# Профилактика основных интернет-рисков и борьба с ними

*Разработал учитель информатики*
*МКОУ ВСОШ № 3*
*МО Усть-Лабинский район*
Мирошниченко Алексей Борисович

# *Интернет-риски*

1.Контентные риски

2. Коммуникационные риски

3. Электронные риски

4. Потребительские риски

# *Контентные риски*

Контентные риски — это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

# Предупреждение контентных рисков

1. *Использование специальных технических средств,чтобы ограничивать доступ ребенка к негативной информации .*
2. *Создания для каждого члена семьи своей учетной записи на компьютере с надёжными паролями.*
3. *Следить за активностью детей в сети Интернет. Просматривать историю посещения сайтов.*
4. *Объяснить детям, что далеко не все, что они могут прочесть или увидеть в интернете – правда. Необходимо проверять информацию, увиденную в интернете.*

# Предупреждение контентных рисков

5. *Поддерживать доверительные отношения с детьми, чтобы всегда быть в курсе с какой информацией они сталкиваются в сети.*
6. *Важно помнить, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую могут выступать более эффективными средствами для обеспечения безопасности детей, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.*

# *Коммуникационные риски*

*Коммуникационные риски непосредственно связаны с общением пользователей в сети Интернет. Это понятие включает в себя "незаконный контакт" и "киберпреследование". Незаконный контакт - это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка. Киберпреследование – это преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями; запугивание; подражание; хулиганство (интернет-троллинг); социальное бойкотирование.*

# *Коммуникационные риски*

- *Незаконный контакт* — это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка
- *Домогательство* — причиняющее неудобство или вред поведение, нарушающее неприкосновенность частной жизни лица.
- *Груминг* — установление дружеских отношений с ребенком с целью изнасилования.
- *Киберпреследование* (или кибер-буллинг) — это преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов.

# Предупреждение груминга

- Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются;
- Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии;
- Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу;
- Не позволяйте вашему ребенку встречаться с онлайн-знакомыми без вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу;
- Интересуйтесь тем, куда и с кем ходит ваш ребенок.

# Основные правила поведения в Сети Интернет

- Нельзя делиться с виртуальными знакомыми персональной информацией, а встречаться с ними в реальной жизни следует только под наблюдением родителей.
- Если интернет-общение становится негативным – такое общение следует прервать и не возобновлять.

# Предупреждение кибербуллинга:

- Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости так же неприятно, как и слышать;
- Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Возможно, стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем;
- Если ребенок стал жертвой буллинга, помогите ему найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички;
- Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;
- Старайтесь следить за тем, что ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

# Как защититься от кибербуллинга:

- Не провоцировать. Общаться в Интернете следует этично и корректно. Если кто-то начинает оскорблять ребенка в Интернете – необходимо порекомендовать уйти с такого ресурса и поискать более удобную площадку.
- Если по электронной почте или другим э-каналам кто-то направляет ребенку угрозы и оскорбления – лучше всего сменить электронные контакты (завести новый email, Skype, ICQ, новый номер мобильного телефона).
- Если кто-то выложил в Интернете сцену киберунижения ребенка, необходимо сообщить об этом администрации ресурса. Можно также обратиться на горячую линию. Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и тем более не всегда знают, как ее предотвратить.

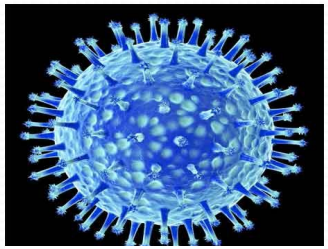
# *Электронные риски*

- Электронные (кибер-) риски — это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д

# *Вредоносные программы*

различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, и др.), которое может нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с интернетом и даже использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

# К вредоносным программам относятся



Вирусы

Черви

Троянские кони

**Шпионские программы**

# Вирусы

вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.

# *Черви*

разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети.

## *Трояна́ская программа (также — трояна́, трояна́нец, трояна́нский конь)*

вредоносная программа, распространяемая людьми, в отличие от вирусов и червей, которые распространяются самопроизвольно.

# Шпионские программы

(альтернативные названия - Spy, SpyWare, Spy-Ware, Spy Trojan) принято называть программное обеспечение, собирающее и передающее кому-либо информацию о пользователе без его согласия. Информация о пользователе может включать его персональные данные, конфигурацию его компьютера и операционной системы, статистику работы в сети Интернет.

# Борьба с вредоносными программами

Для того чтобы успешно противостоять попыткам вирусов проникнуть на ваш компьютер необходимо выполнять два простейших условия: соблюдать правила «компьютерной гигиены» и пользоваться антивирусными программами, поскольку для защиты компьютеров от компьютерных вирусов, как и для защиты живых существ от болезней, используются средства профилактики, позволяющие не допустить попадания вредоносной программы в систему, а также программные средства диагностики и лечения

# Правила «компьютерной гигиены»

- Ни в коем случае не открывайте файлы, присылаемые вам по электронной почте неизвестными людьми;
- Осторожно относитесь к файлам, присылаемым вашими знакомыми и партнерами. Они могут даже и не знать, что с их компьютера вирус незаметно рассылает свои копии людям из их адресной книги;
- Обязательно проверяйте антивирусным сканером с максимальным уровнем проверки все дискеты, компакт-диски и другие мобильные носители информации, а также файлы, получаемые из сети Интернет, и других публичных ресурсов (BBS, электронных конференций и т.д.);
- Проводите полную антивирусную проверку компьютера после его получения из ремонтных служб. Работники этих служб пользуются одними и теми же дискетами для проверки всех компьютеров – они очень легко могут занести компьютерный вирус с другой машины;
- Своевременно устанавливаете «заплатки» от производителей используемых вами операционных систем и программ;
- Для повышения сохранности ваших данных периодически проводите резервную архивацию информации на независимые носители.

# *Виды популярных антивирусных программ*

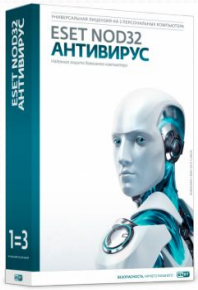
**ПОЛИФАГИ**

**РЕВИЗОРЫ ИЗМЕНЕНИЙ**

**ПОВЕДЕНЧЕСКИЕ БЛОКИРАТОРЫ**

# Лучшие лицензионные антивирусные программы

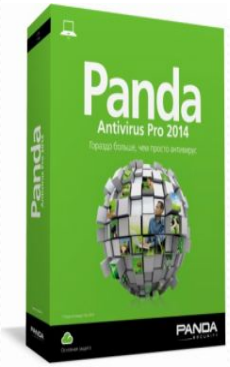

Антивирус Касперского




ESET NOD32 Антивирус


Антивирус Dr.Web для Windows


Avira Antivirus Pro




Panda Antivirus Pro

# *Потребительские риски*

Потребительские риски – злоупотребление в интернете правами потребителя. Включают в себя: риск приобретения товара низкого качества, различные поделки, контрафактная и фальсифицированная продукция, потеря денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибер мошенничества, и др.

# Предупреждение кибермошенничества

- Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;
- Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных;
- Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности:
- Ознакомьтесь с отзывами покупателей
- Проверьте реквизиты и название юридического лица – владельца магазина
- Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs)
- Поинтересуйтесь, выдает ли магазин кассовый чек
- Сравните цены в разных интернет-магазинах.
- Позвоните в справочную магазина
- Обратите внимание на правила интернет-магазина
- Выясните, сколько точно вам придется заплатить
- Объясните ребенку, что нельзя отправлять слишком много информации о себе при совершении интернет-покупок: данные счетов, пароли, домашние адреса и номера телефонов. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.

# Вопросы к классному часу

***1.Какие Интернет-риски вы знаете?***

(Контентные, коммуникационные, электронные, потребительские)

***2. Какие программы называют вредоносными?***

(различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, и др.), которое может нанести вред компьютеру и хранящимся на нем данным. )

***3. Назовите виды популярных антивирусных программ?***

(полифаги, ревизоры изменений, поведенческие блокираторы)

# список использованных ресурсов


- http://www.netpolice.ru/safetips/comm/
- http://pravo.aodb-blag.ru/territoriya_bezopasnosti/kontent_riski/
- http://detionline.com/helpline/risks
- ru.wikipedia.org
- http://z-oleg.com/secur/articles/spyware.php
- http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=639
- http://private-edu.narod.ru/book/borba.html
- http://antivirus-navigator.com/
- http://szkti.ru/polezno/internet-riski