

Информационно-методические материалы

«Как защитить старшего школьника от негативного контента в сети Интернет»

Почему возникает необходимость контролировать ребенка в интернете?

По данным различных исследований дети сейчас активно пользуются интернетом и проводят много времени в сети, часто бесконтрольно. При этом они не задумываются о мерах безопасности, мало знают о средствах защиты в интернете. Часто из-за природной любознательности или случайно попадают на сайты с потенциально опасным содержанием. Старшие школьники, как правило, поддаются рекламным трюкам. Сообщают сведения личного характера о себе и родителях, контактную информацию, готовы продолжить онлайн общение в реальной жизни.

В силу всех этих причин дети часто становятся жертвами преступлений. По сведениям МВД России, число сайтов, содержащих материалы с детской порнографией, увеличилось почти на треть, а количество самих интернет-материалов – в 25 раз. Значительное число сайтов, посвященных суицидам, доступно подросткам в любое время. По информации Генеральной прокуратуры РФ в 2012 году более 93 тыс. детей стали жертвами преступлений.

Безопасность вашего ребенка в интернете – это ваша зона ответственности.

Очевидную опасность представляют:

- сайты порнографической направленности;
- наркосайты;
- сектантские сайты;
- суицид-сайты;
- сайты, разжигающие национальную рознь и расовое неприятие (экстремизм, национализм, фашизм);
- сайты знакомств и др.

Программная реализация набора ограничений при работе детей в сети Интернет носит название «Родительский контроль».

Как установить родительский контроль?

Возможны следующие варианты родительского контроля:

- блокировка (полное закрытие доступа к ресурсу),
- мониторинг (отслеживание посещаемых страниц и запускаемых программ),
- ограничение по времени игры или по запуску определенных приложений.

Разные способы этого контроля предлагают:

- операторы (Билайн, Мегафон, МТС);
- создатели антивирусного ПО (Лаборатория Касперского, AVAST, ESET с пятой версии);
- операционные системы (Windows 7, Windows 8);
- производители специальных программ родительского контроля («Интернет Цензор», NetKids, NetPolice, KidGid, Content Keeper Express, Гоголь, «Кибермама» и др.).

Программные системы сопровождаются подробными иллюстрированными инструкциями, поэтому установка их на компьютер не составляет труда. Достаточно иметь отдельные учетные записи для входа в компьютер: у вас – с правами администратора, у ребенка – с правами пользователя. При этом, как правило, в программах есть возможность выбирать уровни защиты и настроить под свои потребности. Так, минимальный уровень защищает компьютер или планшет от порнографии и угроз безопасности, высокий – от всего «взрослого» содержания, нелегальной деятельности и неизвестных сайтов. Блокировка по времени закрывает доступ к любым сайтам. К примеру, компьютер блокируется с 20:00 до 08:00. Можно установить часы доступа отдельно для каждого дня недели. По истечении положенного времени система завершит работу компьютера автоматически. У мобильных операторов родительский контроль подключается как отдельный тариф через USSD-команду.

Определенные минусы и неудобства у систем родительского контроля тоже есть. Например, при установке максимального фильтра может оказаться закрытым доступ ко многим полезным

ресурсам, просто потому что их нет в основном каталоге системы. При этом и сам ребенок, как правило, ставится в известность, что доступ заблокирован. Такой факт может быть негативно принят вашим ребенком. Возможный выход из ситуации – предварительная беседа с ребенком о важности и пользе систем контроля.

О чем важно беседовать с ребенком?

Обойти все системы контроля при желании ребенок, конечно, сможет. Правильное отношение к проблеме безопасности и грамотное поведение ребенка в сети нужно поддерживать объяснениями плюсов и минусов сети, обсуждением следующих вопросов: какие риски существуют в интернете, какие способы добывания информации используют мошенники, как научиться отличать правду от лжи и т.п. То есть запреты нужно уравнивать профилактикой и объяснениями так, чтобы решение о собственной защите ребенок принимал сам.

Родители должны знать, какие сайты посещает ребенок, в каких социальных сетях он зарегистрирован, в какие онлайн игры он играет, с кем общается в сети.

Убедитесь, что профиль вашего ребенка закрыт. Личные данные должны быть доступны только друзьям, а безопаснее всего вообще не публиковать их в интернете.

Выясните, не спрашивают ли у вашего ребенка: «Сколько зарабатывают твои родители?», «Когда семья собирается в отпуск?».

Узнайте, сколько лет его друзьям в социальных сетях. Обратите внимание на грубые высказывания, на угрозы, на общение с незнакомыми людьми.

Узнайте, чем интересуется ребенок. Убедитесь, что его интересы в сети не опасны.

Научите базовым *правилам поведения*:

- нельзя обсуждать личную жизнь с незнакомыми в реальной жизни людьми (номера телефонов, место жительства, профессия и график работы родителей, наличие ценных вещей и т. д.),
- нельзя выкладывать все фотографии или пересылать их по чьей-либо просьбе,
- нельзя поддерживать онлайн споры и скандалы, поддаваться на провокации и тем более встречаться лично, чтобы «разобраться»,
- нельзя верить любой рекламе и заказывать/покупать что-либо без согласования с родителями,
- нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям,
- нельзя играть в сетевые азартные игры (Федеральный закон от 29.12.2006 № 244-ФЗ (ред. от 23.07.2013)),
- ни при каких обстоятельствах нельзя сообщать пароли даже близкому другу.

Установите правила, сформулируйте договоренности с ребенком и строго следите за их выполнением. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом.

Полезные ссылки:

1. <http://www.rg.ru/2010/12/31/deti-inform-dok.html> - текст федерального закона РФ "О защите детей от информации, причиняющей вред их здоровью и развитию"

2. <http://www.internet-kontrol.ru/> - ресурс «Защита детей от вредной информации в сети интернет».

3. <http://www.microsoft.com/ru-ru/security/family-safety/cyberbullying.aspx> - информация о киберугрозах от корпорации «Майкрософт»

4. http://www.kaspersky.ru/keeping_children_safe - Меры защиты детей в интернете («Лаборатория Касперского»).