|  |
| --- |
| **"Кибербезопасность детей"** |
|  |
|  |
|  |

Сегодня мы не представляем свою жизнь без компьютера и сети Интернет. Интернет представляет собой открытое окно в мир, который также принадлежит взрослым и содержит материалы, не подходящие для детей, поэтому с использованием киберпространства связаны определенные риски.

Как должны родители и взрослые помочь детям избежать все возможные неприятности, чтобы сделать их пребывание в интернете более безопасным, научить их ориентироваться во всемирной сети? Простого ответа не существует. Риски могут быть разными в зависимости от возраста и компьютерной грамотности ребенка.

Конечно же, отказ от использования этих современных технологий не является решением проблемы защиты детей в онлайн-пространстве. Это все равно что запретить ездить автотранспорту по улицам и придворовым территориям, чтобы дети не попадали в ДТП. Во избежание несчастных случаев нужно лишь научить ребенка быть осторожным, соблюдать определенные правила, быть ответственным пешеходом, следовать положительному примеру взрослых. Аналогично наиболее важной задачей взрослых является предупреждение детей об опасностях Интернета, чтобы они вели себя осторожно, обдуманно. Кроме того, необходимо обсуждать с детьми все те вопросы, которые могут у них возникнуть при использовании Интернета.

Итак**, риск первый - это безопасность личной информации на собственном компьютере**, что означает защиту от вирусов, вредоносного ПО и постоянное обновление программного обеспечения. Как защитить в этом случае своих детей? Прежде всего, повысить уровень защиты данных. Это можно сделать путем использования настроек фильтра и параметров фильтрации содержимого, которые доступны во многих программах. Кроме того, велика угроза заражения вредоносным ПО. Ведь для его распространения и проникновения в компьютеры используется целый спектр методов. Чтобы избежать риска потерять личную информацию на компьютере, нужно соблюдать достаточно простые правила безопасности:

* Регулярно обновляйте операционную систему.
* Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.
* Используйте антивирусную программу, которая постоянно обновляет свои базы, и еженедельно проверяйте компьютер на наличие вирусов.
* Создавайте резервные копии важных файлов, так называемые, "бэк-апы" (например, на отдельном, только для этого и предназначенном винчестере или usb-накопителе).
* Будьте осторожны при загрузке содержимого в Интернет. Помните: после публикации информации во всемирной сети ее больше невозможно будет контролировать и удалять каждую ее копию.
* Будьте внимательны при загрузке контента из Интернета: при малейшем сомнении откажитесь от "закачки" данных на свой компьютер.
* Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п). Никому не сообщайте пароли!
* При пользовании интернетом на чужом устройстве, не сохраняйте пароли и не забывайте выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы.
* Объясните все эти правила своим детям!

**Риск второй - это доступ к нежелательному содержимому.**

Это может быть насилие, наркотики, порнография, страницы, подталкивающие к самоубийствам, отказу от приема пищи, убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна содержащие любую информацию, чаще всего порнографического характера.

Такая информация часто бывает заманчивой и может оказывать сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл происходящего и отказаться от просмотра и изучения сайтов с подобным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков непредсказуемо; под впечатлением от таких сайтов дети могут пострадать не только в эмоциональном плане, но также прямой урон может быть нанесен и их физическому здоровью.

Уберечь детей от данной нежелательной информации поможет настройка контентной фильтрации с помощью дополнительных функций антивирусных программ, интернет-браузеров или установки специального программного обеспечения, например, Родительского контроля в Windows Vista или средств Родительского контроля, встроенных в Kaspersky Internet Security.

Если компьютером пользуются и взрослые, то для ребенка лучше создать отдельную учетную запись пользователя, в которой настраивается фильтрация и родительский контроль. При этом вы будете выполнять функции администратора (отдельная учетная запись): вы сможете контролировать системные настройки и устанавливать новое программное обеспечение, ограничивая в таких правах других пользователей компьютера. Не забывайте создавать для работы надежные и защищенные пароли.

Рекомендации:

1. ***Установите компьютер в общей для всей семьи комнате***

В этом случае разговор об Интернете и наблюдение за его использованием станет естественным в повседневной жизни. Обсуждение проблем может стать проще, если компьютер находится в общей комнате. Кроме того, Интернетом можно пользоваться вместе.

1. ***Обсуждайте Интернет***

Проявляйте интерес к действиям ребенка и его друзей как в Интернете, так и в реальной жизни. Расскажите ребенку о прекрасных и увлекательных вещах, которые возможны в Интернете, а также о трудностях, с которыми можно столкнуться. Обсудите с ребенком действия, которые необходимо предпринять, если чувствуется неловкость в какой-либо ситуации в Интернете.

1. ***Узнайте больше об использовании компьютера***

Если вы сами являетесь пользователем Интернета, вам будет проще определить правильную тактику для детей и помочь им найти в Интернете полезный материал. И тем не менее, постоянно повышайте собственный уровень компьютерной грамотности, чтобы знать, как обеспечить безопасность детей (например, посещение курсов, чтение специальной литературы, консультации с экспертами). И регулярно знакомьте всех членов вашей семьи с базовыми принципами безопасной работы на компьютере и в Интернете.

1. ***Используйте Интернет вместе***

Найдите сайты, которые подходят для детей, или узнайте о способах поиска полезной информации: запланируйте совместную туристическую поездку, просмотрите образовательные сайты для помощи в школьных заданиях или найдите информацию об увлечениях детей. Просматривая веб-сайты в Интернете вместе, можно также помочь ребенку оценить значимость найденной информации. Можно добавить любимые сайты в папку «Избранное», чтобы совместно просмотренные ранее веб-сайты можно было открыть одним щелчком мыши.

1. ***Договаривайтесь с ребенком о способе и времени использования Интернета***

Может оказаться полезным согласовать с ребенком время, которое он проводит за компьютером, а также список веб-сайтов, которые он может посещать. Это необходимо обсудить с детьми и прийти к определенному решению, которое всех устраивает.

1. ***Установите доверительные отношения с ребенком***

Это поможет избежать последствий столкновения ребенка с негативным опытом в Интернете. Положительный эмоциональный контакт ребенка с родителями поможет расположить его к трудному разговору о том, что произошло. Ребенок должен вам доверять и понимать, что вы тоже обеспокоены и хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.