МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)

Физико-технический факультет

Кафедра теоретической физики и компьютерных технологий

К У Р С О В О Й П Р О Е К Т

ИЗУЧЕНИЕ И РЕАЛИЗАЦИЯ СПОСОБОВ БЛОКИРОВКИ ВРЕДОНОСНОГО ПО И БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ

Работу выполнил _____ Гайдар Николай Александрович

Курс 3

Направление 09.03.02 Информационные системы и технологии

Научный руководитель
преподаватель_____ Т. В. Арутюнян

Нормоконтролер инженер _____ Г. Д. Цой

Краснодар 2018

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ПО	программное обеспечение
ПК	персональный компьютер
ПНП	потенциально нежелательные программы
ОС	операционная система
IRC	Internet Relay Chat
FTP	File Transfer Protocol
CRC	Cyclical Redundancy Check
KIS	Kaspersky Internet Security
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
IP	Internet Protocol
ICMP	Internet Control Message Protocol

ВВЕДЕНИЕ

В настоящее время язык C++ является одним из самых совершенных и сложных языков программирования. Свое развитие он имеет в 80-х годы в Bell Laboratories. C++ - расширение C, то есть он обеспечивает существенное преимущество языка C++, как над своим прадедом-языком C так и над другими языками программирования высокого уровня: поддержка объектно-ориентированного программирования, перегруженных операций и возможность разработки полномасштабных Windows-приложений.

С помощью языка C++ 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.

Актуальность. В настоящее время модернизации, реструктуризации, всенародной компьютеризации, необходимость защиты операционной системы, локальных вычислительных сетей является особенно актуальной.

Особенностью компьютерного вируса является - возможность генерировать свои копии (не всегда совпадающие с исходным оригиналом) и внедрять их в рабочие системные элементы операционной системы и компьютера. При этом генерирующие потомки компьютерного вируса сохраняют способность к дальнейшему развитию и распространению.

Объектом исследования являются технологии защиты вредоносного программного обеспечения.

Предметом исследования являются методы и особенности создания антивирусов.

Цель работы – изучение и реализация способа выявления зловредного кода и обезвреживание вредоносного программного обеспечения.

Для поставленной цели необходимо выполнить следующие задачи:

1 Изучить научную литературу и техническую документацию по выбранной теме.

2 Провести анализ функционирования, как вирусов, так и антивирусов.

3 Создать алгоритм действия и разработать программу по выявлению «опасных» участков кода и их обезвреживанию.

4 Разработать программу для выявления открытых и уязвимых узлов сети.

Курсовой проект состоит из введения, трёх глав, заключения, списка использованной литературы и двух приложений.

1 Антивирусы и вирусы, механизмы работы

1.1 Компьютерный вирус

Компьютерный вирус - это реализованная небольшая по размерам программа, которая может «добавлять» себя к другим программам, а также использовать их, 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.

Заражение файлов происходит не всегда, а при выполнении определенных условий. После того как вирус выполнит заданные ему действия, он передает управление той программе, в которой он находится, и она работает, как обычно. Тем самым работа зараженной программы выглядит так же, как и незараженной.

Компьютерный вирус может испортить все ваши данные включая фотографии, видеофайлы, аудиофайлы и что немаловажно вывести из строя аппаратную «начинку» вашего электронного помощника.

1.1.1 Классификация вирусов

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

По принципу действия рассмотрим фундаментальные разновидности вирусов:

- загрузочные;
- файловые;

- макровирусы;
- полиморфные-вирусы;
- стелс-вирусы;
- резидентные;
- IRC-черви;
- сетевые.

Загрузочные вирусы используют основной (boot) сектор Master Boot Record жесткого диска 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, 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, UNIX, Slackware, Oracle OS, включая заражения низкоуровневых 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 помощи 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 которых очень затруднительно или невозможно осуществить при помощи антивирусных сигнатур - участков основного кода, специфичных для рассматриваемого вируса. Данное свойство вируса достигается за счет использования двух основных способов – шифрованием тела вируса с непостоянным ключом и генерируемым набором команд расшифровщика или самогенерацией кода выполняемого вируса. Полиморфизм разных уровней сложности встречается в вирусах почти всех типов и видов - от загрузочных и файловых Windows-вирусов и даже макровирусов.

Резидентные вирусы. Под понятием "резидентность" (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. IRC похож на телефонный разговор между абонентами, за исключением того, что в разговоре могут участвовать более двух собеседников, которые обычно объединяются по интересам в отличные друг от друга группы IRC-конференций. 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. Главным преимуществом сетевого вируса является такая возможность, как передать код удаленному серверу, или рабочей станции. «Завершенные» сетевые вирусы могут заставить пользователя запустить вирус на своём компьютере, и пользователь сам того не замечая заражает свой компьютер, и в дальнейшем является распространителем инфекции.

К потенциально нежелательным программам (ПНП) помимо вирусов, относятся также некоторая разновидность вирусов как «троянские кони», утилиты скрытого удаленного зашифрованного администрирования, "ворующие" пароли доступа к аккаунтам в сети Интернет, а также конфиденциальную информацию, защищенную законом. Великое множество «троянских» программ подделываются, как полнофункциональная безобидная программа, вследствие чего многие антивирусы могут и не распознать «вора». Очень часто «трояны» приходят по электронной почте в виде архива и т.д.

Шпионская программа (Spyware) - это программный продукт, проникающий на компьютер без согласия его владельца, целью получения которого является полный доступ над компьютером или электронным

устройством, основная задача которого заключается в регистрировании и передачи конфиденциальных данных.

Зомби (Zombie) - самый «любимый» вирус компьютерных злоумышленников, которые получают доступ к вашему компьютеру посредством подключения данного вируса к сети Интернет, и в дальнейшем машина, зараженная данным видом вируса, выполняет команды и поручения третьих лиц. Таким образом, «компьютеры-зомби», да и любые электронные «устройства-зомби» объединяются в один большой пул, через который в автоматическом режиме идет атака на сайты, сервера, банки и т.д. «Зомби-пулы» способны нарушить работу даже самого хорошо защищенного сайта, над которым работали высококвалифицированные специалисты и при том не один год.

Фишинг (Phishing) - это почтовая рассылка, имеющая ввиду, захват личных конфиденциальных данных для передачи третьим лицам, а также введения получателя фишинг-рассылки в заблуждение, имеющей своей целью получение денежных средств путем применения социальной инженерии.

Фарминг - подвид фишинга, основной идей фарминга является подделка оригинальных сайтов банка, правительства, которые очень сложно отличить от оригинала. Пользователь, попав на «подложный» сайт, обычно ничего не подозревает, но стоит ему ввести свои данные, номер банковской карты или пин-код, то в мгновение ока эти данные оказываются у злоумышленника и все средства в течение одной секунды исчезают в неизвестном направлении.

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 Bluetooth. Мобильные вирусы способны передавать и перехватывать смс сообщения на лету, что делает их почти незаметными, также 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.

1.1.2 Источники вирусов

В XXI веке существует превеликое множество источников получения вируса, но рассмотрим самые распространённые:

- пиратское программное обеспечение (Crack version, Repack Version);
- персональные компьютеры "общего пользования", например, в учебных заведениях типа школа или университет;
- локальные сети;
- глобальные сети (Интернет, i2p, Torrent);
- электронные конференции, файл-серверы ftp;
- «случайные» пользователи компьютера.

Больше всего вирусы любят «размножаться» и захватывать новые неизведанные территории путем использования электронной почты (E-mail), 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 миллионы пользователей сталкиваются с проблемой появления вируса, при скачивании нелицензионного программного обеспечения, а также в поисках бесплатного контента.

Определить состояние заражения вашего компьютера можно 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 ОС, или сбои при запуске.

Каким бы ни был вирус, на любой вирус найдется свое противоядие и защита от непрошенных гостей, которое будет постоянно защищать вас и ваши данные от атак вирусов.

1.1.3 Мотивы написания вирусов

Наиболее простые предпосылки и причины, побуждающие хакеров-взломщиков, да и просто людей создавать 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.

Точкой отсчета становится следующая основная и наиважнейшая задача: добавить какую-либо программу А в основную-исполнимую часть программы Б

таким образом, чтобы программа Б не потеряла своих свойств и функциональности. Для этого требуются глубокие познания как самой системы, так и ее компонентов, под управлением которой будет работать и действовать программа. Перво-наперво это был DOS, простой эмулятор командной строки, имевший серьезные ограничения не только по функциональности, но и по ряду своих технических возможностей, однако он не пользовался популярностью у серьезных программистов и кодеров, программистов-специалистов своего дела.

По прошествии некоторого необходимого количества времени, появлялись различные вариативные версии Windows, которые больше не могли являться обычной надстройкой над DOS, а представляли из себя полноценную ОС как для работы, так и для серфинга в глобальной сети имен Интернет. Интерфейс и широчайший спектр новых функциональных и невообразимых по тем временам опций были более дружелюбны к пользователю, и в свою очередь вирусописателям необходимо было адаптировать и приспособить свой индивидуальный код для этих систем, и продолжать отыскивать в них возможности нанесения ущерба и тяжкого вреда утечке личной конфиденциальной информации.

Вирусы становились соблазнительно красивы и привлекательны внешне, но и их разрушающий эффект становился более значительней и серьезней, год от года.

Необыкновенная по тем временам щедрость внести личный индивидуальный графический аспект в свои вирусы, как часть своей субъективности, позволила большинству авторов и предоставило возможности персонализировать и индивидуализировать свои «творения», например, словосочетание «William Blake» занесенное в Maltese Amoeba. Чем больше расширялся функционал и добавлялось превеликое множество интересных вещей и к тому же совершенствовалось в вирусах, тем более значительными и разрушительными они становились по своему содержанию и масштабам поражения как ОС, так и захвату компьютеров и серверов компаний для личных целей и выгоды.

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 создатели выдумывали неестественные и экзотические имена, для формирования и создания атмосферы недостижимой энигмы, скрытности и безопасности своего настоящего реального имени и приватных данных.

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.

Весомых причин и аргументов для написания компьютерных вирусов у людей немного.

Первая – для удовольствия. Это первая и наиболее основная общепризнанная первопричина. Автору – творцу было просто очень любопытно и интересно, что может случиться, произойти и во что вылиться в дальнейшем его неугасимое желание познания. Люди не осознают и не верят в проблемы и их существование, пока сами с ней не столкнуться.

Вторая первопричина для созидания – это достичь той, кажется недосягаемой мнимой цели, чтобы программный код и дальнейший результат его действий появился на Wildlist, сайте, освещающем шествующие в сети в данный момент по миру вирусы. Например: «Kit clickers», «Script kiddies», «Kit coders». «Kit clickers» просто-напросто используют генераторы вирусов, коих на наш век превеликое множество с различными модификациями. «Script kiddies», которые берут готовые наборы участков кода для создания «своих» вирусов. Популярная и

по сей день программа – вирус, червь «Anna Kournikova», была претворена в жизнь с использованием Kalamar kit. Представленная и рассматриваемая группа не приветствуется как вирусописателями, так и теми, кто занимается защитой информационных и персональных данных.

Первая группа из рассматриваемых содержит в своей команде только тех, кто не ленится работать мышкой и генерировать по 30 вирусов из различных иногда несовместимых блоков кода, нуждающихся для обнаружения в полном разборе и дизассемблировании, анализе и т.д. Хотя именно они и обеспечивают большим объемом работы огромные антивирусные компании и множество как известных, так и не очень, вирусных лабораторий. Обычно штат команды из этого раздела с воодушевленной радостью и гордостью дает интервью в многочисленные издания, тем самым искажая и нанося вред репутации серьезных кодеров и профессиональных хакеров.

Раскрывшиеся серьезные кодеры – эта команды состоит из более опасных образованных кодеров и программистов, которые имеют достаточно большой и неоспоримый опыт как в программировании, так и в проектировании, и могут писать свои приложения на уровне антивирусной индустрии. В уже созданные вирусы они добавляют множество личных процедур и функций, блокирующих при анализе-дизассемблировании получение исходного кода вируса для его дальнейшего обезвреживания и излечения зараженных файлов.

Парадоксально, но именно такие вирусы пишутся и создаются для какого-либо исследования и изучения какого-либо процесса так сказать изнутри, а не для нанесения умышленного вреда конечному пользователю. Нельзя не упомянуть, что права доступа к данному коду имеет достаточно субъективно малое и ограниченное количество людей, и все из той же команды-группировки, или на худой конец этот код становится всеобщим достоянием доступным в сети Интернет, как доказательство найденной лазейки, дыры-уязвимости как программы, так и целого ряда информационных систем. Они ни коим образом не наносят никому ущерба и вреда, а лишь подсказывают направление на

направление, откуда и куда может быть нанесен удар и как могут быть извлечены конфиденциальные данные.

«Рассерженные одиночки» – завершающий и самый опасный тип любознательного хакера. Их не касается какая-либо мораль или закон, и не учитывается процент и глобальность того ущерба, который может понести пострадавший пользователь или организация. Каждый из них имеет свою заветную, индивидуальную, персональную цель. Они не относят себя ни к какой группе кодеров, хакеров, они представляют себя единоличниками в глобальном пространстве. Их задача нанести максимальный ущерб и урон пользовательским данным и получить собственную выгоду. Их не удается подвести под общие рамки и правила вирусописателей, так как у каждого из них своя мораль и идеология, и о ней никто никогда не знает. В данный момент к этой группе относится не такое большое количество людей.

Увлечение – одна из самых неоспоримых движущих сил большинства вирусописателей, именно благодаря этой силе и создаются такие программы, вырастающие из, казалось бы, простого увлечения. У кого-то имеется в распоряжении достаточно много свободного личного времени, которое они проводят за любимым занятием. Это скорее всего относится к молодым, излучающим энергию людям.

Их можно сравнить с первой группой, но чаще всего они очень грамотно программируют, соблюдая все правила, часами смотрят логи на наличие частей пропущенного кода, для выявления ошибки, или раз за разом проверяют и тестируют работоспособность своих творений под различными версиями ОС. Кодеры, как и обыкновенные люди часто помогают друг другу советами, делятся полезной и важной информацией, ночи напролет изучают новые вирусы и их функциональные особенности, или придумывают и реализуют новые идеи. У этой группы нет как таковой поставленной цели и реализуемой задачи: навредить кому-либо, или зацикливаться на одной идее.

1.2 Антивирусные программы

Мир вирусописателей, сформированный в сознании людей некомпетентными и не пытающимися понять истину обозревателями остался далеко в прошлом, и уже не пугает человечество от покупки нового ПО, и необходимости сохранять свои данные. Общий уровень развития и сознания вирусописателей-хакеров растет, как знание программирования и распределенных многопоточных систем.

Уже «завтра» мы будем ежедневно сталкиваться с аналогами, раннее написанных вирусов, из-за халатного отношения большого числа пользователей к своей личной информационной безопасности, и растущего числа любопытных вирусописателей.

Общеизвестным и принятым считается следующее определение:

Антивирус – это программа, которая защищает компьютер от вирусов, то есть разного рода вирусов и инфекций. Основной целью и задачей антивирусных программных продуктов и средств является защита компьютера и обнаружение уже действующих зараженных программ, а также их исцеление и ликвидация путем проверки и восстановления исходного не нарушенного (первоначального) кода, для возможности дальнейшего использования ранее зараженной программы.

Первые антивирусы появились вслед за появлением первых вирусов, только немного позднее, спустя некоторое время, если первый вирус появился в 1971 году, то первый антивирус появился в 1984 году. Сегодня существует и имеется довольно огромное количество вирусов, и антивирусных программных продуктов, как коммерческих, так и распространяющиеся по свободной лицензии, разрабатываемых и поддерживаемых огромными международными корпорациями, например, Microsoft, и небольшими компаниями, например, Alwil Software.

Выделим основные задачи антивирусного программного обеспечения:

- защита компьютера от вирусов и заражения данных;
- обнаружение вирусов и обезвреживание, уже проникших на компьютер;

- лечение компьютера, без нанесения вреда функциональности той или иной программе;

- сведение к первоначальному состоянию данных, до воздействия вирусов.

1.2.1 Антивирусные сканеры

Антивирусные сканеры по своей основной цели являются самыми популярными программными средствами для обнаружения и обезвреживания вирусов. Не уступая по функционалу и ряду решаемых задач, за ними следуют CRC-сканеры. Часто оба рассмотренных нами метода объединяют в одну программу, которая обладает наилучшим качеством обнаружения и скоростью обработки зараженных файлов. На данный момент часто употребляются такие необходимые элементы, как блокираторы, иммунизаторы, мониторы, Sandbox и Cloud Security технологии.

Принципы работы антивирусных сканеров основаны на проверке файлов и выявления в них зловредного участка кода, секторов оперативной памяти, побитного «прохождения» по файлу, а также сверке с базой данных сигнатур самого антивирусного сканера. Для поиска популярных вирусов используются так называемые маски имен и суммы кода хэша.

Маска вируса - некоторая последовательность кода, специфичная для этого конкретного вируса, то есть содержащая последовательность элементов в коде вируса. Если вирус не содержит маски или длина его кода превышает количество содержащихся в нем символов, то используются другие методы обнаружения. Примером такого метода - алгоритмический язык, в котором описаны все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом.

Во многих сканерах используются алгоритмы эвристического сканирования, то есть анализ последовательности в проверяемом объекте, набор необходимой статистики и принятие первичного решения для каждого проверяемого объекта.

К преимуществам сканеров относится их легкость, универсальность, быстродействие и незначительное влияние на операционную систему, к недостаткам – «тяжелые» размеры антивирусных баз, которые сканерам приходится «носить с собой», и в некоторых встречается медленная скорость поиска вирусов.

Действие CRC-сканеров основано на подсчёте CRC-сумм (контрольных сумм) для имеющихся на диске файлов. Эти CRC-суммы хранятся в базе данных антивируса, как и другая информация: длины и количества файлов, даты модификации и т.д. При каждом запуске CRC-сканеры проверяют данные, содержащиеся в их базе данных, с заранее посчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает со значениями, то CRC-сканеры выводят сообщение о том, что файл был изменён или заражён каким-либо вирусом.

CRC-сканеры, в основе своей содержащие «антистелс»-алгоритмы, являются сильным противоядием против вирусов: практически 100% вирусов оказываются «пойманными» почти сразу после их проявления на компьютере. Однако у данного типа антивирусов есть недостаток, который заметно снижает их эффективность и лабильность.

Недостаток состоит в том, что CRC-сканеры не могут поймать вирус в момент его появления в системе, а делают это лишь по прошествии некоторого времени, уже после того, как вирус «пошел» по компьютеру. CRC-сканеры не в силах детектировать вирус в новосозданных файлах, поскольку в их базе данных такая информация не содержится.

Более того, практически ежедневно появляются вирусы, которые используют "слабость" CRC-сканеров, заражают только вновь создаваемые файлы и остаются незаметными для CRC-сканеров.

Антивирусные мониторы - это специальные резидентные программы, которые в основном перехватывают вирусоопасные ситуации и сообщают об этом пользователю.

К вирусоопасным относятся действия на открытие для записи в исполняемые объекты - файлы, запись в загрузочные секторы дисков или MFT HDD (жесткого диска), попытки программ остаться незамеченными или резидентно скрытыми в системе, т.е. именно те действия и логическое сопровождение действия последовательностью длины кода, которое характерно для вирусов в моменты их распространения.

К достоинствам использования антивирусов типа мониторов относится их отличительная черта от всех остальных - обнаруживать и блокировать вирус на стадии его внедрения в компьютер или электронные средства. Как и у каждого представителя поколения антивирусов есть свои сильные стороны, так и слабые, у рассматриваемого вида антивирусов-мониторов есть свои недостатки, к ним относятся существование путей обмана защиты монитора и большое количество ложных срабатываний, что, видимо, и послужило причиной для частичного или полного отказа пользователей от данного вида антивирусных программ.

Необходимо также заметить такое интересное направление антивирусных средств защиты, как антивирусные мониторы, выполненные в виде аппаратных компонентов компьютера. Однако, как и в случае с программными мониторами, такую защиту очень просто и непринужденно обойти. Также к вышеперечисленным недостаткам добавляются следующие проблемы совместимости со стандартными конфигурациями компьютеров и сложности при их установке и настройке, использовании. Всё вышеперечисленное делает встроенные аппаратные мониторы в основном непопулярными средствами на фоне различных типов антивирусной защиты.

Иммунизаторы - исследуемый вид делится на два типа: иммунаторы, сообщающие о вторжении зловреда, и иммунизаторы, блокирующие опасные и нежелательные действия.

Первые обычно дописываются в конец коды длины файлов и при запуске файла каждый раз проверяют его на «некачественное» изменение. Недостаток у таких иммунизаторов всего на всего один, но он летален: совершенная неспособность сообщить о заражении стелс-вирусом. Поэтому такие

иммунизаторы, как и мониторы, не нашли практического применения в наше время.

Второй тип иммунизации защищает систему от поражения вирусом и блокирует подозрительные действия какого-то определённого вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже своих заражённых собратьев.

Для защиты от резидентного вируса в оперативную память компьютера записывается программа, повторяющая точь-в-точь копию вируса, при запуске вирус случайным образом находит её и считает, что система уже заражена. Такой тип иммунизации не является достаточно универсальным, поскольку нельзя проидентифицировать файлы от всех известных и неизвестных вирусов. Однако, несмотря на это, подобные иммунизаторы в качестве меры предзащиты могут вполне надёжно защитить компьютер от нового неизведанного вируса вплоть до того времени, когда он будет детектироваться антивирусными сканерами и комплексными средствами защиты.

Онлайн сканер. Также необходимо отметит, что в мире появились сервисы, позволяющие проверить компьютер, подключенный к Интернету на наличие вирусов. Работают посредством технологии ActiveX или Java. Их преимущество - возможность поиска и лечения на лету зараженных файлов без установки антивирусного средства. Основной минус этого типа сервисов — отсутствие средств профилактики и мониторинга заражения. Наиболее известные и рекомендуемые онлайн сканеры - ESET Online Scanner, Emsisoft Anti-Malware, Dr.Web Cureit, Microsoft Malicious Tool, RAV, Kaspersky Removal Tool, Trend Micro, Comodo AV Scanner.

Antispyware. Популярный на сегодня вид угроз в меню мира вирусов. На сегодня подавляющее большинство антивирусных пакетов «не знает» такое ПО как опасное для жизни и развития информационных систем, так как оно является «пограничным». Это привело к появлению целого поколения утилит для очистки системы от шпионского и мошеннического ПО. Кроме того, некоторые

антивирусные программы и утилиты для профессионалов своего дела (например, AVZ) все же содержат модули опознания spyware.

Онлайн сканер одного файла. В основном занимается только анализом вредоносных, по вашему личному мнению, файлов. Вы просто загружаете на сервер антивирусной лаборатории, выбранный вами объект файловой системы, и вы мгновенно получаете ответ. Время ожидания также зависит от количества программ-эвристов, которыми проводится проверка, и нагрузкой на сервера. Это решение идеально для тех ПК и устройств, где антивирус не установлен, но следует проверить файлы, принесенные, допустим другом. К числу легендарных можно отнести Dr.Web online check, avast! Online Scanner, VirusTotal, Online malware scan.

Firewall. Отчасти данную программу можно отнести к антивирусным средствам защиты двойного назначения (рисунок 1), так как она в режиме реального времени, отражает атаки вирусов и хакеров. Основной механизм — блокировка, сканирование сетевого трафика и обеспечение скрытности и защищенности портов ПК в сети (через блокирование ping, telnet, tracert и других сервисов). Может быть полезна и использована в случаях уже произошедшего сбоя и модифицирования системных файлов (блокирует исходящие несанкционированные попытки соединения). Наиболее популярен сегодня Outpost Firewall в Западных странах мира и на Востоке, в России Avast Free Antivirus от чешской компании Alwil.

Антивирусы-сканеры без монитора. Основная цель – сканирование очистка локальных и внешних сменных носителей от вредоносных воздействий программ паразитов. В отличие от программ все в одном, содержащих в себе целый набор сетевых, в реальном времени экранов и эвристов, не обладают каким-либо встроенным модулем, а также не имеют модуля самозащиты. За счет отсутствия некоторого функционала достигается хорошая производительность и уровень легитимности обнаружения. Самые популярные — Cure it, Clam AntiVirus, Norton Security Scan, Sophos.

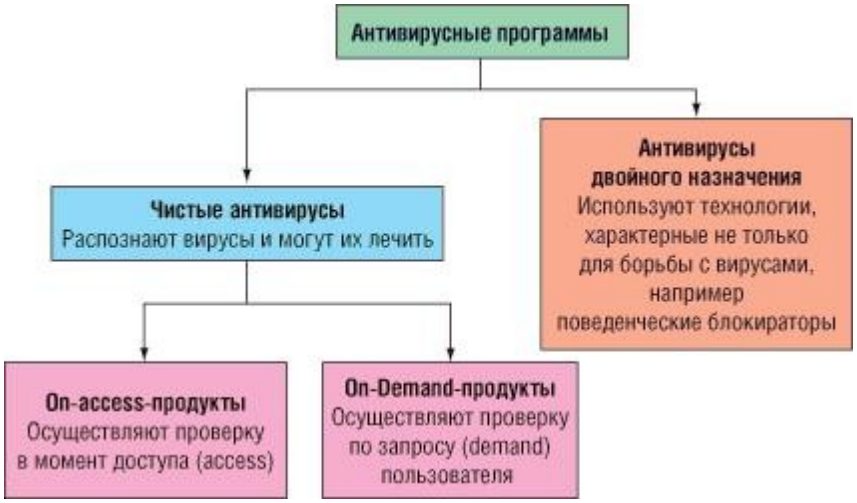

Рисунок 1 - Категории антивирусных средств

1.2.2 Работа антивирусов

Оценка качества выполняемой работы тем или иным антивирусом можно представить в виде следующих немаловажных аспектов:

- оценке качества обнаружения, уровня ложных срабатываний и реакции на новые угрозы;
- оценке скорости работы антивирусных продуктов;
- качеству лечения активного заражения;
- оценке эргономичности антивирусов.

Оценка качества определения и обнаружения, уровня ложных срабатываний и реакции на новые угрозы.

Благодаря современным методам и формам анализа, и исследовательским результатам от широко известной антивирусной лаборатории AV-Comparatives и AV-Test.org, несомненным лидером среди выбранных антивирусов на прохождение теста в плане обнаружения, качества реакции на новые еще неизвестные угрозы и малого уровня ложных срабатываний в сравнении с многими другими является Kaspersky Internet Security, далее - Avast Free Antivirus. Замыкает цепочку Microsoft Security Essentials.

На подавляющем большинстве форумов, к примеру nullewed.ru, в специально завиденные разделы «Лечение системы», на форуме практически постоянно предлагают воспользоваться утилитой нашего отечественного программиста и системного администратора AVZ (бесплатной утилитой Олега Зайцева).

При этом, что немаловажно многие просят решения возникших проблем по восстановлению системы именно после ее лечения с помощью такого именитого программного продукта как Kaspersky Internet Security.

Оценка скорости реагирования антивирусных продуктов - проведенное в марте 2016 года, независимой мировой лабораторией, тестирование на скорость обнаружения вирусов антивирусными продуктами показало, что среди выбранных пакетов антивирусного ПО Kaspersky Internet Security и Avast Free Antivirus оказывают самую наименьшую нагрузку на системные ресурсы. А Microsoft Security Essentials, требует максимальную их выкладку.

Если учитывать потребление оперативной памяти (ОЗУ) продуктами необходимого при выполнении ими прямых обязанностей:

- 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 Т.е., если у компьютера оперативной памяти 2 Гб, то KIS просто заберет львиную долю системных ресурсов, то есть «положит систему». А во всем остальном он «скоростной», неоспоримый лидер.

В заключении сравнительного обзора компания как обычно подводит итоги по проведенному анализу. Платные программы системы комплексной защиты высокого класса Internet Security обладают наибольшими функциональными возможностями и надежным самым высоким уровнем обеспечиваемой защиты в реальном времени среди выбранных ими продуктов.

И как пытаются утверждать многие вирусные лаборатории, именно комплексные защитные системы подходят большинству простых не особо то и

разбирающихся в программах пользователей, поскольку во многих реализован и используется подход «установил и забыл». Нет необходимости устанавливать дополнительные элементы и утилиты защитного программного обеспечения.

В состав многих таких систем опционально входит такой важный и незаменимый компонент, как родительский контроль. Многие продукты содержат в себе функции, такие как: электронные платежи через интернет, изолированная среда (SandBox), виртуальная клавиатура, антифишинг, защита от хакерских атак и другие важнейшие элементы комплексной защиты, позволяющие намного уменшить риски заражения через интернет.

Все многочисленные комплексы класса Internet Security обеспечивают надежную защиту от многих сетевых атак.

Бесплатные же антивирусные пакеты, например, Avast Free Antivirus, стоит устанавливать и настраивать, более опытным и смышлёным пользователям, не забывать, что используемая защита не гарантирует всесторонней защиты.

К бесплатному антивирусу в обязательном в порядке нужна установка дополнительного элемента защитного программного обеспечения: сканера и контролера портов, фаервола, межсетевого экрана и т.д.

Бесплатные антивирусы возможно и нужно использовать только на компьютерах с бюджетной конфигурацией и низкими требованиями к уровню обеспечения информационной безопасности и защищенности. Самые известные бесплатные антивирусные программные пакеты, такие как Avast Free Antivirus или Microsoft Security Essentials отлично подходят только в том случае, если на устройстве пользователя не содержится абсолютно никакой важной информации.

Обычно бесплатные антивирусы в большинстве своем выбирают только опытные пользователи, которым антивирусный продукт подчастую нужен для реализации в качестве «подстраховки».

Из исследований двух известных и имеющих вес на рынке вирусных компаний AV-Comparatives и AV-Test.org, наблюдаем, что в данном обзоре сравнение антивирусных программ, происходит не совсем корректно, т.к. сравнивать решения программ более высокого класса, такого как Internet Security

и бесплатные антивирусы имеющие базовый набор обеспечения безопасности - это неправильно. Комплексная защита имеет и обладает наиболее большим функционалом, нежели бесплатная антивирусная защита, тем более базовая.

Для сравнения, бесплатная версия антивирусного пакета Avast уступает не только конкурентам из смежной области, но и по функциональным возможностям даже своему платному брату Avast Pro.

По оценке качества работы, многих антивирусных программ, тоже имеется свой ряд вопросов. Здесь приводится в сравнение целый комплекс защитных функций KIS, а в частности, как своевременно и качественно они реагируют и обрабатывают новые угрозы, с работой антивирусного ядра тоже не все хорошо и антивирусного анализатора бесплатных пакетов антивирусов.

Например, если взять всем известный бесплатный антивирус чешского производства - Avast, дополнительно установить такой элемент защиты как фаервол Comodo и утилиту Malwarebytes Scaner, то KIS заметно проиграет со своей реализации защиты. При этом потребление оперативной памяти при выполнении своих прямых обязанностей этими защитными средствами будет в целесообразных для большинства пределах 700 Мб, в то время как для KIS необходимо будет 1,5-2 Гб.

Для лечения лучше всего применять специальные для этого созданные программы - лечащие утилиты такие, как DrWeb CureIt, Eset Nod32 Scanner, AVP, то есть утилиты серии LiveCD/USB или утилита AVZ. Все остальные могут нанести вред компьютеру и пользовательским данным, т.к. антивирусные решения фокусируются и предназначены для выявления, пресечения вторжения угроз.

Если сравнивать правильно настроенные компоненты и функционал KIS и Avira Internet Security (решения последних «свежих» версий), то продукт Касперского и здесь проиграет, как при обнаружении вредоносных программ, так и по объему использованию системных ресурсов.

Исходя из выше изложенного, напрашивается вывод о том, что рассматриваемый и проанализированный сравнительный тест компаний AV-

Comparatives и AV-Test.org, был проведен и выполнен не для выявления недостатков Kaspersky Internet Security, а целью показать и прорекламировать пользователям узкоспециализированный продукт для поддержания высокого рейтинга компании.

Итак, многие тесты от известных как антивирусных, так и вирусных лабораторий в той или иной мере, имеют своей целью прорекламировать какой-либо продукт для получения прибыли и дальнейшего развития собственного бизнеса и взаимной выгоды.

И никак не ставят перед собой цель объективно и достаточно широко рассматривать, анализировать и тестировать продукты, для предоставления широкому кругу пользователей наиболее точных и полных результатов того или иного программного средства, рассматриваемого ими.

2 Антивирус в среде C++

2.1 Постановка задачи

Создать приложение в C++ с использованием интегрированной среды разработки QT Creator 5.2.0.

Например: приложение при выполнении загружает файл для сканирования (рисунок 2) и производится его обработка с использованием антивирусной базы данных сигнатур в результате чего получаем обработанный файл (рисунок 3).

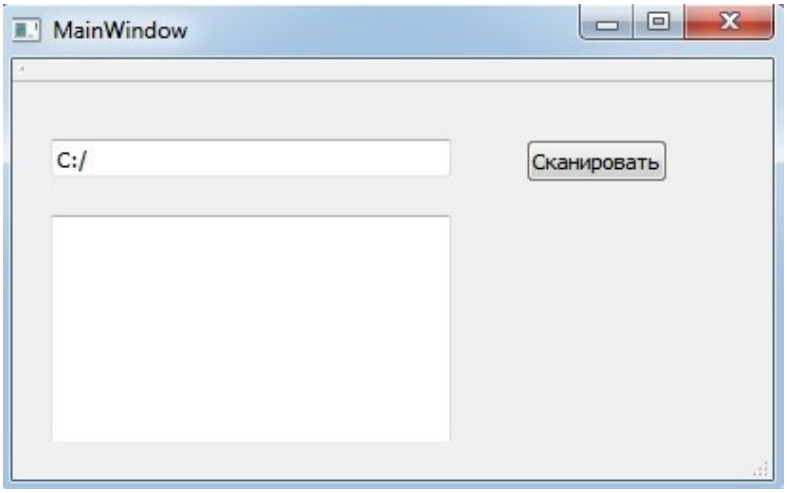

Рисунок 2 - Загрузка и проверка файлов на вирусы из каталога

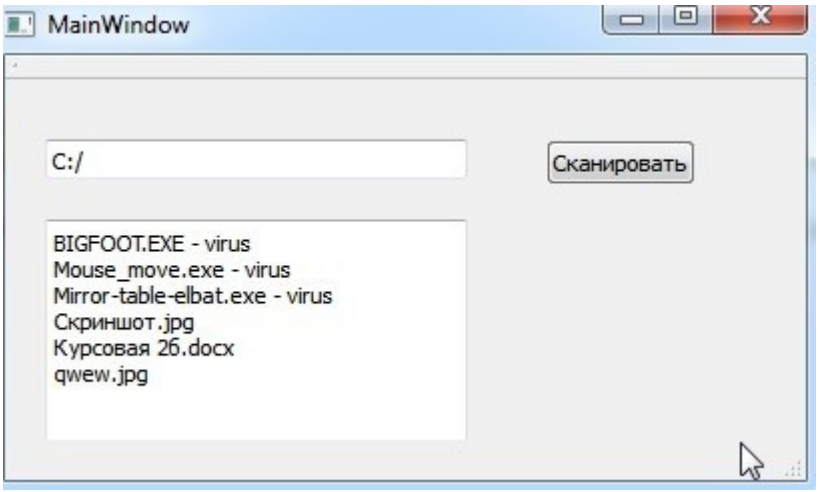

Рисунок 3 - Файлы, обработанные сканером

2.2 Описание метода решения

Для решения задачи использована среда программирования QT Creator. Программа разработана как приложение с использованием функции main.

При запуске программы выполняется загрузка файлов из локального хранилища (жесткого диска), затем программа начинает обработку (инициализацию) файла и поиск зловредного кода.

В силу простоты алгоритма выявления зловредного кода наш сканер сможет находить только вредоносные программы, распространяющиеся цельным

файлом, т.е. не заражающие другие файлы, как PE-Вирусы, и не изменяющие свое действие в процессе собственной деятельности, как полиморфные вирусы.

2.2.1 Алгоритм работы сканера

Алгоритм работы сканера, использующего антивирусные сигнатуры, можно представить в виде нескольких основных пунктов:

- загрузка базы сигнатур;
- открытие проверяемого файла;
- поиск сигнатуры в открытом файле;
- если сигнатура найдена: принятие соответствующих мер;
- если ни одна сигнатура из базы не найдена: закрытие файла и переход к проверке следующего.

Сканеру для работы необходимы сигнатуры, которые хранятся в антивирусной базе данных. База создается и наполняется специальной программой, но может быть и простым txt файлом.

Сигнатура будет состоять из:

- смещения последовательности в файле;
- размера последовательности;
- хэша последовательности.

2.2.2 Конструирование алгоритма

Структурная схема алгоритма приведена на рисунке 4 и рисунке 5. Алгоритм основан на описанном ранее методе решении:

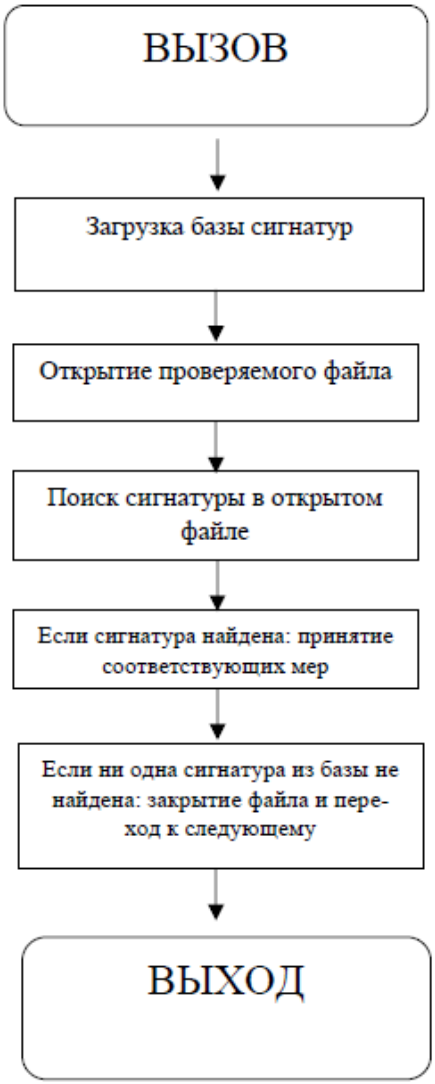

Рисунок 4 - Блок-схема алгоритма сканера

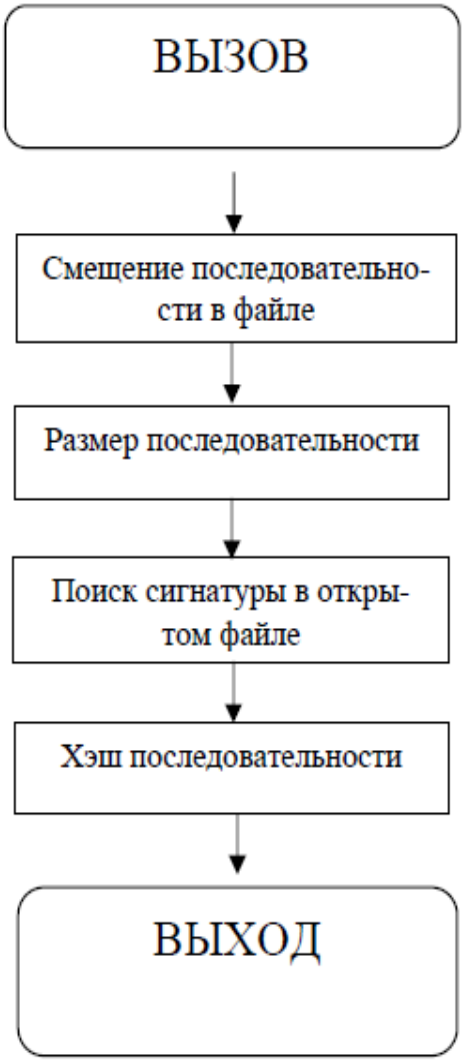

Рисунок 5 - Блок-схема состояния сигнатурных данных

2.3 Описание программы

Программа написана на языке C++ с использованием платформы интегрированного программирования QT Creator 5.2.0 и работает под управлением операционных систем типа Windows. Для успешной работы программы достаточно иметь установленную на машине QT Creator, и файл File.cpp

Исполняемый код (File.cpp) занимает на диске 15 КБ.

2.3.1 Структура программы

Программа реализует алгоритм, указанный в предыдущем разделе. Исходный текст программы (приложение А) содержит основную часть.

Рассмотрим особенности функционирования и реализации этой программы. Выполнение программы начинается с функции main. Данная функция не имеет параметров и возвращаемых значений. Также работа программы завершается при нажатии кнопки выхода.

2.4.2 Руководство пользователя

Для выполнения программы необходимо запустить QT Creator и открыть файл с кодом исходной программы File.cpp

Программа требует наличия исходных данных в виде сигнатуры баз.

Для проверки файлов, требуется прописать путь или директорию до проверяемого файла.

Пользователь при желании может проверить любой файл и произвести его обезвреживание в ручном. Таким образом программа может обрабатывать любые файлы при наличии расширенной установленной библиотеки базы данных сигнатур C++ может просканировать любой файл.

2.4.3 Анализ результатов

В результате выполнения курсового проекта разработана программа на языке C++ в среде QT Creator, реализующая процесс, описанный в постановке задачи. Программа имеет исходных данные в виде базы данных сигнатуры антивируса. Начальное количество данных не может быть изменено в процессе работы программы. Атрибуты обработки файлов заданы статичными данными. Процесс работы программы наглядно отображается на экране. В результате работы программы на выходе имеем информацию о файлах в каталоге.

3 Сканер TCP-портов

3.1 Transmission Control Protocol

Пользователи подавляющего большинства электронных устройств, работающих под управлением известных операционных систем семейства Windows, реализованных на ядре NT используют разные сетевые настройки: протокол Интернета (TCP/IP), для установки соединения с Интернетом через роутер, маршрутизатор, модем либо локальную сеть.

Сетевой протокол - это правила и технические процедуры, позволяющие компьютерам и электронным устройствам, объединенным в одну глобальную сеть, осуществлять соединение и обмен как потоковыми, так и статичными данными. Таким протоколом для глобальной сети Интернет стал TCP/IP, который является стандартом, принятым в 1983 году.

Сокращенное обозначение TCP/IP объединяет огромное количество протоколов, функционирующих между собой и предназначенных для решения самых разных задач. Существуют два основных протокола транспортного уровня: TCP и UDP.

TCP (Transmission Control Protocol), или протокол управления передачей (данных), называется еще протоколом надежной (достоверной) доставки. Это означает, что вся информация, отправляемая по данному протоколу, будет непременно доставлена именно тому, кому она адресована. В TCP перед началом трансферта данных устанавливается многопоточное соединение между отправителем и получателем, а также используется множество методов обнаружения и корректировка наибольшего количества ошибок (коллизий) на каналах приема/передачи информации.

UDP (User Datagram Protocol), или протокол пользовательских данных, его еще зовут протоколом, не внушающим доверия или недостоверным протоколом доставки. Однако с помощью этого протокола, когда нужно, можно быстрее доставлять необходимую информацию, что очень активно используется как в

сетевых играх реального времени, так и в системах быстрого оповещения и реагирования, при передаче видеоданных, а также аудиопотока.

IP (Internet Protocol), название которого дословно переводится – межсетевой протокол. Основную задачу по корректной обработке данных выполняют вышестоящие транспортные протоколы, то IP обращается с ними достаточно небрежно, халатно. Например, пакеты используемых данных могут отправляться в любом самопроизвольном порядке, а не в том, в каком они пребывали вначале пути, дублироваться, приходить к адресату разными способами и каналами приема/передачи данных, повреждаться, терять необходимую достоверную информацию и т.д. При отсутствии данного протокола Интернет никак не сумел бы правильно функционировать, так как именно он связывает две различные электронные системы, находящиеся в разных подсетях, сетях, государствах, странах, континентах.

Именно на рассматриваемом уровне модели TCP/IP существуют различные сетевые адреса, которые мы используем, как некий набор из 4 различных чисел, разделенных точками, например: 127.0.0.1.

По таким уникальным личным номерам IP безошибочно и непрекословно определяет, как получателя, так и отправителя информационных данных. К сетевому уровню также относится малоизвестный простому обывателю протокол ICMP, которому мы должны и даже обязаны командой ping и не менее важной и значимой командой tracert.

Ниже сетевого уровня расположены такие протоколы, среди которых Ethernet, IEEE 802.11, ATM, SLIP и многие другие, мало что дающие понять рядовому пользователю без необходимых базовых знаний, но незаменимые для разработки, например, сетевого оборудования или информационных мобильных устройств.

Основой основ является материальный (физический) уровень – каналы передачи различного множества данных, где не имеется никаких сетевых протоколов, а есть только амплитуды, частоты, модуляции и волны.

3.2 Простейший сканер TCP-портов

Сканер работает по следующему принципу (рисунок 6):

- подключение используемых библиотек и инициализация структуры;
- создание сокет с помощью socket();
- задание диапазона сканируемых портов MinPort и MaxPort;
- проверка доступности портов.

Рисунок 6 - Блок-схема алгоритма сканера TCP-портов

Подключение нужных библиотек и инициализация структуры:

```
#include “stdafx.h”
#include <WinSock2.h>
#include <iostream>
#include <locale.h>
using namespace std;
#pragma comment (lib, "ws2_32.1ib");
```

```
 int _tmain(int argc, _TCHAR* argv[])
{
setlocale(LC_CTYPE, "Russian");
SOCKET sock;
int error;
char ws[1024];
char buff[32];
int MinPort;
int MaxPort;
int port;
```

Проверка на выявление ошибок перед запуском программы:

```
if (FAILEDNISA(WSAGetartup(0x202(WSADATA *)&ws[0])))
error = WSAGetLastError();
cout << " Ошибка WSAStartup" < endl;
 return -1;
```

Создание структуры socket():

```
 if(INVALID_SOCKET = = (sock = socket(AF_INET,SOCK_STREA,0)))
{
error = WSAGetlastError();
cout <<”Ошибка сокета” << endl;
return -1;
}
sockaddr_in sock_addr;
ZeroMemory(&sock_addr, sizeof (sock_addr));
sock_addr.sin_family = AF_INET;
sock_addr.sin_addr.S_un.S_addr = inet_addr("127.0.0.1").;
```

Задание диапазона сканируемых портов:

```
cout<<”Введите минимальный порт”<<endl;
cin>>MinPort;
cout<<”Введите максимальный порт”<<endl;
cin>>MaxPort;
Проверка портов на доступность:
for (MinPort;MinPort <= MaxPortiMinPort++)
{
port=MinPort;
sock_addr.sin_port=htons(port);
if(SOCKET_ERROR=
=(connect(sock,(sockaddr*)&sockaddr,sizeof(sock_addr))))
{
error =WSAGetlastError();
cout << “Порт” << port  << “закрыт”<< endl;
cout << “Порт” << port  << “открыт”<< endl;
system("PAUSE");
}
```

Реализация алгоритма TCP сканера портов на языке программирования Visual C++ 2010 с подключением необходимых библиотек представлена в приложение 2.

3.2.1 Описание программы

Программа написана на языке C++ с использованием платформы интегрированного программирования Microsoft Visual Studio и работает под управлением операционных систем типа Windows. Для успешной работы программы достаточно иметь установленную на машине Microsoft Visual Studio 2010 не ниже, и файл Port.cpp. Исполняемый код Port.cpp занимает 4 КБ.

3.2.2 Общие сведения

Программа реализует алгоритм, указанный в предыдущем разделе. Исходный текст программы (приложение Б) содержит основную часть. Рассмотрим особенности функционирования и реализации этой функции. Выполнение программы начинается с функции main. Данная функция не имеет параметров и возвращаемых значений. Также работа программы завершается при нажатии клавиши, клавиша служит выходом из программы.

3.2.3 Структура программы

Создание нового проекта в Visual Studio 2010:

- запустить Visual Studio 2010;
- файл → Создать → Проект (File → New → Project);
- выберите Visual C++ → Win32;
- выберите "Консольное приложение Win32";
- введите название нового проекта и нажмите "Готово" (Finish);
- в окне редактора кодов осуществляется ввод и обработка непосредственного кода программы или модуля;
- в окно редактора кода следует ввести код (приложение 2) (рисунок 7);
- запустить программу на выполнение (рисунок 8).

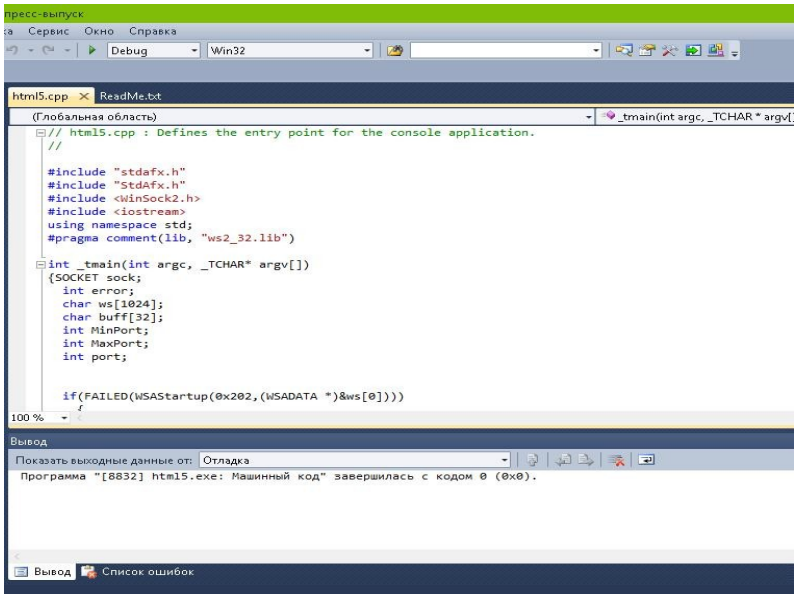

Рисунок 7 - Код программы на Visual C++

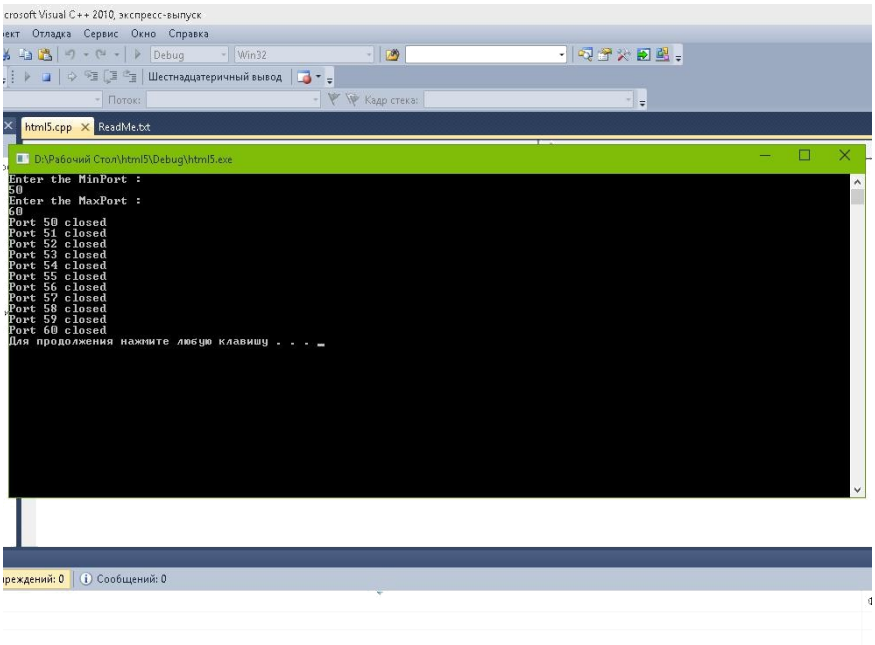

Рисунок 8 - Выполнение программы на Visual C++

Выбранный диапазон портов проверен, порты неуязвимы, для завершения работы программы следует нажать любую клавишу.

3.2.4 Практическая часть

Для выполнения программы необходимо запустить Visual Studio 2010 и открыть файл с кодом исходной программы Port.cpp

Программа требует наличия исходных данных в виде библиотеки Winsock2.h, сразу после успешного запуска выводит на экран сообщение, для ввода диапазона сканируемых портов.

Затем выполняется сканирование заданного диапазона портов.

После вывода на экран информации о просканированных портах программа свою работу не завершает.

Для того, чтобы закрыть и завершить выполнение программы и проверку портов достаточно использовать нажатие любой клавиши или команду выход.

Пользователь при желании может проверить любой порт. Таким образом программа может обрабатывать любой диапазон портов от 0 до 255(256) и проверять их на уязвимости.

3.2.5 Анализ результатов

В результате реализации сканера TCP-портов разработана программа на языке C++ в среде Microsoft Visual Studio 2010, реализующая процесс, описанный в начале главы.

Программа имеет исходные данные в виде базы библиотеки данных Winsock2.h встроенную в среду программирования. Начальное количество данных не может быть изменено в процессе работы программы. Атрибуты обработки портов заданы статичными данными.

Процесс работы программы наглядно отображается на экране.

В результате работы программы на выходе имеем обработанный диапазон портов, проверенный на уязвимости.

ЗАКЛЮЧЕНИЕ

В процессе исследований были изучены методы работы и функционирования вирусов и антивирусов, обработки, фильтрации и распознавания зараженных файлов, также их обезвреживания, в результате чего приобретены практические навыки в этих областях. Для этого использовалась главная начальная функция main, обеспечивающая всю необходимую и правильную работу программы. В процессе исследования были использованы следующие программные средства:

- русифицированная и лицензированная прикладная система разработки Microsoft Visual Studio 2010x32;
- русифицированная прикладная система разработки: QT Creator 5.2.0;
- свободно распространяемая библиотека сигнатуры антивирусных баз.

В ходе исследования были решены следующие задачи:

1 Проведен анализ функционирования, как вирусов, так и антивирусов.

2Изучен алгоритм сигнатурного метода и разработана программа по выявлению «опасных» участков кода.

3Разработан сканер TCP-портов для выявления открытых и уязвимых узлов сети.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Шлее М. Qt4.5. Профессиональное программирование на C++ / М. Шлее. - СПб.: БХВ-Петербург, 2012. - 882 с.

2 Касперски К. Записки исследователя компьютерных вирусов, переиздание / К. Касперски. - М.: Питер, 2014. - 320 с.

3 Яремчук С.А. Защита вашего компьютера / С.А. Яремчук. - М.: Питер, 2015. - 288 с.

4 Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. - М.: ДМК Пресс, 2012. - 544 с.

5 Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с.

6 Партыка Т.Л. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 432 с.

7 Климентьев К. Е. Компьютерные вирусы и антивирусы. Взгляд программиста. / К. Е. Климентьев. - М.: ДМК-Пресс, 2013. - 656 с.

8 Михайлов А.В. Компьютерные вирусы и борьба с ними. / А.В. Михайлов. - М.: Диалог МИФИ, 2013. -104 с.

9 Касперски К. Компьютерные вирусы изнутри и снаружи, переиздание / К. Касперски. - М.: Питер, 2015. - 526 с.

10 Цирлов В.Л. Основы информационной безопасности. Краткий курс. / В.Л. Цирлов. - М.:Феникс, 2012. - 256 с.

11 Роббинс Д. Отладка Windows-приложений / Д. Роббинс. - М.: ДМК Пресс, 2015. - 448 с.

12 Немцова Т.И. Программирование на языке высокого уровня. Программирование на языке C++ / Т.И. Немцова. - М.: ИД ФОРУМ: ИНФРАМ, 2012. - 512 с.

13 Скудис Э. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите / Эд Скудис. - М.: ДМК Пресс, 2017. - 512 с.

14 Трасковский А. В. Сбои и неполадки домашнего ПК / А. В. Трасковский. - СПб.: БХВ-Петербург, 2009. - 512 с.

15 Романов Е. Л. Си/Си++. От дилетанта до профессионала / Е. Л. Романов - М.: ДМК Пресс, 2014. - 581 с.

ПРИЛОЖЕНИЕ А

Антивирус C++.

```
#include "mainwindow.h"
#include "ui_mainwindow.h"
#include <QDir>
#include <QFileInfoList>
#include <QFileInfo>
#include <QFile>
MainWindow::MainWindow(QWidget *parent) :
    QMainWindow(parent),
    ui(new Ui::MainWindow)
{
    ui->setupUi(this);
    ui->lineEdit->setText("C:/");
    connect(ui->pushButton, SIGNAL(clicked(bool)), this, SLOT(spisok()));
}
void MainWindow::spisok()
{
QString line1;
int i=1;bool vir;
QDir dir(ui->lineEdit->text());
QStringList nameFilter; // имя фильтра
// можно задать интересующие расширения nameFilter << "*.png" << "*.jpg"
QFileInfoList list = dir.entryInfoList( nameFilter, QDir::Files );
QFileInfo fileinfo;
foreach (fileinfo, list)
{
vir=true;
ui->textEdit->setText(ui->textEdit->toPlainText()+fileinfo.fileName() +"");
QFile srv;
srv.setFileName(QString::number(i)+".txt");
if (srv.exists())
{
srv.open(QIODevice::ReadOnly);
while (!srv.atEnd())
{
QString line = srv.readLine();
QString a1,a2,sim;
int y=0;
while(line[y]!=' '){
a1=a1+line[y];
y++;
}
while(line[y+1]!=' ' ){
a2=a2+line[y+1];
y++;
}
sim=line[line.length()-3];
int st=a1.toInt();
int st1=a2.toInt();
int k=1;
QFile file;
file.setFileName(fileinfo.absoluteFilePath());
file.open(QIODevice::ReadOnly);
line1 = file.readLine();
while (k!=st)
{
line1 = file.readLine();
k++;
}
file.close();
if(QString(line1[st1-1])!=sim)
{
vir=false;
}
}
i++;
srv.close();
}
if(vir==true)
ui->textEdit->setText(ui->textEdit->toPlainText()+" - virus\n");
else
ui->textEdit->setText(ui->textEdit->toPlainText()+"\n");
}
}
```

ПРИЛОЖЕНИЕ Б

Сканер портов на C++

```
#include "stdafx.h"
#include <WinSock2.h>
#include <iostream>
#include <locale.h>
using namespace std;
#pragma comment (lib, "ws2_32.lib")
int _tmain(int argc, _TCHAR* argv[])
{
setlocale(LC_CTYPE, "Russian");
SOCKET sock;
int error;
char ws[1024];
char buff[32];
int MinPort;
int MaxPort;
int port;
if (FAILED(WSAStartup(0x202,(WSADATA *)&ws[0])))
{
error = WSAGetLastError();
cout << " Ошибка WSAStartup" << endl;
return -1;
}
//устанавливаем socket
if(INVALID_SOCKET == (sock = socket(AF_INET,SOCK_STREAM,0)))

{
error = WSAGetLastError();
cout << "Ошибка сокета" << endl;
return -1;
}
sockaddr_in sock_addr;
ZeroMemory(&sock_addr, sizeof (sock_addr));
sock_addr.sin_family = AF_INET;
sock_addr.sin_addr.S_un.S_addr = inet_addr("127.0.0.1");
// Вводим Port
cout << "Введите минимальный порт :" << endl;
cin >> MinPort;
cout << "Введите максимальный порт :" << endl;
cin >> MaxPort;
for (MinPort;MinPort <= MaxPort;MinPort++)
{
port = MinPort;
sock_addr.sin_port = htons(port);
if(SOCKET_ERROR==(connect(sock,(sockaddr*)&sock_addr,sizeof(sock_addr))))
{error = WSAGetLastError();
cout << "Порт " << port << " закрыт" << endl;
}
else
cout << "Порт " << port << " открыт" << endl;
}
system("PAUSE");
}
```

РЕФЕРАТ

Курсовой проект 45 с., 8 рис., 15 источников, 2 прил.

ВИРУС, АНТИВИРУС, БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА И ИНФОРМАЦИИ, СКАНЕР ПОРТОВ

Объектом исследования являются технологии защиты персонального компьютера от вредоносного программного обеспечения.

Целью работы является изучение и реализация способа выявления зловредного кода и обезвреживание вредоносного программного обеспечения.

В результате выполнения проектной работы проведен анализ функционирования, как вирусов, так и антивирусов, изучен алгоритм сигнатурного метода и разработана программа по выявлению «опасных» участков кода, а также разработан сканер TCP-портов для выявления открытых и уязвимых узлов сети.