

Методические рекомендации педагогам, родителям, учащимся по предотвращению компьютерной зависимости у детей и подростков

В настоящее время Интернет предлагает колоссальное количество возможностей для обучения, жизнь без Всемирной паутины сейчас сложно представить. Посмотреть мультик, скачать фильм, прочитать статьи, поиграть в игры, найти ответ на любой вопрос – возможности безграничны. Конечно, информационные технологии дают нам большие возможности, но вместе с этим могут прийти и большие проблемы. С каждым днем информации в интернете все больше, становится все труднее отсеивать ненужное, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. Сейчас дети практически живут в интернете. Интернет таит в себе множество опасностей для детей.

Существует множество сайтов, пропагандирующих порнографию, проституцию, насилие, войны, межнациональную и религиозную рознь, употребление наркотиков и алкоголя, различные виды мошенничества.

Самым опасным возрастом считается подростковый период. Среди подростков популярны такие ресурсы, как «ВКонтакте», Google, Yandex, YouTube, Instagram, Likee, Tiktok.

Опасность поджидает во время использования интернета не только с ПК, но и со смартфона. Некоторые гаджеты достаточно восприимчивы к вирусам. В девайс вирус может попасть не только при скачивании какой-либо программы.

При таком обилии информации возникает вопрос: как обезопасить детей от нежелательного контента?

Тема кибербезопасности детей требует постоянной совместной работы педагогов и родителей, поэтому так важно повышать грамотность в этой сфере. Об этом должен знать каждый педагог и каждый родитель.

Запреты и жесткий контроль не помогут оградить детей от всех опасностей в интернете. Необходимо вместе с ребенком изучать основы безопасной работы в интернете, чтобы он сам понимал, какие риски могут иметь посещение подозрительных сайтов или общение с незнакомцами.

Правила безопасной работы в интернете

1. Не разглашать тайны. Нельзя раздавать свои персональные данные всем подряд (Ф.И.О, адрес, номера документов). Делать это можно только на официальных государственных сайтах с защищенным соединением (слева от адреса сайта будет значок навесного замка).

2. Замечать поддельные сайты. Фишинг – способ выманивания у человека данных (логина, пароля). Фарминг – процедура скрытного перенаправления жертвы на ложный IP-адрес. Перед тем как перейти по ссылке сайта, изучите ее: часто адрес поддельного сайта похож на настоящий

(например, vk-vk.com, вместо vk.com). Если ввести данные на таком сайте, они становятся известны злоумышленнику.

3. Распознавать злоумышленников. Беспокоиться о безопасности можно в следующих случаях:

- в реальной жизни ребенок не знаком с этим человеком;
- собеседник в разы старше ребенка;
- у собеседника очень мало друзей в соцсети, он зарегистрирован недавно;
- собеседник настоятельно требует фото, какие-либо данные и др.

4. Придумывать разные пароли. Использовать один пароль для всех сайтов – не самое разумное решение. Они должны быть уникальны к каждому сайту. Не используйте в качестве пароля дату рождения, имя любимой кошки, свою фамилию. Добавьте цифр и спецсимволов. Все пароли желательно записывать в блокнот (а лучше держать в голове). Воспользуйтесь менеджером паролей – это программное обеспечение, которое помогает пользователю работать с паролями и PIN-кодами от нескольких аккаунтов.

Советы родителям, как сделать прогулки ребенка в Интернете более безопасными

Конечно же, никто так сильно не отвечает за безопасность детей в Интернете, как сами родители. Ведь только родители могут полностью контролировать своих детей. Не бойтесь пускать детей одних на улицу, бойтесь пускать в интернет!

Избавить ребёнка полностью от гаджетов сегодня невозможно. Минимум, что может сделать родитель, это тщательно следить за контентом и уметь ставить чёткие правила пользования Интернетом. Их необходимо обсудить на родительском собрании:

1. Ограничить время проведения в сети.
2. Использовать средства обеспечения безопасности (антивирусная программа, настройки безопасного поиска, безопасный режим в соцсетях, использовать контентные фильтры).
3. Подключить у провайдера услугу «Детский Интернет».
4. «Родительский контроль». С помощью этой функции в системе Windows можно регулировать использование компьютера детьми.
5. Установить бесплатную программу «Интернет Цензор». Она блокирует сайты, на которые вы не хотите, чтобы заходили с вашего компьютера.
6. Следить, чтобы ребёнок смотрел программы/фильмы с соответствующей маркировкой по возрасту (0+, 6+, 12+, 16+, 18+).
7. Объяснять детям, что не всё то, что пишут в Интернете – правда. Рассказать, в чём опасность «всемирной паутины».
8. Донести до ребёнка, что нельзя где-либо при регистрации указывать реальные имя и фамилию. Помогите юному пользователю подобрать надёжный логин.
9. Мониторить друзей и подписчиков ребёнка в соцсетях (нет ли среди них взрослых людей, незнакомых ребят с другой школы/города/района).
10. Объяснить, что онлайн-друзья могут отличаться при встрече. И пусть онлайн-дружба такой и остаётся (по крайней мере для младших школьников).
11. Быть внимательными к ребёнку. Убедитесь, что он не жертва интернет-буллинга. Если у ребёнка в подписках нет друзей, то, возможно, он удалил их именно потому, что подвергся издёвкам со стороны.
12. Слушать и поддерживать ребёнка в любой ситуации. Проводите больше совместного времени. Старайтесь вместе читать и рассуждать над прочитанным. Отдавайте предпочтение активным играм, чем нахождению в четырёх стенах.
13. Рассказать, что нельзя скачивать файлы, полученные от незнакомых пользователей.
14. Вводить компьютерные игры следует только после формирования игровой и творческой деятельностью, то есть после 6 лет. До этого времени малыш может вполне обойтись без виртуального мира.
15. Помните, что до 7 лет ребёнку не нужен Интернет. Младшим школьникам достаточно 30 минут в день, по мнению педиатров. В 10-12 лет ребёнок может проводить в Интернете не более 1 часа. Старше 12 – не более 1,5 часа.

15. Кроме того, родители тоже должны с осторожностью использовать свои социальные сети. Очень часто взрослые размещают в своём аккаунте фото и видео своих детей. У каждого для этого свои цели: кто-то хочет поделиться с онлайн друзьями фотографиями своих малышей, кто-то использует их для продвижения своего профиля (например, блогеры). В любом случае это большая информационная база для мошенников.

16. Научить детей проверять найденную информацию по другим источникам и разным способам поиска.

17. Поговорить с детьми о недопустимости вражды между людьми и о расизме, убедить их уважать верования других людей.

18. Разъяснить детям нежелательность использования ненормативной лексики, соблюдать определенный этикет.

19. Не разрешать личных встреч с новыми знакомыми из Интернета без вашего одобрения.