Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Новосибирский государственный технический университет»

Кафедра автоматизированных систем управления

ОТЧЕТ ПО ПРАКТИКЕ

_____ Учебная практика: ознакомительная практика_____

(наименование практики в соответствии с учебным планом)

Направление подготовки: _09.03.01 Информатика и вычислительная техника_____

профиль: Программное обеспечение компьютерных систем и сетей

Выполнил:	Проверил:
Студент Дмитриев Николай Евгеньевич	Руководитель от НГТУ Лауферман Ольга Викторовна
	Балл: _____, ECTS_____,
Группа АВТ-212	
	Оценка _____
Факультет АВТФ	«отлично», «хорошо», «удовлетворительно», «неуд.»
«29» декабря 2022 г.	_____
	подпись
	«29» декабря 2022 г.

Новосибирск 2022

Индивидуальное задание на учебную практику: ознакомительную практику

Студент Дмитриев Николай Евгеньевич группы АВТ-212

Место прохождения практики __выпускающая кафедра автоматизированных систем управления

Цели практики:

- иметь представление об основных научных направлениях работы кафедры;
- уметь использовать специализированные программные средства при решении профессиональных задач, уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств, владеть персональным компьютером как средством управления информацией.

Вопросы, подлежащие изучению

На подготовительном этапе:

1. Знакомство с целями, содержанием, местом практики, порядком организации, сроками и порядком защиты, индивидуальным заданием
2. Знакомство с основными научными направлениями работы выпускающей кафедры

На основном этапе:

1. Подготовка реферата по теме «Основные антивирусные программы».

На итоговом этапе:

1. Оформление отчета в форме реферата по учебной практике: ознакомительной практике.
2. Защита отчета в форме реферата по учебной практике: ознакомительной практике.

Ожидаемые результаты учебной практики: ознакомительной практики:

1. Представление об основных научных направлениях работы кафедры.
2. Опыт использования специализированных программных средств при решении профессиональных задач, применения основных методов, способов и средств получения, хранения и переработки информации с помощью компьютеров и компьютерных средств, использования персонального компьютера как средства управления информацией при подготовке реферата по тематике научных направлений работы кафедры как одного из видов научной работы.

Задание выдала: Лауферман Ольга Викторовна

Задание принято к исполнению: _____ «25» декабря 2022 г.

(подпись студента)

Календарный график выполнения задания на практику

Дата	Наименование работ	Отметка о выполнении задания
03.09.22 -25.12.22	Ведение дневника практики.	Отправлен 25.12.22
19.09.22 – 30.09.22	Выбор темы реферата.	30.09.22 выбрана тема «Негативное воздействие компьютера на здоровье человека и способы защиты.»
10.10.22 – 11.10.22	Написание эссе на тему «Мой выбор направления подготовки».	Написано и отправлено 11.10.22
20.10.22 – 25.10.22	Выяснение актуальности и практической значимости темы. Формулировка цели работы и задач, которые необходимо решить для раскрытия темы реферата.	Сформулированы 25.10.22
26.10.22	**Обсуждение и утверждение целей и задач с преподавателем.**	Утверждены 26.10.22
27.10.22	Ознакомление с правилами оформления текста.	Ознакомлен 27.10.22
28.10.22 – 01.11.22	Поиск и конспектирование информации по теме реферата, составление библиографического списка официальных источников информации.	01.11.22 составлен библиографический список источников
02.11.22	**Согласование с преподавателем списка официальных источников информации.**	Список согласован 02.11.22
06.11.22 – 08.11.22	Редакция введения в соответствие с содержанием основной части, написание заключения с обязательным изложением необходимых выводов.	Сделано 08.11.22
09.11.22 – 13.11.22	Форматирование работы в соответствии с требованиями.	Проделано 13.11.22
14.11.22 – 15.11.22	Подготовка презентации по теме реферата: выбор шаблона для оформления презентации, определение содержания презентации.	Выполнена 15.11.22
16.11.22 – 22.11.22	Подготовка всех слайдов презентации.	Выполнена 22.11.22
27.10.22	Работа над докладом: составление плана выступления, проведение репетиции выступления.	Проделано 29.11.22
	Выступление с докладом.	
03.12.22 – 19.28.22	Написание статьи	Отправлена 28.1.23
21.12.22	Прохождение тестирования	Пройдено 20.12.22

09.12.22 – 29.12.22	Создание отчёта по практике.	Отчёт отправлен 30.02.22

Студент группы АВТ-212

ФИО Дмитриев Николай Евгеньевич Подпись_____

Дата 08.11.22

Руководитель практики:

От НГТУ:

Лауферман Ольга Викторовна Подпись_____

Эссе на тему «Мой выбор профессионального направления подготовки»

Сдано в Рукописном/печатном виде

Федеральное государственное бюджетное образовательное учреждение высшего образования

“Новосибирский государственный технический университет”

Кафедра автоматизированных систем управления

РЕФЕРАТ

по учебной практике: ознакомительная практика

на тему

“Основные антивирусные программы”

Выполнил:

Студент 1 курса

Группа:АВТ-212

Дмитриев Николай Евгеньевич

Научный руководитель:

Лауферман Ольга Викторовна

г. Новосибирск

2022 год

Оглавление

Введение

На сегодняшний день компьютер активно используется в повседневной жизни людей. Его возможности используются на работе, при проведение досуга, в быту и других сферах жизни человека. Количество информации, которую предоставляют своему компьютеру, с каждым днём растёт, поэтому люди интересуются защитой своей сохранённой информации.

В интернете появилось большое количество вредоносных программ, которые называются “вирус”.

Вирус – это вредоносная программа, проникающая на компьютер без ведома пользователя (хотя, возможно, при невольном его участии) и выполняющая определенные действия деструктивной направленности. Вирусы – едва ли не главные враги компьютера. Эти программы подобно биологическим вирусам размножаются, записываясь в системные области диска или приписываясь к файлам производят различные нежелательные действия, которые, зачастую, имеют катастрофические последствия. Еще пять лет назад казалось, что со владычеством вирусов покончено – со смертью DOS и DOS-совместимых программ неминуемо должны были исчезнуть и паразитирующие на них вирусы. Ведь если вирус под DOS, заражающий исполняемые файлы .com и .exe-файлы, может написать каждый, кто хоть немного разбирается в программировании, то создать полноценный вирус для Windows гораздо труднее.

Вирус может попасть на компьютер пользователя вместе с дискетой, пиратским компакт-диском или с сообщением электронной почты. Чтобы не стать жертвой этой напасти, каждому пользователю следует хорошо знать принципы защиты от компьютерных вирусов.

Цель реферата: получить представление о компьютерных вирусах и их вреде компьютеру и способы борьбы с ними. Для этого я поставил себе следующие задачи.

1.Найти и проанализировать основную информацию о вирусах.

2.Узнать историю происхождения вируса.

3.Узнать, как выявить вирус на своём компьютере.

4.Найти эффективные способы борьбы с ними.

В данной работе я рассмотрю способы защиты компьютерных систем от вирусных программ. Актуальность реферата заключается в необходимости защиты собственной информации и работоспособности своего компьютера.

История компьютерных вирусов

История появления компьютерных вирусов насчитывает уже почти 40 лет. Один из самых первых вирусов был разработан для компьютера Apple (но, в последствии, он так и не привёл к массовому заражению «яблочных» ПК). Произошло это в 1981 году, а звали «пионера» Elk Cloner (в вольном переводе «клонировщик лосей»). Этот «сохатый» был довольно безобиден, но надоедлив: при каждой загрузке пользователь заражённого компьютера видел на экране забавный (но не для владельца ПК) стишок, после чего компьютер начинал снова работать в обычном режиме.

Elk Cloner заражал компьютеры с дискеты: загружаясь с заражённой дискеты система запускала копию вируса. Никакого серьёзного влияния на работу компьютера он не оказывал, поскольку был написан американским школьником Ричардом Скрента забавы ради. Таким образом, Elk Cloner, который было бы правильнее назвать программой-шуткой, положил начало обширной категории «загрузочных вирусов», так как прописывался в сектор загрузки Apple II. Интересно, что в сети нередко можно встретить утверждение, что под OS X и iOS вирусов не бывает. А первый распространённый вирус для ПК под управлением операционной системы MS DOS, появился в 1986 году, и назывался он Brain (в переводе с английского «мозг»). Впрочем, разработчики этого вируса, пакистанские братья Фарук Альви, не хотели вредить людям: они написали Brain для того, чтобы защитить написанную ими медицинскую программу от нелицензионного копирования.

Работал он так: в случае обнаружения пиратской программы вирус несколько замедлял работу дискеты, а также ограничивал память при взаимодействии с программой. Интересно, что создатели «Мозга» позаботились о том, что при его загрузке пользователь получал не только сообщение о заражении, но и телефон разработчиков, которые обещали выслать «лекарство» (привычных антивирусных программ тогда ещё, разумеется, не было). И слово своё до поры до времени братья держали, однако заражений оказалось так много, что можно было говорить уже о целой эпидемии: пользователи со всего мира стали атаковать несчастный пакистанский номер, и братьям ничего не оставалось, как просто отключить телефон. Так мир пережил первую «пандемию», вызванную компьютерным вирусом.

Признаки появления вирусов

Для маскировки вируса его действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении каких-либо условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и ее работа некоторое время не отличается от работы незараженной. Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователь часто и не замечает, что компьютер работает со "странностями". К признакам появления вируса можно отнести:

• Замедление работы компьютеры;

• Невозможность загрузки операционной системы;

• Частые зависания и сбои в работе компьютера;

• Изменение размеров файла;

• Увеличение количества файлов на диске;

• Изменение даты и времени создания файлов;

• Заметное возрастание времени доступа к жёсткому диску;

• Разрушение файловой структуры;

Основные меры по защите от вирусов

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

• Перед считывание с дисков информации, записанной на других компьютерах, всегда проверять эти диски на наличие вирусов, запуская антивирусные программы.

• При переносе на компьютер файлов в архивированном виде проверять их сразу же после разархивации на жёстком диске, ограничивая область только вновь записанными файлами.

• Периодические проверять на наличие вирусов жёсткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков.

• Проверять антивирусом, все скачанные из интернета файлы.

Антивирусные программы

Антивирусная программа (антивирус) — изначально компьютерная программа, которая предназначена для обезвреживания вирусов и различного рода вредоносного ПО, с целью сохранности данных и оптимальной работы вашего персонального компьютера.

Антивирусное ПО, пришлось ждать не долго, оно появилось сразу после появления первых вредоносных программ. В нынешний момент над разработкой антивирусных программ трудятся целые корпорации во главе с тысячами людей, которые постоянно "латают дыры", чтоб наш информационный мир был более чистым и безопасным.

Антивирусные программы (**антивирусы**) используют два определенных принципа работы (устранения) с вредоносным ПО:

• Сканирование вашего компьютера и сопоставление уже имеющегося вируса с базой данных на сервере определенного производителя.

• Сканирование и обнаружение программ, которые ведут себя подозрительно и могут по определению являться вредоносным ПО.

Основные задачи антивирусов:

• Сканирование файлов и программ в режиме реального времени.

• Сканирование компьютера по требованию.

• Сканирование интернет- графика.

• Сканирование электронной почты.

• Защита от атак веб-узлов.

• Восстановление повреждённых файлов.

Основные антивирусные программы

1. Avast!

Основные характеристики Avast!: Высокий уровень выявления вирусов, троянов и червей. Резидентный (в режиме реального времени) и обычный сканер. Сканирование архивов. Проверка входной и исходной электронной почты. Глубокая интеграция в систему. Проверить тот или иной файл можно непосредственно из проводника Windows, щелкнув по нему правой кнопкой мыши и выбрав надпись "Сканировать...". Карантин Avast! изолирован от операционной системы, что обеспечивает большую безопасность работы. Ни один файл, сохраняемый в карантине не может быть запущен.

2. Doctor.Web

В последнее время стремительно растет популярность антивирусной программы - Doctor Web, которая относится к классу детекторов - докторов, но в отличие от многих других антивирусных порограмм имеет так называемый "эвристический анализатор" - алгоритм,позволяющий обнаруживать неизвестные вирусы.

Главной особенностью "Лечебной паутины" является наличие эвристического анализатора, который подключается ключем /S. Баланса между скоростью и качеством можно добиться, указав ключу уровень эвристического анализа: 0 - минимальный, 1 -оптимальный, 2 - максимальный; при этом, естественно, скорость уменьшается пропорционально увеличению качества. К тому же Dr.Web позволяет тестировать файлы, вакцинированные CPAV, а также упакованные LZEXE, PKLITE, DIET.

Важной функцией является контроль заражения тестируемых файлов резидентным вирусом. При сканировании памяти нет стопроцентной гарантии, что "Лечебная паутина" обнаружит все вирусы, находящиеся там.

3. Panda

Panda Antivirus Platinum 7 — это инновационное антивирусное решение, отлично адаптированное к потребностям небольших организаций и профессионалов. Программа защищает компьютер и от вирусов, и от хакеров.Благодаря таким встроенным функциям, как межсетевой экран и блокиратор скриптов, Platinum 7 гарантирует защиту от вирусов, хакеров и других опасностей, связанных с сетью Интернет, в рамках единого и простого в использовании продукта.

4. Aidtest

Программа Aidstest предназначена для исправления программ, зараженных обычными (неполиморфными) вирусами, не меняющими свой код. Это ограничение вызвано тем, что поиск вирусов этой программой ведется по опознавательным кодам. Зато при этом достигается очень высокая скорость проверки файлов.

Aidstest для своего нормального функционирования требует, чтобы в памяти не было резидентных антивирусов, блокирующих запись в программные файлы, поэтому их следует выгрузить, либо, указав опцию выгрузки самой резидентной программе, либо воспользоваться соответствующей утилитой.

При запуске Aidstest проверяет оперативную память на наличие известных ему вирусов и обезвреживает их. При этом парализуются только функции вируса, связанные с размножением, а другие побочные эффекты могут оставаться. Поэтому программа после окончания обезвреживания вируса в памяти выдает запрос о перезагрузке. Следует обязательно последовать этому совету, если оператор ПЭВМ не является системным программистом, занимающимся изучением свойств вирусов. При чем следует перезагрузиться кнопкой RESET, так как при "теплой перезагрузке" некоторые вирусы могут сохраняться. Вдобавок, лучше запустить машину и Aidstest с защищённой от записи дискетой, так как при запуске с зараженного диска вирус может записаться в память резидентом и препятствовать лечению.

5. ADINF

ADinf относится к классу программ-ревизоров. Семейство программ ADinf – это ревизоры дисков, предназначенные для работы на персональных компьютерах под управлением операционных систем MS-DOS, MS-Windows 3.xx, Windows 95/98 и Windows NT/2000. Работа программ основана на регулярном отслеживании изменений, происходящих на жестких дисках. В случае появления вируса, ADinf обнаруживает его по тем модификациям, которые он выполняет в файловой системе и/или загрузочном секторе диска и информирует об этом пользователя. В отличие от антивирусов-сканеров, ADinf не использует в своей работе "портретов" (сигнатур) конкретных вирусов. Поэтому ADinf особенно эффективен для обнаружения новых вирусов, противоядие для которых еще не придумано.

Особенно следует отметить, что для контроля дисков ADinf не использует функции операционной системы. Он читает диск по секторам и

самостоятельно разбирает структуру файловой системы, что позволяет ему обнаруживать так называемые вирусы-невидимки (стелс-вирусы).

Полезные свойства ADinf не ограничиваются только лишь борьбой с вирусами. По сути ADinf является системой, позволяющей следить за сохранностью информации на дисках и обнаруживать любые, даже малозаметные изменения в файловой системе, а именно, изменения системных областей, изменения файлов, создание и удаление каталогов, создание, удаление, переименование и перемещение файлов из каталога в каталог. Состав контролируемой информации гибко настраивается, что позволяет ставить под контроль только то, что нужно.

Основные проблемы антивирусной индустрии

Какие же могут быть проблемы у антивирусных программ, за исключением обычного маркетингового противоборства? Есть вирусы — и есть антивирусы, которые их ловят. И на первый взгляд, антивирус давно стал обычным потребительским товаром, который практически ничем не отличается от конкурирующих продуктов и который покупают либо за более красивый дизайн, либо потому, что данный продукт был удачно разрекламирован, либо по какой-либо еще совсем не технической причине. Т.е. антивирус вроде как давно должен стать тем самым «commodity», продуктом массового потребления, вроде стиральных порошков, зубных щеток или автомобилей.

Основной вопрос — от каких именно компьютерных угроз защищает данное решение и насколько качественна предоставляемая защита. Антивирус должен защищать от всех видов вредоносных программ, и чем он лучше это делает, тем спокойнее живет его пользователь и дольше и крепче спит системный администратор. И кто этого не понимает теоретически, очень скоро осознает всю глубину проблемы практически — когда вдруг куда-то начинают утекать деньги с банковского счета, компьютер сам по себе начинает звонить по каким-то совершенно «левым» телефонным номерам, внезапно и по непонятной причине резко увеличивается исходящий трафик.

К сожалению, далеко не все антивирусные продукты, которые можно обнаружить на полках магазинов или в сети, дают защиту, близкую к 100%. Большинство продуктов не гарантирует даже 90%-ный уровень защиты! В этом и заключается основная проблема антивирусных компаний на сегодняшний день.

Действия при заражении компьютера вирусом

1.Сразу же выключить питание, чтобы вирус перестал распространяться дальше. Единственное, что можно сделать до выключения питания, - это сохранить результаты текущей работы.

2.Войти в SETUP и включить загрузку с диска A:.

3.Если произошли какие-либо изменения, то необходимо восстановить старые значения.Ни в коем случае не запускать ни одной программы, находящейся на жёстком диске.

4.Необходимо запустить по очереди программы-детекторы.

5.Если программа-детектор обнаружит файловый вирус, то возможны два варианта действий. Если у вас установлена программа-ревизор с лечащем модулем, то восстановление файлов лучше делать с ее помощью. Если такое программы нет, то необходимо воспользоваться для лечения одним из детекторов.

6.После того как все вирусы удалены, необходимо заново перенести операционную систему на жёсткий диск (с помощью команды SYS).

7.Необходимо проверить целостность файловой системы на винчестере (с помощью CHKDSK) и исправить все повреждения.

8.Необходимо ещё раз проверить жёсткий диск на наличие вирусов, если таковых не оказалось, то можно перезагрузиться с винчестера.

9.Необходимо восстановить все необходимые файлы и программы с помощью архива.

10.После того как вирус дезактивирован, вы можете продолжать свою работу. Помимо перечисленных выше пунктов необходимо обращать особое внимание на чистоту модулей, сжатых файлов в архивах (ZIP, ARC, ICE, ARJ и т. д.) и данных в самораспаковывающихся файлах, созданных утилитами типа ZIP2EXE. Если случайно упаковать файл зараженный вирусом, то обнаружение и удаление такого вируса без распаковки файла практически невозможно. В данном случае типичной будет ситуация, при которой все антивирусные программы, неспособные сканировать внутри упакованных файлов, сообщат о том, что от вирусов очищены все диски, но через некоторое время вирус появится опять.

Штаммы вируса могут проникнуть и в резервные копии ПО при обновлении этих копий причем архивы и резервные копии являются основными поставщиками давно известных вирусов. Вирус может годами сидеть в дистрибутивной копии какого-либо программного продукта и неожиданно проявиться при установке программ на новом компьютере.

Заключение

После исследования темы, я пришел к выводу, что несмотря на широкую распространенность антивирусных программ, вирусы продолжают «плодиться». Чтобы справиться с ними, необходимо создавать более универсальные и качественно-новые антивирусные программы, которые будут включать в себя все положительные качества своих предшественников. Я понял, что на данный момент нет такой антивирусной программы, которая гарантировала бы защиту от всех разновидностей вирусов на 100%.

Необходимо следить за тем, чтобы антивирусные программы, используемые для проверки, были самых последних версий. Если к программам подставляются обновления, то необходимо проверить их на «свежесть». Обычно выход новых версий антивирусов анонсируется, поэтому достаточно посетить соответствующие узлы WWW, ftp или BBS.

«Национальность» антивирусов в большинстве случаев не имеет значения, поскольку на сегодняшний день процесс эмиграции вируса в другие страны и иммиграции антивирусных программ ограничивается только скоростью интернета, поэтому как вирусы, так и антивирусы не признают границ.

Список литературы

1.Сычев Ю.Н. Информационная безопасность:учебное пособие,руководство по изучению дисциплины, практикум, тесты, учебная программа.-М.: «АЛЛАНА»,2007

2. Ярочкин В.И. Информационная безопасность:Учебник для студентов вузов.-3-е изд.-М.: «Трикста»,2005

3. Филин С.А. Информационная безопасность: Учебное пособие.-М.: «Альфа-Пресс»,2006

4. Денисов Т.В. «Антивирусная защита» // Мой Компьютер - №4-1999г.

5. Расторгуев С. Программные методы защиты информации в компьютерах и сетях.-М.:Яхтсмен, 1993.- 188с.

6. Защита информации в персональных ЭВМ / Спесивцев А.В., Вегнер В.А., Кружяков А.Ю., Серегин В.В., Сидоров В.А.-М.:Радио и связь, ВЕСТА, 1993. – 191 с.

7. Защита информации. Конфидент. - 1998. - №1.- 96 с.

8. Евгений Касперский «Компьютерные вирусы» (1998)

9. Лаборатория Касперского Kaspersky.ru

Федеральное государственное бюджетное образовательное учреждение высшего образования

“Новосибирский государственный технический университет”

Кафедра автоматизированных систем управления

Статья

По учебной практике: ознакомительная практика

На тему “Основные подходы к процессу программирования”

Выполнил:

Студент 1 курса

Группа:АВТ-212

Дмитриев Николай Евгеньевич

Научный руководитель:

Лауферман Ольга Викторовна

г. Новосибирск

2022 год

Аннотация:

Статья посвящена самым эффективным способам борьбы с компьютерными вирусами. Основным вопросом данной работы является то, какой способ наиболее эффективен. Статья представляет интерес для людей, которые сталкивались с этой проблемой и хотят получить краткое представление о заданной теме.

Ключевые слова:

Компьютерный вирус, антивирусная программа,

Введение

Компьютерный вирус – это небольшая программа, написанная программистом высокой квалификации, способная к саморазмножению и выполнению разных деструктивных действий. На сегодняшний день известно свыше 50 тыс. компьютерных вирусов. Вирусы действуют только программным путем. Они, как правило, присоединяются к файлу или проникают в тело файла. В этом случае говорят, что файл заражен вирусом. Вирус попадает в компьютер только вместе с зараженным файлом. Для активизации вируса нужно загрузить зараженный файл, и только после этого, вирус начинает действовать самостоятельно.

Программа – это описание на формальном языке, понятном компьютеру, последовательности действий, которое необходимо над данными для решения поставленной задачи.

Антивирусная программа - программа, предназначенная для борьбы с компьютерными вирусами. В своей работе эти программы используют различные принципы для поиска и лечения зараженных файлов.
Для нормальной работы на ПК каждый пользователь должен следить за обновлением антивирусов. Если антивирусная программа обнаруживает вирус в файле, то она удаляет из него программный код вируса. Если лечение невозможно, то зараженный файл удаляется целиком.

Характеристика вирусов и их виды

Вирусы созданы специально для поражения других компьютеров, информации, содержащейся на них. Они представляют собой программы, написанные на низшем компьютерном языке, которые автоматически распространяются на другой программный продукт через зараженные носители или при подключении к интернет-ресурсам.

Вирусы бывают трех видов:

– черви. Распространяются через социальные сети, письма, направляемые по электронной почте;

– вирусы. Они получают управление компьютером при запуске зараженных файлов;

– троянские программы. Они наиболее опасны, так как могут производить на чужом компьютере самостоятельные действия, несанкционированные владельцем, уничтожить или повредить файлы, воровать данные.

Вирусы могут находиться в любой части системы компьютера и ждать определенного события или действия, чтобы начать активную работу. Они вполне могут быть неопасными, существовать на компьютере годами, не причиняя особого вреда, создавая лишь некоторые затруднения в работе определенных программ. Стоит отметить, что таких единицы, основная масса вирусов очень опасны, для этого они и созданы.

Сейчас вирусы настолько разработаны, что могут выполнять различные функции. Есть некоторые количество вирусов, которые поражают оперативную память и потом весь компьютер, есть такие, которые существуют недолгое время, производят определенные действия и остаются неопознанными.

Антивирусные программы и их виды

Антивирусные программы постоянно совершенствуются. Это означает, что пользователь должен находится в поиске более эффективной системы защиты персонального компьютера.

Практически все антивирусные программы имеют автоматическое и ручное сканирование системы.

Автоматическое сканирование исследует файлы, скачанные с интернета, на наличие вирусов, а также проверяет CD, DVD диски, флэш накопители, и другие устройства, которые были подключены к ПК с помощью кабеля или по беспроводным технологиям. При ручной настройке антивируса, можно сканировать как отдельные файлы, так и полностью всю систему.

Ввиду того, что хакеры безостановочно создают новые вирусы при помощи компьютеров, антивирусные программы обязаны иметь и непрерывно обновлять собственную базу вирусов, для того, чтобы была возможность обнаруживать их.

В основном все антивирусные программы можно условно поделить на несколько ключевых типов, каждый их которых ориентирован на некоторую доминирующую функцию. Данный перечень программ выглядит так:

– программы-доктора;

– вакцины;

– ревизоры;

– детекторы;

– фильтры;

Каждый из данных компонентов может понадобиться в таком ответственном и нелегком деле, как организация системы защиты информации. Так, например, антивирусные программы, относящиеся к типу докторов, могут не только обнаружить угрозу, но и вылечить систему. Это является крайне актуальным свойством. Тело вируса в данном случае удаляется из пораженного файла. Последний же возвращается в исходное состояние. Такие программы, которые называют флагами, ведут поиск вирусов. При обнаружении таковых, они, прежде всего, уничтожают их и только после этого активируют процессы восстановления.

Они предназначены специально для таких нагрузок. Если же речь идет о детекторах, то данный тип антивирусных программ используется для быстрого поиска вирусов в оперативной памяти и различных носителях.

Такие антивирусные системы и защиты информации не могут быть рассмотрены по отдельности. Особое внимание следует обратить на программы-фильтры. Они разработаны специально для обнаружения в системе подозрительных процессов. Именно благодаря работе антивирусных программ такого типа пользователи периодически могут видеть на мониторе предупреждения о том, что некоторая программа пытает выполнить подозрительное или некорректное действие.

Из вышеуказанных достоинств поиска и устранения вирусных атак является разработка современных методов поиска и обнаружения внешнего воздействия вирусных баз на ПЭВМ. Перспективным направлением является Эвристический анализ.

Эвристический анализ

Эвристический анализ — обнаружение ранее неизвестных вирусов;

Метод эвристического анализа (heuristic-based detection) служит для выявления даже трех вирусов, для которых не существует образцов в базе антивирусной программы. Существует множество различных методов эвристического анализа. Основной принцип-идентифицировать программный код, который является крайне нежелательным для безопасных программных продуктов. Как бы то и ни было, этот метод неточен и может вызвать множество ложных тревог. Хороший эвристический анализ отлично сбалансирован и вызывает минимальное количество ложных тревог при большой доле обнаружения вредоносного ПО. Чувствительность эвристики может быть настроена.

Заключение

Таким образом, каждый производитель антивируса пытается выставить в лучшем свете свое приложение, расписывает его уникальные возможности и функции. Обычному пользователю может оказаться не просто сделать выбор в пользу того или иного программного продукта. Один из критериев, на который стоит обращать внимание при выборе программы- осуществление защиты от вирусов, которые «неизвестны» антивирусу. Ранее такие программы могли лишь справится с теми вредоносными приложениями, сведения о которых находились в их вирусной базе. Но с выходом нового вируса разработчикам не всегда удавалось оперативно выпускать обновления. Поэтому наличие системы «умного сканирования»- существенное преимущество для антивирусной программы.

(Оригинальность 79%)

Библиографический список

1.Антивирусные программы.
https://kompkimi.ru/programms-2/sistemnye-programmy/antivirusy/antivirusnaya-programma-antivirus

2.Филин С.А. Информационная безопасность: Учебное пособие.-М.: «Альфа-Пресс»,2006

3. Сычев Ю.Н. Информационная безопасность:учебное пособие,руководство по изучению дисциплины, практикум, тесты, учебная программа.-М.: «АЛЛАНА»,2007

4. Ярочкин В.И. Информационная безопасность:Учебник для студентов вузов.-3-е изд.-М.: «Трикста»,2005

5. Безруков Н.Н. Классификация компьютерных вирусов MS-DOS и методы защиты от них. - М.: Информэйшн Компьютер Энтерпрайз, 1990. – 48 с.