Безопасность в Интернете

- Опасности
- Поведение в Интернете
- Выводы

Опасности:

- Вирусы, черви и трояны
- Хакеры и взломщики
- Спам в Интернете
- Дополнительные правила

Назад

Вирусы, черви и трояны

- Вирусы и черви представляют собой опасные программы, которые могут распространяться через электронную почту или веб-страницы. Вирусы могут повредить файлы или программное обеспечение, хранящиеся на компьютере.
- Черви распространяются быстрее вирусов — напрямую с одного компьютера на другой. Например, червь электронной почты может осуществлять самостоятельную рассылку по адресам электронной почты из адресной книги пользователя. Интернет-червями осуществляется поиск компьютеров, которые подключены к Интернету и не содержат последние обновления системы безопасности.

Далее

Вирусы, черви и трояны

- **«Троянские кони» (трояны)** являются опасными программами, которые выглядят безопасными, например, играми, но после активации могут повредить файлы; при этом пользователь не будет об этом знать.
- **Антивирусная программа** - программа, предназначенная для предотвращения доступа к персональному компьютеру для вредоносных программ — она обнаруживает инфицированные файлы и удаляет их.

Назад

Хакеры и взломщики

Человек, взламывающий информационные сети или системы организации, либо использующий их без разрешения. Термин «хакер» имеет два значения — он может также означать опытного компьютерного пользователя.

Они могут вторгнуться на незащищенный компьютер через Интернет и воспользоваться им со злым умыслом, а также украсть или скопировать файлы и использовать их в противозаконной деятельности. Лучшим способом защиты компьютера от вторжения является применение брандмауэра и регулярное обновление операционной системы.

Брандмауэр - программное обеспечение или устройство, предназначенное для контроля над обменом данными между сетями или сетью и отдельной компьютерной системой. Например, брандмауэр позволяет ограничивать трафик на основе предварительно заданных правил, которые разрешают обмен данными только между указанными адресами.

Назад

Спам в Интернете

Нежелательная электронная почта, которая, как правило, рассылается в целях прямого почтового маркетинга. Спам почти всегда единовременно рассылается большому кругу получателей. Он приводит к перегрузке систем электронной почты и может заблокировать почтовые ящики. В качестве средства для рассылки спама его отправители иногда используют червей электронной почты.

Далее

Пять правил относительно электронной почты:

- Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их, выбрав команду в меню сообщений.
- Никогда не отвечайте на спам.
- Применяйте фильтр спама поставщика услуг Интернета или программы работы с электронной почтой (при наличии подключения к Интернету).
- Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.
- Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их.

Назад

Дополнительные правила

- **Закрывайте сомнительные всплывающие окна**
  Всплывающие окна — это небольшие окна с содержимым, побуждающим к переходу по ссылке. При отображении такого окна самым безопасным способом его закрытия является нажатие значка X (обычно располагается в правом верхнем углу). Невозможно знать наверняка, какое действие последует после нажатия кнопки «Нет».
- **Остерегайтесь мошенничества**
  В Интернете легко скрыть свою личность. Рекомендуется проверять личность человека, с которым происходит общение. Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете. При запросе предоставления личной информации на веб-сайте всегда просматривайте разделы «Условия использования» или «Политика защиты конфиденциальной информации», чтобы убедиться в предоставлении оператором веб-сайта сведений о целях использования получаемой информации и ее передаче другим лицам.
- **Обсуждайте использование Интернета**
  Большая часть материалов, доступных в Интернете, является непригодной для несовершеннолетних. Обсудите с детьми, как правильно и безопасно использовать Интернет.

Назад

Поведение в Интернете

- **Законы применяются к Интернету**
- **Авторские права**
- **Информационная безопасность**

Назад

Законы также применяются к Интернету

Несмотря на то, что большая часть законов была создана до широкого распространения Интернета, закон также распространяется и на него. Все, что незаконно в обычной жизни, незаконно и в Интернете.

Интернет предоставляет беспрецедентные возможности свободного общения, но они также подразумевают ответственность. Например, владелец веб-сайта всегда несет ответственность за его содержимое и законность самого сайта и места его публикации.

Назад

Авторское право

- Авторским правом защищается способ реализации идеи, но не сама идея. Разрешается копирование материала из Интернета для личного использования, но присвоение авторства этого материала запрещено. Например, при использовании материала в собственной презентации необходимо указать источник.
- Пересылка неразрешенного материала (например, незаконные копии фильмов или музыкальных файлов, доступных в одноранговых сетях) незаконна.
- Копирование программного обеспечения или баз данных, для которых требуется лицензия, запрещено даже в целях личного использования.
- Неразрешенное использование материала может привести к административному взысканию в судебном порядке, а также иметь прочие правовые последствия.

Назад

Об информационной безопасности

- **Помните**
  После публикации информации в Интернете ее больше невозможно будет контролировать и удалять каждую ее копию.
- **Проверяйте**
  Всегда удостоверяйтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.
- **Думайте**
  Благоразумно ли размещать личную информацию на собственном веб-сайте, если невозможно быть уверенным в целях ее использования?
- **Обращайте внимание**
  Имена учеников, их фотографии и другая личная информация из школьного журнала может публиковаться на веб-сайте школы только с согласия учеников и их родителей.

Назад

Выводы:

Защитите свой компьютер

Регулярно обновляйте операционную систему.

Используйте антивирусную программу.

Применяйте брандмауэр.

Создавайте резервные копии важных файлов.

Будьте осторожны при загрузке новых файлов.

Защитите себя в Интернете

С осторожностью разглашайте личную информацию.

Думайте о том, с кем разговариваете.

Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

Соблюдайте правила

Закону необходимо подчиняться даже в Интернете.

При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

Назад