Муниципальное бюджетное образовательное учреждение
“Средняя школа №48 имени героя России Д.С. Кожемякина”

Презентация подготовлена для конкурса “Интернешка”

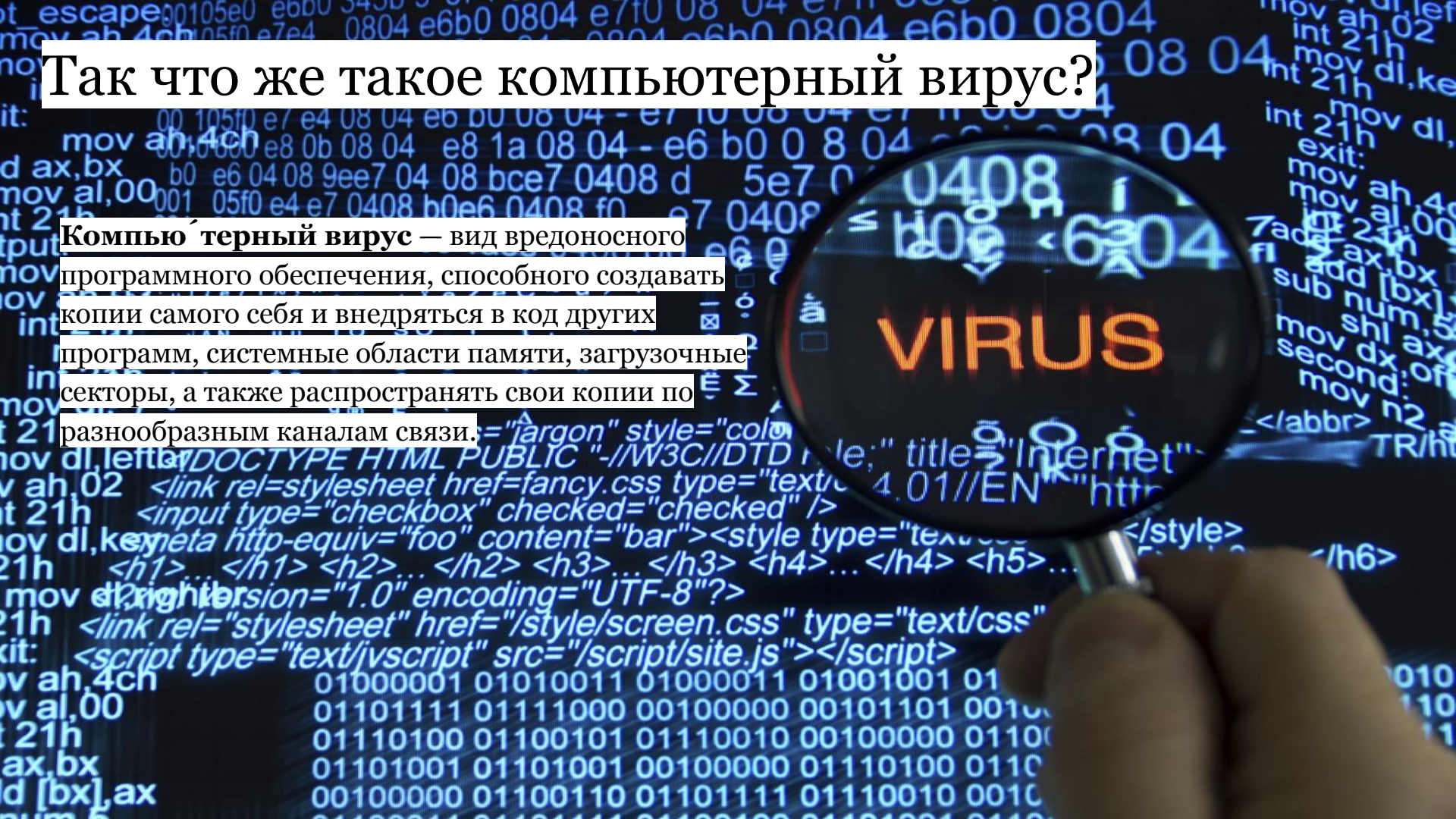
Компьютерные вирусы. Антивирусные программы.

Выполнила:
Ученица 10 класса А
Прошанова Екатерина
Учитель информатики:
Чепасова Наталья Александровна

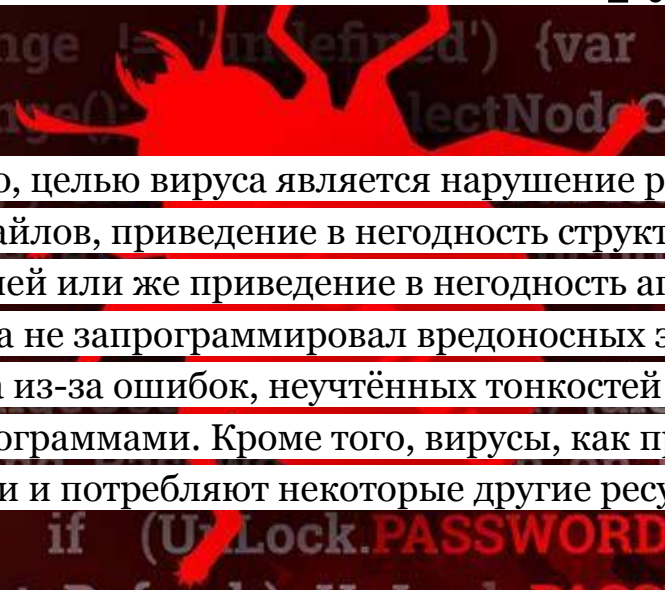
г. Ульяновск, 2016 г.

Так что же такое компьютерный вирус?

Компью́терный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.



Какова цель этих вирусов?



Как правило, целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы.

История компьютерных вирусов

Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ.

Первыми известными вирусами являются Virus 1, 2, 3 и Elk Cloner

Зимой 1984 года появились первые антивирусные утилиты — CHK4BOMB и BOMBSQAD авторства Энди Хопкинса (англ. *Andy Hopkins*). В начале 1985 года Ги Вонг (англ. *Gee Wong*) написал программу DPROTECT — первый резидентный антивирус.

Elk Cloner

Elk Cloner — считается самым первым вирусом, который распространился «in-the-wild», то есть был обнаружен на компьютерах пользователей, а не в системе, на которой он был разработан. Вирус был написан в 1981 году 15-летним школьником Ричардом Скрента для компьютеров Apple II.

Elk Cloner распространялся, заражая операционную систему DOS для Apple II, записанную на гибких дисках. После того, как компьютер загружался с зараженной дискеты, автоматически запускалась копия вируса. Вирус не влиял на работу компьютера, за исключением наблюдения за доступом к дискам. Когда происходил доступ к незараженной дискете, вирус копировал себя туда, заражая её, медленно распространяясь с диска на диск.

Первые вирусные эпидемии

Первые вирусные эпидемии относятся к 1986—1989 годам: Brain.A (распространялся в загрузочных секторах дискет, вызвал крупнейшую эпидемию), Jerusalem (проявился в пятницу 13 мая 1988 года, уничтожая программы при их запуске),червь Морриса (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах).

Тогда же оформились основные классы двоичных вирусов: сетевые черви (червь Морриса, 1987), «троянские кони» (AIDS, 1989), полиморфные вирусы (Chameleon, 1990), стелс-вирусы (Frodo, Whale, 2-я половина 1990).

Классификация вирусов

Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:

1. по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);
2. файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом
3. по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux);
4. по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
5. по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык;
6. по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты.

Распространение

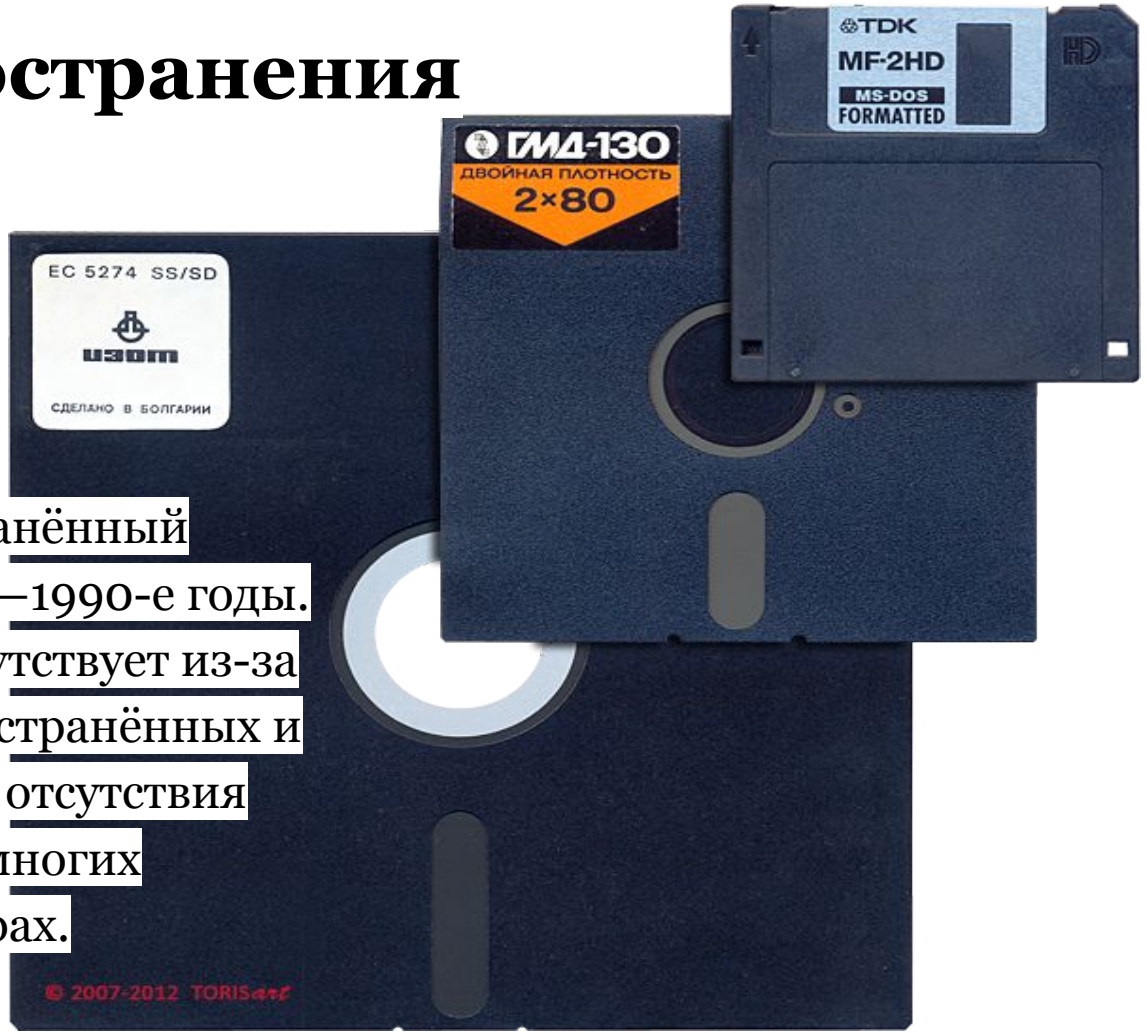
Через интернет, локальные сети и съемные носители.

Механизм

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.

Каналы распространения

Дискеты



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.

USB-флеш-накопители

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

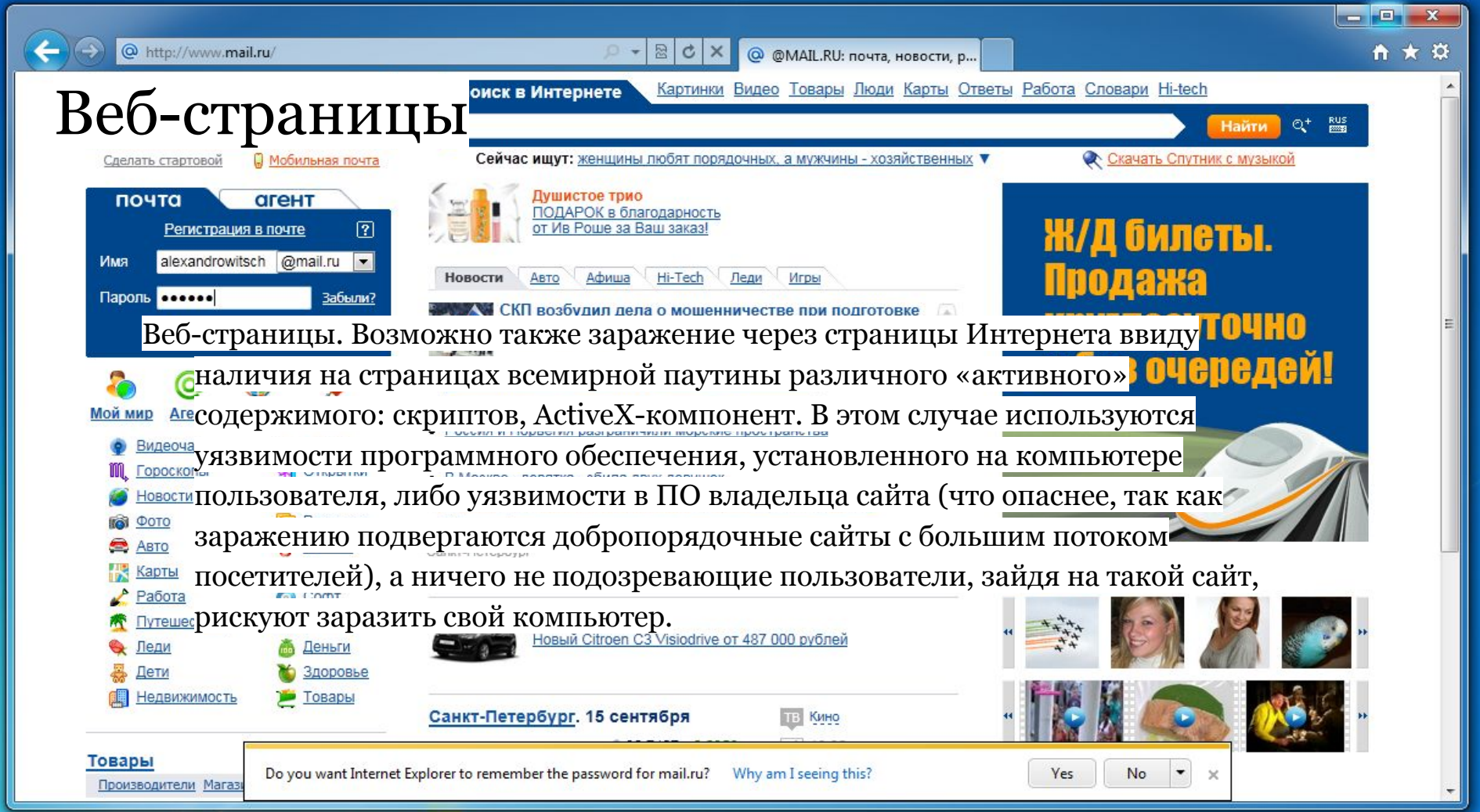
Электронная почта. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то 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

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.

#irc

Веб-страницы



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

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.

Профилактика и лечение

В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

1. Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)
2. Не запускать незнакомые программы из сомнительных источников.
3. Стараться блокировать возможность несанкционированного изменения системных файлов.
4. Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
5. Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
6. Пользоваться только доверенными дистрибутивами.
7. Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
8. Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

Источники

Текст: https://ru.wikipedia.org/

Картинки: google картинки


Спасибо за внимание!