них ставає можливий тільки при наявності даного вірусу в пам'яті.

Щоб комп'ютер заразився вірусом, необхідно, щоб на ньому хоча б один раз була виконана програма, що містить вірус, а саме:

Запущено заражений виконуваний файл або встановлено заражений драйвер.

Проведено початкове завантаження (або навіть завантаження початкового завантаження) із зараженою завантажувальним вірусом дискети.

Відкрито на редагування заражений документ Word для Windows або заражена електронна таблиця Excel.

Звідси випливає, що немає підстав боятися зараження комп'ютера вірусом, якщо:

На комп'ютер переписуються файли, які містять програм і не підлягають перетворенню в програми, наприклад, графічні файли, текстові файли (крім командних файлів і текстів програм), документи редакторів документів типу Лексикону або Multi-Edit, інформаційні файли бази даних і т.д.

На зараженому комп'ютері проводиться копіювання файлів з одного диску на інший чи інші дії, не пов'язані з запуском "чужих" (отриманих з зовні) програм, перезавантаженням з "чужих" дисків або редагуванням "чужих" документів Word для Windows або електронних таблиць Excel.

Крім того, вірус заражає лише програми, і не може заразити обладнання (клавіатуру, монітор і т.д.). Вірус не може заразити або змінити дані, що знаходяться на флешках або знімних дисках із встановленим захистом від запису, а також дані, що знаходяться на апаратно захищених логічних дисках.

Комп’ютерні віруси відрізняються між собою об’єктами, куди їх незаконно заносять, тобто якими об’єктами вони заражаються. Однак деякі віруси заражають різні типи об'єктів.

Файлові віруси

Більшість вірусів поширюються шляхом зараження виконуваних файлів, тобто файлів із іменами розширень .COM та .EXE та накладених файлів (тобто службових файлів, які завантажуються під час запуску інших програм). Такі віруси відомі як файлові віруси. Вірус у заражених виконуваних файлах починає працювати під час запуску програми, в якій він знаходиться. Наприклад Virus.Win9x.CIH.

Завантажувальні віруси

Ще один широко поширений вид вірусів впроваджується в початковий сектор дискет або логічних дисків, де знаходиться завантажувач оперативної

системи, або в початковий сектор жорстких дисків, де знаходиться таблиця розбиття жорсткого диска і невелика програма, що здійснює завантаження з одного з розділів, зазначених у цій таблиці. Такі віруси називаються завантажувальними. Ці віруси починають свою роботу при завантаженні комп'ютера з зараженого диска. Завантажувальні віруси завжди є резидентними і заражають встановлені в комп'ютер носії. Зустрічаються також завантажувальні віруси, що заражають і файли - файлово-завантажувальні віруси.

Для зараження комп'ютера завантажувальним вірусом достатньо всього один раз залишити заражену флешку у порті: в момент перезавантаження комп'ютера. При цьому вірус заразить жорсткий диск комп'ютера. І після цього при завантаженні з жорсткого диска комп'ютера буде запускатися вірус. Наприклад, вірус Virus.Boot.Snow.

Вірус драйверів

Деякі віруси вміють заражати драйвери, тобто файли, які вказуються в пропозиції DEVICE або DEVICEHIGH файлу CONFIG. SYS. Вірус, що знаходиться в драйвері, починають свою роботу при завантаженні цього драйвера з файлу CONFIG. SYS при початковому завантаженні комп'ютера. Зазвичай заражають драйвери, віруси заражають також виконувані файли або завантажувальні сектори дисків, оскільки інакше їм не вдавалося б поширюватися - адже драйвери дуже рідко переписують з одного комп'ютера на інший. Іноді зараження драйверів використовується як етап в стратегії поширення вірусу. Наприклад, вірус JEWS-2339 при завантаженні з виконуваного файлу заражає всі драйвери, виявлені в CONFIG.SYS, а при завантаженні зараженого драйвера стає резидентним і заражає всі файли на носіях (а на жорсткому диску, навпаки, лікує).

Віруси, які заражають пакетні файли

Дуже рідкісний тип вірусу - це вірус, який заражає файли команд. Як правило, ці віруси використовують команди командного файлу (команди ECHO тощо) для створення виконуваного файлу на жорсткому диску (зазвичай у форматі COM), запуску цього файлу, відтворення вірусу та пошкодження дії, після якої цей файл створюється та видаляється . Вірус у заражених пакетних файлах буде працювати, якщо ви запустите пакетний файл, в якому він знаходиться. Іноді виклик зараженого пакетного файлу вставляється у файл AUTOEXEC. BAT.

Макровіруси

Влітку 1995 року з'явився новий різновид вірусів - віруси, що заражають документи Word для Windows версії 6.0 і 7.0. Внаслідок поширеності редактора Word для Windows такі документи є майже на кожному комп'ютері. Довгий час зараження файлів документів вважалося неможливим, так як документи не містили здійснюваних програм. Однак програмісти фірми Microsoft вбудували в документи Word для Windows потужну мову макрокоманд WordBasic. При цьому дії не помітні в редагованому - для їх перегляду і редагування треба вибрати в групі меню Tools (сервіс) пункт Macro (Макрос), а чи багато користувачів взагалі щось чули про цей пункт меню. На цьому WordBasic стало можливо писати віруси. Запуск вірусу відбувається при відкритті на редагування заражених документів. При цьому дії вірусу записуються в глобальний шаблон NORMAL..DOT, так що при нових сеансах роботи з Word для Windows вірус буде автоматично активований. При наявності вірусу, при збереженні редагованих документів на диск під новим ім'ям (командою Save As) вірус копіює свої макроси до записаного на диск документу, так що той виявляється зараженим. Наприклад, вірус Melissa.A.

Таблиця 1.2.

Результати впливу вірусів

Тип вірусу	Результат дії
Файлові віруси	Впроваджено в програми та активовано під час їх запуску.
Завантажте віруси	Напишіть себе в завантажувальному секторі жорсткого диска. При запуску вони поводяться як файлові віруси.
Макровіруси	Існують макроси, які заражають файли документів Word і Excel.
Вірус драйверів	Вони заражають драйвери обчислювальних пристроїв або запускають самостійно, додаючи додатковий рядок до файлу конфігурації.
Мережеві віруси	Заразіть комп'ютер, відкривши вкладений файл у повідомленні електронної пошти. Вони викрадають паролі користувачів і надсилають себе на електронні адреси.

Файли, які не заражаються вірусами

Вірус є програмою, тому об'єкти, що не містять програм і не підлягають перетворенню в програми, не можуть бути зараженими. Наприклад, графічні файли форматів. BMP. PCX. GIF. WMF і ін. Містять тільки опис малюнків, тому як би їх вірус не змінював, при перегляді чи іншому використанні графічного файлу можна отримати спотворений малюнок або повідомлення про неправильний формат файлу, але вірус при цьому запущений бути не може. Іншими словами, програми які не містять об'єкти вірус може тільки зіпсувати, але не заразити. До числа таких об'єктів відносяться текстові файли (крім командних файлів і текстів програм), документи простих редакторів документів типу Лексикону або Multi- Edit, інформаційні файли без даних і т.д.

1.3. Антивірусна гігієна

Якщо яка-небудь з програм-детекторів повідомить про те, що вона знайшла відомий їй вірус, то бажано прочитати в її документації або

вбудованому довіднику відомості про даний тип вірусу. Наприклад, в комплект поставки програм-детекторів Aidstest і Doctor Web входять текстові файли з описами знайомих їм вірусів. Відомості про віруси дозволять Вам оцінити можливі наслідки зараження і вибрати необхідні заходи щодо їх усунення. Наприклад, якщо комп'ютер виявився заражений безпечним завантажувальним вірусом, то крім видалення вірусу з жорсткого диска і флешок, якими Ви користувалися, робити нічого не треба. А усунення наслідків вірусом, що змінює випадково вибрані ділянки диска, можуть бути набагато серйозніше - зазвичай при цьому доводиться заново встановлювати всі пакети програм з дистрибутивів, а власні дані - з резервних копій.

Кожного разу, коли ви заражаєте свій комп’ютер вірусом (або якщо ви підозрюєте про це), важливо дотримуватися певних правил.

Перш за все, не треба поспішати і приймати необачних рішень, непродумані дії можуть призвести не тільки до втрати частини даних, які можна було б відновити, але і до повторного зараження комп'ютера.

Однак заходи потрібно вжити негайно. Якщо ви абсолютно не впевнені, що розпізнали вірус до того, як він став активним на вашому комп’ютері, вам слід вимкнути комп’ютер, щоб не дати вірусу продовжувати руйнівні дії.

Всі дії по виявленню виду зараження і лікування комп'ютера слід виконувати тільки при правильному завантаженню комп'ютера з захищеної від запису "еталонною" диску з операційною системою. При цьому слід використовувати тільки програми (виконані файли), що зберігаються на захищених від запису дисках. Недотримання цього правила може призвести до дуже тяжких наслідків, оскільки при завантаженні DOS або запуску програми з зараженого диска в комп'ютері може бути активований вірус, а якщо працює вірус, лікування комп'ютера буде безглуздим, так як воно буде супроводжуватися подальшим зараженням дисків і програм.

Але для цього є антивірусні програми, які треба встановлювати і їми користуватись.

1.4. Висновки до розділу 1

Отже, однією з глобальних проблем комп'ютеризації мереж та телекомунікаційних мереж є небезпека зараження комп'ютерними вірусами, особливо на рівні користувача, коли може зникнути вся інформація.

В першому розділі розглянуто різновиди вірусів і визначено, що для забезпечення антивірусного захисту необхідно застосовувати антивірусні програми.

РОЗДІЛ 2
АНТИВІРУСНІ ПРОГРАМИ

2.1. Сутність, класифікація та види антивірусних програм

Антивірусна програма - спеціальна програма, призначена для виявлення комп'ютерних вірусів, а також небажаних (класифікуються як шкідливі) програм загалом, а також для відновлення заражених (модифікованих) файлів такими програмами, а також для запобігання - попередження заражень (модифікації) файлів або операційної системи зі шкідливим кодом. Звичайно, крім регулярних резервних копій даних та профілактичних заходів для зменшення ймовірності зараження вірусом слід використовувати антивірусні програми. Якщо ви розглядаєте системи Microsoft, вам слід знати, що антивірус зазвичай працює за такою схемою:

- Пошук підписів вірусів у базі даних антивірусного програмного забезпечення;
- Якщо заражений код виявляється в пам'яті (операційній та / або постійній), процес карантину запускається, і процес блокується.
- Зареєстрована програма зазвичай видаляє вірус, незареєстрована програма вимагає реєстрації та робить систему вразливою.

Види антивірусних програм

Антивірусні програми можна розділити на типи залежно від виконуваних ними функцій.

Детектори (Сканер). Програми-детектори можуть використовуватися для виявлення файлів, заражених одним із декількох відомих вірусів. Деякі

програми-детектори також виконують евристичний аналіз файлів і системних областей носіїв даних, що часто дозволяє виявляти нові віруси, невідомі програмі-детектору. У багатьох програмах-детекторах ви також можете "лікувати" заражені файли або носії даних, видаляючи з них віруси (лікування, звичайно, підтримується лише для вірусів, відомих програмі-детектору).

Фаги (Поліфаген). Програми можуть знайти вірус (фаги) або кілька вірусів (поліфаги) і знищити їх. Сучасні версії зазвичай виконують евристичний аналіз файлів - вони перевіряють файли на наявність вірусоспецифічного коду.

Аудитори. Цей тип антивірусу контролює всі засоби (відомі на момент публікації) зараження комп'ютерів. Таким чином, можна знайти вірус, який був створений після публікації програми аудитора. Часто аудиторів можна налаштувати на те, щоб повідомляти лише про підозрілі (специфічні для вірусу або неприйнятні) зміни, не заважаючи користувачеві. Часто програми моніторингу також можуть «лікувати» заражені файли або томи, видаляючи з них віруси (це можна зробити майже для всіх типів вірусів).

Guardian. Програми Guardian (або фільтри) знаходяться в оперативній пам'яті комп'ютера та сканують на наявність вірусів. Якщо вірус присутній, користувач буде повідомлений про це. Крім того, багато «сторожових собак» перехоплюють дії, які віруси використовують для відтворення та пошкодження (наприклад, намагаються записати в завантажувальний сектор або відформатують жорсткий диск) і повідомляють про них користувача. Користувач може затвердити або відхилити відповідний процес. Сторожові програми можуть розпізнати багато вірусів як можна раніше, коли вірус ще не відтворився і щось зіпсував. Це може мінімізувати пошкодження вірусом.

Вакцини. Використовується для обробки файлів і завантажувальних секторів для запобігання зараженню відомими вірусами (цей метод останнім

часом все частіше застосовується). Як відомо, жоден із цих типів антивірусного програмного забезпечення не пропонує 100% захисту комп'ютера, і бажано використовувати їх разом з іншими пакетами. Вкрай неправильно вибирати лише «найкращу» антивірусну програму.

Анотація:

. Рівень захисту, який забезпечують сторожові програми, не слід переоцінювати, оскільки деякі віруси отримують безпосередній доступ до програм BIOS системи, щоб поширювати та пошкоджувати їх, не використовуючи стандартний спосіб виклику цих програм через переривання, а антивірусні програми-резиденти використовують лише ці переривання Catch.

. Перед перезапуском багато програм сторожового пошуку шукають диски після натискання комбінації клавіш Ctrl + Alt або за запитом програми, вставленої в дисковод гнучких дисків. Однак, якщо завантаження відбувається після натискання кнопки скидання або після ввімкнення комп'ютера, сторожі не зможуть допомогти, оскільки зараження вірусом завантаження відбувається під час завантаження операційної системи, тобто до запуску програм або встановлення драйверів .

Також маємо приклади використання програм вакцинації або імунізаторів, які модифікують програми та засоби масової інформації, щоб вони не заважали роботі програм, але вірус, від якого проводиться щеплення, враховує ті програми або носії, які вже заражені. Ці програми неефективні і більше не будуть розглядатися.

Класифікація антивірусних продуктів

Можна класифікувати антивірусні продукти з ряду причин, таких як: Наприклад: використовувані технології антивірусного захисту, функціональність продукту, цільові платформи.

Відповідно до використовуваних антивірусних технологій захисту:

Класичні антивірусні продукти (продукти, що використовують лише метод виявлення підписів).

Проактивні антивірусні продукти (продукти, що використовують лише проактивні антивірусні технології);

Комбінована продукція (продукція, яка використовує як класичні, так і фірмові та попереджувальні методи захисту.

Відповідно до функціональності продукту:

Антивірусні продукти (продукти, що забезпечують лише захист від вірусів)

Комбіновані продукти (продукти, які не тільки забезпечують захист від шкідливого програмного забезпечення, але також фільтрують спам, шифрують та створюють резервні копії даних та інші функції).

За цільовими платформами:

Антивірусні продукти для сімейства операційних систем Windows

До цього сімейства належать антивірусні продукти для сімейства операційних систем * NIX (BSD, Linux тощо).

Антивірусні продукти для сімейства операційних систем MacOS

Антивірусні продукти для мобільних платформ (Windows Mobile, Symbian, iOS, BlackBerry, Android, Windows Phone 7 тощо)

Антивірусні продукти для корпоративних користувачів також можна класифікувати за об'єктами захисту:

Антивірусні продукти для захисту робочих станцій

Антивірусні продукти для захисту файлових серверів і серверів терміналів

Антивірусні продукти для захисту електронної пошти та Інтернет-шлюзів

Антивірусні бази даних.

Для того, щоб мати можливість використовувати антивірус, ви повинні постійно оновлювати так звані антивірусні бази даних. Вони є інформацією про віруси - як їх знайти і як знешкодити. Оскільки віруси пишуть часто, діяльність

вірусів у мережі повинна постійно контролюватися. Для цього існують спеціальні мережі, які збирають відповідну інформацію. Після збору цієї інформації проводиться аналіз шкідливості вірусу, аналізується його код і поведінка, а потім визначаються варіанти боротьби з вірусом. Більшість вірусів працює з операційною системою. У цьому випадку ви можете просто видалити початкові рядки вірусу з реєстру. У цьому простому випадку процес може бути припинено. Більш складні віруси можуть заражати файли. Наприклад, відомі випадки, як деякі, навіть самі антивірусні програми інфікували інші чисті програми та файли. Тому більш сучасні антивірусні програми можуть захищати свої файли від змін і перевіряти їх цілісність за спеціальним алгоритмом. Тому віруси ускладнились, як і способи боротьби з ними.

Тепер ви можете побачити віруси, обсяг яких становить уже не десять кілобайт, а сотні, а іноді і кілька мегабайт. Як правило, такі віруси написані мовами програмування високого рівня, щоб їх не було легше зупинити. Проте все ще існує ризик вірусів, написаних на низькорівневому коді збірки, такому як мова збірки. Складні віруси заражають операційну систему, а потім стають вразливими та непрацездатними. На жаль, за прогнозами, робота антивірусних компаній найближчим часом буде значно ускладнена через цей факт.

2.2. Технологія використання антивірусних програм

Жодна антивірусна програма не пропонує повний захист від вірусів. Однак спільний доступ до антивірусних програм дає хороші результати, оскільки вони добре доповнюють одна одну.

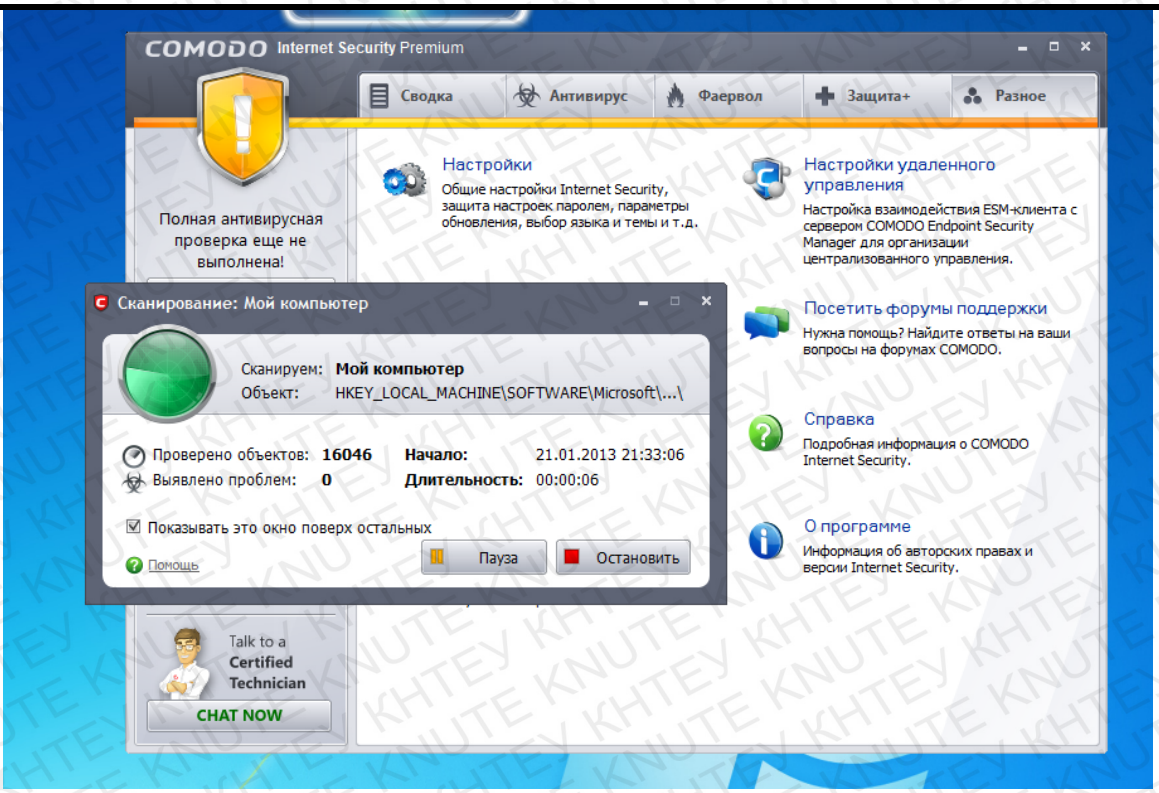

Рис. 2.1. Антивірусне вікно

Вхідні дані із зовнішніх джерел (файли, диски тощо) перевіряються програмою-детектором. Якщо ви забули перевірити ці дані, і заражена програма була виконана, її може "перехопити" сторожова програма. Однак в обох випадках надійно виявляються лише віруси, відомі цим антивірусним програмам. Невідомі віруси, детектори та охоронці, які не містять евристичного аналізатора, взагалі не виявляють (один приклад - програма Aidstest), але мають такий аналізатор - не виявляють більше 80-90% випадків.

The Guard може навіть виявляти невідомі віруси, якщо вони поводяться дуже сміливо, наприклад, якщо ви намагаєтеся відформатувати жорсткий диск або внести зміни до системних файлів або областей жорсткого диска на жорсткому диску. Однак деякі віруси можуть обійти цей контроль. Незначні пошкодження вірусів (зміна програмних файлів, запис у системну область з дискет тощо), як правило, не відстежуються, оскільки ці дії виконують не тільки віруси, але й багато програм.

Якщо вірус не був виявлений детектором або охоронцем, результати його діяльності виявить рецензент програми.

Як правило, сторожові органи повинні постійно працювати на комп'ютері, детектори повинні використовуватися для перегляду даних із зовнішніх джерел даних (файлів та дисків), а аудитори повинні запускатися один раз на день для виявлення та аналізу змін у носіях.

Оновлення антивірусних програм

Детективні програми слід регулярно оновлювати.

Щотижня з'являються нові віруси. Якщо ви використовували версії програм півроку або рік тому, дуже ймовірно, що ці програми невідомі, якщо ви інфіковані вірусом.

Ви можете бути впевнені, що на вашому комп'ютері є вірус, якщо:

Програма детектор повідомляє про наявність відомого вірусу в оперативній пам'яті, у файлах або в системних областях на жорсткому диску.

Рецензент повідомляє про зміни у файлах, які не слід змінювати. Зміни незвично часто вносяться, наприклад. Зміст файлу змінюється, а час його зміни - ні.

Верифікатор повідомляє про зміну в головному завантажувальному записі (головне завантаження, що містить таблицю розділів диска) або в завантажувальному записі (завантажувальний запис), і ви не змінювали розділ диска або не встановлювали нову версію операційної системи і не давали інші причин зміни цієї області диска.

Програма сторожа повідомляє, що програма збирається відформатувати жорсткий диск, змінити системні області жорсткого диска тощо, і ви не скерували жодної програми для виконання таких дій.

Програма аудитора повідомила про наявність у пам'яті «невидимих» вірусів. Це виражається в тому, що для деяких файлів або областей жорсткого диска виводиться різний вміст при читанні в DOS і при читанні через прямий

доступ до жорсткого диска.

Вірус представився вам, показавши повідомлення.

Ви можете запідозрити вірус, якщо:

Антивірусна програма повідомляє про виявлення невідомого вірусу.

Повідомлення, піктограми тощо сторонніх виробників відображаються на екрані або принтері.

Деякі файли пошкоджені.

Деякі програми перестали працювати або перестали працювати належним чином.

Робота на комп'ютері значно уповільнена.

Однак подібні явища можуть бути викликані не вірусом, а скоріше несправними програмами, несправностями обладнання тощо.

Тепер про деякі особливості антивірусних пакетів. Перше, на що слід звернути увагу, - це кількість розпізнаваних підписів - серія символів, які вірус гарантовано розпізнає. Слід зазначити, що виробники використовують різні системи підрахунку підписів: якщо деякі різні версії або подібні відмінні версії вірусів розглядаються як одна підпис, друга враховує всі варіації. Найкращі пакунки виявляють близько 10 000 вірусів, що трохи менше загальної кількості шкідливих програм, доступних сьогодні. Другий параметр - наявність евристичного аналізатора невідомих вірусів. Його наявність дуже корисна, але це значно уповільнює програму.

2.3. Дослідження існуючих програмних засобів антивірусного захисту. Їх порівняльна характеристика

Спробуємо розібратися з найкращими антивірусними продуктами, які на сьогодні є найпоширенішими на українському ринку та в Інтернеті. Ми говоримо про комплексні антивірусні пакети, які забезпечують найвищий рівень захисту вашої інформації.

Серед розробників найбільш відомими є ряд "Лабораторії Касперського", "Eset, NOD32", "Symantec" та "Dr.Web". Почнемо з продуктів словенської компанії «Eset», оскільки ці програми вже стали стандартними, і переважна більшість комп'ютерів у нашій країні оснащені цими антивірусними програмами.

Рис. 2.2. Логотипи найпопулярніших антивірусних програм

Eset NOD32

Інформація з офсайту: «ESET, розробник програмного забезпечення для захисту інформації, існує з 1992 року. Сьогодні ESET - це міжнародна компанія, яка входить до списку 500 найшвидших організацій у галузі інформаційних технологій «Deloitte Technology Fast 500». ESET має офіси у понад 100 країнах. Головний офіс знаходиться у Братиславі, Словаччина. Серед клієнтів ESET - такі компанії, як Canon, Dell та Microsoft. Продукти ESET виграли численні престижні нагороди та є лідерами на ринку програмних рішень для захисту.

ESET пропонує рішення для домашніх та бізнес-користувачів, які допомагають захистити окремі комп'ютери та елементи комп'ютерних мереж від загроз, пов'язаних із шкідливим програмним забезпеченням. Усі продукти

ESET NOD32 використовують запатентовану технологію ThreatSense, яка дозволяє антивірусному рішенню забезпечити неперевершений рівень виявлення та видалення шкідливого програмного забезпечення.

Протягом останніх 10 років вірусний бюлетень перевіряв рішення ESET NOD32 не пропускав жодного вірусу "У дикій природі". За версією австрійської випробувальної лабораторії Andres Clementi AV-Comparatives, антивірус ESET NOD32 був визнаний найкращим продуктом.

Попередник антивіруса ESET NOD32 народився приблизно в той самий час, що і перший комп'ютерний вірус. І це був травень 1988 р. Тоді ж серіал «Лікарня на краю міста» (або «Немочниця на Окраї Места») був дуже популярним на чехословацькому телебаченні. Як ми пам’ятаємо, перші віруси атакували лише сектор взуття, який також знаходиться на «краю» жорсткого диска. В результаті було випущено антивірус "Лікарня на межі" (або "Nemocnica na Okraji Disku", що означає NOD). Можливо, це пов'язано з особливою популярністю та любов'ю. Цей антивірус використовують користувачі із східноєвропейських країн, де слов'янська вимова є більш поширеною. На сьогодні, звичайно, антивірусна система NOD32 принципово відрізняється від перших версій NOD. Кожне покоління антивірусів NOD було ретельно розроблено.

Система перекладена на 32-розрядної основі, про що свідчить префікс "32" для написання NOD32 сьогодні. І ось попереднє окреме написання NOD32 вже є в історії. NOD та 32 були об’єднані, щоб сформувати єдино правильний варіант написання - NOD32, хоча програмне забезпечення ESET NOD32 тепер також підтримує 64-розрядні операційні системи Windows.

Функції програми:

- Захистіть електронні листи від спаму, шахрайства та фішингових повідомлень

- Захистіть конфіденційність шляхом виявлення та знищення програм-шпигунів
- Вбудований брандмауер із виявленням вторгнень для захисту вхідних та вихідних з'єднань
- Неперевершена продуктивність програми
- Зручність для користувачів
- Проактивний захист
- Виявлення вірусів, троянських програм, шпигунських програм та інших загроз
- Встановлення сервера
- Дистанційне управління
- Дзеркальна функція для оновлення антивірусних баз даних з локального сервера»

Антивірус Касперського

"Лабораторія Касперського" - одна з найпопулярніших в Україні та найбільший у Європі виробник засобів захисту від вірусів, спаму та хакерських атак. Компанія є одним із п’яти провідних світових постачальників програмного забезпечення для захисту інформації.

Лабораторія Касперського

«Лабораторія Касперського» - це міжнародна група компаній зі штаб-квартирою в Москві та п’ятьма регіональними відділами, які керують діяльністю місцевих представників та партнерів компанії у відповідних регіонах: у Західній Європі, Східній Європі, Східній та Африці, Північній та Південній Америці, Японії та інших країн Азіатсько-Тихоокеанського регіону. Партнерська мережа компанії об’єднує понад 700 партнерів першого рівня у понад 100 країнах. Технології компанії захищають понад 250 мільйонів користувачів у всьому світі.

Антивірус Касперського - це продукт захисту, який протестували мільйони користувачів по всьому світу. Нове антивірусне ядро пропонує вищу швидкість, а вдосконалений та інтуїтивно зрозумілий користувальницький інтерфейс дозволяє негайно оцінити рівень безпеки системи та нейтралізувати будь-які виявлені загрози безпеки лише за кілька кліків ведмедя.

Ліцензійне програмне забезпечення

«Антивірус Касперського» - створений на основі передових розробок у галузі інформаційної безпеки та відповідає всім сучасним вимогам. Він пропонує надійний захист ваших персональних даних від існуючих загроз безпеці.

Інформація ззовні: Kaspersky Internet Security - найпопулярніший продукт захисту комп'ютерів. Програма містить усе необхідне для безпечної роботи в Інтернеті.

Базовий захист

* Комплексний захист від усіх типів шкідливих програм

* Перевірте файли, електронні листи та Інтернет-трафік

* Автоматичне оновлення бази даних

Розширений захист

* Персональний брандмауер

* Безпечна робота в мережах Wi-Fi та VPN

* Захист від мережевих атак

Запобігання загрозам

* Інноваційна система встановлення правил та моніторингу застосування

* Проактивний захист від нових і невідомих загроз

* Шукайте вразливості в операційній системі та встановленому програмному забезпеченні

* Блокувати посилання на заражені веб-сайти

Захист конфіденційних даних

* Блокувати посилання на фішингові сайти

* Віртуальна клавіатура для безпечного входу та паролів

* Запобігання крадіжці даних, переданих через з'єднання SSL (за допомогою протоколу HTTPS)

* Блокувати несанкціоновані телефонні дзвінки

Захист від небажаного вмісту

* Батьківський контроль

* Захист від спаму

Комплект Dr.Web-антивірусів

Сильний антивірус із сильним алгоритмом виявлення вірусів. Він багатофазний, DrWEB може «читати» стиснуті файли та архіви, файли даних у форматах Word та Excel та деактивувати поліморфні віруси, які за останні

години отримали більше місця для зберігання. Досить сказати, що епідемія дуже небезпечна. Вірус OneHalf зупиняє DrWeb. Евристичний аналізатор DrWeb, який досліджує програми для пошуку специфічних для вірусів областей коду, може знайти близько 90% невідомих вірусів. Коли ви завантажуєте програму, DrWeb перевіряє себе на цілісність, а потім перевіряє оперативну пам'ять - залежно від налаштування, 640 КБ або 1024 КБ (включаючи HMA). Бажано перевірити всю пам'ять. У цьому випадку процес сканування триватиме довше. Однак справа в тому, що віруси можна довго завантажувати у верхню пам'ять. Алгоритм роботи цього антивірусу полягає в тому, що він емулює процесор (створює модель комп'ютерного програмного забезпечення). Нові версії рідко відображаються. Він має зручний інтерфейс, який можна налаштувати.

Остання версія "Dr. Web" (5.0.0.12300)

Інформація ззовні: Doctor Web - провідний російський розробник засобів інформаційної безпеки. Компанія пропонує ефективні антивірусні та антиспамові рішення для великих компаній та державних організацій, а також для приватних користувачів. Антивірусні продукти Dr.Web розробляються з 1992 року і постійно демонструють чудові результати у виявленні шкідливого програмного забезпечення та задоволенні глобальних стандартів безпеки. Компанія Doctor Web має ліцензії, сертифікати відповідності FSTEC та сертифікат лабораторії ICSA Labs. Компанія є сертифікованим партнером Microsoft у галузі ISV / Software Solutions.

Рішення Dr.Web засновані на захисті інформаційних ресурсів вищих органів влади, українських та закордонних міністерств та відомств, найбільших торгових компаній та банків. Відомі Інтернет-портали, хостинг-провайдери та інтернет-провайдери довіряють програмам під брендом Dr.Web.

Переваги рішень Dr.Web:

Рішення сімейства Doctor Web - це передові технології, що містяться в програмах, що забезпечують найвищий рівень захисту інформації.

Антивірус Dr.Web:

• Захист від вірусів, шпигунського, рекламного та потенційно небезпечного програмного забезпечення;

• Можливість встановити на вже заражений комп'ютер і вилікувати заражену систему;

• Мінімальне споживання комп'ютерних ресурсів;

• Повне сканування системної пам'яті комп'ютера, виявлення безтілесних вірусів, які не існують у вигляді файлів;

• Перегляньте багато типів архівів, включаючи вкладені багатотомні файли, що самовідкриваються (SFX), упаковані з усіма типами упаковки.

• Евристичний аналізатор постійно вдосконалюється, щоб ви могли ефективно виявляти віруси, використовуючи ряд неявних функцій.

Антиспам Dr.Web

• Різні технології фільтрування для кожного типу небажаних повідомлень забезпечують високу ймовірність виявлення спаму.

• Незалежність від поштових клієнтів - працює без плагінів (модулів) для електронних програм;

• Значна економія трафіку даних завдяки автономному режиму модуля аналізу спаму.

• Завдяки унікальним технологіям виявлення спаму ви можете оновлювати не частіше одного разу на день та економити трафік користувачів.

• Перевіряйте більше 100 повідомлень на секунду "на льоту" (на комп'ютері з 1,9 ГГц процесором Pentium 4).

• Не вимагає попередньої підготовки;

• Простий у використанні.

Symantec Antivirus

Інформація ззовні: Американська компанія Symantec Corporation, світовий лідер на ринку безпечних Інтернет-технологій, була заснована в 1982 році і має офіси в 40 країнах. Компанія пропонує широкий спектр програмних та апаратних рішень для забезпечення безпеки систем як приватних користувачів, так і малих і великих компаній. Продукція корпорації Symantec широко використовується у всьому світі.

Корпорація Symantec - провідний розробник засобів захисту від вірусів, моніторингу вразливості, систем виявлення вторгнень, фільтрів Інтернету та електронної пошти, а також технологій віддаленого доступу та управління. Продукти Norton SystemWorks, Personal Firewall захищають важливу інформацію та дозволяють керувати мережевими налаштуваннями. Symantec AntiVirus, Norton AntiVirus автоматично видаляє віруси, шпигунське та рекламне програмне забезпечення, не впливаючи на роботу користувача. Symantec Premium AntiSpam, Symantec Hosted Mail Security та Symantec Mail Security для SMTP забезпечують потужний захист електронних листів від вірусів, спаму та іншого небажаного вмісту. Symantec Network Access Control - це комплексне рішення контролю доступу до мережі.

Основні переваги:

- Покращений корпоративний захист та моніторинг від однієї консолі управління.
- Інтегровані веб-графічні звіти
- Він зростає і має підтримку тисяч користувачів
- проста установка
- Раціональна та комфортна робота
- Наявні звіти відповідають основним адміністративним вимогам
- Підтримка клієнта Linux®
- Покращений захист від шпигунського та рекламного ПЗ
- Автоматичне блокування встановлення шпигунських програм
- Виявлення та видалення прихованих програм-шпигунів
- Вказує на ефекти шпіонського програмного забезпечення на основі Symantec Risk Impact Matrix
- Покращений захист від впливу шпигунських програм

Засоби захисту від фальсифікації Symantec запобігають несанкціонованому доступу та атакам антивірусної програми, захищаючи користувачів від вірусів, які намагаються блокувати заходи безпеки.

Працює на основі Symantec ™ Security Response, найкращої у світі організації з досліджень та підтримки Інтернету.

2.3. Висновки до розділу 2

Для знищення вірусів створені спеціальні антивірусні програми для виявлення, лікування заражених файлів і жорстких дисків, виявлення та запобігання підозрілим (специфічним для вірусів) діям. Жодна антивірусна програма не пропонує повний захист від вірусів. Однак спільний доступ до антивірусних програм дає хороші результати, оскільки вони добре доповнюють одна одну.

Звичайно, крім регулярних резервних копій даних та профілактичних заходів для зменшення ймовірності зараження вірусом слід використовувати антивірусні програми. Для того, щоб мати можливість використовувати антивірус, ми повинні постійно оновлювати так звані антивірусні бази даних. Вони є інформацією про віруси - як їх знайти і як знешкодити.

РОЗДІЛ 3
СТВОРЕННЯ ПРОГРАМНОГО ДОДАТКУ АНТИВІРУСНОГО ЗАХИСТУ

3.1. Розробка технічного завдання

В результаті проведеного аналізу було визначено технічне завдання на розробку програми.

Перелік використовуваних термінів

UML - уніфікована мова моделювання (Unified Modeling Language) - це система позначень, яку можна застосовувати для об'єктно-орієнтованого аналізу і проектування. Його можна використовувати для візуалізації, специфікації, конструювання та документування програмних систем.

Загальна інформація про проєкт:

1. Призначення технічного завдання: розробка антивірусної програми для захисту від простих вірусів.
2. Цільова аудиторія це будь-який користувач комп’ютера, який бажає захистити свій ПК.

Технології та сценарій реалізації системи:

1. Інсталяція: розпакування архіву.
2. Платформа: комп’ютер.
3. Підтримувані пристрої: додаток має працювати на Windows 7, 8, 8.1, 10.
4. Локалізація: англійська.

Функціональні вимоги:

Ситуація: Сканування на шкідливе ПО.

1. Користувач відкриває програму.
2. Програма після запуску демонструє головний екран додатку.
3. Користувач вибирає в програмі папку/файл/диск який імовірно пошкоджений вірусом.
4. Програма сканує вибраний користувачем файл/папку/диск.
5. Після сканування програма виводить результат у полі, у вигляді шляху до файлів з вірусами.
6. Програма пропонує дії з ураженими файлами (пропустити/очистити).

7а. Після вибору дії «пропустити», програма повертається на головний екран додатку.

7б. Після вибору дії «очистити», програма звітує про очищення (успішне/не успішне) та повертається на головний екран додатку.

Опис інтерфейсу

Форма виклику головного вікна антивірусу, в якій знаходиться кнопка “Start” яка виконує цю функцію.

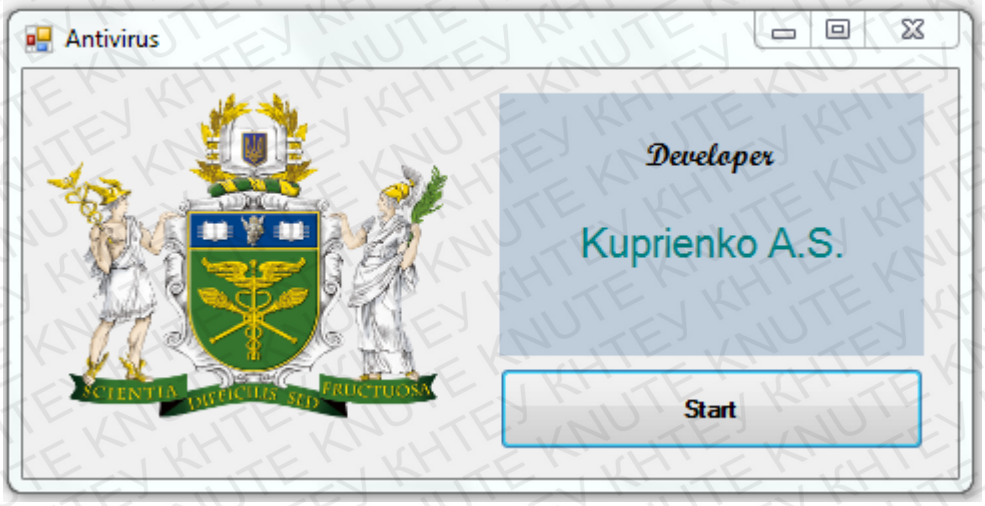

Рис. 3.1. Стартова форма

Основна форма із системною діагностикою має кнопки “Browse”, “Scan”, “Diagnostic” та “Hach-Check”.

Кнопка “Scan” не працює якщо попередньо не зазначено місце сканування за допомогою кнопки “Browse”.

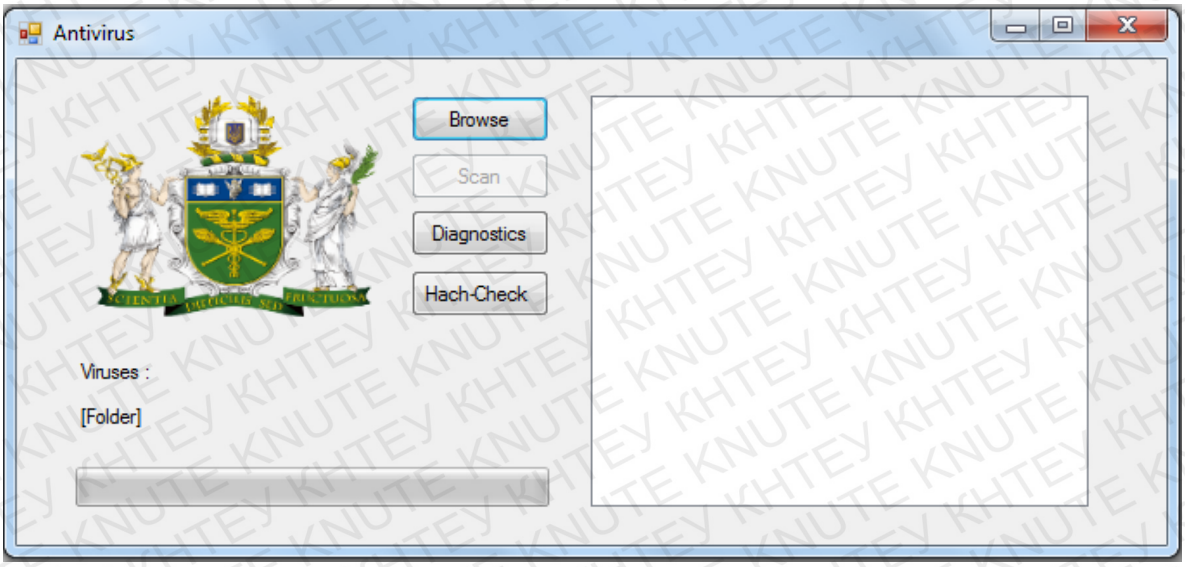

Рис. 3.2. Головна форма

Кнопка “Browse” викликає наступне вікно для вибору місця сканування:

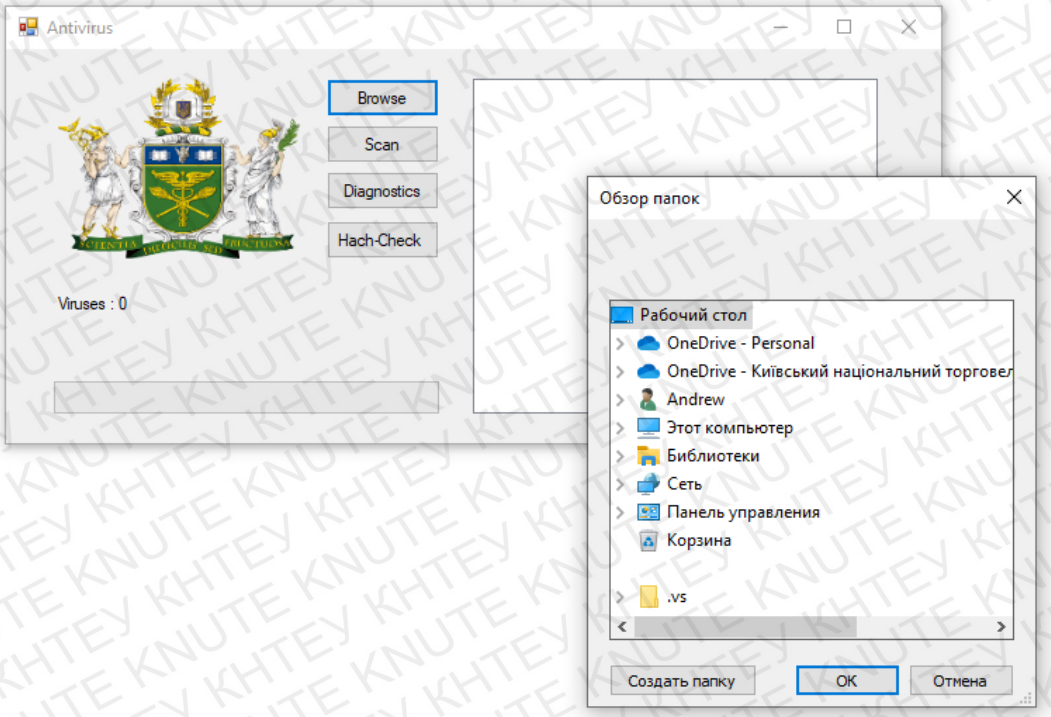

Рис. 3.3. Робота кнопки “Browse”

Після сканування на головному вікні программи відображаються проблемні файли та їх кількість.

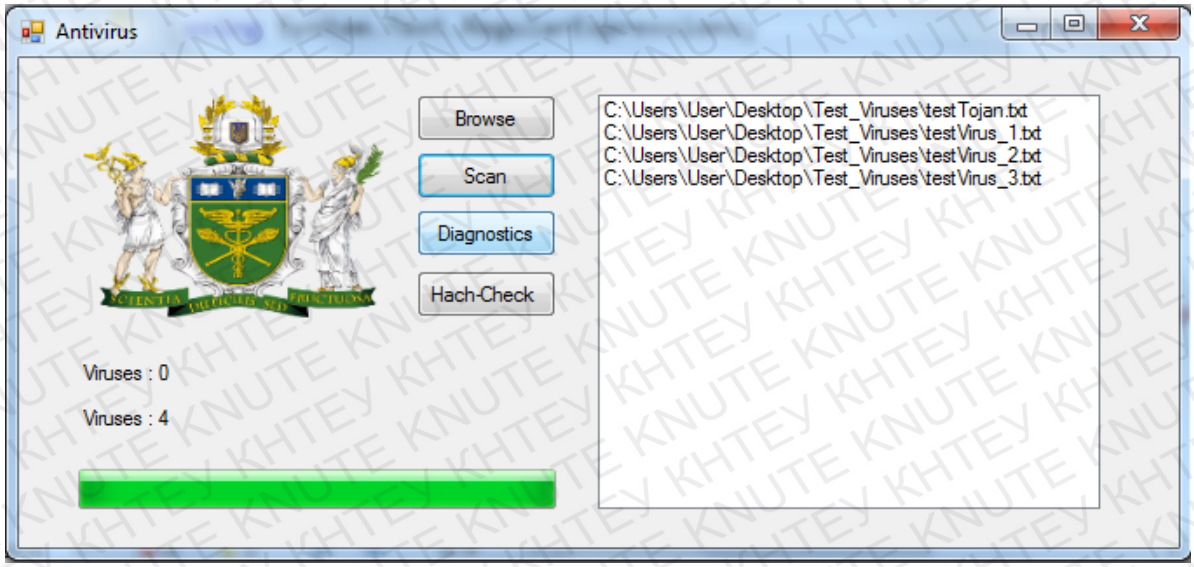

Рис. 3.4. Результат сканування

Кнопка “Diagnostic” демонструє вікно із загальними відомостями про роботу системи та програми.

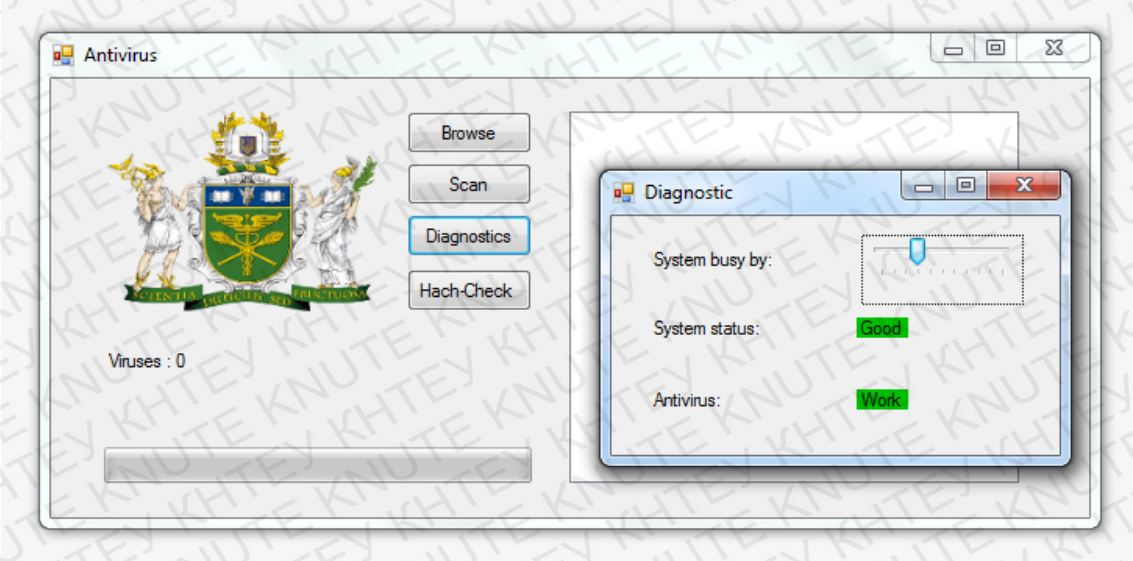

Рис. 3.5. Вікно діагностики

Додаткова форма для перевірки файлу хешем яка викликається кнопкою “Hach-Check”.

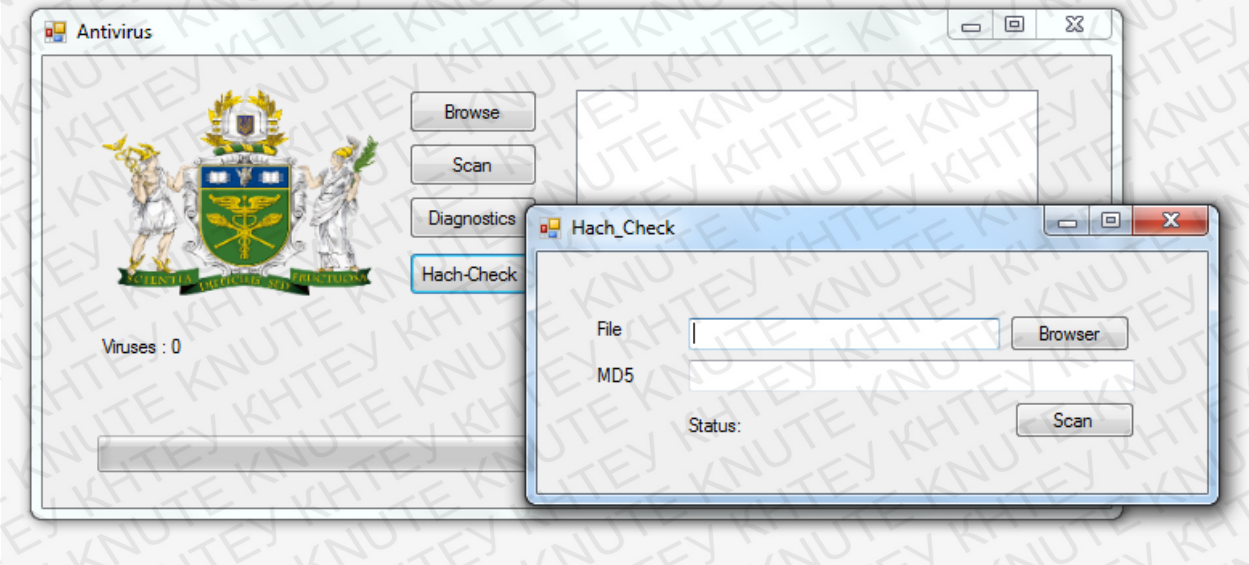

Рис. 3.6. Вікно “Hach-Check”

3.2 Визначення алгоритму створення програми

Принцип роботи додатку висвітлений в UML діаграмах вказаних нижче.

В use case діаграммі показано принцип роботи прогами у найпростішій формі. Так як це може розуміти користувач.

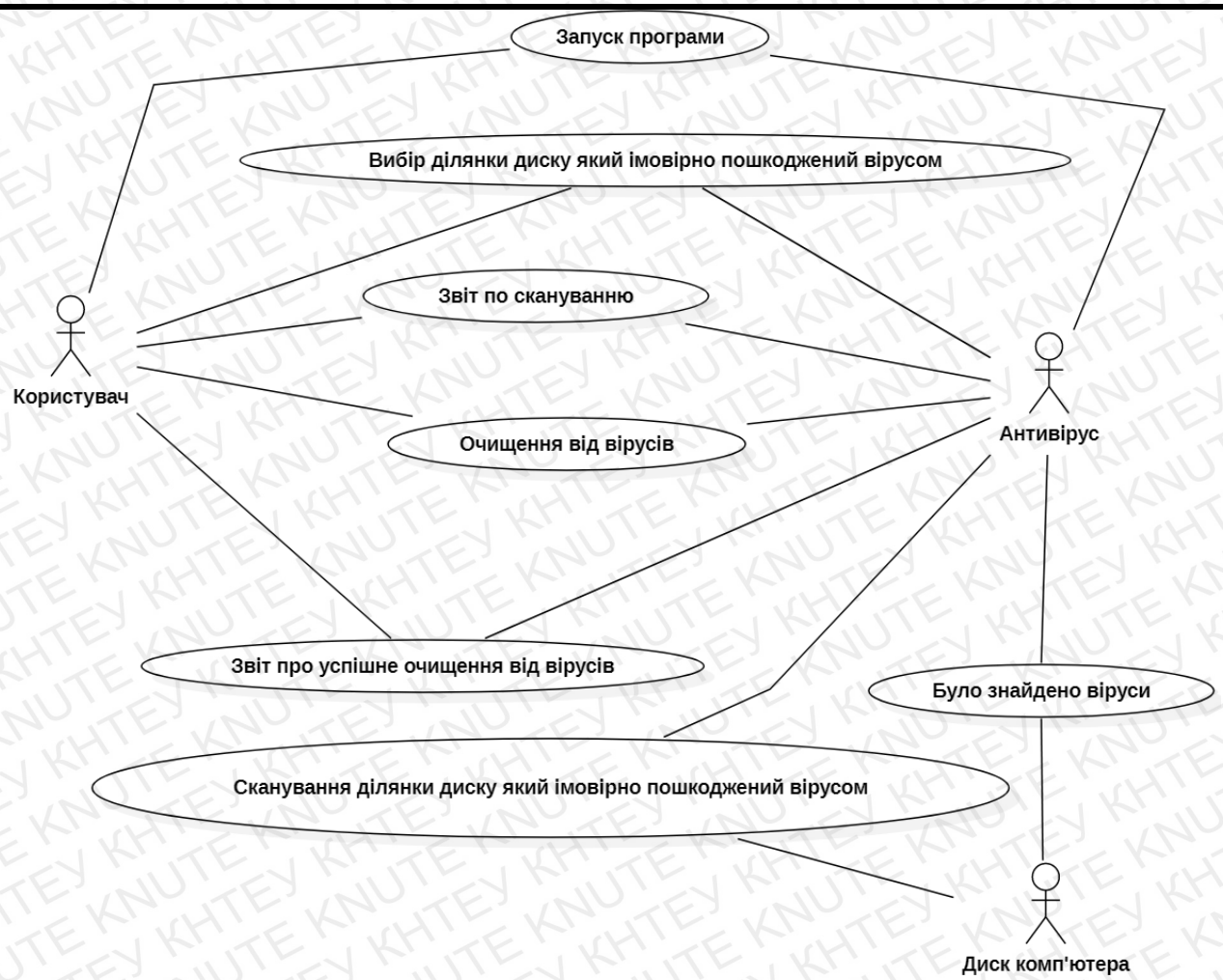

Рис. 3.7 Use case діаграма

В діаграммі діяльності робота антивірусу показана більш детально. Вже більше для розуміння розробника. Ця діаграма демонструє покрокові дії користування.

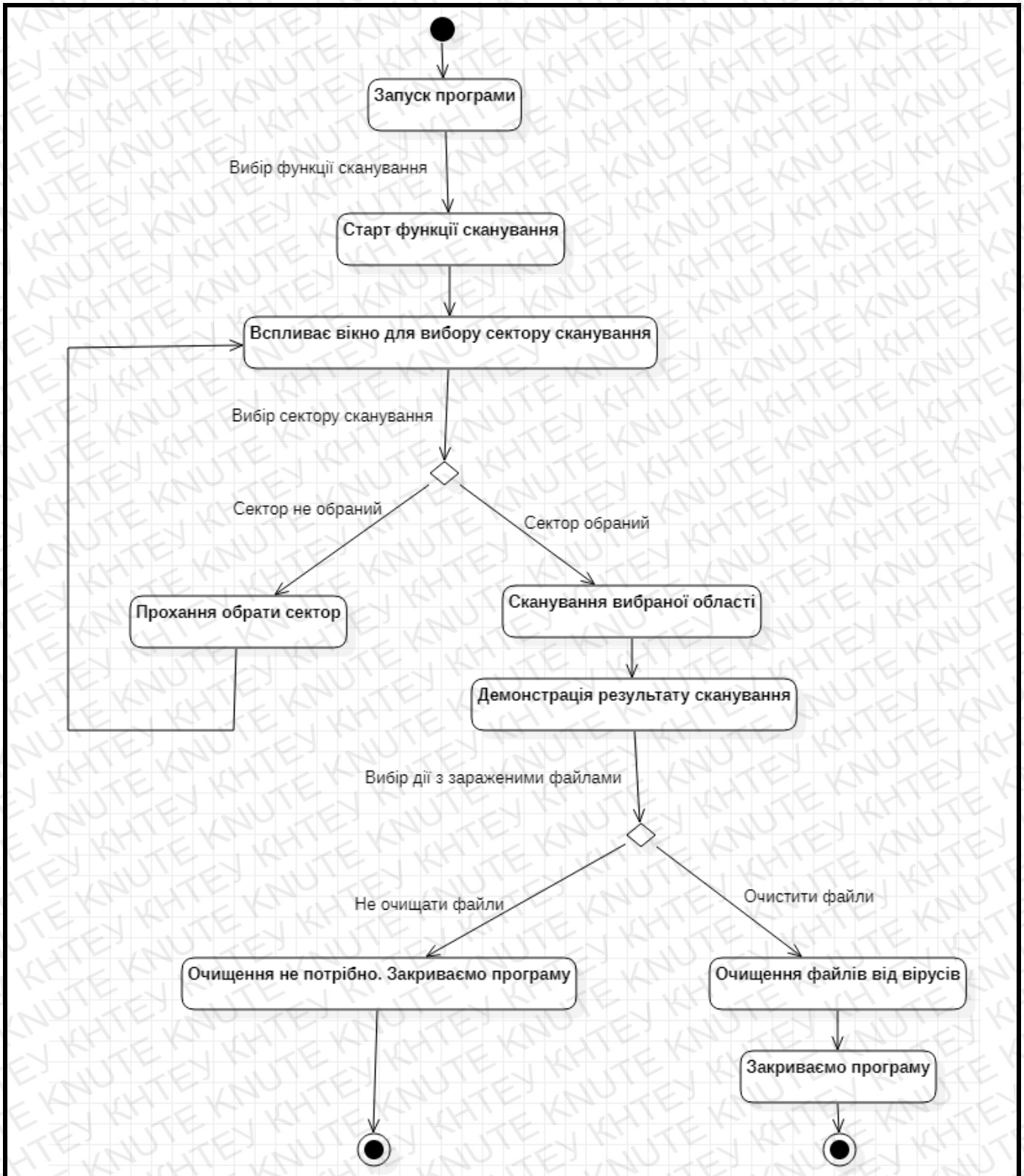

Рис. 3.8. Діаграма діяльності

В діаграммі станів показуються стани програми на кожному кроці роботи.

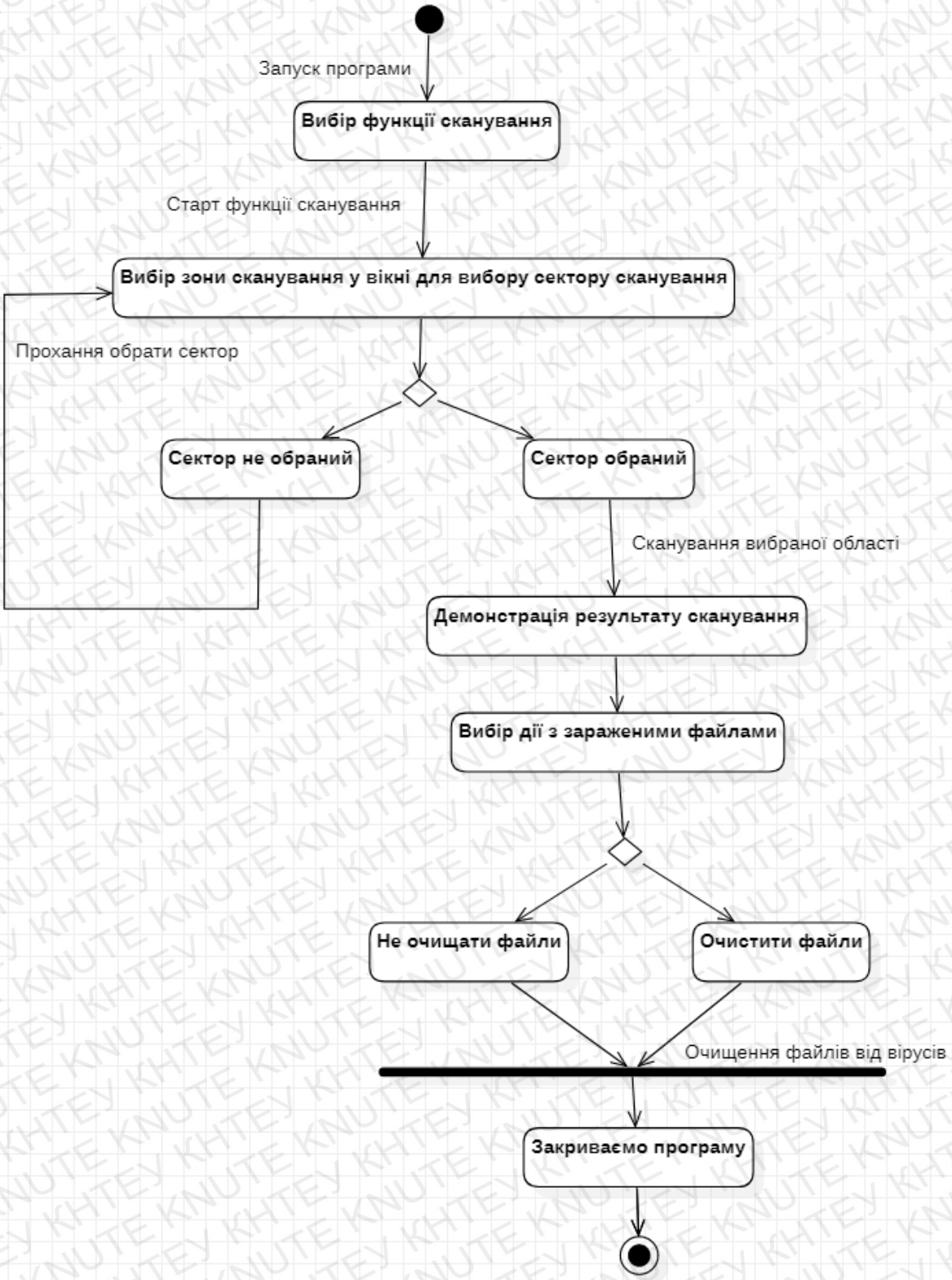

Рис. 3.9. Діаграма станів

Діаграма послідовностей демонструє детальний принцип роботи програми.

Рис. 3.10. Діаграма послідовностей

3.3 Створення програми та її апробація

Створення програми

Перед тим я писати сам код, ми розробили план, за яким буде працювати наша программа. Для цієї задачі ми використали UML діаграми створені в StarUML.

StarUML - програмний інструмент моделювання, який підтримує UML. StarUML підтримує одинадцять різних типів діаграм, прийнятих в нотації UML 2.0. Він активно підтримує підхід MDA (Model Driven Architecture), реалізуючи концепцію профілів UML. Середовище розробки StarUML чудово налаштовується відповідно до вимог користувача і має високий ступінь розширюваності, особливо в області своїх функціональних можливостей. Використання StarUML, одного з провідних програмних інструментів моделювання, гарантує досягнення максимальної продуктивності і якості ваших програмних проектів.

Далі, маючи сформований принцип роботи нашого антивірусу, переходимо до написання коду програми. Для цього чудово підійде Visual

Studio від компанії Microsoft.

Microsoft Visual Studio — серія продуктів фірми Майкрософт, які включають інтегроване середовище розробки програмного забезпечення та ряд інших інструментальних засобів. Ці продукти дозволяють розробляти як консольні програми, так і програми з графічним інтерфейсом, в тому числі з підтримкою технології Windows Forms, а також веб-сайти, веб-застосунки, веб-служби як в рідному, так і в керованому кодах для всіх платформ, що підтримуються Microsoft Windows, Windows Mobile, Windows Phone, Windows CE, .NET Framework, .NET Compact Framework та Microsoft Silverlight.

Microsoft Visual Studio має в собі увесь необхідний для проекту функціонал і навіть більше. Ця універсальна платформа дає можливість пацювати не тільки з C#, а і з багатьма іншими мовами програмування: Visual Basic .NET, Visual C++, Visual F# та багатьма іншими.

Мовою програмування, для створення гри була обрана C#, представлена в стандартному пакеті платформи Microsoft Visual Studio. Мова має строгу статичну типізацію, підтримує поліморфізм, перевантаження операторів, вказівники на функції-члени класів, атрибути, події, властивості, винятки.

Хід виконання роботи по розробці антивірусу висвітлено на рисунках в Додатку Б.

Апробація програми

Підготовка файлів вірусів: 3 віруси (скрипти у файлах) та 1 троян.

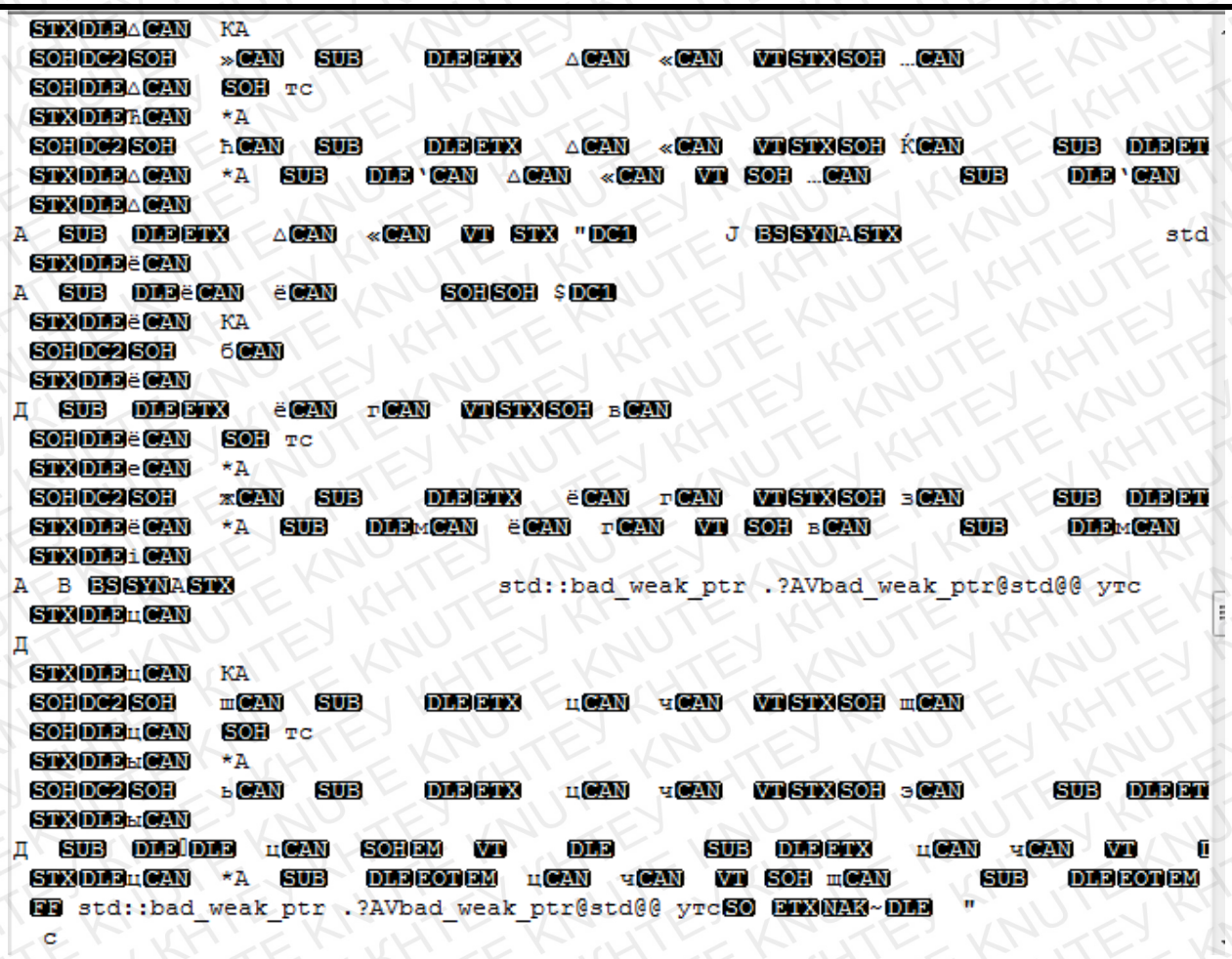

Рис. 3.11. Файл 1 пошкоджений вірусом

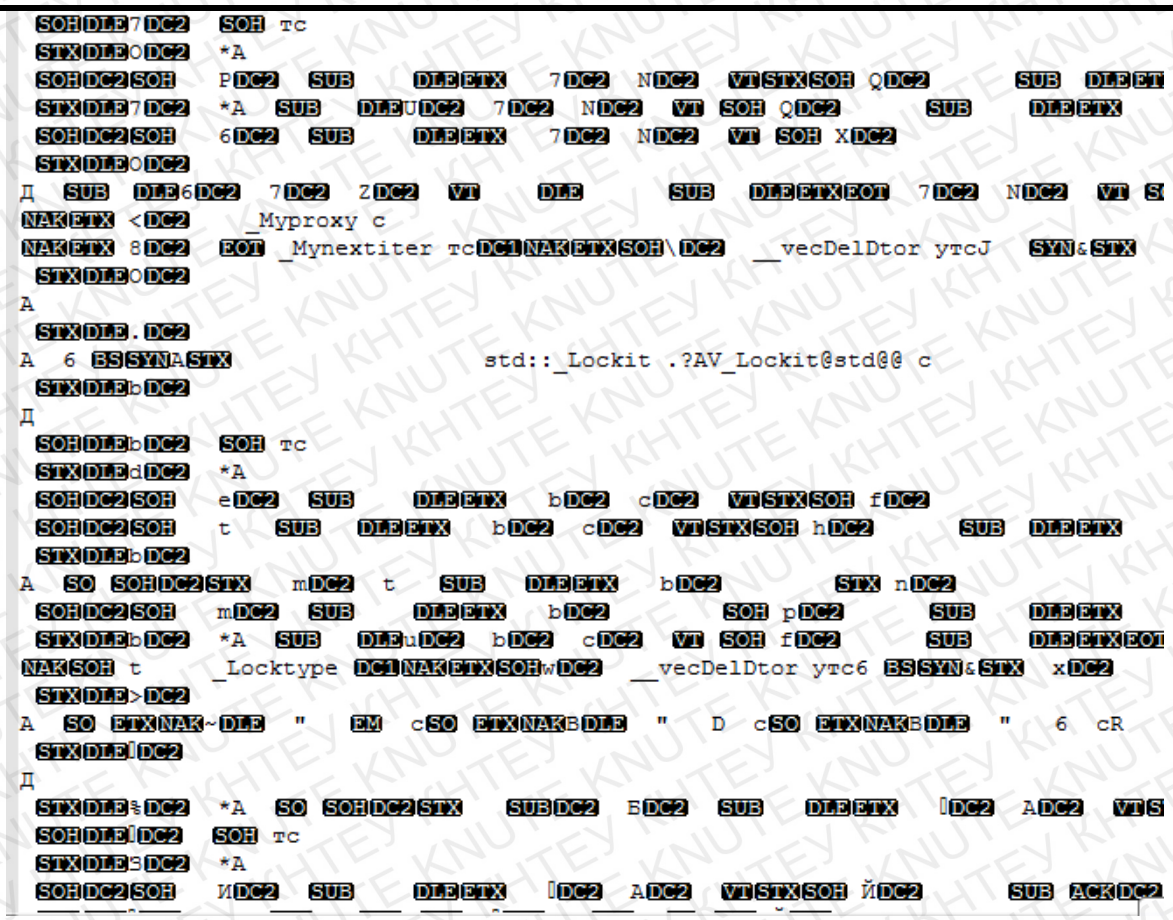

Рис. 3.12. Файл 2 пошкоджений вірусом

База даних хешу для перевірки хешу файлів (файл знаходиться в бібліотеках проектів).

```
73185e6fcb29f8ad13496be7499ca272
3ba6e302c6d872dc8bf71050e9f4c2f0
19b6e1839dae0a8243c5473cb9d6bf80
3ba70d4dcaf1817cac0feb0cb2cd26c0
42ba439f8b3fb128de98fd8a54afcc90
2d8413cfd8ed5e5a531bed229fabd8a0
53e2229ce9e603653f251f5c1e686da0
19ea92fa6a19e3816f378b740126aac0
47eb494feb0ba8b754ddc307b74b6ac0
3baa5dc9aaf6afc704d9da1469b15080
19f5637cb22acf0bafeafbe0c9113c80
2d8497ef9d319ce87d0433a6ef6442a0
54f90b9c90523e1edc0267731122a380
19b5b75e0f0d4cdf4f4e53d7bb88a150
47a924d66521ef6fc912a9320f24ab14
3bac2e87fad88c7d2db502b3ced8ee50
47d749a078eee4632c791c1023536c10
2d84a717f2363448e7c6a67a375d4060
55d4d92145a741c3a31c818dd8c8baa0
19d72e95151f4a9b36ab46f2910ee970
3bb0087cae30faaaa2839c2c86f5ab20
47fcf496edc0bdbac04f982be7955202
19bdcef9565023c8fade5660b5a42c20
47da90fa530bd702e1e9f78c862f4746
3bb4cea0a167f2b3506f189ff4bd2940
55e317b481a9c0b65154d480f0e7ce60
2d85d4acbf3472cc4cc427bedc2ab821
19e6b83eaed4e4f51f5690015272be40
425487f5b3d82e580b3ea3d716e07ec0
3bb933183b7e5472a6155fb65d1c8b80
550bcecfa7f0efedcb9eef0a962c8640
19f70a443aeb361f2d93347bbd45f000
2d85ef08de99173946509ace927504d0
```

Рис. 3.13. Хеш файли

Скануємо папку з 4 вірусами і отримуємо результат у вигляді їх виявлення програмою (Рис. 3.4).

Діагностуємо систему:

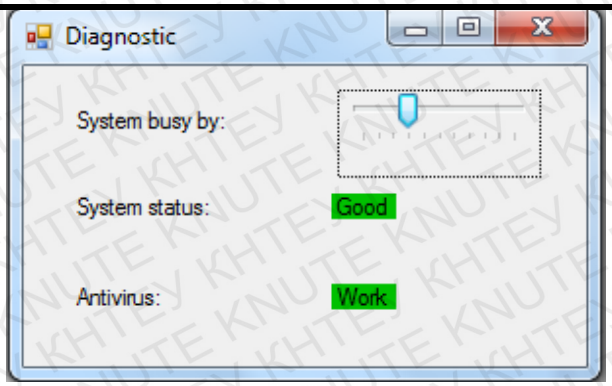

Рис. 3.14. Вікно діагностики

Як бачимо, навантаження системи невелике. Стан системи стабільний. Наш антивірус працює.

Перевіримо файл на наявність хешу

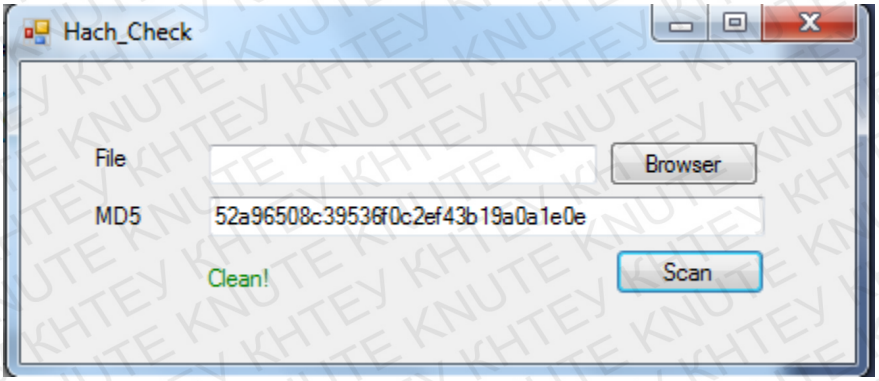

Рис. 3.15. Вікно “Hach-Check”

Це чисто!

3.4 Висновки до розділу 3

Було проведено огляд користувальницького інтерфейсу програми та тестування правильної роботи з тестовими вірусами. З чого можна сказати, що програма працює коректно і виконує всі передбачені для неї завдання!

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Комп’ютерний вірус - це спеціально написана невелика програма, яка може записувати свої копії в комп’ютерні програми, що містяться у виконуваних файлах, системних дисках, драйверах, документах тощо. Ці копії зберігають здатність "розмножуватися".

Якщо ви підозрюєте чи підозрюєте, що ваш комп’ютер заражений вірусом, ось декілька основних ознак зараження комп’ютером:

. Комп’ютер працює повільніше, ніж зазвичай.

. Комп’ютер перестає реагувати або продовжує збій.

. Комп’ютер виходить з ладу та перезавантажується кожні кілька хвилин.

. Комп’ютер перезапуститься мимовільно. Крім того, комп’ютер працює не так, як зазвичай.

. Додаткові компоненти, встановлені на вашому комп'ютері, не працюватимуть належним чином.

. Помилка визначення доступу до диска.

. Не вдалося правильно надрукувати документи.

. З’являються незвичні повідомлення про помилки.

. Меню та діалоги відображаються спотвореними.

. Нещодавно відкрите вкладення має подвійне розширення (JPG, VBS, GIF або EXE).

. З якоїсь причини антивірус вимкнено. Його також не можна перезапустити.

. Антивірусну програму неможливо встановити або запустити.

. На робочому столі з’являються нові піктограми, які там ніхто не

розміщував, або значки, які не стосуються останніх встановлених програм.

. Динаміки раптом відтворюють дивні звуки чи музику.

. Додатки мимоволі видаляються з комп’ютера.

Кожного разу, коли ви заражаєте свій комп’ютер вірусом (або якщо ви підозрюєте про це), важливо дотримуватися певних правил.

По-перше, не треба поспішати і приймати необачних рішень. Окрім втрати деяких даних, які можна відновити, необдумані дії можуть призвести до повторного зараження комп'ютера.

Однак заходи потрібно вжити негайно. Якщо ви абсолютно не впевнені, що розпізнали вірус до того, як він став активним на вашому комп’ютері, вам слід вимкнути комп’ютер, щоб не дати вірусу продовжувати руйнівні дії.

Будь-які дії щодо виявлення природи зараження та лікування комп’ютера повинні виконуватися лише в тому випадку, якщо комп’ютер належним чином запущений з дискового «довідкового» диска, що містить лише операційну систему. Використовуйте лише програми (виконувані файли), які зберігаються на захищених від запису носіях. Недотримання цього правила може мати серйозні наслідки, тому що якщо ви завантажите DOS або запустите програму на своєму комп’ютері із зараженого жорсткого диска, вірус може бути активований.

Лікування вірусу, як правило, є простим, але іноді (зі значним збитком від вірусу) це дуже важко. Якщо у вас недостатньо знань і досвіду для роботи з комп’ютером, зверніться за допомогою до досвідчених колег.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Курс користувачів ПК. Автори: Г. В. Саєнко та Т. Б. Волобуєва. 2016 рік.
2. Стажування з інформатики. Автори: В.Д. Дуденко; О.М. Макарчук; М.О. Патланжоглу.
3. Караванова Т. П. Розвиток креативності студентів у вивченні інформатики: авторська програма для поглиблення вивчення інформатики.-Чернівці: ОНМІПО, 2016.-44с.
4. Рудненко В. Д., Макарчук О. М., Патланжоглу М. О. Практичний курс з інформатики / За ред. Мадігон В.М. - К.: Фенікс, 2017. -304 с.
5. Глушаков С. В., Персональний комп'ютер. Навчальний курс.-Харків: Фомо; М .: ТОВ Компанія «Видавничий дім Аст», 2018.-499с.
6. Генеральна асамблея Гордієнка Україна приєднується до Світової інформаційної системи. // Нові настанови. - 2018 - №5 - С. 64-67.
7. Демінський SO гроші в Інтернеті. // Політика і культура. - 2019. - (5 (88) / 13-19. лютого. - С. 34-36.
8. Docker.io. Docker [Електронний ресурс] / Docker.io – https://www.docker.com/
9. Daemon [Електронний ресурс] / Wikipedia - https://uk.wikipedia.org/wiki/Daemon_(computing)
10. Kubernetes.io. Kubernetes [Електронний ресурс] / Kubernetes.io - https://kubernetes.io
11. Molyneaux I. The Art of Application Performance Testing / Ian Molyneaux .. - 209 с. - (O'Reilly Media).
12. Software Performance [Електронний ресурс] / Wikipedia - https://en.wikipedia.org/wiki/Software_performance_testing

13. Automated Verification of Load Tests Using Control Charts / THD Nguyen, A. Bram, J. Zhen Ming, H. Ahmed E. // Asia-Pacific Software Engineering Conference. - 2011. - С. 282-289.

14. The httperf HTTP load generator [Електронний ресурс] - https://github.com/httperf/httperf

15. Rational Performance Tester [Електронний ресурс] - https://en.wikipedia.org/wiki/Rational_Performance_Tester.

16. Інформація про UML
https://uk.wikipedia.org/wiki/Unified_Modeling_Language

17. Інформація про StarUML
https://usermanual.wiki/Document/userguide.1128996068/html

18. Інформація про Microsoft Visual Studio
https://uk.wikipedia.org/wiki/Microsoft_Visual_Studio

19. Інформація про мову програмування C#
https://uk.wikipedia.org/wiki/C_Sharp

ДОДАТКИ

Додаток А

Лістинг програми

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.IO;
using System.Text.RegularExpressions;

namespace Antivirus_V2
{
   public partial class Form1 : Form
   {
      int viruses;
      string[] virusList = new string[] { "virus", "tojan", "hack", "hacker" };
      public Form1()
      {
         InitializeComponent();
      }

      private void button1_Click(object sender, EventArgs e)
      {
         folderBrowserDialog1.ShowDialog();
         label2.Text = folderBrowserDialog1.SelectedPath;
         viruses = 0;
         label1.Text = "Viruses : " + viruses.ToString();
         progressBar1.Value = 0;
         listBox1.ClearSelected();
         button2.Enabled = true;
      }

      private void button2_Click(object sender, EventArgs e)
      {
         List<string> search =   Directory.GetFiles(@folderBrowserDialog1.SelectedPath,"*.*").ToList();
         progressBar1.Maximum = search.Count;
         foreach(string item in search)
         {
            try
            {
               StreamReader stream = new StreamReader(item);
               string read = stream.ReadToEnd();
               foreach (string st in  virusList)
               {
                  if(Regex.IsMatch(read,st))
```

```
                {
                    viruses += 1;
                    label2.Text = "Viruses : " + viruses;
                    listBox1.Items.Add(item);
                }
                progressBar1.Increment(1);
            }
        }
        catch(Exception ex)
        {
            //
        }
    }
}

    private void button3_Click(object sender, EventArgs e)
    {
        Hach_Check form = new Hach_Check();
        form.Show();

    }

    private void Form1_Load(object sender, EventArgs e)
    {

    }

    private void Form1_FormClosing(object sender, FormClosingEventArgs e)
    {
        Application.Exit();
    }

    private void button4_Click(object sender, EventArgs e)
    {
        Diagnostic form = new Diagnostic();
        form.Show();
    }
  }
}


        using System;
        using System.Collections.Generic;
        using System.ComponentModel;
        using System.Data;
        using System.Drawing;
        using System.Linq;
        using System.Text;
        using System.Windows.Forms;
        using System.Security.Cryptography;

        static string GetHashString(string s)
        {
            byte[] bytes = Encoding.Unicode.GetBytes(s);
```

```
        MD5CryptoServiceProvider CSP = new MD5CryptoServiceProvider();

        byte[] byteHash = CSP.ComputeHash(bytes);

        string hash = string.Empty;
        foreach (byte b in byteHash)
        { hash += string.Format("{0:x2}", b); }

        return hash;
       }

public aftorizacia()
       {
         InitializeComponent();
       }

       public void find_lp_for_text(string login, string password)
       {
        if (find_lp(login, password) == true)
        {
          label3.ForeColor = Color.Green;
          label3.Text = "Нажмите кнопку <<Авторизоваться>>";
          pictureBox1.ImageLocation = GlobalCorrectClass.path_image;//
          button1.Enabled = true;
          button2.Enabled = false;

        }
        else//если не существует
        {
         label3.ForeColor = Color.Red;
         label3.Text = "гическая переменная”
        }
       }

       public static bool find_lp(string login, string password)
       {
         var query_student = from student in ClassHotEnt.ht.students
                             select student;

         bool b_lp = false;

         foreach (var strd in query_student)
         {

           if (strd.login_student == GetHashString(login)/
              && strd.password_student == GetHashString(password))/
           {
              b_lp = true;
              GlobalCorrectClass.path_image = strd.foto_student;/       }
         }
         return b_lp;//возврат
       }

       private void button1_Click(object sender, EventArgs e)
       {
```

```
            if (label3.ForeColor == Color.Green)
            {

              GlobalCorrectClass.login = GetHashString(LoginTextBox.Text);
                    GlobalCorrectClass.password = GetHashString(PasswordTextBox.Text)


            aftorizacia.ActiveForm.Close();
            }
            else
            {
               MessageBox.Show("Вы не" + /
        !");
            }
          }

          private void button2_Click(object sender, EventArgs e)
          {
            anketa anket = new anketa();
            anket.Show();/

          }

          private void aftorizacia_Load(object sender, EventArgs e)
          {
            /
            label3.ForeColor = Color.DarkBlue;
            label3.Text = "!";

          }

          private void LoginTextBox_TextChanged(object sender, EventArgs e)
          {
            find_lp_for_text(LoginTextBox.Text, PasswordTextBox.Text);
          }

          private void PasswordTextBox_TextChanged(object sender, EventArgs e)
          {

            find_lp_for_text(LoginTextBox.Text, PasswordTextBox.Text);
          }

using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.IO;
using System.Linq;
using System.Security.Cryptography;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
```

```
namespace Antivirus_V2
{
    public partial class Hach_Check : Form
    {
        public Hach_Check()
        {
            InitializeComponent();
        }
        public string GetMD5FromFile(string filenPath)
        {
            using (var md5 = MD5.Create())
            {
                using (var stream = File.OpenRead(filenPath))
                {
                    return BitConverter.ToString(md5.ComputeHash(stream)).Replace("-", string.Empty).ToLower();
                }
            }
        }

        private void button2_Click(object sender, EventArgs e)
        {
            OpenFileDialog ofd = new OpenFileDialog();
            ofd.Filter = "Textfiles | *.txt";
            if (ofd.ShowDialog() == DialogResult.OK)
            {
                tbMD5.Text = GetMD5FromFile(ofd.FileName);
            }
        }

        private void button1_Click(object sender, EventArgs e)
        {
            try
            {
                var md5signatures = File.ReadAllLines("MD5base.txt");

                if (md5signatures.Contains(tbMD5.Text))
                {
                    lblStatus.Text = "Infected!";
                    lblStatus.ForeColor = Color.Red;
                }

                else
                {
                    lblStatus.Text = "Clean!";
                    lblStatus.ForeColor = Color.Green;
                }
            }
            catch
            {
                lblStatus.Text = "Error Program";
                lblStatus.ForeColor = Color.Red;
            }
        }
    }
}
```

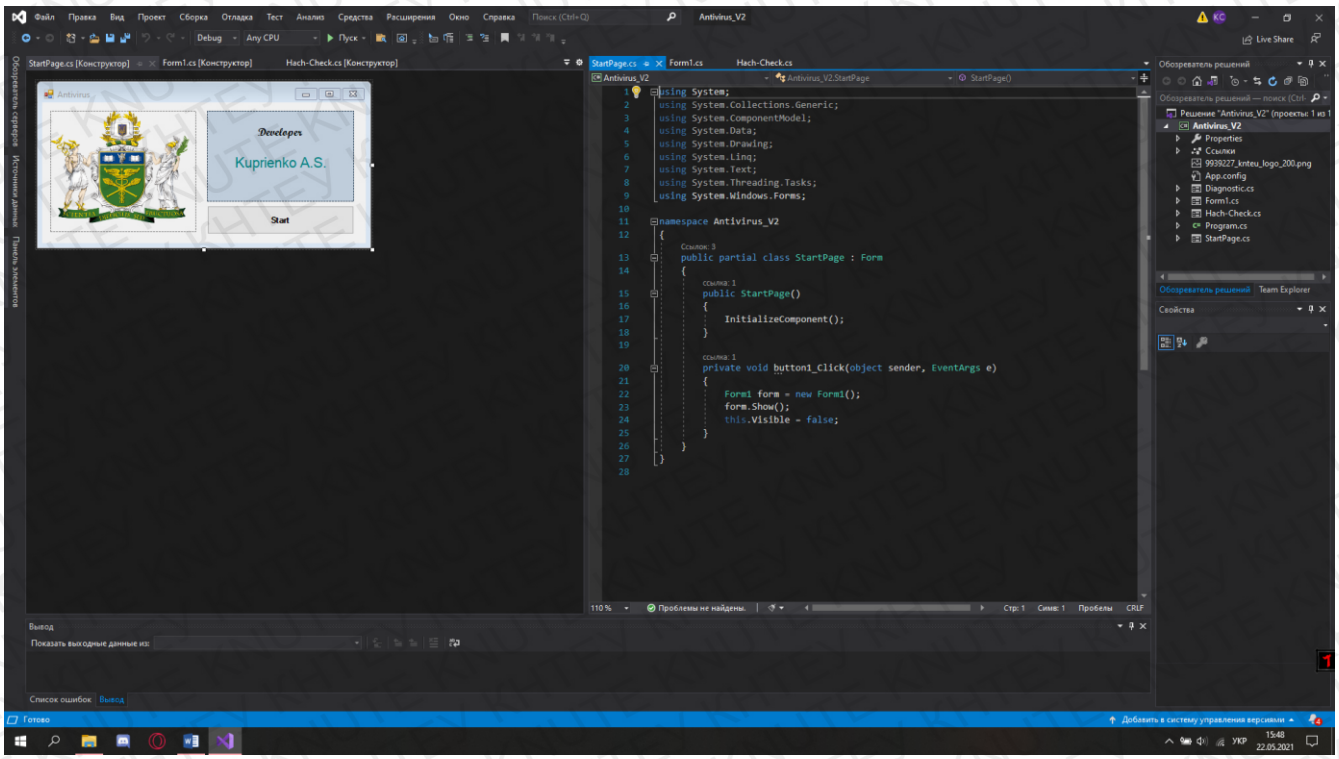

Рис. Б1. Стартове вікно

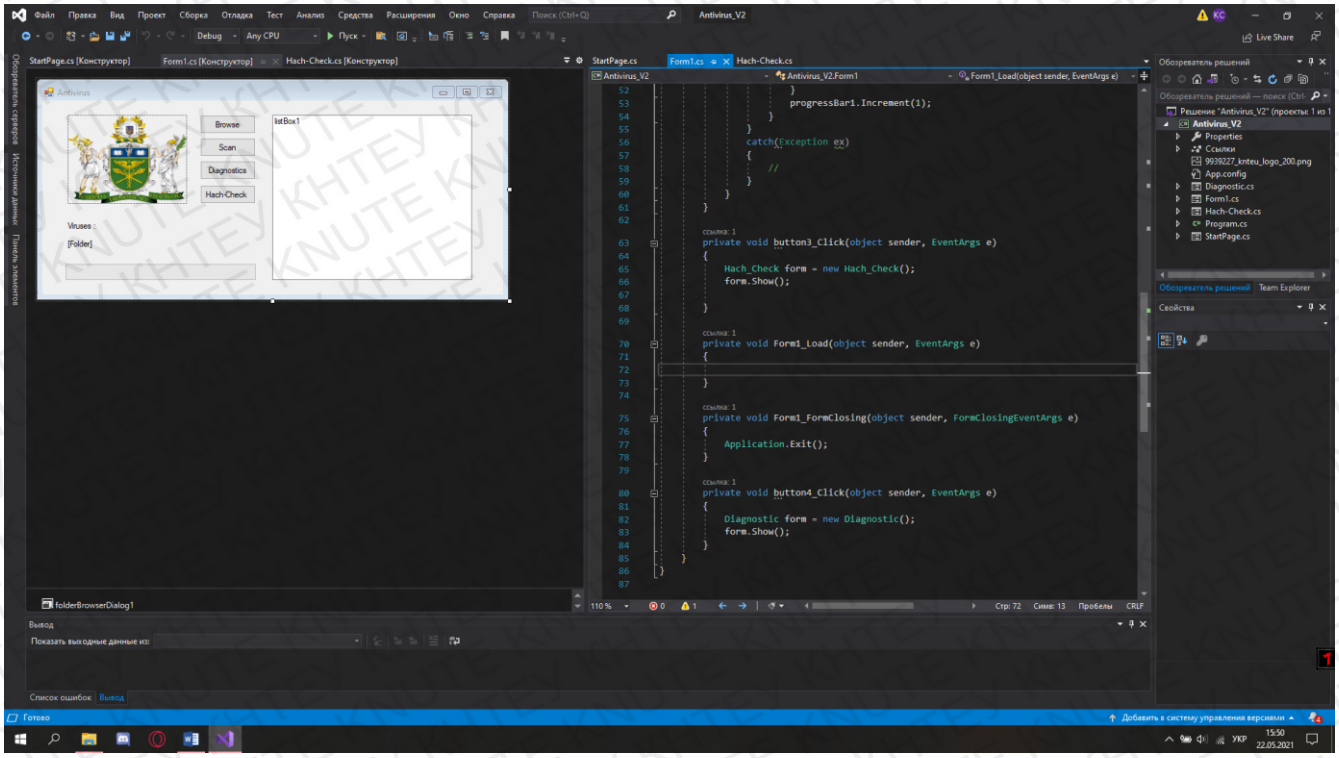

Рис. Б2. Головне вікно

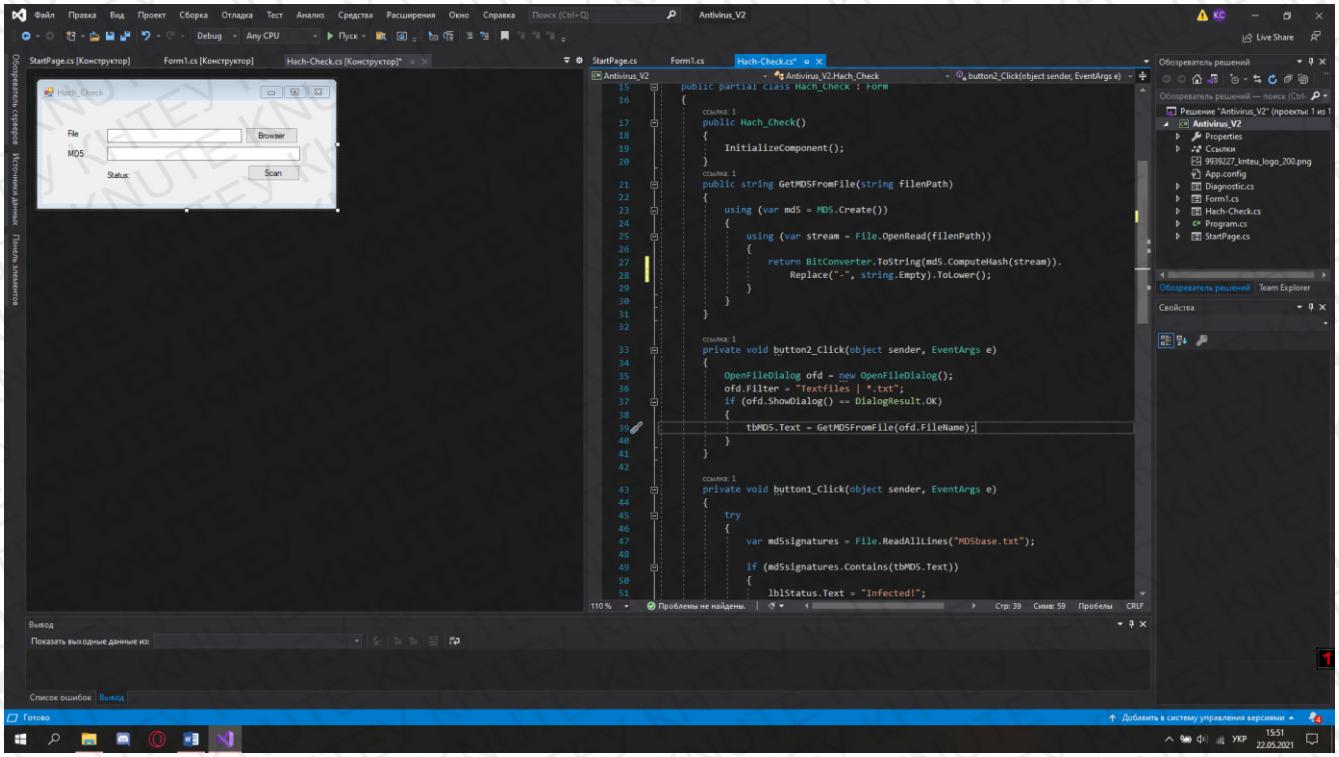

Рис. Б3. Вікно Hech-Check

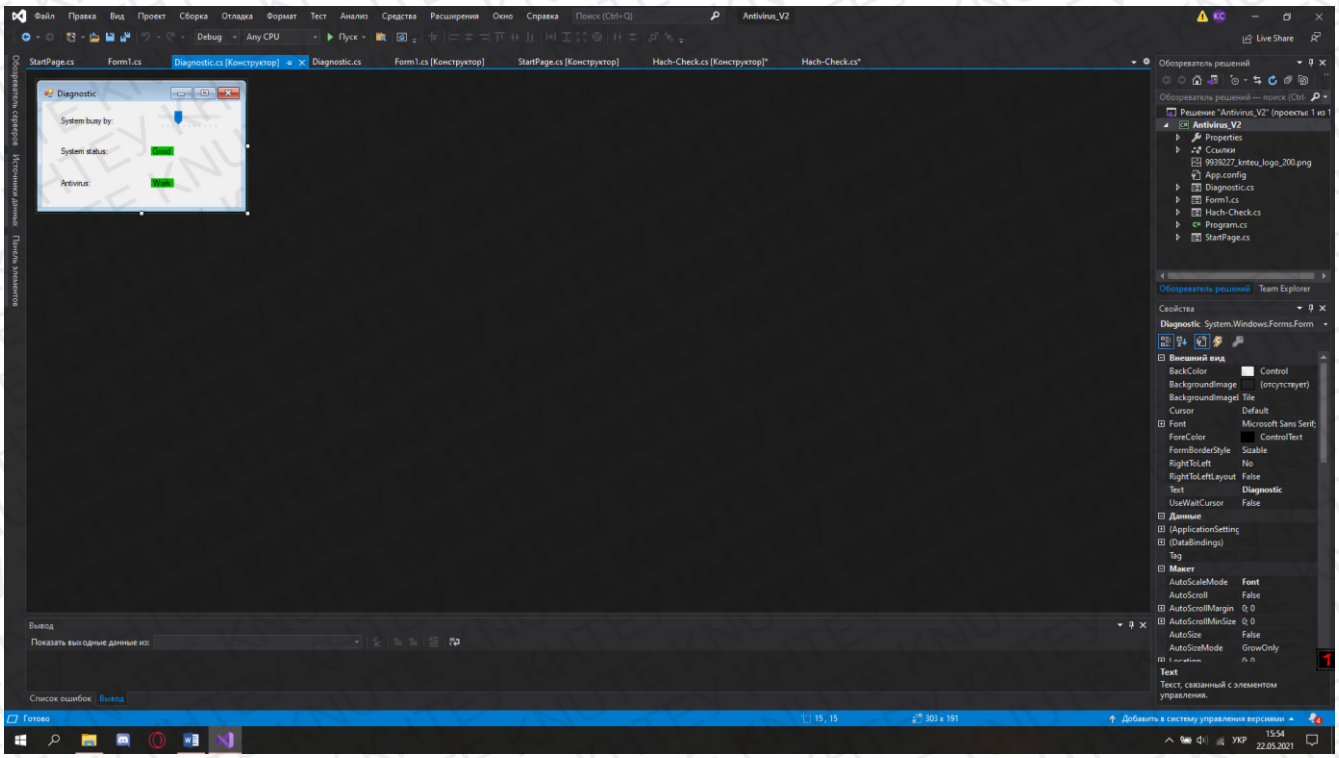

Рис. В4. Вікно діагностики