Родительское собрание

Тема: «Безопасность детей в сети Интернет»

Целевая аудитория: родители обучающихся.

Цель: повышение осведомленности и информированности родителей о безопасности детей в Интернете и о возможности использования его ресурсов.

Вид собрания: тематическое

Форма собрания: беседа

Оборудование: ноутбук, проектор, экран, мультимедийная презентация «Безопасность детей в сети Интернет», памятка для школьников, учителей, родителей «Как защититься от интернет-угроз» (Национальный узел Интернет-безопасности в России), брошюра «Безопасность детей в сети Интернет» (издательство корпорации Майкрософт), бланки для подведения итогов «Плюс-минус-интересно».

Ход собрания

(собрание сопровождается показом презентации «Безопасность детей в сети Интернет»)

1. **Организационный момент.**

Родители проходят, рассаживаются на места. Определяется готовность родителей к работе. Озвучивается тема собрания: «Безопасность детей в сети Интернет».

1. **Целеполагание и мотивация к деятельности.**

Родителям предлагается 3 вопроса для обсуждения. Каждый высказывает свое мнение по каждому вопросу.

Вопросы для обсуждения.

- Чем является компьютер в вашей семье? Приведите примеры ситуаций из вашей жизни, связанных с положительными и отрицательными эмоциями по поводу использования компьютера.

- Какую пользу извлекает Ваш ребенок при использовании сети Интернет?

- Знаете ли Вы, какие опасности ждут Вашего ребенка в сети Интернет?

3. Постановка проблемы.

Сегодня все больше компьютеров подключаются к Интернету. И с каждым годом аудитория Сети молодеет. Интернет предоставляет детям и молодежи невероятные возможности для совершения открытий, общения и творчества.

Прекрасное место для обучения, для общения с друзьями, для отдыха, для заведения новых знакомств.

Через Интернет дети и подростки открывают для себя мир, формируют собственную личность. Но, как и реальный мир, Сеть не безопасна, в виртуальном мире мы можем встретить все те же проблемы, что и в реальном.

И главная задача взрослых – обеспечение безопасности работы ребенка с мировой паутиной. Следует понимать, что, подключаясь к Интернету, ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Проблема защиты детей в Сети находит самый широкий резонанс, и это не случайно.

1. **Основной этап собрания, раскрытие темы.**

Давайте сначала разберемся, а какие угрозы могут ожидать наших детей в сети Интернет.

I. Основные угрозы для детей в сети Интернет

1. Системы мгновенного обмена сообщениями

Системы обмена мгновенными сообщениями (например, MSN Messenger, Yahoo! Messsenger, Google Talk, ICQ…) стали широко используемым каналом общения для молодых людей. Это не могло остаться незамеченным со стороны кибер-преступников, которые быстро сделали его основным каналом для своей деятельности.

Одна из самых опасных угроз заключается в том, что преступники, используя данные программы, обманывают детей и подростков и представляются им другим человеком, чем они есть на самом деле.

В этих программах пользователи авторизуются с использованием адреса электронной почты и пароля. Например, если кто-то узнает данные другого пользователя и подключится к программе от его лица, то остальные люди, с которыми этот пользователь общается, будут думать, что они общаются именно с данным пользователем, хотя это не так. Если Вы обмениваетесь информацией или файлами с этим псевдо-пользователем, то преступник сможет легко ими завладеть. Именно по этой причине очень важно не распространять любую конфиденциальную информацию (персональные данные, фактический адрес проживания, банковские реквизиты и пр.) через подобные небезопасные каналы связи, как системы обмена мгновенными сообщениями.

Другая опасность состоит еще в том, что к подобным преступлениям часто прибегают педофилы. Их задача – собрать сведения о детях и подростках, а затем договориться с ними о реальной встрече или заставить их пойти на встречу. Педофилы зачастую представляются другими молодыми людьми, профессиональными фотографами или т.п.

Образование – это самый лучший способ защитить детей от подобного рода угроз. Посоветуйте им не общаться с незнакомцами, причем не только в онлайне, но и в обычном мире. Дети должны обладать достаточной уверенностью, чтобы быть способными открыто обсуждать с родителями или учителями свои проблемы.

Другой **потенциальный риск** в обмене мгновенными сообщениями – это инфицирование вирусами и вредоносными кодами. Почти 60% червей (вредоносные коды, которые распространяют сами себя), обнаруженных антивирусной лабораторией PandaLabs на протяжении первого полугодия, были созданы для распространения через системы обмена мгновенными сообщениями. Некоторые из них созданы для кражи паролей к онлайн-банкам. В этом случае в большей степени рискуют сами родители, потому что будут украдены их банковские данные, и, следовательно, могут пропасть их деньги.

Существуют простые способы, которые могут быть полезны для предотвращения случаев проникновения вредоносных кодов на компьютеры через системы обмена мгновенными сообщениями: не открывайте файлы и не нажимайте на ссылки, которые Вы получили через эти системы. По крайней мере, не делайте этого, пока точно не убедитесь, что человек, который их Вам прислал, является именно тем, кем он себя называет.

2. Электронная почта

Электронная почта – это другой источник опасности для молодых ребят. В этом случае также существует несколько угроз:

- Во-первых, это спам. Очень часто данный тип нежелательной почты используется для рекламы различных предложений: от казино до лекарств. Дети более подвержены доверять сообщениям, которые представлены в данных письмах, со всеми вытекающими отсюда последствиями. Они могут получить доступ к онлайн-казино и проиграть большую сумму денег, или они могут купить лекарства или даже наркотики с большим риском для своего здоровья.
- Другой риск связан с вирусами и вредоносными программами, которые могут попасть на компьютер. Как правило, они распространяются через сообщения в электронной почте, которые имеют определенную тематику (реклама новых фильмов, эротические фотографии, скачивание игр и т.д.) и предлагают пользователям нажать на ссылку или скачать файл, являющиеся причиной инфекции. Данная техника известна как «социальная инженерия». Многие взрослые люди становятся жертвами данной техники, что уж говорить про детей, которые очень легко могут стать жертвами.

Лучший способ защитить детей и подростков от этих угроз – это **научить их быть бдительными по отношению к письмам из неизвестных источников**. Они должны знать, что большинство из написанного в этих письмах является ложью, и что они никогда не должны открывать файлы или нажимать на ссылки в письмах подобного рода.

3. Программы обмена файлами

Обмен файлами в сетях является еще одним из основных источников распространения инфекций. Большинство вредоносных кодов (преимущественно, черви) копируются в папки с этими программами под заманчивыми именами (названия фильмов, программ и т.д.) для того, чтобы привлечь внимание других пользователей, которые захотят скачать эти файлы и запустить их на своих компьютерах.

По сути дела, это еще один вариант социальной инженерии: названия файлов могут быть умышленно созданы таким образом, чтобы привлечь именно детей и подростков, которые по незнанию скачают вредоносные программы на свои компьютеры.

Именно по этой причине детям следует знать, какие файлы они могут скачивать, а какие скачивать нельзя. Более того, очень хорошая идея – это **проверять каждый скаченный файл с помощью решения безопасности** до момента их первого открытия / запуска.

Если при запуске файла возникает ошибка или открывается диалоговое окно с вопросом о лицензии или предложением скачать дополнительный кодек, то подобные действия должны сразу же Вас заставить быть бдительным, потому что, скорее всего, данный файл содержит в себе вирусы или другое вредоносное программное обеспечение.

4. Социальные сети и блоги

Сайты социальных сетей (например, Facebook, MySpace, одноклассники, Вконтакте) широко используются для распространения фотографий и видео, общения с людьми и пр., так же как и блоги. В обоих случаях необходимо создавать персональный профиль для того, чтобы получить к ним доступ. Эти профили, зачастую, содержат такую конфиденциальную информацию как имя, возраст и т.д.

Детям следует постоянно напоминать, что необязательно предоставлять эту информацию, а достаточно только указать адрес электронной почты и имя, которое может быть псевдонимом. Нельзя распространять такую информацию, как возраст, адрес проживания, а также свои фотографии и видео.

Многие подростки используют блоги в качестве своих персональных дневников. Как правило, такие онлайн-журналы содержат значительно более

широкую информацию, чем следовало бы публиковать. Крайне важно предотвратить публикацию любых данных, которые могли бы идентифицировать пользователя как ребенка или подростка, а также содержать информацию о месте проживания, учебы и другую персональную конфиденциальную информацию.

Аналогично, в некоторых социальных сетях, например в MySpace, есть возможность обмениваться файлами с другими пользователями. Необходимо отдельно обратить внимание ребенка на то, какими файлами он может обмениваться с другими пользователями и кому он может разрешить просматривать эту информацию. Совсем не сложно, например, разместить свои фотографии, но защитить их паролем, который будет доступен только своим друзьям и семье.

Родителям следует знать об этих новых сервисах, а также о том, как они работают и какие риски они представляют для пользователей. Родители также должны быть способны проинструктировать своих детей о том, как использовать эти сервисы правильно и безопасно.

5. Мобильные телефоны с выходом в Интернет

Стремительное распространение сотовых телефонов во всем мире сделало их одним из основных направлений для проведения кибер-атак за последние несколько лет. Исследование показало, что такие технологии как Bluetooth (позволяет обмениваться файлами между устройствами по беспроводному каналу) и высокоскоростной доступ в Интернет сделали сотовые телефоны очень уязвимыми для атак.

В настоящее время сотовые телефоны широко используются детьми и подростками. Соответственно, они сталкиваются с точно такими же рисками, как и при использовании ПК, подключенного к Интернету.

Во-первых, сейчас широко распространены системы обмена мгновенными сообщениями для сотовых телефонов. Дети могут войти в чаты в любой момент, при этом не важно, где они находятся физически, и столкнуться с теми рисками, о которых мы подробно говорили выше: кража персональных данных, педофилы, распространение вирусов и вредоносных программ и т.д.

Спам также начинает одолевать сотовые телефоны. За последние несколько лет SMS-сообщения с рекламой всех типов продуктов и сервисов наводнили сотовые телефоны во всем мире. Большая часть подобной рекламы – это реклама порнографии. Это означает, что дети могут столкнуться с подобной информацией не только при выходе в Интернет со своего компьютера, но и при использовании собственного мобильного телефона.

В результате, родители также должны контролировать то, как дети пользуются своими сотовыми телефонами. Поэтому мы рекомендуем родителям покупать своим детям сотовые телефоны без встроенных

функций, которые могли бы подвергать их такому риску (подключение к Интернету, SMS, наличие Bluetooth и т.д.), а подросткам необходимо объяснять, как следует безопасно использовать свой сотовый телефон. Постоянно напоминайте им, чтобы они не отвечали на сообщения из подозрительных и неизвестных источников и не соглашались на встречу с незнакомцами.

II. Советы по безопасности, или Как Вы можете защитить своих детей.

1. Создайте список домашних правил Интернета при участии детей.
2. Используйте программы по защите детей в сети.

Существует ряд программ, позволяющих защитить собственного ребенка от посещения, нежелательных сайтов.

Программа «Интернет-Цензор» – Интернет—фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов.

Хотите оградить ребенка от опасных и вредных сайтов?
Используйте **бесплатное** программное обеспечение «Интернет Цензор» - это быстро и очень просто!

Программа «Интернет Цензор» предназначена для предотвращения посещения сайтов, противоречащих законодательству РФ, а также любых сайтов деструктивной направленности лицами моложе 18 лет. Программа обеспечивает родителям полный контроль за деятельностью в сети их детей. Программа надежно защищена от взлома и обхода фильтрации.

Более подробную информацию о программе, возможность бесплатно скачать программу вы можете на странице **http://www.icensor.ru/soft/**

Родителям демонстрируется работа с данной программой, показывается, как можно добавить сайт в «белый» или «черный» список.

1. Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы вы говорили о чем-то другом.
2. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
3. Позволяйте детям заходить на детские сайты только с хорошей репутацией.
4. Научите детей никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете.
5. Научите детей не загружать программы без вашего разрешения — они могут ненарочно загрузить вирус или шпионскую программу.

6. Чтобы ребенок не мог заниматься чем-то посторонним без вашего ведома, создайте для него учетную запись с ограниченными правами.
7. Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит их или угрожает. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам об этом. Похвалите их и побуждайте подойти еще раз, если случай повторится.
8. Настаивайте на том, чтобы дети предоставили вам доступ к своей электронной почте, чтобы вы могли убедиться, что они не общаются с незнакомцами.
9. Расскажите детям об ответственном поведении в Интернете. Ребята ни в коем случае не должны использовать Сеть для хулиганства, сплетен или угроз другим.

III. Обзор Интернет-ресурсов по теме: «Безопасность в сети Интернет»

Если вы обеспокоены безопасностью ребенка при его работе в Интернете или при использовании мобильной связи, если ребенок подвергся опасности или стал жертвой сетевых преследователей и мошенников, обратитесь на линию помощи «Дети онлайн». Эксперты помогут решить проблему, а также проконсультируют по вопросу безопасного использования детьми мобильной связи и Интернет;

Позвоните по телефону 8−800−25−000−15 (звонок по России бесплатный, прием звонков осуществляется по рабочим дням с 9−00 до 18−00 мск).
Или направьте Ваше письмо по адресу: helpline@detionline.com
Подробнее о Линии помощи вы можете узнать на сайте http://detionline.com

И последний мой совет Вам – будьте внимательны к своим детям!

1. **Подведение итогов (рефлексия)**

Для подведения итогов урока можно воспользоваться **упражнением «Плюс-минус-интересно».** Родителям предлагается заполнить таблицу из трех граф. В графу «П» - «плюс» записывается все, что понравилось на собрании, информация, которая, по мнению родителя, может быть ему полезна. В графу «М» - «минус» записывается все, что не понравилось, показалось скучным, вызвало неприязнь, осталось непонятным, или информация, которая, по мнению родителя, оказалась для него не нужной. В графу «И» - «интересно» родители вписывают все любопытные факты, о которых узнали и что бы еще хотелось узнать по данной проблеме, вопросы к учителю.