**Безопасное использование возможностей электронного обучения в общеобразовательных организациях**

Проект «Безопасное использование возможностей электронного обучения в общеобразовательных организациях посвящён формированию культуры безопасного использования компьютерного оборудования и ресурсов сети Интернет обучающимися общеобразовательных организаций. Основа содержания проекта опирается на положение о Научно-образовательном центре ИПИ РАН – АО ИОО «Безопасное использование возможностей электронного обучения» от 26 июня 2013 года.

При этом :

первое направление – проведение работы с обучающимися, направленной на формирование культуры безопасного использования компьютерного оборудования и ресурсов сети Интернет в рамках классных часов и различных внеклассных мероприятий;   
второе – проведение просветительской работы с родителями по указанной проблематике;   
третье направление – обмен опытом по проблеме проекта через выступления на видеоконференциях, семинарах, публикацию статей в журналах и сборниках конференций.

**Классный час   
Играем в кибердетективов**

Занятие проводится в форме беседы-викторины.

**Идея проведения:** учитель задает вопросы и фиксирует ответы на доске, дети получают жетоны за ответы.

**Сравнение незнакомцев в реальной жизни и онлайн**

1. Подготовить 2-3 фотографии взрослых людей – мужчин и женщин, находящихся на улице Можно взять изображение киногероя – например, Гарри Поттера.

Продемонстрировать фотографий детям. Задать вопросы к каждой фотографии:

* Расскажите, что это за человек? На что Вы обратили внимание? Сколько ему(ей) лет? Где он? Во что он одет? Чем он занимается?
* А киногерой (Г.Поттер) - он настоящий? Его можно встретить на улице? Нет? А кого можно? Правильно, артиста, который играл роль.
* Кто-нибудь из вас подойдет к нему на улице и расскажет ему свое имя и фамилию, расскажет, где он живет, где учится? Нет? Почему? (Потому что он – незнакомец)
* А к другому человеку, не артисту станете подходить и все о себе рассказывать? Тоже нет? (Правильно. В Интернете так же как и на улице, полно незнакомых людей, но почему-то в этом случае нет такого же ощущения, как на улице).
* А может ли вы получить письмо по электронной почте от Гарри Поттера? Что это может означать? Что Гарри Поттер написал это письмо? Или кто-то взял себе этот псевдоним? А чем отличается незнакомец в сети? (Он может взять любой псевдоним и может быть любого возраста.

Показать детям фотографии тех же людей, которых обсуждали как незнакомцев на улице:

* Может ли любой из них быть твоим новым сетевым знакомым? Может.

(Он назвал какое-то имя как свое, может назвать и фамилию. Может показать фотографию. Но и имя, и фамилия, и фотография могут оказаться ненастоящими, как, например, Гарри Поттер).

* Как проверить, говорит ли он правду? Какие будут предложения? Например: Можно спросить в какой школе учится, узнать как зовут учителей. Можно эти данные проверить на сайте той школы, какая будет названа. Но, если ты смог зайти на сайт, чтобы проверить, так же мог зайти и твой сетевой «новый знакомый» и взять данные оттуда. Какие гарантии, что этот человек не имеет плохих намерений? Гарантий нет.
* А если твой новый сетевой «знакомый» предложит встретиться где-нибудь лично? Как правильно поступить? Сразу согласиться и идти? Обсудить с родителями? (Обязательно обсудить с родителями).
* Можно ли идти на встречу одному? (Обязательно нужно, чтобы тебя сопровождал взрослый, может, не держал за руку, но находился поблизости. Ведь мы обсудили, что люди в Интернете могут выдавать себя за других).

**Вывод:**

В Интернете, так же как и на улице, в окружении незнакомых людей, надо соблюдать осторожность. Нельзя давать никому в сети своего настоящего имени и фамилии, нельзя давать никакой личной информации.

* Как вы думаете, что относится к личной информации? (Имя, фамилия, имена и фамилия членов твоей семьи, адрес, номер телефона, пароль).

**Правило:** В Интернет необходимо свое имя и фотографию заменять псевдонимом и аватаром.

* Кто знает, что такое аватар? (Это графическое представление пользователя. Аватар может быть одно или- двухмерным изображением в веб-форумах, чатах, порталах, блогах, социальных сетях. Об этом поговорим дальше).

Тем ребятам, кто активнее всех предлагал версии ответов и участвовал в обсуждении, в конце урока присвоить звание Кибердетектив и вручить медали (5-10 медалей).

© ИПИ ФИЦ ИУ РАН

© АО ИОО

**Родительское собрание**

**Как распознать обман?**

Дети находят способы противостоять родительскому контролю их занятий в Интернете

Продолжавшиеся долгое время среди психологов и педагогов дискуссии «Социальные сети – это хорошо или плохо?» завершает сама жизнь. Независимо от мнений специалистов, социальное общение – это данность нынешнего времени, так же, как автомобили, электричество, телевидение. И нужно просто учиться жить в этой данности и грамотно себя вести. На предыдущих собраниях говорилось о том, что необходимы доверительные отношения с ребенком. Но при этом ребенка надо контролировать, а для этого родителям необходимо знать, на какие ухищрения идут дети, как они вводят в заблуждение своих родителей. Задача этого материала – информирование родителей.

Как показывают результаты исследований, дети проводят в Интернете как минимум на два часа дольше, чем считают их родители.

А чтобы минимизировать родительский контроль их занятий в Интернете они:

1.Чистят историю браузера;

2. Удаляют или прячут переписку в Аське или цепочки в смс;

3. Используют компьютер, который родители не используют и не смогут проверить;

4. Используют мобильные устройства с выходом в Интернет;

5. Настройками ограничивают доступ только для друзей;

6. Регистрируются в сети под вымышленным именем;

7. Заводят новый почтовый адрес не известный родителям;

8. Закрывают браузер, когда родители входят в комнату;

9. Изменяют детали или лгут по поводу своих онлайн занятий.

Что можно посоветовать родителям?

Для многих родителей Интернет нередко представляется списком сайтов, относительно которых надо быть в курсе: Facebook, Twitter, Вконтакте, Мой мир и т.д., в то время, как практически каждый месяц появляются новые, о которых родители даже не подозревают, содержащие реальные специфические риски. Как показывают результаты исследований, в настоящее время, если родители и беседуют с ребенком, то это, как правило, происходит с детьми младшего возраста. При этом подростки остаются несколько в стороне. Это не означает, что они более защищены, просто, родителям следует поменять характер бесед с детьми старшего возраста, перенося фокус со стоимости бренда, пользовательских тарифов у разных операторов на виды занятий в интернете. При этом нельзя не признать, что отследить занятия ребенка становится все сложнее. Пребывание в одной комнате с ребенком не равносильно знанию того, чем он в этот момент занимается. Каждый месяц появляются новые приложения или сайты. В то время, как попытки отслеживать все появляющиеся новинки, равносильны тяжелой неравной борьбе, можно использовать другой подход. Он заключается в изучении общих принципов, способов использования детьми социальных медиа, смс-сообщений, фотографий, а не в привязке к какому-то конкретному сайту или приложению.

1. Проверяйте фото и видео ваших детей. Просматривайте их персональные странички, телефоны на предмет удаленных файлов и текущего содержимого. Родители регистрируются в той же сети, что и ребенок, просят включить их в друзья и таким образом быть в курсе того, с кем ребенок общается. Если же ребенок не проявляет доброй воли, родителям имеет смысл проявить изобретательность и использовать возможность стать фоловером ребенка. Поиск в Интернете поможет выбрать дополнительные инструкции по восстановлению удаленных фотографий или видео практически для всех моделей телефонов.

2. Просматривайте текстовые сообщения, которые отправляет и получает ваш ребенок. Проверьте время, когда сообщения были отправлены. Многие дети продолжают общение гораздо дольше того времени, когда родители думают, что они уже спят. Многие провайдеры предлагают программы родительского контроля, позволяющие контролировать и ограничивать время суток, в течение которого разрешен доступ.

3. Проверьте правильность всех настроек, чтобы личные данные случайно не стали доступными для посторонних. Проверяйте эту информацию регулярно до тех пор, пока ваш ребенок пользуется этим приложением. То, что нормальным образом используется сегодня, возможно, не будет тем же образом использоваться и завтра.

4. Контролируйте историю поисков вашего ребенка, причем, проверяйте не только телефон, компьютер, но и планшет, читалку, игровую приставку - все устройства, имеющие выход в Интернет. Не принимайте обещания вашего ребенка, что он не будет использовать устройства ненадлежащим образом, т.к. подобная доверчивость в действиях может иметь далеко идущие последствия. Если вы не хотите проверять историю на каждом устройстве, то отключите на части из них функции позволяющие получить доступ к внешнему миру. Если вы не знаете, как проверить историю, или подозреваете, что она может быть удалена, следует рассмотреть вопрос об установке программного обеспечения для мониторинга. Помните, что игровые сайты, социальные сети и даже программы совместной подготовки документов могут быть использованы для приватного общения с другими пользователями. Оценивайте как то, что ребенок размещает, так и контент, размещаемый другими. Вам лучше знать, что является приемлемым для вашего ребенка.

Будьте бдительны.

© ИПИ ФИЦ ИУ РАН

© АО ИОО