Panda Software:

Детям о вирусах

ЧАСТЬ 1
КОМПЬЮТЕРНЫЕ ВИРУСЫ

Глава 1: Как все начиналось

1. Кто изобрел вирусы и зачем?

Первые вирусы были придуманы не для нанесения вреда – совсем наоборот! Они были созданы в виде игр.

Много лет назад, несколько инженеров разработали маленькие программы, способные делать копии самих себя. Целью игры было отправлять эти программы друзьям, чтобы посмотреть, какая из них сделает больше собственных копий. Игрок, которому удавалось заполнить компьютеры других, объявлялся победителем.

2. Почему они называются вирусами?

Потому что компьютерные вирусы совсем как те крохотные существа, которые вызывают болезни. Например, когда у тебя простуда – это вирус пытается делать свои копии, и для этого ему нужен твой организм. Но это заставляет тебя чихать и у тебя поднимается температура…

Ну вот, компьютерные вирусы такие же. Чтобы делать свои копии, им надо заразить компьютеры и в то же время повредить их. Вот почему они называются вирусами.

3. Первые вирусы

Первые вирусы были довольно разнообразными. Некоторые были ужасными, так как могли уничтожить всю информацию на компьютере, но не все были такими.

Например, один вирус, который появился в начале 1999 года, всего лишь показывал фейерверки на экране компьютера, который он заразил. Вот почему его назвали ‘Happy99’.

4. Какими простыми они были!

Несколько лет назад компьютеры были не такими как сейчас. На них не было Windows или Linux, и даже экраны были не цветными! Они были гораздо более простыми машинами чем те, которыми мы пользуемся сегодня, и то же самое относилось к их программам. Интернета не существовало, электронной почты – тоже.

Компьютерные вирусы были также очень простыми, так как им совсем не нужно было быть сложными для того, чтобы работать.

5. Забавная часть

Хотя вирусы всегда обладают вредными эффектами, некоторые из них заставляют улыбнуться. Например, есть вирус, который показывает машину скорой помощи, которая ездит взад-вперед по экрану.

Другой ‘ложный’ вирус - это просто текст в электронном письме, в котором говорится, что это несовершенный вирус, который не способен сам причинить вред, поэтому тебя просят удалить несколько файлов, разбить детали компьютера или даже поджечь его!

6. Упражнения

1. Сколько названий компьютерных вирусов ты знаешь? А биологических вирусов?
2. Поищи в Интернете и найди материал про 5¼ диски, первый

способ распространения вирусов.
3. Обсуди со своим учителем и одноклассниками: забавны ли компьютерные вирусы?

Глава 2: Что тебе следует знать

1. Это не магия, это…

Компьютерные вирусы не создаются какой-нибудь магией. Совсем как Windows или игры, в которые ты играешь на своем компьютере, вирусы создаются людьми. Чтобы сделать это, они используют странные наборы знаков и слов, которые называются ‘язык программирования’, так что такой язык используется как для игры СИМС, так и для вредоносных вирусов.

2. Королева программ

Компьютерам нужен ‘мозг’, чтобы работать. Без него они были бы не больше, чем просто набор электронных деталей, и они не знали бы, что им надо делать! В компьютерах этот ‘мозг’ называется ‘операционная система’. Есть разные виды таких систем, но самая распространенная называется Windows. На всей Земле миллионы компьютеров, на которых установлена Windows, вот почему она известна как 'Королева Программ’.
Но также по этой причине большинство вирусов создаются для работы под Windows, так как именно в таком случае они смогут заразить миллионы компьютеров.

3. Сети

Иногда мы говорим, что вирус заразил ‘сеть’. Сеть – это несколько компьютеров, соединенных друг с другом, чтобы люди, работающие за этими компьютерами, могли общаться друг с другом, пользоваться одной программой или другим оборудованием, таким как принтеры.
Есть вирусы, разработанные для того, чтобы наносить вред сетям: так что если один компьютер заражается, то заразятся все остальные в сети.

4. Всемирная сеть Интернет

Теперь ты знаешь, что такое сеть. Ну а теперь давай попытаемся представить много сетей по всему миру, соединенных друг с другом. Это и называется Интернетом. Вот почему Интернет еще известен как ‘Всемирная сеть'.
Благодаря Интернету мы можем пользоваться программами на компьютерах, которые на самом деле находятся на другой стороне земного шара.

5. Упражнения

1. Посмотри на различные компакт-диски и определи, на каких находятся операционные системы.
2. Посмотри, сможешь ли ты узнать различные видимые элементы операционной системы.
3. Обсуди со своим учителем и одноклассниками: как Интернет влияет на нашу повседневную жизнь?

Глава 3: Типы вирусов

1. Вирусы, черви и троянцы

Здесь всегда присутствует путаница: несмотря на то, что все они называются вирусами, они не одинаковы и делают разные вещи. В основном существуют три типа вирусов. Давай рассмотрим, что они из себя представляют.

- Все началось с вирусов

Первыми появились вирусы. Они разработаны, чтобы копировать себя, заражая компьютеры. Но при этом они обычно уничтожают файлы.

- Извивающиеся черви

Компьютерные черви очень любят распространяться с одного компьютера на другой, и как можно быстрее. По этой причине они обычно не останавливаются, чтобы сделать что-нибудь еще на компьютере. В отличие от вирусов, им ничего не надо уничтожать, чтобы делать свои копии. Однако иногда они могут распространяться так быстро, что занимают слишком много места на компьютере и мешают людям пользоваться компьютерами или сетями.

- Троянские войны

Знаешь историю о Троянском коне? Много лет назад греки и троянцы воевали друг с другом. Хитроумным грекам пришла в голову великолепная идея, как пробраться в неприступный город Трою. Они построили огромного деревянного коня, и притворились, что возвращаются в свою страну, оставив его как подарок победителям. Троянцы забрали коня внутрь города и стали праздновать победу. Тем временем, греческие солдаты, которые спрятались внутри коня, вылезли и открыли ворота своим товарищам, которые незаметно вернулись.

Так вот, существуют некоторые вирусы, которые используют такой же трюк для проникновения в компьютеры. Иногда они прячутся в других программах. Троянцы не созданы для самокопирования или уничтожения файлов, но они могут делать множество других вещей, например, красть пароли, которые ты используешь для входа на свои любимые страницы.

- Секундочку… это еще не все!

Вирусы - не единственные программы, опасные для компьютеров. Существуют другие программы, некоторые со странными названиями вроде ‘логические бомбы’, которые могут быть настолько же, или еще более опасными, чем вирусы.

2. Двойные неприятности

Недавно люди, создающие вирусы, поняли, что могут соединять вместе два и более вида вирусов, чтобы причинять еще больше повреждений компьютерам. Это значит, что теперь существуют 'черви/троянцы' которые распространяются быстро, как черви, но действуют как троянцы.

3. Упражнения

1. Сколько существует типов вирусов?
2. Поищи сходства между компьютерными и биологическими вирусами.
3. Обсуди со своим учителем и одноклассниками: подходящие ли названия ‘вирус’, ‘червь’ и ‘троянец’? Почему?

Глава 4: Что делают вирусы?

1. Видимые эффекты

Некоторые вирусы не повреждают компьютер, они просто показывают изображение с текстом или картинкой.

Но другие очень опасны. Некоторые даже могут удалить все содержимое жесткого диска твоего компьютера! Другие могут мешать тебе войти в Интернет или играть в твои любимые игры.

2. Городские мифы

Важно чтобы ты знал, что могут делать вирусы с твоим компьютером, но также важно тебе знать, что они не могут делать. Ты наверно слышал, как люди рассказывают сказки о том, что вирусы могут делать всякие ужасные вещи, но

очень часто это неправда.
- Компьютерные вирусы не влияют на людей и не вызывают заболевания.
- Вирусы не могут ломать вещи. Худшее, что они могут сделать - это уничтожить информацию на компьютере, но они не могут сломать сам компьютер.
- Вирусы всегда можно удалить с компьютера.
- Вирусы всегда создаются людьми.

3. Упражнения

1. Как бы ты попытался сломать монитор, просто вводя команды с клавиатуры?
2. Какие файлы на твоем компьютере ты бы не хотел потерять больше других? Почему?
3. Обсуди со своим учителем и одноклассниками: почему люди придумывают истории, например, о том, что компьютерные вирусы могут убить человека?

Глава 5: Самые знаменитые вирусы

1. Пятница 13 - не фильм!

Это один из самых опасных вирусов, когда-либо существовавших. Он называется ‘Пятница-13’ потому, что удаляет много файлов на компьютере, когда наступает эта дата. Но тебе не стоит волноваться, он заражает только операционные системы MS-DOS и не может причинить вреда Windows.

2. Берегись Микеланджело

‘Микеланджело’ – это один из старейших и известнейших вирусов. Он начинает работать 6 марта, в день рождения Микеланджело – знаменитого художника, скульптора и архитектора. Одно время люди боялись, что он заразит гораздо больше компьютеров, чем он на самом деле сделал, но, в конце-концов оказалось, что от него было больше дыма, чем огня!

3. Вероломная Мелисса

Мелисса – имя подружки создателя этого очень опасного вируса. Этот вирус/червь первым стал распространяться по электронной почте и застал врасплох многих пользователей.

4. CIH-разрушитель

Этот вирус, также известный под названием ‘Чернобыль’, действительно опасен. Он широко распространялся и удалял особую часть памяти компьютеров под названием BIOS, в результате чего компьютеры переставали работать. Однако он просто убирает содержимое микросхемы из памяти, но не уничтожает ее, так что когда данные снова сохраняются в память, компьютер снова будет прекрасно работать.

5. Мальчик-пузырь

До появления ‘BubbleBoy’ все были уверены, что вирус надо активировать, чтобы он смог заразить компьютер. Но этот вирус мог стереть жесткий диск, когда несчастный пользователь открывал электронное письмо… И не нужно было ни одного щелчка мышью!

6. Запятнанная любовь

Печально известный вирус ‘Loveletter’ (Любовное письмо) занимает заслуженное место в истории компьютерных вирусов. В мае 2000 года этот вирус заразил миллионы компьютеров по всему миру, притворяясь романтическим посланием. Что хуже, появились различные версии этого

вируса.

7. Ядовитый карлик

Названный в честь тигра Шер-Хана из Маугли, вирус 'SirCam' быстро распространялся по электронной почте, и его жертвы не могли работать: не могли подключаться к Интернету, открывать программы, проверять жесткий диск антивирусом…. не могли ничего!

8. Красная тревога!

Несмотря на то, что вирусы в основном нападают на компьютеры пользователей, CodeRed был разработан для атаки больших компьютеров в компаниях (они называются 'серверы'). Избавиться от этого вируса было сложной задачей, потому что при выключении этих серверов люди во всей компании не могут работать.

9. Это все продолжается и продолжается…

У вирусов есть определенный жизненный цикл. Они заражают, затем их обнаруживают, и вскоре они прекращают распространяться. Тем не менее, существуют несколько действительно упрямых вирусов, например, Klez.I, которые не прекращают заражать компьютеры. Когда его впервые обнаружили пару лет назад, он продолжал появляться на компьютерах по всему миру. Совсем как кролик в знаменитой рекламе батареек, он все работает и работает и работает...

10. Вирус, который нокаутировал Интернет

SQLSlammer был еще одним историческим вирусом. Как CodeRed, его целью было поражение компаний, а не обычных пользователей компьютеров. Он распространялся с необыкновенной скоростью (всего за несколько часов облетел весь мир) и практически остановил работу Интернета на некоторое время.

11. Бластермания

Когда все были на выходных, появился странный вирус 'Blaster'. Пользователям не надо было ничего делать для его распространения, они просто подключались к Интернету – и все, вред нанесен. Blaster пользуется уязвимостью (так называемой 'дырой'), которая есть в некоторых операционных системах, чтобы проникать в компьютер без твоего ведома. После чего он, конечно, лезет и на другие компьютеры…

12. Вирусный Шумахер

Если бы существовали гонки вирусов, Mydoom бы непременно победил. За короткий промежуток времени он умудрился заразить миллионы компьютеров. И это еще не все - Mydoom заставил веб-страницу www.sco.com на некоторое время прекратить работу.

13. Упражнения

1. Вспомнишь ли ты другие вирусы, кроме описанных в этой главе?
2. Расставь названия вирусов напротив типов компьютеров, которые они заражают

CodeRed
Blaster
Серверы в компании SQLSlammer Персональные компьютеры
Loveletter
Melissa

3. Обсуди со своим учителем и одноклассниками: если вирус становится известным, будут ли люди относиться лучше к его создателю?

Глава 6: Розыгрыши

1. Не верь ни единому слову...

Вне всякого сомнения, ты или один из твоих друзей видели электронное письмо, в котором вас предупреждали об опасном вирусе, который может причинить серьезные повреждения. Эти письма – полные враки. Если бы появился настолько опасный вирус, ты, скорее всего, бы услышал об этом по телевизору.

Такие письма называются розыгрышами, то есть они говорят неправду. Иногда они даже просят тебя удалить файлы с твоего компьютера. Не обращай на это внимания, иначе твой компьютер просто перестанет работать.

Так что будь осторожен и не попадайся на розыгрыши!

2. Так зачем люди создают эти розыгрыши?

Некоторые люди используют эти розыгрыши как способ узнать множество электронных адресов, чтобы затем посылать на них рекламу.

В других случаях они просто хотят сыграть шутку или навредить людям без особой причины.

3. Как мне поступать с розыгрышами?

Если ты получишь розыгрыш, удали его и забудь. Никому его не пересылай, даже если он показался тебе смешным. Так ты сможешь остановить его распространение среди других людей, которые могут в него поверить.

4. Спасите мишку!

Одним из примеров розыгрыша является вирус ‘маленький мишка’. Он сообщает, что существует очень опасный вирус, который заразил много компьютеров, причем их владельцы ничего об этом не знают. Также в нем говорится, что вирус содержится в файле, на иконке которого изображен медвежонок. И все, что тебе надо сделать, чтобы удалить вирус - это удалить файл с такой иконкой.

Но дело в том, что этот файл не вирус. И если ты удалишь его, Windows перестанет правильно работать.

5. Как заметить их?

Распознать розыгрыши гораздо проще, чем кажется. Прочитай подсказки, и ты всегда будешь защищен от них:

- Когда они рассказывают о вирусе, они всегда упоминают все плохие вещи, которые он делает. По их словам, это всегда самый ужасный вирус из всех существовавших.
- Они часто представляются работниками известных компаний, например Microsoft.
- Они иногда сообщают, что если ты несколько раз перешлешь сообщение, то можешь выиграть приз.
- Некоторые также делают вид, что содержат деловые предложения, позволяющие заработать много денег.

6. Упражнения

1. Какие из этих текстов являются типичным розыгрышем:

Тема: Берегитесь, вирус!

Вчера IBM сообщили о новом быстро распространяющемся вирусе. Если вы получите письмо с темой “Привет”, вы должны немедленно удалить его, так как оно может привести в негодность ваш компьютер. Перешлите это сообщение всем друзьям в вашей адресной книге!

Тема: Вирусная тревога

23 числа этого месяца Panda Software (www.viruslab.ru) обнаружила вирус, который приводит к падению серверов. Вся информация об этом вирусе доступна на веб-странице Panda Software.

Тема: Берегитесь!

Если вы найдете файл с именем cmd.exe или command.com на вашем компьютере, удалите его немедленно, так как это опасный вирус и против него нет известного лекарства.
2. Опрос: Какую самую немыслимую историю ты слышал в жизни?
3. Обсуди со своим учителем и одноклассниками: кому выгодны эти ложные истории?

Глава 7. Как проникают вирусы?

1. Все дороги ведут... в твой компьютер

Давно, когда не было Интернета и электронной почты, у вирусов было мало способов проникновения в компьютер. Они были более или менее вынуждены использовать флоппи-диски для распространения с одной системы на другую. Однако появление Интернета создало много возможностей для вирусов. Электронная почта является самым частым способом их распространения в наши дни. Но скачанные фильмы, музыка или игры тоже могут быть очень опасны. Как мы рассказывали раньше, Интернет сам по себе является сетью компьютеров, и это может позволить другим людям проникнуть в твой компьютер.
Настоящая проблема заключается в людях, которые хотят проникнуть в компьютеры других людей для того, чтобы красть или просто уничтожать информацию. Для этого они иногда используют троянцев, которых затем могут использовать как угодно.

2. Даже твой PlayStation

Компьютерные игры, DVD и даже игровые приставки могут содержать вирусы. Так что ты должен всегда убеждаться, что программы поступают из надежного источника.

3. Нельзя доверять даже лучшему другу

Ладно, все не так плохо.... но почти так. Представь себе, что кто-то дал твоему другу замечательную игру, и она ему так понравилась, что он дал ее поиграть тебе. Будь осторожен. Ведь возможно, что это игра заразит твой компьютер, и вы будете заражены вместе с другом.

И более всего, никогда не доверяй друзьям, с которыми ты знакомишься в ‘чатах’. Никогда не принимай файлы, если они их пришлют тебе, неважно насколько классными они тебе кажутся. Откуда ты знаешь, что это не хакер, который пытается напасть на твой компьютер?

4. Плавай по Интернету... но остерегайся акул!

Как мы говорили раньше, скачанные из Интернета файлы являются любимым способом вирусов для проникновения на твой компьютер. Неважно, насколько известную программу ты скачиваешь, важен сайт, с которого ты ее качаешь. Представь, что ты хочешь скачать рекламный ролик Властелина Колец. Человек, который скачивал его до тебя, мог добавить в него троянца и положить его на сайт, чтобы его скачали другие. Ты все равно сможешь посмотреть фильм, но вместе с этим установишь троянца!

5. Бойся мула!

Несомненно, ты знаешь кого-нибудь, кто пользуется P2P программами, чтобы обмениваться и скачивать музыку, фильмы и игры из Интернета. Таких программ много: eMule (и-Мул), KaZaA, WinMX...
Лучше всего избегать таких программ, так как они сейчас стали другим популярным методом проникновения вирусов на твой компьютер. Многие вирусы запрограммированы на распространение с ложными именами через такие программы для того, чтобы ты подумал, что это фильмы, песни или игры.

Так что когда ты скачиваешь их на свой компьютер, вместо своей любимой песни ты на самом деле скачиваешь вирус.

6. А как насчет сотовых?

Кажется, что теперь создатели вирусов заинтересовались сотовыми телефонами. И особенно последними моделями, которые являются почти мини-компьютерами.

И хотя этот интерес начался с простых испытаний, призванных показать, можно ли заразить сотовый телефон, сейчас появляется все больше и больше вирусов с такой же целью. Скоро мы можем услышать о вирусе, который помешает тысячам людей разговаривать по сотовым телефонам. Тем не менее, не стоит слишком волноваться – к тому времени как это случится, у тебя будут способы защитить свой телефон от заражения вирусом.

7. Упражнения

1. Какими способами вирус может проникнуть в компьютер.
2. Как без твоего ведома может установиться троянец?
3. Обсуди со своим учителем и одноклассниками: стоит ли рисковать, скачивая программы с неизвестных сайтов?

Глава 8: Оружие против вирусов

1. Лучше защититься, чем потом лечиться

К тому времени, как ты дойдешь до этой главы, ты будешь знать, что такое вирусы, как они работают и что они могут делать, а чего не могут.

Но тебе также следует помнить, что заражения вирусом можно избежать, если принять правильные меры предосторожности. Также как есть люди, создающие вирусы, есть другие люди, посвятившие себя борьбе с ними, которые делают все, чтобы создатели вирусов не добились своей цели.

Вот почему существуют программы, называемые антивирусами, которые обнаруживают и уничтожают вирусы прежде, чем они смогут причинить какой-либо вред. Например, если червь попытается проникнуть на твой компьютер, спрятавшись в электронном письме, антивирус обнаружит его и сразу же уничтожит, так что ты сможешь быть уверен, что письма, которые к тебе приходят, не заражены.

2. Всегда обновленный

Теперь ты знаешь, как защититься от вирусов, но будь внимателен! Только то, что у тебя на компьютере установлен антивирус, не значит, что он остановит их всех. Чтобы сделать это, его надо обновлять каждый день. Почему? Это очень просто. Многие люди заняты постоянным созданием вирусов, и каждый день появляются новые вирусы. Антивирус следует постоянно обновлять для того, чтобы он узнавал этих новых врагов.

В антивирусных компаниях работают люди, изучающие вирусы и создающие лекарства против каждого нового вируса. После того как лекарство выпущено, его нужно встроить в программу-антивирус в твоем компьютере для того, чтобы антивирус смог находить самые новые вирусы. Вот почему твой антивирус должен быть всегда обновлен.

3. Новые антивирусные решения

Некоторые вирусы так быстры, что у пользователей совсем не остается времени, чтобы защитить себя перед тем, как вирусы заразят миллионы компьютеров. Чтобы блокировать и уничтожать вирус антивирусные решения должны иметь информацию о нем. Это значит, что лекарства, разработанные антивирусными компаниями, должны быть установлены на компьютер. Если это не делать каждый день, любой новый вирус

может стать причиной катастрофы.
Те, кто делает такие супер-быстрые вирусы, пытаются воспользоваться временем, которое проходит между обновлениями антивируса на твоем компьютере. Поэтому некоторые компании разработали новые разумные технологии, которые могут узнавать вирусы по тому, как они ведут себя. Это значит, что эти технологии не нужно обновлять, чтобы предотвратить нападение даже самого нового вируса. Если твой антивирус обладает такой технологией, твой компьютер будет гораздо сильнее защищен.

4. Если не знаешь - спрашивай!

В любом случае, нужно быть внимательным. Например, представь, что по какой-то причине твой антивирус не обновлен, или что ты - первый человек, получивший новый вирус. Если ты видишь что-либо необычное на своем компьютере или получаешь сообщение от кого-то, кого не знаешь (или даже если знаешь) и оно кажется странным... ничего не делай. Найди кого-нибудь, кто поможет тебе проверить компьютер. Так ты избежишь неприятных сюрпризов.

5. Упражнения

Обсуди со своим учителем и одноклассниками: правда или неправда, что:
1. Установить на компьютер антивирус достаточно, чтобы защитить тебя от вирусов.
2. Новые вирусы появляются каждый день.
3. Когда ты получаешь странное электронное письмо, ты должен открыть его и посмотреть, что внутри.

ЧАСТЬ 2
ДРУГИЕ ОПАСНОСТИ ИНТЕРНЕТА

Глава 1: Основы

1. Вредоносное ПО - что это за слово?

Странное слово, не так ли? Но значение его очень простое. Как ты узнаешь из второй части, вирусы—не единственная опасность в Интернете. К сожалению, существует множество людей, которые любят причинять вред, и постоянно придумывают новые способы делать это.
Было создано так много программ, причиняющих повреждения, что для них придумали новое слово. Так как 'ПО' (программное обеспечение) используется для описания всех программ, которые ты используешь на своем компьютере, 'вредоносное ПО' используется для описания тех программ, которые могут повредить твой компьютер.

2. Другие опасности в Интернете

Теперь ты знаешь об одном виде вредоносного ПО: вирусах. Но существует множество других, которые также могут наносить вред компьютерам. Основные виды это:
- Шпионское ПО: программы, которые наблюдают за тем, что ты делаешь, и рассказывают это людям с плохими намерениями.
- Шутки: программы, гадко подшучивающие над тобой.
- Спам или мусорная почта: это вся та утомляющая реклама, которую тебе шлют, но о которой ты никогда не просил.
- Дозвонщики: они могут заставить твой модем подключиться к Интернету

через очень дорогие телефонные номера.
- Программные уязвимости: они позволяют людям, которые называются хакерами, проникать в твой компьютер и делать на нем что угодно.

- Утилиты скрытого управления: программы, которые помогают хакерам проникать в компьютеры.

3. Не обожгись: используй брандмауэр

Вирусы и хакеры иногда используют 'коммуникационные порты' для проникновения в компьютеры. Эти порты – что-то вроде маленьких дверей, через которые компьютеры подключаются к Интернету, получают и посылают электронные письма или скачивают файлы. Но если ты не примешь правильные меры предосторожности, вирус или хакер может запросто открыть их и нанести вред твоему компьютеру.

Чтобы не дать этому случиться, лучше всего использовать брандмауэр - это инструмент, который проверяет, чтобы никто не использовал порты на твоем компьютере для вредоносных действий. Так что если хакер попытается проникнуть и украсть что-нибудь, твой брандмауэр остановит происходящее, закрыв порт и подав тебе сигнал.

4. Упражнения

1. Достаточно ли одного антивируса для защиты твоего компьютера?
2. Сколько видов вредоносного ПО ты можешь вспомнить?
3. Обсуди со своим учителем и одноклассниками: получали ли вы когда-нибудь вредоносное ПО? Раздражало ли оно вас?

Глава 2: Так много писем…

1. Что такое спам?

Спам - это электронные письма с рекламой, которые приходят день за днем, хотя ты никогда не просил, чтобы их тебе слали.

Название *спам* происходит от сцены в одной старой комедийной передаче, где единственным блюдом в меню ресторана был спам (консервы) и как-то раз отряд викингов вошел туда, скандируя: “спам, спам, спам…”

Вот почему, по крайней мере, по слухам, вся эта реклама называется спам.

2. Это всего лишь электронные письма, но…

Может быть, кажется, что спам только надоедает и ничего больше, но он также может причинять вред. Каждый день люди получают миллионы спам-писем, только подумай о том, сколько времени тратится по всему миру - если не читать, а просто удалять их!

И спам может также содержать вирусы или прочие вредоносные программы, которые используют такие письма для быстрого распространения.

3. Каждое второе письмо…

Может быть, ты получаешь всего четыре или пять спам-писем каждый день, так что это для тебя небольшая проблема. Но представь себе большую корпорацию, в которой работают 3 тысячи человек. Теперь умножь эти четыре-пять писем на 3000 (без калькулятора! Хе-хе..) Это около 15 тысяч спам-сообщений каждый день. Поэтому для крупных организаций это реальная проблема, которая может помешать им правильно работать.

Чтобы справиться с этой проблемой, люди в организации, которые занимаются защитой сети, обычно устанавливают систему под названием ‘фильтр

содержимого’. Это просто: системе говорят, что нужно не пускать письма с определенными рекламными словами.

4. Даже сами письма могут быть опасны

Спам не только надоедливый приставала, он также может быть опасен. Есть люди с плохими намерениями, которые, если узнают твой электронный адрес, могут присылать тебе всякие вещи: фотографии, которые тебе не следует видеть, оскорбления или даже угрозы тебе и

твоей семье. Если ты когда-нибудь встретишься с таким, не отвечай, а сразу же<0} скажи об этом своим родителям или учителям. Они знают, что надо сделать, чтобы эти люди прекратили беспокоить тебя.

5. Упражнения

1. Получал ли ты электронные письма с рекламой? Сколько?
2. Что ты должен делать, если к тебе приходит спам?
3. Обсуди со своим учителем и одноклассниками: как могут зарабатывать деньги люди, которые рассылают спам?

Глава 3: Дозвонщики: кто будет оплачивать счет?

1. Очень дорогая угроза

Дозвонщики очень опасны, так как вред, который они причиняют, влияет не только на твой компьютер: они могут заставить твой телефонный счет вырасти до небес!

Но прежде чем ты поймешь, что такое дозвонщик, тебе нужно понять кое-что еще. Когда ты подключаешься к Интернету, используя телефонную линию, ты в действительности набираешь телефонный номер, который подключает тебя к серверу, а этот сервер подключает тебя к Интернету.

Эти серверы обладают особыми телефонными номерами, поэтому, когда ты подключаешься к ним, это стоит тебе не дороже чем, к примеру, позвонить другу.

Дозвонщики также используются для подключения к Интернету, но они используют другие телефонные номера, которые стоят гораздо больше, чем те, которые используются нормальными серверами. Проблема в том, что существуют дозвонщики, которые изменяют номер, используемый для подключения к Интернету на один из этих номеров.

Это значит, что каждый раз, когда ты подключаешься к Интернету, это будет стоить тебе целое состояние. И тебе придется заплатить за это, несмотря на то, что ты даже не будешь знать, что случилось.

2. Как их остановить?

Так как это серьезная проблема, был разработан метод для борьбы с ней. Он заключается в программе, которая запоминает номер, который ты обычно используешь для подключения к Интернету. Таким образом, если дозвонщик пытается изменить твое подключение, набрав другой номер, программа

обнаружит это и даст тебе сигнал, сообщая номер, который пытается быть набран и спрашивая, хочешь ли ты подключиться или нет. Если ты увидишь такое сообщение, и ты не уверен, что тебе делать, ничего не трогай и попроси кого-нибудь помочь тебе.

3. Упражнения

1. Проверь номер, который обычно использует твой модем для подключения к Интернету.
2. У тебя на компьютере когда-нибудь был дозвонщик? Какой номер он набирал?
3. Обсуди со своим учителем и одноклассниками: стоит ли оплачивать дорогие телефонные счета просто потому, что ты не был осторожен с файлами, скачанными из Интернета?

Глава 4: Кто-то следит за тобой - программы-шпионы

1. Хитрые и опасные

Программы-шпионы - это один из самых частых типов вредоносных программ.

Эти программы разработаны шпионить за тем, что ты делаешь на своем компьютере, особенно когда ты подключаешься к Интернету. Они собирают информацию о веб-страницах, которые ты обычно посещаешь, количестве времени, которое ты проводишь в Интернете и том, какой компьютер ты используешь.
Затем программа-шпион посылает эту информацию без твоего ведома другим людям, которые, в свою очередь могут начать слать тебе спам или даже проникнуть в твой компьютер!

2. Никому не рассказывай

Чтобы установиться на компьютер, программы-шпионы прячутся в других программах, таких как демо-версии игр, то есть, когда ты устанавливаешь такую демо-версию, одновременно устанавливается программа-шпион.
Но обычно не очень трудно защитить себя от них, так как есть специальные программы, разработанные для того, чтобы обнаруживать и уничтожать программ-шпионов. Установи такую на свой компьютер, и никто не сможет шпионить за тобой!

3. Упражнения

1. За какими действиями может следить шпионская программа?
2. Как программа-шпион проникает в твой компьютер?
3. Обсуди со своим учителем и одноклассниками: нормально ли следить за

пользователями Интернета для того, чтобы специально адаптировать под них рекламу?

Глава 5: Берегись хакеров!

1. Хакер — кто это такой?

Хакеры – это люди, которые очень любят компьютеры и проводят много времени, исследуя компьютерную безопасность. К сожалению, они также любят исследовать компьютеры других людей. Они находят способ проникнуть на твой компьютер и когда проникнут, им просто необходимо оглядеться, сломать что-нибудь или натворить еще каких-нибудь гадостей на твоем компьютере.
Они называют себя по разному: есть ‘хакеры’, которые считают себя ‘хорошими’, так как они ничего не ломают – те, кто ломают, называются ‘крякеры’. Потом есть ‘ламеры’ которые в действительности мало знают, но следуют указаниям хакеров, чтобы добиваться того же самого: ломать и красть информацию.
Потом есть ‘скриптеры’ которые похожи на ламеров, но создают вирусы. Они берут код вируса, немного играют с ним и делают вид, что создали что-то. Они не очень много знают о программировании, но из-за них производителям антивирусов все равно приходится производить новые системы лечения.

2. Не будь ламером!

Хотя некоторые люди до сих пор восхищаются хакерами, не пытайся подражать им. Если ты будешь выполнять их инструкции, ты всего лишь попадешь в серьезные неприятности. Когда они описывают то, что они делают, это может казаться простым, но они не скажут тебе самого главного – правду обо всех хитроумных уловках, которые они используют, чтобы скрыть свои следы.

Правоохранительные органы всех стран мира пристально наблюдают за такими действиями, так что, если ты хочешь избежать неприятностей, ты знаешь как себя вести…

3. Хорошо смеется тот…

Лучше всего забыть о существовании хакеров, но быть защищенным от них. Твой компьютер, даже если он не кажется чем-то особенным, может оказаться

полезным инструментом для хакеров, так что тебе надо убедиться в том, что они не могут напасть на тебя.
Как? Просто установить антивирус, который может обнаруживать троянцев и другие утилиты, используемые хакерами, и брандмауэр, который помешает им проникнуть в твою систему.

4. Упражнения

1. Проверь меры безопасности твоего компьютера, защищающие от хакеров.
2. Поищи на своем компьютере файлы, в которых записана активность твоего компьютера, они называются логи. Попроси своего учителя помочь тебе или показать тебе пример, если ты не можешь их найти.
3. Обсуди со своим учителем и одноклассниками: заслуживают ли хакеры восхищения?

Глава 6: Опасные самоделки: утилиты скрытого управления

1. Скрытые, но эффективные...

Хакеры используют множество программ для своих темных делишек. Эти программы называются 'утилиты скрытого управления', и они являются инструментами, которые нужны хакерам для проникновения в компьютеры других людей.
Они не сильно распространены потому, что если они бы стали слишком известны, пользователи были бы настороже. Несмотря на это, лучшие антивирусы способны находить их и предупреждать тебя, если хакер пытается использовать их на твоем компьютере.

2. Почему я?

Хакеры используют эти утилиты для того, чтобы проникать в твой компьютер и красть информацию. Даже если ты думаешь, что твоя информация для них не важна, для хакеров могут быть полезными даже пароли от твоей почты или серийные номера для игр.
И что хуже, они могут использовать твой компьютер для проведения атак против других компьютеров или кражи с них информации. Это приведет к тому, что ты будешь выглядеть преступником, и даже не будешь знать об этом!

3. Держись подальше от неприятностей...

Утилиты скрытого управления часто выглядят привлекательно. Они притворяются программами, с помощью которых ты можешь развлечься, подсматривая за компьютерами своих друзей или двигая их указателем мыши. Но одновременно могут использовать тебя, а ты даже не будешь знать об этом. Оставь эти программы в покое, и так ты избежишь неприятностей.

4. Упражнения

1. Найди шесть программ на своем компьютере, которые можно использовать как инструменты для выполнения каких-нибудь действий.
2. Узнай источник слова ‘хакер’. Почему ты думаешь, этих людей называют ‘хакерами’?
3. Обсуди со своим учителем и одноклассниками: хорошие ли люди – хакеры?

Глава 7: Чаться… но будь осторожен

1. Не все в Интернете хорошо

Одна из прелестей Интернета – это то, что ты можешь развлекаться. Ты можешь переписываться с друзьями, играть с людьми даже по другую сторону Земли, и чатиться со множеством людей одновременно.

Но не забывай, что ты не видишь людей, с которыми говоришь, и иногда другой человек может хотеть большего, чем просто немного початиться. Есть много воров, мошенников и прочих преступников, которые пользуются чатами и притворяются такими, как ты. Они могут постараться заставить тебя выдать личные данные о себе, например: где ты живешь, твой номер телефона или адрес школы. **НИКОГДА** не давай никому информацию о себе, кроме своего имени, даже не говори фамилию. И если кто-нибудь в чате скажет или спросит о вещах, которые заставят тебя почувствовать себя неуютно или не понравятся, **СРАЗУ ЖЕ** скажи об этом кому-нибудь, или, даже лучше - просто закончи разговор.

2. IRC-войны

Когда ты общаешься в чате, там есть множество людей, которые просто хотят раздражать тебя, и у них есть много способов это сделать. Например, один способ – это притвориться тобой и посылать от твоего имени так много данных на сервер, что тебя выкинут за надоедание. Это называется нюк-атака.
Или наоборот, они могут слать столько данных на твой компьютер, что они заблокируют его или 'зафлудят', и он перестанет работать.

3. Держи защиту включенной!

Чтобы не дать никому такое сделать, когда ты в чате, тебе следует защититься. Чтобы помочь тебе в этом существуют программы, которые создают барьер между твоим компьютером и Интернетом для того, чтобы никто не смог

проникнуть в твой компьютер без твоего разрешения. Они называются 'брандмауэры'.
Лучше всего иметь персональный брандмауэр, который подстраивается специально под твой компьютер. В компаниях тоже есть брандмауэры, но гораздо более сложные и иногда находящиеся в компьютерах размером со шкаф! Иметь такой дома было бы все равно, что пытаться расколоть орех кувалдой!
Если у тебя установлен работающий брандмауэр, ты будешь гораздо сильнее защищен.

4. Никогда не ходи на встречи с незнакомцами

Несомненно, ты завел много друзей в Интернете, особенно в чатах. В этом нет ничего плохого, но ты должен быть осторожен. Есть люди, которые заинтересованы в детях и подростках, таких как ты, но совсем не так, как твои родители. Мы говорим о взрослых, которые используют чаты и притворяются твоим ровесником, и возможно с теми же интересами что и ты, для того чтобы назначить встречу с тобой или сделать тебе непристойные предложения. Некоторые из них попытаются заставить тебя дать им информацию о себе, чтобы найти тебя.
Поэтому никогда не давай информацию о себе никому в Интернете, даже если ты общался с этим человеком в чате. И конечно, никогда не соглашайся на встречи с кем-нибудь, кого ты встретил в чате. Тебе всегда стоит сказать своим родителям или учителю, чтобы они смогли узнать, кто этот человек и какие у него намерения.
Не стесняйся говорить, что кто-то беспокоит тебя. Ты всего лишь делаешь правильную вещь.

5. Никогда не принимай подарков от незнакомцев

Несомненно, ты используешь или по крайней мере знаешь о программах, которые позволяют чатиться, и называются 'клиенты обмена мгновенными сообщениями'. Это программы, такие как ICQ ("аська"), MSN Messenger и т.д. Эти чаты отличаются тем, что они приватные и обычно общение происходит только между двумя людьми.

Они также позволяют тебе вместе с сообщениями слать своим друзьям файлы.
Иногда эти системы используют люди с плохими намерениями, чтобы слать файлы с вирусами или другими вредоносными программами, которые установятся на твой компьютер, если ты откроешь их. Поэтому тебе всегда стоит быть осторожным и не принимать никакой файл от людей, которых ты не очень хорошо знаешь, и которые могут обмануть тебя.

6. Упражнения

1. Сопоставь следующие названия продуктов с их ролью в Интернете.
mIRC Антивирус и брандмауэр
Messenger Программа обмена мгновенными сообщениями
Вирусы и другие угрозы – о них нужно знать 34
www.viruslab.ru
Eudora Интернет-обозреватель
Netscape Чат
Internet Explorer Электронная почта
Platinum Internet Security
2. Как ты узнаешь, что кто-то пытался ограбить тебя или причинить тебе вред?
3. Обсуди со своим учителем и одноклассниками: что надо делать, если кто-то надоедает тебе или если ты раскрыл ему информацию, которую не стоило раскрывать в чате?
Вирусы и другие угрозы – о них нужно знать 35
www.viruslab.ru

Глава 8: Практические шутки

1. Не такие смешные, как кажутся...

В Интернете ты можешь найти любые вещи: например, шутки, которые ты можешь послать своим друзьям. Их очень, очень много, и некоторые могут быть очень смешными.
Но некоторые из этих шуток могут оказаться не столь смешными. Некоторые из них, например, притворяются _____вирусами, и могут заставить тебя поверить, что
они удаляют информацию, форматируют твой диск или делают подобные вещи.
А что если ты не поймешь, что это шутка? Представь себе, какая возникнет паника. Затем постарайся рассказать своему учителю, что ты потерял всю свою работу, тогда тебе, скорее всего, не будет весело!
И когда ты обнаруживаешь что это шутка… Сначала – паника, затем – рассказ всем об этом, и потом все смеются над тобой, что ты купился на шутку. Ну и денек…

2. Лучше смеяться, чем плакать

Если у тебя есть такие ‘хорошие’ друзья, которые посылают тебе такие шутки, лучше не открывать их и не пересылать никому. Ты всех избавишь от кучи неприятностей.
Если ты получишь что-то такое, скажи людям больше не посылать это, в этом нет смысла.

3. Упражнения

Обсуди следующие идеи со своим учителем и одноклассниками:
Вирусы и другие угрозы – о них нужно знать 36
www.viruslab.ru
1. Смешны ли такие Интернет-шутки?
2. Смешно ли посылать такие шутки друзьям?
Вирусы и другие угрозы – о них нужно знать 37
www.viruslab.ru

Глава 9: Дыры в компьютере? Именно так!

1. Закрой дверь!

Операционные систем и компьютерные программы не всегда идеально защищены. Иногда существуют лазейки, через которые кто-нибудь (или что-нибудь) может проникнуть без твоего ведома. Совсем как шпион пробирается сквозь систему безопасности здания, чтобы украсть секретную информацию. Эти маленькие дырки в системе называются 'уязвимостями' или 'дырами в защите'. Иногда они могут быть не важными, и все что тебе необходимо делать - это соблюдать осторожность при использовании компьютера. Но иногда они представляют серьезный риск для безопасности. Например, вирус Blaster распространялся именно из-за дыры безопасности в Windows.

2. Простые, но эффективные

Способ закрывать такие дыры безопасности – следить за бюллетенями безопасности, которые публикуют создатели программ для того, чтобы пользователи были в курсе новостей безопасности. Правда, существует одна проблема… почти невозможно прочитать все такие бюллетени, и даже если бы ты смог, не просто понять технические описания, которые иногда не понимают даже те, кто их пишет!

Если ты хочешь убедиться, что ты действительно защищен, лучше всего посещать сайт создателя программ, установленных на твоем компьютере, чтобы заделывать найденные дыры безопасности. И делать это раз в одну или две недели, это не отнимет у тебя много времени!

3. Упражнения

1. Подключись к странице обновления производителя твоей операционной системы и обнови ее до последней версии.
2. Сходи на веб-страницу твоей любимой игры и посмотри, есть ли на ней какие-нибудь улучшения к игре, которые ты можешь скачать.
3. Обсуди со своим учителем и одноклассниками: когда в программе обнаружена дыра безопасности, лучше сразу известить всех или ждать пока ее починят? Помни, что хакеры тоже узнают о ней и поспешат воспользоваться, и пользователям следует защитить себя до этого.

Глава 10: Осторожней с тем, что ты видишь в Интернете!

Несомненно, ты знаешь, что в Интернете ты можешь найти все виды информации, но ты, вероятно, также знаешь, что там есть много вещей, которые тебе не стоит видеть. Существуют веб-страницы с очень неприятными картинками и текстом даже для взрослых, и ты ничего не потеряешь, не увидев их.

Также страницы со взрослыми картинками могут открываться сами собой, а иногда страницы, которые ты не собирался смотреть могут появляться, просто если ты пытаешься, например, сходить на сайт своей любимой группы. В таком случае, возможно, на твоем компьютере есть троянец, или это рекламная программа показывает рекламу. Как обычно, лучше всего сказать родителям или учителям, что случилось… и не беспокойся, они тебе поверят!

ПРИЛОЖЕНИЕ

ГЛОССАРИЙ

ЧАТ: Текстовое общение в режиме реального времени через Интернет.

ДОЗВОНЩИК: Программа, которая часто используется для вредных перенаправлений Интернет-подключений. В таком случае она отключает правильное телефонное соединение с Интернетом и переподключается через

очень дорогую телефонную линию. Очень часто пользователь узнает об этом, только когда ему приходит огромный счет за телефон.
БРАНДМАУЭР: Это барьер, способный защищать информацию в системе или сети при подключении к другой сети, например к Интернету.
ФЛУД: Непрерывная отправка большого сообщения или текста на компьютер через системы сообщений для того, чтобы переполнить или 'зафлудить' систему, что приведет к ее сбою.
ХАКЕР: Человек, производящий нелегальный или неавторизованный доступ к компьютеру.
УТИЛИТА СКРЫТОГО УПРАВЛЕНИЯ: Программа, которую использует хакер для того, чтобы выполнять действия, причиняющие проблемы пользователю зараженного компьютера (она позволяет хакеру контролировать зараженный компьютер, красть конфиденциальную информацию, сканировать порты и т.д.).
РОЗЫГРЫШ: Это не вирус, а ложное сообщение о якобы появившемся вирусе.
IRC: Это текстовое общение через Интернет, в котором также можно передавать файлы.
ВРЕДОНОСНОЕ ПО: Все программы, документы и сообщения, которые могут оказывать негативное влияние на ИТ-системы пользователей.
НЮК: Сбой или потеря сетевого подключения, вызванные умышленно.

Компьютер, на котором проведена нюк-атака, также может быть блокирован.
ЯЗЫК ПРОГРАММИРОВАНИЯ: Набор инструкций, команд и правил, который используется для создания программ.
КОММУНИКАЦИОННЫЙ ПОРТ: Точка, через которую компьютер передает информацию (входящую и исходящую) по TCP/IP.
СЕТЬ: Группа компьютеров или других ИТ-устройств, подключенных вместе через кабель, телефонную линию, электромагнитные волны (спутник и т.д.) для коммуникации и совместного использования ресурсов. Интернет является огромной сетью, состоящей из подсетей с подключенными к ним миллионами компьютеров.
СЕРВЕР: ИТ-система (компьютер), которая предлагает определенные сервисы и ресурсы (коммуникация, приложения, файлы и т.д.) другим компьютерам (называемым клиентами), которые подключаются к нему по сети.
СПАМ: Незапрашиваемая электронная почта, обычно содержит рекламу. Такие сообщения, обычно рассылаемые массово, могут быть очень надоедливыми и тратить как время, так и ресурсы.
ШПИОНСКОЕ ПО: Программы, которые отсылают информацию с компьютера без ведома пользователя.
ТРОЯНЕЦ: Если выражаться точно, троянец не является вирусом, хотя их часто путают. На самом деле это программы, которые попадают в компьютер под видом безобидных программ, устанавливают себя и выполняют действия, которые нарушают на конфиденциальность пользователя. Название Троянец происходит из легенды о Троянском коне в греческой мифологии.
ВИРУС: Вирусы – это программы, которые могут проникать в компьютеры и ИТ-системы разными путями, и наносить воздействие, которое варьируется от лишь надоедливого до высоко разрушительного и наносящего непоправимый ущерб.
УЯЗВИМОСТЬ: Недочеты или дырки в защите программы или ИТ-системы, которые часто используют вирусы как способ заражения.
ЧЕРВЬ: Он подобен вирусу, но отличается от него тем, что создает свои копии (или своей части).__