БЕЗОПАСНЫЙ 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!

СПРАВОЧНАЯ ИНФОРМАЦИЯ

По последним данным, в России:

Средний возраст начала самостоятельной работы в Сети для России сейчас составляет 10 лет. Примерно 30% российских детей, пользующихся Интернетом, проводят в Сети ежедневно более трех часов в день.

Одним из наиболее любимых способов знакомства с информацией и ее публикации в Сети для детей являются социальные сети, ярким примером которых является «ВКонтакте».

СПРАВОЧНАЯ ИНФОРМАЦИЯ

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

самые "любимые" детьми ресурсы –
социальные сети (78%);
в них проводится до 60 минут в день.

ВКонтакте

одноклассники.ru

СПРАВОЧНАЯ ИНФОРМАЦИЯ

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

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

СПРАВОЧНАЯ ИНФОРМАЦИЯ

- *использование электронной почты, сервисов мгновенного обмена сообщениями, чатов;*

- *ведение блогов и пр.*

- *40% получают непосредственные предложения о встречах "в реале".*

Безопасность сети

Использование Интернета является безопасным, если выполняются

ТРИ ОСНОВНЫЕ ПРАВИЛА

1

Защитите свой компьютер

- **Применяйте брандмауэр.**

Брандмауэр представляет собой программный или аппаратный комплекс, который проверяет данные, входящие через Интернет или сеть, и в зависимости от параметров брандмауэра блокирует или разрешает их передачу на компьютер. Брандмауэр поможет предотвратить проникновение хакеров или вредоносного программного обеспечения (такого как черви) в ваш компьютер через сеть или Интернет. Брандмауэр также помогает предотвратить отправку вредоносных программ на другие компьютеры.

Следующая иллюстрация показывает работу брандмауэра. Как кирпичная стена создает физическую преграду, брандмауэр создает препятствие между Интернетом и компьютером.

Защитите свой компьютер

2. *Не открывайте файлы, полученные от неизвестных корреспондентов*

Электронная почта и мгновенные сообщения позволяют быстро обменяться информацией с друзьями, родственниками и одноклассниками. Но если не проявить необходимой осторожности, электронная почта и мгновенные сообщения могут распространить вирусы и черви. Основная масса вредоносных программ попадает в компьютер через электронную почту теми, кто нечаянно попытался открыть зараженный файл. Не дайте себя одурачить! Ни в коем случае нельзя открывать файл, вложенный в письмо электронной почты или мгновенное сообщение, если его отправитель неизвестен и вы не ожидаете получения файла.

Защитите свой компьютер

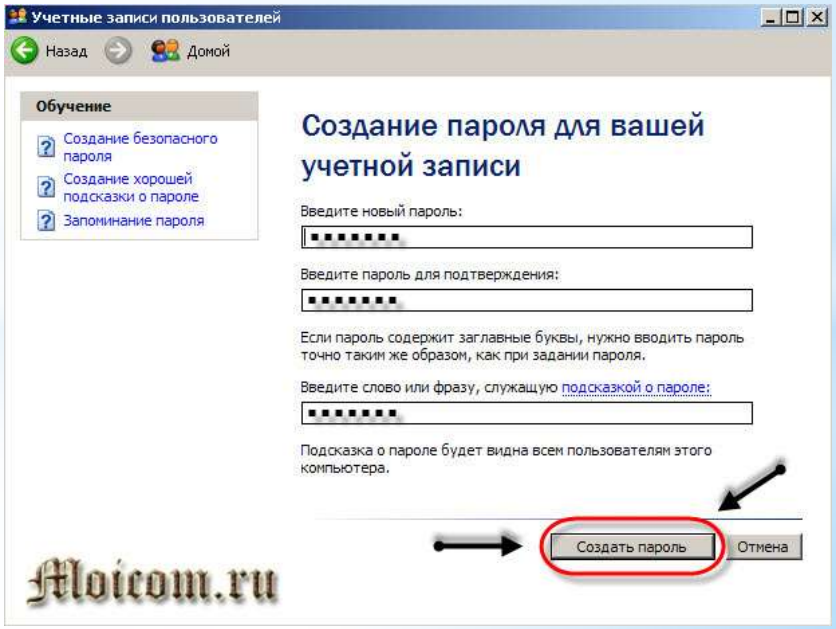
3.*Программы-шпионы.*

Ваш браузер погряз во всплывающих окнах? На экране компьютера появились панели, которые вы не загружали? Возможно, вы стали жертвой программы-шпиона. Она занимается сбором вашей личной информации, не предупреждая об этом и не спрашивая на то разрешения. Получить эту вредоносную программу можно при скачивании музыки или программ обмена файлами; загрузки бесплатных игр с подозрительных сайтов или других программ.

Защитите свой компьютер

4.Пароль защищает ваш компьютер и блокирует возможность его использования.

Пароли являются первой линией защиты от злоумышленников, шутников или беспечного соседа по комнате. Если вы не пользуетесь паролем для входа в компьютер, кто угодно может получить доступ.



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

Помните!

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

ТРИ ОСНОВНЫЕ ПРАВИЛА

2

Защитите себя в Интернете

- *Думайте о том, с кем разговариваете.*

При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.

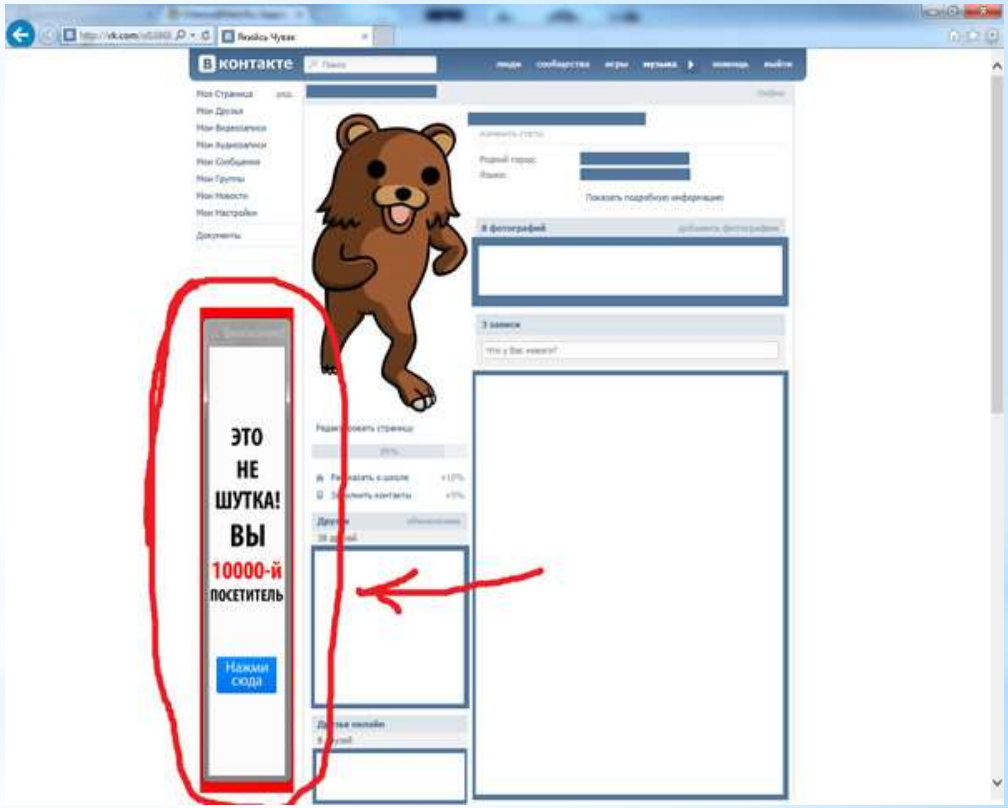
- *Всегда удостоверяйтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.*

Защитите себя в Интернете

- ***Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.***

Защитите себя в Интернете

- ✓ ***Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него.***
  В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.



Защитите себя в Интернете

- ✓ ***Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.***

Защитите себя в Интернете

- ***Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом.***

- ***Если вас кто-то расстроил или обидел, расскажите все взрослому.***

Помните!

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

ТРИ ОСНОВНЫЕ ПРАВИЛА

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.*

Думай о других пользователях

- ✓ *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!

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

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 (например, в дискуссионных группах).

Помните!

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

Интернет является общественным ресурсом.

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