МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Казанский (Приволжский) федеральный университет»

ИНСТИТУТ МАТЕМАТИКИ И МЕХАНИКИ ИМ. Н.И. ЛОБАЧЕВСКОГО

КАФЕДРА ТЕОРИИ И ТЕХНОЛОГИЙ ПРЕПОДАВАНИЯ МАТЕМАТИКИ И ИНФОРМАТИКИ

Направление: 050202.65: Информатика с дополнительной специальностью

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Создание консольного приложения с использованием среды MS Visual Studio

Работа завершена:

"___"_____ 201_ г. _____ (З.С.Капкаев)

Работа допущена к защите:

Научный руководитель
к.т.н., доцент

"___"_____ 201_ г. _____ (Т.Ю.Гайнутдинова)

Заведующий кафедрой
д.п.н., профессор

"___"_____ 201_ г. _____ (Л.Р. Шакирова)

Казань – 2015

СОДЕРЖАНИЕ

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, т.е. 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 - веке 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.

Цель выпускной квалификационной работы – разработка консольного приложения в среде программирования C++ для выявления зловредного кода и его обезвреживания.

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 методические рекомендации для учителя информатики по написанию программы: сканера TCP-портов для выявления открытых и уязвимых узлов сети.

Выпускная квалификационная работа состоит из введения, трёх глав, заключения, списка использованной литературы, приложений, а также отдельного дополнительного материала в виде пяти вариантов теста по 10 вопросов каждый, подготовленных для системы MyTestStudent.

ГЛАВА I
АНТИВИРУСЫ И ВИРУСЫ, МЕХАНИЗМЫ РАБОТЫ

1.1. Что есть вирус на самом деле

Компьютерный вирус - это реализованная небольшая по размерам программа, которая может «добавлять» себя к другим программам, а также использовать их (т.е. «заражать» 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 (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.) [19].

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 [8].

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.

1.1.1. 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 (MBR) жесткого диска или винчестера для заражения, также такие вирусы получили большее распространение при использовании флэш карт для хранения данных [5]. 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 [7]. 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 низкоуровневых драйверов для взаимодействия аппаратной части компьютера с программным обеспечением. Существуют вирусы, которые имеют оригинальные тексты программ, библиотечные или объектные модули [7].

Макровирусы (macro viruses) являются также программным продуктом написанном на макроязыках, встроенных в системы обработки данных (табличные процессоры, текстовые процессоры и т.д.) [17]. 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 [10].

Стелс-вирусы любыми способами и средствами скрывают свой факт присутствия в системе [20]. 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 [9].

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" (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 [14]. Таким образом, ре-

зидентные 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 [8].

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 [9].

К **сетевым** относятся вирусы, которые распространяются посредством перемещения по глобальной сети, в частности во всемирной паутине [10]. 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 [9]. 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 [4]. 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 [9]. 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 - 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.

1.1.2. Откуда и куда: источники вирусов

В XXI веке существует превеликое множество источников получения вируса, итак 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, к примеру, гости пришедшие поздравить друга, заглянувшие на пару минут и т.д.

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 [8]. 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 [9].

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.

1.1.3. Кто и зачем пишет вирусы

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.

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 [18].

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 - «электронным злодеям» 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 [16].

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 подавному 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 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.

1.1.4. Мотивы написания вирусов

Окунемся в историю и попробуем понять не только первопричины, но и ответить на вопрос: «Зачем люди пишут вирусы?». На это есть несколько весомых причин и аргументов.

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. «Kit coders». Представленная и рассматриваемая группа не приветствуется как вирусописателями, так и теми, кто занимается защитой информационных и персональных данных [18].

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 [23].

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 [19].

«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[2]. 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 (своего рода бета-тестирование). 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 [4].

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 [11].

Не составит труда догадаться, что 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 [22]. 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:

1. Защита компьютера от вирусов и заражения данных, хранящихся на нем.

2. Обнаружение вирусов и обезвреживание, уже проникших на компьютер.

3. Лечение компьютера, без нанесения вреда функциональности той или иной программе.

4. 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 [5]. 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 обнаруже-

ния 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 [7].

Маска вируса - некоторая последовательность кода, специфичная для этого конкретного вируса, т.е. содержащая последовательность элементов в коде вируса [7]. 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, т.е. анализ последовательности в проверяемом объекте, набор необходимой статистики и принятие первичного решения для каждого проверяемого объекта [5].

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 сов-

падает со значениями, то CRC-сканеры выводят сообщение о том, что файл был изменён или заражён каким-либо вирусом [3].

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 [13]. 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 [3].

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, гаджеты [6]. Как и у каждого представителя поколения «человек» есть свои положительные (сильные) стороны, так и отрицательные, 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 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 [4].

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 [13].

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. Мир знает сервисы, позволяющие проверить компьютер, подключенный к сети Интернет 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 — отсутствуют средства 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 [17].

— 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 [14].

— 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, при-

несенные, допустим соседом. К числу легендарных можно отнести Dr.Web online check, avast! Online Scanner, VirusTotal, Online malware scan [19].

— Firewall. Отчасти данную программу можно отнести к антивирусным средствам защиты двойного назначения (Рис. 1), так как она в режиме реального времени, отражает атаки вирусов и хакеров (компьютерных злоумышленников). Основной механизм — блокировка, сканирование сетевого трафика и обеспечение скрытности и защищенности портов ПК в сети (через блокирование ping, telnet, tracert и других сервисов) [15].

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 и 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 [14].

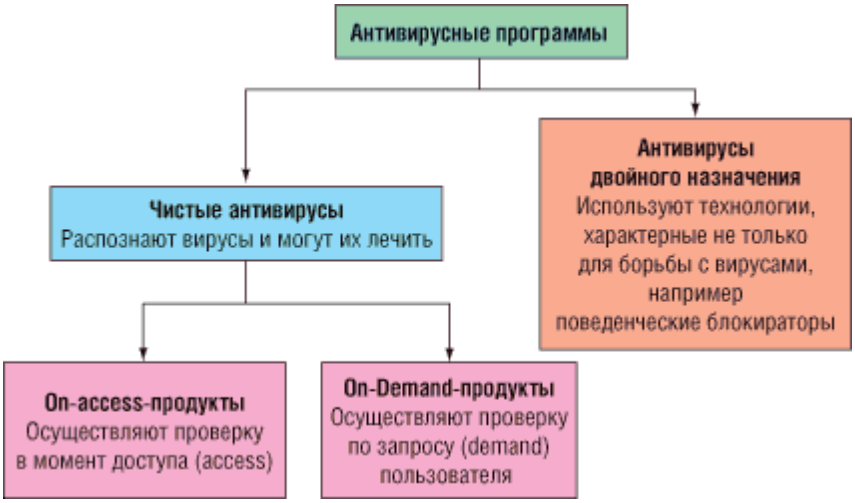

Рис. 1. Категории антивирусных средств

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 2014 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 (т.е. свободной оперативной памяти) необходимого (для X86 и X64 архитектур соответственно) 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 [17].

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 [19]. 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 ком-

плексной 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 этоого 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 прорекламиро-

вать 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.

1.2.3. Эффективность защиты

Попытаемся ответить на один вопрос: «Действительно ли современные антивирусные средства эффективны?»

У миллионов пользователей по всему миру будь то компьютер, ноутбук, планшет или смартфон подключен и функционирует Интернет. А значит, среда и скорость распространения вирусов стала такой же, что и распространения антивирусных баз сигнатур. Опережение антивирусов над вирусами свелось практически к нулю [2].

Вместо операционных систем на достаточно широко известной основе MS DOS (а это, также, вся линейка включающая: Win1.xx–Win3.xx, Win95/96/98/ME) на электронные устройства пришло следующее поколение ядра - Windows NT в реализации Windows 2000/XP. Теперь ядро операционной системы, её код и обрабатываемы данные, надёжно отделены и изолированы от адресного пространства имен обычных прикладных программ, не относящихся к системным[9].

Вирусы пишут ради собственной выгоды и получения блага. Более того, именно «вирусы», практически по прошествии малого количества времени 3-4 года, исчезли с компьютеров и различных девайсов пользователей. Им на смену пришли всевозможные «черви», «троянские кони»,

«блокираторы», ориентированные для получения материальных благ - денег.

В 2000-2005 годах антивирусы не уже могли лечить заражённые сложными вирусами - троянами машины. Вот файловое заражение – запросто, сколько душе угодно, а когда исполняемые модули внедряются в операционную систему – нет. На этом за последние 15 лет выросла целая индустрия «anti–malware»: Spybot Search&Destroy, Ad-Aware, SpySweeper и их различные многовариативные собратья [3].

Антивирусная многомиллиардная индустрия достаточно быстро поняла и осознала, что деньги как вода, утекают из их рук и за короткий срок наверстала упущенное [21].

Вот только скорости распространения вирусов и антивирусных сигнатур повлиял на уровень предотвращений заражения, и не в лучшую сторону, он значительно снизился. Антивирусы стихийно и все больше опаздывают. И практически в реальности уже почти ничего не спасает – ни эвристик, ни поведенческий блокиратор, не анализатор поведения. Программисты и хакеры, которые пишут и создают вирусы, обходят любые мыслимые и немыслимые уровни защиты.

При этом на подавляющем большинстве форумов и хелп-досках с различной периодичностью всплывают темы в ретро стиле: «Антивирус А пропустил заражение, он плохой. Посоветуйте хороший». Человеку советуют и рекомендуют «хороший», который остаётся в привилегированном статусе вплоть до следующего пропуска или заражения [20]. После чего цикл поиска и решения проблемы «хорошего антивируса» повторяется.

При этом возникает отличный парадокс – новые разрабатываемые технологии предотвращения заражения, показывающие абсолютные результаты превосходной защиты в тестах на предотвращение заражения (так именуемые «динамические тесты»), не могут занять место под солнцем, т.к. пришли на рынок довольно-таки сравнительно поздно [4]. Инерция сознания, подавляющего количества людей просто не позволяет и не предостав-

ляет им возможности искать ничего реально «защищающего», кроме антивирусов, и многие так и считают: «Стоит антивирус, я защищен». А на самом то деле защита тождественно равна антивирусу. А ведь антивирусы не лучшие в задаче предотвращения и лечения заражения.

Есть необъятное количество компьютерных изданий, журналисты которых должны и даже обязаны следить за интересными инновационными новинками и писать о них, информируя широкие массы. А они не пишут. Значит, новые технологии защиты плохие?

Да нет, всё не так просто и прозрачно. Когда кто-то создаёт новый, инновационный продукт для рынка, где нет устоявшихся «хороших практик», технологий и лидеров, о нем, безусловно, напишут. Но если это не так, то никто ничего писать и даже думать не будет.

И причин тут несколько:

1. Журналисты - такие же люди. Зачем что-то искать и о чём-то новом писать, если можно сидя на своем удобном насиженном месте получать приличные гонорары за уже имеющиеся разработки, лишь корректируя их.

2. Из-за инерции сознания, пользователи не теребят журналистов писать новые статьи про инновационные средства защиты. Так зачем про них писать и оповещать широкие круги, если читателям не интересно, они не купят и не порекомендуют журнал?

3. Все издания существуют на доходы от рекламы. И антивирусная индустрия спонсирует значительную её часть. Если издание начнёт печатать настоящие «живые» статьи, где говорится о ненадёжности и халатном отношении как антивирусов, так и компаний их производящих, то на следующий же день, или даже через час к нему непременно заглянут представители PR-отдела дистрибьютора или самого производителя антивируса и антивирусных средств, скажут, что сотрудничать с таким изданием, хоть и имеющим вес на мировой арене им невыгодно.

1.2.4. Return on Investment

Попытаемся разобраться в следующем вопросе: «Почему крупные мировые производители и бренды антивирусной индустрии ничего, фактически и практически, нового не предлагают потребителям?»

Все это, как и многое другое зависит от крупных производителей средств защиты, для большинства которых это является лишь средством ведения и поддержания бизнеса. У каждого своего направления, кто-то производит и продаёт Кока-Колу, кто-то - антивирусы. И существенных различий между этими симбиотическими бизнес-процессами нет.

Неизвестные и не «пропиаренные» производители средств защиты, являются воистину неистощимыми энтузиастами, оперируют такими понятиями как «надёжность средства защиты», «адекватность модели угроз» и, может и звучит банально, но гордо «профессиональная компетентность».

Крупные мировые производители оперируют лишь одним кратким термином– ROI.

ROI (Return on Investment) – это «уровень возврата инвестиций». Если кто-то вложился в какое-то производство сигнатурного движка нового поколения для выявления и обнаружения угроз, то сначала деньги нужно вернуть с прибылью и процентами, поделиться ею с акционерами, высшим менеджментом, а уже потом, может быть, сделать или закупить что-нибудь новенькое [19].

И мнение какого-то неизвестного потребителя никого тут не тревожит и не волнует, а подавное большинство настолько запугано и загнано в рамки, что его можно заставить поверить в надёжность чего и кого угодно. Например, Fake антивирусы. Они выглядят, как антивирусы, они сканируют, как антивирусы, они требуют деньги, как антивирусы, они симулируют работу, как антивирусы. Вот только проблемка в том, что не защищают, скорее, наоборот, помогают злоумышленникам завладеть вашей личной информацией.

Рассмотрим один знаменитый пример: в 2005 году не малоизвестная Лаборатория Касперского успешно интегрировала в свою продуктовую линейку программ поведенческий блокиратор. В то замечательное время его не было и не могло быть, по ряду существенных проблем ни в одном антивирусе. И всего пара каких-то стартапов (CyberHawk, после покупки PC Tools'ом- ThreatFire, компания представляет из себя, на данный момент, частью корпорации Symantec, и Sane Security Promary Response Safe Connect, что куплен был когда-то у AVG), безуспешно пытающиеся пробиться в прессу и в массы, завоевать себе место под солнцем.

Через пять лет, ближе к 2010 году, многие производящие стартапы были скуплены за бесценок более крупными игроками, их программные продукты были просто-напросто проинтегрированы в текущие выпускаемые продуктовые линейки именитых брендов. Не иметь у себя в антивирусе поведенческий блокиратор стало нефешенебельно и нерентабельно для большинства производителей [6]. Пробиться в широкие круги и завоевать признание тем стартапам до того, как их купили, так и не получилось.

Превеликое множество доверяет лишь «большим именам», крупным мировым производителям средств реализации информационной защиты, то вам придётся подождать ещё как минимум лет пять-десять, пока текущие инвесторы не получат свои кровные с заоблачными процентами.

Откуда же берётся теневая многомиллионная экономика на зловредном программном обеспечении и ее реализации? А берётся она из простого положительного сальдо между украденными у простого пользователя ресурсами и временем минус стоимость обхода средств защиты [2]. Всё очень просто, логично и систематично.

Какова же на самом деле стоимость обхода и взлома современных антивирусных программных средств? Принимая во внимание то, что эпидемии случаются с завидной регулярностью, а большинство пользователей всё же имеют установленный антивирусный продукт с регулярно обновляемыми сигнатурными антивирусными базами, то результат весьма неуте-

шителен - стоимость обхода современного брендового антивируса достаточно низка, чтобы экономика на зловредном программном обеспечении не имела ни малейшего шанса к существованию и развитию.

Происходит все по одному простому и известному сценарию, потому что все антивирусы, даже самые инновационные и неизвестные реализуют «чёрносписочный» подход к обеспечению целостности информационных данных. Это обозначает лишь одно «я знаю, что это плохой модуль (плохое непредвиденное, зловредное поведение программы), я его блокирую». Достаточно просто подменить или еще проще, замаскировать модуль, обманув сигнатуру и притвориться «хорошо себя ведущей» – всё «оборона прорвана».

Пока информация способная предотвратить несанкционированные и неинициализированные действия дойдет от производителя до пользователя, пройдет львиная часть ценного времени: часов, секунд… Можно смело брать города и страны, никого, не боясь и ничего не опасаясь. А чтобы антивирус больше не мешал своими громкими восклицаниями и различными напоминаниями, взять, да и выключить его. Ничего сложного и сверхъестественного в этом нет.

И только принципиально отличные от уже накатанных и стандартных методов реализации защиты, а также иные подходы способны настолько увеличить стоимость обхода средства защиты, что продолжать «черный» бизнес на зловредном программном обеспечении станет вообще невыгодным и немыслимо дорогим. Почему?

Рассмотрим теневую экономику обхода новых средств защиты изнутри.

Если не брать во внимание список реестра вирусных подходов, то можно выделить всего два основополагающих:

1. На основе «белых списков». То есть, запрещаем запуск и функционирование всего того, про что мы не знаем, что оно заведомо хорошее, незараженное вирусом.

2. На основе популярной модели «песочницы», изолируя потенциально опасные процессы от всех остальных и операционной системы.

Многие представленные на данный момент решения неприменимы ни в одном массовом продукте, поскольку пользователю очень тяжело ими пользоваться. Такие программы будут с завидной частотой выдавать неприемлемое количество ошибок как при обновлениях используемого программного обеспечения, так и при выполнении своих первоочередных задач, например, пока они не попадут в единую центральную базу, хранящую огромную базу контрольных сумм незараженных модулей. Кроме того, на практике все подобные, казалось бы, на первый взгляд уникальные технологии решения, имеют врождённые и патогенные недостатки в виде проблем в работе с файлами как архивными, так и с более большим объемом чем в 10-15 Гбайт одним файлом, содержащими скрипты, поскольку скрипт - это лишь набор обычных текстовых строк, а интерпретируют и инициализируют эти строчки команды к действию вполне себе легитимные (зачастую – основные системные) исполняемые файлы [4]. Так что обойти их либо достаточно тривиально и легко, либо практически невозможно и нереализуемо одним человеком, хакером-одиночкой (но и работать с ними, при этом, также будет практически очень сложно и долго).

Если же рассматривать популярный в последнее время технологию защиты в виде SandBox, то нахождение дыр в тех из них, которые уже давно на мировой арене, достаточно нетривиальная задача, но решаемая при приложении некоторых усилий. Задача, посильная многим профессиональным хакерам, а их многочисленным группировкам тем более, время которых стоит достаточно очень дорого и под частую не по карману даже среднестатистической компании с персоналом в 200-300 человек. Стоимость обхода хорошо реализованной и исполненной с соблюдением всех требований «песочницы» может вылиться заказчику в сотни тысяч и даже миллионов долларов и оказаться довольно таки продолжительной процедурой не только ожидания, но и внедрения. [10].

При использовании либо решений на белых списках, либо «песочниц» бизнес на зловредном программном обеспечении и теневой экономике становится всё менее и менее рентабельным, с каждой следующей итерацией защита становится всё крепче, а обход её всё дороже.

Также следует отметить, что использование инновационных сервисов и реализация новейших, еще неизвестных хакерам и большому числу программистов механизмов защиты, способствует стабильности и устойчивости такого глобального пространства и множества имен как Интернет.

Лишь реализуя и вовремя внедряя новые технологии возможно создание идеального электронного мира, без вирусов и программ шпионов, без возникновения «компьютерных» эпидемий и кражи личных конфиденциальных данных.

ГЛАВА II
КОНСОЛЬНЫЙ АНТИВИРУС В СРЕДЕ C++

2.1. Постановка задачи

Создать консольное приложение в VC++ с использованием интегрированной среды разработки Microsoft Visual Studio.

Например:

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

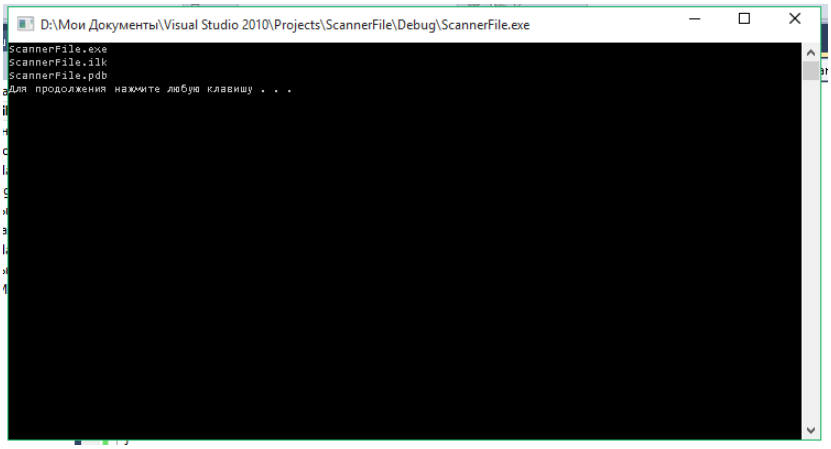

Рис. 2. Загрузка и проверка файлов на вирусы

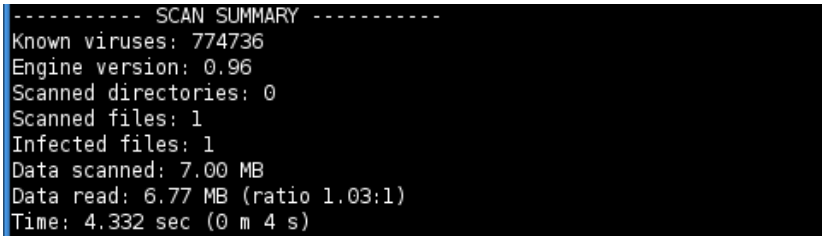

Рис. 3. Файлы, обработанные сканером

2.2. Запуск и настройка VISUAL STUDIO

Создание нового проекта в Visual Studio 2010:

1. Файл → Создать → Проект (File → New → Project) (Рис. 4)

2. Выберите Visual C++ → Win32 (Рис. 5)

3. Выберите "Консольное приложение Win32"

(Win32 Console Application) (Рис. 6)

4. Введите название нового проекта и нажмите "ОК"

5. Нажмите "Готово" (Finish)

6. В окне редактора кодов осуществляется ввод и обработка непосредственного кода программы или модуля. (Рис. 7)

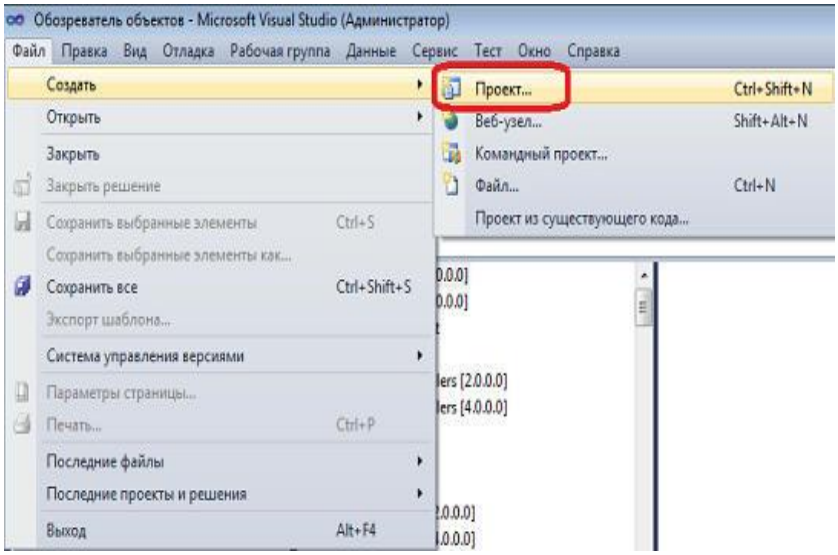

Рис. 4. Файл⟶ Создать проект

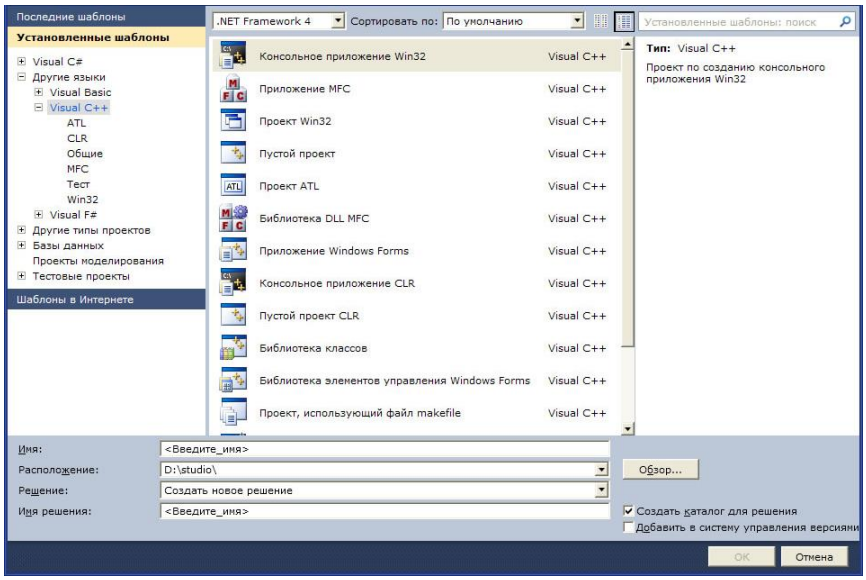

Рис. 5. Visual C++ → Win32

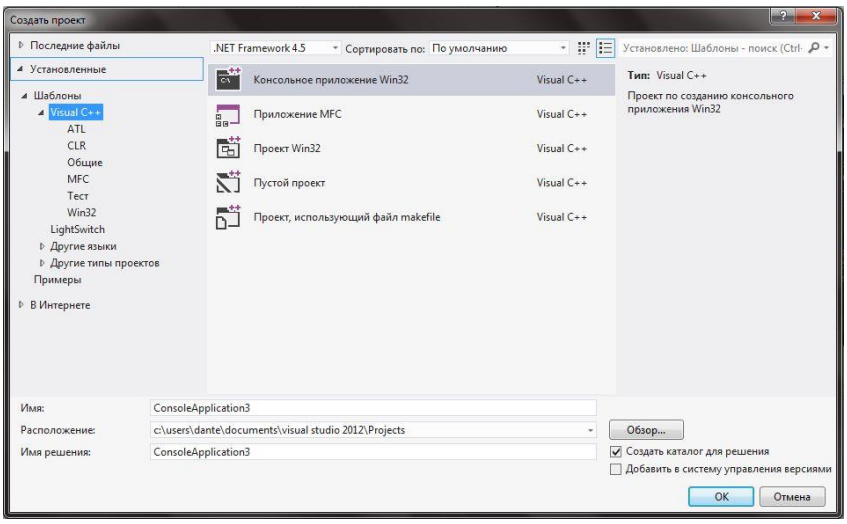

Рис. 6. Консольное приложение Win32 Visual C++

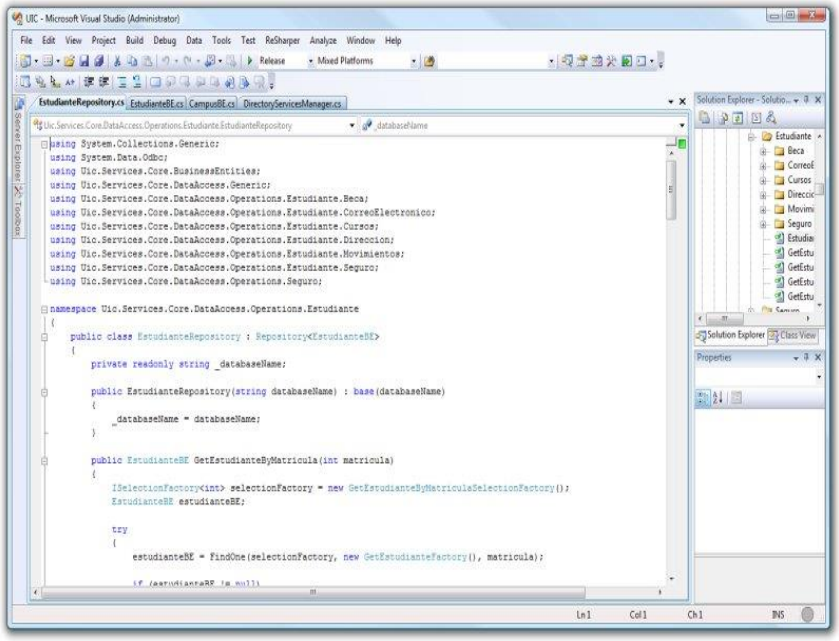

Рис. 7. Окно-редактор кода Visual C++

2.3. Алгоритмизация решения задачи

2.3.1 Описание метода решения

Для решения задачи использована среда программирования Visual Studio C++. Программа разработана как консольное 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 [11].

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.

Сигнатура будет состоять из:

- Смещения последовательности в файле
- Размера последовательности
- Хэша последовательности

2.3.2. Конструирование алгоритма

Структурная схема алгоритма приведена на (Рис. 8) и (Рис.9). Алгоритм основан на описанном ранее методе решении:

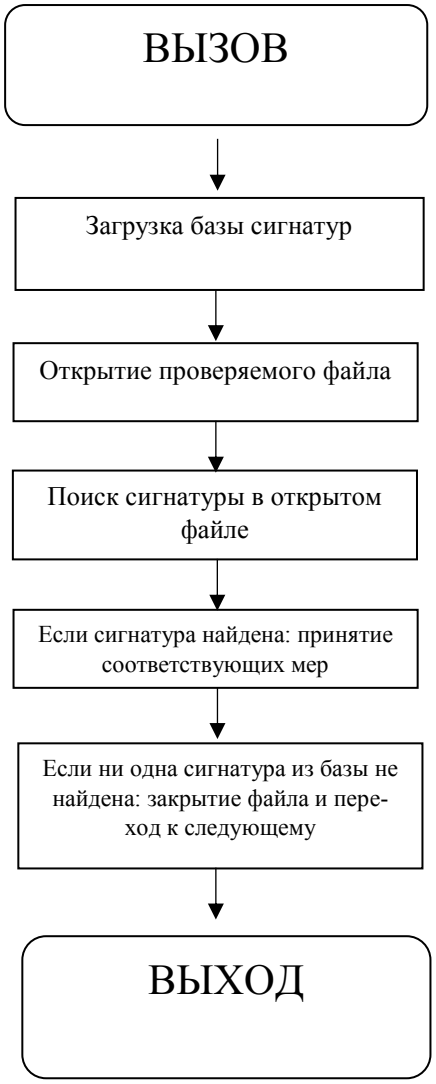

Рис. 8. Блок-схема алгоритма сканера

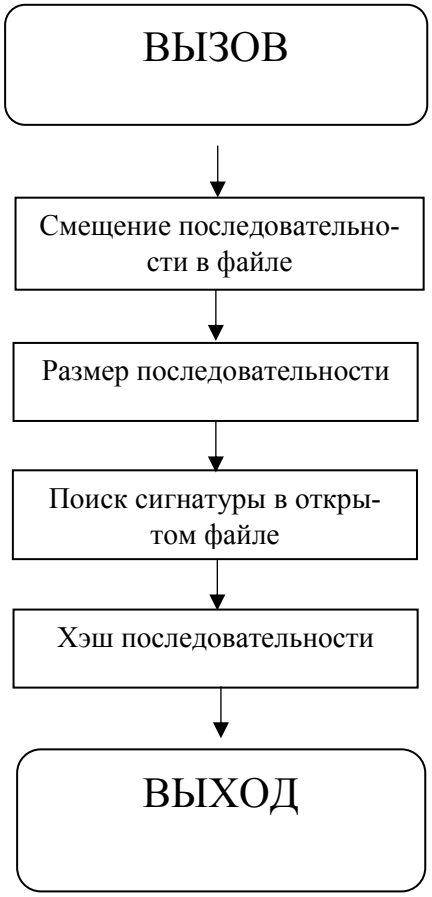

Рис. 9. Блок-схема состояния
сигнатурных данных

2.4. Описание программы

2.4.1. Общие сведения

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 ZAVBFile.cpp

Исполняемый код (ZAVBFile.cpp) занимает на диске 4 КБ.

2.4.2. Структура программы

Программа реализует алгоритм, указанный в предыдущем разделе. Исходный текст программы (см. Приложение) содержит основную часть (функция main).

Таблица 1

Сводная таблица функции

Название	Назначение	Возвращаемое значение	Формальные параметры
main	Головная функция программы	нет	да

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.

2.4.3. Руководство пользователя

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

Программа требует наличия исходных данных в виде сигнатуры баз, сразу после успешного запуска выводит на экран сообщение, что загрузка базы прошла успешно.

После вывода на экран сообщения программа свою работу не завершает.

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

Для того, чтобы закрыть и завершить выполнение и проверку файлов достаточно использовать команду закрытия: exit.

Пользователь при желании может проверить любой файл и произвести его обезвреживание как в автоматическом режиме, так и в ручном. Таким образом программа может обрабатывать любые файлы при наличии расширенной установленной библиотеки базы данных сигнатур& Visual C++ может просканировать и обезвредить практически любой зараженный файл.

2.4.4. Анализ результатов

В результате выполнения курсовой работы разработана программа на языке C++ в среде Microsoft Visual Studio 2010, 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 обработанный ранее зараженный файл отличный от исходного (проверяемого).

Данное консольное приложение для обнаружения и обезвреживания вирусов является открытой и свободно распространяемой программой, в результате чего, ей может воспользоваться любой желающий.

Для учителя информатики она не является основной для изучения, так как её нет в программе и школьном курсе информатики, но данную программу и представленный материал следует использовать, на элективных курсах для развития и улучшения понимания основ и приемов программирования в различных программных средах и языках программирования.

Учителю информатики данная тема будет полезна тем, что он обретет опыт и навыки ориентирования и программирования, а также устранения проблем при работе вирусов и их воздействия на систему, станет лучше понимать и разбираться как работают программы «паразиты» и антивирусные пакеты, осознает важность защиты и сохранения конфиденциальной информации

Узнает, что такое «вирус» и «антивирус» в полном объеме, будет обладать навыками программирования в среде интегрированного программирования Microsoft Visual Studio.

Ученики при изучении данной темы поймут и узнают больше о том, что такое «вирусоопасность», «антивирусный пакет», для чего оно нужно, где используется, а также приобретут практические навыки не только в программировании, но и в защите информации и сохранения ее конфиденциальной.

ГЛАВА III
СКАНЕР TCP-ПОРТОВ

В этой главе рассмотрена реализация простейшего сканера TCP-портов, который будет проверять их доступность и затем организует временное соединение с ними.

Как известно человечество всегда стремилось реализовать свои идеи и мечты, жить лучше, постигать что-то новое, неизведанное. Именно реализация помогла людям создать множество инновационных проектов, воплотить свои мечты в жизнь и помочь миллионам.

Реализация неотъемлемая часть любого процесса созидания, воплощения.

Реализация - осуществление какого-либо плана, идеи, замысла и т. п.

Итак, приступим к действию, сначала взглянем внутрь самого TCP протокола и узнаем, что это такое и с чем его едят.

3.1. TCP

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 [14].

Сокращенное обозначение TCP/IP объединяет огромное количество протоколов, функционирующих между собой и предназначенных для реше-

ния 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 [12]. 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 [12]. 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. [15].

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. Реализуем простейший сканер TCP-портов

Сканер работает по следующему принципу (Рис.10):

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

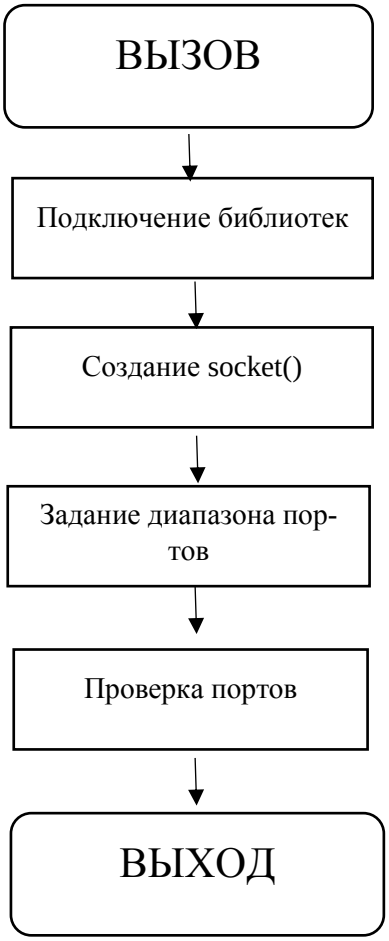

Рис. 10. Блок-схема алгоритма сканера TCP-портов

Реализация алгоритма TCP сканера портов на языке программирования Visual C++ 2010 с подключением необходимых библиотек [1]:

Подключение библиотек и инициализация структуры:

```
#include "stdafx.h"
#include "StdAfx.h"
#include <WinSock2.h>
#include <iostream>
using namespace std;
#pragma comment(lib, "ws2_32.lib")

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

Проверка на выявление ошибок перед запуском программы:

```
 if(FAILED(WSAStartup(0x202,(WSADATA *)&ws[0])))
  {
    error = WSAGetLastError();
    cout << "WSAStartup error" << endl;
    return -1;
  }
```

Создание структуры socket():

```
      if(INVALID_SOCKET == (sock = socket(AF_INET,SOCK_STREAM,0)))
      {
         error = WSAGetLastError();
         cout << "Socket error" << 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 << "Enter the MinPort :" << endl;
        cin >> MinPort;
        cout << "Enter the MaxPort :" << endl;
        cin >> MaxPort;
```

Проверка портов на доступность:

```
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 << "Port " << port << " closed" << endl;
      else
           cout << "Port " << port << "Open" << endl;
      }

   system("PAUSE");
}
```

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 ScanPort.cpp

Исполняемый код (ScanPort.cpp) занимает на диске 4 КБ.

3.2.2. Общие сведения

Программа реализует алгоритм, указанный в предыдущем разделе. Исходный текст программы (см. Приложение) содержит основную часть (функция main).

Таблица 2

Сводная таблица функции

Название	Назначение	Возвращаемое значение	Формальные параметры
main	Головная функция программы	нет	да

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:

1. Запустить Visual Studio 2010 (Рис. 11)
2. Файл → Создать → Проект (File → New → Project) (Рис. 12)
3. Выберите Visual C++ → Win32 (Рис. 13)
4. Выберите "Консольное приложение Win32"
(Win32 Console Application) (Рис. 14)
5. Введите название нового проекта и нажмите "Готово" (Finish) (Рис. 15)
6. В окне редактора кодов осуществляется ввод и обработка непосредственного кода программы или модуля (Рис. 16)
7. В окно редактора кода следует ввести код (Приложение 2) (Рис. 17)
8. Запустить программу на выполнение (Рис. 18)

Рис. 11. Запуск Visual Studio

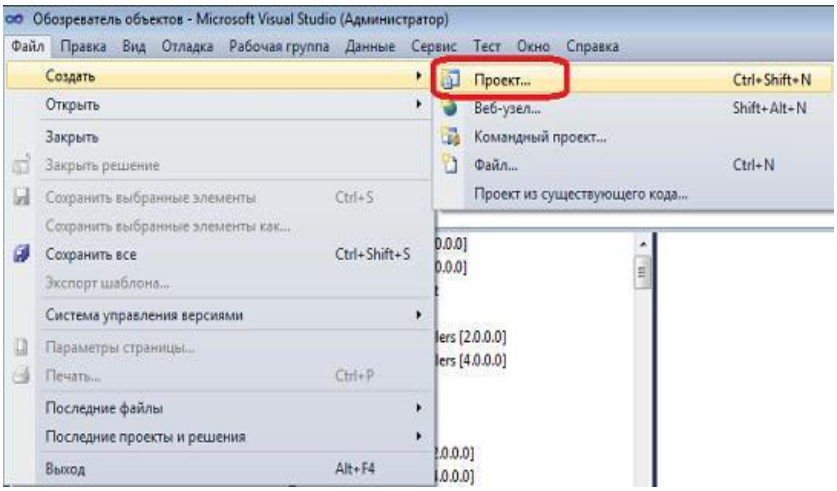

Рис. 12. Файл⟶ Создать проект

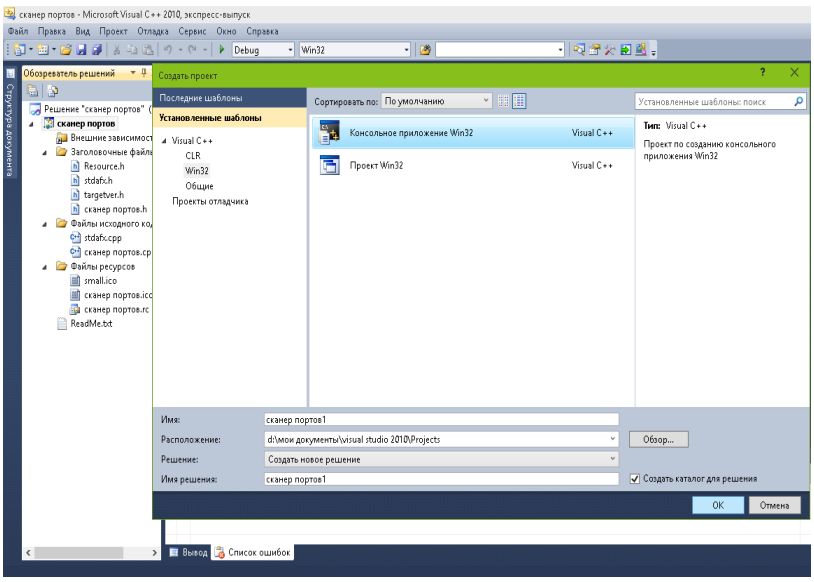

Рис. 13. Visual C++ → Win32

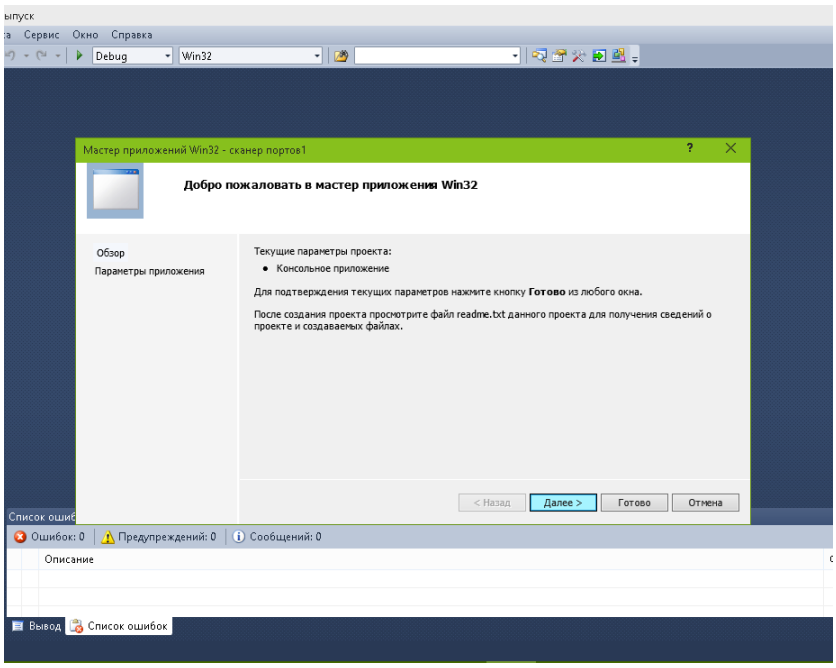

Рис. 14. Консольное приложение Win32 Visual C++

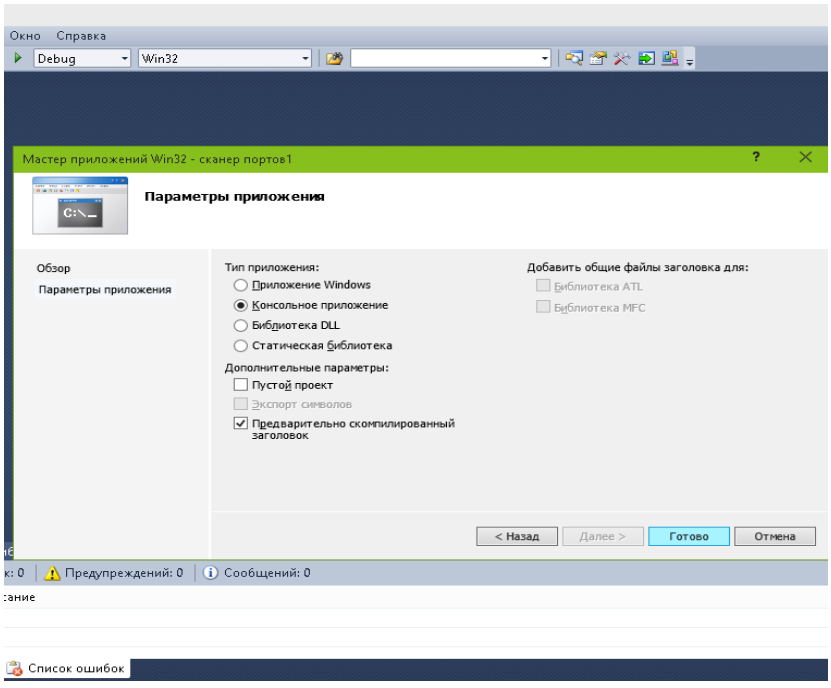

Рис. 15. Ввод имени нового проекта

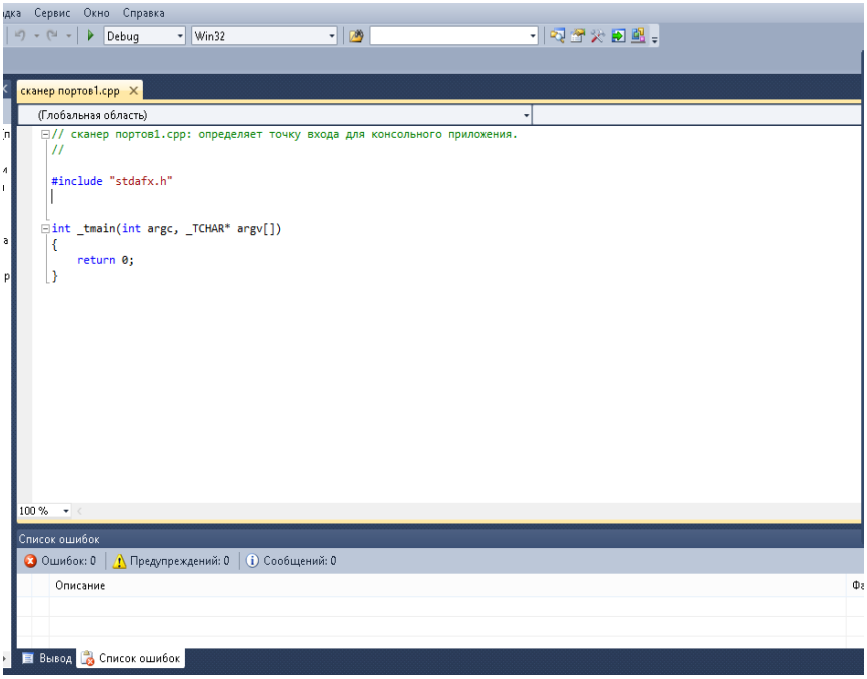

Рис. 16. Окно-редактор кода Visual C++

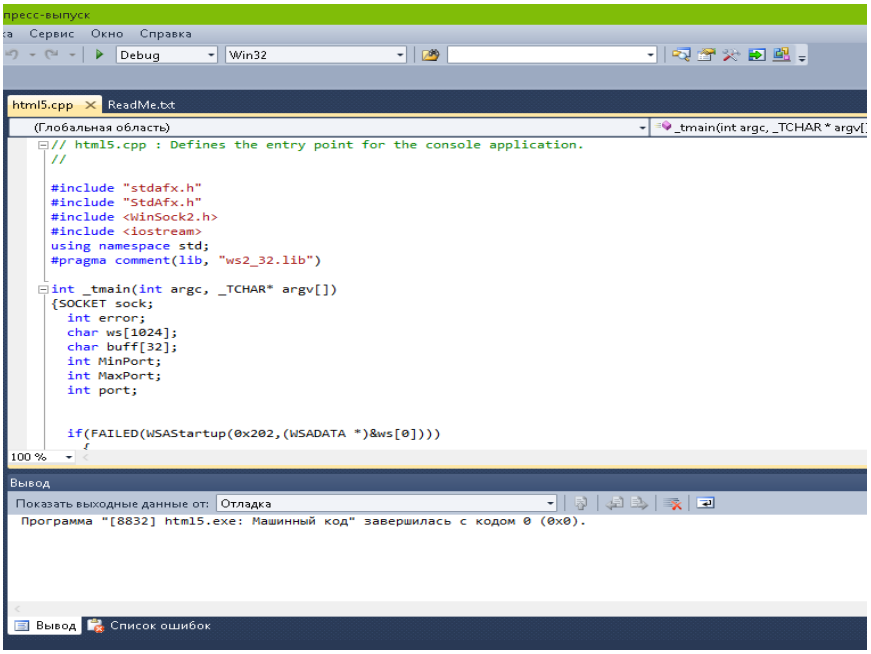

Рис. 17. Код программы на Visual C++

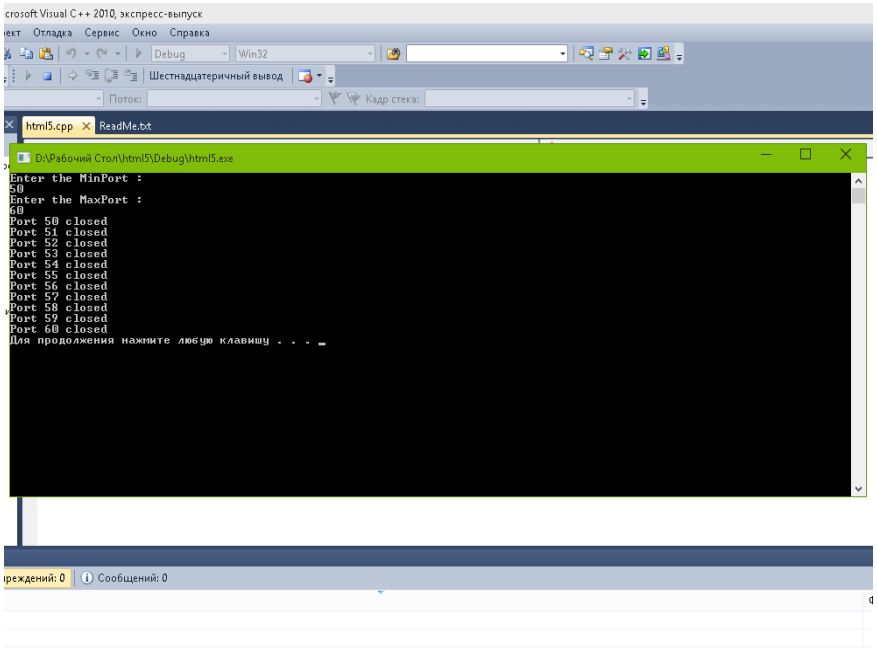

Рис. 18. Выполнение программы на Visual C++

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 ScanPort.cpp

Программа требует наличия исходных данных в виде библиотеки Winsock2.h, сразу после успешного запуска выводит на экран сообщение-запрос, 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 консольный программы. В процессе исследования были использованы следующие программные средства:

- русифицированная и лицензированная прикладная система разработки: Microsoft Visual Studio 2010x32;
- свободно распространяемая библиотека сигнатуры антивирусных баз от Clam AV.

В ходе исследования были решены следующие задачи:

- проведен анализ функционирования, как вирусов, так и антивирусов;
- создан алгоритм действия и разработана программа по выявлению «опасных» участков кода и их обезвреживанию;
- разработаны методические рекомендации для учителя информатики по написанию программы: сканера TCP-портов для выявления открытых и уязвимых узлов сети.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Qt4.5. Профессиональное программирование на C++ / М. Шлее. - СПб.: БХВ-Петербург, 2010. - 882 с. - (В подлиннике). - ISBN 978-5-9775-0398-3. http://znanium.com/bookread.php?book=350671
2. Записки исследователя компьютерных вирусов / К. Касперски. - М.: Питер, 2006. -320 с. - ISBN: 5-469-00331-0 http://www.livelib.ru/book/1000092510
3. Защита Вашего Компьютера / С.А. Яремчук. - М.: Питер, 2008. - 288 с. - ISBN: 978-5-388-00236-5 http://seomurena.ru/name/8000-183737-zashitavashegokomputera.html
4. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. http://znanium.com/bookread.php?book=408107
5. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5, 1000 экз. http://znanium.com/bookread.php?book=335362
6. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2008. - 432 с.: ил.; 60x90 1/16. - (Проф. обр.). (п) ISBN978-5-91134-246-3,3000экз. http://znanium.com/catalog.phpbookinfo=167284
7. Компьютерные вирусы и антивирусы. Взгляд программиста. / К. Е. Климентьев. - М.: ДМК-Пресс, 2013. - 656 с. - ISBN: 978-5-94074-885-4 http://lynxlab.org/11421-kompjuternye-virusy-i-antivirusy-vzgljad.html
8. Компьютерные вирусы и борьба с ними. / А.В. Михайлов. - М.: Диалог-МИФИ, 2011. -104 с. - ISBN 978-5-86404-236-6 http://compinterlit.net/960-kompjuternye-virusy-i-borba-s-nimi-a-v-mihajlov.html
9. Компьютерные вирусы изнутри и снаружи / К. Касперски. - М.: Питер,2006. - 526 с. - ISBN 5-469-00982-3 http://al24.ru/pdf_kniga_2663.html
10. Основы информационной безопасности. Краткий курс. / В.Л. Цирлов. - М.:Феникс, 2008. - 256 с. - ISBN 978-5-222-13164-0 http://rutracker.org/forum/viewtopic.php?t=1013955

11. Отладка Windows-приложений [Электронный ресурс] / Д. Роббинс; Пер. с англ. - М.: ДМК Пресс, 2009. - 448 с., ил. - (Серия «Для программистов»). - ISBN 5-94074-085-5. http://znanium.com/bookread.php?book=407747

12. Программирование на языке высокого уровня. Программир. на языке С++: Уч. пос. / Т.И.Немцова и др.; Под ред. Л.Г.Гагариной - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 512 с.: ил.; 60x90 1/16 + CD-ROM. - (Проф. обр.). (п) ISBN 978-5-8199-0492-3, 1000 экз. http://znanium.com/bookread.php?book=244875

13. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите [Электронный ресурс] / Эд Скудис; Пер. с англ. - М.: ДМК Пресс, 2009. - 512 с.: ил. - (Серия «Защита и администрирование»). - ISBN 5-94074-170-3. http://znanium.com/bookread.php?book=408590

14. Сбои и неполадки домашнего ПК [Электронный ресурс] / А. В. Трасковский. - 2-е изд., перераб. и доп. - СПб.: БХВ-Петербург, 2009. - 512 с.: ил. - (Самоучитель). - ISBN 978-5-94157-964-8. http://znanium.com/bookread.php?book=489309

15. Си/Си++. От дилетанта до профессионала. Электронное учебное пособие по дисциплинам "Информатика", "Программирование», «Технология программирования" для студентов 1-2 курсов направления 230100: учебное пособие / Е. Л. Романов - Новосибирский государственный технический университет, № гос. регистрации 0321000528, 2010. - 581 с. http://ciu.nstu.ru/kaf/persons/91/edu_actions/metod

ИНТЕРНЕТ - ИСТОЧНИКИ

16. Всемирная история заражений – http://lenta.ru/articles/2014/11/18/virus/

17. Информационные технологии – http://habrahabr.ru/

18. Кто и зачем пишет вирусы – http://zillya.ua/ru/kto-i-zachem-pishet-virusy

19. Лаборатория Касперского – http://securelist.ru/

20. Рейтинги антивирусов – http://it-sektor.ru/proplachennaya-stat-ya-ili-kak-nakruchivaut-reyiting-antivirusov.html

21. Форум программистов – http://codenet.ru/

22. Форум программистов и сисадминов – http://cyberforum.ru/

23. Центр исследования компьютерной преступности – http://crime-research.ru/

Приложение 1

Консольный антивирус C++

Код программы (Листинг)

Код на языке 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, 4 * 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;
}

bool ZAVBFileReader::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, 4 * 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;
}
```

Приложение 2

Сканер портов на C++

Код программы (Листинг)

Код на языке VC++:

```
#include "stdafx.h"
#include <WinSock2.h>

#include <iostream>
Using namespace std;
#pragma comment (lib, "ws2_32.lib")
int _tmain(int argc, _TCHAR* argv[])
{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 << "WSAStartup error" << endl;
return -1;
}
//устанавливаем socket
if(INVALID_SOCKET == (sock = socet(AF_INET,SOCK_STREAM,0)))
```

```
{
error = WSAGetLastError();
cout << "Socket error" << 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 << "Enter the MinPort :" << endl;
cin >> MinPort;
cout << "Enter the MaxPort :" << 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 << "Port " << port << " closed" << endl;
else
cout << "Port " << port << "Open" << endl;
}
system("PAUSE");
}
```

Приложение 3

Контрольные измерительные материалы

ОБЩИЕ СВЕДЕНИЯ

Контрольные измерительные материалы (КИМ) выполнены в виде тестов с выбором нескольких или одного правильного ответа, а также с выбором своего индивидуального ответа. Все КИМы выполнены для работы в программе MyTestStudent версии 10.0 и выше. Всего КИМ содержит пять вариантов тестов с соответствующими расширениями: *mtf. Также тесты представлены в формате *doc, что позволяет преподавателю, без труда как править их, так и проводить проверку, после «ручного» тестирования. Правильные варианты ответов также содержатся в файлах с расширением *doc.

Время прохождения одного теста с 10 вопросами – 10 минут.

Тест: «Компьютерная безопасность»

Вариант №1

(10 вопросов)

Верные варианты ответов выделены жирным.

Вопрос 1:

Заражение компьютерными вирусами может произойти в процессе ...

a) печати на принтере;

b) работы с файлами;

c) форматирования дискеты;

d) выключения компьютера.

Вопрос 2:

Компьютерным вирусом является:

a) программа проверки и лечения дисков,

b) любая программа, созданная на языках низкого уровня,

c) программа, скопированная с плохо отформатированной дискеты,

d) специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью " размножаться ".

Вопрос 3:

Что необходимо иметь для проверки на вирус жесткого диска?

a) защищенную программу

b) загрузочную программу

c) файл с антивирусной программой

d) флеш-карту с антивирусной программой, защищенную от записи

Вопрос 4:

Какая программа не является антивирусной?

a) AVP

b) Defrag

c) Norton Antivirus

d) Dr Web

Вопрос 5:

Как вирус может появиться в компьютере?

a) переместиться с гибкого диска

b) при решении математической задачи

c) при подключении к компьютеру модема

d) самопроизвольно

Вопрос 6:

Как происходит заражение "почтовым" вирусом?

a) при открытии зараженного файла, присланного с письмом по e-mail

b) при подключении к почтовому серверу

c) при подключении к web-серверу, зараженному "почтовым" вирусом

d) при получении с письмом, присланном по e-mail, зараженного файла

Вопрос 7:

Заражению компьютерными вирусами могут подвергнуться...

a) графические файлы

b) программы и документы

c) звуковые файлы

d) видеофайлы

Вопрос 8:

Компьютерный вирус можно обнаружить с помощью ...

a) специальных программ

b) специальных аппаратных средств

c) счетчика Гейгера

d) визуально

Вопрос 9:

Что делать при обнаружении вируса?

a) продолжить работу

b) лечить зараженные файлы

c) отформатировать зараженный диск

d) открыть(запустить) зараженный файл

Вопрос 10:

Что из перечисленного ниже не является средством борьбы с компьютерным вирусом?

a) Norton antivirus

b) Dr.Web

c) AVP

d) Far-manager

Тест: «Компьютерная безопасность»

Вариант №2

(10 вопросов)

Верные варианты ответов выделены жирным.

Вопрос 1:

Сопоставьте названия программ и изображений

Укажите соответствие для всех 6 вариантов ответа:

1) 

2) 

3) 

4) 

5) 

6) 

Ответы:

3__ Antivir

4__ DrWeb

1__ Nod 32

6__ Antivirus Kaspersky

2__ Avast

5__ Antivirus Panda

Вопрос 2:

RAID-массив это

Выберите один из 5 вариантов ответа:

1) Набор жестких дисков, подключенных особым образом

2) Антивирусная программа

3) Вид хакерской утилиты

4) База защищенных данных

5) Брандмауэр

Вопрос 3:

Выразите свое согласие или несогласие

Укажите истинность или ложность вариантов ответа:

__ Почтовый червь активируется в тот момент, когда к вам поступает электронная почта

__ Если компьютер не подключен к сети Интернет, в него не проникнут вирусы

__ Файловые вирусы заражают файлы с расширениями *.doc, *.ppt, *.xls

__ Чтобы защитить компьютер недостаточно только установить антивирусную программу

__ На Web-страницах могут находится сетевые черви

Вопрос 4:

Отметьте составные части современного антивируса

Выберите несколько из 5 вариантов ответа:

1) Модем

2) Принтер

3) **Сканер**

4) **Межсетевой экран**

5) **Монитор**

Вопрос 5:

Вредоносные программы - это

(выберите один из вариантов ответа)

Выберите один из 5 вариантов ответа:

1) шпионские программы

2) **программы, наносящие вред данным и программам, находящимся на компьютере**

3) антивирусные программы

4) программы, наносящие вред пользователю, работающему на зараженном компьютере

5) троянские утилиты и сетевые черви

Вопрос 6:

К вредоносным программам относятся:

(выберите несколько вариантов ответа)

Выберите несколько из 5 вариантов ответа:

1) **Потенциально опасные программы**

2) **Вирусы, черви, трояны**

3) **Шпионские и рекламмные программы**

4) Вирусы, программы-шутки, антивирусное программное обеспечение

5) Межсетевой экран, брандмауэр

Вопрос 7:

Сетевые черви это

Выберите один из 5 вариантов ответа:

1) Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты

2) Вирусы, которые проникнув на компьютер, блокируют работу сети

3) Вирусы, которые внедряются в документы под видом макросов

4) Хакерские утилиты, управляющие удаленным доступом компьютера

5) **Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей**

Вопрос 8:

К биометрической системе защиты относятся:

(выберите несколько вариантов ответа)

Выберите несколько из 5 вариантов ответа:

1) Защита паролем

2) Физическая защита данных

3) Антивирусная защита

4) **Идентификация по радужной оболочке глаз**

5) **Идентификация по отпечаткам пальцев**

Вопрос 9:

Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется...

Выберите один из 5 вариантов ответа:

1) **Загрузочный вирус**

2) Макровирус

3) Троян

4) Сетевой червь

5) Файловый вирус

Вопрос 10:

Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию.

Верный ответ: «Троян»

Тест: «Компьютерная безопасность»

Вариант №3

(10 вопросов)

Верные варианты ответов выделены жирным.

Вопрос 1:

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются

Выберите один из 4 вариантов ответа:

1) пароли

2) анкеты

3) коды

4) ярлыки

Вопрос 2:

От несанкционированного доступа может быть защищён:

Выберите несколько из 4 вариантов ответа:

1) каждый диск

2) папка

3) файл

4) ярлык

Вопрос 3:

К биометрическим системам защиты информации относятся системы идентификации по:

Выберите несколько из 9 вариантов ответа:

1) отпечаткам пальцев

2) характеристикам речи

3) радужной оболочке глаза

4) изображению лица

5) геометрии ладони руки

6) росту

7) весу

8) цвету глаз

9) цвету волос

Вопрос 4:

Какие существуют массивы дисков RAID?

Выберите несколько из 4 вариантов ответа:

1) RAID 0

2) RAID 1

3) RAID 10

4) RAID 20

Вопрос 5:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) Для создания массива этого уровня понадобится как минимум два диска одинакового размера. Запись осуществляется по принципу чередова-

ния: данные делятся на порции одинакового размера (A1, A2, A3 и т.д.), и поочерёдно распределяются по всем дискам, входящим в массив.

2) Массивы этого уровня построены по принципу зеркалирования, при котором все порции данных (A1, A2, A3 и т.д.), записанные на одном диске, дублируются на другом.

1) RAID 0

2) RAID 1

Вопрос 6:

Выберите типы вредоносных программ:

Выберите несколько из 6 вариантов ответа:

1) Вирусы, черви, троянские и хакерские программы

2) Шпионское, рекламное программное обеспечение

3) Потенциально опасное программное обеспечение

4) Операционная система Linux

5) Операционная система Windows

6) Microsoft Office

Вопрос 7:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) сигнатуры. Сигнатура - это некоторая постоянная последовательность программного кода, специфичная для конкретной вредоносной программы.

2) алгоритмы эвристического сканирования, т.е.анализа последовательности команд в проверяемом объекте.

1) Для поиска известных вредоносных программ используются

2) Для поиска новых вирусов используются

Вопрос 8:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) автоматически при старте операционной системы и работает в качестве фонового системного процессора, проверяя на вредоносность совершаемые другими программами действия. Основная задача состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера.

2) по заранее выбранному расписанию или в произвольный момент пользователем. Производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера.

1) Антивирусный монитор запускается

2) Антивирусный сканер запускается

Вопрос 9:

Компьютерные вирусы -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Вопрос 10:

По "среде обитания" вирусы можно разделить на:

Выберите несколько из 6 вариантов ответа:

1) загрузочные

2) файловые

3) макровирусы

4) очень опасные

Тест: «Компьютерная безопасность»

Вариант №4

(10 вопросов)

Верные варианты ответов выделены жирным.

Вопрос 1:

Руткит - это...

Выберите один из 5 вариантов ответа:

1) вредоносная программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю

2) разновидность межсетевого экрана

3) программа использующая для распространения Рунет (Российскую часть Интернета)

4) вредоносная программа, маскирующаяся под макрокоманду

5) программа для скрытого взятия под контроль взломанной системы

Вопрос 2:

Компьютерные вирусы это

Выберите несколько из 5 вариантов ответа:

1) Вредоносные программы, наносящие вред данным.

2) Программы, уничтожающие данные на жестком диске

3) Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.

4) Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера

5) Это скрипты, помещенные на зараженных интернет-страничках

Вопрос 3:

Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...

Выберите один из 5 вариантов ответа:

1) Загрузочный вирус

2) Макровирус

3) Файловый вирус

4) Сетевой червь

5) Троян

Вопрос 4:

Укажите порядок действий при наличии признаков заражения компьютера

Укажите порядок следования всех 3 вариантов ответа:

2) Сохранить результаты работы на внешнем носителе

3) Запустить антивирусную программу

1) Отключиться от глобальной или локальной сети

Вопрос 5:

Вирус поражающий документы называется

Выберите один из 5 вариантов ответа:

1) Троян

2) Файловый вирус

3) Макровирус

4) Загрузочный вирус

5) Сетевой червь

Вопрос 6:

Найди соответствие.

Укажите соответствие для всех 3 вариантов ответа:

1) заражают загрузочный сектор гибкого или жёсткого диска.

2) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске.

3) существуют для интегрированного офисного приложения Microsoft Office.

1) загрузочные вирусы

2) файловые вирусы

3) макровирусы

Вопрос 7:

Сетевые черви -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация

может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Вопрос 8:

Сетевые черви бывают:

Выберите несколько из 4 вариантов ответа:

1) Web-черви

2) почтовые черви

3) черви операционной системы

4) черви MS Office

Вопрос 9:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) Профилактическая защита от таких червей состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.

2) Профилактическая защита от таких червей состоит в том, что не рекомендуется открывать вложенные в сообщения файлы, полученные от сомнительных источников. А также рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.

1) Web-черви

2) почтовые черви

Вопрос 10:

Наиболее эффективны от Web-червей, Web-антивирусные программы, которые включают:

Выберите несколько из 3 вариантов ответа:

1) межсетевой экран

2) модуль проверки скриптов

3) антивирусный сканер

Тест: «Компьютерная безопасность»

Вариант №5

(10 вопросов)

Верные варианты ответов выделены жирным.

Вопрос 1:

Межсетевой экран (брандмауэр) -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредонос-

ной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Вопрос 2:

Троянская программа, троянец -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Вопрос 3:

Троянские программы бывают:

Выберите несколько из 4 вариантов ответа:

1) утилиты удалённого администрирования

2) программы - шпионы

3) рекламные программы

4) программы удаления данных на локальном компьютере

Вопрос 4:

Найди соответствие.

Укажите соответствие для всех 3 вариантов ответа:

1) троянские программы данного типа являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий, в том числе они могут быть использованы для обнаружения и передачи конфиденциальной информации.

2) троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

3) эти программы встраивают рекламу в основную полезную программу и могут выполнять функцию троянских программ. Эти программы могут скрытно собирать различную информацию о пользователе компьютера и затем отправлять её злоумышленнику.

1) Троянские утилиты удалённого администрирования

2) Троянские программы - шпионы

3) Рекламные программы

Вопрос 5:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера.

2) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров.

1) DoS – программы

2) DDos – программы

Вопрос 6:

Руткит -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Вопрос 7:

Межсетевой экран позволяет:

Выберите несколько из 5 вариантов ответа:

1) блокировать хакерские DoS - атаки, не пропуская на защищаемый компьютер сетевые пакеты с определённых серверов

2) не допускать проникновение на защищаемый компьютер сетевых червей

3) препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере

4) видеть действия котрые выполняет пользователь на другом компьютере

5) использовать принтер подключённый к другому компьютеру

Вопрос 8:

Кто разработал антивирусную программу Dr.Web?

1)Анатолий Данченко;

2)Валерий Игорев;

3)Александр Климов;

4)Игорь Данилов.

Вопрос 9:

Что относится к основным источникам заражения компьютера?

1)Жесткий диск;

2)Флешки;

3)Интернет;

4)Принтер.

Вопрос 10:

Одним из популярных антивирусов является:

1) антивирус Касперского;

2) Norton;

3)Dr.Web.

4)Avast

5)Zemana