Приложение

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 замка́).

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.