МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних наук,
управління та адміністрування
Кафедра інформаційних технологій

Бакалаврська кваліфікаційна робота

на тему: Розробка системи для пошуку віддаленого шкідливого програмного забезпечення

Виконав студент 4 курсу групи К-25
Спеціальність 122 комп'ютерні науки
Перетятко Дмитро Олександрович

Керівник асистент
Бучинська Ірина Вікторівна

Консультант к.геогр.н., доцент
Коваленко Людмила Борисівна

Рецензент к.т.н., доцент
Гнатовська Ганна Арнольдівна

Одеса 2020

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ПНП – потенційно небезпечні програми;

ADINF – Adinf Cure Module;

AVP − AntiVirus Program;

BBS − Bulletin Board System;

IRC − Internet Relay Chat**;**

TSR − Terminate and Stay Resident.

ВСТУП

У сучасному світі актуальним постає питання про боротьбу з комп'ютерними вірусами.

Кожен з нас хоч раз стикався з такою ситуацією, яка заважала нормальній роботі комп’ютера, як вірус. Після появи перших ПК і тоді ще не розвинутого Інтернету були віруси, які передавалися при обміні інформацією. В той час віруси розповсюджувалися на всі носії інформації, знищували тисячі файлів і програм причому їх ніяк не можна було висліджувати та видалити. Антивірусні програми тоді ще були простими та не могли повністю знищувати комп’ютерні віруси. Розробкою антивірусів займаються великі компанії. З розвитком інформаційних технологій антивірусні програми покращувалися та могли відстежувати та знищувати більшість вірусів та запобігаючи їх розмноженню зберігаючи працездатність ПК.

Сучасні ж антивірусні програми можуть відстежувати та знищувати десяток тисяч вірусів за короткий відрізок часу. Сьогодні з розвиненим Інтернетом, заразити свій комп’ютер стало набагато легше. Його можна підхопити будь-де, у веб-сторінці, в електронних листах,через які він передається в систему. Вірус передається в завантажених через Інтернет програмах в які його вбудовують, причому він активується після того як буде встановлена та чи інша програма яка була завантажена через Інтернет. Вірус заражає файли , копіюється в них, тим самим розповсюджується по всій системі.

Метою роботи є розроблення консольного додатку в середовищі програмування C++ для виявлення злоякісного коду та його знешкодження.

Для поставленої меті необхідно вирішити наступні завдання:

- вивчити наукову літературу і технічну документацію з обраної теми;
- провести аналіз функціонування, як вірусів, так і антивірусів;
- розробити програму по виявленню «небезпечних» ділянок коду і їх знешкодження.

Кваліфікаційна робота містить вступ, 4 глави, висновки, 11 рисунків, 3 таблиці , 19 посилань.

1 АНАЛІЗ ОСНОВНИХ КОМП’ЮТЕРНИХ ВІРУСІВ

Комп’ютерний вірус – це злоякісне програмне забезпечення, яке копіює себе до файлів, в програмні коди, області пам’яті та розповсюджується по всій системі. Його основною задачею є розповсюдження. Це поширення супроводжується видаленням операційної системи та блокуванням нормальної роботи користувача. Навіть автор вірусу, який не запрограмував його на шкідливі ефекти , все одно буде порушувати роботу, приводити до збоїв та непередбачуваної взаємодії із системними даними Також віруси можуть займати місце на носіях інформації та використовувати ресурси комп'ютера. Вірус був названий по аналогії з біологічним вірусом за схожу дію розповсюдження [1][1)].

"Розмноження" нічим не відрізняється від копіювання програмою файлу з однієї директорії в іншу. Відмінність лише в тому, що ці дії проводяться без відома користувача, тобто на екрані нічого не з'являється навіть повідомлень. У всьому іншому він − звичайнісінька програма, яка використовує ті чи інші команди комп'ютера. Причому його дублікати не збігаються з оригіналом. Комп'ютерні віруси – одні з підвидів великого класу програм, званих шкідливими кодами [2][2)].

1.1 Історія появи вірусів

Ідея комп'ютерних вірусів виникла задовго до появи персональних комп'ютерів. В1959 році американський вчений Л. С. Пенроуз опублікував в журналі "Scientific American" статтю, присвячену само відтворюваним механічним структурам. У цій статті була описана найпростіша модель

[1)] [1] Лабораторія Касперського. URL: http://securelist.ru/ (Дата звернення 30.04.2020)

[2)] [2] Михайлов А.В. Комп'ютерні віруси і боротьба з ними. М.: ДіалогМІФІ, 2011. 104 с. ISBN 978-5-86404-236-6.

двомірних структур, здатних до активації, розмноження, мутацій, захоплення. Незабаром дослідник з США Ф. Г. Сталь реалізував цю модель за допомогою машинного коду на IBM 650.

В ті часи комп'ютери були величезними, складними в експлуатації та надзвичайно дорогими машинами, тому їх власниками могли стати лише великі компанії або урядові обчислювальні та науково-дослідні центри. Але ось 20 квітня 1977 року з конвеєра сходить перший "народний" персональний комп'ютер Apple II. Ціна, надійність, простота і зручність в роботі визначили його широке поширення в світі. Загальний обсяг продажів комп'ютерів цієї серії склав понад три мільйонів штук (без урахування його численних копій, таких, як Правец 8М / С, Агат і ін.), що на порядок перевищувала кількість всіх інших ЕОМ, що були в той час. Тим самим доступ до комп'ютерів отримали мільйони людей самих різних професій, соціальних верств і менталітету. Саме тоді з'явилися перші прототипи сучасних комп'ютерних вірусів, адже були виконані дві найважливіші умови їх розвитку − розширення "життєвого простору" і поява засобів поширення.

Надалі умови ставали все більш і більш сприятливими для вірусів. Асортимент доступних пересічному користувачеві персональних комп'ютерів розширювався, крім гнучких 5-дюймових магнітних дисків з'явилися жорсткі, бурхливо розвивалися локальні мережі, а також технології передачі інформації за допомогою звичайних комутованих телефонних ліній. Виникли перші мережеві банки даних BBS (Bulletin Board System), або "дошки оголошень", значно полегшували обмін програмами між користувачами. Пізніше багато хто з них переросли у великі онлайнові довідкові системи (CompuServe, AOL і ін.). Все це сприяло виконання третьої найважливішої умови розвитку і поширення вірусів − стали з'являтися окремі особистості та групи людей, що займаються їх створенням. Хто пише вірусні програми і навіщо? Це питання (з проханням вказати адресу і номер телефону) особливо

хвилює тих, хто вже піддався вірусній атаці і втратив результати багаторічної копіткої роботи. Сьогодні портрет середньостатистичного автора віруса виглядає так: чоловік, 23 роки, співробітник банку або фінансової організації, що відповідає за інформаційну безпеку або мережеве адміністрування. Однак за даними, його вік трохи нижче (14-20 років), він вчиться або не має заняття взагалі. Головне, що об'єднує всіх творців вірусів – це бажання виділитися і проявити себе, нехай навіть на Геростратовому терені. 90-ті роки, які ознаменувалися розквітом глобальної мережі Інтернет, виявилися найбільш благодатним часом для комп'ютерних вірусів. Сотні мільйонів людей по всьому світу волею-неволею стали "користувачами", а комп'ютерна грамотність стала майже так само необхідна, як уміння читати і писати. Якщо раніше комп'ютерні віруси розвивалися в основному екстенсивно (тобто росло їх число, але не якісні характеристики), то сьогодні завдяки вдосконаленню технологій передачі даних можна говорити про зворотне. На зміну "примітивним предкам" приходять все більше "розумні" і "хитрі" віруси, набагато краще пристосовані до нових умов проживання. Сьогодні вірусні програми вже не обмежуються псуванням файлів, завантажувальних секторів або програванням нешкідливих мелодій. Деякі з них здатні знищувати дані на мікросхемах материнських плат. При цьому технології маскування, шифрування і поширення вірусів часом дивують навіть самих бувалих фахівців.

1.2 Опис типів комп’ютерних вірусів

Залежно від місця існування розрізняють файлові віруси, завантажувальні та макровірус [3][1)]. Спочатку найпоширенішою формою комп'ютерної "зарази" були файлові віруси, що "мешкають" у теках

[1)] [3] Шаньгина В.Ф. Інформаційна безпека комп'ютерних систем і мереж: Навчальний посібник. М.: ИД ФОРУМ: ИНФРА-М, 2012. 416 с. ISBN 9785-8199-0331-5 1000.

операційної системи комп'ютера. До них відносяться, "overwriting" − вірус (від англ. "записувати поверх"). Потрапляючи в комп'ютер, вони записують свій код замість коду файлу, що заражається, знищуючи його вміст. І тому він перестає працювати та не відновлюється. Це досить примітивні віруси: вони дуже швидко себе виявляють і не можуть стати причиною епідемії. Інший тип "файлових шкідників" − так звані паразитичні віруси. Вони залишають заражені дані повністю або частково працездатними, але змінюють їх вміст, можуть копіювати себе в початок, кінець або середину . Так, "cavitys-віруси (від англ. "порожнина") записують свій код у свідомо невживані дані.

Ще "хитріше" поводяться "companion віруси (від англ. "приятель", "компаньйон")[4][1]. Вони не змінюють сам файл, але створюють для нього file-двійник, що при запуску зараженого файлу управління отримує саме цей двійник, тобто вірус. Companion-віруси, що працюють під DOS, використовують особливість цієї операційної системи яка буде виконувати файли з розширенням COM, а потім вже з розширенням EXE. Такі віруси створюють для EXE-файлів двійники, що мають те ж саме ім'я, але з розширенням COM. Вірус записується в Сом-файл і ніяк не змінює оригінал. При запуску зараженого файлу DOS першим виявить і виконає саме Сом-файл, тобто вірус, а вже потім вірус запустить файл з розширенням EXE. Іноді companion-віруси просто перейменовують його, що заражається, а під старим ім'ям записують на диск свій власний код. XCOPY.EXE перейменовується в XCOPY.EXD, а вірус записується під ім'ям XCOPY. Подібного типу віруси були виявлені у багатьох операційних системах − не лише в DOS, але і в Windows і OS/2. Є інші способи створювати файли-двійники. Віруси типу "path-companion" грають на особливостях DOS PATH

[1]) [4] Климентьєв К. Е. Комп'ютерні віруси і антивіруси. Погляд програміста. М.: ДМК-Пресс, 2013. 656 с. ISBN: 978-5-94074-885-4.

− ієрархічному записі місця розташування файлу в системі DOS. Вірус копіює свій код під ім'ям файлу, що заражається, але поміщає його не в ту ж директорію, а на один рівень вище. В цьому випадку DOS першим виявить і запустить саме файл-вірус. Принцип дії завантажувальних вірусів обґрунтований на алгоритмах запуску операційної системи. Ці віруси заражають завантажувальний сектор (boot-сектор) дискети або вінчестера − спеціальну область на диску, що містить програму початкового завантаження комп'ютера. Якщо змінити вміст завантажувального сектора, то ви навіть не зможете запустити ваш комп'ютер.

Макровіруси − різновид комп'ютерних вірусів, створених за допомогою макромов, вбудованих в популярні офісні застосування на кшталт Word, Excel, Access, PowerPoint, Project, Corel Draw та ін. Макромови використовуються для написання спеціальних програм (макросів), що дозволяють підвищити ефективності роботи офісних застосувань[5][1)]. Наприклад, в Word можна створити макрос, що автоматизує процес заповнення і розсилки факсів. Тоді користувачеві досить буде ввести дані в поля форми і натиснути на кнопку − усе інше макрос зробить сам. Біда в тому, що, окрім корисних, в комп'ютер можуть потрапити і шкідливі макроси, що мають здатність створювати свої копії і здійснювати деякі дії без відома користувача, наприклад змінювати зміст документів, стирати файли або директорії [6][2)]. Приклад макровірусу зображений на рис.1.

[1)] [5] Інформаційні технології. URL: http://habrahabr.ru/ (Дата звернення 02.05.2020)

[2)] [6] Цирль В.Л. Основи інформаційної безпеки. Короткий курс. М.: Фенікс, 2008. 256 с. ISBN 978-5-222-13164-0.

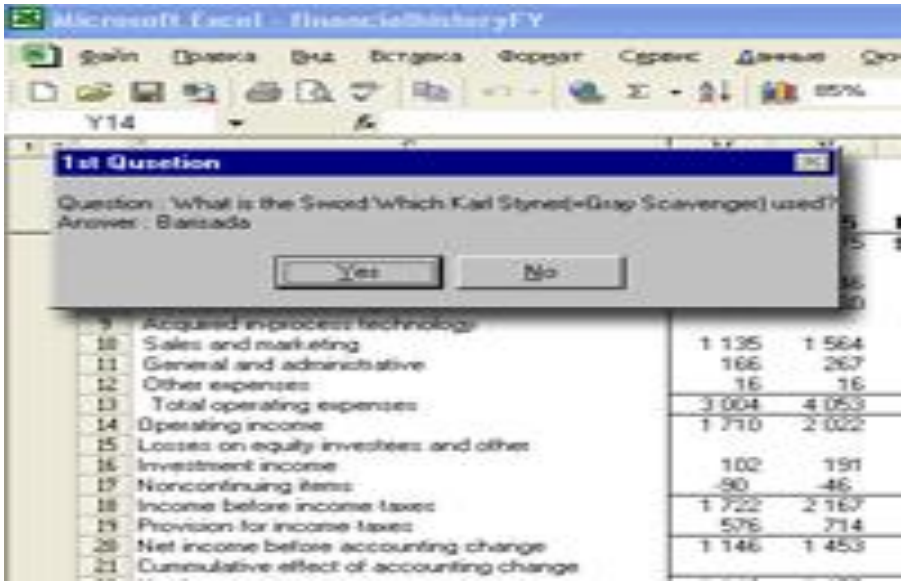

Рисунок 1 − Приклад макровірусу

Стелс-віруси будь-якими способами і засобами приховують свій факт присутності в системі [7][1)]. Відомі стелс-віруси майже всіх типів, за винятком Windows-вірусів і вірусів, написаних під Unix системи. При спробі виявлення стелс-вірус маскує себе під нешкідливу програму, видаючи помилковий «чистий» код.

До поліморфних вірусів належать ті з них, які торік дуже важко або неможливо здійснити за допомогою антивірусних сигнатур − ділянок основного коду, специфічних для даного вірусу. Дана властивість вірусу досягається за рахунок використання двох основних способів – шифруванням тіла вірусу з непостійним ключем і генеруванням набором команд расшифровщика або самогенерації коду виконуваного вірусу [8]. Поліморфізм різних рівнів складності зустрічається у вірусах майже всіх

[1)] [7] Рейтинги антивірусів. URL: http://it-sektor.ru/proplachennaya-stat-ya-ili-kaknakruchivaut- reyiting-antivirusov.html (Дата звернення 02.05.2020)

[2)] [8] Касперски К. Комп'ютерні віруси зсередини і зовні. М.: Питер, 2006. 526 с. ISBN 5-469-00982-3

типів і видів − від завантажувальних і файлових Windows-вірусів і навіть макровірусів.

Резидентні віруси. Під поняттям "резидентність" (TSR − Terminate and Stay Resident) розуміється здатність вірусів залишати свої сліди перебування в оперативній пам'яті комп'ютера, перехоплювати події (наприклад, звернення до папки або розділу жорсткого диска) і при цьому запускати механізми зараження «чистих» файлів [9][1)]. Таким чином, резидентні віруси виконують свою роботу, яка приносить шкоду, не тільки під час використання користувачем будь-якої програми, але і після того, як програма закривається і надалі не використовується користувачем.

Нерезидентні віруси, дуже активно проявляють себе в короткий проміжок часу – тільки в момент завантаження зараженої ними ж програми. Для свого розвитку вони шукають незаражені файли на диску і заражають їх зсередини. Після закриття зараженої програми вірусом їх дію і вплив на саму ОС зводиться до нуля. Тому, заражені файли, з якими попрацював нерезидентний вірус значно простіше вилікувати, ніж видалити файл цілком [10][2)].

Черв'як. IRC (Internet Relay Chat) − це протокол, який використовується для комунікації користувачів в мережі Інтернет в реальному часі. Цей, протокол, один з численних дозволяє користувачам спілкуватися між собою за допомогою Інтернет – "розмови" за допомогою спеціальних програм, розроблених на належному рівні.

IRC схожий на телефонну розмову між абонентами, за винятком того, що в розмові можуть брати участь більше двох співрозмовників, які зазвичай об'єднуються за інтересами в відмінні одна від одної групи IRC-конференцій.

[1)] [9] Трасковскій А. В. Збої і неполадки домашнього ПК. 2-е изд., Перераб. і доп. СПб.: БХВ-Петербург, 2009. 512 с. ISBN 978-5-94157-964-8

[2)] [10] Михайлов А.В. Комп'ютерні віруси і боротьба з ними. М.: ДіалогМІФІ, 2011. 104 с. ISBN 978-5-86404-236-6

Також в цих програмах існує можливість обміну різними типами файлів – саме цю функцію і використовують IRC-черв'яки [8][1)].

До мережевих відносяться віруси, які розповсюджуються за допомогою переміщення по глобальній мережі, зокрема у всесвітній павутині [11][2)].

Головною перевагою мережевого вірусу є така можливість, як передати код віддаленого сервера, або робочої станції. «Завершення» мережеві віруси можуть змусити користувача запустити вірус на своєму комп'ютері, і користувач сам того не помічаючи заражає свій комп'ютер, і в подальшому є розповсюджувачем інфекції.

До потенційно небажаних програм (ПНП) крім вірусів, відносяться також деяка різновид вірусів як «троянські коні», утиліти прихованого віддаленого зашифрованого адміністрування, "крадуть" паролі доступу до аккаунтів в мережі Інтернет, а також конфіденційну інформацію, захищену законом. Безліч «троянських» програм підробляються, як повнофункціональна нешкідлива програма, внаслідок чого багато антивіруси можуть і не розпізнати «злодія». Дуже часто «трояни» приходять по електронній пошті у вигляді архіву і т.д. Шпигунська програма (Spyware) – це програмний продукт, здатний проникати на комп'ютер без згоди його власника, метою отримання якого є повний доступ над комп'ютером або електронним пристроєм, основне завдання якого полягає в реєструванні і передачі конфіденційних даних.

Зомбі (Zombie) – самий «улюблений» вірус комп'ютерних зловмисників, які отримують доступ до вашого комп'ютера за допомогою підключення даного вірусу до мережі Інтернет, і в подальшому машина, заражена даним видом вірусу, виконує команди і доручення третіх осіб .

[1)] [8] К. Касперски Комп'ютерні віруси зсередини і зовні /. М .: Питер, 2006. 526 с. ISBN 5-469-00982-3 http://al24.ru/pdf_kniga_2663.html

[2)] [11] Цирль В.Л. Основи інформаційної безпеки. Короткий курс. М.: Фенікс, 2008. 256 с. ISBN 978-5-222-13164-0

Таким чином, «комп'ютери-зомбі», та й будь-які електронні «пристрою-зомбі» об'єднуються в один великий пул, через який в автоматичному режимі йде атака на сайти, сервера, банки і т.д. «Зомбіпули» здатні порушити роботу навіть самого добре захищеного сайту, над яким працювали висококваліфіковані фахівці і при тому не один рік.

Фішинг (Phishing) – це поштова розсилка, що має на увазі, захоплення особистих конфіденційних даних для передачі третім особам, а також введення одержувача фішинг-розсилки в оману, що має на меті отримання грошових коштів шляхом застосування соціальної інженерії.

Фармінг – підвид фішингу, основним змістом фармінга є підробка оригінальних сайтів банку, уряду, які дуже складно відрізнити від оригіналу [9][1)]. Користувач, потрапивши на «підроблений» сайт, зазвичай нічого не підозрює, але варто йому ввести свої дані, номер банківської карти або пін-код, то в одну мить ці дані виявляються у зловмисника і всі засоби протягом однієї секунди зникають в невідомому напрямку.

Мобільні віруси – це спеціалізоване шкідливе ПО, розроблене для невеликих гаджетів, що має своєю основною метою отримання конфіденційної інформації. В основному господарі своїх електронних вихованців і не підозрюють про те, що їх пристрій заражено і несе собою шкоду не тільки для нього самого, але і для оточуючих, шляхом передачі даних через відкриті точки доступу Wi-fi і 3G, а також - все рідше Bluetooth [1][2)].

Мобільні віруси здатні передавати і перехоплювати смс повідомлення на льоту, що робить їх майже непомітними, також більш-менш сучасні,

---

[1)] [9] Трасковскій А. В. Збої і неполадки домашнього ПК. 2-е изд., Перераб. і доп. СПб.: БХВ-Петербург, 2009. 512 с. ISBN 978-5-94157-964-8

[2)] [1] Лабораторія Касперського. URL: http://securelist.ru/ (Дата звернення 30.04.2020)

адаптовані віруси записують розмови, архівують дії користувача і збирають інформацію про приватне життя власника гаджета.

Легендарними і поширеними мобільними вірусами, в наш час є: Cabir, Comwar, Brador, Viver а також, їх багатомільйонні допрацьовані і вдосконалені побратими, здатні дізнатися все за п'ять хвилин і навіть за лічені секунди.

1.3 Хто і навіщо пише віруси

Найбільш прості передумови і причини, які спонукають хакерів - зломщиків, та й просто людей створювати так би мовити «комп'ютерні віруси», тобто віруси – допитливість і таємничість. З самого витоку історії появи перших вірусів, першопричини так і не змінилися. Зазвичай все відбувається, як і у переважної більшості інших, так званих, хакерів - злочинців електронного світу: допитливість і непідробна захопленість комп'ютерними і електронними технологіями, немислима тяга до секретної та прихованої від більшості очей надсекретної інформації. Точкою відліку стає наступна основна і найважливіша задача: додати будь-яку програму А в основну – здійсненну частину програми Б таким чином, щоб програма Б втратила своїх властивості і функціональності. Для цього потрібні глибокі пізнання як самої системи, так і її компонентів, під керуванням якої буде працювати і діяти програма. Першо-наперво це був DOS, простий емулятор командного рядка, який мав серйозні обмеження не тільки по функціональності, але і по ряду своїх технічних можливостей, однак він не користувався популярністю у серйозних програмістів і кодерів, програмістів-фахівців своєї справи [14][1)].

[1)] [14] Хто і навіщо пише віруси. URL: http: // zillya .ua / ru / kto-i-zachem-pishetvirusy (Дата звернення 05.05.2020)

Після деякого необхідної кількості часу, з'являлися різні варіативні версії Windows, які більше не могли бути звичайною надбудовою над DOS, а являли собою повноцінну ОС як для роботи, так і для серфінгу в глобальній мережі імен Інтернет. Інтерфейс і найширший спектр нових функціональних і неймовірних на той час опцій були більш доброзичливі до користувача, і в свою чергу вірусописьменниками − «електронним лиходіям» необхідно було адаптувати і пристосувати свій індивідуальний код для цих систем, і продовжувати шукати в них можливості нанесення шкоди і тяжкого шкоди витоку особистої конфіденційної інформації.

Віруси ставали спокусливо красиві і привабливі зовні, але і ефект їх руйнівної шкоди ставав більш значніше і серйозніше, рік від року. Незвичайна на ті часи щедрість внести особистий індивідуальний графічний аспект в свої віруси, як частину своєї суб'єктивності, дозволила поготів більшості авторів і надало можливості персоналізувати і індивідуалізувати свої «творіння», наприклад, словосполучення «William Blake» занесене в Maltese Amoeba. Чим більше розширювався функціонал і додавалося безліч цікавих речей і до того ж удосконалювалося у вірусах, тим значнішими і руйнівними вони ставали за своїм змістом і масштабами ураження як ОС, так і захоплення комп'ютерів і серверів компаній для особистих цілей і вигоди.

Віруси з'являлися повільно і були за своїм призначенням і основним принципом, лише параграмою імен. Багато авторів − творці вигадували неприродні і екзотичні імена, для формування і створення атмосфери недосяжною Енігми, скритності-безпеки свого справжнього реального імені і приватних даних [15][1)]. Написання і творення вірусів блискавично швидко стало цікавити колосальну кількість безлічі людей і груп, об'єднаних спільними прагненнями домогтися, досягти рівня тих, хто має можливості і

[1)] [15] Всесвітня історія заражень. URL:http://lenta.ru/articles/2014/11/18/virus/ (Дата звернення 05.05.2020)

здатний «заразити» комп'ютер на іншому боці земної кулі парою натиснень спеціальних комбінацій клавіш.

1.4 Мотиви написання вірусів

Зануримося в історію і спробуємо зрозуміти не тільки першопричини, а й відповісти на питання: «Навіщо люди пишуть віруси?». На це є кілька вагомих причин і аргументів. Перша − для задоволення. Це перша і найбільш основна загальновизнана першопричина. Автору-творцеві було просто дуже цікаво і цікаво, що може трапитися, статися і під що вильється в подальшому його незгасимі бажання пізнання. Люди не усвідомлюють і не вірять в проблеми і їх існування, поки самі з нею не зіткнутися. Друга причина для творення - це досягти тієї, здається недосяжною уявної цілі, щоб програмний код і подальший результат його дій з'явився на Wildlist, сайті, що висвітлює в мережі в даний момент по всьому світі віруси. Наприклад: «Kit clickers», «Script kiddies», «Kit coders». «Kit clickers» просто-напросто використовують генератори вірусів, яких на наше століття безліч з різними модифікаціями. «Script kiddies», які беруть готові набори ділянок коду для створення «своїх» вірусів. Популярна і донині програма − вірус, черв'як «Anna Kournikova», була втілена в життя з використанням Kalamar kit. «Kit coders».

Представлена і розглянута група не вітається як вірусописьменники, так і тими, хто займається захистом інформаційних і персональних даних [14][1)]. Перша група з розглянутих містить в своїй команді тільки тих, хто не лінується працювати мишкою і генерувати по 30 вірусів з різних іноді несумісних блоків коду, які потребують для виявлення в повному розборі і дизасемблюванні, аналізі і т.д.

[1)] [14] Хто і навіщо пише віруси. URL: http: // zillya .ua / ru / kto-i-zachem-pishetvirusy (Дата звернення 05.05.2020)

Хоча саме вони і забезпечують більший обсяг роботи величезні антивірусні компанії і безліч як відомих, так і не дуже, вірусних лабораторій. Зазвичай штат команди з цього розділу з натхненній радістю і гордістю дає інтерв'ю в численні видання, тим самим спотворюючи і завдаючи шкоди репутації серйозних кодерів і професійних хакерів.

Розкрилися серйозні кодери − ця команда складається з більш небезпечних освічених кодеров і програмістів, які мають досить великий і незаперечний досвід як в програмуванні, так і в проектуванні, і можуть писати свої додатки на рівні антивірусної індустрії. Вже до створених вірусів вони додають безліч особистих процедур і функцій, які блокують при аналізі – дизасемблюванні отримання вихідного коду вірусу для його подальшого знешкодження та лікування заражених файлів [16][1)].

Парадоксально, але саме такі віруси пишуться і створюються для будь-якого дослідження і вивчення будь-якого процесу так би мовити зсередини, а не для нанесення навмисної шкоди кінцевому користувачеві. Не можна не згадати, що права доступу до даного коду має досить суб'єктивно мала і обмежена кількість людей, і все з тієї ж команди-угруповання, або на худий кінець цей код стає загальним надбанням доступним в мережі Інтернет, як доказ знайденої лазівки, діри-уразливості як програми, так і цілого ряду інформаційних систем, або на худий кінець цей код стає загальним надбанням доступним в мережі Інтернет, як доказ знайденої лазівки, діри-уразливості як програми, так і цілого ряду інформаційних систем.

Вони жодним чином не завдають нікому шкоди, а лише підказують напрямок на напрямок, звідки і куди може бути завдано серйозний удар і як можуть бути вилучені конфіденційні дані [1][2)].

[1)] [16] Центр дослідження комп'ютерної злочинності. URL: http://crimeresearch.ru/ (Дата звернення 08.05.2020)

[2)] [1] Лабораторія Касперського. URL: http://securelist.ru/ (Дата звернення 30.04.2020)

«Розгнівані одинаки» – завершальний і найнебезпечніший тип допитливого хакера. Їх не стосується будь-яка мораль або закон, і не враховується відсоток і глобальність тих збитків, які може понести потерпілий користувач або організація. Кожен з них має свою заповітну, індивідуальну, персональну мету. Вони не відносять себе ні до якої групи кодерів, хакерів, вони представляють себе одноосібниками в глобальному просторі. Їх завдання завдати максимального збитку і шкоди для користувача даних і отримати власну вигоду [17][1)]. Їх не вдається підвести під загальні рамки і правила вірусів, так як у кожного з них своя мораль і ідеологія, і про неї ніхто ніколи не знає. В даний момент до цієї групи належить не така велика кількість людей. Захоплення – одна з найбільш незаперечних рушійних сил більшості вірусів, саме завдяки цій силі і створюються такі програми, які виростають із, здавалося б, простого захоплення.

В когось є у розпорядженні досить багато вільного особистого часу, який вони проводять за улюбленим заняттям. Їх можна порівняти з першою групою, але частіше за все вони дуже грамотно програмують, дотримуючись усіх правил, годинами дивляться логи на наявність частин пропущеного коду, для виявлення помилки, або раз по разу перевіряють і тестують працездатність своїх творінь під різними версіями ОС (свого роду бета - тестування). Кодери, як і звичайні люди часто допомагають один одному порадами, діляться корисною і важливою інформацією, ночами безперервно вивчають нові віруси і їх функціональні особливості, або придумують і реалізовують нові ідеї. У цієї групи немає як такої поставленої мети і реалізованої завдання: нашкодити кому-небудь, або зациклюватися на одній ідеї.

[1)] [17] Касперски К. Записки дослідника комп'ютерних вірусів. М.: Питер, 2006. 320 с. ISBN: 5-469-00331-0

1.5 Опис антивірусу

Антивірусна програма − це комп'ютерна програма, спеціально створена для пошуку та знешкодження вірусів. Оскільки вона може виявити вірус, то вона знає і відповідні засоби боротьби з ним. Незважаючи на це, кожен день виходить більше 20 нових вірусів, що антивірусні програми не здатні виявити. Тому регулярне оновлення антивірусних баз є основою для успішного пошуку і знищення цих шкідливих кодів. Ефективність антивірусної програми залежить, головним чином, від її здатності оновлюватися щодня. На жаль, сьогодні не існує стовідсоткових методів захисту від комп'ютерних вірусів. Це пояснюється тим, що кожен день у світі створюється декілька десятків нових комп'ютерних вірусів.

Процес розробки антивірусних заходів відстає від процесу створення вірусів на декілька тижнів (а можливо, й місяців), і саме в цей час віруси завдають великих збитків. Всі існуючі заходи боротьби з комп'ютерними вірусами можна умовно поділити на дві категорії: профілактичні заходи; заходи щодо знищення комп'ютерних вірусів та лікування заражених програм і даних[18] [1)].

Особливу увагу треба приділяти саме профілактичним заходам, тобто заходам, які можуть запобігти зараженню комп'ютера та втраті цінних даних. На жаль, за сучасних умов не допустити зараження комп'ютерними вірусами майже неможливо: для цього не треба користуватись комп'ютерними мережами, гнучкими дисками з інших комп'ютерів, піратським програмним забезпеченням тощо.

За статистикою через зараження вірусами проходить кожний комп'ютер. Саме тому головним та надійнішим профілактичним заходом вважається резервне копіювання даних. Резервні копії всіх цінних даних

[1)] [18] Роббінс Д. Налагодження Windows-додатків; М.: ДМК Пресс, 2009. 448 с., ISBN 5-94074-085-5.

рекомендується зберігати на компакт-дисках або інших жорстких дисках. Зберігання копії на гнучкому диску або на тому самому жорсткому диску не дає гарантії безпеки.

1.6 Класифікація антивірусів

Програми-детектори: призначені для знаходження заражених файлів одним із відомих вірусів. Деякі програми-детектори можуть також лікувати файли від вірусів або знищувати заражені файли. Існують спеціалізовані

(тобто призначені для боротьби з одним вірусом) детектори та поліфаги (можуть боротися з багатьма вірусами):

- програми-лікарі: призначені для лікування заражених дисків і програм (лікування програми полягає у вилученні із зараженої програми тіла вірусу, також можуть бути як поліфагами, так і спеціалізованими);
- програми-ревізори: призначені для виявлення зараження вірусом файлів, а також знаходження ушкоджених файлів. Ці програми запам'ятовують дані про стан програми та системних областей дисків у нормальному стані (до зараження) і порівнюють ці дані у процесі роботи комп'ютера. В разі невідповідності даних виводиться повідомлення про можливість зараження;
- лікарі-ревізори: призначені для виявлення змін у файлах і системних областях дисків й у разі змін повертають їх у початковий стан;
- програми-фільтри: призначені для перехоплення звернень до операційної системи, що використовуються вірусами для розмноження і повідомляють про це користувача (останній має можливість дозволити або заборонити виконання відповідної операції, такі програми є резидентними, тобто вони знаходяться в оперативній пам'яті комп'ютера);

– програми-вакцини: використовуються для обробки файлів і boot-секторів із метою попередження зараження відомими вірусами (в останній час цей метод використовується все частіше).

2 АНАЛІЗ АНТИВІРУСНОЇ ПРОГРАМИ

2.1 Опис антивірусної програми DRWEB

Один з кращих антивірусів із сильним алгоритмом знаходження вірусів. Поліфаг, здатний перевіряти файли в архівах, документи Word і робочі книги Excel, виявляє поліморфні віруси, котрі в останній час, отримують все більше поширення. Приклад роботи антивірусної програми DR WEB зображений на рис. 2

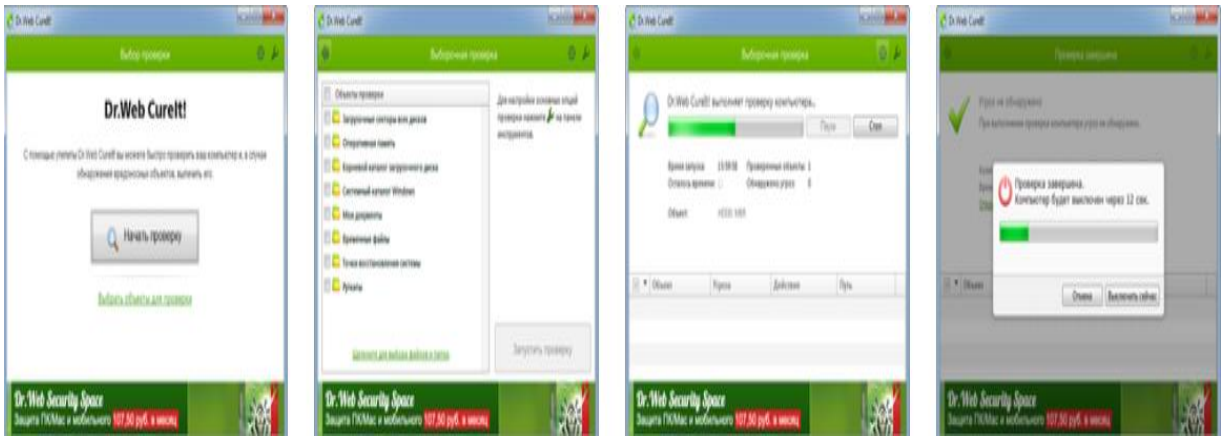

Рисунок 2 − Приклад роботи антивірусної програми DR WEB

Достатньо сказати, що епідемію дуже небезпечного вірусу OneHalf зупинив саме DrWeb. Евристичний аналізатор DrWeb, досліджуючи програми на наявність фрагментів коду, характерних для вірусів, дозволяє знайти майже 90% невідомих вірусів. При завантаженні програми в першу чергу DrWeb перевіряє самого себе на цілісність, після чого тестує оперативну пам'ять. Програма може працювати у діалоговому режимі, має дуже зручний інтерфейс користувача, який можна настроювати.

2.2 Опис антивірусної програми ADINF

Антивірус-ревізор диска ADINF (Avanced DiskINFoscope) дозволяє знаходити та знищувати, як існуючі звичайні, stealth- і поліморфні віруси, так і зовсім нові. Антивірус має в своєму розпорядженні лікуючий блок ревізору ADINF − Adinf Cure Module, який може знешкодити до 97% всіх вірусів. Цю цифру наводить "ДіалогНаука", виходячи з результатів тестування, котре відбувалося на колекціях вірусів двох визнаних авторитетів в цій області − Д.Н.Лозинського й фірми Dr.Solomon's (Великобританія).

ADINF завантажується автоматично у разі вмикання комп'ютера і контролює boot-сектор і файли на диску (дата й час створення, довжина, контрольна сума), виводячи повідомлення про їх зміни. Завдяки тому, що ADINF здійснює дискові операції в обхід операційної системи, звертаючись до функцій BIOS, досягаються не тільки можливість виявлення активних stealth-вірусів на рівні переривання Int 13h, але і висока швидкість перевірки диску. Якщо знайдено boot-вірус, то ADINF просто відновить попередній завантажувальний сектор, котрий зберігається в його таблиці.

Якщо вірус є файловим, то тут на допомогу приходить лікуючий блок Adinf Cure Module, який на основі звіту основного модуля про заражені файли порівнює нові параметри файлів із попередніми, які зберігаються в спеціальних таблицях. При виявленні розбіжностей ADINF відновлює попередній стан файлу, а не знищує тіло вірусу, як це роблять поліфаги. Приклад роботи антивірусної програми ADINF зображений на рис. 3

Рисунок 3 − Приклад роботи антивірусної програми ADINF

2.3 Опис антивірусної програми AVP

Антивірус AVP (AntiVirus Program) відноситься до поліфагів, у процесі роботи перевіряє оперативну пам'ять, файли, в тому числі архівні, на гнучких, локальних, мережних і CD-ROM дисках, а також системні структури даних, такі як завантажувальний сектор, таблицю розділів і т.д. Програма має евристичний аналізатор, котрий, за твердженнями розробників антивірусу здатний знаходити майже 80% усіх вірусів.

Програма AVP є 32-розрядним додатком для роботи в середовищі операційних систем Windows 98, NT і 2000, має зручний інтерфейс, а також одну з найбільших у світі антивірусну базу. Нові бази антивірусів до AVP з'являються приблизно один раз у тиждень і їх можна отримати з Internet. Ця програма здійснює пошук і вилучення найрізноманітніших вірусів, у тому числі: поліморфних, або вірусів, що самошифруються; стелс-вірусів, або вірусів-невидимок; нових вірусів для Windows. Приклад антивірусної програми AVP зображений на рис. 4.

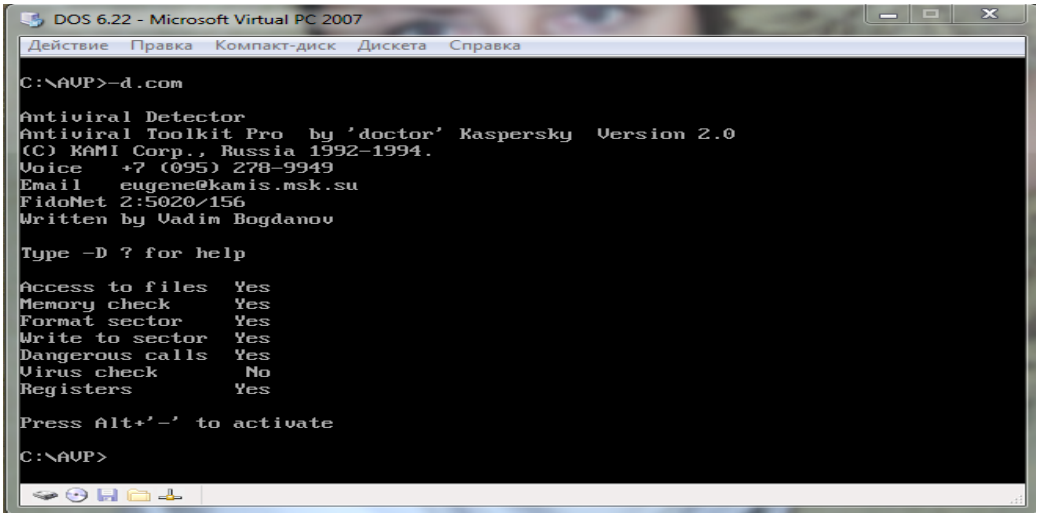

Рисунок 4 – Приклад антивірусної програми AVP

3 ОПИС АНТИВІРУСНИХ СКАНЕРІВ

Антивірусні сканери з своєї основної мети є найбільш популярними програмними засобами для виявлення та знешкодження вірусів. Не поступаючись по функціоналу і ряду завдань, за ними слідують CRC-сканери. Часто обидва розглянутих нами методу об'єднують в одну програму, яка володіє найкращим якістю виявлення і швидкістю обробки заражених файлів. На даний момент часто вживаються такі необхідні елементи, як блокатори, імунизатори, монітори, Sandbox і Cloud Security технології.

Принципи роботи антивірусних сканерів засновані на перевірці файлів та виявлення в них злісного ділянки коду, секторів оперативної пам'яті, побітного «проходження» по файлу, а також звірку з базою даних сигнатур самого антивірусного сканера. Для пошуку популярних вірусів використовуються так звані маски імен і суми хеш-коду. Маска вірусу − деяка послідовність коду, специфічна для цього конкретного вірусу, тобто містить послідовність елементів в коді вірусу . Якщо вірус не містить маски або довжина його коду перевищує кількість містяться в ньому символів, то використовуються інші методи виявлення.

Прикладом такого методу − алгоритмічна мова, в якому описані всі можливі варіанти коду, які можуть зустрітися при зараженні подібного типу вірусом.

У багатьох сканерах використовуються алгоритми евристичного сканування, тобто аналіз послідовності в об'єкті, що перевіряється, набір необхідної статистики та прийняття первинного рішення для кожного об'єкта, що перевіряється.

До переваг сканерів відноситься їх легкість, універсальність, швидкодія і незначний вплив на операційну систему, до недоліків – «важкі» розміри

антивірусних баз, які сканерів доводиться «носити з собою», і в деяких зустрічається повільна швидкість пошуку вірусів.

Дія CRC-сканерів заснований на підрахунку CRC-сум (контрольних сум) для наявних на диску файлів. Ці контрольні суми зберігаються в базі даних антивіруса, як і інша інформація: довжини та кількості файлів, дати модифікації і т. д. При кожному запуску CRC-сканери перевіряють дані, що містяться в їх базі даних, з заздалегідь розрахованими значеннями. Якщо інформація про файл, записана у базі даних, не збігається зі значеннями, то CRC-сканери виводять повідомлення про те, що файл був змінений або заражений яким-небудь вірусом.

CRC-сканери, в основі своїй містять «антистелс» − алгоритми, є сильною протиотрутою проти вірусів: практично 100% вірусів виявляються «спійманими» майже відразу після їх прояви на комп'ютері. Однак у даного типу антивірусів є недолік, який помітно знижує їх ефективність і лабільність.

Недолік полягає в тому, що CRC-сканери не можуть зловити вірус в момент його появи в системі, а роблять це лише через деякий час, вже після того, як вірус «пішов» по комп'ютеру. CRC-сканери не можуть знайти вірус у новостворених файлах, оскільки в їх базі даних така інформація не міститься.

Більше того, практично щодня з'являються віруси, які використовують "слабкість" CRC-сканерів, заражають тільки новостворювані файли і залишаються непомітними для CRC-сканерів.

Антивірусні монітори − це спеціальні резидентні програми, які в основному перехоплюють вірусо-небезпечні ситуації і повідомляють про це користувачеві. До переваг використання антивірусів типу моніторів відноситься їх відмінна риса від всіх інших - виявляти і блокувати вірус на стадії його впровадження в комп'ютер або електронні засоби, гаджети. Як і у кожного представника покоління «людина» є свої позитивні сильні сторони,

так і негативні, у розглянутого виду антивірусів − моніторів є свої недоліки, до них відносяться : існування шляхів обману захисту монітора і велика кількість помилкових спрацьовувань, що, мабуть, і послужило причиною для повної відмови від даного виду антивірусних програм.

Необхідно також зауважити таке цікаве напрямок антивірусних засобів захисту, як антивірусні монітори, виконані у вигляді апаратних компонентів комп'ютера. Однак, як і у випадку з програмними моніторами, такий захист дуже просто і невимушено обійти. Також до вище перелічених недоліків додаються наступні проблеми сумісності зі стандартними конфігураціями комп'ютерів і складності при їх установці та налаштування, використання. Все перераховане вище робить вбудовані апаратні монітори в основному непопулярними засобами на тлі різних типів антивірусного захисту.

Імунізатори − досліджуваний вид ділиться на два типи: імунатори, повідомляють про вторгнення зловмисників, і імунізатори, блокуючі небезпечні і шкідливі дії . Перші зазвичай дописуються в кінець коду довжини файлів і при запуску файлу кожен раз перевіряють його на «неякісне» змінення.

Недолік у таких імунізаторів всього на всього один, але він летальний: досконала нездатність повідомити про зараження "стелс"-вірусом. Тому такі імунізатори, як і монітори, не знайшли практичного застосування в наш час.

Другий тип імунізації захищає систему від ураження вірусом і блокує підозрілі дії якогось певного виду. Файли на дисках модифікуються таким чином, що вірус приймає їх за вже своїх заражених побратимів . Для захисту від резидентного вірусу в оперативну пам'ять комп'ютера записується програма, що повторює точнісінько копію вірусу, при запуску вірус випадковим чином знаходить її і вважає, що система вже заражена.

Такий тип імунізації не є достатньо універсальним, оскільки не можна проіндетифікувати файли від всіх відомих і невідомих вірусів. Однак,

незважаючи на це, подібні імунізатори як заходи попереднього захисту можуть цілком надійно захистити комп'ютер від нового незвіданого вірусу аж до того часу, коли він буде знайдений антивірусними сканерами і комплексними засобами захисту.

Онлайн сканер. Світ знає сервіси, які дозволяють перевірити комп'ютер, підключений до мережі Інтернет на наявність вірусів. Вони працюють за допомогою технології ActiveX або Java. Їх перевага – можливість пошуку і лікування на льоту заражених файлів без установки антивірусного ПЗ. Основний мінус цього типу сервісів – відсутність профілактики і моніторингу зараження. Найбільш відомі і рекомендовані онлайн сканери – ESET Online Scanner, Emsisoft Anti-Malware, Dr.Web,Cureit, Microsoft Malicious Tool, RAV, Kaspersky Removal Tool, Trend Micro,Comodo AV Scanner .

Онлайн сканер «одного файлу». В основному займається тільки аналізом шкідливих, на вашу особисту думку, файлів. Ви просто завантажуєте на сервер антивірусної лабораторії, вибраний вами об'єкт файлової системи, і ви миттєво отримуєте відповідь. Час очікування залежить від кількості програм-євристів, якими проводиться перевірка, і навантаженням на сервер. Це рішення ідеально для тих ПК і пристроїв, де антивірус не встановлено, але слід перевірити файли, принесені, припустимо сусідом. До числа легендарних можна віднести Dr.Web online check, avast! Online Scanner, VirusTotal, Online malware scan.

Firewall. Частково цю програму можна віднести до антивірусних засобів захисту подвійного призначення, так як вона в режимі реального часу, відбиває атаки вірусів і хакерів (комп'ютерних зловмисників). Основний механізм − блокування, сканування мережевого трафіку і забезпечення скритності і захищеності портів ПК в мережі (через блокування ping, telnet, tracert і інших сервісів). Може бути корисна і використана у

випадках збою і модифікування системних файлів (блокує вихідні несанкціоновані спроби з'єднання). Найбільш популярний сьогодні Outpost Firewall в Західних країнах світу і на Сході, в Росії Avast Free Antivirus від чеської компанії Alwil. Головне вікно Firewall зображено на рис. 5.

Рисунок 5 − Головне вікно Firewall

Антивіруси-сканери без монітора. Основна мета – сканування і очищення локальних і зовнішніх змінних носіїв від шкідливих впливів програм паразитів. На відміну від програм все в одному, що містять в собі цілий набір мережевих, в реальному часі екранів і Евріста, що не мають будь-якого вбудованим модулем, а також не мають модуля самозахисту. За рахунок відсутності деякого функціоналу досягається хороша продуктивність і рівень легітимності виявлення. Самі популярні − Cure it, Clam AntiVirus, Norton Security Scan, Sophos.

3.1 Робота антивірусів

Оцінка якості виконуваної роботи тим чи іншим антивірусом можна представити у вигляді наступних важливих аспектів: оцінці якості виявлення, рівня помилкових спрацьовувань і реакції на нові загрози; оцінці швидкості роботи антивірусних продуктів; якості лікування активного зараження; оцінці ергономіки антивірусів. Оцінка якості визначення і виявлення, рівня

помилкових спрацьовувань і реакції на нові загрози. Завдяки сучасним методам і формам аналізу, і дослідницьким результатами від широко відомої антивірусної лабораторії AVComparatives і AV-Test.org, безсумнівним лідером серед обраних антивірусів на проходження тесту в плані виявлення, якості реакції на нові ще невідомі загрози і малого рівня помилкових спрацьовувань в порівнянні з багатьма іншими є Kaspersky Internet Security, далі − Avast Free Antivirus. Замикає ланцюжок Microsoft Security Essentials. На переважній більшості форумів, наприклад nullewed.ru, в спеціальні розділи «Лікування системи», на форумі практично постійно пропонують скористатися утилітою нашого вітчизняного програміста і системного адміністратора AVZ (безкоштовною утилітою Олега Зайцева). При цьому, що важливо багато просять вирішити виниклі проблеми з відновлення системи саме після її лікування за допомогою такого іменитого програмного продукту як Kaspersky Internet Security. Оцінка швидкості реагування антивірусних продуктів – проведена в березні 2014 року, незалежною світовою лабораторією, в результаті , тестування на швидкість виявлення вірусів антивірусними продуктами показало, що серед обраних пакетів антивірусного ПО Kaspersky Internet Security і Avast Free Antivirus надають саму найменше навантаження на системні ресурси. А Microsoft Security Essentials, вимагає максимальну їх викладення. Якщо враховувати споживання оперативної пам'яті (ОЗУ) продуктами (тобто вільної оперативної пам'яті) необхідного (для X86 і X64 архітектур відповідно) при виконанні ними прямих обов'язків: Avast Free Antivirus – 1024 Мб для Windows 7, Vista, Windows 8; Kaspersky Internet Security – 1 Гб / 2 Гб для Windows Vista, 7, 8, Windows 10 Technical Preview; Microsoft Security Essentials – 512 Мб Тобто, якщо у комп'ютера оперативної пам'яті 2 Гб, то KIS просто забере левову частку системних ресурсів, тобто «покладе систему». А в усьому іншому він «швидкісний», незаперечний лідер. У

висновку порівняльного огляду компанія як зазвичай підводить підсумки по проведеному аналізу. Платні програми системи комплексного захисту високого класу Internet Security мають найбільші функціональні можливості і надійний найвищий рівень забезпеччення захисту в реальному часі серед обраних ними продуктів[5][1)]. І як намагаються стверджувати більшість вірусних лабораторії, саме комплексні захисні системи підходять більшостям користувачів , які не розбираються в программах , оскільки використовують підхід «встановив і забув». Немає необхідності встановлювати додаткові елементи і утиліти захисного програмного забезпечення. До складу багатьох таких систем опціонально входить такий важливий і незамінний компонент, як Батьківський контроль[1][2)]. Багато продуктів містять в собі функції, такі як: електронні платежі через інтернет, ізольоване середовище (SandBox), віртуальну клавіатуру, антифішинг, захист від хакерських атак і інші найважливіші елементи комплексного захисту, що дозволяють набагато зменшити ризики зараження через інтернет.

Всі численні комплекси класу Internet Security забезпечують надійний захист від багатьох мережевих атак. Безкоштовні же антивірусні пакети, наприклад, Avast Free Antivirus, варто встановлювати і налаштовувати, більш досвідченим і тямущим користувачам, не забувати, що використовуваний захист не гарантує всебічного захисту. До безкоштовного антивірусу в обов'язковому в порядку потрібна установка додаткового елемента захисного програмного забезпечення: сканера і контролера портів, фаєрвола, брандмауера і т.д.

Безкоштовні антивіруси можливо і потрібно використовувати тільки на комп'ютерах з бюджетною конфігурацією і низькими вимогами до рівня забезпечення інформаційної безпеки і захищеності. Найвідоміші безкоштовні

---

[1] [5] Інформаційні технології. URL: http://habrahabr.ru/ (Дата звернення 02.05.2020)

[2] [1] Лабораторія Касперського. URL: http://securelist.ru/ (Дата звернення 30.04.2020)

антивірусні програмні пакети, такі як Avast Free Antivirus або Microsoft Security Essentials відмінно підходять тільки в тому випадку, якщо на пристрої користувача не міститься абсолютно ніякої важливої інформації. Зазвичай безкоштовні антивіруси в більшості вибирають тільки досвідчені користувачі, яким антивірусний продукт потрібен для реалізації в якості «підстраховки». З досліджень двох відомих на ринку вірусних компаній AV-Comparatives і AV-Test.org, спостерігають, що в даному огляді порівняння антивірусних програм, відбувається не зовсім коректно, тому що порівнювати рішення програм більш високого класу, такого як Internet Security і безкоштовні антивіруси , які мають базовий набір забезпечення безпеки – це неправильно. Комплексний захист має і володіє найбільш великим функціоналом, ніж безкоштовний антивірусний захист, тим більше базовий.

Для порівняння, безкоштовна версія антивірусного пакета Avast поступається не тільки конкурентам з суміжної області, а й по функціональним можливостям навіть своєму платному братові Avast Pro. За оцінкою якості роботи, багатьох антивірусних програм, теж є свій ряд питань. Тут наводиться в порівняння цілий комплекс захисних функцій KIS, а зокрема, як своєчасно і якісно вони реагують і обробляють нові загрози, з роботою антивірусного ядра теж не все добре і антивірусного аналізатора безкоштовних пакетів антивірусів. Наприклад, якщо взяти всім відомий безкоштовний антивірус чеського виробництва – Avast, додатково

встановити такий елемент защітикак фаєрвол Comodo і утиліту Malwarebytes Scaner, то KIS помітно програє зі своєю реалізації захисту. При цьому споживання оперативної пам'яті при виконанні своїх прямих обов'язків цими захисними засобами буде в доцільних для більшості межах 700 Мб, в той час як для KIS необхідно буде 1,5-2 Гб. Для лікування найкраще застосовувати спеціальні для етоого створені програми – лікуючі

утиліти такі, як DrWeb CureIt, Eset Nod32 Scanner, AVP, тобто утиліти серії LiveCD / USB або утиліта AVZ. Всі інші можуть завдати шкоди комп'ютеру і призначених для користувача даних, тому що антивірусні рішення фокусуються і призначені для виявлення, припинення вторгнення загроз. Якщо порівнювати правильно налаштовані компоненти і функціонал KIS і Avira Internet Security (рішення останніх «свіжих» версій), то продукт Касперського і тут програє, як при виявленні шкідливих програм, так і за обсягом використання системних ресурсів. Виходячи з вище викладеного, напрошується висновок про те, що даний і проаналізований порівняльний тест компаній AVComparatives і AV-Test.org, був проведений і виконаний не для виявлення недоліків Kaspersky Internet Security, а метою показати і прорекламувати користувачам вузькоспеціалізований продукт для підтримки високого рейтингу компанії . Отже, багато тестів від відомих як антивірусних, так і вірусних лабораторій в тій чи іншій мірі, мають на меті прорекламувати який-небудь продукт для отримання прибутку і подальшого розвитку власного бізнесу і взаємної вигоди. І ніяк не ставлять перед собою мету об'єктивно і досить широко розглядати, аналізувати і тестувати продукти, для надання широкому колу користувачів найбільш точних і повних результатів того чи іншого програмного засобу, що розглядається ними.

3.2 Аналіз ефективності захисту

У мільйонів користувачів по всьому світу будь то комп'ютер, ноутбук, планшет або смартфон підключений і функціонує Інтернет. Тобто середовище і швидкість розповсюдження вірусів стала такою ж, що і поширення антивірусних баз сигнатур. Випередження антивірусів над вірусами практично звелося до нуля . Замість операційних систем на досить широко відомої основі MS DOS (а це, також, вся лінійка включає: Win1.xx–

Win3.xx, Win95/96/98/ME) на електронні пристрої прийшло наступне покоління ядра Windows NT у реалізації Windows 2000/XP. Тепер ядро операційної системи, її код і оброблюємі дані, надійно розділені та ізольовані від адресного простору імен звичайних прикладних програм, не належать до системних. Віруси пишуть заради власної вигоди та отримання блага. Саме «віруси», практично через малий проміжок часу 3-4 роки, зникли з комп'ютерів і різних девайсів користувачів. Їм на зміну прийшли всілякі «черв'яки», «троянські коні», «блокувальники», орієнтовані для одержання матеріальних благ − грошей. У 2000-2005 роках антивіруси вже не могли лікувати заражені складними вірусами-троянами машини. Ось файлове зараження – запросто, скільки душі завгодно, а коли впроваджуються у виконувані модулі операційну систему – ні. На цьому за останні 15 років зросла ціла індустрія «anti-malware»: Spybot Search&Destroy, Ad-Aware, SpySweeper і їх різні многоваріативними побратимами . Антивірусна багатомільярдна індустрія досить швидко зрозуміла та усвідомила, що гроші як вода, витікають з їх рук і за короткий термін надолужила згаяне . Ось тільки швидкості розповсюдження вірусів і антивірусних сигнатур вплинув на рівень запобіганню зараження, і не в кращу сторону, він значно знизився. Антивіруси стихійно і все більше спізнюються. І практично в реальності вже майже нічого не рятує – ні евристик, ні поведінковий блокує, не аналізатор поведінки. Програмісти та хакери, які пишуть і створюють віруси, які обходять будь-які мислимі та немислимі рівні захисту. На більшості форумів і хелп-дошках з різною періодичністю спливають теми у ретро стилі: «А Антивірус пропустив зараження, він поганий. Порадьте хороший». Людині радять і рекомендують «хороший», який залишається в привілейованому статус аж до наступного пропуску або зараження . Після чого цикл пошуку і вирішення проблеми «хорошого антивіруса» повторюється. Виникає відмінний парадокс – нові розроблювані технології запобігання зараження,

показують абсолютні результати захисту в тестах на запобігання зараження (так іменовані «динамічні тести»), не можуть зайняти місце під сонцем, т. к. прийшли на ринок досить-таки порівняно пізно . Антивіруси не кращі в задачі запобігання і лікування зараження. Коли хтось створює новий, інноваційний продукт для ринку, де немає усталених «хороших практик», технологій та лідерів, про нього напишуть. Але якщо це не так, то ніхто нічого писати думати не буде. І причин тут декілька:

- журналісти − такі ж люди (навіщо щось шукати та про щось нове писати, якщо можна сидячи на своєму зручному насидженому місці отримувати пристойні гонорари за вже наявні розробки, лише коригуючи їх);
- за інерцією свідомості, користувачі не смикають журналістів писати нові статті про інноваційні засоби захисту
- всі видання існують на доходи від реклами (антивірусна індустрія спонсорує значну її частину; якщо видання почне друкувати справжні «живі» статті, де йдеться про ненадійність як антивірусів, так і компаній, що їх виробляють, то на наступний же день, або навіть через годину до нього неодмінно завітають представники PR-відділу дистриб'ютора або самого виробника антивірусних засобів, скажуть, що співпрацювати з таким виданням, хоч і мають вагу на світовій арені їм невигідно).

3.3 Аналіз Return on Investment

Спробуємо розібратися в наступному питанні: «Чому великі світові виробники і бренди антивірусної індустрії нічого, фактично і практично, нового не пропонують споживачам?» Все це, як і багато іншого залежить від великих виробників засобів захисту, для більшості яких це є лише засобом ведення і підтримки бізнесу. У кожного свого напрямку, хтось виробляє і

продає Кока-Колу, хтось – антивіруси. І істотних відмінностей між цими симбіотичними бізнес-процесами немає. Невідомі і не «пропіарені» виробники засобів захисту, є воістину невичерпними ентузіастами, оперують такими поняттями як «надійність засобів захисту», «адекватність моделі загроз» і, може і звучить банально, але гордо «професійна компетентність». Великі світові виробники оперують лише одним коротким терміном- ROI. ROI (Return on Investment) – це «рівень повернення інвестицій». Якщо хтось вклався в якесь виробництво сигнатурного двигуна нового покоління для виявлення загроз, то спочатку гроші потрібно повернути з прибутком і відсотками, поділитися нею з акціонерами, вищим менеджментом, а вже потім, може бути, зробити або закупити щось небудь новеньке [1] [1)]. І думка якогось невідомого споживача нікого тут не турбує і не хвилює, а поготів більшість настільки залякане і загнано в рамки, що його можна змусити повірити в надійність чого і кого завгодно. Наприклад, Fake антивіруси. Вони виглядають, як антивіруси, вони сканують, як антивіруси, вони вимагають гроші, як антивіруси, вони симулюють роботу, як антивіруси.

Ось тільки проблемка в тому, що не захищають, скоріше, навпаки, допомагають зловмисникам заволодіти вашою особистою інформацією.

Розглянемо один знаменитий приклад: в 2005 році не маловідома Лабораторія Касперського успішно інтегрувала в свою продуктову лінійку програм поведінковий блокувач. В той чудовий час його не було і не могло бути, по ряду істотних проблем ні в одному антивірусі. І все пара якихось стартапів (CyberHawk, після покупки PC Tools'ом-ThreatFire, компанія представляє з себе, на даний момент, частиною корпорації Symantec, і Sane Security Promary Response Safe Connect, що куплений був колись у AVG), безуспішно намагалися пробитися в пресу і в маси, завоювати собі місце під сонцем. Через п'ять років, ближче до 2010 року, більшість , що виробляють

[1] [1] Лабораторія Касперського. URL: http://securelist.ru (Дата звернення 30.04.20)

стартапи були скуплені за безцінь більшими гравцями, їх програмні продукти були просто-напросто проінтегровані в поточні випуски продуктові лінійки іменитих брендів. Не мати у себе в антивірусі поведінковий блокує стало нефешенебельно і нерентабельно для більшості виробників [19][1)]. Пробитися в широкі кола і завоювати визнання тим стартапам до того, як їх купили, так і не вийшло. Безліч довіряє лише «великим іменам», великим світовим виробникам засобів реалізації інформаційного захисту, то вам доведеться почекати ще як мінімум років п'ять-десять, поки поточні інвестори не отримають свої кревні з захмарними відсотками. Звідки ж береться тіньова багатомільйонна економіка на образами програмному забезпеченні і її реалізації?

А береться вона з простого позитивного сальдо між вкраденими у простого користувача ресурсами і часом мінус вартість обходу засобів захисту [17][2)]. Все дуже просто, логічно і систематично. Яка ж насправді вартість обходу і злому сучасних антивірусних програмних засобів?

Беручи до уваги те, що епідемії трапляються із завидною регулярністю, а більшість користувачів все ж мають встановлений антивірусний продукт з регулярно оновлюваними сигнатурними антивірусними базами, то результат вельми невтішний - вартість обходу сучасного брендового антивіруса досить низька, щоб економіка на злоякісному програмному забезпеченні не мала ні найменшого шансу для існування і розвитку.

Досить просто підмінити або ще простіше, замаскувати модуль, обдуривши сигнатуру і прикинутися «добре себе поводячою» – все «оборона прорвана». Поки інформація здатна запобігти несанкціонованим і

[1)] [19] Партика Т.Л. Інформаційна безпека: Навчальний посібник для студентів закладів середньої проф. обр. 3-е изд., М.: Форум, 2008. 432 с. ISBN978-591134-246-3,3000

[2)] Записки дослідника комп'ютерних вірусів / К. Касперски. М .: Питер, 2006. 320 с. ISBN: 5-469-00331-0

неініціалізовані дії дійдуть від виробника до користувача, пройде левова частина цінного часу: годин, секунд ... Можна сміливо брати міста і країни, нікого, не боячись і нічого не побоюючись. А щоб антивірус більше не заважав своїми гучними вигуками і різними нагадуваннями, взяти, та й вимкнути його. Нічого складного і надприродного в цьому немає. І тільки принципово відмінні від уже торованих і стандартних методів реалізації захисту, а також інші підходи здатні настільки збільшити вартість обходу засобів захисту, що продовжувати «чорний» бізнес на програмному забезпеченні стане взагалі невигідним і немислимо дорогим. Чому? Розглянемо тіньову економіку обходу нових засобів захисту зсередини. Якщо не брати до уваги список реєстру вірусних підходів, то можна виділити всього два основоположних:

- на основі «білих списків» (тобто, забороняємо запуск і функціонування всього того, про що ми не знаємо, що воно свідомо гарне, незаражених вірусом);
- на основі популярної моделі «пісочниці», ізолюючи потенційно небезпечні процеси від всіх інших і операційної системи.

Багато представлених на даний момент рішення неприйнятні ні в одному масовому продукті, оскільки користувачеві дуже важко ними користуватися. Такі програми будуть із завидною частотою видавати неприйнятну кількість помилок як при оновленнях використовуваного програмного забезпечення, так і при виконанні своїх першочергових завдань, наприклад, поки вони не потраплять в єдину центральну базу, що зберігає величезну базу контрольних сум незаражених модулів. Крім того, на практиці всі подібні, здавалося б, на перший погляд унікальні технології рішення, мають вроджені і патогенні недоліки у вигляді проблем в роботі з файлами як архівними, так і з більш великим обсягом ніж в 10-15 Гбайт одним файлом, що містять скрипти , оскільки скрипт – це лише набір

звичайних текстових рядків, а інтерпретують і ініціалізують ці рядки команди до дії цілком собі легітимні (найчастіше – основні системні) виконувані файли [13] [1)]. Так що обійти їх або досить тривіально і легко, або практично неможливо і не реалізовується через одного чоловіка, хакером-одного чоловіка, хакером-одинаком (але і працювати з ними, при цьому, також буде практично дуже складно і довго). Якщо ж розглядати популярну останнім часом технологію захисту у вигляді SandBox, то знаходження дірок в них, які вже давно на світовій арені, досить нетривіальне завдання, але вирішуване при додатку деяких зусиль.

Завдання, посильна багатьом професійним хакерам, а їх численому угруповуванню тим більше, час яких коштує досить дуже дорого і під часту не по кишені навіть середньостатистичної компанії з персоналом в 200-300 чоловік. Вартість обходу добре реалізованої і виконаної з дотриманням всіх вимог «пісочниці» може вилитися замовнику в сотні тисяч і навіть мільйонів доларів і опинитися досить таки тривалою процедурою не тільки в очікувані, а й в впроваджені. [12] [2)].

При використанні або рішень на білих списках, або «пісочниць» бізнес на програмному забезпеченні і тіньовій економіці стає все менш і менш рентабельним, з кожною наступною итерацией захист стає все міцніше, а обхід її все дорожче. Також слід зазначити, що використання інноваційних сервісів і реалізація нових, ще невідомих хакерам і великому числу програмістів механізмів захисту, сприяє стабільності і стійкості такого глобального простору і безлічі імен як Інтернет. Лише реалізуючи і вчасно впроваджуючи нові технології можливе створення ідеального електронного

[1)] [13] Шаньгина В. Ф. Захист комп'ютерної інформації. Ефективні методи і засоби. М.: ДМК Пресс, 2010. 544 с. ISBN 978-5-94074-518-1

[2)] [12] Цирль В.Л.Основи інформаційної безпеки. Короткий курс. М.: Фенікс, 2008. 256 с. ISBN 978-5-222-13164-0б

світу, без виникнення «комп'ютерних» епідемій і крадіжки особистих конфіденційних даних.

3.4 Огляд сучасних ативірусних програм

3.4.1 Огляд AVP

Антивірус AVP є продуктом Лабораторії Касперського. Він надає користувачеві захист від вірусів, шпигунських програм, а також невідомих загроз за допомогою проактивного захисту, яка включає в себе компонент HIPS. Але він можливий лише в разі старших версій, іменованих «Kaspersky Internet Security 2009+, де '+' є порядковим номером попереднього регістру, щорічно збільшується на одиницю відповідно до номером року, наступним за роком випуску чергової версії антивіруса » .

Основні функції AVP відображені в табл. 1.

Таблиця 1− Основні функції AVP

Функція	Її характеристика
Базовий захист	– захист від вірусів, троянських програм і хробаків; – захист від шпигунських та рекламних програм; – перевірка файлів в автоматичному режимі і на вимогу; – перевірка поштових повідомлень (для будь-яких – поштових клієнтів); – перевірка інтернет-трафіку (для будь-яких інтернет-браузерів); – проактивний захист від нових шкідливих програм; – перевірка Java і Visual Basic-скриптів; – захист від прихованих битих посилань; – постійна перевірка файлів в автономному режимі; – постійний захист від фішингових сайтів.
Запобігання загроз	– пошук вразливостей в ОС і встановленому ПЗ; – аналіз і усунення вразливостей в браузері Internet Explorer; – блокування посилань на заражені сайти;

Функція	Її характеристика
	– розпізнавання вірусів за способом їх встановлення; – глобальний моніторинг загроз (Kaspersky – Security Network).

Продовження табл. 1

Функція	Її характеристика
Відновлення системи і даних	– можливість установки програми на заражений комп'ютер; – функція самозахисту програми від – вимкнення або зупинки; – відновлення коректних налаштувань системи після видалення шкідливого ПЗ; – наявність інструментів для створення диска аварійного відновлення.
Захист конфіденційних даних	– блокування посилань на фішингові сайти; – захист від всіх видій кейлогерів.
Зручність використання	– зручність використання автоматичного налаштування програми в процесі установки; – готові рішення (для типових проблем); – наочне відображення результатів роботи програми; – інформативні діалогові вікна для прийняття користувачем обгрунтованих рішень; – можливість вибору між простим (автоматичним) та інтерактивним режимами роботи; – цілодобова технічна підтримка; – автоматичне оновлення баз.

У цього антивіруса є дві модифікації: Kaspersky Anti-Вірус Personal і Kaspersky Anti-Virus Personal Pro. Розберемося, які між ними існують

відмінності. Основна відмінність версії Pro – унікальні можливості захисту документів від макровірусів, а також можливість стеження за вмістом диска. Йдеться про наявність таких компонентів, як Office Guard, інтегрований в середу MS Office 2000 / XP, і Inspector. Головна перевага Office Guard, в основу якої лягли принципи поведінкового блокіратора, полягає в тому, що на відміну від класичних антивірусів, які виявляють віруси по унікальному програмного коду (т. е. послідовності символів), Office Guard блокує шкідливі макроси по властивій їм поведінці. Ця здатність виключає саму можливість функціонування макровірусів. Що не має аналогів в світі ревізор Inspector відстежує всі можливі зміни на диску і по команді користувача відновлює модифіковані файли і завантажувальні сектора. Програма значно скорочує час перевірки дисків антивірусним сканером, так як після закінчення перевірки дисків на зміни , Inspector може передати на перевірку сканера тільки нові і змінені файли. Існує ще одна утиліта від Лабораторії Касперського – Kaspersky Virus Removal Tool. Вона є безкоштовною антивірусною утилітою від всесвітньо відомої компанії «Лабораторія Касперського». AVPTool призначена для боротьби з вірусами і будь-якими шкідливими додатками. Але варто відзначити, що дана програма не є повноцінним антивірусом, проте здатна сканувати жорсткий диск комп'ютера і виявляти заражені файли, видаляючи їх або ізолюючи в карантин.

До головних особливостей Kaspersky Virus Removal Tool можна віднести наступні:

- досить зручний і простий інтерфейс програми;
- можливість інсталяції на уражену вірусами комп'ютер (в тому числі − в безпечному режимі операційної системи);
- комплексна перевірка комп'ютера;
- можливість як автоматичного, так і ручного лікування комп'ютера від вірусів, шкідливих програм, троянів;

– можливість лікування комп'ютера від рекламного і шпигунського програмного забезпечення як в ручному, так і в автоматичному режимі;

– лікування в ручному і автоматичному режимі комп'ютера від всіляких видів руткітів.

Мабуть, одним з основних переваг Kaspersky AVPTool є той факт, що ця антивірусна програма не конфліктує з будь-якими іншими антивірусами, це дає можливість використовувати її, як засіб для забезпечення додаткового рівня захисту комп'ютера. Також додана функція запуску з флешки, тому не обов'язково встановлювати програму на комп'ютер, якщо можна запустити її з флешнакопітеля, тим більше, що розробники самі заявили, що дана утиліта призначена строго для оперативного виявлення і видалення, або ізоляції заражених файлів. Однак в якості постійного антивірусного рішення для забезпечення безпеки комп'ютера ця програма не підходить - для цього необхідний антивірус, який буде функціонувати в постійному, штатному режимі, наприклад, Kaspersky CRYSTAL. Однак, хоч ця версія безкоштовна, в ній також є свої недоліки. Наприклад, Kaspersky Virus Removal Tool не в змозі забезпечити захист системи в реальному часі. Крім того, в програмі відсутня модуль автоматичного оновлення вірусних сигнатур, а це означає, що для кожної нової перевірки комп'ютера на наявність вірусів необхідно буде заново завантажити програму з новими антивірусними базами. Однак і ці недоліки не зможуть перекрити переваги цієї антивірусної утиліти.

3.4.2 Огляд Norton Antivirus

Norton Antivirus – це антивірусна програма, яка випускається американською компанією Symantec. Остання версія вийшла в 2014 році. Компанія Symantec більше 15 років представляє свою продукцію на ринку професійних програмних засобів, щоб забезпечити максимальну продуктивність і безпеку робочих станцій і серверів. Компанія вважається

визнаним лідером майже у всіх секторах ПЗ, де представлені програми компанії, включаючи антивірусні рішення і службові пакети.

До основного переліку функцій Norton Antivirus відносяться наступні:

– автоматично видаляє віруси, "хробаків", "троянські" програми;
– перевіряє і знешкоджує вхідні і вихідні повідомлення електронної пошти;
– виявляє і блокує віруси в файлах, вкладених в повідомлення служби обміну миттєвими повідомленнями;
– автоматично завантажує оновлення системи антивірусної безпеки для захисту від нових загроз;
– технологія Worm Blocking дозволяє виявляти зараження "Хробаками" (такими, як Nimda) у вихідних поштових повідомленнях;
– технології Script Blocking і Worm Blocking дозволяють виявити нові загрози ще до того, як для них буде створений опис вірусів;
– передбачені покрокові інструкції для установки програми, в тому числі, і на заражені вірусами системи.

Ще одним плюсом є надання інформації про продуктивність, а також необхідні попередження, що стосуються вірусних загроз. У Norton Antivirus присутній відмінна функція, яка відображає вплив різних файлів і програм на фунціональность і продуктивність комп'ютера, а також походження таких файлів. Програми здатна оцінити загрози файлів ще до їх завантаження. Прога швидко знаходить навіть приховані cookie і без праці їх видаляє. Цікавою новинкою можна вважати Norton Bootable Recovery Tool. Цей засіб дає можливість вилікувати навіть такі комп'ютери, які черезвелику міру зараженості можуть не завантажуватися.

Функціональність інструментів, пропонованих антивірусом Norton Antivirus, говорить про її однозначних переваги і приналежності до категорії

сучасного антивірусного програмного забезпечення найвищого класу. Даний продукт популярний, тому що є високоякісним, чим користуються пірати комп'ютерного ПО, продаючи на ринок велику кількість неякісних копій цього антивіруса. Фірма-розробник змушена застосовувати більш досконалі способи захисту своїх програм.

З 2004 року Symantec вводить додаткову процедуру активації програми. Цей захід спрямований на боротьбу з масовим піратством. цей захід не гарантує тільки ліцензійне використання програми, але для піратів необхідність активувати програму представить додаткові проблеми.

Технології, які використовуються Norton Antivirus, представлені в таблиці нижче (табл. 2)

Таблиця 2 – Технології Norton AntiVirus і їх короткий опис

Технологія	Короткий опис
Striker32	Технологія призначена для виявлення вірусів і відновления даних, пошкоджених найбільш складними вірусами, що часто неможливо здійснити за допомогою звичайних антивірусних засобів.
Bloodhound	Технологія евристичного аналізу дозволяє виявляти нові і невідомі макровіруси , використовуючи власну евристичну технологію. Bloodhound може автоматично пропускати чисті файли і затримувати інфіковані ще до активації вірусів
Navex	Технологія дозволяє оновлювати антивірусний механізм (антивірусну базу та саму програму) Norton AntiVirus для визначення нових типів вірусів. Сканування та інсталяція відбуваються автоматично.
Worm Blocking	Технологія призначена для нейтралізації "черв'яків" у вихідній пошті і запобігання їх подальшого поширення на інші комп’ютери.

Script Blocking	Технологія забезхпечує захист від швидко поширюваних вірусів на основі скриптів.

3.4.3 Огляд Dr Web

Dr.Web – це загальна назва сімейства програмного антивірусного ПЗ для різних платформ (Windows, OS X, Linux,мобільні платформи) і лінійки програмно-апаратних рішень (Dr.Web Office Shield), а також рішень для забезпечення безпеки всіх вузлів корпоративної мережі. Розробляється компанією «Доктор Веб». Dr.Web CureIt! ідеально підходить для ситуацій, коли установка антивіруса виявляється неможливою в результаті дій вірусів або по будь-якій іншій причині, тому що він не вимагає установки, працює під 32- і 64-бітними операційними системами сімейств Microsoft Windows і Microsoft Windows Server і постійно оновлюється і доповнюєтьсясвіжими вірусними базами, що забезпечує ефективний захист від вірусів і інших шкідливих програм. Крім цього, Dr.Web CureIt! автоматично визначає мову, яку використовує операційна система.

Продукти захищають комп'ютер від вірусів, троянського, шпигунського та рекламного ПЗ, хробаків, руткітів, хакерських утиліт, програм-жартів, а також невідомих загроз з допомогою різних технологій реального часу і превентивного захисту.

До основних технологій відносяться:

- можливість установки антивіруса на заражений комп'ютер;
- виявлення і лікування складних, шифрованих вірусів і руткітів;
- можливість налаштування копіювання важливих даних в захищене сховище, що дозволяє користувачам самостійно відновлювати пошкоджені дані без необхідності звернення до служби технічної підтримки.

Підтримка більшості існуючих форматів упакованих файлів і архівів, в тому числі багатотомних саморозпаковуються архівів. Компактна вірусна база і невеликий розмір оновлень. Один запис у вірусній базі дозволяє визначати до тисячі подібних вірусів. Оновлення вірусних баз виробляються в міру виявлення нових вірусів, до декількох разів на годину. Розробники антивірусного продукту відмовилися від випуску оновлень вірусних баз по якомусь графіку, оскільки вірусні епідемії не підкоряються таким. Кросплатформеність – використовується єдина вірусна база і єдине ядро антивірусного сканера на різних платформах ОС. Низький вплив на продуктивність системи. Завдяки технологіям оптимізації, свідомо чисті файли не перевіряються компонентами Dr.Web, що знижує навантаження на систему. До унікальним технологіям Dr. Web відносяться технології, представлені в табл. 3.

Таблиця 3 – Унікальні технології Dr.Web і їх характеристики

Технологі	Характеристики
Fly-code	Емулятор з динамічною трансляцією коду, реалізує механізм універсального розпакування вірусів, захищених від аналізу та детектування одним або ланцюжком нових або невідомих пакувальників. Це дозволяє розпакувати файли, захищені, наприклад, ASProtect, EXECryptor, VMProtect і тисячами інших пакувальників і протекторів, включаючи невідомі антивірусу.
Origins Tracing	Послідовність дій по виявленню шкідливих об'єктів, доповнює традиційний евристичний аналізатор, який дає можливість значно підвищити рівень детектування раніше невідомих шкідливих программ.Також використовується в Dr.Web для Android.
Anti-rootkit API (ArkAPI)	Підсистема, використовуює універсальні алгоритми нейтралізації загроз. Завдяки цій системі нейтралізується загроза всіма компнентами антивіруса. Також використовуєтьсяв Dr.Web Curelt.
Dr.Web	Механізм боротьби з руткітами, реалізований в вигляді

Shield	драйверу. Забезпечує низькорівневий доступ до вірусних об’єктів, захованих в глибинах ОС.
SelfPROtect	Модуль самозазисту захищає компоненти антивіруса (файли, ключі реєстру, процеси) від зміни та видалення злоякісним ПЗ.

Продовження табл..3

Технологія	Характеристики
Dr.Web Cloud	Сервіс перевірки посилань і файлів на серверах компанії Doctor Web в режимі реального часу дозволяє антивірусу використовувати найбільш свіжу інформацію про небезпечні ресурси та файли.
Dr.Web Process Heuristic (DPH)	Технологія реального часу,яка захищає від нових. Найбільш актуальних злоякісних програм, розлоблених з розрахунком на не знахождення традиційними сигнатурними і евристичними механізмами, які ще не поступили на аналіз в антивірусну лабораторію, що означає їх невідомими для антивірусної бази Dr.Web на момент проникнення в систему.
Dr.Web Process Dumper (DPD)	Технологія реального часу, значно підвищує рівень детектування нових загроз – відомих вірусній базі Dr.Web, але закртих під новими пакувальниками.
Dr.Web HyperVisor	Компонет підготовлений до запуску та роблячий нижче рівня операційної системи, що забезпечує контроль всіх програм, процесів і роботи самої ОС, а також неможливість перехоплення злоякісними програмами контролю понад захищеною Dr.Web системою.
Dr.Web ShellGuard	Технологія, яка закриває шлях в комп’ютер для експлойтів – злоякісних об’єктів, які намагаються використовувати уразливості, в тому числі ще не відомі нікому , крім вірусописьменниками (уразливістю нульового дня), з цілью отримання контролю над атакуючими додатками або операційною системою в цілому.

3.4.4 Огляд ESET NOD32

NOD32 – антивірусний пакет, що випускається словацькою фірмою Eset. Виник в кінці 1998 року. Назва спочатку розшифровувалася як Nemocnica na Okraji Disku («Лікарня на краю диска», перефразована назва популярного тоді в Чехословаччині телесеріалу «Лікарня на околиці міста»).

Велика частина коду антивіруса написана на мові асемблера, тому для нього характерно мале використання системних ресурсів і висока швидкість перевірки з налаштуваннями за умовчуванням.

Модулі і компоненти:

- NOD32 − повідомлення про вірус;
- Antivirus MONitor (AMON);
- On-access (резидентний) сканер, який автоматично перевіряє файли перед здійсненням доступу до них;
- NOD32«On-demand» сканер, який можна запустити уручну для перевірки окремих файлів або сегментів диска. Цей модуль можна також запрограмувати на запуск в години з найменшим завантаженням;
- Internet MONitor (IMON);
- резидентний сканер, що працює на рівні Winsock і що перешкоджає попаданню заражених файлів на диски комп'ютера. Даний модуль перевіряє Інтернет-трафік (HTTP) і вхідну пошту, отриману по протоколу POP3;
- E-mail MONitor (EMON);
- додатковий модуль для перевірки вхідних/вихідних повідомлень через інтерфейс MAPI, наприклад, в Microsoft Outlook і Microsoft Exchange;

– Document MONitor (DMON)Використовує запатентований інтерфейс Microsoft API для перевірки документів Microsoft Office (включаючи Internet Explorer).

4 ОПИС КОНСОЛЬНОГО АНТИВІРУСУ В СЕРЕДОВИЩІ C++

4.1 Постанова задачі

Створити консольний додаток в VC++ з використанням інтегрованого середовища розробки Microsoft Visual Studio. Консольний додаток запускає файл для сканування (рис. 6) і виконується його обробка з використанням антивірусної бази даних в результаті чого отримуємо оброблений файл представлений на рис. 7

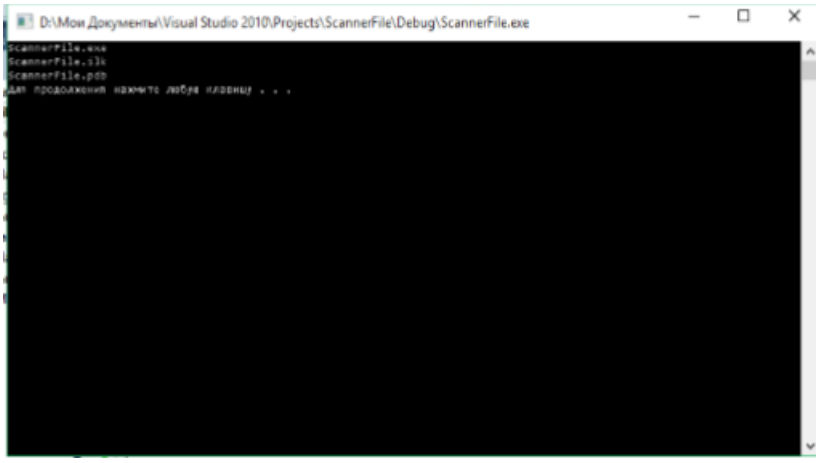

Рисунок 6 − Загрузка та перевірка файлу на віруси

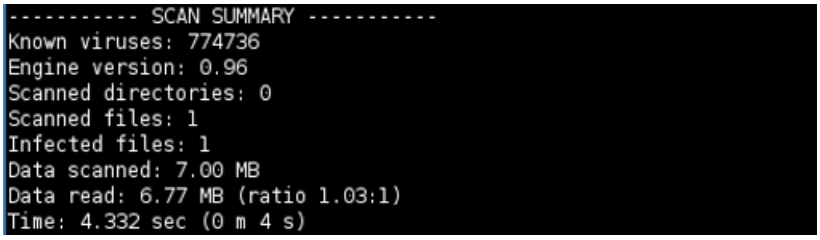

Рисунок 7 − Файли оброблені сканером

Налаштування і запуск VISUAL STUDIO

Створення нового проекту в Visual Studio 2010: Додати

1. Файл → Створити → Проект (File → New → Project) (рис. 8);

2. Виберіть Visual C ++ → Win32 (рис. 9) ;

3. Виберіть "Консольний додаток Win32" (Win32 Console Application) (рис. 10);

4 . Введіть назву нового проекту і натисніть "ОК" ;

5. Натисніть "Готово" (Finish) ;

6.У вікні редактора кодів здійснюється введення та обробка безпосереднього коду програми або модуля. (рис. 11).

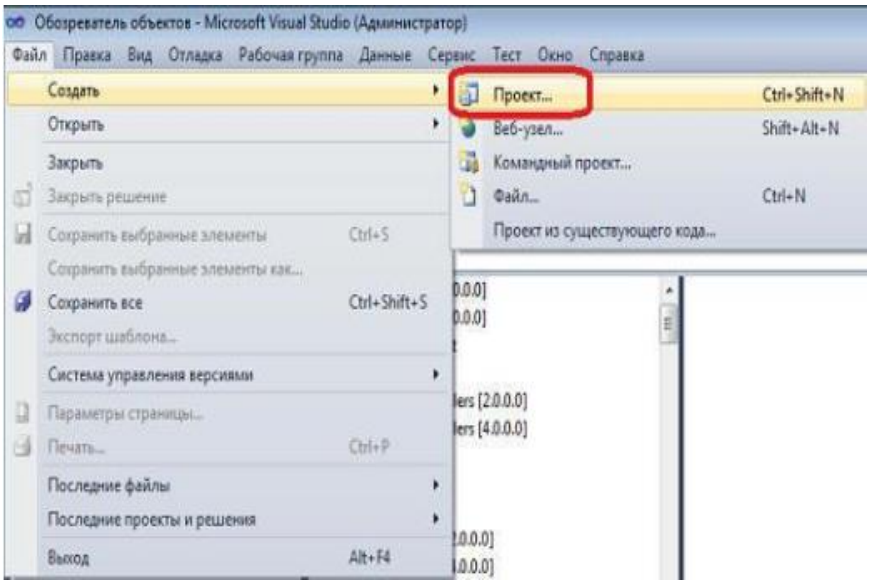

Рисунок − 8 Приклад створення проекту

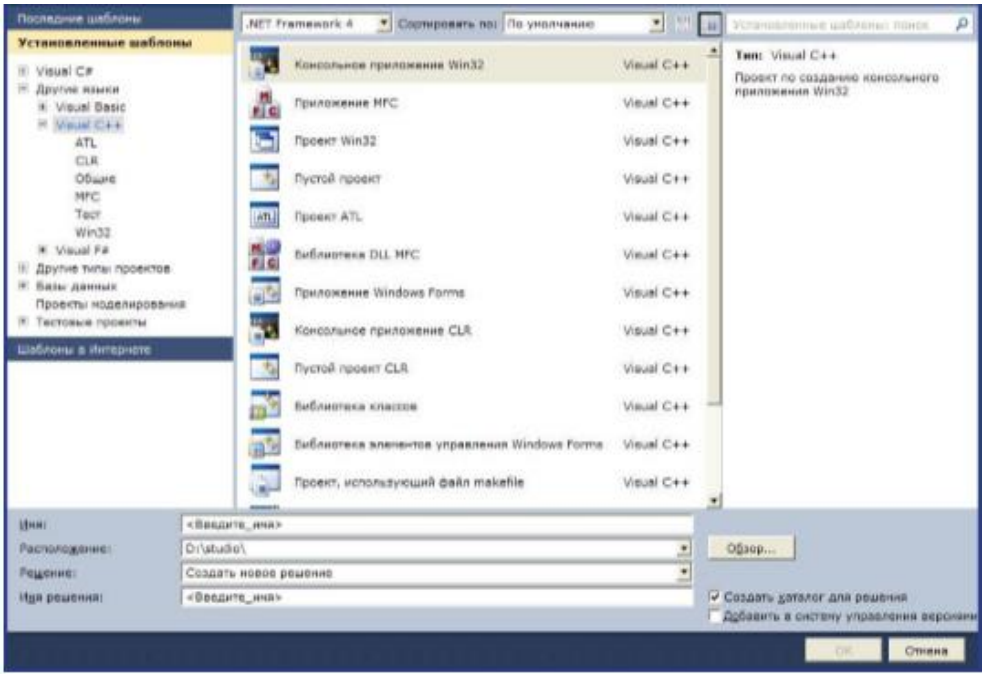

Рисунок 9 − Visual C ++ → Win32

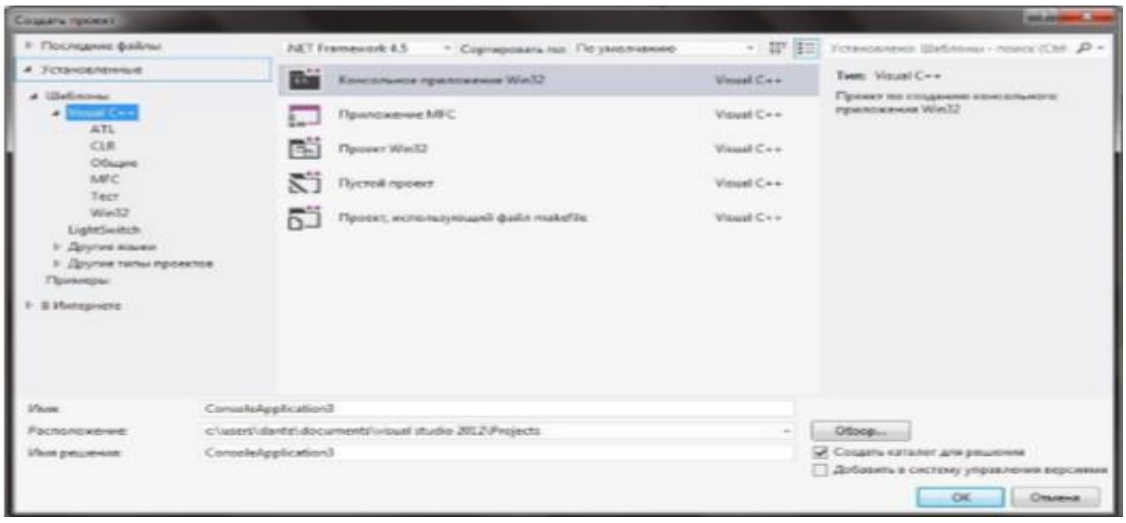

Рисунок10 − Консольний додаток Win32

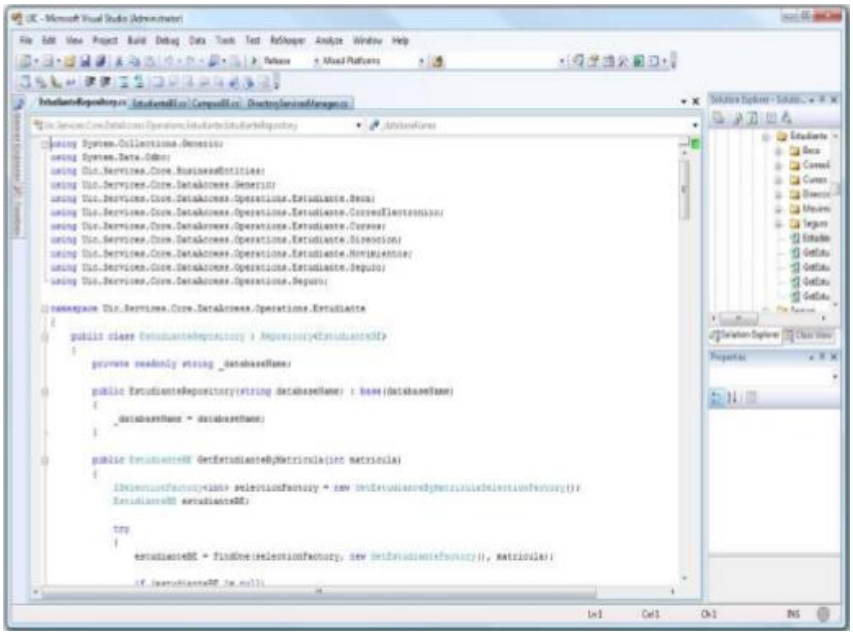

Рисунок 11 − Вікно-редактор коду

4.2 Алгоритмізація вирішення завдання

4.2.1 Опис методу рішення

Для вирішення завдання використане середовище програмування Visual Studio C ++. Програма розроблена як консольний додаток з використанням функції main. При запуску програми виконується

завантаження файлів з локального сховища (жорсткого диска), потім програма починає обробку (ініціалізацію) файлу і пошук шкідливого коду. В силу простоти алгоритму виявлення шкідливого коду наш сканер зможе знаходити тільки шкідливі програми, що поширюються цільним файлом, тобто не заражають інші файли, як PE-Віруси, і не змінюють свою дію в процесі своєї діяльності, як поліморфні віруси.

4.2.2 Алгоритм роботи сканера

Алгоритм роботи сканера, що використовує антивірусні сигнатури, можна представити у вигляді декількох основних пунктів:

- завантаження бази сигнатур;
- відкриття перевіряється файлу;
- пошук сигнатури в відкритому файлі;
- якщо сигнатура знайдена − прийняття відповідних заходів;
- якщо жодна сигнатура з бази не знайдена − закриття файлу і перехід до перевірки наступного сканер для роботи необхідні сигнатури, які зберігаються в антивірусній базі даних. База створюється і наповнюється спеціальною програмою. Сигнатура буде складатися з;
- зміщення послідовності в файлі;
- розміру послідовності;
- кешу послідовності.

4.3 Структура програми

Програма написана на мові C++ с використанням платформи інтегрованого програмування Microsoft Visual Studio і працює під управлінням операційних систем типу Windows. Для успішного виконання роботи програми досить мати встановлену на машині Microsoft Visual Studio

не нижче 2010, і файл ZAVBFile.cpp. Виконавчий код (ZAVBFile.cpp) займає на диску всього 4 КБ.

Оригінальний текст програми містить основну частину (функція main). Виконання програми починається з функції main. Ця функція не має параметрів і значень. Також робота програми завершується при натисканні клавіші, клавіша служить виходом з програми.

4.4 Аналіз результатів

В результаті виконання роботи розроблена програма на мові C++ в середовищі Microsoft Visual Studio 2010 реалізує процес, описаний на початку глави. Процес роботи програми наочно відображається на екрані. В результаті роботи програми на виході маємо оброблений раніше заражений файл відмінний від вихідного.

ВИСНОВОК

В процесі дослідження мною були вивчені методи роботи та функції вірусів і антивірусів, обробка, фільтрація та індетифікація інфікованих файлів, також їх знешкодження, в результаті чого набув практичних навичків в цих областях. Для цього використовувалася головна початкова функція main, яка забезпечувала всю правильну та необхідну роботу консольної програми. В результаті досліджень були застосовані такі програмні засоби :

- русифікована і ліцензована прикладна система розробки: Microsoft Visual Studio 2010x32;
- вільно розповсюджена бібліотека сигнатури антивірусних баз від Clam AV.

В ході дослідження були вирішені наступні завдання:

- вивчити наукову літературу і технічну документацію з обраної теми;
- провести аналіз функціонування, як вірусів, так і антивірусів;
- розробити програму по виявленню «небезпечних» ділянок коду і їх знешкодження.

ПЕРЕЛІК ПОСИЛАНЬ

1. Лабораторія Касперського. URL: http://securelist.ru/ (Дата звернення 30.04.2020).
2. Михайлов А.В. Комп'ютерні віруси і боротьба з ними. М.: ДіалогМІФІ, 2011. 104 с. ISBN 978-5-86404-236-6.
3. Шаньгина В.Ф. Інформаційна безпека комп'ютерних систем і мереж: Навчальний посібник. М.: ИД ФОРУМ: ИНФРА-М, 2012. 416 с. ISBN 9785-8199-0331-5 1000.
4. Климентьєв К. Е. Комп'ютерні віруси і антивіруси. Погляд програміста. М.: ДМК-Пресс, 2013. 656 с. ISBN: 978-5-94074-885-4.
5. Інформаційні технології. URL: http://habrahabr.ru/ (Дата звернення 02.05.2020).
6. Цирль В.Л. Основи інформаційної безпеки. Короткий курс. М.: Фенікс, 2008. 256 с. ISBN 978-5-222-13164-0.
7. Рейтинги антивірусів. URL: http://it-sektor.ru/proplachennaya-stat-ya-ili-kaknakruchivaut- reyiting-antivirusov.html (Дата звернення 02.05.2020).
8. Касперски К. Комп'ютерні віруси зсередини і зовні. М.: Питер, 2006. 526 с. ISBN 5-469-00982-3 .
9. Трасковскій А. В. Збої і неполадки домашнього ПК. 2-е изд., СПб.: БХВ-Петербург, 2009. 512 с. ISBN 978-5-94157-964-8.
10. Михайлов А.В. Комп'ютерні віруси і боротьба з ними. М.: ДіалогМІФІ, 2011. 104 с. ISBN 978-5-86404-236-6 .
11. Касперски К. Комп'ютерні віруси зсередини і зовні. М.: Питер, 2006. 526 с. ISBN 5-469-00982-3 http://al24.ru/pdf_kniga_2663.html.
12. Шаньгина В.Ф. Захист комп'ютерної інформації. Ефективні методи і засоби. М.: ДМК Пресс, 2010. 544 с. ISBN 978-5-94074-518-1.

13. Хто і навіщо пише віруси. URL: http: //zillya.ua/ru/kto-i-zachem-pishetvirusy (Дата звернення 05.05.2020).
14. Всесвітня історія заражень. URL:http://lenta.ru/articles/2014/11/18/virus/ (Дата звернення 05.05.2020).
15. Центр дослідження комп'ютерної злочинності URL:http://crimeresearch.ru/. (Дата звернення 08.05.2020)
16. Касперски К. Записки дослідника комп'ютерних вірусів. М.: Питер, 2006. 320 с. ISBN: 5-469-00331-0 .
17. Роббінс Д. Налагодження Windows-додатків. М.: ДМК Пресс, 2009. 448 с. ISBN 5-94074-085-5.
18. Партика Т.Л. Інформаційна безпека: Навчальний посібник для студентів закладів середньої проф. обр. М.: Форум, 2008. 432 с. ISBN978-591134-246-3.

ДОДАТОК

Консольний антивірус C++

Код програми (Лістинг)
Код на мові VC++:

```
//zoternik ZAV
 //подключение библиотек
 #include <cv.h>
#include <highgui.h>
 #include <stdlib.h>
 #include <stdio.h>
int main(int argc, char* argv[])
ZAVBFile::ZAVBFile () {
this->RecordCount = 0;
}
//! Закрытие файла
void ZAVBFile::close(){
if(hFile.is_open()) hFile.close();
 }
  //! Проверка состояния файла
 bool ZAVBFile::is_open(){
 return hFile.is_open();
 }
  //! Получение числа файлов
  DWORD ZAVBFile::getRecordCount (){
 return this->RecordCount;  }
//! Открытие файла
bool ZAVBFileWriter::open(PCSTR FileName){
if (FileName == NULL) return false;
// - Если файл не найден то создаем его прототип
if(!isFileExist(FileName)){
hFile.open(FileName, ios::out | ios::binary);
if(!hFile.is_open()) return false;
hFile.write("AVB", 3);// - Сигнатура файла
hFile.write((PCSTR)&this->RecordCount,   sizeof(DWORD));   //   -
Число записей
// - Иначе открываем и проверяем валидность
}else{
hFile.open(FileName, ios::in | ios::out | ios::binary);
if (!hFile.is_open()) return false;
// - Проверка сигнатуры
CHAR Sign[3];
hFile.read((PSTR)Sign, 3);
if(memcmp(Sign, "AVB", 3)){
hFile.close(); // - Это чужой файл
return false;
```

```
}
// - Читаем число записей
hFile.read((PSTR)&this->RecordCount, sizeof(DWORD));
}
return true;
}
bool ZAVBFileWriter::addRecord(PSAVRecord Record){
if (Record == NULL || !hFile.is_open()) return false;
// - Перемещаемся в конец файла
hFile.seekp(0, ios::end);
// - Добавляем запись
hFile.write((PSTR)&Record->Signature.Offset,  sizeof(DWORD));  //
- Смещение сигнатуры
hFile.write((PSTR)&Record->Signature.Lenght,  sizeof(DWORD));  //
- Размер сигнатуры
hFile.write((PSTR)&Record->Signature.Hash,  sizeof(DWORD)); //  -
Контрольная сумма
hFile.write((PSTR)&Record->NameLen,  sizeof(BYTE));  //  -  Размер
имени
hFile.write((PSTR)Record->Name, Record->NameLen); // - Имя
// - Смещаемся к числу записей
hFile.seekp(3, ios::beg);
// - Увеличиваем счётчик записей
this->RecordCount++;
hFile.write((PSTR)&this->RecordCount, sizeof(DWORD));
return true;
}
bool ZAVBFileReader::open(PCSTR FileName){
if(FileName == NULL) return false;
// - Если файл не найден, то создаем его прототип
if(isFileExist(FileName)){
hFile.open(FileName, ios::in | ios::out | ios::binary);
if(!hFile.is_open()) return false;
// - Проверка сигнатуры
CHAR Sign[3];
hFile.read((PSTR)Sign, 3);
if(memcmp(Sign, "AVB", 3)){
hFile.close(); // - Это чужой файл
return false;
}
// - Читаем число записей
hFile.read((PSTR)&this->RecordCount, sizeof(DWORD));
}else{ return false; }
return true;
}
boolZAVBFileReader::readNextRecord(PSAVRecord Record){
if(Record == NULL || !hFile.is_open()) return false;
hFile.read((PSTR)&Record->Signature.Offset, sizeof(DWORD)); // -
Смещение сигнатуры
```

```
hFile.read((PSTR)&Record->Signature.Lenght, sizeof(DWORD)); // -
Размер сигнатуры
hFile.read((PSTR)&Record->Signature.Hash, *sizeof(DWORD)); // -
Контрольная сумма
hFile.read((PSTR)&Record->NameLen, sizeof(BYTE)); // - Размер
имени
Record->allocName(Record->NameLen);
hFile.read((PSTR)Record->Name, Record->NameLen); // - Имя
  return true;
}
```