Министерство образования Республики Беларусь

Учреждение образования  
«Белорусский государственный университет  
информатики и радиоэлектроники»

Факультет компьютерных сетей и систем

Кафедра электронный вычислительных машин

Дисциплина: Системное программирование обеспечение вычислительных   
машин

К ЗАЩИТЕ ДОПУСТИТЬ

\_\_\_\_\_\_\_\_\_\_\_И. И. Фролов

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА  
к курсовой работе  
на тему

Кроссплатформенный вирус, распространяющийся по USB

БГУИР КР 1-40 02 01 304 ПЗ

Студент А.С. Веденичев

Руководитель М. Г. Базанов

МИНСК 2018

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ

[**ВВЕДЕНИЕ** 3](#_Toc516235558)

[**1 ПОСТАНОВКА ЗАДАЧИ** 4](#_Toc516235559)

[**2 ОБЗОР ЛИТЕРАТУРЫ** 5](#_Toc516235560)

[**3 СТРУКТУРА ВЫХОДНЫХ ДАННЫХ** 9](#_Toc516235561)

[**5 ОПИСАНИЕ ФУНКЦИЙ** 13](#_Toc516235562)

[**6 РАЗРАБОТКА ПРОГРАММНЫХ МОДУЛЕЙ** 14](#_Toc516235563)

[**ЗАКЛЮЧЕНИЕ** 16](#_Toc516235564)

[ПРИЛОЖЕНИЕ А 18](#_Toc516235565)

[ПРИЛОЖЕНИЕ Б 19](#_Toc516235566)

[ПРИЛОЖЕНИЕ В 20](#_Toc516235567)

# **ВВЕДЕНИЕ**

С помощью языка Си можно решать различные задачи, начиная от простых консольных приложений, заканчивая готовым коммерческим программным продуктом. С появлением компьютеров и языков программирования, появились и вирусы. Первые вирусы появились в прошлом веке нашего столетия, а термин «компьютерный вирус» появился позднее.

Компьютерный вирус - это реализованная небольшая по размерам программа, которая может «добавлять» себя к другим программам, выполнять различные зловредные действия на электронном вычислительном оборудовании. Программа, в которой содержится вирус, называется «зараженной». Когда такая программа начинает работу, то сначала управление получает не пользователь, а вирус. Вирус ищет и «заражает» программы, а также выполняет зловредные действия, которые в последствие парализуют работу компьютера или вычислительной техники (например, заменяет и добавляет свой код в исполняемые файлы программ или MFT-таблицу, «засоряет» переполняет оперативную память, свободное пространство на жестком диске и т.д.). Компьютерный вирус может испортить все ваши данные включая фотографии, которые были хорошим поводом вспомнить приятные моменты, видеофайлы, аудиофайлы и что немаловажно вывести из строя аппаратную «начинку» вашего любимого электронного помощника.

# **1 ПОСТАНОВКА ЗАДАЧИ**

В рамках курсового проекта необходимо разработать исследовательский вирус, распространяющийся по сети для операционной системы Windows.

# **2 ОБЗОР ЛИТЕРАТУРЫ**

В наше непростое информационное время известно несколько тысяч разновидностей вирусов. По опасности для операционной системы вирусы могут быть безобидными, которые кроме самокопирования больше ничем 7 не занимаются, до фатальных, которые вследствие своих действий приво- дят к разрушению всей системы и аппаратной части электронных схем.

По принципу действия рассмотрим фундаментальные разновидности вирусов:

Загрузочные вирусы используют основной (boot) сектор Master Boot Record (MBR) жесткого диска или винчестера для заражения, также такие вирусы получили большее распространение при использовании флэш карт для хранения данных. Так при вставке, зараженной «флешки» в компьютер загрузочный вирус инъецирует и сам компьютер. Принцип действия загрузочных вирусов строится на алгоритмах внезапности захвата запуска операционной системы при включении или перезагрузке компьютера.

Файловые вирусы. К данной группе относятся вирусы, которые при своем зловредном действии тем или иным способом используют файловую систему хранения какой-либо ОС (Операционной системы) исполняемой на компьютере. Файловые вирусы - вредители используют практически все исполняемые файлы всех известных используемых ОС в мире. В настоящее время известны вирусы: наносящие вред всем типам выполняемых объектов стандартной ОС; поражающие основные файлы других операционных систем - Windows 6.x, UNIX, Slackware, Oracle OS, включая заражения драйверов для взаимодействия аппаратной части компьютера с программным обеспечением. Существуют вирусы, которые имеют оригинальные тексты программ, библиотечные или объектные модули.

Макровирусы (macro viruses) являются также программным продуктом написанном на макроязыках, встроенных в системы обработки данных (табличные процессоры, текстовые процессоры и т.д.). Макровирусы записывают свой код в файлы данных – в основном это документы, набранные в текстовом редакторе или электронные таблицы. Для своего развития такие вирусы используют возможности макроязыков и при их по- мощи переносят сами себя из одного зараженного ими же файла (файла- документа или таблицы) в другие незараженные. Очень распространёнными на данный момент являются вирусы, которые непосредственно используют и заражают пакет офисной платформы Microsoft Office.

Стелс-вирусы любыми способами и средствами скрывают свой факт присутствия в системе. Известны стелс-вирусы почти всех типов, за исключением Windows-вирусов и вирусов, написанных под Unix системы. При попытке обнаружения стелс-вирус маскирует себя под безобидную программу, выдавая ложный «чистый» код.

К полиморфным вирусам относятся те из них, обнаружение кото- рых очень затруднительно или невозможно осуществить при помощи анти- вирусных сигнатур - участков основного кода, специфичных для рассмат- риваемого вируса. Данное свойство вируса достигается за счет использова- ния двух основных способов – шифрованием тела вируса с непостоянным ключом и генерируемым набором команд расшифровщика или самогенера- цией кода выполняемого вируса [9]. Полиморфизм разных уровней сложности встречается в вирусах по- чти всех типов и видов - от загрузочных и файловых Windows-вирусов и даже макровирусов.

Резидентные вирусы. Под понятием "резидентность" (TSR - Terminate and Stay Resident) понимается способность вирусов оставлять свои следы пребывания в оперативной памяти компьютера, перехватывать события (например, обращение к папке или разделу жесткого диска) и при этом запускать механизмы заражения «чистых» файлов. Таким образом, резидентные вирусы выполняют свою работу, приносящую вред, не только во время использования пользователем какой-либо программы, но и после того, как программа закрывается и далее не используется пользователем.

Нерезидентные вирусы, очень активно проявляют себя в короткий промежуток времени - только в момент загрузки зараженной ими же программы. Для своего развития они ищут незараженные файлы на диске и заражают их изнутри. После закрытия зараженной программы вирусом их действие и влияние на саму ОС сводится к нулю. Поэтому, зараженные файлы, с которыми поработал нерезидентный вирус значительно проще вылечить, нежели удалить файл целиком.

Черви. IRC (Internet Relay Chat) - это протокол, используемый для коммуникации пользователей в сети Интернет в реальном времени. Этот, протокол, один из многочисленных позволяет пользователям общаться между собой посредством Интернет "разговора" при помощи специальных программ, разработанных на должном уровне. Также в данных программах существует возможность обмена различными типами файлов - именно данную функцию и используют IRC-черви.

К сетевым относятся вирусы, которые распространяются посредством перемещения по глобальной сети, в частности во всемирной паутине. «Завершенные» сетевые вирусы могут заставить пользователя запустить вирус на своём компьютере, и пользователь сам того не замечая заражает свой компьютер.

Мобильные вирусы - это специализированное вредоносное ПО, разработанное для небольших гаджетов, имеющей своей основной целью получение конфиденциальной информации. В основном хозяева своих электронных питомцев и не подозревают о том, что их устройство заражено и несет собой вред не только для него самого, но и для окружающих, путем передачи данных через открытые точки доступа Wi-fi и 3G, а также - все реже Bluetooth [19]. Мобильные вирусы способны передавать и перехватывать смс сообщения на лету, что делает их почти незаметными, также более-менее современные, адаптированные вирусы записывают разговоры, архивируют действия пользователя и собирают информацию о частной жизни собственника гаджета. Легендарными и распространенными мобильными вирусами, в наше время являются: Cabir, Comwar, Brador, Viver а также, их многомиллионные доработанные и усовершенствованные собратья, способные узнать все за пять минут и даже считанных секунд.

Больше всего вирусы любят «размножаться» и захватывать новые неизведанные территории путем использования электронной почты (Email), мгновенных сообщений (Push-up), сети Интернет, а особенно на мобильных устройствах. Поэтому очень важно соблюдать правила безопасности и быть осмотрительным как в сети, так и за ее пределами. Не стоит открывать письма, пришедшие к вам от незнакомцев, или кликать на привлекающий всеми цветами радуги рекламный баннер. Вирусы могут шифроваться под видом интересных картинок, звуковых и видеофайлов, «полезных» программ, антивирусов. Каждый день миллиарды пользователей сталкиваются с проблемой появления вируса, при скачивании нелицензионного программного обеспечения, а также в поисках бесплатного контента. А как определить, заражен ли ваш компьютер вирусом? Это возможно узнать с помощью невооруженного глаза при наличии следующих признаков. Признаки вирусов: неожиданное увеличение количества данных на диске; уменьшение размеров свободной оперативной памяти; вывод на экран нежелательных сообщений и изображений; подача непредусмотренных звуковых сигналов; неправильная работа или отказ работавших программ; заметное ухудшение быстродействия компьютера; частые сбои в работе компьютера, экраны смерти или BSOD; изменение размера файлов; исчезновение файлов и папок; невозможность загрузки операционной системы, или сбои при запуске. Каким бы ни был вирус, на любой вирус найдется свое противоядие и защита от непрошенных гостей, будет постоянно защищать вас и ваши данные от атак вирусов.

# **3 СТРУКТУРА ВЫХОДНЫХ ДАННЫХ**

Выходными данными являются непосредственно действия самого вируса, у нас есть 5 возможностей развития событий. В первом случае рабочий стол компьютера начинает беспрерывно заполняться вылетающими новыми окнами блокнота. Во втором случае блокируются любые действия на компьютере. В третьем случае воспроизводится мелодия из сериала «Бригада». В четвертом заставляет наш курсор бегать по монитору, совершенно не слушаясь управляющей мыши. В пятом случае начинают открываться случайные приложения.

Демонстрация первого случая видна на (Рис. 1).

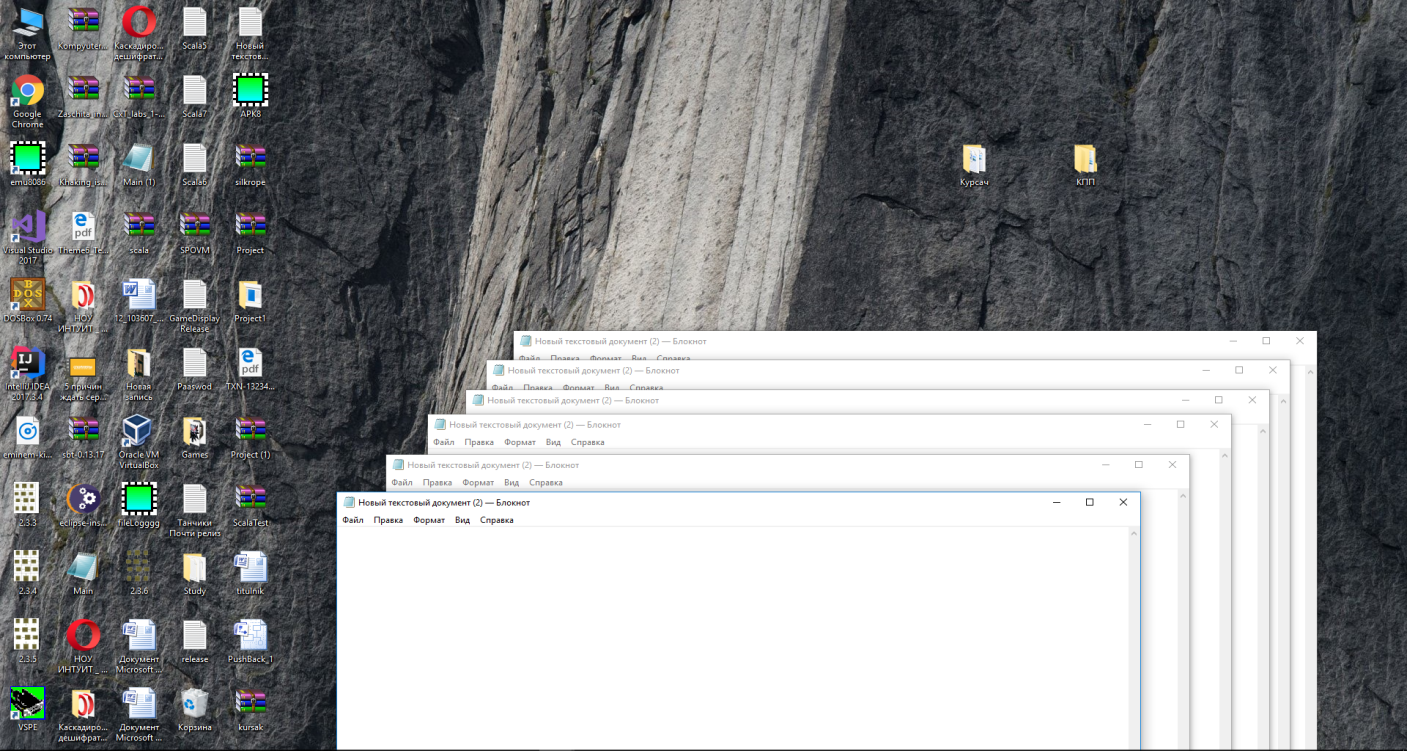


Рис. 1 – Демонстрация тестирования

Сам вирус располагается на гугл диске, доступен по открытой ссылке любому пользователю, имеющему данную ссылку, закачивается вирус, в виде исполняемого файла с расширением .exe который находится в архивированном пакете, с паролем – «12345».

Ссылка на гугл диск и расположение файла можно увидеть на (Рис. 2).

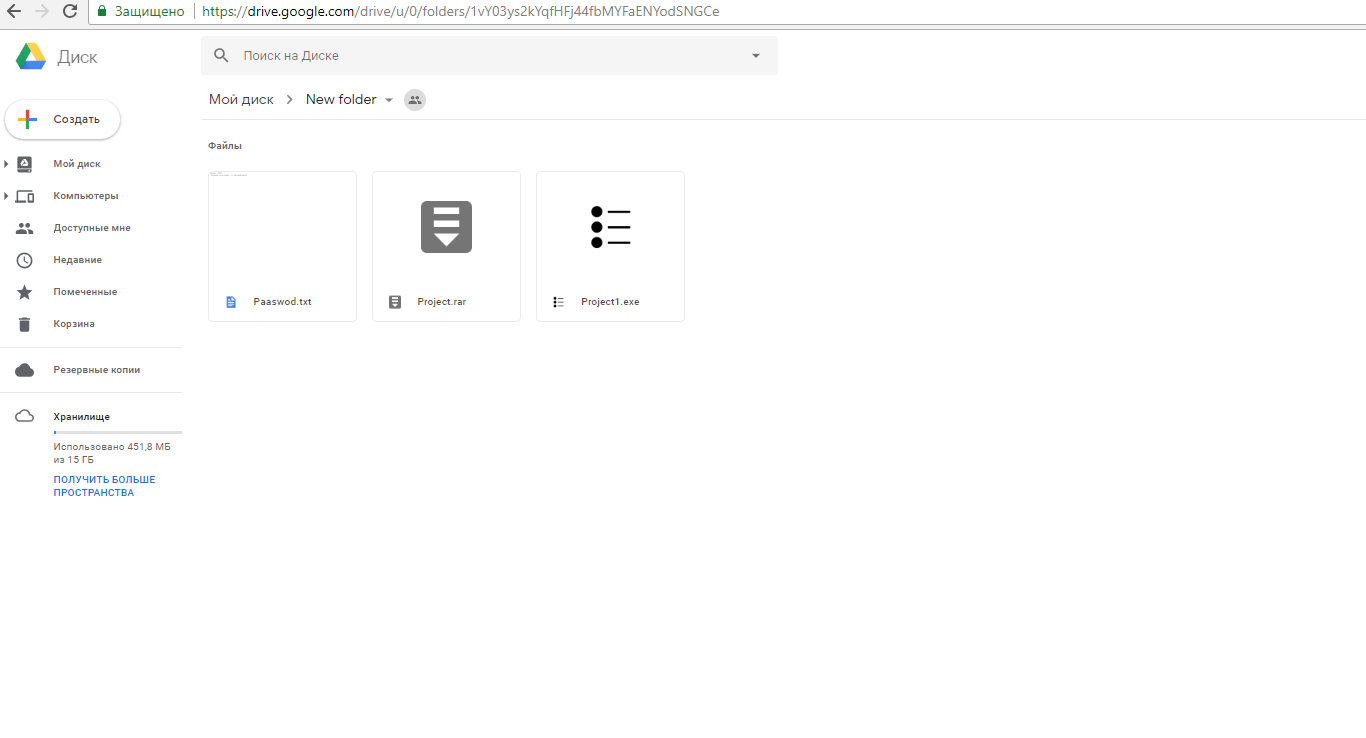


Рис. 2 – Местонахождение исполняемого файла в сети

**4 РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**

Пользователь получает ссылку на наш исполняемый файл, скачивает его, при этом не получая никаких уведомлений об угрозе безопасности. В блокноте, который доступен пользователю, так же по ссылке, он может узнать пароль от архива и прочитать сообщение о том, что антивирус может ругаться при запуске исполняемого файла, т.к. данное приложение без «таблетки» и находится на стадии бета - тестирования.

Запуск и извлечение файла из архива предоставлен на (Рис. 3).

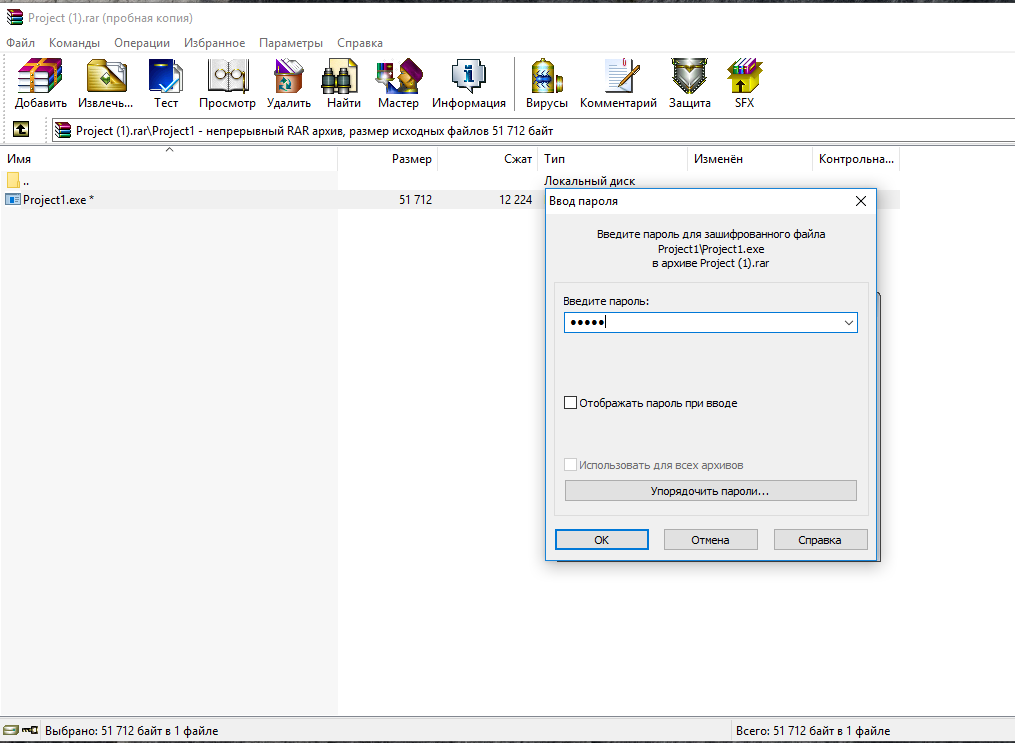


Рис. 3 – Запуск и извлечение файла из архива

Пользователь извлекает файл из архива в указанную папку, вводя пароль указанный в блокноте, запускает файл начинается заражение компьютера

вирусом, происходит одно из 5ти действий описанных в структуре выходных данных, так же вирус записывается в автозагрузку, поэтому перезагрузка не спасет.

# **5 ОПИСАНИЕ ФУНКЦИЙ**

Main() - главная функция, генерирует случайное число, соответствующее типу исполняемой вредоносной информации. Блокирует пользовательский ввод. Устанавливает наш вирус в автозагрузку. Создает новый поток и запускает бесконечный цикл где каждый раз выполняется та команда которую сгенерировал рандом случайных чисел.

SetUp() – устанавливает нашу программу в автозагрузку.

Run(int ID) – запускает сгенерированную рандомом команду.

Beeper() – команда, принцип в воспроизведении мотива из сериала «Бригада», с Саней белым сериальчик.

OpenStuff() – Открывает программки, стандартные.

Hibernation() – Усыпляет наш компьютер.

CrazyMouse() – Заставляет курсор летать по экрану не слушаясь мышки или тачпада.

DWORD WINAPI DestroyWindows(LPVOID) – Ищет окно по названию и закрывает его. Использует функцию FindWindow, если ее значение не равно null, значит окно обнаружено и его пора закрыть.

# **6 РАЗРАБОТКА ПРОГРАММНЫХ МОДУЛЕЙ**

**5.1 Схема алгоритмов**

5.1.1 Схема алгоритма основной программной функции main().

Представлена в приложении А.

5.1.2 Схема алгоритма функции Beeper(), воспроизводящей саундтрек из «Бригады».

Представлена в приложении Б.

**5.2 Основной метод.**

Для алгоритма по шагам рассмотрим метод main(), данный метод является главным методом в программе.

1. Начало.

2. Генерируем случайное число от 0 до 6.

3. Записываем ее в переменную random.

4. Останавливаем полностью пользовательский ввод методом BlockInput(), путем передачи ему значения true.

5. Запускаем метод SetUp(), тем самым записывая наш вирус в автозагрузку.

6. Возвращаем возможность пользовательского ввод методом BlockInput(), путем передачи ему значения false.

7. Создаем новый поток в котором и будет произведено удаление окон которые пользователь будет пытаться открыть в своих бессмысленных попытках спасти своего электронного помощника.

8. Переходим на начало бесконечного цикла.

9. Запускаем метод Run(), который будет выполнять указанную нами команду, путем передачи ему сгенерированного значения через переменную random.

10. Ожидаем 10 миллисекунд.

11. Переходим к шагу 8.

11. Конец.

**5.2 Воспроизведение мелодии.**

Для алгоритма по шагам рассмотрим метод Beeper(), реализующий вызов саундтрека из сериала «Бригада».

1. Начало.

2. Переходим к циклу for(), в котором создаем локальную переменную iFreq, зануляя ее, создаем условие о том, что цикл продолжается пока iFreq не равен COUNT, устанавливаем инкрементацию переменной iFreq.

3. Присваиваем переменной Freq элемент массива frequency, под индексом равным iFreq.

4. Присваиваем переменной Dur элемент массива longevity, под индексом равным iFreq.

5. Передаем переменные Freg и Dur, функции Beep() соответственно.

6. Переходим ко 2му шагу.

7. Конец.

# **ЗАКЛЮЧЕНИЕ**

Вирусы – это весьма интересное явление в IT сфере, сотни и тысячи компьютеров заражены вредоносным ПО по всему свету, компании терпят миллионные убытки из-за несостоятельности отделов информационной безопасности. Вирусы, как таковые, способны выполнять неограниченный стек функций, который задает сам разработчик вредоносного кода. Путем внедрения вируса можно сделать с устройством жертвы что душе угодно, выкрасть информацию, навредить цифровому устройству, дезинформировать различные отделы, тем самым снизив эффективность фирмы или корпорации. Но, не стоит забывать, что помимо необъятного стека вредоносных возможностей вирусов, они так же способны содействовать благополучной работе зараженного устройства, вирус есмь инструмент, вредоносный или благоприятный для зараженного устройство, это лишь зависит от целей, которые преследовал сам программист.

Наиболее простые предпосылки и причины, побуждающие хакеров - взломщиков, да и просто людей создавать так сказать «компьютерные микробы», то есть вирусы – любознательность и таинственность. С самого истока истории появления первых вирусов, первопричины так и не изменились. Обычно все происходит, как и у преобладающего большинства других, так именуемых, хакеров – преступников электронного мира: любознательность и неподдельная увлеченность компьютерными и электронными технологиями, немыслимая тяга к секретной и скрытой от большинства глаз сверхсекретной информации.

Обратим своё внимание и неутомимый интерес на серию патогенных вирусов, которые при инициализации и начале обработки своего кода выдавали: «Smoke me a kipper I'll be back for breakfast, unfortunately some of your data won't». Это было экспериментом со стороны хакеров заставить обычного пользователя помнить, о том, как он приобрел злополучный вирус и в какое время дня или ночи. Вирусы появлялись медленно и были по своему назначению и основному принципу, лишь параграммой имен. Многие авторы - создатели выдумывали неестественные и экзотические имена, для формирования и создания атмосферы недостижимой энигмы, скрытности-безопасности своего настоящего реального имени и приватных данных [16]. Написание и созидание вирусов молниеносно быстро стало интересовать колоссальное количество множества людей и групп, объединённых общими стремлениями добиться, достичь уровня тех, кто имеет возможности и способен «заразить» компьютер на другой стороне земного шара парой нажатий специальных комбинаций клавиш.

Благодаря данной курсовой работе я изучил природу IT вирусов, их классификацию, способы передачи и хранения, API функции, а так же познакомился с некоторыми уязвимостями Windows.

# ПРИЛОЖЕНИЕ А

Структурная схема

# ПРИЛОЖЕНИЕ Б

Структурная схема

# ПРИЛОЖЕНИЕ В

Листинг