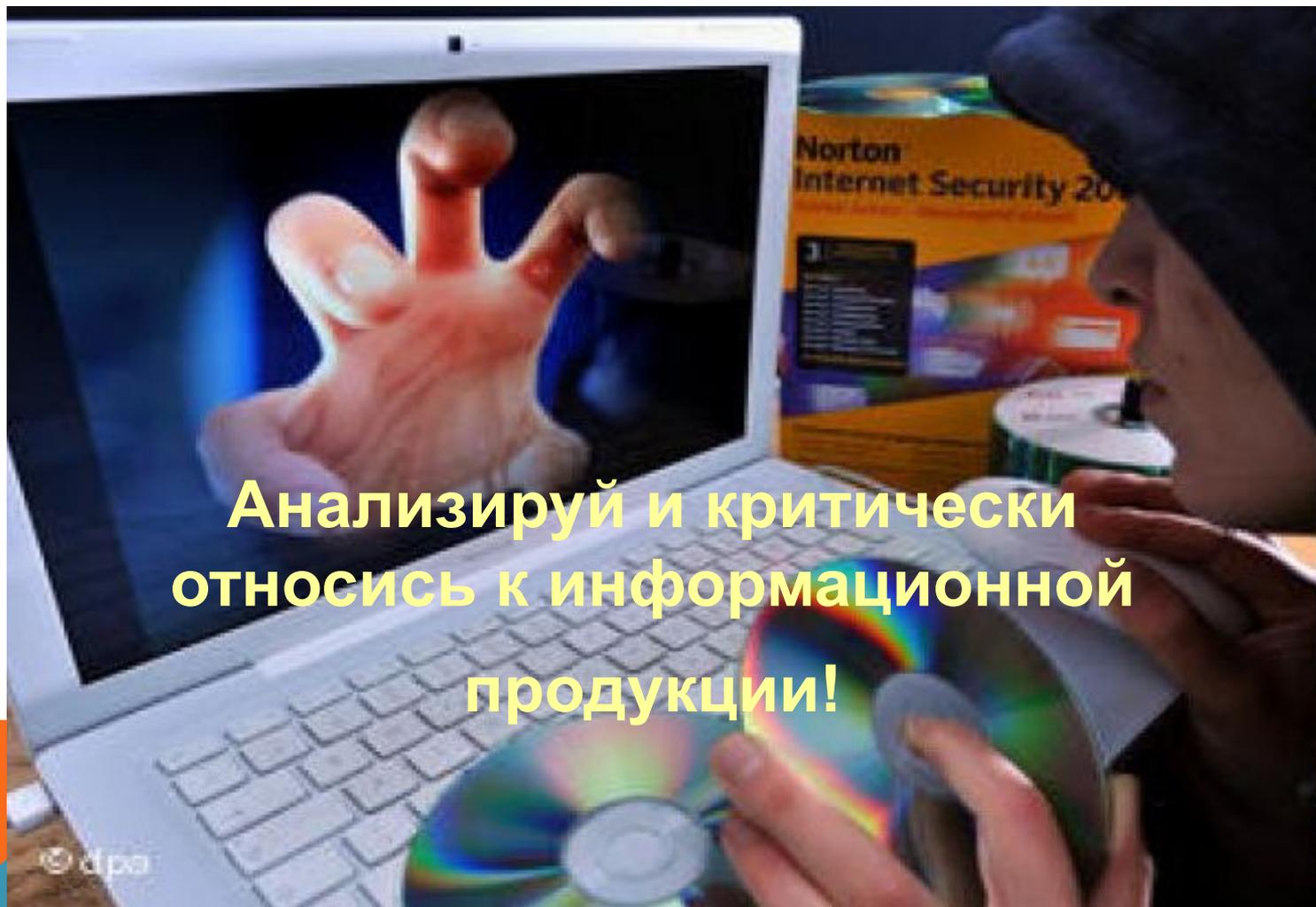


Информационная безопасность в сети Интернет



**Анализируй и критически
относись к информационной
продукции!**

**Средства
массовой
коммуникации, в т.ч.
Интернет**

Образование

**ИСТОЧНИКИ
ИНФОРМАЦИИ**

Литература

Искусство

Личное общение

**Система
социально-
воспитательной
работы**

**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 -
10 лет (в 2009 году - 11 лет); и
сегодня
наблюдается тенденция к
снижению возраста до 9 лет;**

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

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.



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;**



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.



СПРАВОЧНАЯ ИНФОРМАЦИЯ



- 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".

ДАВАЙТЕ ВМЕСТЕ ПОДУМАЕМ!



- Почему тема информационной безопасности является важной и почему эти вопросы должны обсуждаться в школе?
- Из возможных причин, какие можно выделить аспекты, связанные с сущностью Интернета и его значимостью как средства общения?

Использование Интернета является безопасным,
если выполняются

ТРИ ОСНОВНЫЕ ПРАВИЛА

Защитите свой компьютер

1

- Регулярно обновляйте операционную систему.
- Используйте антивирусную программу.
- Применяйте брандмауэр.
- 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.



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

Помните!

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

ТРИ ОСНОВНЫЕ ПРАВИЛА

Думай о других пользователях

3

- **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!

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.

ОПИСАНИЕ РАБОТЫ

Используемая литература и Интернет-ресурсы:

В.В. Гафнер Информационная безопасность: учебное пособие: ГОУ ВПО «Уральский государственный педагогический университет», Екатеринбург, 2009, ч. 1,2.

"Основы безопасности детей и молодежи в Интернете" — интерактивный курс по

Интернет-"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.aspx#>

Вопросы безопасности - сайт от компании Symantec

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

21region.org