Муниципальное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа №2

ИНДИВИДУАЛЬНЫЙ ИТОГОВЫЙ ПРОЕКТ
НА ТЕМУ

«Компьютерные вирусы»

Выполнил:
Тучков Михаил Денисович,
ученик 9 класса МБОУ СОШ № 2

Руководитель проекта:
Шибаев Сергей Юрьевич,
учитель информатики
МБОУ СОШ № 2

с.Южаково
2020 г.

Оглавление

ВВЕДЕНИЕ

В настоящее время компьютер прочно вошел в повседневную жизнь, и без них уже не может обойтись ни один человек. И в связи с этим особенно обострилась проблема защиты информации.

Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Большинство пользователей компьютеров обеспокоены тем, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность.

К сожалению, сегодня массовое применение персональных компьютеров оказалось связанным с появлением самовоспроизводящихся программ - вирусов которые препятствуют нормальной работе ПК, разрушающих файловую структуру дисков и наносящих ущерб информации, хранимой в компьютере.

До середины 20 века термин «вирус» использовался лишь в медицине, обозначая инфекционный агент, вызывающий заболевание, но с появлением, развитием и усложнением компьютерной техники, систем хранения, обработки и передачи информации, а также соответствующего программного обеспечения возник новый класс программ, известный теперь как компьютерные вирусы

Цель исследовательской работы:

Изучение пути проникновения компьютерных вирусов, виды компьютерных вирусов, а также методы борьбы с ними.

ЗАДАЧИ:

1. Изучить литературу по выбранной теме проекта.
2. Узнать, что такое компьютерные вирусы и когда они появились.
3. Описать классификацию и основные виды вирусных программ.
4. Выявить средства профилактики и борьбы с вирусами.
5. Рассмотреть меры ответственности за нарушения в информационной сфере в России.
6. Развивать навыки самостоятельной работы с материалами сети Интернет и учебной литературой

Гипотеза исследования: если человек знает больше о компьютерных вирусах, то он сможет осуществить более эффективную профилактику заражения компьютера.

Предмет исследования: компьютерные вирусы

Актуальность: Компьютерные вирусы довольно распространенное явление, и методы защиты и борьбы с ними постоянно требуют совершенствования и модернизации и если не принимать меры по устранению компьютерных вирусов, то они смогут исказить или уничтожить жизненно-важную информацию, которая может привести не только к финансовым и временным потерям, но и вызвать человеческие жертвы.

Методы исследования: изучение СМИ, литературы и Интернет - ресурсов.

Глава I. Основные понятия

1.1 Что такое компьютерные вирусы и когда они появились

Понятие «компьютерные вирусы» на слуху у каждого. Однако, многие пользователи имеют слабое представление о самой природе вирусов, хотя они распространены повсеместно и могут значительно повлиять на безопасность каждого.

Что такое компьютерный вирус? Компьютерный вирус — вид вредоносного программного обеспечения, способный создавать копии самого себя и внедряться в код других программ, а также распространять свои копии по разнообразным каналам связи с целью, удаления файлов, блокирования работы пользователей или же приведение в негодность аппаратных комплексов компьютера. Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения.

Идея компьютерных вирусов впервые обсуждалась в серии лекций математика Джона фон Неймана в конце 1940-х годов; в 1966 году вышла его монография «Теория самовоспроизводящихся автоматов» – по сути, это мысленный эксперимент, рассматривающий возможность существования «механического» организма – например, компьютерного кода – который бы повреждал машины, создавал собственные копии и заражал новые машины аналогично тому, как это делает биологический вирус.

По началу, компьютерные вирусы создавали программисты энтузиасты. Но сегодня почти все современные вирусы создаются злоумышленниками и совсем не для игрушек, а с целью заполучить конфиденциальные данные пользователя или использовать его компьютер в личных целях.

В 1961 году инженеры Виктор Высоцкий, Дуг Макилрой и Роберт Моррис из фирмы Bell Telephone Laboratories разработали маленькие программы, способные делать копии самих себя. Это были первые вирусы. Они были созданы в виде игры, которую инженеры назвали «Дарвин», целью которой было отправлять эти программы друзьям, чтобы посмотреть, какая из них уничтожит больше программ оппонента и сделает больше собственных копий. Игрок, которому удавалось заполнить компьютеры других, объявлялся победителем.

В начале 1970-х годов в прототипе современного Интернета - военной компьютерной сети APRAnet - был обнаружен вирус Creeper. Эта программа была в состоянии самостоятельно войти в сеть через модем и передать свою копию удаленной системе. Это был безобидный вирус.

В 1981 году появился вирус Elk Cloner. Он записывался в загрузочные сектора дискет, к которым шло обращение. Проявлялся вирус следующим образом: Elk Cloner переворачивал изображение на экране, заставлял мигать текст, выводил разнообразные сообщения.

В 1983 году Лен Эйделман впервые употребляет термин "вирус" в применении к саморазмножающимся компьютерным программам. В этом же году Фред Коэн, родоначальник современной компьютерной вирусологии, на

семинаре по компьютерной безопасности демонстрирует вирусоподобную программу, способную внедряться в другие объекты, а годом позже дает научное определение термину "компьютерный вирус".

В 1986 году зарегистрирована первая глобальная эпидемия вируса. Вирус Brain, заражающий загрузочные сектора дискет, в течение нескольких месяцев распространился практически по всему миру.

1988 год – вторая глобальная эпидемия. Вирус Jerusalem обнаружил себя сам: в пятницу, 13-го, он уничтожал все запускаемые на зараженном компьютере файлы. Ноябрь 1988 года: повальная эпидемия настоящего сетевого вируса, получившего название червь Морриса. Вирус заразил более 6000 компьютерных систем в США (включая Исследовательский центр NASA). В это время стали появляться первые компании-разработчики антивирусного программного обеспечения.

Декабрь 1989 года: некий злоумышленник разослал по разным адресам 20.000 дискет, содержащих "троянца". Через 90 загрузок операционной системы на зараженном ПК программа делала невидимыми все файлы и оставляла на диске только один читаемый файл - счет, который следовало оплатить и отослать по указанному адресу.

1.2 Основная классификация компьютерных вирусов

На данный момент существует немало разновидностей компьютерных вирусов и несколько подходов к классификации компьютерных вирусов по их характерным особенностям:

1) по среде обитания вируса
2) по способу заражения
3) по деструктивным возможностям
4) по особенностям алгоритма работ

По среде обитания вирусы бывают:

Файловые вирусы — вирусы поражающие исполняемые файлы, написанные в различных форматах. Соответственно в зависимости от формата, в котором написана программа это будут двоичные файлы (EXE, COM), файлы динамических библиотек (DLL), драйверы (SYS), командные файлы (BAT, CMD) и т.п

Сетевые вирусы — вирусы, распространяющиеся в различных компьютерных сетях и системах. (Macro, Word, ShareFun и Win. Homer)

Загрузочные вирусы — вирусы поражающие загрузочные сектора (Boot сектора) дисков или сектор, содержащий системный загрузчик (Master Boot Record) винчестера.

Макровирусы — вирусы поражающие файлы Microsoft Office. (например,Word,Excel).

Flash вирусы — вирусы, поражающие микросхемы FLASH памяти BIOS.

Файлово - загрузочные вирусы — вирусы, заражающие как файлы, так и загрузочные сектора. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему и их труднее обнаружить.

По способу заражения вирусы бывают:

Резидентные вирусы — вирусы, которые при инфицировании компьютера оставляют свою резидентную часть в памяти. Они могут перехватывать прерывания операционной системы, а также обращения к инфицированным файлам со стороны программ и операционной системы. Эти вирусы могут оставаться активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы — вирусы, не оставляющие своих резидентных частей в оперативной памяти компьютера. Некоторые вирусы оставляют в памяти некоторые свои фрагменты не способные к дальнейшему размножению такие вирусы считаются не резидентными.

По деструктивным возможностям вирусы бывают:

Безвредные вирусы — это вирусы, никак не влияющие на работу компьютера за исключение, быть может, уменьшения свободного места на диске и объема оперативной памяти.

Неопасные вирусы — вирусы, которые проявляют себя в выводе различных графических, звуковых эффектов и прочих безвредных действий.

Опасные вирусы — это вирусы, которые могут привести к различным сбоям в работе компьютеров, а также их систем и сетей.

Очень опасные вирусы — это вирусы, приводящие к потере, уничтожению информации, потере работоспособности программ и системы в целом.

По особенностям алгоритма работы вирусы бывают:

Вирусы спутники (companion) — эти вирусы поражают EXE-файлы путем создания COM-файла двойника, и поэтому при запуске программы запустится, сначала COM-файл с вирусом, после выполнения своей работы вирус запустит EXE-файл. При таком способе заражения «инфицированная» программа не изменяется.

Вирусы «черви» (Worms) — вирусы, которые распространяются в компьютерных сетях. Они проникают в память компьютера из компьютерной сети, вычисляют адреса других компьютеров и пересылают на эти адреса свои копии. Иногда они оставляют временные файлы на компьютере но некоторые могут и не затрагивать ресурсы компьютера за исключением оперативной памяти и разумеется процессора.

«Паразитические» — все вирусы, которые модифицируют содержимое файлов или секторов на диске. К этой категории относятся все вирусы не являющиеся вирусами-спутниками и вирусами червями.

«Стелс-вирусы» — представляющие собой программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков подставляют вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы.

«Полиморфные» (самошифрующиеся или вирусы-призраки, polymorphic) — вирусы, достаточно трудно обнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

«Макро-вирусы» — вирусы этого семейства используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). В настоящее время наиболее распространены макро-вирусы, заражающие текстовые документы редактора Microsoft Word.

1.3 Основные виды вирусных программ

Существует несколько основных типов вирусов:

Червь – вредоносная программа, целью которой является забить компьютер всяким мусором для того, чтобы он стал медленным и неуклюжим. Червь способен саморазмножаться, но не может быть частью программы. Чаще всего заражение этим вирусом происходит посредством электронных писем.

Троянская программа (Троян, Троянский конь) – эта программа полностью оправдывает свое название. Она проникает в другие программы и скрывается там до момента, когда программа-хозяин будет запущена. До запуска хозяйской программы вирус не может нанести вред. Чаще всего троянский конь используется для удаления, изменения или кражи данных. Самостоятельно троян размножатся не может.

Программы шпионы – эти программы занимаются сбором информации о пользователе и его действиях. Чаще всего они воруют конфиденциальную информацию: пароли, адреса, номера карт/счетов и т. д.

Зомби – такое название вредоносные программы получили, оттого, что и в самом деле делают из компьютера «безвольную» машину, подчиняющуюся злоумышленникам. Проще говоря, нехорошие люди могут управлять чьим-либо компьютером посредством этих вредоносных программ. Чаще всего пользователь даже не знает, что его компьютер уже не только его.

Программа - блокировщик (баннер) – эти программы блокируют доступ к операционной системе. При включении компьютера пользователь видит всплывающее окно, в котором обычно его в чем-то обвиняют: нарушении авторских прав или скачивании пиратского программного обеспечения. Далее, следуют угрозы полного удаления всей информации с компьютера. Для того чтобы этого избежать пользователь должен пополнить счет определенного телефона или отослать СМС. Только вот, даже если пользователь проделает все эти операции, баннер с угрозами никуда не денется.

Загрузочные вирусы – поражают загрузочный сектор винчестера (жесткого диска). Их целью является существенное замедление процесса загрузки операционной системы. После длительного воздействия этих вирусов на компьютер существует большая вероятность не загрузить операционную систему совсем.

Эксплойт – это специальные программы, которые используются злоумышленниками для проникновения в операционную систему через ее уязвимые, незащищенные места. Используются для проникновения программ, которые воруют информацию, необходимую для получения прав доступа к компьютеру.

Фарминг – вредоносная программа, осуществляющая контроль над браузером пользователя и направляющая его на фальшивые сайты злоумышленника. Во «внутренности» браузера эти паразиты попадают при

помощи троянов и червей. При этом будут отображаться только фальшивые сайты, даже если адрес был введен правильно.

Фишинг – так называются действия, когда злоумышленник рассылает электронные письма своим жертвам. В письмах обычно находится просьба о подтверждении личных данных: ФИО, пароли, PIN-коды и т. д. Таким образом, хакер может выдать себя за другого человека и, к примеру, снять все деньги с его счета.

Шпионское ПО – программы, пересылающие данные пользователя сторонним лицам без его ведома. Шпионы занимаются тем, что изучают поведение пользователя и его излюбленные места в Интернете, а затем демонстрируют рекламу, которая однозначно будет ему интересна.

Руткит – программные средства, которые позволяют злоумышленнику беспрепятственно проникать в программное обеспечение жертвы, а затем полностью скрыть все следы своего пребывания. Полиморфные вирусы – вирусы, которые маскируются и перевоплощаются. Во время работы они могут менять собственный код. А посему их очень сложно обнаружить.

Программный вирус – программа, которая прикрепляется к другим программам и нарушает их работу. В отличии от трояна компьютерный вирус может размножаться и в отличии от червя для успешной работы ему нужна программа, к которой он может «прилипнуть». Таким образом, можно сказать, что вредоносная программа (Malware) – это любая программа, которая была создана для обеспечения доступа к компьютеру и хранящейся в нем информации без разрешения владельца этого самого компьютера. Целью таких действий является нанесение вреда или хищение какой-либо информации. Термин «Вредоносная программа» является обобщенным для всех существующих вирусов. Стоит помнить, что программа, пораженная вирусом, уже не будет работать правильно. Поэтому ее нужно удалить, а затем установить заново.

Глава II. Защита ПК от вредоносных программ

2.1 Пути проникновения вирусов в компьютер и признаки их появления

В распространении вирусов с одной виноват человек, с другой стороны - отсутствие средств защиты у операционной системы. Основными путями проникновения вирусов являются:

- хранилище, на котором находятся зараженные вирусом файлы;
- компьютерная сеть, в том числе система электронной почты и Internet;
- жесткий диск, на который попал вирус в результате работы с зараженными программами;
- вирус, оставшийся в оперативной памяти после предшествующего пользователя.

Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS, BAT. Крайне редко заражаются текстовые файлы.

Признаки заражения

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин.

2.2.Обнаружение, меры по защите и методы профилактики компьютерных вирусов

Для защиты информации от вирусов используются общие и программные средства.

К общим средствам, помогающим предотвратить заражение и его разрушительных последствий, относят:

- резервное копирование информации (создание копий файлов и системных областей жестких дисков);
- избегание пользования случайными и неизвестными программами. Чаще всего вирусы распространяются вместе с компьютерными программами;
- перезагрузка компьютера перед началом работы, в частности, в случае, если за этим компьютером работали другие пользователи;
- ограничение доступа к информации, в частности физическая защита хранилищ во время копирования файлов с неё;
- применение лицензионного программного обеспечения;
- применение различных защитных средств при работе на компьютере в любой информационной среде (например, в Интернете);
- проверка на наличие вирусов файлов, полученных по сети.

К программным средствам защиты относят разные антивирусные программы (антивирусы). Антивирус - это программа, выявляющая и обезвреживающая компьютерные вирусы.

Существуют, как и бесплатные антивирусы, так и платные. К бесплатным относятся Avast! Free Antivirus, Microsoft Security Essentials, Comodo Antivirus и т.д. К платным относятся Kaspersky Internet Security, Dr.Web Антивирус, Avast Professional Edition.

Следует заметить, что вирусы в своём развитии опережают антивирусные программы, поэтому даже в случае регулярного пользования антивирусов, нет 100% гарантии безопасности. Антивирусные программы могут выявлять и уничтожать лишь известные вирусы, при появлении нового компьютерного вируса защиты от него не существует до тех пор, пока для него не будет разработан свой антивирус.

Однако, много современных антивирусных пакетов имеют в своём составе специальный программный модуль, называемый эвристическим анализатором, который способен исследовать содержимое файлов на наличие кода, характерного для компьютерных вирусов. Это даёт возможность своевременно выявлять и предупреждать об опасности заражения новым вирусом.

Типы антивирусных программ.

Различают следующие типы антивирусных программ.

1) программы-детекторы: предназначены для нахождения заражённых файлов одним из известных вирусов. Некоторые программы-детекторы могут также лечить файлы от вирусов или уничтожать заражённые файлы. Существуют специализированные, то есть

предназначенные для борьбы с одним вирусом детекторы и полифаги, которые могут бороться с многими вирусами;

2) программы-лекари: предназначены для лечения заражённых дисков и программ. Лечение программы состоит в изъятии из заражённой программы тела вируса. Также могут быть как полифагами, так и специализированными;

3) программы-ревизоры: предназначены для выявления заражения вирусом файлов, а также нахождение повреждённых файлов. Эти программы запоминают данные о состоянии программы и системных областей дисков в нормальном состоянии (до заражения) и сравнивают эти данные в процессе работы компьютера. В случае несоответствия данных выводится сообщение о возможности заражения;

4) лекари-ревизоры: предназначены для выявления изменений в файлах и системных областях дисков и, в случае изменений, возвращают их в начальное состояние.

5) программы-фильтры: предназначены для перехвата обращений к операционной системе, которые используются вирусами для размножения и сообщают об этом пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции. Такие программы являются резидентными, то есть они находятся в оперативной памяти компьютера.

6) программы-вакцины: используются для обработки файлов и boot-секторов с целью предупреждения заражения известными вирусами (в последнее время этот метод используется все чаще).

Если не принимать меры для защиты от компьютерных вирусов, то следствия заражения могут быть очень серьёзными.

2.3 Ответственность за правонарушения в информационной сфере

В ряде стран законодательство предусматривает ответственность за компьютерные преступления, в том числе за внедрение вирусов. Так, например, на территории Российской Федерации преступления в сфере компьютерной информации преследуются уголовным кодексом. Глава 28 УК РФ содержит 3 статьи в составах, которых предусмотрены санкции за преступления в сфере компьютерной информации.

Статья 272 УК РФ. Неправомерный доступ к компьютерной информации, а именно: за неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Статья 273 УК РФ. Создание, использование и распространение вредоносных компьютерных и создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

Статья 274 УК РФ . Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, означающее нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред

Статья 274.1 УК РФ. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

Деяния, предусмотренные данными статьями уголовного кодекса Российской Федерации, наказываются уголовными штрафами, принудительными работами, лишением свободы на срок до десяти лет, лишением права занимать определенные должности или заниматься определенной деятельностью на различные сроки.

ЗАКЛЮЧЕНИЕ

В ходе работы над проектом я исследовал основные понятия о компьютерных вирусах, а именно: что такое компьютерные вирусы и когда они появились, классификацию и основные виды вирусных программ, выявил средства профилактики и борьбы с вирусами, рассмотрел меры ответственности за нарушения в информационной сфере.

Несомненно, что в наше время компьютеризация проникла во все сферы нашей жизни. А используя персональные гаджеты невозможно не пользоваться Интернетом и различными устройствами транспортировки и хранения информации. В связи с этим создается большая вероятность заражения вирусами. В настоящее время известно более 500000000 программных вирусов, число которых непрерывно растет. При изучении литературы и доступной информации по теме, выбранного мной проекта «Компьютерные вирусы» я пришел к следующему выводу.

На персональные компьютеры и другие устройства с выходом в Интернет необходимо устанавливать антивирусные программы. Но не один антивирус не может дать стопроцентной гарантии, что вирус не проникнет в систему. Защищенность от вирусов зависит и от грамотности пользователя. Применение вкупе всех видов защит позволит достигнуть высокой безопасности компьютера, и соответственно, информации

Для того чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:

— оснастите свой компьютер современными антивирусными программами и постоянно обновляйте их вирусные базы;

— перед считыванием с носителя информации, записанной на других компьютерах, всегда проверяйте эти устройства на наличие вирусов, запуская антивирусные программы своего компьютера;

— при переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

— периодически проверяйте на наличие вирусов жесткий диск компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи носителя, предварительно загрузив операционную систему с защищенной от записи системного диска;

— всегда защищайте свои устройства от записи при работе на других компьютерах, если на них не будет производится запись информации;

— обязательно делайте архивные копии на съемных носителях ценной для вас информации;

— не оставляйте съемные носители при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами;

— используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей;

— для обеспечения большей безопасности применения антивируса необходимо сочетать с повседневным использованием ревизора диска.

Я считаю, что при выполнении работы поставленная цель по изучению проблемы возникновения компьютерных вирусов, выявлению признаков их появления и путей проникновения в компьютер, углубления знаний о мерах по защите и профилактике от компьютерных вирусов достигнута.

Следовательно, подтверждается гипотеза проекта: на основе полученной информации о компьютерных вирусах, способах их проникновения и мерах по предотвращению, мы сможем осуществить профилактику заражения компьютера.

Практическая значимость исследования состоит в следующем: разработанный проект может быть использован учащимися, педагогами и другими пользователями в работе с компьютером

Список использованных ресурсов

1. Безруков Н.Н. Компьютерные вирусы. - М.: Наука, 2010.
2. Интернет – ресурс «Виды компьютерных вирусов» https://welcom-comp.ru/antivir_pc/58-vidy-kompyuternyh-virusov.html
3. Интернет – ресурс «Классификация компьютерных вирусов» https://hitechnic31.ru/klassifikaciya-kompyuternyh-virusov/
4. Интернет – ресурс «Краткая история компьютерных вирусов» https://www.kaspersky.ru/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds
5. Интернет – ресурс «Основные методы защиты от компьютерных вирусов» https://studopedia.ru/18_61807_osnovnie-metodi-zashchiti-ot-kompyuternih-virusov.html
6. Интернет – ресурс «Типы антивирусных программ» https://www.sites.google.com/site/komputernyevirusyreshetnikova/home/tipy-antivirusnyh-programm
7. Информатика: Учебник / под ред. Проф. Н.В. Макаровой. - М.: Финансы и статистика, 2007.
8. Леонтьев В.П. Новейшая энциклопедия персонального компьютера. – М.: ОЛМА – ПРЕСС Образование, 2007
9. Мостовой Д.Ю. Современные технологии борьбы с вирусами // Мир ПК. - №8. - 2012.
10. Трофимова И.А., О.В. Яровая. Информатика в схемах и таблицах. - М.; ЭСМО, 2010
11. Уголовный кодекс Российской Федерации
12. Энциклопедия тайн и сенсаций / Подгот. текста Ю.Н. Петрова. - Мн.: Литература, 1996.

Список приложений