Задание 1.

А) Определение компьютерного вируса - набор команд (программных или иных), который производит и распространяет свои копии в компьютерных системах и/ или компьютерных сетях и преднамеренно выполняет некоторые действия, нежелательные для законных пользователей системы или специально написанная, небольшая по размерам программа, которая может приписывать себя к другим программам т. е. “заражать” их, а также выполнять различные нежелательные действия в компьютере.

Это программа, которая распространяется с одного компьютера на другой и препятствует работе компьютера. Вирус компьютера может повредить или удалить данные на компьютере, использовать программу электронной почты для распространения вирусов на другие компьютеры или даже удалить все данные на жестком диске.

Компьютерные вирусы часто распространяются вложениями в сообщениях электронной почты или мгновенными сообщениями. Таким образом, никогда не открывать вложение электронной почты, если вы не знаете, кто отправил сообщение или ожидаете вложение электронной почты. Вирусы могут быть замещения в виде вложений изображений, приветствия или аудио- и видеофайлов. Компьютерные вирусы также распространяются через скачиваемые файлы в Интернете. Их можно скрыть в программном обеспечении или в других файлах или программах, которые можно скачать.

Б) Свойства вирусов:

1) способность к саморазмножению и эволюции;

2) высокая скорость распространения;

3) избирательность поражённых систем (каждый вирус поражает определённые системы и

группы);

4) способность “заражать” “незаражённые” системы;

5) трудность борьбы с вирусами;

6) увеличивается быстрота появлений модификаций и новых поколений вирусов

Задание 2.

Всякая дискета размечена на секторы и дорожки. Секторы объединяются в кластеры. Среди секторов есть несколько служебных, используемых операционной системой для собственных нужд (в этих секторах не могут размещаться данные пользователя). Среди служебных секторов есть один - так называемый сектор начальной загрузки (boot-sector). В секторе начальной загрузки хранится информация о дискете – количество поверхностей, количество дорожек, количество секторов и пр. Программа начальной загрузки

(ПНЗ) должна загрузить саму операционную систему и передать ей управление.

При включении компьютера первым делом управление передается программе начальной загрузки, которая хранится в постоянном запоминающем устройстве. Эта программа тестирует оборудование и при успешном завершении проверок пытается найти дискету в дисководе А:

Нормальная схема начальной загрузки следующая:

ПНЗ (ПЗУ) – ПНЗ (диск) – Система

Теперь рассмотрим работу при наличии вируса. В загрузочных вирусах выделяют две части – голову и хвост. Хвост может быть пустым.

Пусть имеется чистая дискета и зараженный компьютер. Как только этот вирус обнаружит, что в дисководе появилась подходящая жертва – в нашем случае не защищенная от записи и еще не зараженная дискета, он приступает к заражению.

Заражая дискету, вирус производит следующие действия:

- выделяет некоторую область диска и помечает ее как недоступную операционной системе; в традиционном случае занятые вирусом секторы помечаются как сбойные (bad);
- копирует в выделенную область диска свой хвост и оригинальный
- (здоровый) загрузочный сектор;
- замещает программу начальной загрузки в загрузочном секторе
- (настоящем) своей головой;
- организует цепочку передачи управления согласно схеме.

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору. В цепочке ПНЗ (ПЗУ) – ПНЗ (диск) – Система появляется новое звено:

ПНЗ (ПЗУ) – Вирус – ПНЗ (диск) – Система.

Задание 3.

Причины появления и распространения вирусов скрыты с одной стороны в психологии человека, с другой стороны - с отсутствием средств защиты у операционной системы.

Основные пути проникновения вирусов:

- дискета, на которой 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.

Следует заметить, что компьютерные вирусы способны заражать лишь компьютеры.

Механизм проникновения

Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение:

- внедряя себя в исполняемый код других программ,
- заменяя собой другие программы,
- прописываясь в автозапуск и другое.

Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы.

Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с **эксплоитом**, использующим уязвимость.

Эксплоит – это такая программа, которая написана с цельюэксплуатации (использования) конкретной дыры(уязвимости)в конкретном приложении(ОС, обычная программа, веб-приложение).

Вирусы, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске:

1. управление сначала передалось ему
2. после выполнения всех его команд снова вернулось к рабочей программе.

Получив доступ к управлению, вирус прежде всего переписывает сам себя в другую рабочую программу и заражает ее.

После запуска программы, содержащей вирус, становится возможным заражение других файлов.

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

После заражения программы вирус:

1. может выполнить какую-нибудь диверсию, не слишком серьезную, чтобы не привлечь внимания
2. не забывает возвратить управление той программе, из которой был запущен.

Каждое выполнение зараженной программы переносит вирус в следующую программу. Таким образом, заразится все программное обеспечение.

- Каналы проникновения:
- **Дискеты**. Самый распространённый канал заражения в 1980—1990-е годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов на многих современных компьютерах.
- **Флеш-накопители (флешки)**. В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, портативные цифровые плееры, а с 2000-х годов всё большую роль играют мобильные телефоны, особенно смартфоны (появились мобильные вирусы). Использование этого канала ранее было преимущественно обусловлено возможностью создания на накопителе специального файла autorun.inf, в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. В Windows 7 возможность автозапуска файлов с переносных носителей была отключена.
- **Электронная почта**. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.
- **Системы обмена мгновенными сообщениями**. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

- **Веб-страницы**. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компонент. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, рискуют заразить свой компьютер.
- **Интернет и локальные сети (черви)**. Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Уязвимости — это ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак

Задание 4.

Лаборатория Касперского является одним из самых популярных и надежных представителей рынка антивирусных программ в мире. Несмотря на то, что главный офис ее находится в России, продукция Касперского пользуется огромным спросом во всех частях света, предоставляя свои услуги более чем в 200 странах. За годы своего существования, эта компания добилась значительных достижений в деле защиты и сохранения электронной информации.

Ежедневно появляющиеся угрозы безопасности для ПК и других устройств, заставляют специалистов Лаборатории Касперского искать все новые пути их устранения. Однако, данной продукции свойственен и стандартный для наиболее популярных антивирусных программ набор функций, позволяющий оградить пользователей от самых распространенных и опасных типов угроз, связанных с эксплуатацией ПК.

Такими функциями являются:

- личный брандмауэр с системой IDS/IPS;
- выявление вредоносного кода;
- самообновление баз;
- полноценная защита от вирусов;
- проведение анализа по сигнатурным базам;
- стандартная защита от всех видов интернет-атак;
- исследование файлов;
- интернет-трафик и почта, в режиме постоянного мониторинга;
- недопущение утечек личной информации;
- родительский контроль;
- протекция от фишинга и спама.

Плюсы и минусы антивируса Касперского

Конечно, как и любая продукция, антивирусная программа Касперского обладает, как положительными, так и отрицательными сторонами, которые определяют сами пользователи, доверившие защиту своих персональных компьютеров лаборатории Касперского.

Преимущества антивируса Касперского:

1. Обеспечение качественной и надежной защиты ПК, независимо от типа угроз.
2. Удобство в использовании и приятный дизайн.
3. Регулярные обновления.

Недостатки антивируса Касперского:

1. Влияет на скорость обработки информации, замедляя работу системы.
2. Навязчивость некоторых функций.
3. Совершает ошибки при распознавании вирусов, путая их с нормальными файлами.

Несмотря на различность мнений, относительно эффективности использования антивируса Касперского, его с уверенностью можно назвать одним из лучших антивирусов современности. Это утверждение, безусловно, подтверждает наличие большого количества наград, полученных лабораторией Касперского от различных международных организаций за достижения в области защиты ПК и других электронных устройств.

Пользуясь данным антивирусом, можно быть спокойным при совершении каких-либо электронных сделок, включая покупку товаров, перевод средств, оплату услуг и др. Безопасность таких действий гарантируется, как при использовании электронной клавиатуры, так и сенсорного монитора.

Однако, подводя итог, необходимо отметить дороговизну антивируса Касперского. Цена любой его версии превышает среднерыночную цену антивирусных программ. Но, учитывая все вышеперечисленные достоинства, можно сделать вывод о том, что такая переплата не заставит пользователей пожалеть о сделанном выборе.