



БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

Интернет – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов.



Самые опасные угрозы сети Интернет

- **Вредоносные программы**
- **Кража информации**
- **Халатность сотрудников**
- **Хакерские атаки**
- **Финансовое мошенничество**
- **Спам**
- **Аппаратные и программные сбои**

Компьютерный вирус — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).



КЛАССИФИКАЦИЯ ВИРУСОВ



ПО ПОРАЖАЕМЫМ ОБЪЕКТАМ

Файловые вирусы. Это вирусы-паразиты, которые при распространении своих копий обязательно изменяют содержимое исполняемых файлов, при этом файлы, атакованные вирусом, в большинстве случаев полностью или частично теряют работоспособность)

Загрузочные вирусы. Это компьютерные вирусы, записывающиеся в первый сектор гибкого или жесткого диска и выполняющиеся при загрузке компьютера.

Скриптовые вирусы. Требуют наличия одного из скриптовых языков (Javascript, VBScript) для самостоятельного проникновения в неинфицированные скрипты.

Макровирусы. Это разновидность компьютерных вирусов разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office.

Вирусы, поражающие исходный код. Вирусы данного типа поражают или исходный код программы, либо её компоненты (OBJ-, LIB-, DCU- файлы) а так же VCL и ActiveX компоненты.

ПО ПОРАЖАЕМЫМ ОПЕРАЦИОННЫМ СИСТЕМАМ И ПЛАТФОРМАМ

- DOS
- Microsoft Windows
- Unix
- Linux



ПО ТЕХНОЛОГИЯМ, ИСПОЛЬЗУЕМЫМ ВИРУСОМ

Полиморфные вирусы. Вирус, который при заражении новых файлов и системных областей диска шифрует собственный код.

Стелс-вирусы. Вирус, полностью или частично скрывающий свое присутствие в системе, путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.)

Руткит. Программа или набор программ для скрывания следов присутствия злоумышленника или вредоносной программы в системе.

ПО ЯЗЫКУ, НА КОТОРОМ НАПИСАН ВИРУС

- ассемблер
- высокоуровневый язык программирования
- скриптовый язык
- и др.



По дополнительной вредоносной функциональности

Бэкдоры. Программы, которые устанавливает взломщик на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе

Шпионы. Spyware — программное обеспечение, осуществляющее деятельность по сбору информации о конфигурации компьютера, деятельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя.

Ботнеты. Это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.

Создание и распространение
вредоносных программ (в том числе
вирусов) преследуется в России
согласно Уголовному кодексу РФ
(глава 28, статья 273)



ПРАВОВОЙ ЛИКБЕЗ

Существует Доктрина информационной безопасности РФ, согласно которой в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, детскими порносайтами и обеспечению информационной безопасности в сетях ЭВМ.

Международный День безопасного Интернета

был учрежден по инициативе Европейской комиссии в 2004 году и с тех пор вышел далеко за пределы Европы.

Его отмечают более 70 стран мира, в том числе и Россия. Отмечается ежегодно во второй вторник февраля.



Цель Дня безопасного Интернета:



«...поддержка граждан в безопасном, этичном и эффективном использовании Интернет - технологий»

Unsafe

Insafe – некоммерческая организация – главный координатор Дня безопасного Интернета в мире.

The image features a central graphic of several network cables with RJ45 connectors, some in blue and some in black, arranged in a starburst pattern. The background is a vibrant blue with a subtle pattern of binary code (0s and 1s) and the word "Internet" repeated in a light, semi-transparent font. The entire graphic is framed by a white, curved border that gives the impression of a computer monitor or a presentation slide.

БОРЬБА С СЕТЕВЫМИ УГРОЗАМИ

Установите комплексную систему защиты!

- Ⓜ Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, фаерволл, антиспам – фильтр и еще пару – тройку модулей для полной защиты вашего компьютера.
- Ⓜ Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур, лучше всего настроить программу на автоматическое обновление.



Будьте осторожны с электронной почтой!

- Ⓜ Не стоит передавать какую-либо важную информацию через электронную почту.
- Ⓜ Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения.
- Ⓜ Программы Microsoft Outlookи Windows Mail помогают блокировать потенциально опасные вложения.



Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari, а лучше Яндексом!

- Ⓢ Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera.
- Ⓢ IE до сих пор удерживает первую строчку в рейтинге популярности, но лишь потому, что он встроен в Windows.
- Ⓢ Opera была очень популярна в России из-за ее призрачного удобства и реально большого числа настроек.
- Ⓢ Уровень безопасности сильно хромает как у одного, так и у второго браузера, поэтому лучше им и не пользоваться вовсе.



Обновляйте операционную систему Windows!

- ⊗ Постоянно обновляйте операционную систему Windows.
- ⊗ Корпорация Microsoft периодически выпускает специальные обновления безопасности, которые могут помочь защитить компьютер.
- ⊗ Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки вх



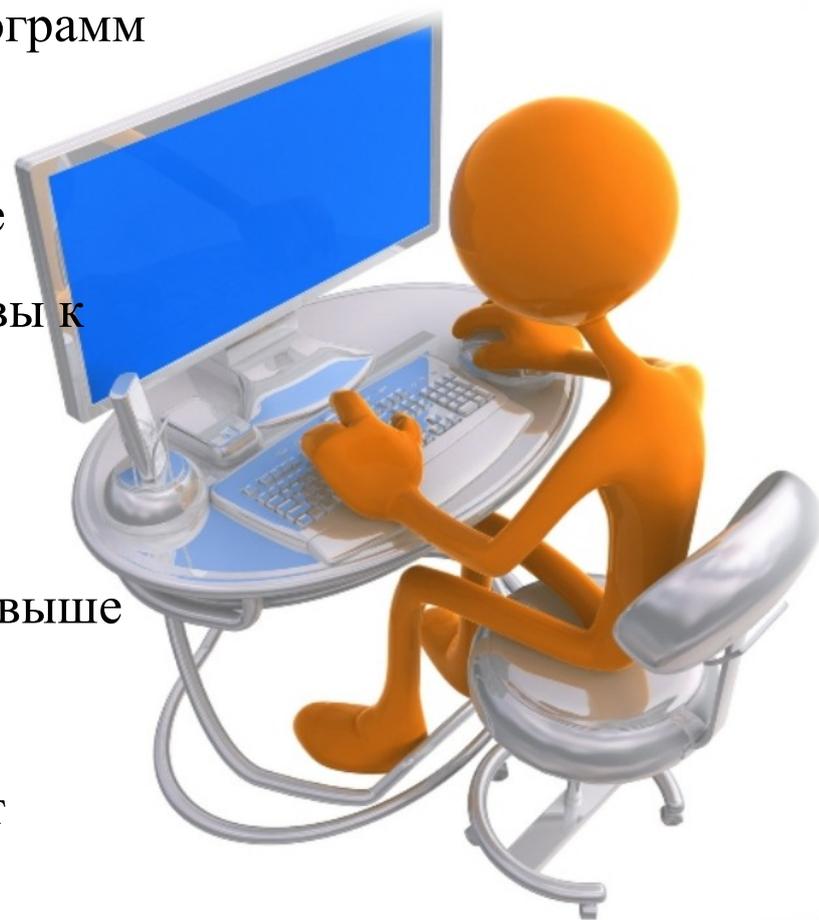
Не отправляйте SMS-сообщения!

- Ⓢ Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.
- Ⓢ При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.
- Ⓢ Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.



Пользуйтесь лицензионным программным обеспечением!

- Ⓜ Если вы скачиваете пиратские версии программ или свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить вирус на свой компьютер.
- Ⓜ Причем, чем программа популярнее, тем выше такая вероятность.
- Ⓜ Лицензионные программы избавят Вас от подобной угрозы!



Используйте брандмауэр!

- Ⓢ Используйте брандмауэр Windows или другой брандмауэр, оповещающий о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру.
- Ⓢ Он также позволяет запретить вирусам, червям и хакерам загружать потенциально опасные программы на компьютер.



Используйте сложные пароли!

- Ⓜ Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам.
- Ⓜ В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — 2-4 часа, но чтобы взломать семисимвольный пароль, потребуется 2-4 года.
- Ⓜ Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.



Делайте резервные копии!

- Ⓜ При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена.
- Ⓜ Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жестком диске.



Функция «Родительский контроль» обезопасит вас!

- Ⓜ Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.
- Ⓜ Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.



САМОСТОЯТЕЛЬНАЯ РАБОТААА

Интерактивный тест:

<https://moretestov.com/other/test-bezopasnost-v-seti-internet>

ДОМАШНЕЕ ЗАДАНИЕ

Интерактивный тест на платформе «Учи.ру» в личном кабинете (задание от учителя)

Рефлексия

Ребята, что наиболее значимое вы сегодня узнали или чему научились на уроке?

Что вам может пригодиться в жизни, какие значимые умения вы приобрели?

Какую бы вы сегодня себе поставили оценку?

СПАСИБО ЗА ВНИМАНИЕ

