Информационная безопасность в сети Интернет

Анализируй и критически относись к информационной продукции!

Проблемы информационной безопасности

Основные понятия

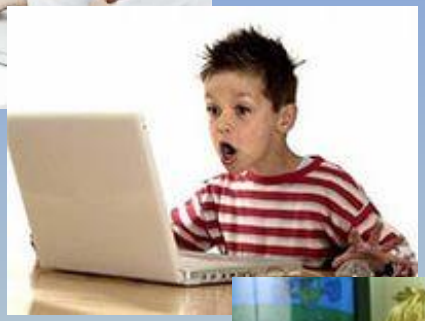
Безопасность – отсутствие угроз, либо состояние защищенности от угроз.

Информация – сведения или сообщения.

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.

Любое из этих средств может быть использовано на благо или во вред личности!

Интернет молодеет!



По последним данным, в России:
средний возраст начала самостоятельной работы в Сети - 10 лет (в 2009 году - 11 лет); и сегодня
наблюдается тенденция к снижению возраста до 7 лет;

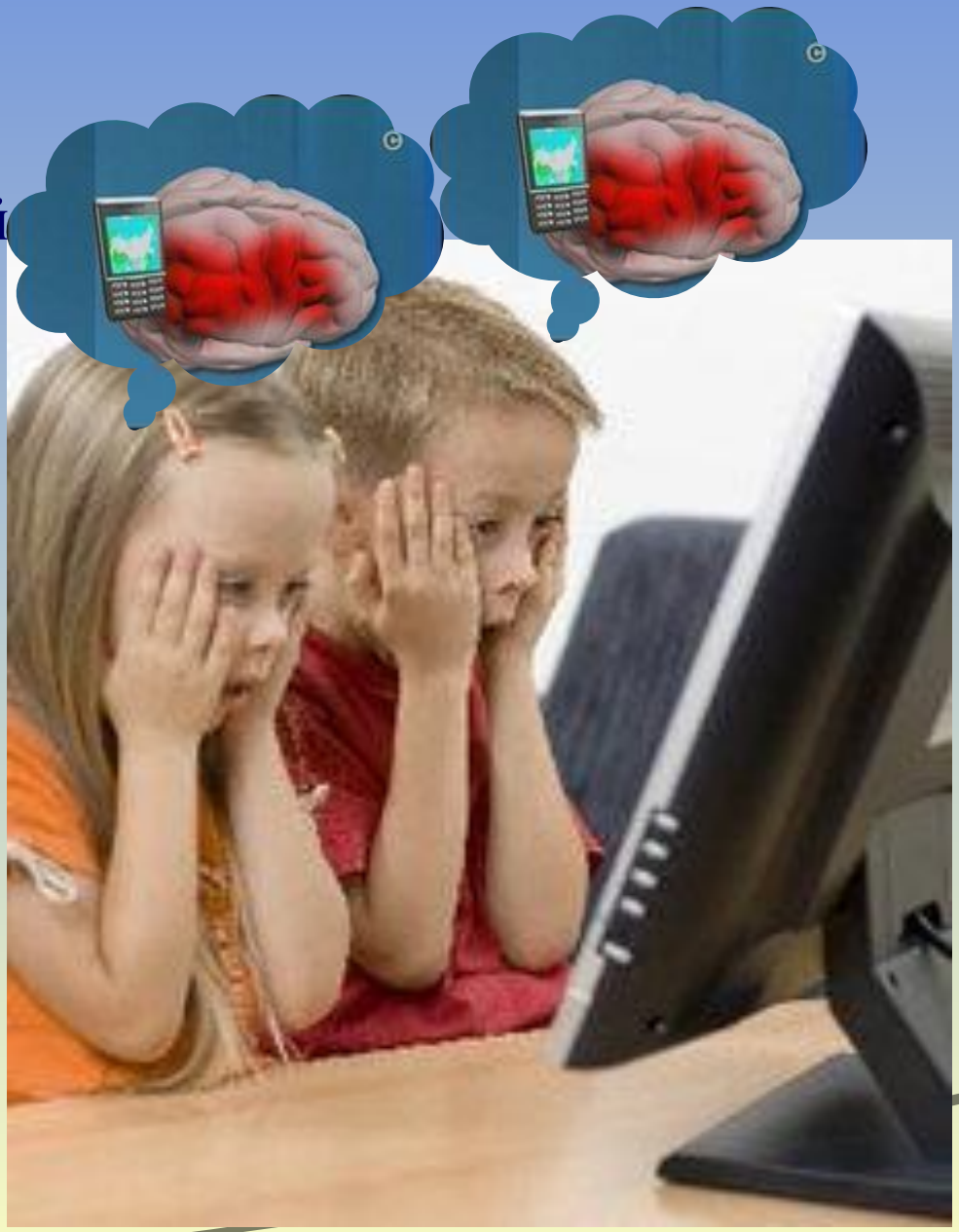
30% несовершеннолетних проводят в Сети более 3 часов в день (при норме 2 часа в неделю!)

Ежедневная детская аудитория Рунета:
46% (13-14 лет),
54% (15-16 лет);

самые "любимые" детьми ресурсы – социальные сети (78%).

Помимо социальных сетей, среди несовершеннолетних популярны следующие виды и формы онлайн-развлечений

- **сетевые игры;**
- **просмотр и скачивание фильмов, клипов, аудиофайлов, программ;**
- **обмен файлами;**



Осторожно! Опасно! Вредно!

- использование электронной почты, сервисов мгновенного обмена сообщениями, чатов;
- ведение блогов и пр.
- 4% детей сталкиваются в Интернете с порнографической продукцией
- 40% получают непосредственные предложения о встречах "в реале".

МОЖЕТ НАМ ВМЕСТЕ СТОИТ ПОДУМАТЬ!

– Почему тема информационной безопасности является важной и почему эти вопросы должны обсуждаться в школе?

– Из возможных причин, какие можно выделите аспекты, связанные с сущностью Интернета и его значимостью как средства общения?

Интернет является общественным ресурсом.

В Интернете необходимо следовать основным правилам так же, как правилам дорожного движения при вождении.

Помните!

После публикации информации в Интернете ее больше невозможно будет контролировать и удалять каждую ее копию.

1

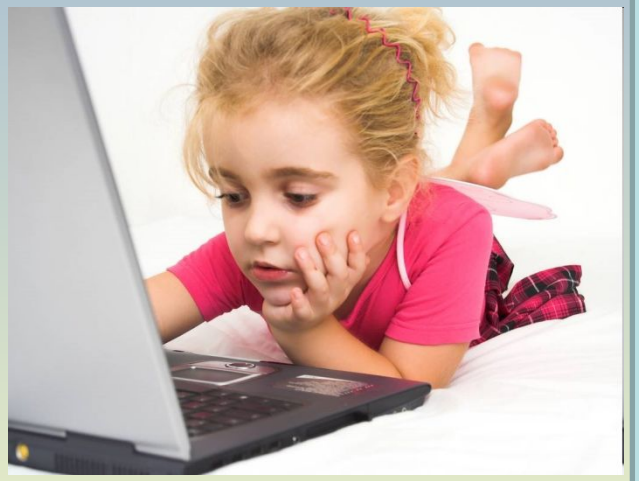
Защитите свой компьютер

- **Регулярно обновляйте операционную систему.**
- **Используйте антивирусную программу.**
- **Создавайте резервные копии важных файлов.**
- **Будьте осторожны при загрузке содержимого.**

Помните!
В Интернете не вся информация надежна и не все пользователи откровенны.

2

Защитите себя в Интернете



- **Думайте о том, с кем разговариваете.**

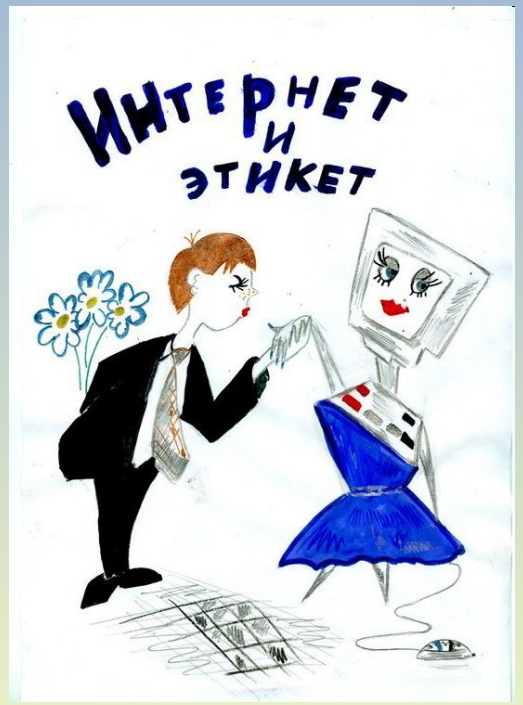
Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете. При запросе предоставления личной информации на веб-сайте всегда просматривайте разделы «Условия использования» или «Политика защиты конфиденциальной информации», чтобы убедиться в предоставлении оператором веб-сайта сведений о целях использования получаемой информации и ее передаче другим лицам.

Всегда удостоверяйтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.

Помните!
Неразрешенное использование материала может привести к административному взысканию в судебном порядке, а также иметь прочие правовые последствия.

3

Думай о других пользователях



- **Закону необходимо подчиняться даже в Интернете.**
- **При работе в Интернете будь вежлив с другими пользователями Сети.**

- **Имена друзей, знакомых, их фотографии и другая личная информация не может публиковаться на веб-сайте без их согласия или согласия их родителей.**

- **Разрешается копирование материала из Интернета для личного использования, но присвоение авторства этого материала запрещено.**
- **Передача и использование незаконных материалов (например, пиратские копии фильмов или музыкальных произведений, программное обеспечение с надорванными защитными кодами и т.д.) является противозаконным.**
- **Копирование программного обеспечения или баз данных, для которых требуется лицензия, запрещено даже в целях личного использования.**

Помните!

Большая часть материалов, доступных в Интернете, является непригодной для несовершеннолетних.

Будьте бдительны и осторожны!

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 (например, в дискуссионных группах).

Борьба с сетевыми угрозами

Установите комплексную систему защиты!

- Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, 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 Outlooku Windows Mail помогают блокировать потенциально опасные вложения.

Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari!

- 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 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.

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.

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 входа.

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.

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!

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.

ОПИСАНИЕ РАБОТЫ

Данная презентация является демонстрационным материалом для проведения внеклассных мероприятий по проблемам информационной безопасности.
Презентация выполнена в программе MSPowerPoint
Объем презентации – 14 слайдов.

Используемая литература и Интернет-ресурсы:

"Основы безопасности детей и молодежи в Интернете" — интерактивный курс по Интернет-безопасности.
Портал Сети творческих учителей. http://www.it-n.ru/communities.aspx?cat_no=71586&tmpl=com
Вопросы обеспечения информационной безопасности от компании Microsoft
http://www.microsoft.com/rus/protect/default.mspx#
Вопросы безопасности - сайт от компании Semantec
http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs_teach_kids
Ребенок в сети. Сайт от компании Panda http://www.detionline.ru/
Специальный портал созданный по вопросам безопасного использования сети Интернет.
Безопасный Интернет http://www.saferinternet.ru/.
sevastopolcc.wordpress.com
www.unmultimedia.org